

Features - Image Level ProxyHost iDataAgent

TABLE OF CONTENTS

OVERVIEW

SYSTEM REQUIREMENTS - IMAGE LEVEL PROXYHOST /DATAAGENT

INSTALLATION

- Install the Image Level ProxyHost iDataAgent
- Install the Image Level ProxyHost iDataAgent - Unix

BACKUP DATA - IMAGE LEVEL PROXYHOST /DATAAGENT

RESTORE DATA - IMAGE LEVEL PROXYHOST /DATAAGENT

CONFIGURATION

- Subclients - Image Level ProxyHost iDataAgent

MANAGEMENT

- Backup Job History
 - Restore Job History
-

Overview - Image Level ProxyHost iDataAgent

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 Image Level ProxyHost iDataAgent](#)
 - [License Requirement](#)
 - [Snapshot Support](#)
 - [LAN Copy Manager](#)
 - [Disaster Recovery Considerations](#)
-

INTRODUCTION

Unlike the file system iDataAgent which backs up folders and files, the Image Level ProxyHost iDataAgent backs up complete volumes or mount points, and restores them using Volume Level Restore; for certain operating systems it is also able to restore folders and files using a File Level Restore. Generally, only blocks that contain data are backed up; empty blocks are not, with the following notes:

- For FAT16/FAT32 volumes, all blocks on a drive are backed up, even if the blocks contain no data.
- For Image Level on Unix, this functionality can be turned off, so that even the empty blocks are backed up, by configuring the `dDisableDataBlock` registry key.

The Image Level ProxyHost iDataAgent enables the use of third party vendors' split mirrors and snapshot technology to greatly reduce the effects of backup operations on the production server. This iDataAgent can use third party software to create a point-in-time copy of the production server data mounted on to the backup host and the backup is started from this secondary host. The Image Level ProxyHost software performs the following functions:

- Utilizes user defined batch files to perform necessary system operations (e.g., snapping the BCV) prior to backing up the data
- Coordinates the backup functions on the backup host
- Provides path translation, which allows data to be browsed as it appears within the more familiar production server file system, rather than as it appears within the backup host file system. For example, assume that `D:\` on the production server is mirrored by `J:\` on the backup host. Although the `folder1\files` directory is actually backed up from the backup host as `J:\folder1\files`, it appears in the browse view as `D:\folder1\files`, just as it appears on the production server.

The Image Level ProxyHost iDataAgent is installed on the production server only, but the same File System iDataAgent (i.e., Windows File System) and Image Level iDataAgent must be installed on both the production server and backup host.

SUPPORTED DATA TYPES

The following file system types are supported for backup and restore operations:

IMAGE LEVEL PROXYHOST ON WINDOWS

- File Allocation Table (FAT) file systems - Volume Level Restore only
- New Technology File Systems (NTFS) - both Volume Level and File Level Restores
- RAW volumes - Volume Level Restore only

It is possible to restore data from one file system type to another through Volume Level Restore. The following such Volume Level Restores are supported:

- NTFS ==>> FAT
- NTFS ==>> RAW
- FAT ==>> RAW

After such a restore, sometimes Windows Explorer may still show the volume having the same file system type as before the restore, even though Computer Management shows the new (correct) type. After a reboot, Windows Explorer will show the correct file system type. For File Level Restores, only data backed up from NTFS volumes can be browsed and restored to NTFS or FAT volumes.

IMAGE LEVEL PROXYHOST ON UNIX

The following table lists the file systems and restore types supported by the Image Level ProxyHost iDataAgent for Unix, for each supported operating system:

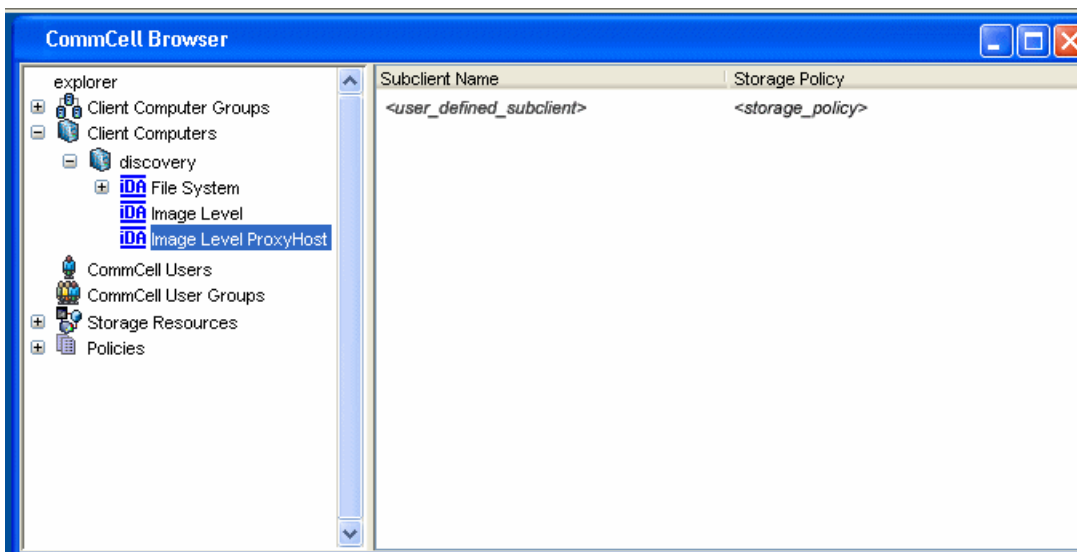
The following table lists the file systems and restore types supported by the Image Level iDataAgent for Unix, for each supported operating system:

File System	Operating System	Back Up Data Blocks Only	Volume Restore	File Restore
Unix File System (UFS) Includes read-only partitions on Unix, as long as the production server and backup host are configured as the same computer	Solaris	X	X	X
Extent 2 File System (ext2)	Linux	X	X	X
Extent 3 File System (ext3)	Linux	X	X	X
VERITAS File System (VxFS)	Solaris		X	
Veritas Volume Manager (VxVM 3.1 and 3.5)	Solaris	X	X	

- The Unix QSnap® (cxbf) driver does **not** support volumes created by Solaris Volume Manager.
- When volumes are backed up using Image Level ProxyHost, sharing attributes for volumes and folders are not retained.
- The Image Level and Image Level ProxyHost iDataAgents on Unix can perform a File Level Restore only when the OS of the Client computer and the MediaAgent are the same.

TREE LEVELS IN THE IMAGE LEVEL PROXYHOST iDATAAGENT

When the Image Level ProxyHost iDataAgent is installed, the following levels are automatically created in the CommCell Browser:



discovery: Client

<user_defined_subclient>: User-defined subclients

Image Level ProxyHost: Agent

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.

SNAPSHOT SUPPORT

The Image Level ProxyHost iDataAgent is designed to work in conjunction with the following snapshot engines, which provide snapshot functionality for data protection operations:

- QSnap for the Image Level ProxyHost iDataAgents

For more detailed snapshot support information, refer to [Support Information - Snapshot Engines](#).

LAN COPY MANAGER

The Image Level ProxyHost iDataAgent uses LAN Copy Manager to read block-level data directly from the specified volume(s) on the backup host and transmit it to the specified MediaAgent (which can be installed on the same machine, thus avoiding LAN use.) For more information, see [Copy Managers](#).

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.

[Back to Top](#)

System Requirements - Image Level ProxyHost iDataAgent

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

The following requirements are for the Image Level ProxyHost iDataAgent:

If using this Agent with a snapshot engine, refer to [System Requirements- Image Level ProxyHost iDataAgent - Snapshots Support](#) information on the operating system vendors supported for each snapshot engine with this Agent.

OPERATING SYSTEM		PROCESSOR
LINUX	RED HAT ENTERPRISE LINUX	
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-78 (Update 7)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-67 (Update 6)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-55 (Update 5)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-42 (Update 4)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux AS 4.0 with kernel 2.6.9-34 (Update 3)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 6 Advanced Platform with kernel 2.6.32-71	x64
	Red Hat Enterprise Linux 6 Advanced Platform with kernel 2.6.32-71	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-92 (Update 2)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-8	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-53 (Update 1)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-238 (Update 6)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-238 (Update 6)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-194 (Update 5)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-194 (Update 5)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-164 (Update 4)	Intel Pentium or compatible minimum required
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-164 (Update 4)	x64
	Red Hat Enterprise Linux 5 Advanced Platform with kernel 2.6.18-128 (Update 3)	Intel Pentium or compatible minimum required
	SUSE LINUX (SLES)	
	SuSE Linux 11 Enterprise Server with kernel 2.6.32.12-0.7 (Update 1)	Intel Pentium or compatible minimum required
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.21 (Update 2)	Intel Pentium or compatible minimum required
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.46-0.12 (Update 1)	Intel Pentium or compatible minimum required
SOLARIS	Solaris 9 with a minimum of Service Packs 111711-02	Sparc5 or higher recommended
	Solaris 10.x	Sparc5 or higher recommended
WINDOWS	WINDOWS 2008	
	Microsoft Windows Server 2008 R2 Editions*	All Windows-compatible processors supported
	*Core Editions not supported	

Microsoft Windows Server 2008 32-bit and x64 Editions*

All Windows-compatible processors supported

WINDOWS 2003

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

All Windows-compatible processors supported

HARD DRIVE

LINUX AND SOLARIS

240 MB minimum of hard drive space for software

100 MB of additional hard disk space for log file growth

10 MB of temp space required for install or upgrade (where the temp directory resides)

WINDOWS

116 MB minimum of hard disk space for software/ 549 MB recommended

50 MB of additional hard disk space for log file growth

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

MEMORY

WINDOWS

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

LINUX AND SOLARIS

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

Swap space = 2*RAM size

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.

PERIPHERALS

DVD-ROM drive

Network Interface Card

Fiber Channel card (HBA) if the data to be protected resides on SAN-attached volumes

MISCELLANEOUS

The File System iDataAgent will be automatically installed during installation of this software, if it is not already installed. For System Requirements specific to the File System iDataAgent, refer to System Requirements - Microsoft Windows File System iDataAgent.

On Solaris computers, the operating system must have been installed with at least the `user level software` option selected.

NETWORK

TCP/IP Services configured on the computer.

NET FRAMEWORK

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

MICROSOFT VISUAL C++

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

SELINUX

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

package must be installed on the client.

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

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

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

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

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

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

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

SELinux is now configured to work with this application.

DISCLAIMER

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

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

Install the Image Level ProxyHost iDataAgent - Windows

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Cluster Selection
- Select Components for Installation
- Configuration of Other Installation Options
- Download and Install Latest Packs
- Client Group Selection
- Schedule Automatic Update
- Storage Policy Selection
- Configure QSnap
- Verify Summary of Install Options
- Install Remaining Cluster Nodes
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the Image Level ProxyHost iDataAgent and the QSnap snapshot enabler on both cluster and non-clustered environment.

The Image Level ProxyHost iDataAgent is installed on the computer from which the iDataAgent secures data. (This computer is referred to as the *Client* computer in this install procedure.) In addition, the Image Level iDataAgent must be installed on the Client computer.

Verify that the computer in which you wish to install the software satisfies the minimum system requirements; refer to System Requirements - Image Level ProxyHost iDataAgent and System Requirements - Image Level iDataAgent.

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.

CLUSTER SPECIFIC

- Before you can install this Agent in the cluster group in a clustered environment, you must first install QSnap on all physical nodes of the cluster. Install QSnap - Windows provide step-by-step instructions for installing these components on physical nodes.
- Once the Windows File System iDataAgent and QSnap are installed on all physical nodes in the cluster, the Image Level ProxyHost iDataAgent and Windows File System iDataAgent can be installed from the active node in the cluster group using the following procedure. The software can also be automatically installed on all available passive nodes when the software is installed in the cluster group, or you can choose to install any passive node(s) separately.
- Check the following on the cluster computer in which you wish to install the software:
 - Cluster software is installed and running.
 - Active and passive nodes are available.
 - Disk array devices configured with access to the shared array.
 - Public Network Interface Card is bound first, before the private Network Interface Card. (Does not apply to NetWare Cluster.)

BEFORE YOU BEGIN

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

INSTALL PROCEDURE

GETTING STARTED

1. 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**.

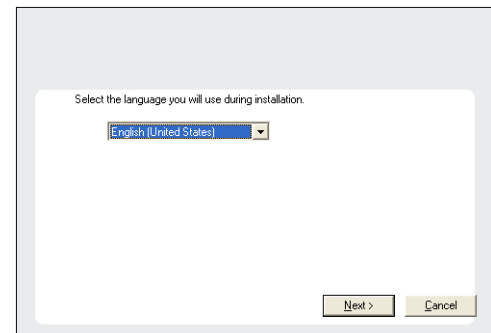
2. Place the Software Installation Disc for the Windows platform into the disc drive.
After a few seconds, the installation program is launched.

If the installation program does not launch automatically:

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

NOTES

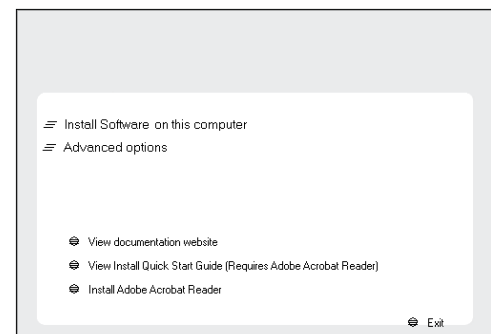
- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.
3. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



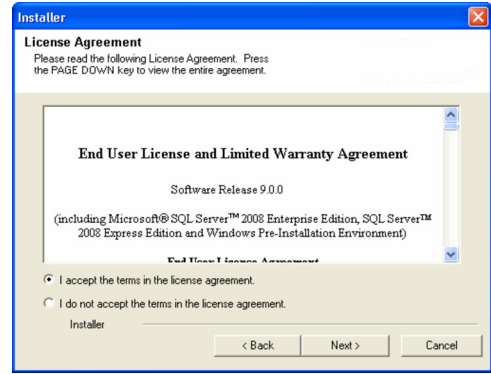
4. Select the option to install software on this computer.

NOTES

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

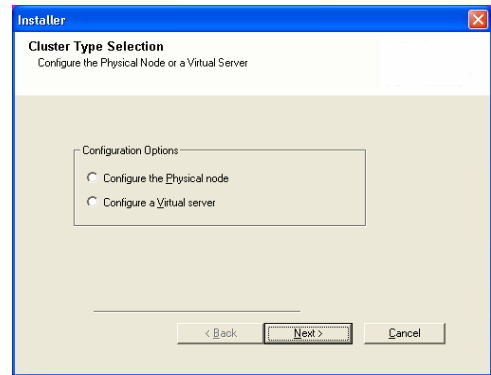


5. Read the license agreement, then select **I accept the terms in the license agreement**.
Click **Next** to continue.

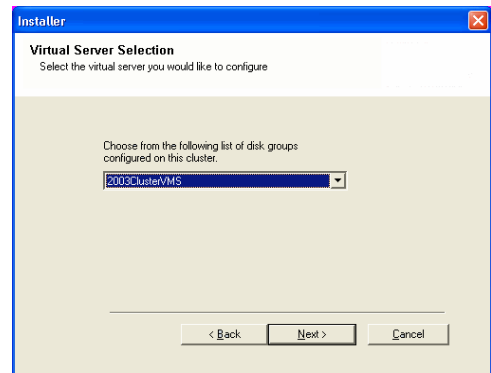


CLUSTER SELECTION

6. Select **Configure a Virtual Server**.
Click **Next** to continue.



7. Select the disk group in which the cluster group resides.
Click **Next** to continue.



SELECT COMPONENTS FOR INSTALLATION

8. Select the component(s) to install.

NOTES

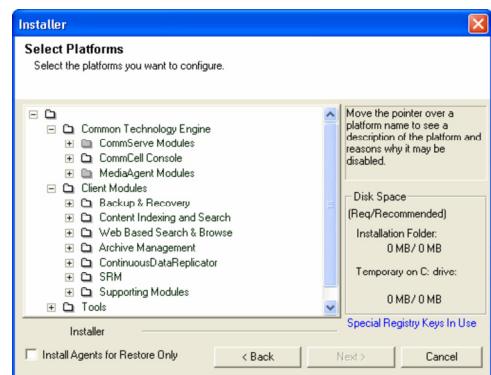
- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
- If you wish to install the agent software for restore only, select **Install Agents for Restore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

Click **Next** to continue.

To install the Image Level ProxyHost iDataAgent, expand the following `Client Modules` folder, `Backup & Recovery` folder and `File System` folder. Then select the following:

- Image Level ProxyHost iDataAgent

When you select the Image Level ProxyHost iDataAgent for installation, the



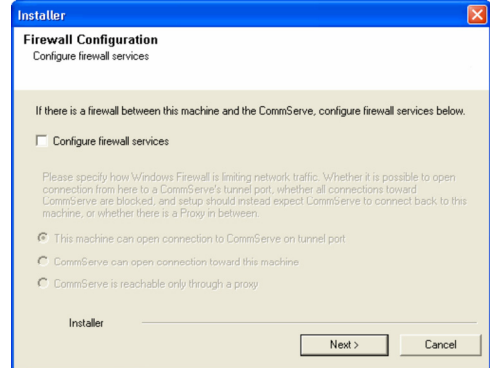
appropriate Windows File System iDataAgent, the QSnap snapshot enabler, and the Image Level iDataAgent are automatically selected for installation.

CONFIGURATION OF OTHER INSTALLATION OPTIONS

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

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

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

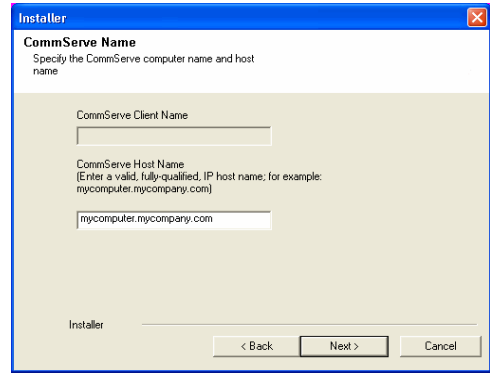


- Enter the fully qualified domain name of the CommServe Host Name. This should be TCP/IP network name. e.g., computer.company.com.

NOTES

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

Click **Next** to continue.

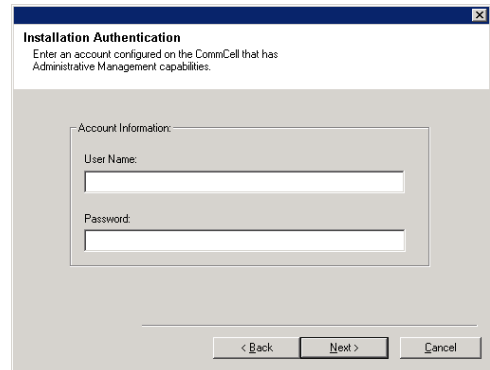


- Enter the **username** and **password** associated with an external domain user account or a CommCell user account to authorize the installation of this agent.

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.

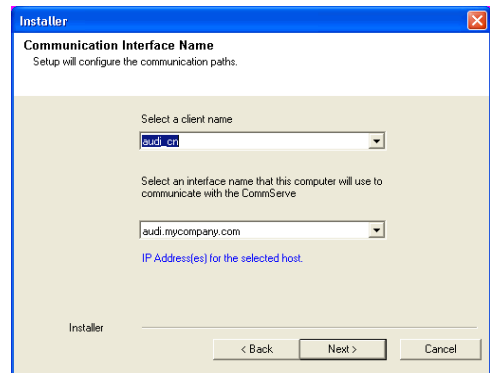


- Enter the following:
 - The local (NetBIOS) name of the client computer.
 - The TCP/IP IP host name of the NIC that the client computer must use to communicate with the CommServe Server.

NOTES

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

Click **Next** to continue.



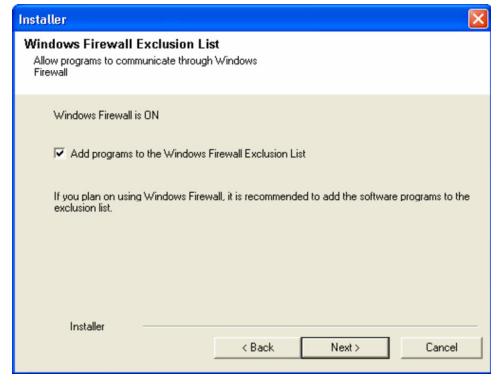
- Select **Add programs to the Windows Firewall Exclusion List**, if you wish to add CommCell programs and services to the Windows Firewall Exclusion List.

NOTES:

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

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

Click **Next** to continue.



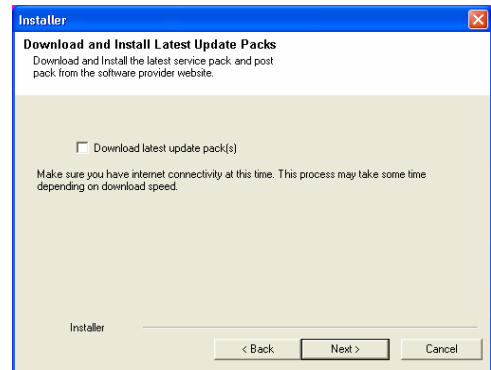
DOWNLOAD AND INSTALL LATEST PACKS

14. Select **Download latest update pack(s)** to automatically download and install the latest service packs and/or post packs if applicable at the end of this agent install.

NOTES

- Internet connectivity is required to download updates.
- Updates are downloaded to the following directory:
<software installation>/Base/Temp/DownloadedPacks.
They are launched silently and installed automatically for the first instance.

Click **Next** to continue.



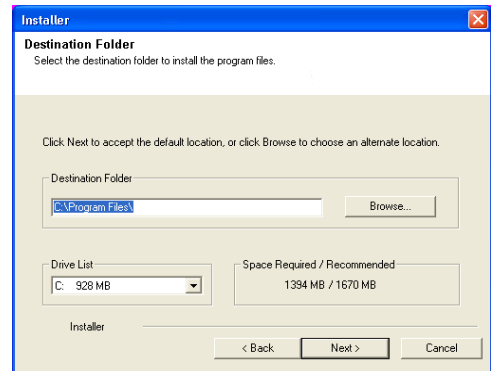
15. Specify the location where you want to install the software.

NOTES

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

Click **Browse** to change directories.

Click **Next** to continue.



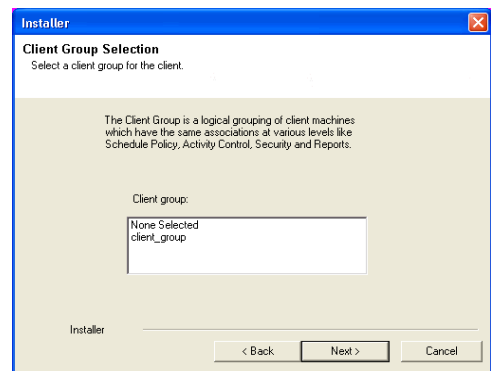
CLIENT GROUP SELECTION

16. Select a Client Group from the list.

Click **Next** to continue.

NOTES

- This screen will be displayed if Client Groups are configured in the CommCell Console. For more information, see [Client Computer Groups](#).



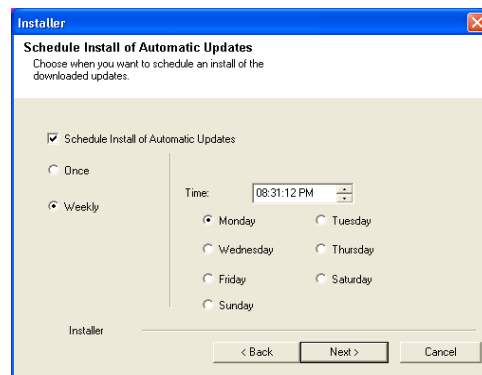
SCHEDULE AUTOMATIC UPDATE

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

NOTES

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

Click **Next** to continue.



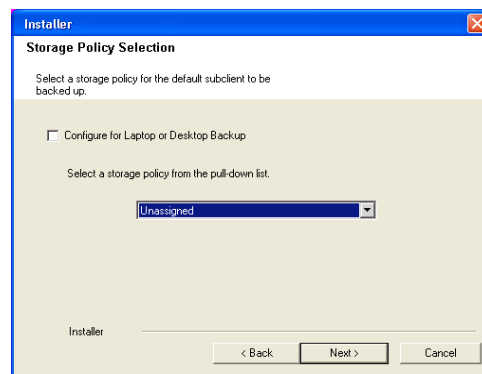
STORAGE POLICY SELECTION

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

NOTES

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

Click **Next** to continue.



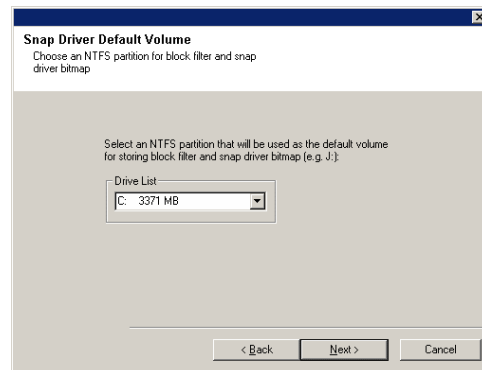
CONFIGURE QSNAP

- From the drop-down list, select an NTFS partition that will be used as the default volume for bitmap file storage.

NOTES

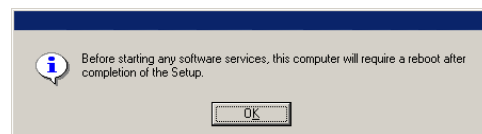
- For standard installation, you can select any available NTFS formatted drive as the default volume for bitmap file storage.
- For cluster installation, the default location for storing the bitmap file is the corresponding shared volume. After the installation is complete, see Change the QSnap Bitmap Location for step-by-step instructions on changing the bitmap location.
- Only NTFS volumes will be shown in the drop-down list.

Click **Next** to continue.



- Setup reminds you that the computer must be restarted, after the installation completes, before you can use this Agent.

Click **OK** to continue.



VERIFY SUMMARY OF INSTALL OPTIONS

- Verify the summary of selected options.

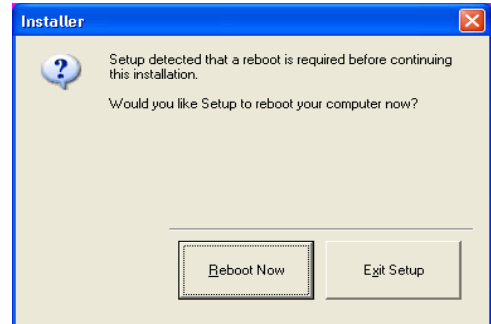
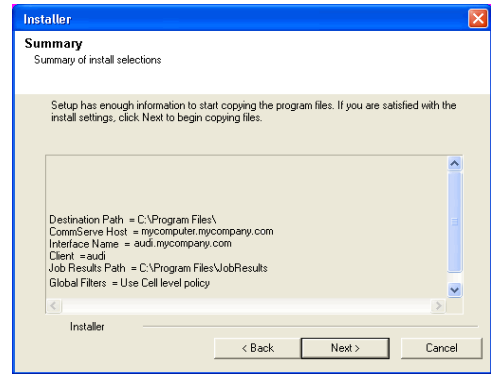
NOTES

- 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.

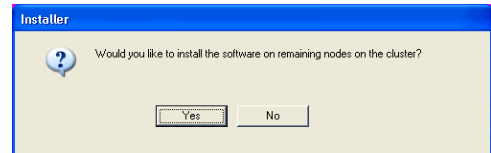
The install program now starts copying the software to the computer. This step may take several minutes to complete.

22. The System Reboot message may be displayed. If so, select one of the following:
- **Reboot Now**
If this option is displayed without the **Skip Reboot** option, the install program has found files required by the software that are in use and need to be replaced. If **Reboot Now** is displayed without the **Skip Reboot** option, reboot the computer at this point. The install program will automatically continue after the reboot.
 - **Exit Setup**
If you want to exit the install program, click **Exit Setup**.



INSTALL REMAINING CLUSTER NODES

23. To install/upgrade the software on the remaining nodes of the cluster, click **Yes**.
To complete the install for this node only, click **No**.

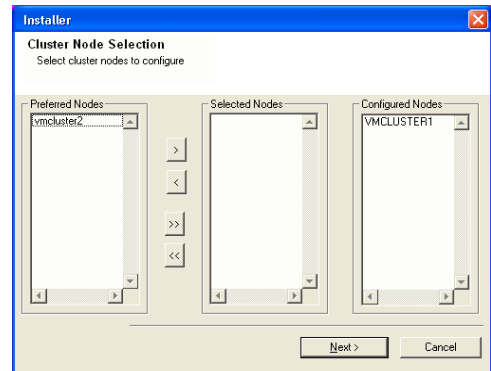


24. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

NOTES

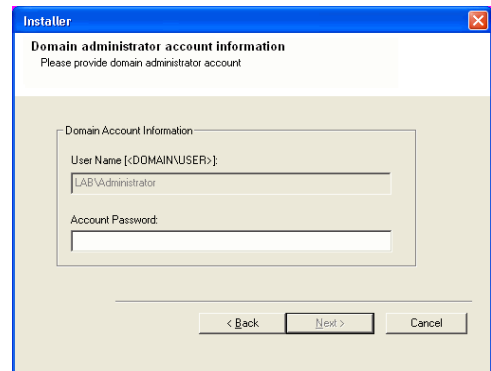
- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed. For more information, see Multi Instancing.

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



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

Click **Next** to continue.



26. The progress of the remote install for the cluster nodes is displayed; the install can be

interrupted if necessary.

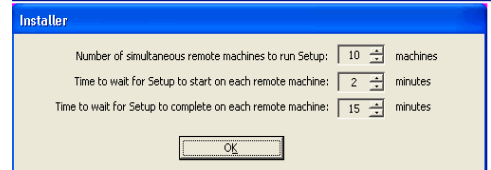
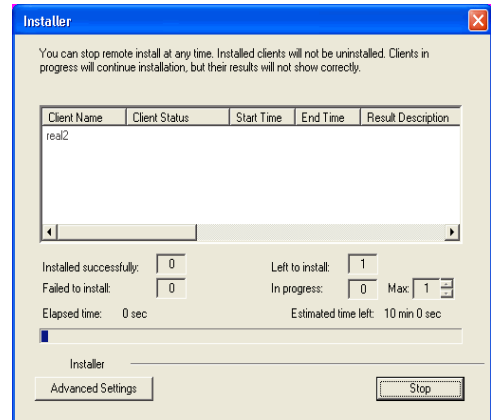
Click **Stop** to prevent installation to any nodes after the current ones complete.

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

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

NOTES

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

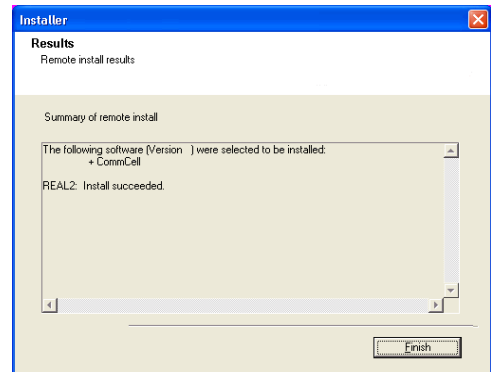


27. Read the summary for remote installation to verify that all selected nodes were installed successfully.

NOTES

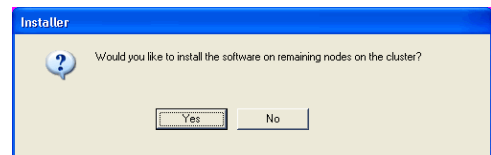
- If any node installation fails, you must manually install the software on that node once the current installation is complete. (See Manually Installing the Software on a Passive Node for step-by-step instructions.)
- The message displayed on your screen will reflect the status of the selected nodes,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

Click **Next** to continue.



INSTALL REMAINING CLUSTER NODES

28. To install/upgrade the software on the remaining nodes of the cluster, click **Yes**. To complete the install for this node only, click **No**.

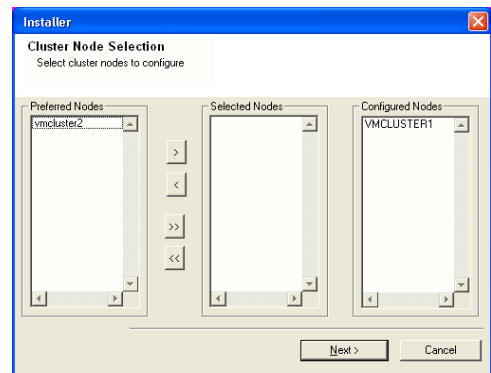


29. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

NOTES

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

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



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

Click **Next** to continue.

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

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

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

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

NOTES

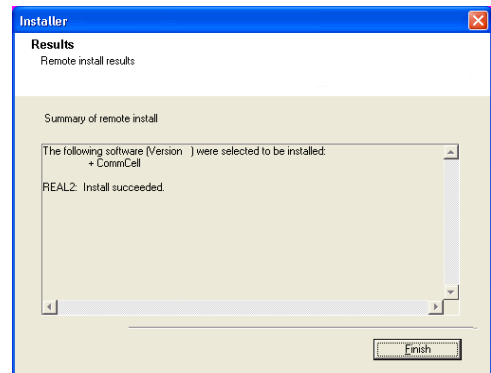
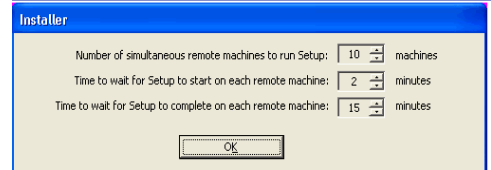
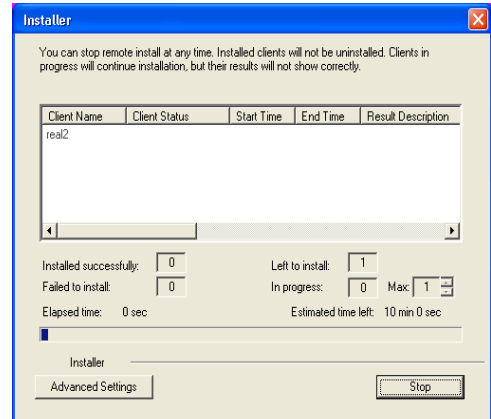
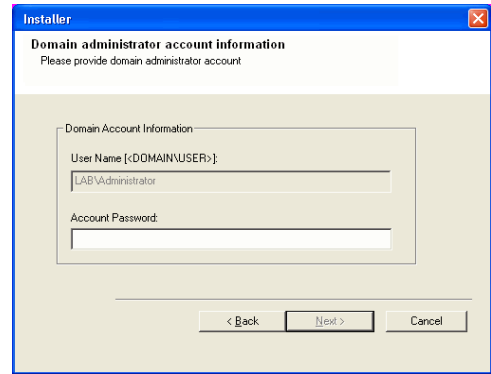
- If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures, see Manually Installing the Software on a Passive Node.

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

NOTES

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

Click **Next** to continue.



SETUP COMPLETE

33. Click **Next** to continue.

NOTES

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

34. Select from the following:

- If the **Reboot Now** button is displayed, a reboot is required before you can use the software. You can click this button to restart the computer now, or choose to perform the restart at another time. If the **Reboot Now** button is not displayed, it will not be necessary to restart the computer.
- Click **Finish** to exit the program.

NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed/upgraded, 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.

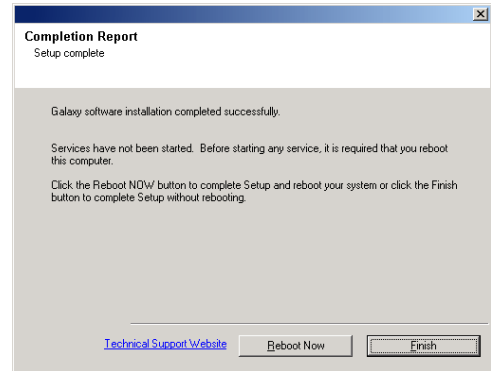
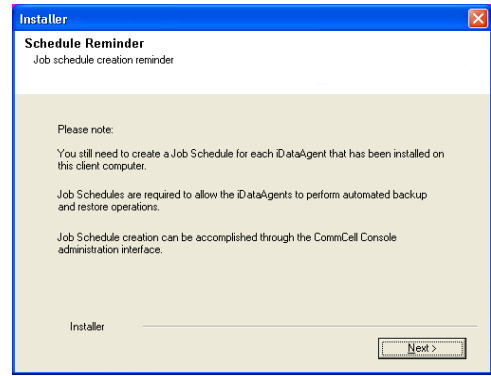
This procedure is now complete.

35. Note that the following will automatically be filtered:

- The physical cluster nodes will automatically filter all shared disk resources.
- Cluster group will automatically filter all physical disk resources.

NOTES

- For information on adding your own filters, see Add a Data Protection Filter for a Subclient.



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.

Install the Image Level ProxyHost iDataAgent - UNIX

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Select Components for Installation
- Base Software Installation
- Enable Global Filters
- Client Group Selection
- Storage Policy Selection
- Block Filter and Snap Driver (CVGxCXBF) Installation
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the Image Level ProxyHost iDataAgent. The Image Level ProxyHost iDataAgent for UNIX is installed on the computer from which the iDataAgent secures data. (This computer is referred to as the *Client* computer in this install procedure.)

You must install the Image Level iDataAgent for Unix on the client before you can install the Image Level ProxyHost iDataAgent for Unix on the client. Otherwise, the Image Level ProxyHost installation will fail. When you install the Image Level iDataAgent for Unix, the Unix File System iDataAgent and QSnap (CVGxCXBF) are automatically installed as well. All of these components are required in order to install the Image Level ProxyHost iDataAgent. See Install the Image Level iDataAgent - Unix for step-by-step Image Level installation procedures.

Verify that the computer in which you wish to install the software satisfies the minimum requirements specified in System Requirements - Image Level ProxyHost iDataAgent.

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 and MediaAgent must be installed and running (but not necessarily on the same computer), before you can install the Agent.
- Ensure there is an available license on the CommServe for the Agent.
- Verify that you have the Software Installation Disc that is appropriate to the destination computer's operating system.

BEFORE YOU BEGIN

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

INSTALL PROCEDURE

GETTING STARTED

1. If you are installing the software from CD, run the following command to mount the CD:

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

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

```
./cvpkgadd -allow-newer-commserve
```

2. The product banner and other information is displayed.
Press **Enter** to continue.
3. Read the license agreement. Type **y** and press **Enter** to continue.
4. Enter the number corresponding to the setup task you want to perform.

NOTES

- For Install data protection agents on this computer option, follow the steps described in this procedure.
- Advance options provide additional setup features such as record and play setup,

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

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

- 1) Install data protection agents on this computer

creating a custom package and External Data Connector Agent software.

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

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

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

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

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

Press **Enter** to continue

NOTES

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

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

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

NOTES

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

Verify the default network interface name.

Press **Enter** to accept the default network interface name and continue, or Type the default network interface name, and then press **Enter** to continue.

NOTES

- This prompt will be displayed only when you have multiple network interfaces for the computer.

8. Specify the client name for the computer.

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

2) Advance options

3) Exit this menu

Your choice: [1]

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

1) All platforms (32 bit)

2) FS and MA only (64 bit)

Your choice: [1]

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

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

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

1) Add another package to stone.company.com

2) Install Calypso on a virtual machine

3) Exit

Your choice: [1]

Network interface with the following IPs have been found available on your system. One of these interfaces should be associated with the physical machine being installed. It will also be used by the CommServe to initiate connections to the physical machine. Note that you will be able to additionally customize Datapipe Interface Pairs used for the backup data traffic later in the Calypso Java GUI.

Please select the correct network interface below.

1) client (201.42.33.598)

2) hk97::489:9glg:hk8d:9490

3) client.company.com (hr90:8842:2:78:013:8ghh:hg8k:9x54)

Interface number: [1]

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

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

Please specify the client name for this machine.

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

Physical Machine Client name: [angel]

SELECT COMPONENTS FOR INSTALLATION

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

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

NOTES

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

Install Calypso on physical machine client.company.com

Select the Calypso module that you would like to install

[] 1) Media Agent [1301] [CVGxMA]

[] 2) FileSystem IDA [1101] [CVGxIDA]

>) >>>> NEXT PAGE >>>>>

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

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

BASE SOFTWARE INSTALLATION

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

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

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

NOTES

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

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

NOTES

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

Press **Enter** to continue.

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

NOTES

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

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

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

14. Specify the location for the log files.

NOTES

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

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

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

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

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

Press **Enter** again to continue.

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

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

NOTES

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

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

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

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

1) Download from the software provider website.

2) Use the one in the installation media

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

Your choice: [1] 2

Keep Your Install Up to Date - Latest Service Pack

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

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

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

Press <ENTER> to continue ...

Please specify where you want us to install Calypso binaries.

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

Installation Directory: [/opt]

..

Calypso will be installed in /opt/calypso.

Press ENTER to continue ...

Please specify where you want to keep Calypso log files.

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

Log Directory: [/var/log]

..

Calypso log files will be created

in /var/log/calypso/Log_Files.

Press ENTER to continue ...

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

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

Group name: dba

REMINDER

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

Press <ENTER> to continue ...

Every instance of Calypso should use a unique set of network ports to avoid interfering with other instances running on the same machine.

The port numbers selected must be from the reserved port number range and have not been registered by another application on this machine.

Please enter the port numbers.

Port Number for CVD : [8600]

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

Port Number for EvMgrC: [8602]

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

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

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

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

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

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

NOTES

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

CommServe Host Name:

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

Enter your CommCell user name and password:

NOTES

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

User Name :

Password :

Press <ENTER> to continue ...

Click **Enter** to continue.

ENABLE GLOBAL FILTERS

20. Type the appropriate number for configuring Global Filters for the default subclient and press Enter to continue.

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

NOTES

- Select **Use Cell level Policy** to inherit the global filter policy configuration set for the CommCell, i.e., if the **Use Global Filters on All Subclients** option is selected in the **Global Filters** dialog box (from the CommCell Console's Control Panel), then this policy will be applied to the default subclient as well. If is not selected, then the global filters will not be applied to the default subclient.
- Select **Always use Global filters** to always apply the global filters policy to the default subclient regardless of the policy set for the CommCell.
- Select **Do not use Global filters** to disregard applying the global filters to the default subclient regardless of the policy set for the CommCell.

- 1) Use Cell level policy
- 2) Always use Global filters
- 3) Do not use Global filters

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

CLIENT GROUP SELECTION

21. Type the number of a Client Group and press **Enter**.

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

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

NOTES

- This screen will be displayed only if Client Groups are configured for the CommCell. For more information, see Client Computer Groups.

- [] 1) Unix
- [] 2) DR
- [] 3) DKS

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

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

STORAGE POLICY SELECTION

22. Enter the number corresponding to the storage policy through which you want to back up the File System iDataAgent and then press **Enter** to continue.

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

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.

- 1) SP_StandAloneLibrary2_2
- 2) SP_Library3_3
- 3) SP_MagLibrary4_4
- 4) fornax_fornax_HWCmp
- 5) ranger_ranger_HWCmp
- 6) fornax_fornax_ClnCmp
- 7) fornax_fornax_MACmp
- 8) fornax_fornax_NoCmp

- If desired, you can change your storage policy selection at any time after you have installed the client software. Storage Policy: [3]
- 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.

BLOCK FILTER AND SNAP DRIVER (CVGXCXBF) INSTALLATION

23. To install **CVGxCXBF** package, type **Yes** and press **Enter** to continue.
- NOTES:**
- Skip to Setup Complete to install this package at a later time.
24. Press **Enter** to continue.
25. Make your selection and press **Enter**.
- NOTES**
- This prompt is displayed only if the directory identified in the previous Step does not exist.
26. Record this mount point for use later when mounting a volume to it.
Press **Enter**.
27. The install program now starts copying the software to the computer. The progress of the operation is displayed.
28. Press **Enter** to continue.
29. The install program now starts copying the software to the computer. The progress of the operation is displayed.
Press **Enter** to continue.
- Cxbuf provides snapshot facility and also monitors the device to provide incremental support. You can chose to install now or you can install later.
- Do you want to install? [Yes]
- For every snapshot taken CXBF driver creates a sparse file where it puts copy-on-write data blocks and block bitmap. These COW files are created in a dedicated directory that should satisfy a few requirements:
- 1) It should be a local directory for performance reasons,
 - 2) It should have sufficient amount of space,
 - 3) In case of Solaris UFS, it should have journaling turned off.
- COW Cache Directory: [/space/opt/calypso2/CXBF/cache]
- Directory "<dir_name>" does not exist.
- 1) Create this directory and continue
 - 2) Retry input
- Your choice: [1]
- Please make a note of this mount point and use it for mounting the cache volume in the Volume Explorer after install has completed.
- Press <ENTER> to continue ...
-
.....
.....
.....
- Successfully copied xx files
- Successfully installed CVGxCXBF.
- Press ENTER to proceed with CVGxImgIDA install ...
-
.....
.....
.....
- Successfully copied xx files
-
.....
.....
- Successfully installed CVGxImgIDA
- Press ENTER to continue ...

SETUP COMPLETE

30. Enter the number corresponding to the **Exit** option and then press **Enter** to continue.
The installation is now complete.
- Certain Calypso packages can be associated with a virtual IP, or in other words, installed on a "virtual machine" belonging to some cluster. At any given time the virtual machine's services and IP address are active on only one of the cluster's servers. The virtual machine can "fail-over" from one server to another, which includes stopping services and deactivating IP address on the first server and activating the IP address/services on the other server.
- Currently you have Calypso installed on physical node stone.company.com.
- Now you have a choice of either adding another package to the existing installation or configure Calypso on a virtual machine for use in a cluster.
- 1) Add another package to stone.company.com
 - 2) Install Calypso on a virtual machine
 - 3) Exit
- Your choice: [1]

POST-INSTALL CONSIDERATIONS

GENERAL

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

Backup - Image Level ProxyHost

Topics | How To | Related Topics

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

Overview

Supported Backup Types

Image Level ProxyHost Backup Jobs

Backup Considerations

- [Metafile Creation](#)

Advanced Backup Options

OVERVIEW

Plan your backup jobs for this agent by reviewing the following information:

- For an overview of backup jobs, see [Backup Data](#).
- For a list of supported data types for this agent, see [Supported Data Types](#).
- For information on subclients, see [Subclients](#)
 - For information on configuring subclients for this agent, see [Subclients - SAN iDataAgents](#).

SUPPORTED BACKUP TYPES

This agent supports the following backup types:

- Full Backups
- Incremental Backups
- Synthetic Full Backups
- CXBF Backups
- Non-CXBF Backups

IMAGE LEVEL PROXYHOST BACKUP JOBS

This agent has the following unique functionality.

The Image Level ProxyHost iDataAgent backs up the blocks of complete volumes, and restores them using either Volume Level Restore or File Level Restore. Each backup for the iDataAgent on a Unix platform is either a CXBF backup or a non-CXBF backup.

CXBF BACKUPS

CXBF backups are run on Unix platforms for this agent. To run a CXBF backup, QSnap must be installed on the client and you must configure a CXBF subclient. For more information, see [Subclients - SAN iDataAgents](#). For a step-by-step procedure, see [Run a CXBF Backup \(Image Level/Image Level ProxyHost\)](#).

NON-CXBF BACKUPS

Non-CXBF (Checksum) backups are run on Unix platforms for this agent. To run a non-CXBF (Checksum) backup, you must configure a non-CXBF (Checksum) subclient and also provide a supported snapshot. For more information, see [Subclients - SAN iDataAgents](#). For a step-by-step procedure, see [Run a non-CXBF Backup \(Image Level/Image Level ProxyHost\)](#).

BACKUP CONSIDERATIONS

Before performing any backup procedures for this agent, review the following information:

- [Metafile Creation](#)

- Selecting the Skip Metafile Creation option in the Advanced Backup Options screen will increase performance but disables the ability to restore data using a File Level restore. This will also apply to any Synthetic Full backups created from such a backup.
- If File Level restores will never be used for this client, instead of manually selecting the Skip Metafile Creation option for each job, edit the `SkipMetaFileCreation` registry key to automatically skip metafile creation for all backup jobs.
- For the Image Level and Image Level ProxyHost iDataAgents, if a backup job is suspended either by the user or the Job Controller during metadata collection, the job will automatically resume from the scan phase.
- Do not modify any data on the secondary volume once the hardware snapshot has completed. In some cases, this could cause data loss or data inconsistency, because any change on the secondary volume will be backed up and this will cause data inconsistency between the primary volume and secondary volume.
- For Solaris, under conditions of heavy I/O, such as is expected during block-level backups and QR volume creation, we recommend that you do not enable the UFS logging option on the client machine.
- Before performing the first full backup of a volume, defragment it. This will ensure that the minimum number of extents will need to be backed up, resulting in better performance and lower storage requirements.
- Although a subclient can contain multiple volumes, you cannot perform a File Level Restore of the subclient, as no metafile is created. To allow metafile creation, enabling File Level Restores, you can create multiple subclients, each containing a unique volume.
- If the backup extent size is changed, the next backup will be converted to a full backup.
- You should configure the next backup after an in-place restore to be a full backup, so as to take advantage of data block copy. Even if only some of the volumes of a subclient were restored, all the volumes in the subclient should be backed up as full. The software does not enforce this, but it is recommended.

[Back to Top](#)

Backup - Image Level ProxyHost - How To

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

[Run a CXBF Backup](#)

[Run a non-CXBF Backup](#)

[Start a Backup \(Differential backups are not supported\)](#)

[Start a Synthetic Full Backup](#)

[Schedule Backups](#)

[Start a Backup in the Suspended State](#)

[Start a Backup on New Media](#)

[Start a Backup that Marks Media Full on Completion](#)

[Start a Backup that Skips Metafile Creation](#)

[Start a Backup that Releases Resources during the meta-data collection phase](#)

[Start a Backup that Reserves Resources Before Scan](#)

[Start a Backup with a Set Job Priority](#)

[Start a Backup with Vault Tracking enabled](#)

RUN A CXBF BACKUP

Related Topics

- [Subclients - SAN iDataAgents](#)

Required Capability: See Capabilities and Permitted Actions

▶ To run a CXBF backup:

1. Ensure that QSnap is installed on the client.
2. Configure the subclient.
3. From the Subclient Properties (General) dialog box, select the **CXBF** option.

- Run the backup. (Select from any of the appropriate procedures below to start or schedule a backup for instructions.)
-

RUN A NON-CXBF BACKUP

Related Topics

- Subclients - SAN iDataAgents
- Pre/Post Processes

Required Capability: See Capabilities and Permitted Actions

▶ To run a non-CXBF backup:

- Configure the subclient.
 - From the Subclient Properties (General) dialog box, select the **Checksum** option.
 - Provide the appropriate PreScan and PostBackup scripts for snap and mount operations. For more information, see Pre/Post Processes for Data Protection Operations: Image Level and Image Level ProxyHost iDataAgents.
 - Run the backup. (Select from any of the appropriate procedures below to start or schedule a backup for instructions.)
-

START A BACKUP

Before You Begin

- Depending on your agent, you can perform the following types of backup operations: **Full**, **Incremental**, **Differential** or **Synthetic Full**.
 - Read Full Backups before performing a Full Backup.
 - Read Incremental Backups before performing an Incremental Backup.
 - Read Differential Backups before performing a Differential Backup.
 - Read Synthetic Full Backups before performing a Synthetic Full Backup.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job:

- From the CommCell Browser, expand **Client Computers** by double-clicking **Client Computers | iDA File System | defaultBackupSet**. The default and other subclients (if available) are displayed on the right-hand windowpane.
- To back up the default subclient, right-click the subclient, and click **Backup**.
- From the Backup Options dialog box, select **Run Immediately**.
- Select **Full**, **Incremental**, **Differential** or **Synthetic Full** backup.

In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see When a Non-Full Backup is Automatically Converted to a Full Backup.

- Click **OK**. You can track the progress of the backup job from the **Job Controller** window. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically. Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.
- When the backup has completed, the Job Controller displays **Completed**.

After running a backup, you may want to verify the backup data. You can do this by viewing the Backup History. For more information, see Backup Job History.

- You can also run backups of the following:
 - For a user-defined backup set or instance, right-click the backup set you want to back up, click **All Tasks**, and click **Backup All Subclients**.
 - For the Lotus Notes Document iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup Default Backup Set**.
For the Lotus Notes Database iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup All Subclients**.
 - For Agents that do not have backup set or instance levels, to back up all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
 - If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
 - Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A SYNTHETIC FULL BACKUP

Before You Begin

- Read Synthetic Full Backups before performing a Synthetic Full Backup.
- For SharePoint Document, for a versioned document that has multiple versions, all of the backed up versions can be viewed in the **View All Versions** window and restored, until a Synthetic Full backup is run. After running the Synthetic Full backup you can only view and restore the latest backed up version for the document.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job:

1. From the CommCell Browser, expand **Client Computers** by double-clicking **Client Computers | iDA File System | defaultBackupSet**. The default and other subclients (if available) are displayed on the right-hand windowpane.
2. To back up the default subclient, right-click the subclient, and click **Backup**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select **Synthetic Full** backup.

Running an incremental backup immediately before the synthetic full ensures that any new or recently changed data is included in the synthetic full.

Running an incremental backup immediately after the synthetic full ensures that any new or recently changed data since the backup that occurred prior to the synthetic full, but was not included in the synthetic full, is backed up by the incremental. Remember, a synthetic full consolidates data; it does not actually back up data from the client computer.

5. Click **OK**. You can track the progress of the backup job from the **Job Controller** window. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically. Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.
6. When the backup has completed, the **Job Controller** displays *Completed*.

After running a backup, you may want to verify the backup data. You can do this by viewing the Backup History. For more information, see Backup Job History.

You can also run synthetic full backups of the following:

- For a user-defined backup set or instance, right-click the backup set you want to back up, click **All Tasks**, and click **Backup All Subclients**.
- For the Lotus Notes Document iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup Default Backup Set**.
For the Lotus Notes Database iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup All Subclients**.
- For Agents that do not have backup set or instance levels, to back up all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
 - If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
 - Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

SCHEDULE BACKUPS

You can schedule backups to occur with the following procedure. You will be prompted to create a schedule for the data protection operation after selecting your data protection options.

Before You Begin

- **All Agents**
 - Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To schedule a backup operation:

1. From the CommCell Browser, select one of the following:
 - To back up a subclient, right-click the subclient and click **Backup**.
 - To back up a backup set or instance, right-click the backup set or instance, click **All Tasks**, and click **Backup All Subclients**.
 - To back up the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.

- For the Lotus Notes Document iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup Default Backup Set**.
For the Lotus Notes Database iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup All Subclients**.
 - For Agents that do not have backup set or instance levels, to back up all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
 3. From the Backup Options dialog box, select the type of backup that you want to initiate. In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see [When a Non-Full Backup is Automatically Converted to a Full Backup](#).
 4. Click **Schedule**. Click **OK** to continue.
 5. From the Schedule Details (Schedule Details) dialog box, create a schedule for this operation. For step-by-step instructions, see [Create a Job Schedule](#). Click **OK** to continue.
 6. Your backup operation will execute according to the specified schedule.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP IN THE SUSPENDED STATE

Use the following procedure to start a backup in the suspended state.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See [Capabilities and Permitted Actions](#)

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see [When a Non-Full Backup is Automatically Converted to a Full Backup](#).
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Startup) tab, and select **Startup in suspended state** and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate

multiple data streams.

START A BACKUP ON NEW MEDIA

Use the following procedure to start a backup on new media.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup 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.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP THAT MARKS MEDIA FULL ON COMPLETION

Use the following procedure to start a backup that marks media full on completion.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.

- For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
 3. From the Backup Options dialog box, select **Run Immediately**.
 4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
 5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
 6. Click on the Advanced Backup Options (Media) tab, and select **Mark media full after successful operation** and click **OK**.
 7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
 8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP THAT SKIPS METAFILE CREATION

Use the following procedure to start an Image Level or Image Level ProxyHost iDataAgent backup that skips metafile creation. For more information, see one of the following:

- Skip Metafile Creation - Image Level
- Skip Metafile Creation - Image Level ProxyHost

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent.
- If File Level restores will never be used for this client, instead of manually selecting the Skip Metafile Creation option for each job, edit the `SkipMetaFileCreation` registry key to automatically skip metafile creation for all backup jobs.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. Select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Media) tab, and select **Skip Metafile Creation** and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays **Completed**.

Starting a backup on a backup set, instance or agent level causes the system to start individual backup jobs for each subclient contained therein. If the subclients are associated with the same storage policy, then their jobs will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP THAT RELEASES RESOURCES DURING THE META-DATA COLLECTION PHASE

Use the following procedure to start a backup that Releases Resources during the meta-data collection phase.

Before You Begin

- **All Agents**

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent.

- **Image Level**

- If File Level restores will never be used for this client, instead of manually selecting the Skip Metafile Creation option for each job, edit the `SkipMetaFileCreation` registry key to automatically skip metafile creation for all backup jobs.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. Select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Media) tab, and select **Release Resources during meta-data collection phase** and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays **Completed**.

All Agents

Starting a backup on a backup set, instance or agent level causes the system to start individual backup jobs for each subclient contained therein. If the subclients are associated with the same storage policy, then their jobs will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP THAT RESERVES RESOURCES BEFORE SCAN

Use the following procedure to start a backup that reserves the backup media before the scan phase.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For the Microsoft SQL Server iDataAgent, to backup a database, right-click the database you want to backup, click **All Tasks**, and click **Backup Database**.
 - For the Microsoft SQL Server iDataAgent, to backup up an instance, right-click the instance you want to backup, click **All Tasks**, and click **Backup SQL Server**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Media) tab, and select **Reserve Resources before scan** and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.
9. When the backup has completed, Job Controller displays *Completed*.

Starting a backup on a backup set, instance or agent level causes the system to start individual backup jobs for each subclient contained therein. If the subclients are associated with the same storage policy, then their jobs will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP WITH A SET JOB PRIORITY

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

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See *Capabilities and Permitted Actions*

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.

Backup is Automatically Converted to a Full Backup.

5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Startup) tab, and select **Change Priority** and then enter a value. Click **OK** to continue.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP WITH VAULT TRACKING ENABLED

Use the following procedure to start a backup with Vault Tracking enabled.

For additional information, see the following:

- VaultTracker
- VaultTracker Enterprise

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the **Vault Tracking** tab, and select the vault tracking options you want to use and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Back To Top

Restore Data - Image Level ProxyHost

Topics | Related Topics

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

Overview

Restore Considerations for this Agent

Restore Destinations

- In-Place Restore
- Out-of-Place Restore
- Cross-Platform Restores
- Restore to Network Drive/NFS-Mounted File System

OVERVIEW

The following page describes the agent-specific restore options. Additional restore options are accessible from the Related Topics menu.

The Image Level ProxyHost iDataAgent performs the following types of restore operations:

- File Level Restore - You can browse the files/folders in your backup and select the files/folders you want to restore.
- Volume Level Restore - You can browse the volumes you have backed up and select a volume to restore.

When restoring data, you can, if desired, restore the data to a file system type that differs from the type in which it originated. For example, you can restore NTFS data to a FAT file system and restore FAT data to an NTFS file system. FAT file systems do not support Discretionary Access Control Lists (DACL); therefore, any NTFS data that you restore to a FAT partition loses its original access privileges. Conversely, when FAT file system data is restored to an NTFS file system, the restored data inherits the DACL of the destination directory.

[Back to Top](#)

RESTORE CONSIDERATIONS FOR THIS AGENT

Before performing any restore procedures for this agent, review and verify the following information.

GENERAL

- Review the general restore requirements described in [What You Need to Know Before Performing a Restore](#).
- When restoring Image Level ProxyHost data, you can, if desired, restore the data to a file system type that differs from the type in which it originated. For example, you can restore NTFS data to a FAT file system and restore FAT data to an NTFS file system. FAT file systems do not support Discretionary Access Control Lists (DACL); therefore, any NTFS data that you restore to a FAT partition loses its original access privileges. Conversely, when FAT file system data is restored to an NTFS file system, the restored data inherits the DACL of the destination directory.
- It is recommended that you restore data to the same type of operating system from which it was backed up.
- It is important to note that when performing a restore, the Job Controller will show the source machine even though the destination machine may be different.
- You should configure the next backup after an in-place restore to be a full backup, so as to take advantage of data block copy. Even if only some of the volumes of a subclient were restored, all the volumes in the subclient should be backed up as full. The software does not enforce this, but it is recommended.

FILE LEVEL RESTORE:

- Supported only for certain operating systems and file system types; see [Supported Data Types](#).
- The Image Level and Image Level ProxyHost iDataAgents on Unix can perform a File Level Restore only when the OS of the Client computer and the MediaAgent are the same.
- For a Windows MediaAgent, the Index Cache folder must reside on an NTFS partition.
- If metadata was not collected during a backup, a File Level restore cannot be performed. This might result from having selected the Skip Metatile Creation option in the Advanced Backup Options screen, or as a result of failure to collect metadata during the backup, in which case the system generated an Event Message warning of the failure.
- Do not restore:

- hidden objects
- system files
- recycler files
- Image Browse is not supported. A no-image browse operation returns the most recent version of the data that existed back to the most recent full backup, rather than returning an image of the specified entity (i.e., file system/directory). To perform a File Level Restore of an entity to a point in time, you will need to Browse back in time, to the point in time you want to restore.
- When a File Level restore is started, metadata is restored prior to the actual restore of files, and during this time, a message might indicate the Index Cache is being restored, although it already exists. Also, the media containing this metadata will be mounted into the library even if this media does not contain the data from the full backup.
- An Out-of-Place File Level Restore to a non-existing path may be reported as successful, even though no files were restored.

VOLUME LEVEL RESTORE:

- For a Volume Level Restore, you must select the **Browse only Volumes** option in the **Browse Options** dialog box, or the restore operation will be a File Level Restore.
- Do not run Volume Level restore if destination volume contains OS files.
- When performing a Volume Level Restore, the destination volume will adopt the file system type of the restored data. Thus, for instance, if you restore an NTFS volume to a FAT destination volume, the destination volume will be NTFS as a result of the Volume Level Restore.
- When restoring a volume changes its file system type (see Supported Data Types), sometimes Windows Explorer may still show the volume having the same file system type as before the restore, even though Computer Management shows the new (correct) type. After a reboot, Windows Explorer will show the correct file system type.
- The destination volume must be at least as large as the volume from which the data was backed up. This is true regardless of the amount of data that is actually restored. For example, if you back up a 10 GB volume that contains 100 MB of data, you can only restore that data to a volume that is 10 GB or larger. The restore operation will fail if the destination volume is smaller than the source volume. We recommend that you restore data to a volume that is at least 1 MB larger than the source volume.

Windows Logical Disk Manager (LDM) displays the size of a volume in round numbers. Consequently, LDM may display the same size for two volumes with slightly different block counts. To get the exact size of a volume, open the Windows Explorer, right-click the volume, and select **Properties**. The volume's capacity in bytes is its exact size.

If no destination volume is specified, the system attempts to restore to a volume on the **Destination Computer** with the same name as the one being restored. If no such volume exists, the restore operation fails.

[Back to Top](#)

RESTORE DESTINATIONS

By default, the Image Level ProxyHost iDataAgent restores a volume or file(s) to the primary host from which it originated (not the backup host); this is referred to as an in-place restore. If desired, you can also restore the data to a different Image Level ProxyHost client. Keep in mind the following considerations when performing such restores:

- The destination client must reside in the same CommCell as the client whose data was backed up.
- Each of these restore destination types are available for both Volume Level restores as well as File Level restores, both for Windows and Unix.

The following section enumerates the types of restore destinations that are supported by the Image Level ProxyHost iDataAgent. See Restore/Recover/Retrieve Destinations - Support for a list of Agents supporting each restore destination type.

IN-PLACE RESTORE

- Same path/destination

OUT-OF-PLACE RESTORE

- Same path/destination
- Different path/destination

CROSS-PLATFORM RESTORES

- Same Operating System - Different Version

Cross-Platform, File Level restores are supported as follows:

- Windows 2000 data can be restored to Windows 2003
- Windows 2003 data can be restored to Windows 2000

RESTORE TO NETWORK DRIVE/NFS-MOUNTED FILE SYSTEM

For File Level Restores only, besides restoring data to a client computer's local drive, you can also restore data to a UNC path. (See Restore to Network Drive/NFS-Mounted File System for comprehensive information.)

[Back to Top](#)

Basic Restore

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

[Overview](#)

[Time Range Options](#)

OVERVIEW

There are two functions that help you retrieve backed up data from the backup media: Browse and Restore. Browse operations allow you to view the data that has been backed up for a client computer without actually restoring the data. Restore operations retrieve the data from the backup media and restore it to the desired location.

In the CommCell Browser, the Browse and various Restore commands appear in the right-click menus at the agent, instance and/or backup set levels, depending on agent.

Using the Restore commands, i.e., restoring without browsing, is most appropriate when you want to restore the latest backup job for an agent, instance or backup set and want to retain the current file structure.

In certain situations and for supported agents, Restore operations can run without utilizing the Browse feature. For example, if you know the path/name of the volume of the data that you want to restore, you can restore it without browsing. In these agents, this procedure is most appropriate when the number of paths for the data that you want to restore is small or when the data that you want to restore is at a single volume. If you want to restore data from many different paths or volumes, you should probably select the data from the Browse window.

TIME RANGE OPTIONS

In a Basic Restore, point-in-time data can be restored by specifying time range options in the Advanced Restore Options (Time Range) dialog box. See Time Range Options for Basic Restore for step-by-step instructions. When a time range is specified for a Basic Restore, the latest version of the backup job within the given time range will be restored.

Basic Restore - How To

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

[Basic Restore](#)

[Time Range Options for Basic Restore](#)

BASIC RESTORE

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 restore data without using browse:

1. From the CommCell Browser, right-click the agent, instance or backup set that contains the data you want to restore, click **All Tasks** and then click the available **Restore** command (command names vary by agent).
2. In the **Restore** dialog box, type the starting path of the data you want to restore.
3. From the **Restore Options** and **Advanced Restore Options** dialog boxes, select the restore options that you want to use. When you accept all the default settings, you will be restoring the selected data to its original location. See Restore Backup Data for complete information on the agent-specific

restore options.

4. 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**.

You can monitor the progress of the restore job in the Job Controller. While the job is running, you can right-click the job in the Job Controller and select **Detail** to view information on the job.

After the data has been restored, you will see a job completion message in the Job Controller and Event Viewer.

TIME RANGE OPTIONS FOR BASIC RESTORE

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 provide time range options for basic restore:

1. From the CommCell Browser, right-click the agent, instance or backup set that contains the data you want to restore, click **All Tasks** and then click the available **Restore** command (command names vary by agent).
2. In the **Restore** dialog box, type the starting path of the data you want to restore.
3. From the **Restore Options** and **Advanced Restore Options** dialog boxes, select the Time Range tab.
4. In the Advanced Restore Options (Time Range) dialog box, clear the **Show Deleted Items** option, if required.

In the Specify Restore Time area select the **Time Zone** for the time range options. Select the **Exclude Data Before** option and select the start date and time from which you wish to restore data, and select the **Browse Data Before** option and select the end date and time until which you wish to restore data.

5. Click **OK** in the Advanced Restore Options dialog box.
6. Click **OK** in the Restore Options dialog box to execute the restore.

[Back To Top](#)

Browse and Restore

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

OVERVIEW

There are two functions that help you retrieve backed up data from the backup media: browse and restore. In the CommCell Browser, the browse and variously-named restore commands appear, depending on agent, in the right-click menus at the agent, instance and/or backup set levels.

Browse operations allow you to view data that has been backed up by the agent on the client computer and select all or some of that data. Depending on the agent, there are several options available to customize your browse. See Browse Data for comprehensive information on Browse operations.

Restore operations allow you to retrieve data from backup media and restore it to the desired location. Restoring without browsing is most appropriate when you want to restore the latest backup job for an agent, instance or backup set and want to retain the current file structure. See Basic Restore for more information on restoring without using browse.

Browse and Restore

The Browse and Restore procedure is a sequential procedure that combines the two procedures. When you select a **Browse** command from the CommCell Browser, you can define and run one of many potential browse sequences. At the end of the browse, when you are looking at the resulting information presented in the Browse window, you can continue with a restore procedure simply by selecting data and clicking the **Recover All Data** button. As with the browse, depending on the agent, there are several options available to customize your restore.

Perform a **browse and restore** operation when you want to:

- restore from an earlier backup
- restore only select files/objects
- restore deleted files/objects

- when you don't want or don't need to retain the current file structure
 - utilize browse options
-

Browse and Restore - How To

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

BROWSE AND RESTORE

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. From the CommCell Browser, right-click the agent, instance, backup set, or Legal hold set (for Legal Hold data) that contains the data you want to restore, click **All Tasks** and then click the available **Browse** command (command names vary by agent).
2. Run a browse operation. See Browse Data for a list of customized browse operations and their step-by-step instructions. If you accept all defaults, you will be browsing the latest backups for the selected data.
3. From the Browse window, Select Objects From the Browse Window for Restore.
4. From the agent's **Restore Options** and **Advanced Restore Options** dialog boxes, select the restore options that you want to use. For agents with multiple tabs, do not click **OK** until you have used all of the desired tabs. When you accept all the default settings, you will be restoring the selected data to its original location. See Restore Backup Data for access to complete information on the agent-specific Restore Destination options and procedures available.
5. When restoring encrypted data, refer to Data Encryption for comprehensive feature information and procedures for using the Encryption tab of the Advanced Restore Options dialog box.
6. 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**, schedule the job, and then click **OK**.
 - If you want to run the job now, accept or click **Run Immediately** in the same tab and then click **OK**.

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

[Back To Top](#)

Subclients - SAN iDataAgents

Topics | How To | Related Topics

Overview

Configurable Properties

Things to Consider when Creating and Configuring SAN Subclients

- Image Level and Image Level ProxyHost iDataAgents
- ProxyHost iDataAgent

OVERVIEW

The following table shows subclient creation and configuration details specific to SAN iDataAgents.

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
Image Level	volumes or mount points	No	No	Yes	N/A	CXBF (Unix), checksum (Unix)	None
Image Level ProxyHost	volumes or mount points	No	No	Yes	N/A	CXBF (Unix), checksum (Unix)	None
ProxyHost	volumes, folders, or mount points	No	No	Yes	N/A	None	None

For Image Level on Unix and Image Level ProxyHost on Unix, you can configure CXBF subclients or non-CXBF (checksum) subclients to enable snapshot and backup capabilities. For more information, see Snapshot Options.

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.

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.

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.

The Filters tab is only available for the ProxyHost iDataAgent.

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](#).

For Image Level or Image Level ProxyHost on Unix, if you configure a checksum subclient, you must provide the appropriate PreScan and PostBackup scripts to enable snap and mount capabilities. For more information on checksum subclients, see [Snapshot Options](#). For more information on configuring the scripts, see [Pre/Post Processes for Data Protection Operations: Image Level and Image Level ProxyHost iDataAgents](#).

SNAPSHOT OPTIONS

If installed on the client, QSnap can be enabled to back up locked files or to provide volume-level snapshot functionality and utilize the integrated block-filter driver. On Unix clients, for some supported agents, any volume that you add to a subclient is automatically configured as a CXBF Device, which is required to back up the volume. Other agents will require using Volume Explorer to create CXBF devices. Depending on the agent, and for specific scenarios, Volume Explorer can or should also be used to configure these devices. If QSnap is enabled, the CommCell Configuration Report displays a superscript Q in the subclient column. For step-by-step instructions for the supported file system iDataAgents, see [Enable QSnap on a Subclient](#). Also, see [Configure a CXBF Device in Volume Explorer](#) as appropriate.

For Image Level and Image Level ProxyHost on Unix, you can configure subclients to enable a specified snapshot for backup. Specifically, you can configure a CXBF subclient to use QSnap, or you can configure a non-CXBF (checksum) subclient to use a supported snapshot that you desire. To this purpose, you can use the **Incremental Support Using** field in Subclient Properties (General). CXBF subclient configuration requires that QSnap be installed on the client; however, a QSnap install does not require you to configure the subclient as a CXBF subclient. If you use a snapshot other than QSnap (i.e., if you are configuring a checksum subclient), you must provide the appropriate PreScan and PostBackup scripts. For more information on configuring these scripts, see [Pre/Post Processes for Data Protection Operations: Image Level and Image Level ProxyHost iDataAgents](#).

STORAGE POLICIES

You can associate the subclient to a storage policy. For more information, see [Storage Policies](#).

SUBCLIENT NAME

You can rename a subclient. For step-by-step instructions, see [Rename a Subclient](#).

USER ACCOUNTS

The following pertains to the ProxyHost, Image Level on Windows, Image Level ProxyHost iDataAgents:

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

See the section for your agent in [User Accounts and Passwords](#) for more information.

USER SECURITY

You can perform the following functions:

- Identify the user groups to which this CommCell object is associated.
- Associate this object with a user group.
- Disassociate this object from a user group.

For more information, see [User Administration and Security](#).

VOLUME SHADOW SERVICE (VSS) BACKUPS

When using the Image Level iDataAgent in conjunction with a Windows iDataAgent that supports VSS, you can specify whether Volume Shadow Service (VSS) will be used to back up data for this subclient. If VSS is enabled, the CommCell Summary Report displays a superscript Q in the subclient column. For more

information, see VSS for the Image Level iDataAgent.

THINGS TO CONSIDER WHEN CREATING AND CONFIGURING SAN SUBCLIENTS

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

IMAGE LEVEL AND IMAGE LEVEL PROXYHOST /DATAAGENTS

- Subclient content can only be either a volume or a mount point.
- The Windows 2000 and higher operating systems allow you to add new volumes to the existing file system name space without using new drive letters. For each volume that you add in this manner, Windows establishes a mount point, a pointer from the directory to the target data. Mount points are supported subclient content.
- For the Windows Image Level iDataAgent, you can add volumes to existing subclient content or remove them. However, whenever volumes are added or removed, the next backup job will be converted to a full backup.
- For Oracle BLI backups using the Image Level iDataAgent, each subclient is expected to quiesce one instance at a time. Do not configure an Image Level subclient's content with more than one Oracle instance; create separate subclients for each Oracle instance.
- For Solaris, if the slice 0 partition is empty and the disk is allocated space from slice 1 onwards, then slice 1 will be considered as slice 0 by the agent. So, from whatever slice partition you start to allocate space on the disk, that particular slice will be considered as slice 0.
- Do not specify the same volume as subclient content for both an Image Level and Image Level ProxyHost subclient.
- The size of a volume defined as subclient content will not be displayed until after the first backup and a refresh the CommCell Browser view.

PROXYHOST /DATAAGENT

- For the ProxyHost iDataAgent, subclients are used to back up different portions of the file system on a client computer. Each subclient is a designated subset of a production server to back up host data path mappings. You can create multiple subclients with each subclient containing a unique set of the production server data paths.
- There are certain situations in ProxyHost where running multiple simultaneous backups is not advisable. The snapshot utility can only be used by one subclient at a time, and any other subclient trying to access that utility while it is already in use will fail. Therefore, we advise that you stagger your multiple subclient backups so that the PreScan phase of each backup will not overlap.
- When you back up Exchange 2000 data with the ProxyHost iDataAgent, one storage group should not span multiple subclients.

[Back to Top](#)

Subclients - SAN iDataAgents - How To

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

-
- [Add/Edit a Data Protection Filter for a Subclient \(ProxyHost\)](#)
 - [Associate a Subclient to a Storage Policy](#)
 - [Change Account for Executing Pre/Post Commands \(Data Protection\) \(all agents running on Windows platforms\)](#)
 - [Configure a Subclient for Pre/Post Processing of Data Protection Operations](#)
 - [Configure Subclient Content](#)
 - [Configure the Subclient for Data Encryption \(Image Level, ProxyHost, Image Level ProxyHost\)](#)
 - [Create a New Subclient](#)
 - [Delete a Data Protection Filter from a Subclient \(ProxyHost\)](#)
 - [Delete a User-Defined Subclient](#)
 - [Enable or Disable Operations](#)
 - [Enable Software Compression for a Subclient \(Image Level, ProxyHost, Image Level ProxyHost\)](#)
 - [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 \(Image Level, ProxyHost, Image Level ProxyHost\)](#)
 - [View Data Paths Associated with a Subclient](#)
 - [View Subclient Content](#)

ADD/EDIT A DATA PROTECTION FILTER FOR A SUBCLIENT

Before You Begin

- Review Filters.
- Do not change the data protection or discovery filter of a subclient that has a data protection operation in progress.
- The system does not allow you to add entries that are not content of a particular subclient to that subclient's filter.
- For BlueArc and EMC Celerra (running at least DART OS 5.6.x) subclients, the filter string with or without wildcards must match the name or path of the file or directory being filtered.
- For NetApp subclients only name type filters (with wildcards) are supported:
 - You cannot enter paths as a filter (e.g. /vol/vol0/data1). Since NetApp does not support the use of paths in filters, if there are multiple files with the same name, even though they may be in different directories, all of them will be excluded from backups.
 - Name of the file or directory must exactly match the filter string.
 - You can specify a maximum of 32 strings in the exclude list.

Select the desired procedure:

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

Required Capability: Capabilities and Permitted Actions

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

1. From the CommCell Browser, right-click the subclient whose data protection or discovery filter you want to add, and then click **Properties** from the shortcut menu.
2. Click the Filters tab of the Subclient Properties dialog box.
3. For Exchange Mailbox, Exchange Mailbox/Public Folder Archiver Agents and Exchange Compliance Archiver, to specify a mailbox or folder that you want to exclude from data protection operations:
 - Click the upper **Add** button.
 - From the Browse window, expand the mailbox tree of the client computer.
 - Click the mailbox or folder that you want to exclude from the backup/archive operations on the selected subclient, and then click **Add**. (Repeat this step for each additional entry.)
 - From the Browse window, click **OK**.
The mailboxes or folders that you selected appear as entries in the upper pane. Repeat this step if you want to add more mailboxes and/or folders to the filter.
4. For NAS NDMP 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.

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.

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 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.
 - 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.
 - 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.
 - 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.
- If you want to associate this subclient with an All Agent Types schedule policy, click **Associate with Generic Schedule Policy**, and then select that schedule policy from the drop-down list box. Click **OK**.
 - If you want to associate this subclient with a specific schedule policy, click **Associate to schedule policy**, and then select the schedule policy from the drop-down list box. Click **OK**.
 - If you have selected to define a schedule for this subclient:
 - Click **Schedule**.
 - From the Backup/Archive Options dialog box, select the type of data protection operation that you want to schedule.
 - If you want to set Advanced Backup/Archive Options, click **Advanced**.
 - After selecting the data protection type and any advanced options, click **OK**. The **Schedule Details** dialog box appears.
 - From the Schedule Details tab, select the scheduling options that you want to apply, then click **OK**.
 - If you don't want to create a data protection schedule at this time, click **Do Not Schedule**, and then click **OK**.

This task is now complete.

DELETE A DATA PROTECTION FILTER FROM A SUBCLIENT

Before You Begin

- Review Filters.
- Do not change the data protection or discovery filter of a subclient that has a data protection operation in progress.
- File Archiver for Windows/Unix Agents: We recommend that you don't delete the following entries from the exclusion filter, as it could cause your file system to be inoperable. For Windows, these include: *.dll, *.bat, *.exe, *.cur, *.ico, *.lnk. For Unix, these include *.a, *.ksh, *.csh, *.sh, *.lib, *.so.

Required Capability: Capabilities and Permitted Actions

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

1. From the CommCell Browser, right-click the subclient whose data protection or discovery filter you want to delete, and then click **Properties** from the shortcut menu.
2. Click the Filters tab of the Subclient Properties dialog box.
3. To delete an entry from the Exclusions list, click the entry in the upper pane then click the upper **Delete** button. (Repeat this step for each entry that you want to delete.)
4. To delete an entry from the Exceptions list (if applicable for your agent), click the entry in the lower pane then click the lower **Delete** button. (Repeat this step for each entry that you want to delete.)
5. Click **OK** to save your changes.

NOTES

- Whenever you delete an entry from the exclusion filter, check if the exceptions list (i.e., lower pane) contains any entries that are children of the deleted data (if applicable for your agent). If so, you should delete them as described in Step 4 since they no longer need to be listed. The system automatically deletes any exceptions that are children of a deleted exclusion unless you used wildcard expressions in the exclusion path.
- When you change a data protection or discovery filter, the change is effective the next time the subclient is backed up/archived.
- Data will not be backed up in a differential backup for a subclient after a filter was removed.
- Since Incremental backups only back up data that has been modified since the last backup, previously filtered files whose filters are now removed, will not

be backed up unless they have been modified since that last backup. To back up previously filtered files that have not been modified but whose filters have been removed since the last backup, you need to run a Full backup.

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

DELETE A USER-DEFINED SUBCLIENT

Related Topics:

- Command Line Interface - qdelete subclient
- Subclients

Required Capability: See Capabilities and Permitted Actions

▶ To delete a user-defined subclient:

1. From the CommCell Browser, right-click the user-defined subclient that you want to delete, and then click **Delete** from the shortcut menu.
2. A confirmation message is displayed, asking if you want to delete the subclient. Click **No** to cancel the deletion and retain the subclient, or click **Yes** to continue the deletion. If you click **Yes**:
 - the subclient, and any data that may have been protected/archived by the subclient are logically deleted, and you can no longer access the corresponding data for recovery/retrieve purposes. However, the data remains valid for the length of time specified by the associated retention period. Some agents allow you to browse data from a deleted subclient provided that the Browse Data Before date and time precedes the time that the user-defined subclient was deleted.
 - for agents that support a default subclient, once the user-defined subclient is deleted its contents are automatically reallocated to the default subclient the next time a data protection/archive/discovery operation is run on the default subclient to ensure data protection coverage.
 - the system deletes the selected subclient node and removes it from the CommCell Browser.
 - the system deletes any data protection/archive and recovery/retrieve job schedules that are associated with the subclient.

ENABLE OR DISABLE OPERATIONS

Required Capability: See Capabilities and Permitted Actions

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

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

1. From the CommCell Browser, right-click the CommServe, client computer group, client computer, agent, or subclient, and then click **Properties** from the short-cut menu.
2. From the Activity Control tab of the associated Properties dialog box, select or clear option(s), as desired.
3. Click **OK**.



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

ENABLE OR DISABLE SOFTWARE COMPRESSION FOR A SUBCLIENT

Before you Begin

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

Required Capability: Capabilities and Permitted Actions

▶ To enable software compression for a subclient:

1. From the CommCell Browser, right-click the subclient for which you wish to enable software compression and then click **Properties**.
2. Click the **Storage Device** tab and from the Data Storage Policy tab, select the storage policy from the **Storage Policy** list. If applicable for the selected agent, click the Log Storage Policy tab and select a storage policy from the **Transaction Log Storage Policy** list.
3. Then click the Storage Device (Data Transfer Option) tab and choose the appropriate compression option for this subclient.

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

This task is now complete.

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

Before You Begin

- We recommend not removing a pre/post process for a subclient that is currently running a data protection or archive operation.
- Review the Overview and Agent-Specific Guidelines for your agent before removing pre/post processes for data protection/archive operations.

Required Capability: Capabilities and Permitted Actions

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

1. From the CommCell Browser, right-click the subclient for which you want to remove a pre/post process, and then click **Properties** from the shortcut menu.
 2. Click the Pre/Post Process tab of the Subclient Properties dialog box.
 3. Click the text inside the space that corresponds to one of the following phases for which you want a pre/post process removed, then press the **Delete** key:
 - PreScan
 - PreArchive
 - PreCopy
 - PreSnap
 - PostBackup
 - PostScan
 - PostArchive
 - PostCopy
 - PostSnap
 4. Repeat Step 3 for any additional processes that you want to remove.
 5. Click **OK**.
-

RENAME A SUBCLIENT

Before You Begin

- You can rename a subclient at any time. However, we recommend that you don't rename a subclient while a data protection or archive operation is running on that subclient.
- In cases where a subclient is renamed using the same name as a deleted subclient, the system will append a Unix time stamp to the deleted subclient's name in data protection job history reports and views to distinguish the two subclients. For example, `subclientname_1104257351`.

Required Capability: See Capabilities and Permitted Actions

▶ To rename a subclient:

1. From the CommCell Browser, right-click the subclient that you want to rename, and then click **Properties** from the shortcut menu.
2. From the Subclient Properties (General) tab, or the QR Agent Subclient Properties (General) tab, type the new name in the **Subclient Name** field, and then click **OK**.

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

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

Before you Begin

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

Required Capability: Capabilities and Permitted Actions

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

1. From the CommCell Browser, right-click a subclient and then click **Properties**.
For the DB2, DB2 DPF, Informix, Oracle, Oracle RAC, SAP, or Sybase 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**.
 2. From the Subclient Properties dialog box, click the **Content** tab (or **Databases** tab for Lotus Notes) to view the contents of the subclient.
 3. Click **OK** to close the dialog box.
-

[Back To Top](#)

Backup Job History

Topics | How To | Related Topics

Overview

Items That Were Backed Up

Items That Failed

Pruning Backup History Information

Supported Features

Content Indexing History Information

OVERVIEW

You can view the backup and restore history of *iDataAgents*, *BackupSets/Instances*, and subclients.

The **Backup Job History Filter** dialog box allows you view detailed, historical information about backup jobs. Once you have chosen your filter options, they are displayed in the **Backup Job History** window.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

From this window, you can right-click a backup job to:

- Browse the data backed up by the backup set or instance from the **Backup Job History** window. This is provided as right-click option for each job. (This menu option, when selected, initiates the **Browse Options** dialog box preset with the values needed to browse the data.)
 - Browse the snapshots created during SnapProtect backup
 - View items that failed during the backup job
 - View details of the backup job
 - View files that were not indexed during a backup job that performed content indexing
 - View associated media
 - View events of the backup job
 - View a list of items that were backed up
 - View a list of items that were moved to media for a SnapProtect backup job
 - View the log files of the backup job.
 - View the RMAN log of an Oracle backup job.
 - View the BRTools log of a SAP for Oracle job. You can view the BRTools log for only those jobs that were initiated from the CommCell Console.
-

ITEMS THAT WERE BACKED UP

The **View backup file list** option allows you to view a list of the files that were backed up during a backup job, along with the data sizes of each backed up file. The **View backed up messages** option allows you to view a list of messages that were backed up by using, along with the alias name, display name, email address, sender name, and recipient of each message.

From these windows you can conduct searches based on a particular string, allowing to find particular files quickly and easily.



It is not recommended that this option is used to view a very large list of items that were backed up (such as lists that total over 100,000 items). It is suggested that the Browse option is used to find a list of backed up items in such cases.

See [View the Items That Were Protected During a Data Protection Operation](#) for step-by-step instructions.

ITEMS THAT FAILED

The items that failed for a data protection operation include individual files that may fail the job even though a particular job completed successfully. You can determine the degree of success for these jobs 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.

Also, keep in mind that you will need to run a full backup after adding failed files to the filter in order to remove them.



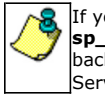
A listing of files and folders that failed is not available for the Quick Recovery Agent, or the Image Level and Image Level ProxyHost iDataAgents. These agents do not perform a file level backup/copy.

Certain application related files can never be backed up by the File System iDataAgent due to the nature of the data. For example, Microsoft SQL Server database files cannot be backed up by the File System iDataAgent. In this and other similar circumstances, consider entering files such as these as exclusions in the corresponding subclient filter.

See [View the Items That Failed For a Data Protection Operation](#) for step-by-step instructions.

PRUNING BACKUP HISTORY INFORMATION

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



If you have installed the SQL Server iDataAgent, do not use the stored procedure **sp_delete_backuphistory**, **sp_delete_database_backuphistory** and **sp_delete_backup_and_restore_history** provided by Microsoft clean up backup history. By default backup history is automatically pruned from the CommServe database and the Microsoft SQL Server, as necessary.

SUPPORTED FEATURES

- NAS iDataAgents do not support the ability to view items that failed.
- The Image Level and Image Level ProxyHost iDataAgents do not support the ability to Browse the data of a selected backup job in Backup Job History.

CONTENT INDEXING HISTORY INFORMATION

Content Indexing history can also be viewed of iDataAgents, BackupSets/Instances, and subclients. The following information is displayed:

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](#).

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/migrated 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](#).

[Back to Top](#)

Backup Job History - How To

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

[View Backup Job History](#)

[View the Items That Were Protected During a Data Protection Operation](#)

[View the Items That Failed For a Data Protection Operation](#)

[View Job History Details](#)

[View the Media or Mount Paths of a Job History](#)

[View the Events of a Job History](#)

[View the Items that were Moved to Media during SnapProtect Backup](#)

[View the Log Files of a Job History](#)

View the Items that Were Not Indexed During Content Indexing

View the Items that Were Successfully Content Indexed

Resubmit a Backup Job

VIEW BACKUP JOB HISTORY

▶ To view backup history:

1. From the CommCell Browser, right-click the entity (client computer, iDataAgent, backup set or subclient) whose backup history you want to view, click **View**, and then click **View Backup History**.
2. From the Backup History filter window select the filter options, if any, that you want to apply, and then click OK. The system displays the Backup Job History window.
3. Click **OK**.

VIEW THE ITEMS THAT WERE PROTECTED DURING A DATA PROTECTION OPERATION



This option is available for File System-like agents.

Required Capability: none required

▶ To view the list of items that were protected during 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 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 operation whose list of protected items you want to view, and then select **View backup file list/View Backed Up Messages**. The **Backup file List** window displays a list of the backed up files/messages that were included in the backup job. You can use the **Search** option to find items in the window.
4. Click **File -> Exit**.
5. Click **Close** from the **Job History** window.

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 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 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 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 WERE MOVED TO MEDIA DURING SNAPPROTECT BACKUP



This option is available for the SnapProtect Backup.

▶ To view the list of items that were moved to tape during SnapProtect Backup.

1. From the CommCell Browser, right-click the entity whose history of data protection 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 operation whose list of items moved to media you want to view, and then select **View Backup Copy file listing**. The **Backup file List** window displays a list of the backed up files that were included in the backup copy job. You can use the **Search** option to find items in the window.



- To view the files moved to media for a backup copy job, right-click the SnapProtect backup job corresponding to the Backup Copy job and select **View Backup Copy file listing**.
- View backup items will not display anything for a Backup Copy job.

4. Click **File** -> **Exit**.
5. Click **Close** from the **Job History** window.

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.

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 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.

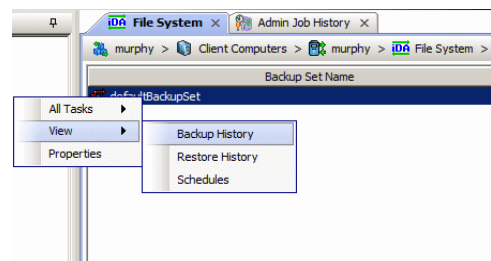
RESUBMIT A BACKUP JOB

▶ To resubmit a backup job:

1. From the CommCell Browser, right-click the subclient whose backup history you want to view, click **View**, and then click **View Backup History**.

Additionally, you can view the backup history for a client computer, iDataAgent, or backup set. However, the dialogs displayed may be different.

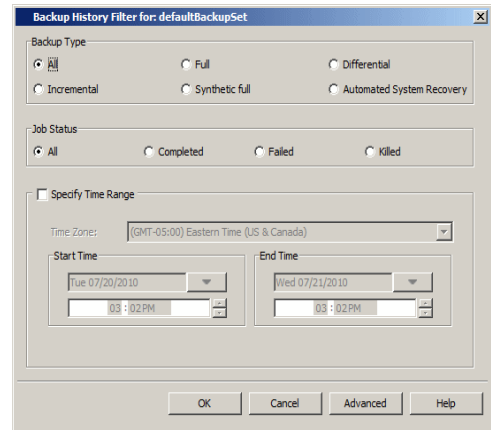
Note, if viewing the backup history for a client computer, right-click the computer name and select **Job History**.



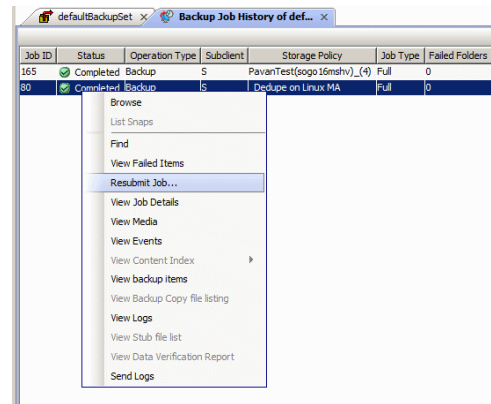
2. From the Backup History filter window select the filter options, if any, that you want to apply, and then click OK. The system displays the Backup Job History window.

Note: If viewing the job history for a client computer, ensure that the **Backup** radio button is selected.

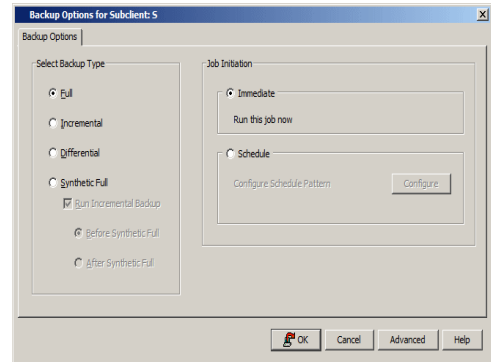
3. The Backup Job History window displays with the specified filter options.
4. Right-click on any job, and select **Resubmit Job**.



5. From the Backup Options dialog box, select the job options appropriate for the job you want to restart.

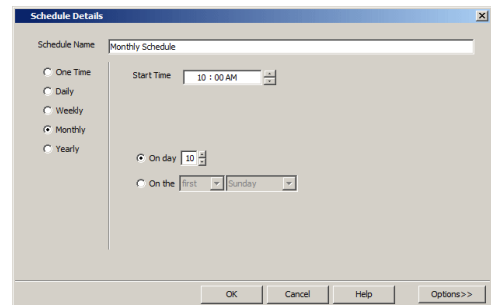


6. If you need to run the backup operation immediately, select **Immediate** from the **Job Initiation** tab. Go to step 11.
7. If you need to schedule the restore operation, select **Schedule** from the Job Initiation tab and click **Configure**.
8. From the **Schedule Details** dialog box that appears, select the appropriate scheduling options.



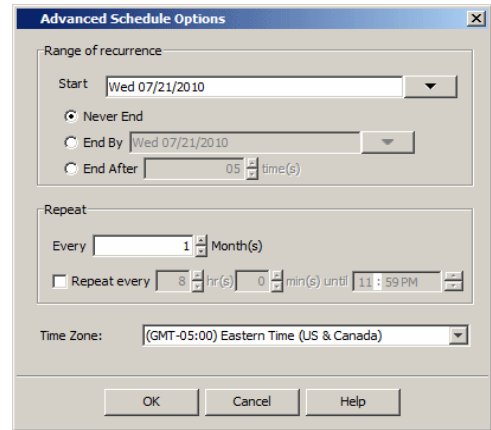
Click **Options** to view the Advanced Schedule Options dialog box.

9. From the **Advanced Schedule Options** dialog box:
 - **Range of recurrence:** Specify the date on which you want this schedule to take effect.



- **Repeat:** Select the value for which you want to run the job repeatedly on the day in which the job is scheduled to run.
- **Time Zone:** Select a specific time zone from which the job schedule time will be based.

Click **OK** to close the **Advanced Schedule Options** dialog box.



10. Click **OK** to close the **Schedule Details** window.
11. Click **OK** to close the job restart window.

[Back to Top](#)

Restore Job History

Topics | How To | Related Topics

Overview

Items That Restored

Supported Features

OVERVIEW

The **Restore History Filter** dialog box allows you to view detailed, historical information about restore jobs.

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

Once you have chosen your filter options, they are displayed in the **Restore Job History** window. From this window you can right-click a restore job to:

- View Restore Items; items in the job that were **Successful**, **Failed**, **Skipped** or **All**. These items, if any, will be listed in the **Restored Files** window.
 - View Job Details of the restore job. The job details will be listed in the **Job Details** window.
 - View Events of the restore job. The job events will be listed in the **All Found Events** window.
 - View Log files of the restore job. The job log files will be listed in the **Log File** window.
 - View the RMAN Log of an Oracle restore job. The RMAN Log will be listed in the **Oracle Restore Log** window.
 - View the BRTools log of a SAP for Oracle restore job. You can view the BRTools log for only those jobs that were initiated from the CommCell Console.
-

ITEMS THAT ARE RESTORED

When viewing files that are restored in the **Restored Files** window, each of the files is listed with the restore status level appended at the end of the file path. The possible status levels are: `RESTORED`, `FAILED` and `OLDER`.

Successfully restored files will be listed with `RESTORED` appended to the file path. If files are not restored/recovered due to errors, the file paths will be appended with `FAILED`. Under some circumstances, the system may not restore/recover certain files because they are older versions of the same files already present in the files system; these files are appended with the word `OLDER`.

SUPPORTED FEATURES

Consider the following.

- NAS iDataAgents do not support the ability to view failed/successful item lists.
 - Restore Job History will not display Oracle `rman_util` jobs at the instance level.
-

[Back to Top](#)

Restore History - How To

Topics | How To | Related Topics

[View Restore Job History](#)

[View the Events of a Job History](#)

[View the Media of a Job History](#)

[View the Log Files of a Job History](#)

VIEW RESTORE JOB HISTORY

▶ To view the restored items associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job restore history you want to view, click **View**, and then click **Restore 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 restored items you want to view; click **View Restore Items**, and select from the type of items to view: **Successful**, **Failed**, **Skipped** or **All**.
 4. The **Restored Files** window will display the selected type of restored items for the job.
 5. Click **OK**.
-

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 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](#)