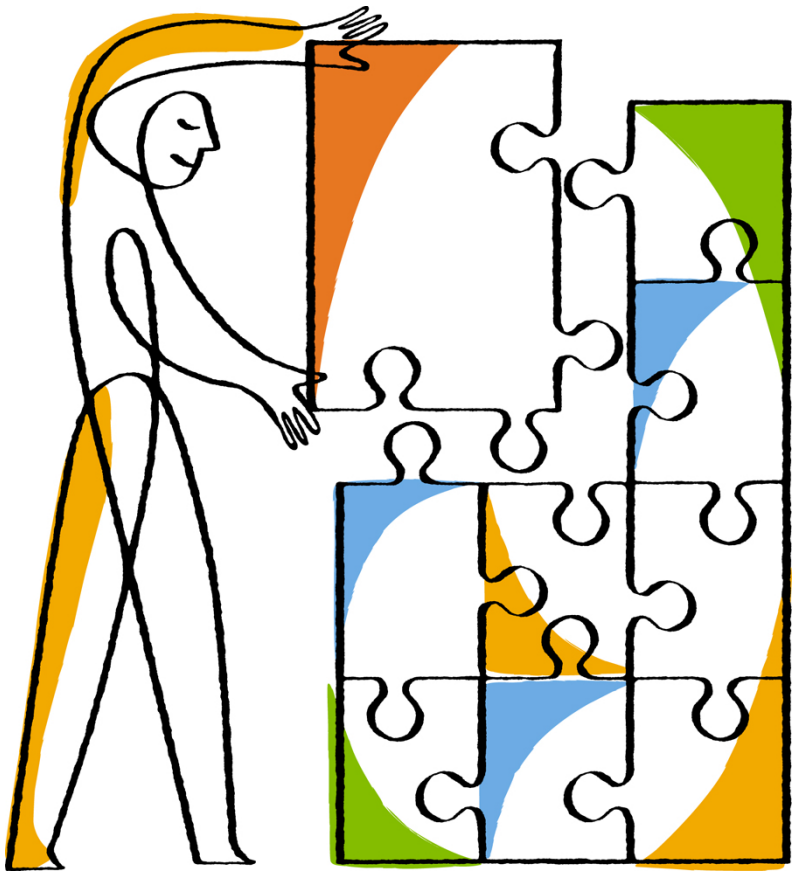
SnapProtect® Management Software 10.0

Upgrade Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1(408) 822-6000
Fax: +1(408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08672_A0
Date: December 2013

TABLE OF CONTENTS

1 Upgrading SnapProtect 9.0 to SnapProtect 10.0

Upgrading SnapProtect 9.0 to SnapProtect 10.0 requires preparation and post-upgrade procedures.

1.1 Overview of the upgrade process

The upgrade process includes the following phases.

- Preparing for the upgrade

  You must review the pre-upgrade considerations and verify that your system meets the requirements for perfoming the upgrade.

- Downloading the software installation package

  You must download the latest software installation package from the NetApp Support Site.

- Upgrading the CommServe database

  Before performing the upgrade, you must create a Disaster Recovery Backup of the production CommServe database and upload the database to NetApp Support for a precheck on the database.

- Upgrading SnapProtect software

  After you receive a successful status check from NetApp Support, you can perform the upgrade.

- Post-upgrade considerations

  You must review the post-upgrade considerations and complete the tasks based on the system configuration.

2 Preparing for the upgrade

Before contacting NetApp Support for a SnapProtect 9.0 to SnapProtect 10.0 database upgrade, you must ensure that you have reviewed the upgrade considerations and met the requirements.

You must review the following pre-upgrade considerations.

- Server considerations
- Modern data protection
- Virtualization
- Snapshot copy management

2.1 Server considerations before upgrading

You must consider issues with the following components before upgrading:

- CommCell component
- CommServe and CommCell Console
- MediaAgent
- Web server and Web Console

2.1.1 CommCell component issues before upgrading

You should review the CommCell component issues prior to upgrading.

Description
Client Version Before upgrading the CommServe, make sure that all the clients are in Version 9 or above. Only clients with software Version 9 are supported once the CommServe is upgraded. New features will not be available until the client is upgraded. Additionally, some existing features may not function as expected when the CommServe is upgraded to the current version. See Backward Compatibility Issues for more information on mixed version issues.
Supported Operating System/Application Version Before upgrading the CommCell components (CommServe, MediaAgents and Clients), make sure to check the System Requirements to see if the operating system/application version is supported in the current version. Additionally, several operating systems/applications are deprecated in the current version. See End-of-Life, Deprecated and Extended Support for more information. If the operating system/application version is not supported, ensure that the operating system/application is upgraded to a supported version first.
Jobs Before upgrading the CommCell components (CommServe, MediaAgents and Clients), make sure that there are no active jobs running in the CommServe. The upgrade will fail if any job is running during the upgrade process.
Renamed Licenses Several features and product licenses have been renamed and deprecated in this release. Before upgrading the CommCell verify the license-related comprehensive information on products and platforms that have been deprecated or placed on Extended Support. These licenses are explained in the following sections: • Renamed Feature Licenses • Renamed Product Licenses • Deprecated Licenses
Resource Pack If the Resource Pack utility is installed on the client computer which you want to upgrade, make sure to uninstall the utility before upgrading the client to the current version.
Client Certificate Authentication When you upgrade clients to the current software version in a lock-down mode on CommCell, it is recommended that you disable the lock-down mode for the upgrade to complete successfully. In a lock-down mode the authentication of client certificates is enforced during installation. Use the following criteria when planning the client upgrade: 1. Disable the certificate authentication for the CommServe.

Description
2. Upgrade the clients. 3. Enable the certificate authentication for the CommServe. For step-by-step instructions on enabling/disabling certificate authentication, see Enforce Client Certificate Authentication on the CommServe.
Upgrading Clients in a Microsoft cluster environment It is required that each node maintains its status (Active or Passive) throughout the upgrade session. If the Active node needs a reboot during the upgrade process, upon reboot, it should be made an Active node again before resuming the upgrade operation. If the status of the nodes (Active or Passive) is not maintained throughout the upgrade session, then the cluster plug-in resource may get removed after the upgrade operation is complete.

2.1.2 CommServe and CommCell Console issues before upgrading

You should review the CommServe host and CommCell Console issues before upgrading.

Description
CommServe must have at least Service Pack 7 installed Before upgrading the CommServe to the current release, make sure that the CommServe computer has at least Service Pack 7 (SP7) of Version 9 installed.
CommServe upgrade now requires at least three times the size of the current database Before upgrading the CommServe, make sure that the free disk space on the CommServe computer is at least three times the size of your current database. For more information, see FAQs - Upgrades.
CommServe SQL server login credentials Before upgrading the CommServe, make sure you have the login credentials for the CommServe SQL server.
Database Engine The CommServe Database Engine will be upgraded to Microsoft SQL Server 2008 database with the service pack during the CommServe upgrade. If SQL Server has a later Service Pack, make sure to download and install the service pack and/or critical updates after the CommServe upgrade. SQL Server 2008 is not supported on Windows 2000. If your CommServe resides in Windows 2000, upgrade the operating system prior to the CommServe upgrade. SQL Server 2008 is applicable for CommServe, CommNet Server, and Content Indexing Engine.

Description
CommServe and SQL Server on different computers not supported Installing the CommServe and the SQL Server on different computers is no longer supported on this release. If you have this setup configured on a previous release, it is recommended that you move the CommServe database back to the CommServe computer before the upgrade. See Upgrade the CommServe and Database Engine on Separate Computers for more information.
Deprecated versions for CommServe The CommServe software is no longer supported on computers running Windows 32-bit versions and Windows Server 2003 editions. Refer to Deprecated Platforms for a comprehensive list. You can migrate existing CommServe to a Windows x64-bit Server using Install/Upgrade the CommServe With an Existing Database. Refer to System Requirements for a list of supported versions.
Java Runtime Environment (JRE) The software can function with JRE version 1.7.x or higher. If a JRE version 1.7.0_17 or higher is available, the software will use the existing JRE software. If JRE version is lower than 1.7.0_17, or no JRE version is available at all, you will be prompted to install JRE version 1.7.0_17. You can run the CommCell Console as a Remote Web-Based Application without installing the software; provided IIS is installed and running on the CommServe computer. Alternatley the CommCell Console and IIS can run on an different computer. However, you must manually install JRE in this case. When running the applet Java™ Runtime Environment (JRE) SE v1.6.0_06 is recommended - can be installed from the software installation disc.
CommCell Console Shortcut If you have created or copied shortcuts for the CommCell Console on your desktop or Start menu, you should delete them before the upgrade and re-copy the new shortcut which is created during the upgrade.
Update MediaAgents and Clients with the latest service pack Prior to upgrading the CommServe, make sure the MediaAgents and Clients are updated with the latest Service Pack of the previous version.

2.1.3 MediaAgent component issues before upgrading

You should review the MediaAgent issues before upgrading.

Description
Upgrade Sequence Upgrade the MediaAgent first, before upgrading the clients attached to the MediaAgent. Make sure to upgrade all the clients associated with the MediaAgent as soon as the MediaAgent is upgraded. New features will not be available until the MediaAgent is upgraded. Additionally, some existing features may not function as expected when the CommServe is upgraded to the current release. See Backward Compatibility Issues for more information on mixed version issues.
Upgrade all the related MediaAgents All related MediaAgents must be upgraded together. MediaAgents are considered as 'related' for the following features: • Index Cache Server - All MediaAgents associated with an Index Cache Server. • Subclients in a backupset or instance - All MediaAgents associated with the subclients in a backupset or instance must be upgraded together, especially if the wildcards are used to define the contents of any of the subclients. • Auxiliary Copy - Auxiliary Copy operations are not supported if the source and destination MediaAgents are not at the same release.
Libraries Ensure that no tapes are mounted in the drives of libraries attached to the MediaAgent you wish to upgrade.
Optical Library is deprecated Optical Library is deprecated in the current release. When you upgrade a MediaAgent with an Optical Library attached, the upgrade will fail. In such situations, the MediaAgent with the Optical Library can remain in the previous version or you can deconfigure the Optical Library and then perform the upgrade.
Show deleted files across cycles Browse and Find operations will not show deleted items across cycles, if MediaAgent is at an earlier version of the software than the CommServe. It is recommended to upgrade all MediaAgents to the same version as the CommServe.

Description
Mount path location Before upgrading MediaAgent, if you have created Disk Library under <Software_Installation_Directory> location change the mount path location to different location and then copy all the content (files and folders) under the existing mount path to new mount path. Use the following steps to change the mount path location: 1. From the Version 9 CommCell Console, click the **Control Panel** icon. 2. From the **Control Panel**, click the **Library and Drive Configuration** icon. 3. Select the MediaAgent whose devices you want to detect and click **OK**. 4. Click **OK** to continue. 5. Locate the disk library for which you wish to move the mount path. 6. Right-click the mount path that you wish to move and then select **Properties**. 7. From the **Mount Path Properties** dialog box, enter the new path: • If you select **Local Path**, click **Browse** to select a mount path, or type a mount path. • If you select **Network Path**, type the user name and password to access the network share. Click **Browse** to select a mount path, or type a mount path. 8. Click **OK** to save the information. The mount path is moved to the specified location. 9. Copy all files and folder available under old mount path location to new mount path location.

2.1.4 Web server and Web Console issues before upgrading

You should review the Web server and Web Console issues before upgrading.

Description
Not backward compatible The Web Server and Web Console are not backward compatible. When the CommServe is upgraded to the current software version, the Web Server and Web Console must also be upgraded.
Cannot be remotely installed from the CommCell Console The Web Server and Web Console cannot be remotely installed from the CommCell Console. You can install them using the interactive install method.
Web Client renamed The Web Console was referred as ‘Web Client’ in the previous releases. When the Web Client is upgraded to the current version, both the Compliance Search and the Web Console components are

Description
installed as part of the upgrade.
Deprecated versions for Web Server • The Web Server software is no longer supported on computers running Windows 32-bit versions and Windows Server 2003 editions. • You must decommission the existing Web Server on 32-bit and install a new Web Server on Windows x64-bit Server. Refer to System Requirements for a list of supported versions.
Deprecated versions of Web Console • The Web Server software is no longer supported on computers running Windows 32-bit versions and Windows Server 2003 editions. Refer to System Requirements - Web Server for a list of supported versions. • The Web Console software is no longer supported on computers running Windows 32-bit versions. Refer to System Requirement - Web Console for a list of supported versions.

2.2 Modern data protection issues before upgrading

You should review data protection issues before upgrading.

Component	Description
Active Directory	**User priviledges** To upgrade Active Directory iDataAgent, you require specific user privileges. Before upgrading, review the User Privileges table to identify the privileges.
DB2 iDataAgent	**Pre-upgrade considerations** Make sure to stop the DB2 services before upgrading SnapProtect on a DB2 client. • Insufficient memory may cause 32-bit client upgrades to fail on AIX computers as memory requirement has increased due to added functionality. In such cases, it is recommended to grant read permissions for others (chmod o+r) on shared libraries and executables during upgrade so that the services start without issues. This can be done by setting the sAIXGrantReadPermForOthers registry key on the CommServe. See Troubleshooting - Upgrades for more information. • Before performing a remote upgrade on an AIX client computer, installed binaries should have read permissions for other users. Use the following steps to add read permissions to other users: 1. Ensure that no jobs are running on any SnapProtect instance. You have to restart SnapProtect services for all instances to

Component	Description
	change the permissions. 2. From the Command Prompt, run the following command: *cvpkgchg* 3. Type **2** and press **Enter**. 4. Select the type of permission that you want to assign to other users and press **Enter**. 5. Type **Yes** to change the permissions. 6. Restart SnapProtect services for all instances to change the permissions.
Exchange Server	**Browse from Backup Set Level is not supported on clients from previous version** If the CommServe is upgraded and client is still at an older version and the content of the defaultBackupSet is modified, then browse will operations will not work from the Backup Set level. In such cases, • Browse and Restore at the Subclient level. • Upgrade the Client computer and related MediaAgent to the same version as the CommServe and then run a Browse and Restore operation at the Backup Set level.

Image Level iDataAgent	**Changing settings before upgrade**
	
	• If you have manually changed any of these settings in the previous release, they will not be preserved after the upgrade:
	  ○ COW cache size (Minimum and Maximum)
	  ○ COW cache location
	• The required CVD resource dependencies set on the virtual node of the cluster will not be preserved in the upgrade.

	QSnap If you are using the QSnap snapshot enabler with this agent, see The Block Filter Driver and Bitmaps for important information about how the QSnap block filter operates.
Microsoft SharePoint Server	**Upgrade not available** Upgrade in the current release is not available for Microsoft SharePoint Server. Before upgrading the CommServ, you must uninstall the Microsoft SharePoint Server.
NAS iDataAgent	**Automatically upgraded with CommServe** NAS iDataAgent is automatically upgraded with the CommServe.

Component	Description
Oracle iDataAgent	**Pre-upgrade considerations** • Insufficient memory may cause 32-bit client upgrades to fail on AIX computers as memory requirement has increased due to added functionality. In such cases, it is recommended to grant read permissions for others (chmod o+r) on shared libraries and executables during upgrade so that the services start without issues. This can be done by setting the sAIXGrantReadPermForOthers registry key on the CommServe. See Troubleshooting - Upgrades for more information. • Before performing a remote upgrade on an AIX client computer, installed binaries should have read permissions for other users. Use the following steps to add read permissions to other users: 1. Ensure that no jobs are running on any SnapProtect instance. You have to restart SnapProtect services for all instances to change the permissions. 2. From the Command Prompt, run the following command: *cvpkgchg* 3. Type **2** and press **Enter**. 4. Select the type of permission that you want to assign to other users and press **Enter**. 5. Type **Yes** to change the permissions. 6. Restart SnapProtect services for all instances to change the permissions.
ProxyHost	**Upgrade - Merged Product** The functionality in this product is now available in SnapProtect Backup. We recommend that you transition to SnapProtect Backup. Contact your Software Provider if you need assistance in transitioning to SnapProtect Backup. New installations and upgrades are not supported.
SnapProtect-OSSV Plug-in	**Upgrade** The SnapProtect-OSSV Plugin continues to be supported in Version 10. We strongly recommend transitioning to the new SnapProtect for Open System capabilities, which enables file catalog and tape integration with native SnapProtect clients. See the IMT for supported platforms and applications.
SAP iDataAgents	**Pre-upgrade Considerations**

Component	Description
	• Insufficient memory may cause 32-bit client upgrades to fail on AIX computers as memory requirement has increased due to added functionality. In such cases, it is recommended to grant read permissions for others (chmod o+r) on shared libraries and executables during upgrade so that the services start without issues. This can be done by setting the sAIXGrantReadPermForOthers registry key on the CommServe. See Troubleshooting - Upgrades for more information. • Before performing a remote upgrade on an AIX client computer, installed binaries should have read permissions for other users. Use the following steps to add read permissions to other users: 1. Ensure that no jobs are running on any SnapProtect instance. You have to restart SnapProtect services for all instances to change the permissions. 2. From the Command Prompt, run the following command: *cvpkgchg* 3. Type **2** and press **Enter**. 4. Select the type of permission that you want to assign to other users and press **Enter**. 5. Type **Yes** to change the permissions. 6. Restart SnapProtect services for all instances to change the permissions.
UNIX File System iDataAgents	**Pre-upgrade considerations** • Insufficient memory may cause 32-bit client upgrades to fail on AIX computers as memory requirement has increased due to added functionality. In such cases, it is recommended to grant read permissions for others (chmod o+r) on shared libraries and executables during upgrade so that the services start without issues. This can be done by setting the sAIXGrantReadPermForOthers registry key on the CommServe. See Troubleshooting - Upgrades for more information. • Before performing a remote upgrade on an AIX client computer, installed binaries should have read permissions for other users. Use the following steps to add read permissions to other users: 1. Ensure that no jobs are running on any SnapProtect instance. You have to restart SnapProtect services for all instances to change the permissions.

Component	Description
	2. From the Command Prompt, run the following command: *cvpkgchg* 3. Type **2** and press **Enter**. 4. Select the type of permission that you want to assign to other users and press **Enter**. 5. Type **Yes** to change the permissions. 6. Restart SnapProtect services for all instances to change the permissions.
	Tru64 File System is on Extended Support Tru64 File System is on Extended Support and cannot be upgraded. Refer Product on Extended Support for more information.
	Browse from Backup Set Level is not supported on clients from previous version If the CommServe is upgraded and client is still at an older version and the content of the defaultBackupSet is modified, then browse will operations will not work from the Backup Set level. In such cases, • Browse and Restore at the Subclient level. • Upgrade the Client computer and related MediaAgent to the same version as the CommServe and then run a Browse and Restore operation at the Backup Set level.
Windows File System iDataAgent	**Browse from Backup Set Level is not supported on clients from previous version** If the CommServe is upgraded and client is still at an older version and the content of the defaultBackupSet is modified, then browse will operations will not work from the Backup Set level. In such cases, • Browse and Restore at the Subclient level. • Upgrade the Client computer and related MediaAgent to the same version as the CommServe and then run a Browse and Restore operation at the Backup Set level.
	Number of Objects Backed up appears higher on a Client with Older Version of the software If the MediaAgent and CommServe are in the current version and client is in the previous version, then the number of objects displayed in the Job Details dialog box is higher as the parent/root folders of files that are not changed are also taken into account in this release.

2.3 Virtualization issues before upgrading

You should review virtualization issues before upgrading.

Component	Description
VMware	**Upgrade not available** Upgrade in the current release is not available for this product.
	MediaAgent upgrade If Virtual Server iDataAgent and MediaAgent are installed on the same client computer, you cannot upgrade the MediaAgent.
	CommServe upgrade If Virtual Server iDataAgent and CommServe are installed on the same client computer, you cannot upgrade the CommServe.
	ESX Server Instance upgrade You cannot upgrade the Virtual Server iDataAgent if you have configured an instance for an ESX server using 9.0 Virtual Server iDataAgent. Before upgrading the Virtual Server iDataAgent, change the instance type from ESX server to vCenter for all instances, then upgrade the Virtual Server iDataAgent.
	Upgrade when the file level and volume level backups are configured You cannot upgrade the Virtual Server iDataAgent if you have configured file level and volume level backups using 9.0 Virtual Server iDataAgent. Before upgrading the Virtual Server iDataAgent, change the file level or volume level backup to disk level backup for all subclients and then upgrade the Virtual Server iDataAgent. After the upgrade, consider the following: • You cannot restore VMDK files from the old volume level backups. • You can restore the guest files and folders from the old volume level and file level backups. However, you must browse to the older backup and then restore the data. If you have scheduled any restores (File level restore or VMDK restore), the restore job will fail. For more information, refer to Restoring Files and Folders and Browse and Restore Data Before a Specified Backup Time.
	Upgrading Proxies in Master Configuration All the proxies in the Master configuration and the master proxy must be upgraded simultaneously. If any proxy is not upgraded, the scheduled backup jobs may fail.
	Upgrading the Proxy that is used for Movement to Media Operation

Component	Description
	During the SnapProtect operation, you can use a separate proxy for movement to media operation. When you upgrade any such proxy, ensure that the proxy which is used for the SnapProtect backup is upgraded. For more information refer to Using Separate Proxy for Backup Copy and SnapProtect Configuration.

2.4 Snapshot copy management issues before upgrading

You should review Snapshot copy management issues before upgrading.

Component	Description
VMware and Exchange Mailbox	Before performing a Snap Mining job, consider the following: • If you are upgrading the Exchange Mailbox iDataAgent on a virtual machine, you must upgrade the Virtual Server iDataAgent on the Proxy computer, which is used to perform the SnapProtect backup of the virtual machine. • When you upgrade the Exchange Mailbox iDataAgent and Virtual Server iDataAgent, the next Exchange Mining backup will automatically convert to Full backup.

2.5 Frequently Asked Questions

See Frequently Asked Questions for more information about general considerations during upgrade.

3 Downloading the software installation package

You must download the software installation package from the NetApp Support Site to perform the upgrade.

4 Upgrading the CommServe Database

Before running the upgrade for a SnapProtect 9.0 to SnapProtect 10.0 database, you must contact NetApp Support for a pre-upgrade check. You have to upload the backup of a production CommServe database to NetApp Support.

NetApp Support verifies the database and on a successful status check, you can run the upgrade to SnapProtect 10.0.

4.1 Space Requirements

Before running the upgrade, you must ensure the free disk space on the CommServe host system is at least three times the size of the current database size. The size of the CommServe database will be the same as the size of the Disaster Recovery Backup file (`<cs_sitename>_FULL.dmp`).

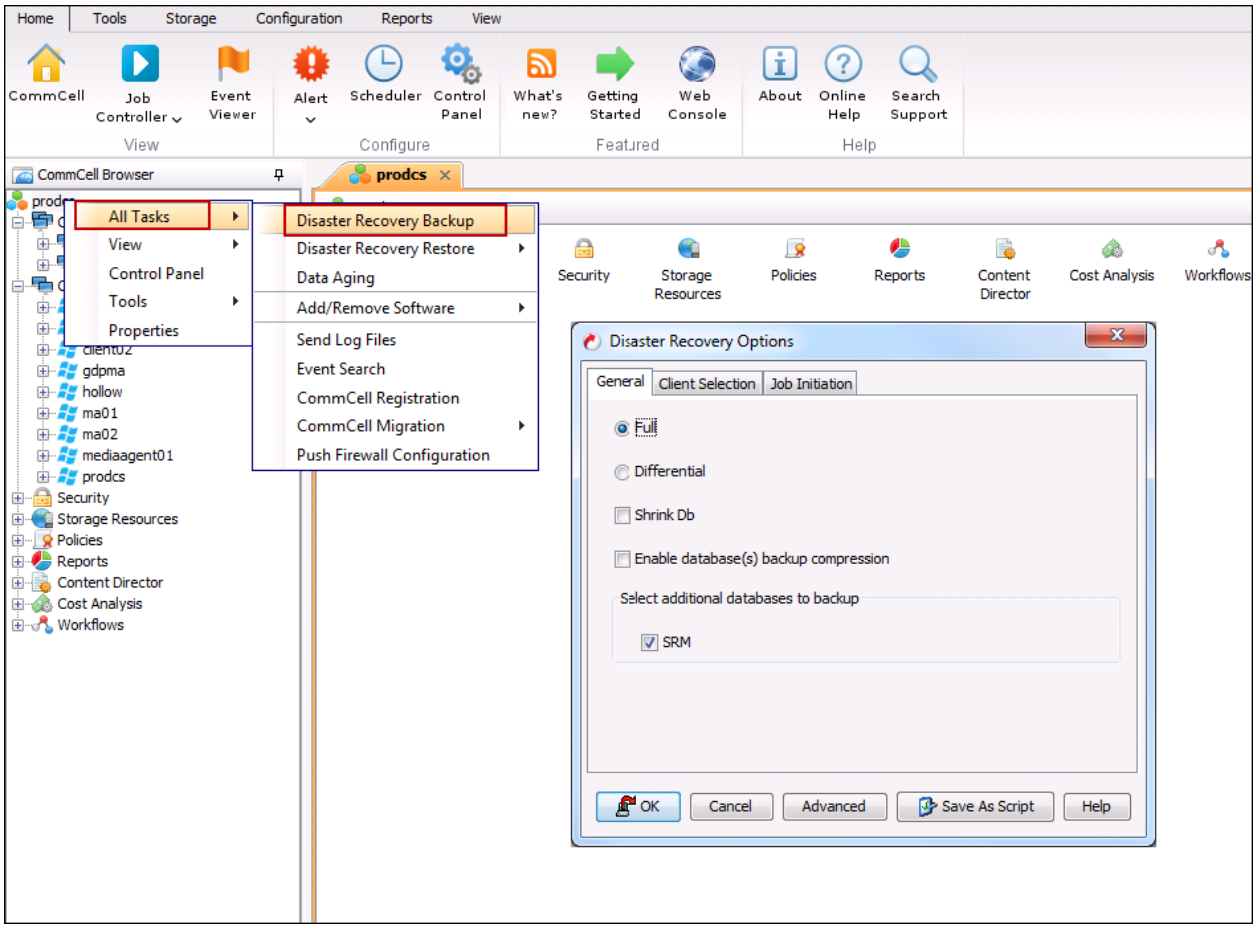
4.2 Creating the CommServe database backup

You must perform a Disaster Recovery Backup of a production CommServe database.

Important:The database upgrade fails if SharePoint iData agent is installed on the CommServe host. If you have installed the SharePoint iData agent on the CommServe host, you must uninstall the agent and then create a backup of the production CommServe database.

1. From the CommCell Browser, right-click the **CommServe**, point to **All Tasks**, and then click **Disaster Recovery Backup**.
2. By default, the backup type is selected as **Full**.
3. Click the **Client Selection** tab to backup up the log files from clients with your CommCell.
4. Select the client(s) from the available list of clients.
5. Click **OK** to run the job immediately.

Make sure the that the associated disaster recovery folder (SET_XXX folder) is saved and available in a safe location.

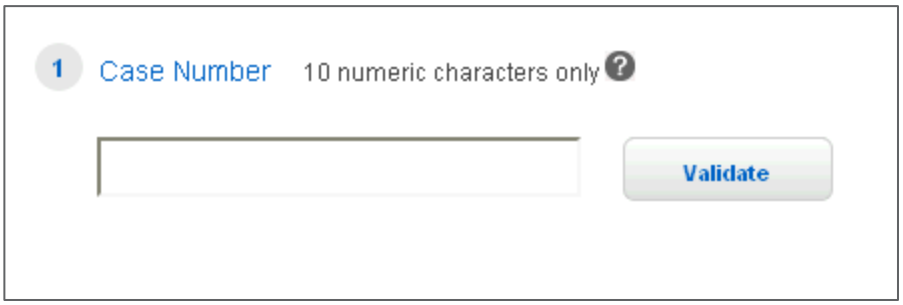


The Disaster Recovery Backup file is created when a Disaster Recovery backup is performed from the CommCell Console. Disaster Recovery Backup files are located in the `SET_XXX` folders (where XXX is replaced by a sequential number and the folder with the highest number contains the latest Disaster Recovery Backup set). The `SET_XXX` folders are located in the File System directory selected during the installation of CommServe. This folder contains a number of files, including a `.dmp` file.

4.3 Uploading the CommServe database to NetApp Support

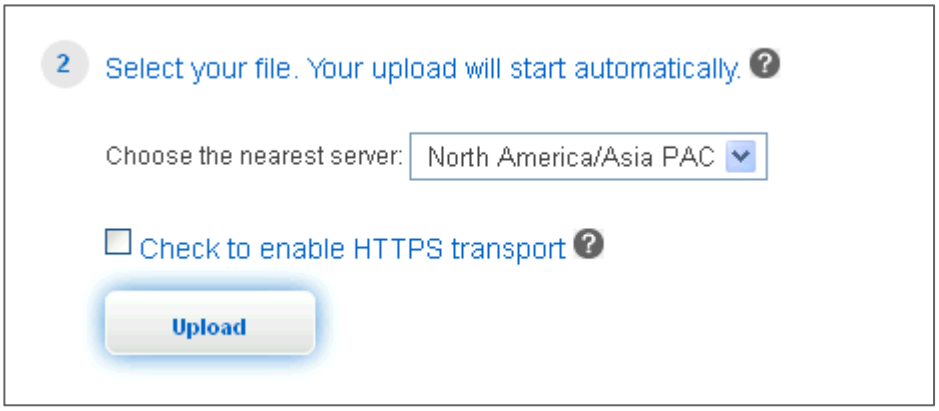
You must contact NetApp Support to check the Disaster Recovery Backup of the production CommServe database. You must upload the CommServer database Disaster Recovery backup to NetApp Support using the NetApp File Upload Utility.

1. Go to upload.netapp.com.
2. If Aspera Connect plug-in is not installed on your computer, you must complete the on-screen instructions to install Aspera Connect.
3. In order to associate the database backup file you are uploading with the support case number given by NetApp Support, type the 10 digit case number. Click **Validate**.



4. After the support case number is validated, select the nearest server to which you want to upload the database backup file.

   Note: You can select only one file during the upload.



5. Select the **Check to enable HTTPS transport** check box, if you want to use HTTPS transport for the upload.

   Note: You can choose this option if the outbound TCP and UDP ports 33001 are not accessible. The HTTPS uploads face limitations with speed and reliability. You must check with your network administrator before enabling the outbound ports for HTTPS transport.

6. Click **Upload** to select the database backup file that you want to upload.

NetApp Support runs a check on the database backup and acknowledges if the database meets the minimum system requirements. If the status check determines that your environment is not ready, NetApp support provides details on the additional actions to be performed before running the another database

check against the Disaster Recovery backup. After you receive a successful status check notice, you can upgrade the CommServe database.

4.4 Upgrading the CommServe database

If you have installed SnapProtect 9.0, upgrade to SnapProtect 10.0 is supported. If the version currently installed is not listed, contact NetApp Support.

> **Note**: For optimal performance, it is recommended that you upgrade the client to the same version as the CommServe database after upgrading the database.

You can migrate existing CommServe to a Windows x64-bit Server using Install/Upgrade the CommServe With an Existing Database.

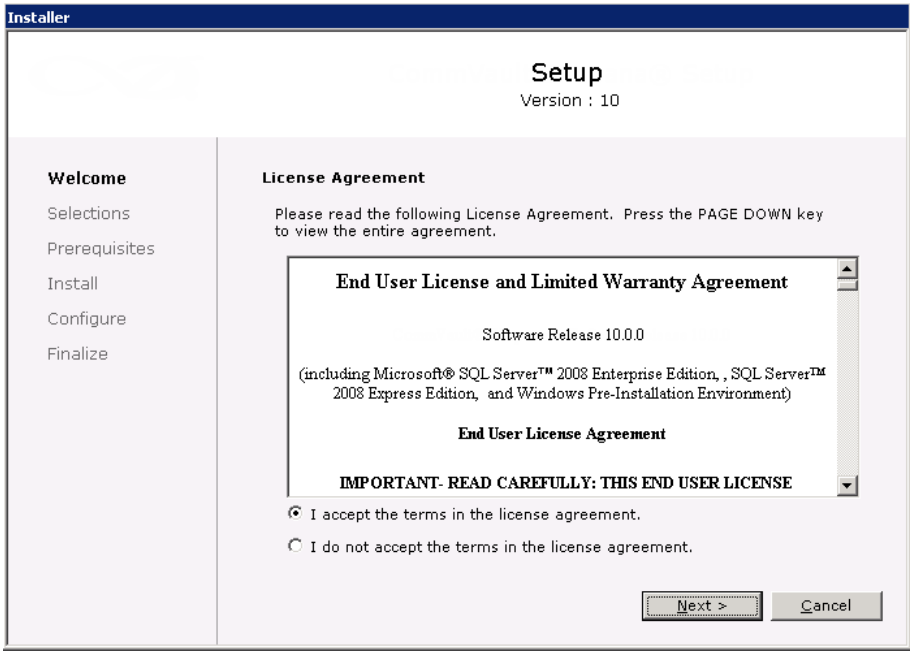
4.4.1 Before you begin upgrading the database

- You must have reviewed the minimum requirements specified in System Requirements
- You must have verified that the latest Service Pack of previous release is installed on the CommServe system
- You must have downloaded the latest software package from the NetApp Support Site
- You must have verified the production CommServe database Disaster Recovery Backup with NetApp Support

4.4.2 Upgrading the database

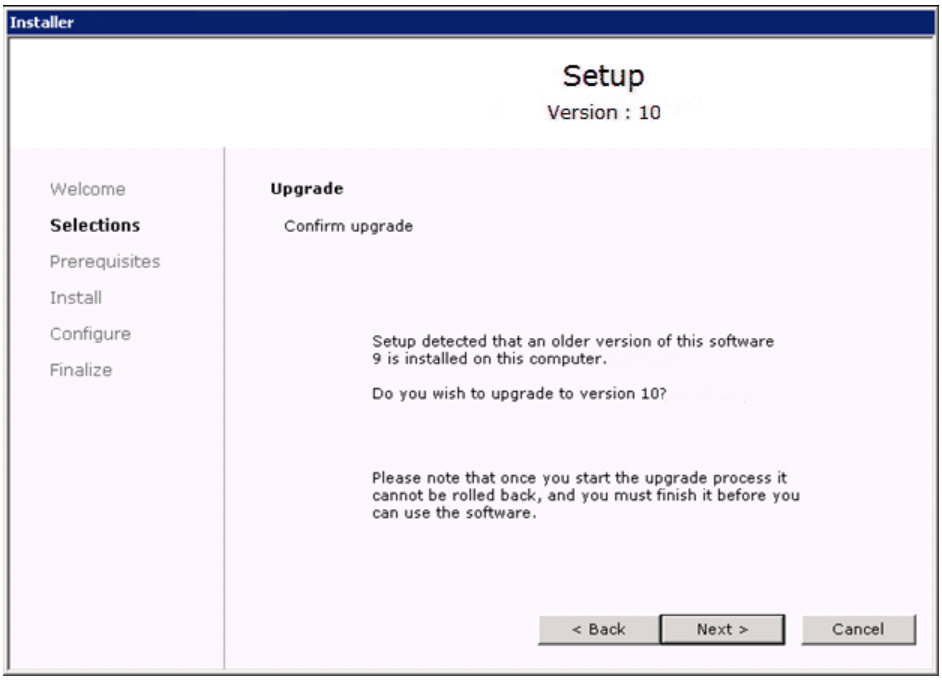
1. If you are upgrading a CommServe on a cluster, you must first upgrade the Microsoft SQL Server, as described in the SQL Server Upgrade section. You can skip this step if the SQL database has been already upgraded.
2. Log on to the CommServe as an Administrator or as a member of the Administrator group on that computer.
3. Make sure that there are no active jobs in the CommServe before you start the upgrade. Upgrade will fail if there is any job running during the upgrade process.
4. Disable Anti-virus software on the computer.
5. Run **SetupAll.exe** from the Software Installation Discs.
6. Click **I accept the terms in the license agreement**.

   Click **Next**.



7. Click **Next** to continue with the upgrade.

   Note: The older version number depends on the version in the computer and may look different from the example shown.

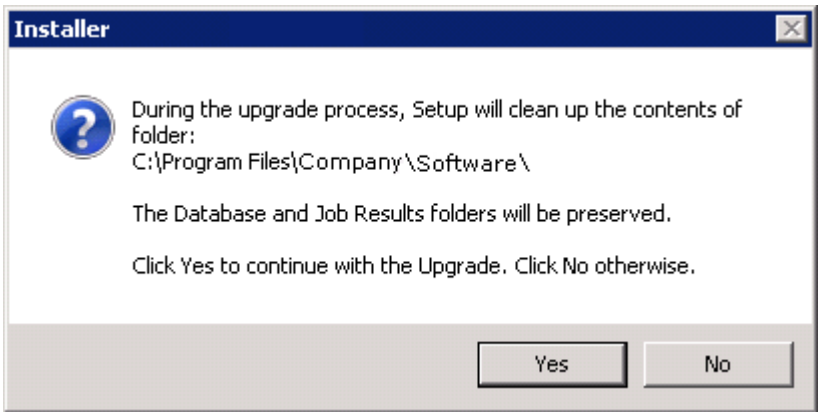


8. Click **Yes** to continue.

   Note: The upgrade process deletes and replaces this folder with newer files. To preserve this, move them to another location before clicking **Yes**.

   The upgrade process does not save any files such as command line scripts or folders from the <software installation path> folder.

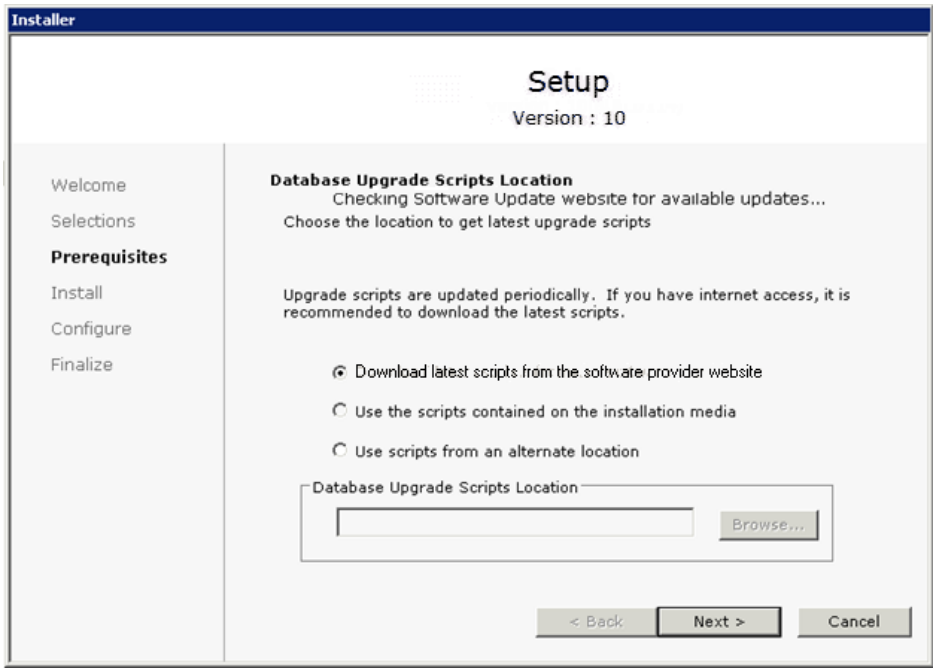
Clicking **No** will exit the upgrade program.



9. Click **Next** to download the latest upgrade scripts from the software provider website. Make sure you have internet connectivity for downloading the scripts.

   The upgrade program copies the necessary database scripts to the install location before running them.

   Note: Select “Use the scripts contained on the installation media” to continue the upgrade from the current location.
   Select “Use scripts from an alternate location”, if you have the software package in an alternate location. Type the location of the software package directory, or click Browse to choose the location.



10. Click **Yes** to back up the CommServe database.

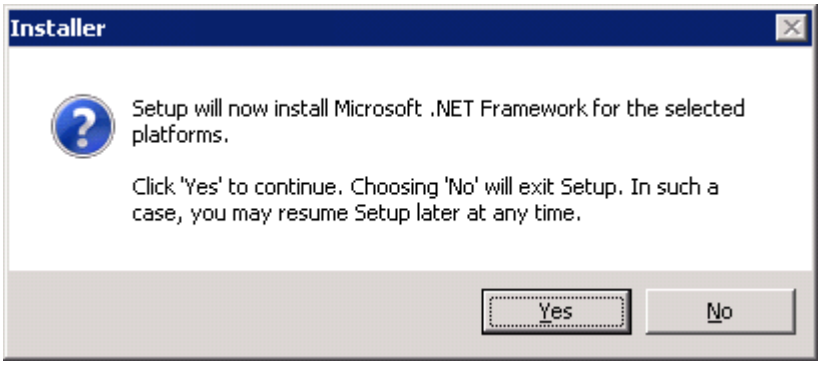
    Note: Clicking **No** will abort the upgrade.
    The size of the CommServe Disaster Recovery depends on the size of the CommServe Database Engine in your environment and may look different from the example shown.

11. Click **Yes** to install the Java Runtime Environment (JRE) or click **No** if you would like to use the JRE Version already available in your computer.

    Note: This prompt will be displayed only if the computer is running a JRE version older to the one supplied in this installation program or no JRE version is available at all. See System Requirements - CommServe for more information on JRE versions.

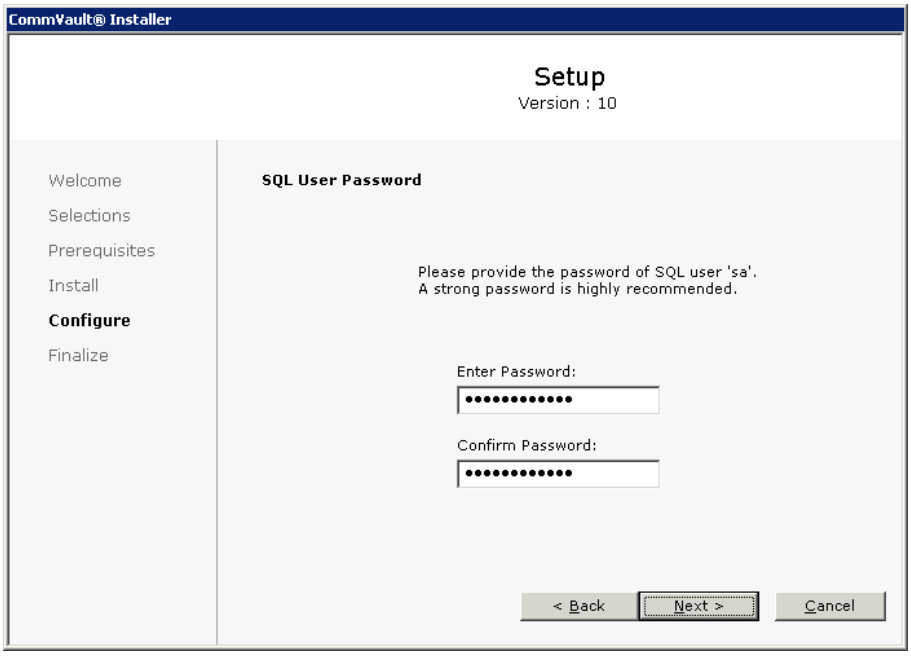
12. Click **Yes** to install Microsoft .NET Framework.

    Note: This option will only appear if Microsoft .NET Framework has not been installed on this computer.

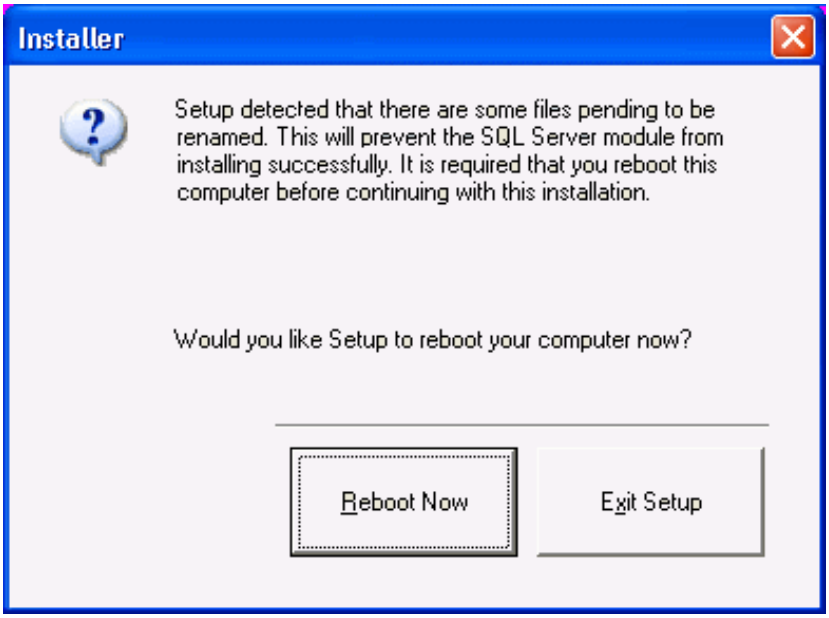


13. Specify the SQL Server System Administrator password.
    Click **Next**.

    Note: This is the password for the administrator's account created by SQL during the installation.



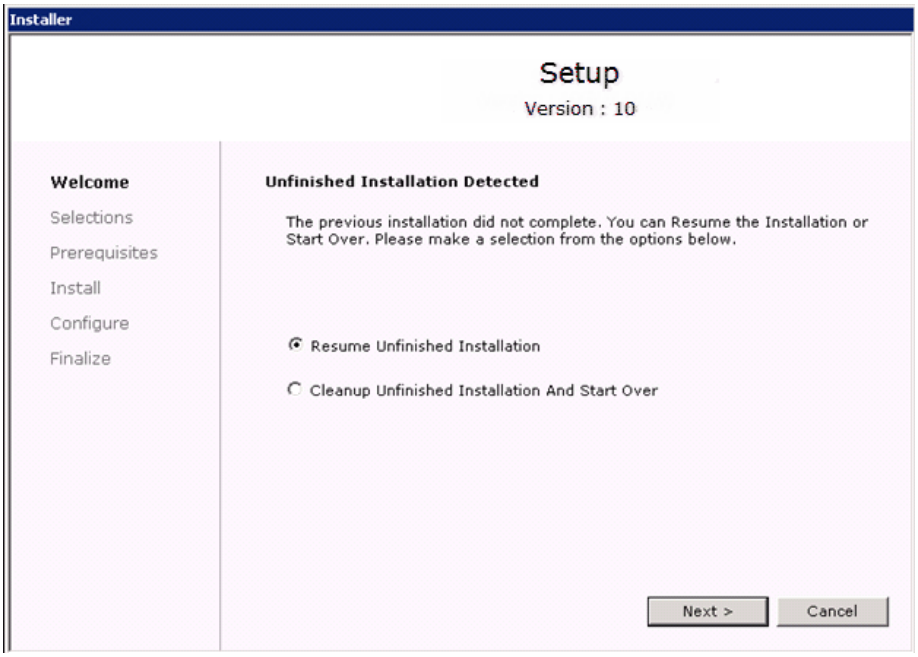
14. Click **Reboot Now**.



5 Upgrading the SnapProtect software

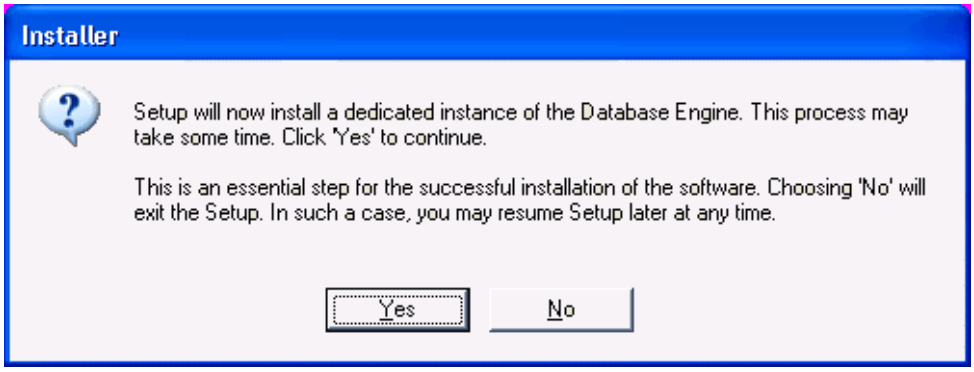
1. After the reboot, run **SetupAll.exe** from the Software Installation Discs or the downloaded software installation package.

2. Click **Next** to resume the installation.



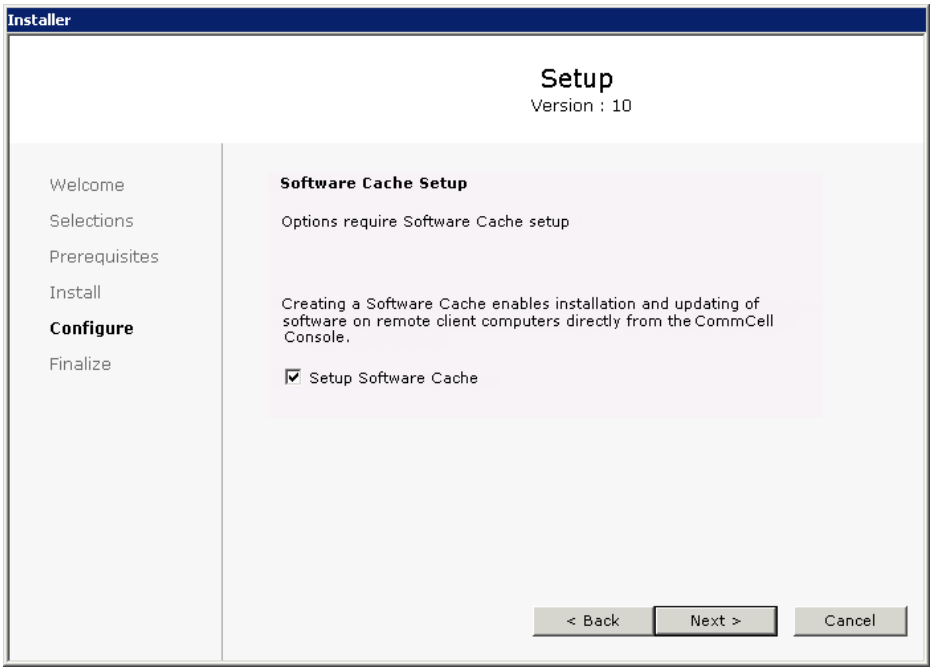
3. Click **Yes** to set up a dedicated instance of Microsoft SQL Server for the CommServe Server.

   Note: This prompt will only be displayed if SQL Server database instance is not installed on this computer. Clicking No will exit the install program.



4. Click **Next**.

   If you do not want to allow the CommServe to install software and updates to remote client computers, click to clear the **Setup Software Cache** check box and then click **Next**.

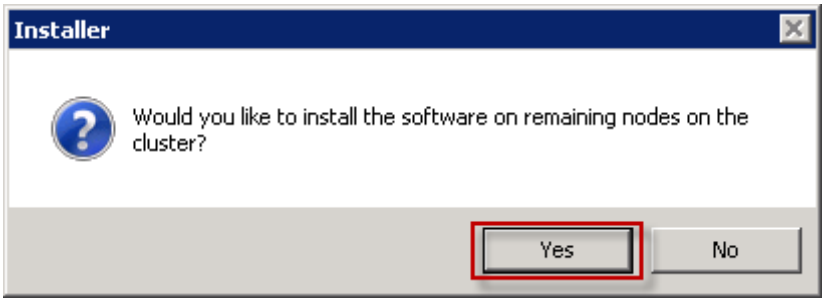


5. Verify the summary and Click **Install**.

   Note: The Summary on your screen will reflect the components installed on the computer, and may look different from the example shown. The upgrade program now starts the upgrade process. This step may take several minutes to complete.

6. Click **Yes**.

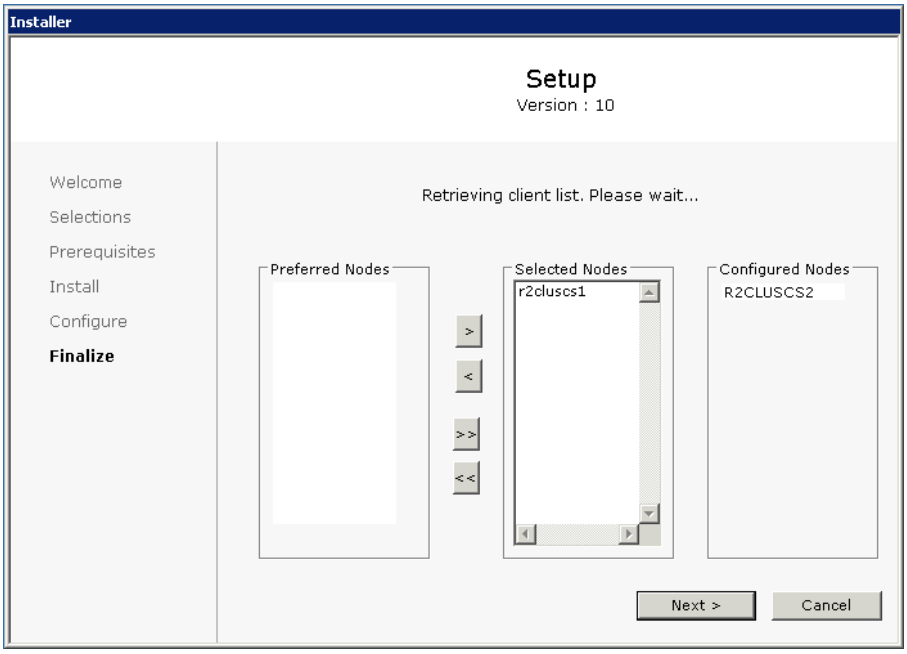
   You will see this dialog box if you are upgrading a clustered CommServe.



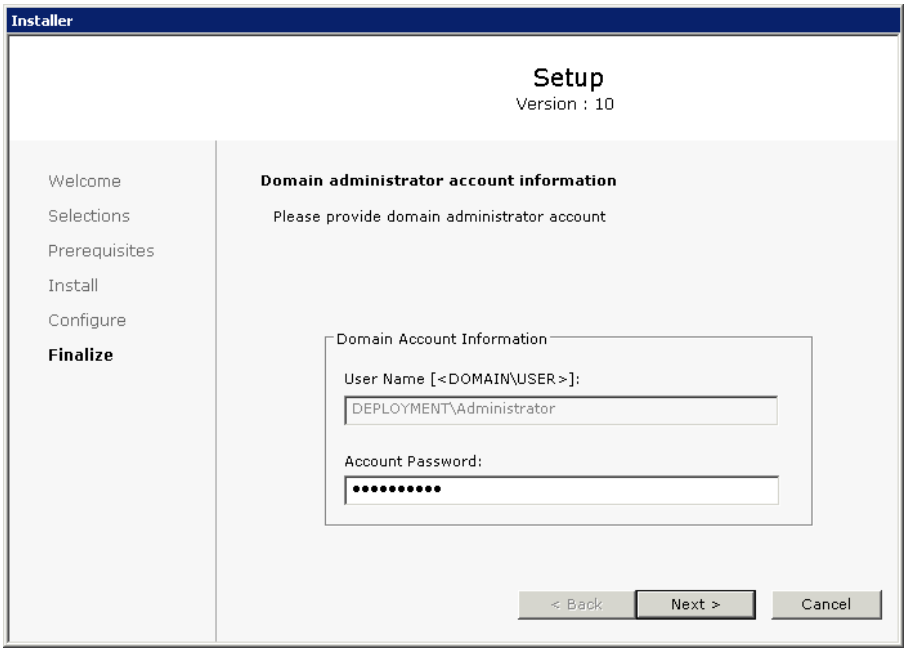
7. Select the cluster nodes where you also want to upgrade the CommServe from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

   Click **Next**.

   Note: The list of Preferred Nodes displays all the nodes found in the cluster. It is recommended that you select the cluster nodes that are configured to host this cluster group. Do not select nodes that already have multiple instances installed.

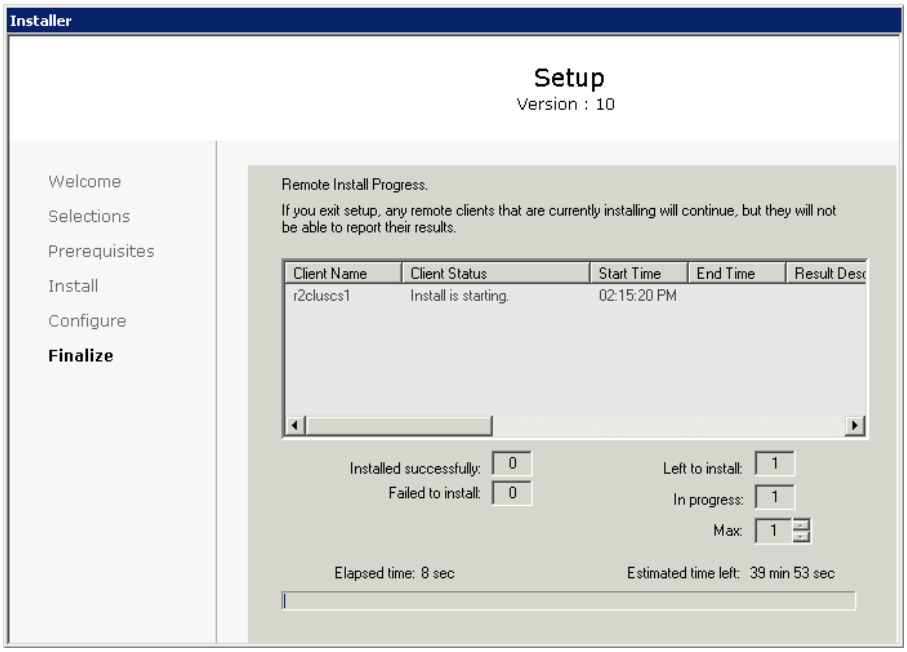


8. Type the **Password** for the Domain Administrator account to upgrade the CommServe on the selected cluster nodes.
   Click **Next**.



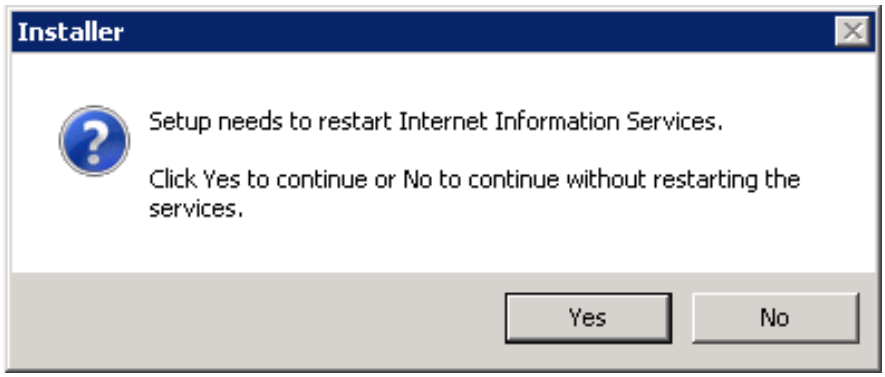
9. The progress of the remote upgrade for the cluster nodes is displayed.

   Note: If the remote upgrade of a cluster node fails to complete or is interrupted, you will need to separately upgrade the software on that node using the steps described in Manually Installing the Software on a Passive Node. For example, the install may fail if one of the cluster nodes is not in the cluster group domain.



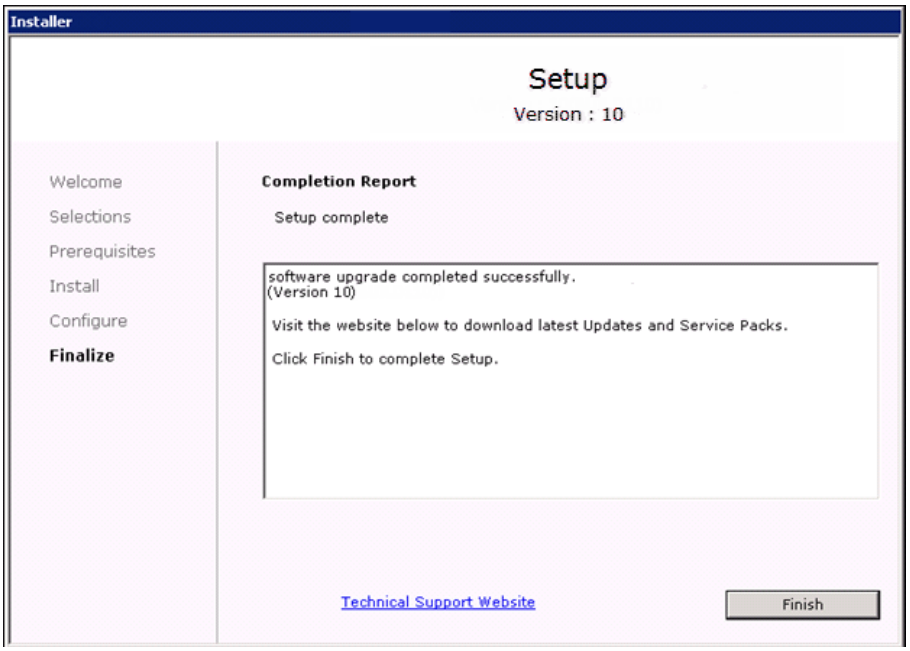
10. Click **Finish**.

11. Click **Yes**.



12. Click **Finish** to complete the upgrade.

    Note: The Completion Report will reflect the components upgraded on the computer, and may look different from the example shown.



6 Post-upgrade considerations

You should review the following considerations after upgrading:

- Server considerations
- Modern data protection
- Virtualization
- Snapshot copy management

6.1 Server considerations after upgrading

You must consider issues with the following components after upgrading:

- CommCell component
- CommServe and CommCell Console
- MediaAgent
- Web server and Web Console

6.1.1 CommCell component issues after upgrading

You should review CommCell component issues after upgrading.

Description
Firewall If you have a direct connection setup where the client computer connects to the CommServe (one-

Description
way firewall), you will have to configure the firewall settings of the CommServe and client computer using the CommCell Console. Following the firewall configuration, you will be able to install new components on the upgraded client computer.
Registry Keys • Information from user created registry keys is stored in the operating systems temp directory during the upgrade. The name of the file is **GalaxyReg_OLD_But_Not_New.txt**. Re-create these registry keys, if necessary. • The values in all the system created registry keys are set to default after the upgrade. If any of these values were modified prior to the upgrade, the modified values are stored in the operating systems temp directory within **GalaxyReg_MIX_OLD_New_Diff.txt**.
Deconfigured Clients When a CommServe is upgraded, deconfigured clients will be automatically upgraded to the current version in the database. If you wish to reactivate this client, make sure to use the current software version during installation.
Cluster Plug-in resource in a Microsoft cluster environment If the status of the nodes (Active or Passive) is not maintained throughout the upgrade session, then the cluster plug-in resource may get removed after the upgrade operation is complete. In such a case, do the following to recreate your cluster plug-in resource: 1. From the **CommCell Console**, right-click the <*Cluster Group Client*>, and click **Properties**. 2. Click **Advanced** on the **Client Computer Properties** dialog box, and then click the **Cluster Group Configuration** tab. 3. Click the **Force Sync configuration on remote nodes** checkbox to force the cluster configuration on the remote clients.
Cluster Group Configuration after Upgrade The following consideration is applicable if you have created a new cluster group after upgrading the clients residing in a cluster environment to the current release: • Before configuring the newly created cluster group from the CommCell Console, install the required components on all the physical computers using interactive install procedure, and then configure the newly created cluster group from the CommCell Console. • If you want to configure the newly created cluster group for the components that were already installed on the Virtual node, first interactively install these components on all the physical computers, and then configure the cluster group for these components from the CommCell Console.

6.1.2 CommServe and CommCell Console issues after upgrading

You should review CommServe and CommCell Console issues after upgrading.

Description
SQL Server Settings Verify the following setting by viewing the Server Properties using the Microsoft SQL Server Management Studio: • In the Memory page, the dynamically configured Maximum memory should be 50% of the physical memory available in the CommServe computer. • The user-defined senders e-mail address is not retained after the upgrade. From the **Control Panel**, open the **E-Mail and IIS Configuration** dialog box and specify the e-mail address in the **Senders Address** box under the **E-Mail Server** tab. • If Activity Control was disabled on the client prior to the upgrade, enable it after the upgrade using the **Activity Control** tab from the **Client Computer Properties** dialog box in the CommCell Console. • Some existing features may not function as expected when the CommServe is upgraded and the Clients/MediaAgents remain in an older version of the software. See Backward Compatibility for more information on such features.
Upgrade MediaAgent associated with the Disaster Recovery Backup policy After upgrading the CommServe, make sure that the MediaAgent associated with the Disaster Recovery policy is also upgraded to the same version in order to perform the Disaster Recovery backups successfully.
Upgrade MediaAgent to enable browse and restore operations using Web Console After upgrading the CommServe, if you want to browse and restore from MediaAgent using Web Console, make sure the MediaAgent is also upgraded to the current version.
Network ports If you have upgraded the CommServe using the Database Upgrade tool, and later if you restore the upgraded database to the newly installed (fresh) database, then the port numbers used by the Web Console and CommCell Console in the earlier version will be changed to the new default port numbers that are used in the current release. • By default, Web Console uses port number **80** in the current release. • By default, CommCell Console uses port number **81** in the current release. Make sure that these port numbers are not used by any other application.
Web administration If the CommServe was configured for Web administration manually after the install in the previous version, then after upgrading the CommServe, you should re-configure the CommServe for Web administration manually.

6.1.3 MediaAgent issues after upgrading

You should consider MediaAgent issues after upgrading.

Description
Libraries with I/E port If you had used nUseImpExpBitForImport registry key to prevent exported media in I/E port to be re-imported back to the library after reset in previous release, then you will have to manually enable the corresponding option at the library level from CommCell Console in the current release. See Prevent Import of Exported Media after Resetting a Library for step-by-step instructions.
Index cache Index cache now requires 5% more storage space. Verify and ensure that you have sufficient disk space for the index cache in the current release. Also note that the default value of Index Retention Criteria is now changed to 15 days. (Previously this was 35 days.) However, if you have changed the default value, the changed value will be carried forward after the upgrade. As **Index Retention Criteria** affects the number of days for which the index cache is retained and as additional space is now required for the index cache, ensure that the value of **Index Retention Criteria** specified in **MediaAgent Properties (Catalog)** tab is set appropriately after the upgrade.
First incremental backup after upgrade After upgrading the MediaAgent to version 10, the first incremental backups will require additional time to complete. The additional time is required to convert the index of that subclient to version 10 format.

6.1.4 Web server and Web Console issues after upgrading

You should consider Web server and Web Console issues after upgrading.

Description
Changing the Web Console URL provided in the CommCell Console By default, when the Web Console is installed on multiple computers, the Web URL link provided in the CommCell Console points to the computer where the Web Console was installed first. When upgrading multiple Web Console computers to the current release, the URL link in the CommCell Console will be updated to point to the computer that was upgraded first. This could mean that the new URL may not be from the original Web Console computer (which got installed first). You can manually update the Web Console URL link using the following command: `qoperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si WebConsoleURL -si y -si "http://hostname:port/webconsole/clientDetails/`

Description
`fsDetails.do?clientName=CLIENTNAME"` where: • **hostname** is the hostname of the computer where the Web Console is installed • **port** is the port number used by the Web Console
Browsing client data When the CommServe and Web Server are upgraded browsing the client data from the Web Console may fail if the MediaAgent is not upgraded. Hence, it is recommended to upgrade all MediaAgents to the same version as the CommServe and Web Server.

6.2 Modern data protection considerations after upgrading

You should review data protection issues after upgrading.

Component	Description
Image Level iDataAgent	**Backing up after upgrade** • It is strongly recommended that you run a Full Backup after the upgrade. Upgrading the agent will NOT automatically convert the next incremental update to a Full Backup. • Image agents will no longer support differential backup, and the differential backups scheduled before the upgrade will run as full backups. Change your existing schedules with differential backups appropriately.
NAS iDataAgent	**Integrating components** In the current version, the NDMP Remote Server (NRS) and File System Restore Enabler (NRE) components are integrated as follows: • The NDMP Remote Server is part of the MediaAgent software. • The File System Restore Enabler is part of the File System iDataAgent software. In Version 9, these add-on components had to be installed separately for the NAS iDataAgent.
Oracle iDataAgent	**Data aging after upgrade** After upgrade, we recommend that you manually run a **CROSSCHECK** and, if necessary, **DELETE EXPIRED BACKUP** from RMAN prior to running a data aging operation, in cases where a backup piece has been manually deleted (or marked expired) in the Recovery Catalog. Otherwise, the CommServe database is not made aware of the change and it would become out of sync with the Recovery Catalog. This manual task ensures that the CommServe database is properly synchronized with the Recovery Catalog before data aging is run.

Component	Description
	Reboot required after upgrading on Windows After upgrading the Oracle iDataAgent on a Windows client, you need to reboot the client.
	Registry keys Following an upgrade of the CommServe to the current release, manually add the OracleDeleteAgedBackupPiece registry key on the CommServe. Even if this registry key was previously added as a matter of course and was on the CommServe, it must be added again following an upgrade of the specified CommServe. The following registry keys are now available in the Media Management Configuration (Data Aging) dialog box. (See Data Aging of Job History Data for step-by-step instructions on how to access this dialog box.) • `archiverRestoreHistoryLifeSpan` is now the **Days to keep the archiver restore job histories** option. • jobHistoryLifeSpan is now the **Days to keep successful backup job histories** option.

Windows File System iDataAgent	**Changes in the phases associated with a backup job**
	
	To speed up backups, in the current version, the backup job will complete after the scan phase if no files in a subclient were changed or added. Backup and archive index phases will not be performed.
	
	When you upgrade a client from the previous version to the current version, this option is not available by default. To enable this option make sure that **SkipEmptyBackup** key is created in the gxGlobalParam table and its value is set to 1.To disable this option later, you can set the value of this key to 0.
	
	Use the following steps to enable/disable this key:
	
	1. From the CommCell Browser, right-click <*CommServe*> and point to **Properties**.
	2. Click the **Additional Settings** tab.
	3. Click **Add**.
	4. In the **Name** box, type SkipEmptyBackup.
	5. Select **CommServDB.GXGlobalParam** from the **Category** list.
	6. Select **INTEGER** from the **Type** list.
	7. In the **Value** box, type:
	  • **1**, if you want to enable this key.
	  • **0**, if you want to disable this key later.
	8. Click **OK** twice.

6.3 Virtualization issues after upgrading

You should consider virtualization issues after upgrading.

Component	Description
VMware	**Using additional proxies to backup virtual machines** After upgrading a client, you can use multiple proxies for load balancing and failover while backing up virtual machines. You can also assign a specific proxies for each subclient. In such scenario, a full backup of the virtual machines in the subclient is performed irrespective of the selected backup type. For details, refer to Using Proxy Teaming For Highly Scalable Fault Tolerant Backups.
	Viewing backup job details after the upgrade If you are viewing the job details of any backup job, performed before the upgrade, the **Virtual Machine Status** tab will not appear in the **Job Details** dialog box. However, if you perform a backup after the upgrade and then view the job details of the backup job, the **Virtual Machine Status** tab will appear in the **Job Details** dialog box. For details, refer to Viewing Details of the Backup Job.
	Backup of failed virtual machines after upgrade After upgrading a client, to back up only the failed virtual machines in any subclient, follow these steps: 1. After upgrading a client, perform a full or incremental backup of the subclient which contains the failed virtual machines. 2. Right-click the subclient and click Backup. 3. Click Advanced and select the Backup failed VMs only (Virtual Server) check box. 4. Perform the incremental backup of the subclient. For details, refer to Backup Failed Virtual Machines.
	Upgrading the Client where you have uninstalled and installed the Virtual Server iDataAgent If you uninstalled the version 9.0 Virtual Server iDataAgent and re-installed it again on a client, then you must reboot the client before upgrading it to version 10.0. If you do not reboot the client, the vStorage services will not start automatically and the upgrade job will fail.
	Re-register the VM File Recovery Plugin after upgrading Web Server and Web Console You must re-register the Plugin when you upgrade the Web Server and Web Console. When you upgrade the web server and web console, port

Component	Description
	80 will be set for Tomcat services and port 81 will be used for web console. The web console URL will set to port 82. When you un-register and re-register the VM File Recovery Plugin using CommCell console, the vCenter automatically registers with new a URL for web console. Before re-registering the plugin, ensure that the client has latest version of Virtual Server iDataAgent. For details, refer to Unregistering and Re-registering the Plug-In.
Microsoft Hyper-V	**Upgrade for Hyper-V hosts configured for failover Clusters** If Hyper-V hosts are configured for failover clusters then after upgrading a client, you can continue to use individual nodes while backing up virtual machines. If you want to use multiple nodes for backing up virtual machines, you can add the nodes to the upgraded client. It is recommended to configure a new Virtualization Client with the exact same content as that of the upgraded client. Note that, in this case you will not be able to view the backup history and the backed up content from previous version.

6.4 Windows MediaAgent upgrade

See Windows MediaAgent Upgrade, for more information about upgrading Windows MediaAgent.

6.5 UNIX MediaAgent upgrade

See UNIX MediaAgent Upgrade, for more information about upgrading UNIX MediaAgent.

Copyright Information

Trademark Information