

Quick Start Guide - SnapProtect

TABLE OF CONTENTS

INSTALL COMMSERVE, MEDIAAGENT AND FILE SYSTEM IDATAAGENT

OPEN COMMCELL CONSOLE

CONFIGURE A STORAGE DEVICE

CONFIGURE A STORAGE POLICY

SETUP CLIENTS

CLIENTS

VIRTUAL SERVER (VMWARE)

- Deployment
- Configuration
- Storage Array Configuration
- Backup
- Vault/Mirror Copy
- Movement to Media
- Restore

EXCHANGE DATABASE

- Deployment
- Configuration
- Storage Array Configuration
- Backup
- Vault/Mirror Copy
- Movement to Media
- Restore

ORACLE (UNIX)

- Deployment
- Configuration
- Storage Array Configuration
- Backup
- Vault/Mirror Copy
- Movement to Media
- Restore

MICROSOFT SQL SERVER

- Deployment
- Configuration
- Storage Array Configuration
- Backup
- Vault/Mirror Copy
- Movement to Media
- Restore

NAS

- Deployment
- Configuration
- Storage Array Configuration
- Backup
- Vault/Mirror Copy
- Movement to Media
- Restore

VIRTUAL SERVER (MICROSOFT HYPER-V)

- Deployment
- Configuration
- Storage Array Configuration
- Backup
- Vault/Mirror Copy

Movement to Media
Restore

SAP FOR ORACLE (UNIX)

Deployment
Configuration
Storage Array Configuration
Backup
Vault/Mirror Copy
Movement to Media
Restore

DB2 (UNIX)

Deployment
Configuration
Storage Array Configuration
Backup
Vault/Mirror Copy
Movement to Media
Restore

UNIX FILE SYSTEM

Deployment
Configuration
Storage Array Configuration
Backup
Vault/Mirror Copy
Movement to Media
Restore

WINDOWS FILE SYSTEM

Deployment
Configuration
Storage Array Configuration
Backup
Vault/Mirror Copy
Movement to Media
Restore

Getting Started



Initial deployment and successful run of SnapProtect backup may take around 4 weeks due to the various environment dependencies. The following parameters are known to affect the deployment and initial run and hence need a thorough evaluation:

- Firmware versions on the array
- Device types
- Mode of access
- Security configuration
- Operating Systems interacting with the storage array
- Application layout on the storage array LUNs

INSTALL COMMSERVE™ MEDIAAGENT AND FILE SYSTEM IDATAAGENT

The first step in setting up a CommCell™ is to install the CommServe, MediaAgent and File System iDataAgent.

- **CommServe™** communicates with all clients and MediaAgents and coordinates all operations such as backups, restores, copies, media management, etc. within a CommCell.
- **MediaAgent** manages the transmission of data between clients and backup media.
- **File System iDataAgent** performs the backup and restore of the clients data

The following sections describe how to install all the above components in a computer.

1. Verify that the computer in which you wish to install satisfies the following System Requirements:
 - System Requirements - CommServe
 - System Requirements - MediaAgent
 - System Requirements - Microsoft Windows File System iDataAgent
2. Run **Setup.exe** from the Software Installation Disc.
3. Select the required language.
Click **Next**.

RELATED TOPICS

License Requirements

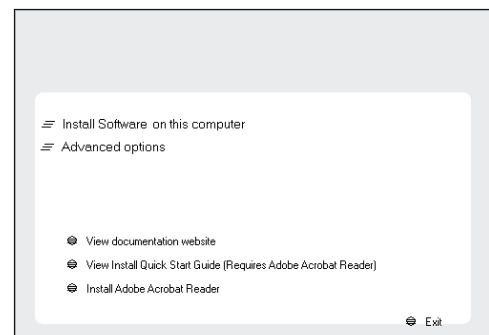
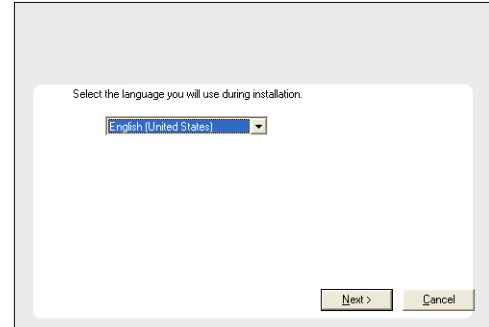
Review the licenses required for the SnapProtect feature.

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. Click **Next**.



6. Click **OK**.

7. Select **I accept the terms in the license agreement**.
Click **Next**.

8. Select the following component(s) to install:

- Expand **CommServe Modules** and click **CommServe**.
- Expand **CommNet** and clear **CommNet Server**.
- Expand **CommCell Console** and clear **CommNet Browser**.
- Expand **MediaAgent Modules** and click **MediaAgent**.

9. Click **YES** to install Microsoft .NET Framework package.

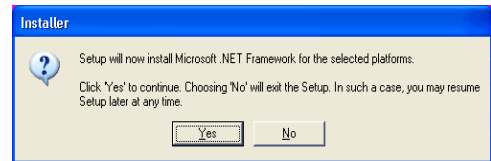
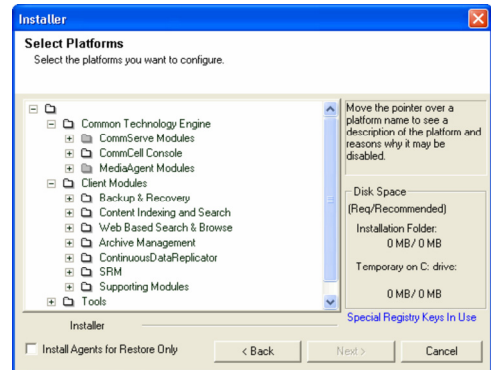
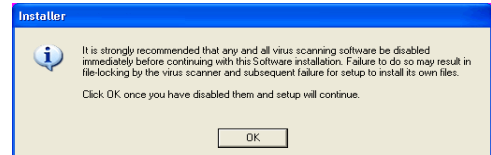
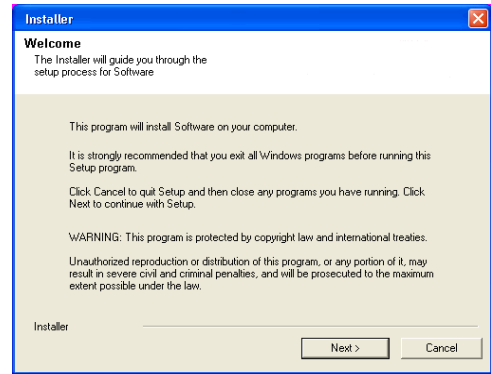
NOTES

- This prompt is displayed only when Microsoft .NET Framework is not installed.
- Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable package.

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

NOTES

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



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

- Verify the Installation Path for the Database Engine.
Click **Browse** to change the default location.
Click **Next**.

NOTES

- This is the location where you want to setup the Microsoft SQL Server System databases.
- If you plan to perform VSS enabled backups on the CommServe computer, it is recommended that the CommServe database is not installed on the system drive. VSS restores could cause system state restore issues.
- The install program installs the database instance.

- Verify **MSSQL Database Installation Path**.
Click **Browse** to change the default location.
Click **Next**.

NOTES

- This is the location where you want to install Microsoft SQL Server.
- This step may take several minutes to complete.

- If this message is displayed, click **Reboot Now** to continue. The install program will automatically resume from the point of failure after the reboot.

If the install program does not automatically resume after the reboot:

- 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**.

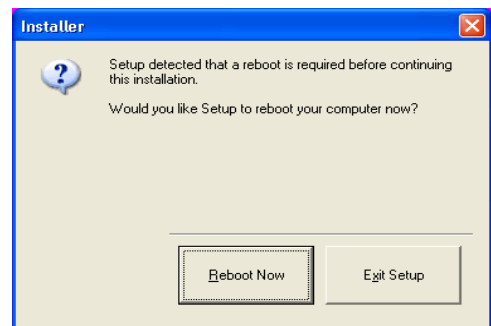
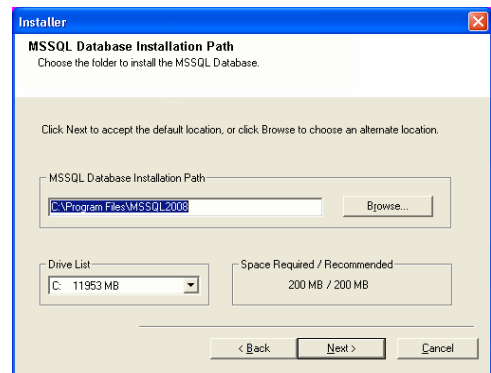
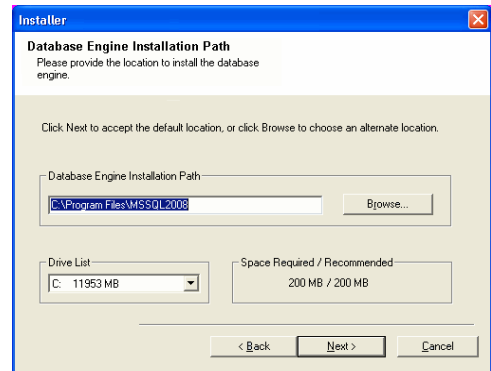
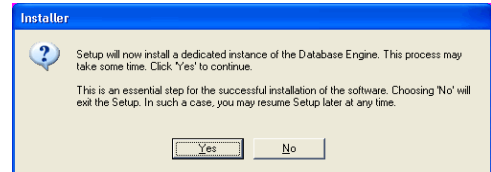
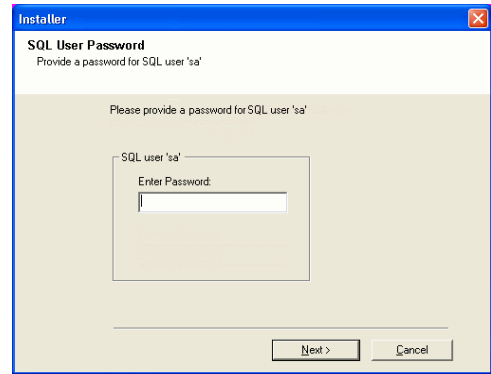
NOTES

- Click the **Skip Reboot** option if it is displayed and continue with the installation. You can reboot at a later time if the option is displayed.

- Click **Next**.

NOTES

- The **CommServe Client Name** and **CommServe Host Name** are automatically



populated.

Note down the **CommServe Client Name**.

This is needed later to launch the CommCell Console.

16. Click **Next**.

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 you wish to configure other firewalls, select **Add programs to the Windows Firewall Exclusion List**.

After the installation, make sure to Configure Windows Firewall to Allow CommCell Communication.

17. Click **Next**.

18. Verify the default location for software installation.

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

Click **Next**.

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.

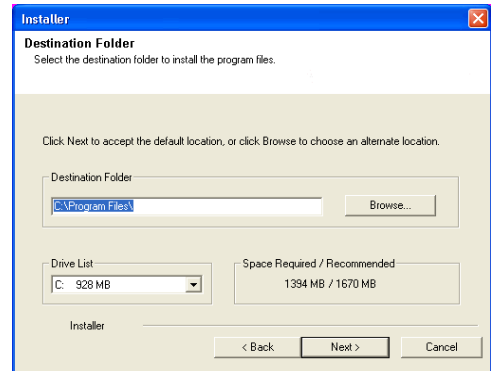
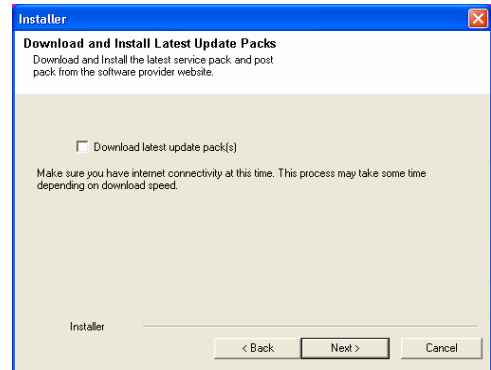
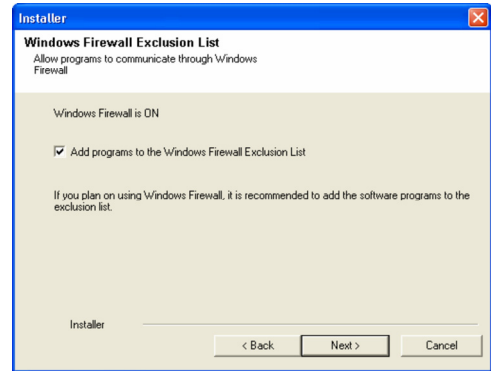
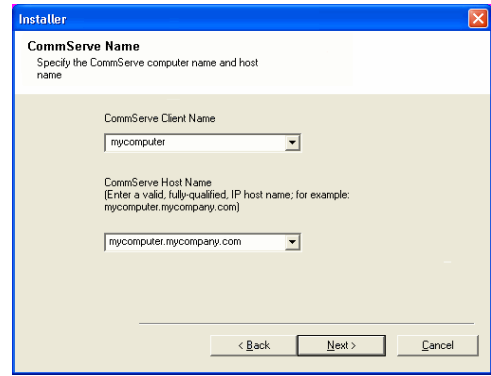
19. Verify the location of the database.

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

Click **Next**.

NOTES

- Do not specify a mapped network drive.
- Ensure that the drive has at least 1GB of free space.
- The directory file path selected should not be located on a FAT drive. A FAT drive



cannot be supported as the location for this database because it does not allow a temporary sparse file to be generated when creating the database snapshot, which is required for data verification.

- 20. Select the **Create a New Database** option and click **Next** to continue.

NOTES

- This screen may look different from the example shown.

- 21. Enter the network or local path where Disaster Recovery Backup files should be stored.

Click **Next**.

NOTES

- If you selected **Use Network Path**, you must enter the **Network share username** and the **Network share password**.
 - The Network share username is the domain\username of the user that has administrative rights to the Disaster Recovery Backup destination path.
 - The Network share password is the password of the network share username.

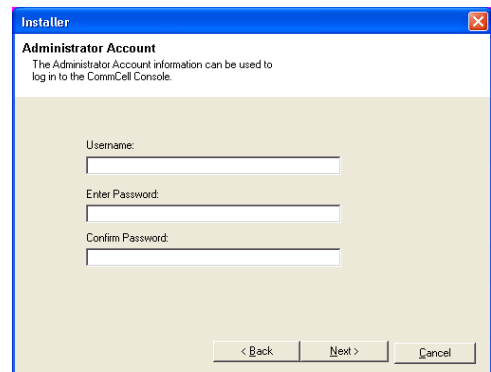
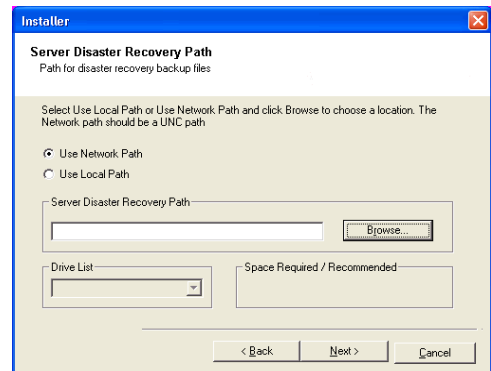
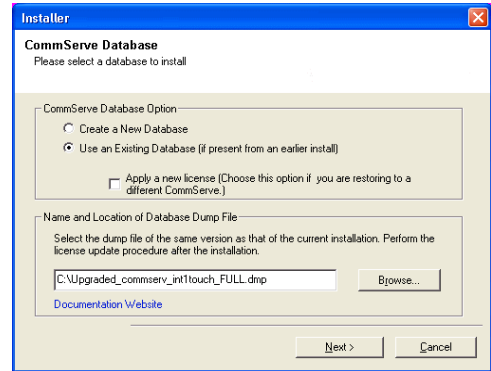
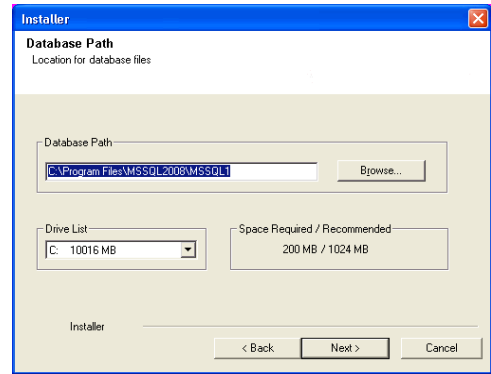
- 22. Enter the **CommCell Username** and **CommCell Password**.

Click **Next**.

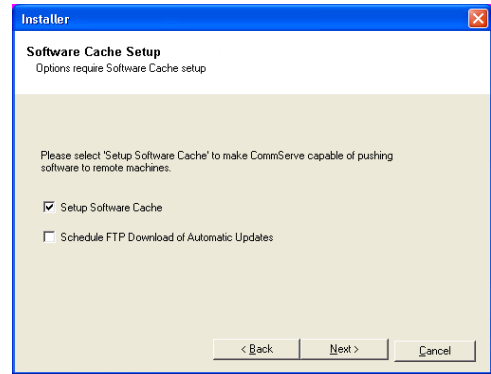
Make note of the **CommServe Username** and **CommCell Password**.

This is needed later to launch the CommCell Console.

- 23. Click **Next**.



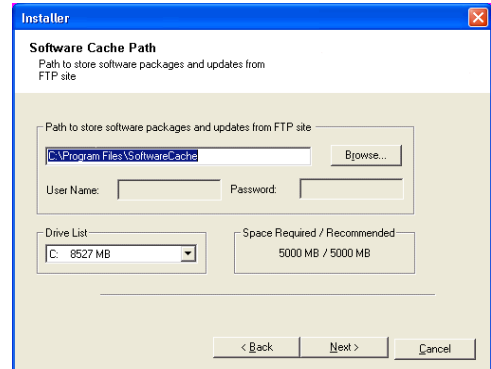
24. Verify the location where the update files from the FTP site should be stored.
 Click **Browse** to change the default location.
 Click **Next**.



25. Click **Next**.

NOTES

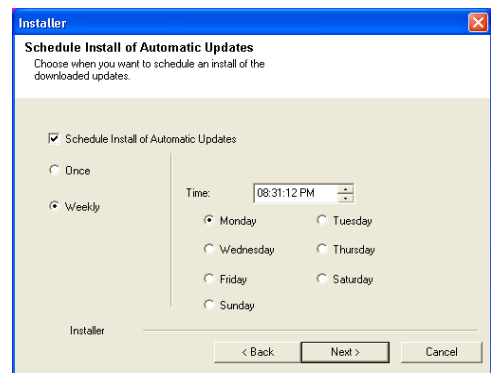
- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.



26. Click **Yes** to configure the CommCell Console for web administration.

NOTES

- The Internet Information Server (IIS) must be installed on this computer in order to configure for web administration.
- Configuring this computer for web administration allows you to:
 - Access the CommCell Console and Books Online from a remote computer using a Web browser.
 - View CommCell reports via a Web browser.
 - Access Books Online by clicking the Help button (the icon with a ?) in the CommCell Console.

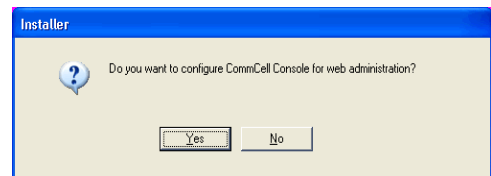


27. Select **Yes** to stop Removable Storage Services on the MediaAgent.

NOTES

- This prompt will not appear if Removable Storage Services are already disabled on the computer.

Click **Next**.



28. Click **OK**.

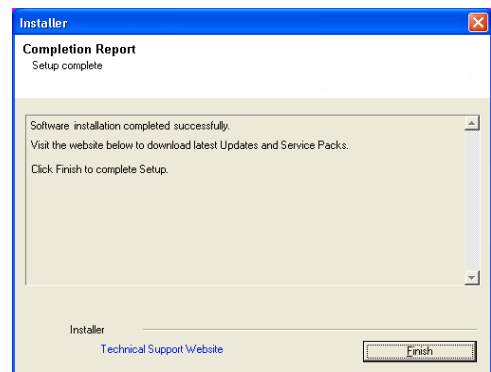
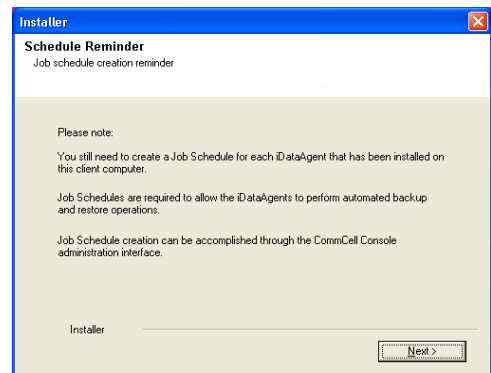
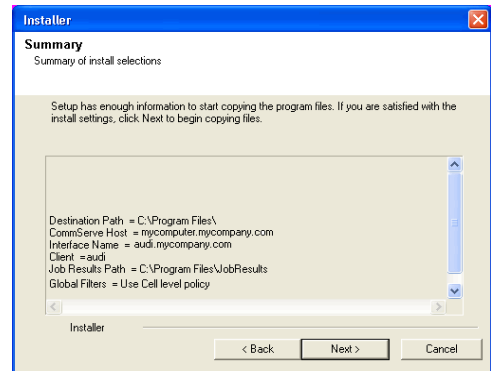
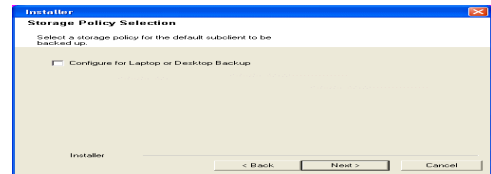
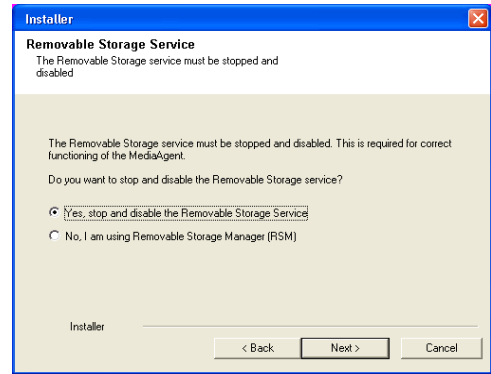
29. Click **Next**.

NOTES

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

30. Click **Next**.

31. Click **Finish**.



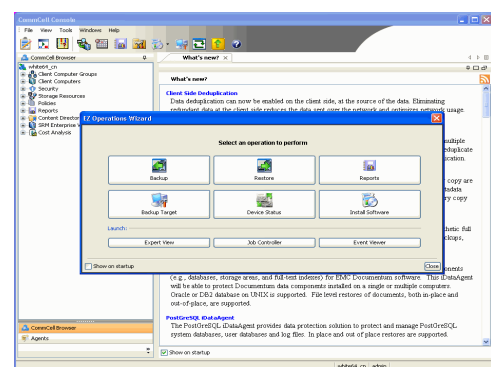
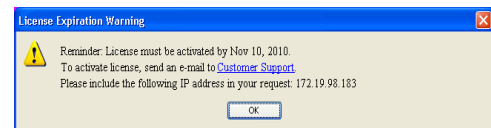
Getting Started

◀ Previous Next ▶

OPEN COMMCELL CONSOLE

CommCell Console is the graphical user interface that helps you to run backups and restores. In addition the CommCell Console also provides a number of other features to help you control and manage the data.

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
Select **bull** from the Programs menu and then select **Calypso**.
Click **CommCell Console GUI**.
2. Enter the **User Name** and **Password** that you entered in step 22 during the installation.
Enter the **CommCell** name that you entered in step 15 during the installation.
Click **OK** to continue.
3. If you have not activated the license yet, you will receive a reminder prompt.
Click **OK** to continue.
4. The CommCell Console will be displayed.

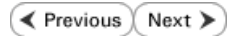


If the **EZ Operations Wizard** is not displayed double-click the icon in the toolbar to display **EZ Operations Wizard**.



◀ Previous Next ▶

Getting Started



CONFIGURE A STORAGE DEVICE

It is necessary to configure the storage devices (Tape or Disc devices) controlled by the MediaAgent. Device configuration allows the MediaAgent to communicate with the specific device.

You may have one or more storage devices available for protecting data. The following sections describe how to configure the following:

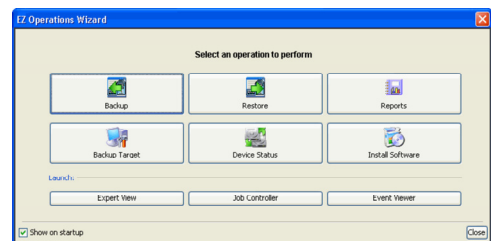
- **Option 1:** Configuring a Disc Device
- **Option 2:** Configuring a Tape Device

Depending on the type of storage device attached to your MediaAgent, you can configure one or both of these devices.

Refer to the **Configuration** section in the Media Management web if you have other types of devices.

OPTION 1: CONFIGURING A DISC DEVICE

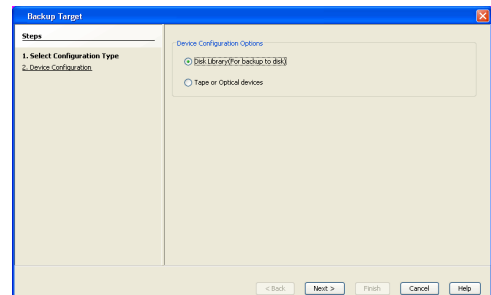
1. Click the **Backup Target** button on **EZ Operations Wizard**.



If the **EZ Operations Wizard** is not displayed double-click the icon in the toolbar.

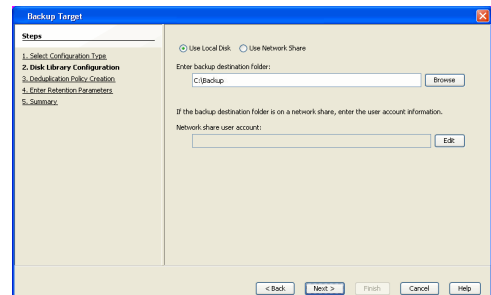


2. Click **Disc Library (For backup to disc)** and click **Next**.

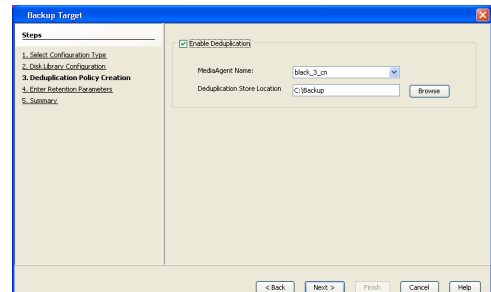


3.
 - Click **Use Local Disk**.
 - Type the name of the folder in which the disc library must be located in the **Enter backup destination folder** box or click the **Browse** button to select the folder.
 - Click **Next**.

If you click the **Use Network Share** option you will be prompted for the credentials (user name and password) to access the share.

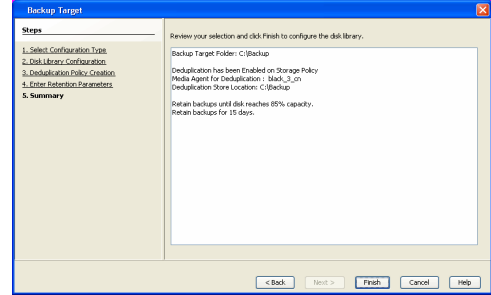
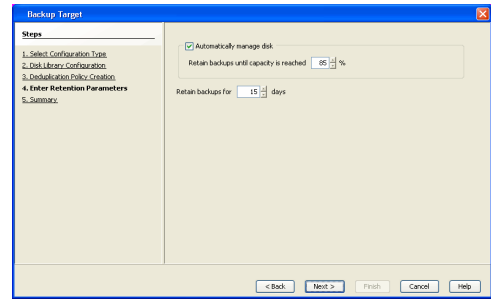


4.
 - Click and select the **Enable Deduplication** option - this will save disc space for storage.
 - Type the name of the folder in which the deduplication database must be located in the **Deduplication Store location** box or click the **Browse** button to select the folder.
 - Click **Next**.



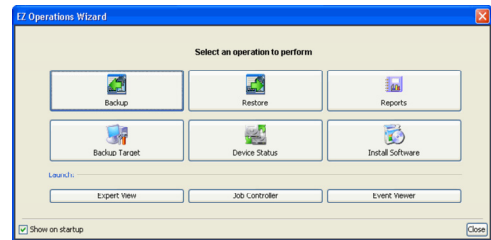
5. Click **Next**.

6. Click **Finish**.



OPTION 2: CONFIGURING A TAPE DEVICE

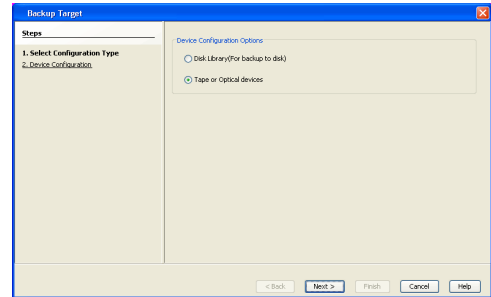
1. Click the **Backup Target** button on **EZ Operations Wizard**.



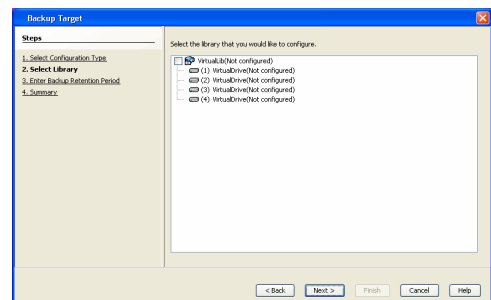
If the **EZ Operations Wizard** is not displayed double-click the icon in the toolbar.



2. Select **Tape or Optical devices**.
Click **Next**.

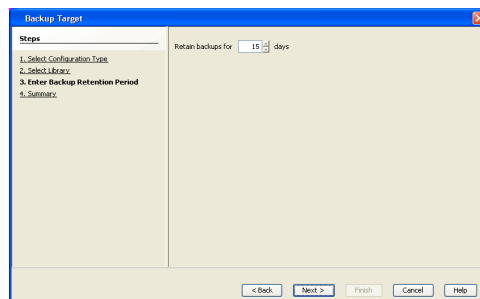


3. Click and select the library you wish to configure.
Click **Next**.

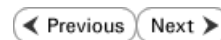
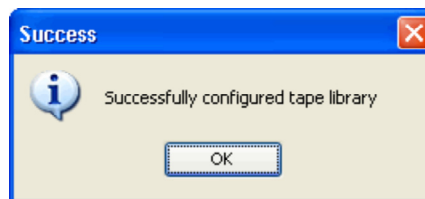
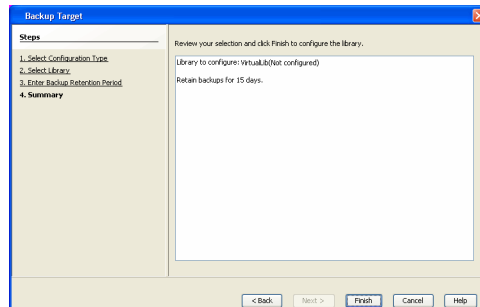


4. Click **Next**.

5. Click **Finish**.



6. Click **OK**.



Getting Started

◀ Previous Next ▶

CREATE THE STORAGE POLICY

A Storage Policy is automatically created when you configure a device.

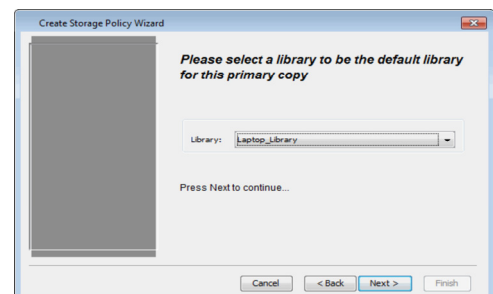
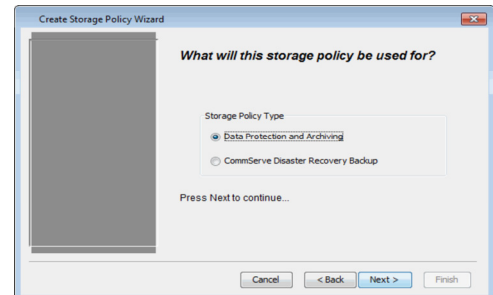
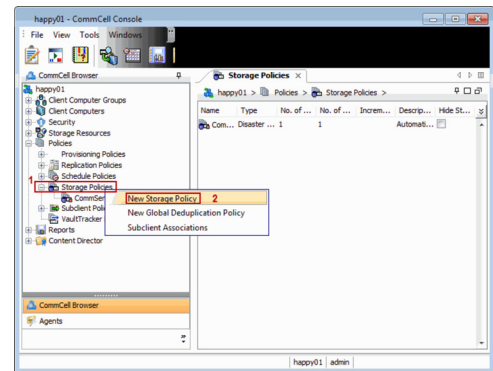
A storage policy acts as a channel through which data is transferred to the storage device. As the name indicates, a storage policy allows you to establish a comprehensive set of storage parameters - such as data retention, streams, deduplication, etc., for the data channeled through the storage policy.

If needed, you can create a new storage policy. During the creation of a Storage Policy, a new disk library is created to store metadata backup for SnapProtect operations. If there are existing disk libraries, you may select one.

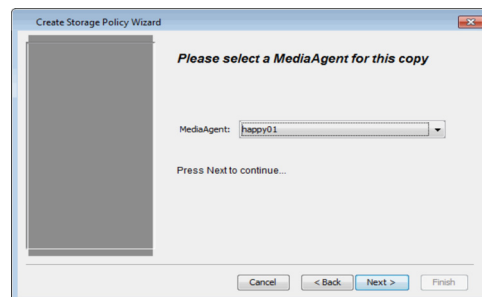
USING DISK LIBRARY

Use the following steps to create a storage policy using disk library:

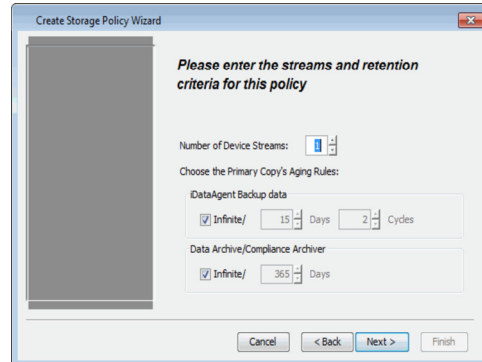
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.
2. Click **Next**.
3. Specify the name of the **Storage Policy** in the **Storage Policy Name** box and then click **Next**.
4. In the **Library** list, select the disk library to which the primary copy should be associated and then click **Next**.



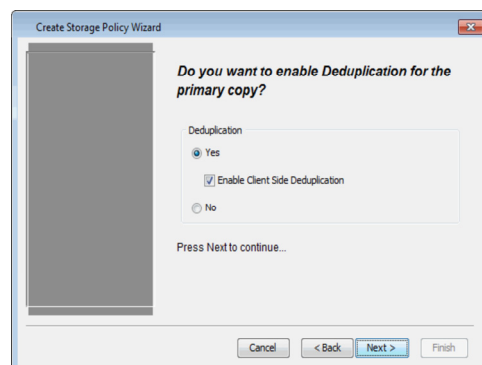
5. In the **MediaAgent** list, select a MediaAgent and then click **Next**.



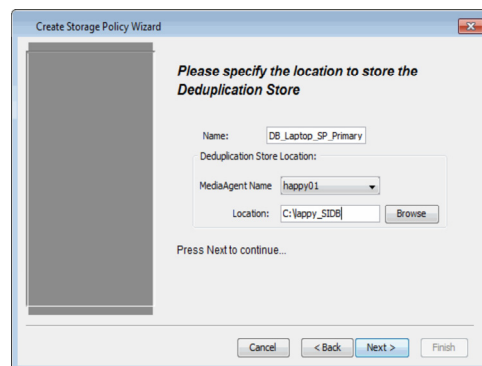
6. Click **Next**.

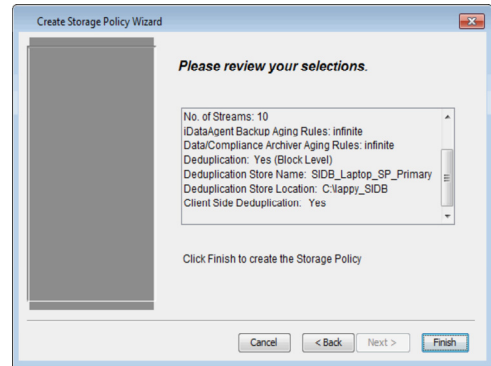


7. Click **Next**.



- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

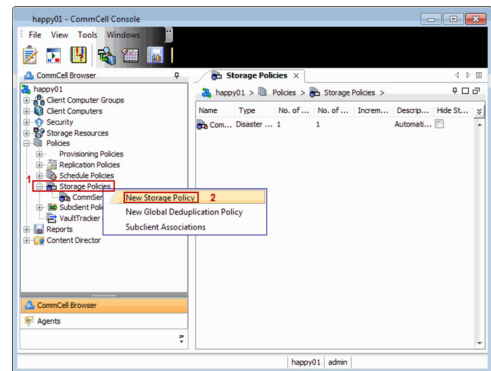




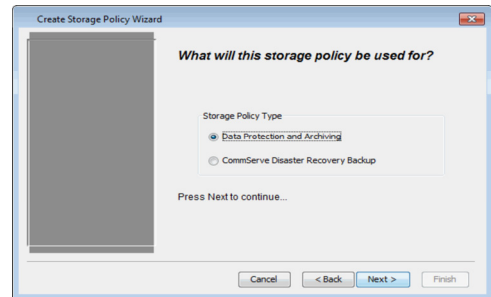
USING TAPE LIBRARY

Use the following steps to create a storage policy using tape library:

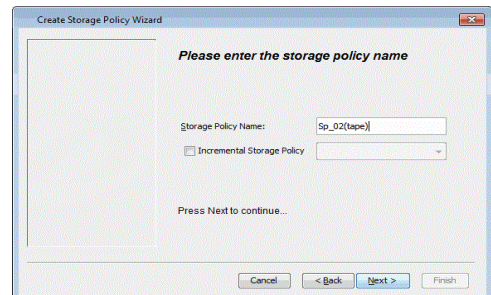
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



3. Specify the name of the **Storage Policy** in the **Storage Policy Name** box and then click **Next**.



4. In the **Library** list, select the tape library to which the primary copy should be associated and then click **Next**.

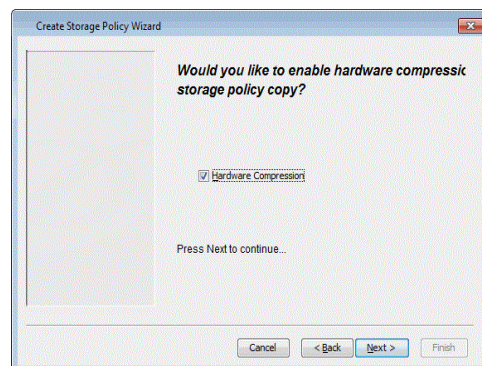
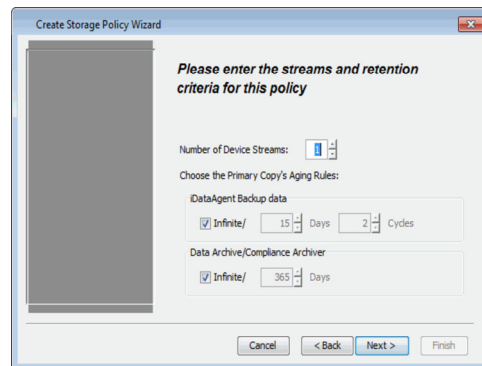
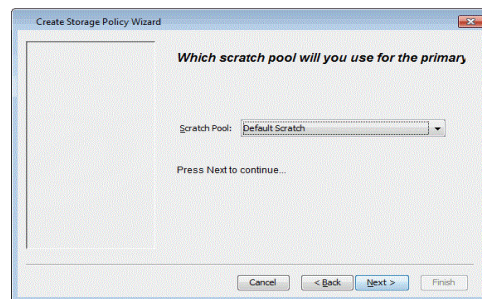
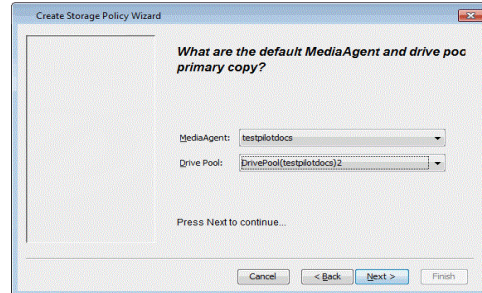
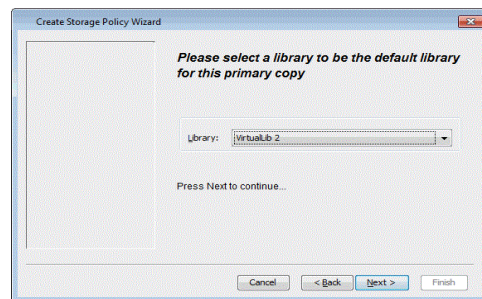
5.
 - In the **MediaAgent** list, select a MediaAgent.
 - From the **Drive Pool** list, select a default drive pool and then click **Next**.

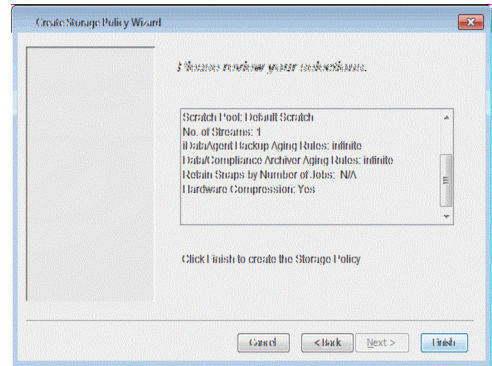
6. From the **Scratch Pool** list, select the default scratch pool and then click **Next**.

7. Click **Next**.

8. By default **Hardware Compression** is enabled, click **Next** to continue.

9. Review the details and click **Finish** to create the Storage Policy.





Getting Started

[← Previous](#) [Next →](#)

CHOOSE THE CLIENT TYPE

SUPPORTED AGENTS - CHOOSE THE AGENT TO CONFIGURE
VMWARE
EXCHANGE DATABASE
ORACLE
MICROSOFT SQL SERVER
NAS
HYPER-V
SAP FOR ORACLE
DB2
UNIX FILE SYSTEM
WINDOWS FILE SYSTEM

[← Previous](#) [Next →](#)

Getting Started - VMware Deployment

◀ Previous Next ▶

WHERE TO INSTALL

Install the software directly on the proxy computer that can communicate with the ESX Server. It is not recommended to install the software in a clustered environment.

INSTALL THE VIRTUAL SERVER IDATAAGENT (VMWARE)

Use the following procedure to directly install the software from the installation package or a network drive.

1. Run **Setup.exe** from the Software Installation Package.
2. Select the required language.
Click **Next**.
3. Select the option to **Install Calypso on this 64-bit computer**.
Your screen may look different from the example shown.
4. Select **I accept the terms in the license agreement**.
Click **Next**.
5.
 - Expand **Client Modules | Backup & Recovery | File System**, and select **Virtual Server Agent**.
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
 - Click **Next**.

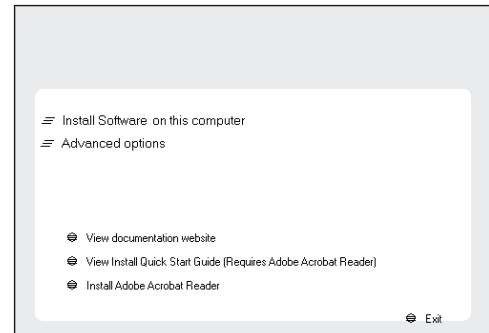
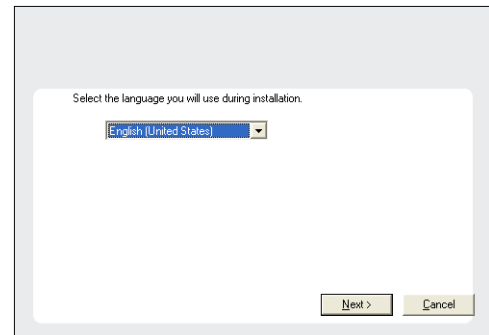
BEFORE YOU BEGIN

Download Software Packages

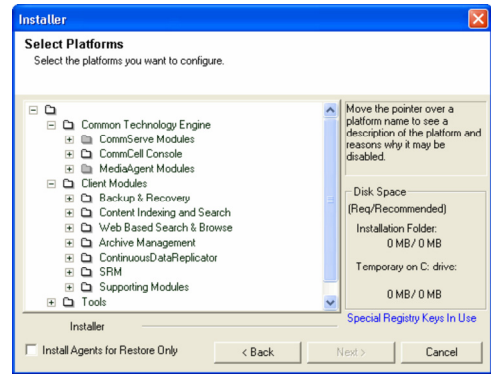
Download the latest software package to perform the install.

SnapProtect Support - Platforms

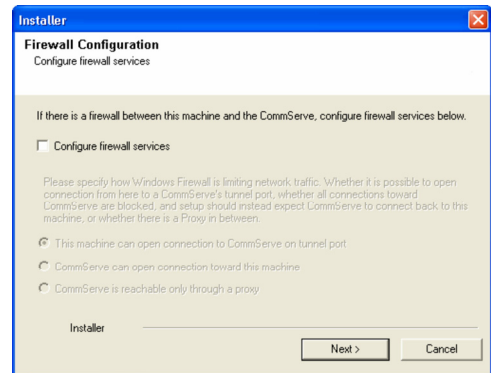
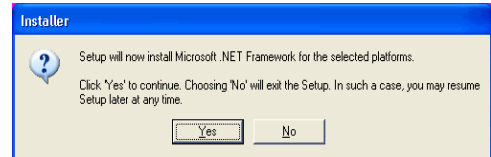
Make sure that the computer in which you wish to install the software satisfies the minimum requirements.



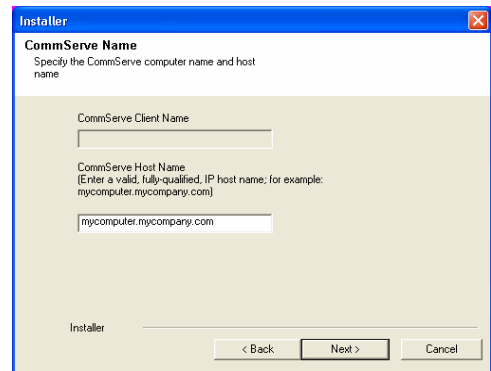
6. Click **YES** to install Microsoft .NET Framework package.
 - This prompt is displayed only when Microsoft .NET Framework is not installed.
 - Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.
7. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.
 For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.
 If firewall configuration is not required, click **Next**.



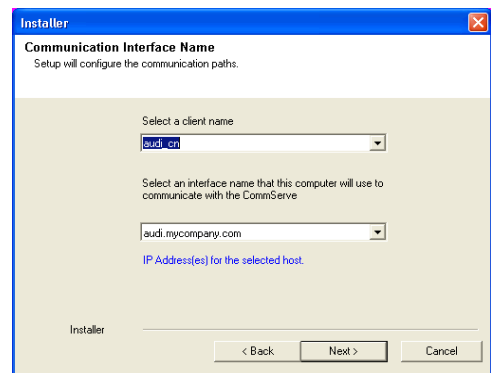
8. Enter the fully qualified domain name of the **CommServe Host Name**.
 Click **Next**.
 Do not use space and the following characters when specifying a new name for the CommServe Host Name:
`\ | ` ~ ! @ # $ % ^ & * () + = < > / ? , [] { } ; : ' " ' "`



9. Click **Next**.



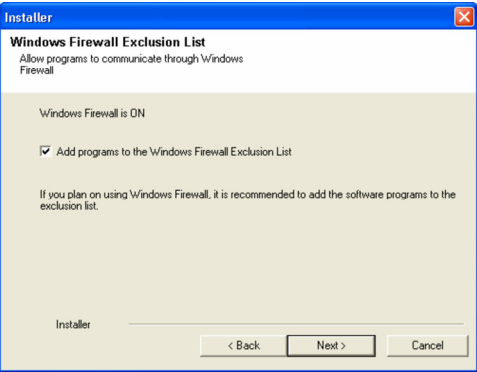
10. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.



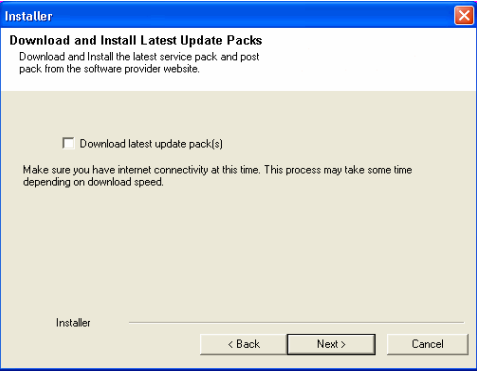
Click **Next**.

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

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



11. Click **Next**.



12. Verify the default location for software installation.

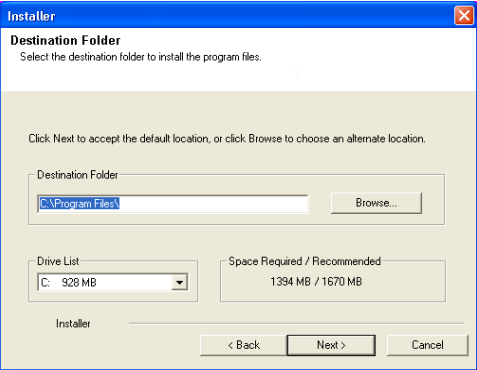
Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

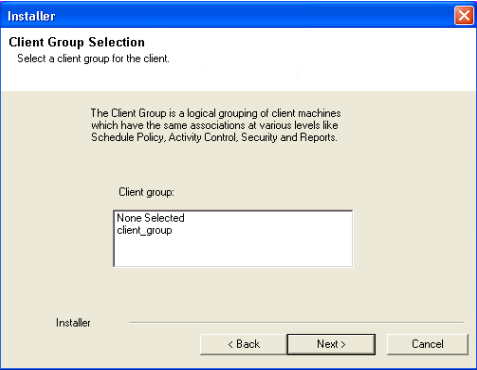
It is recommended that you use alphanumeric characters only.



13. Select a Client Group from the list.

Click **Next**.

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



14. Click **Next**.

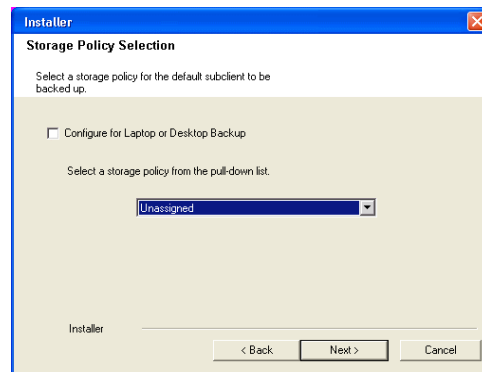
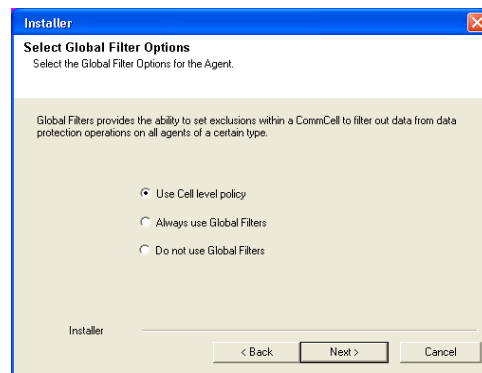
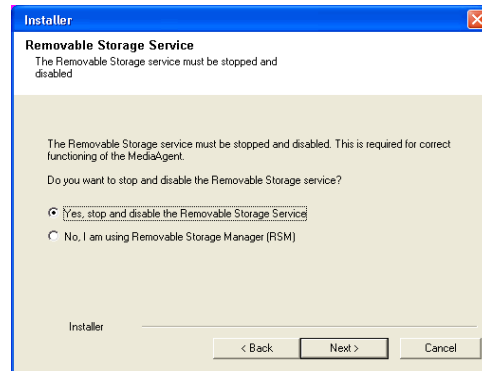
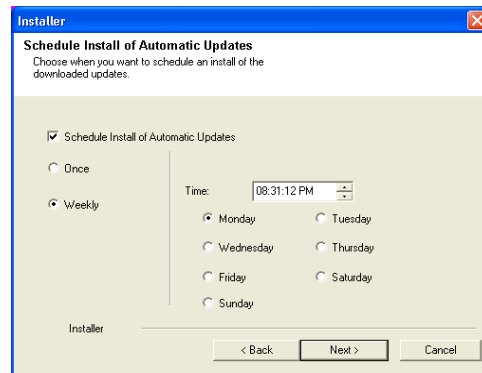
- 15. Select **Yes** to stop Removable Storage Services on the MediaAgent.
Click **Next**.

This prompt will not appear if Removable Storage Services are already disabled on the computer.

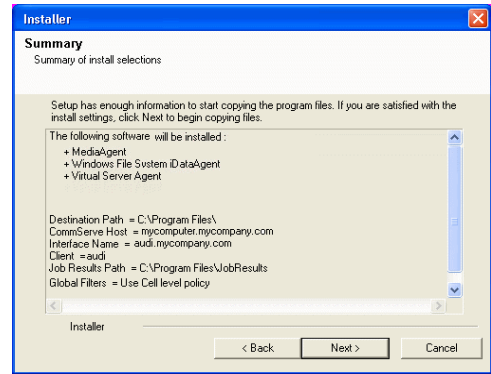
- 16. Click **Next**.

- 17. Select a **Storage Policy**.
Click **Next**.

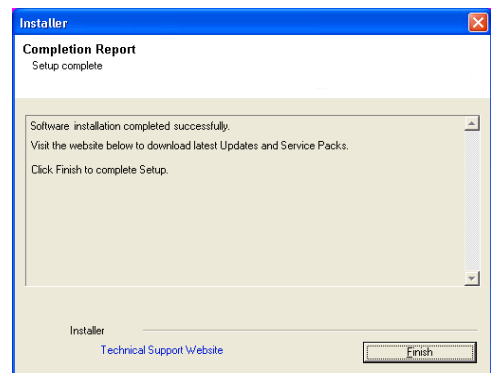
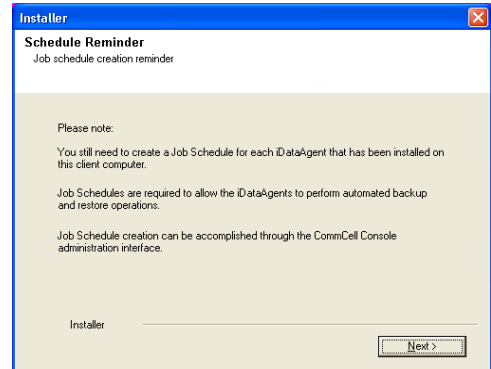
- 18. Click **Next**.



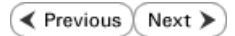
19. Click **Next**.



20. Click **Finish**.



Getting Started - VMware Configuration



CONFIGURATION

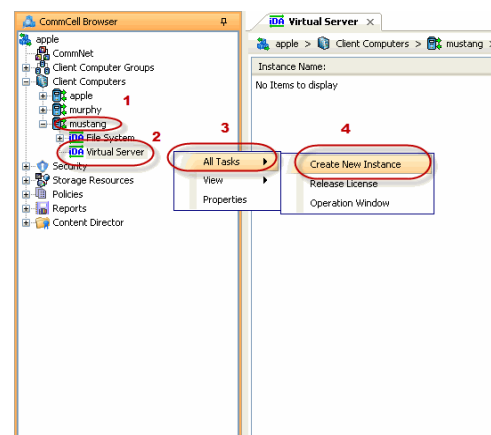
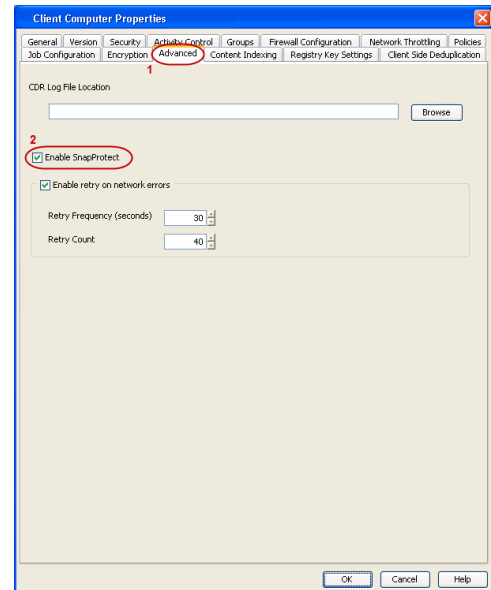
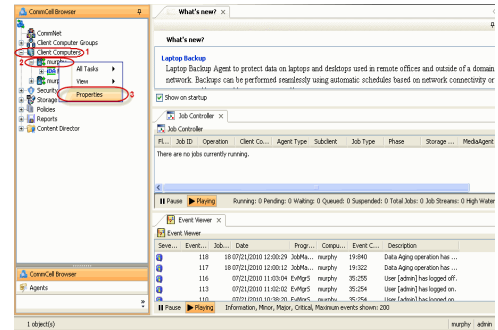
Once the Virtual Server *iDataAgent* has been installed, configure an Instance, a Backup Set and a Subclient to facilitate backups. The following sections provide the necessary steps required to create and configure these components for a first SnapProtect backup of a Virtual Center.

1.
 - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.

2.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.

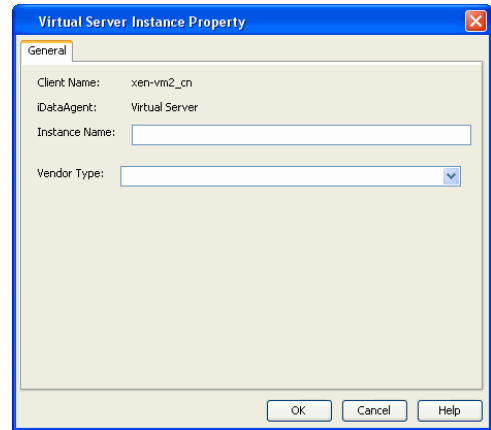
3.
 - From the CommCell Browser, navigate to **<Client>** | **Virtual Server**.
 - Right-click the **Virtual Server** agent and click **All Tasks** | **Create New Instance**.

4.
 - Enter the **Instance Name**.
 - Select **VMware** from **Vendor Type** menu.

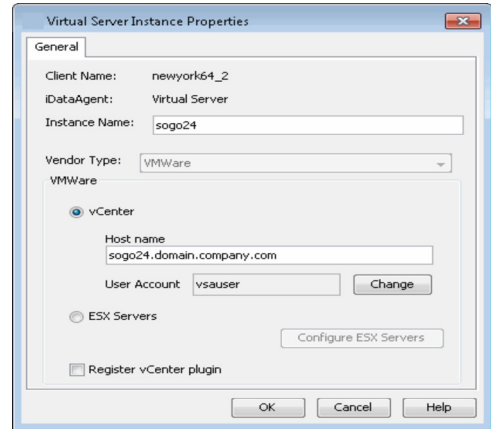


5.
 - Click **Virtual Center**.

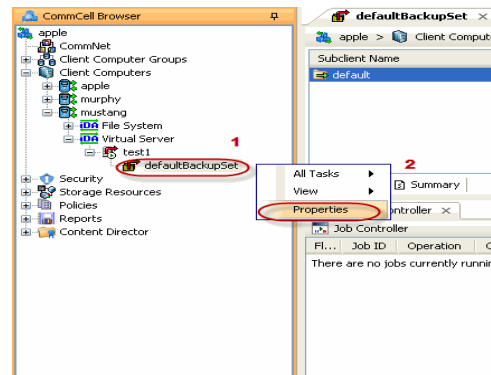
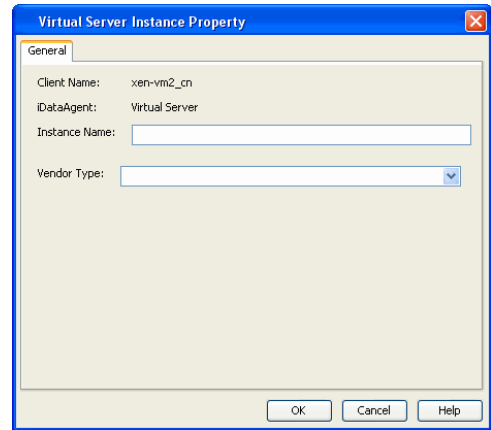
ESX Server instances are not supported for SnapProtect operations.
 - Click **Configure Password**.
 - Enter the username and password associated with the Virtual Center.



6. Click **OK** to save the instance.



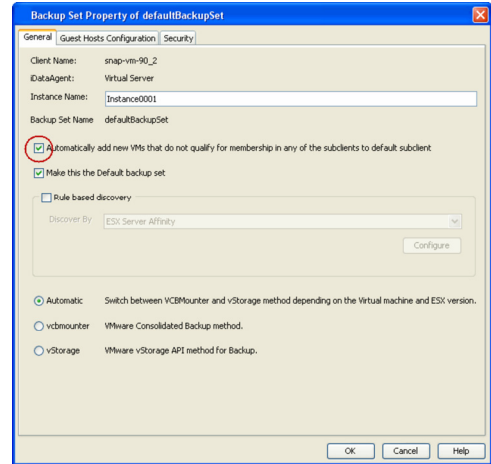
7.
 - From the CommCell Browser, right-click the **Default Backup Set**.
 - Click **Properties**.



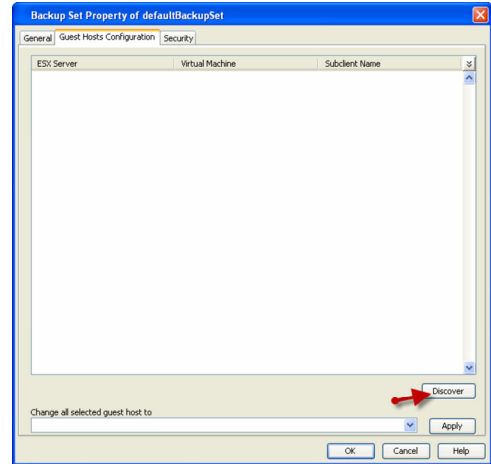
8.
 - Select **Automatically add new VMs that do not qualify for membership in any of the subclients**.

- Click **OK**.

Selecting this option is not recommended. If selected, ensure that all the virtual machines are residing on the same storage device.

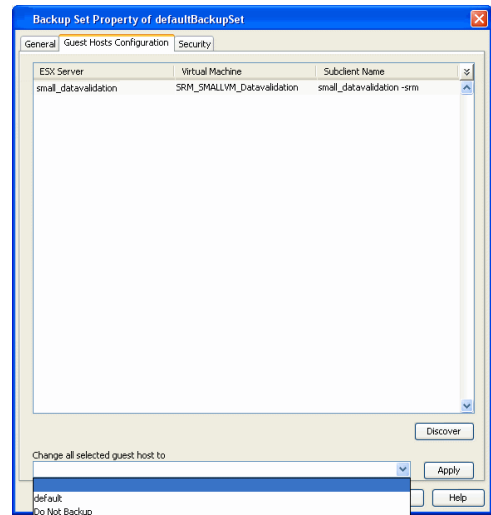


9. Click **Discover** on the **Guest Hosts Configuration** tab.
The discovery process might take several minutes to complete.



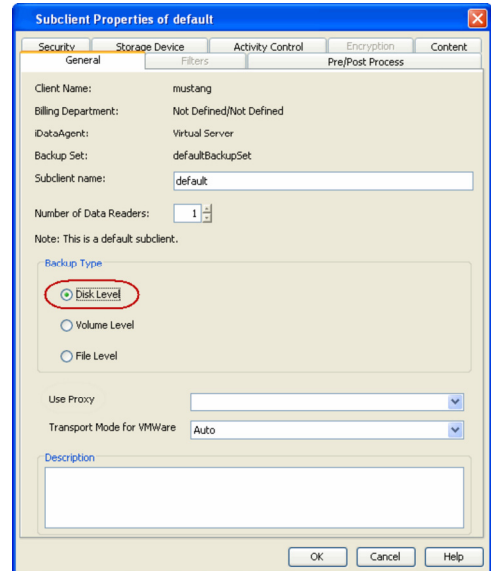
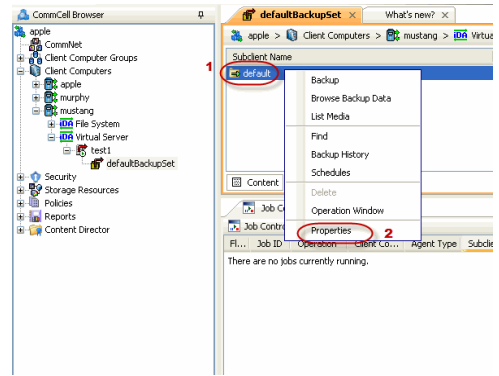
10.
 - Select a virtual machine to back up from the **Virtual Machine** column.
Ensure the virtual machine selected is not a VM template.
Virtual machine templates are not supported for backup.

- Select the default subclient from the **Subclient** column for the virtual machine you want to back up.
- Click **Apply**.
- Click **OK**.

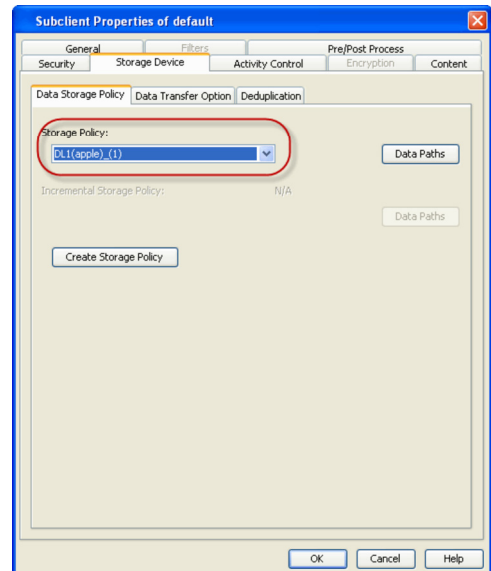


11.
 - From the CommCell Browser, navigate to the default subclient.
 - Click **Properties**.

12. Ensure **Disk-Level** from Backup Types is selected.



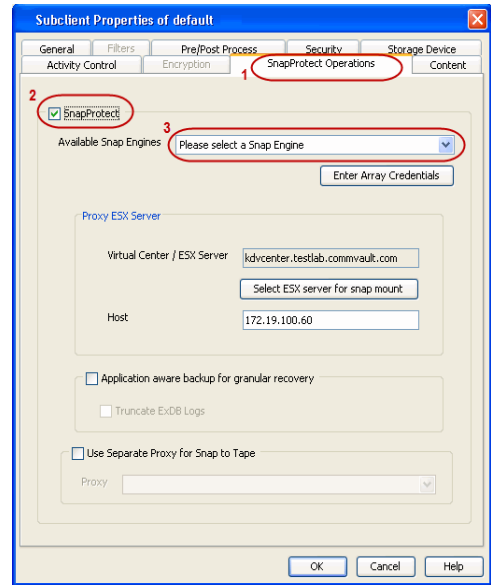
13.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.



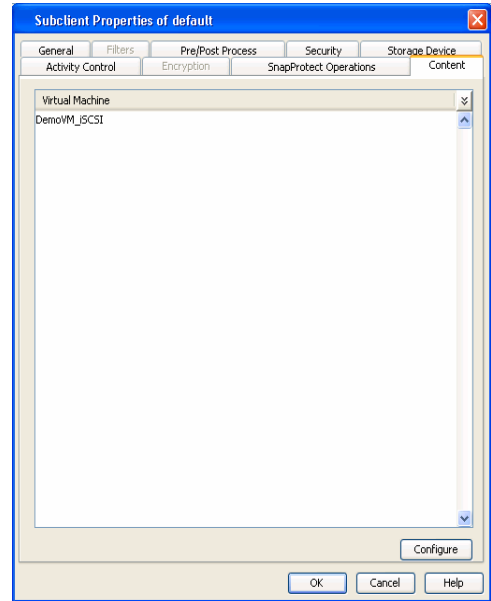
14.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - Click **Use Separate Proxy for Snap to Tape** if you want to perform SnapProtect operations in a different Virtual Server client computer.
 Select the client computer from the **Proxy** list.
 - Selecting a proxy from the **Use Proxy** option in the

General tab is not applicable for SnapProtect operations.

- When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.
- Ensure that the selected proxy ESX Server is not part of any Clustered Storage Group/Initiator group.



- 15.
- Click the **Content** tab.
 - Click **Configure** if you need to configure an additional virtual machine for the subclient.
 - Click **OK**.



SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

Click **Next** ► to Continue.

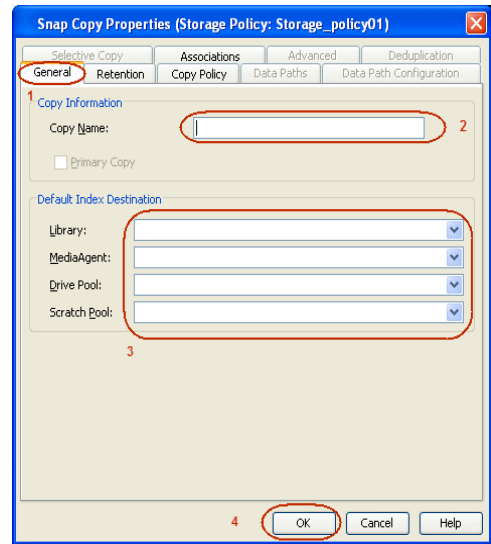
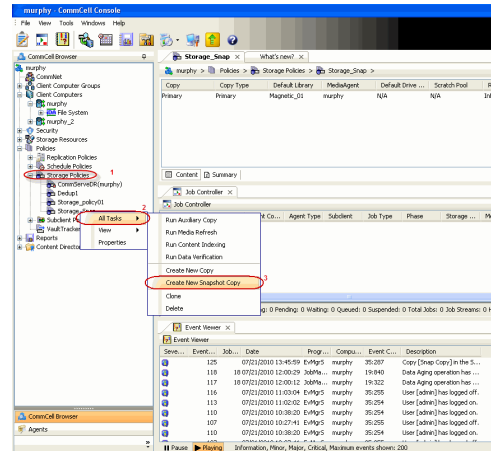
CREATE A SNAPSHOT COPY



Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.

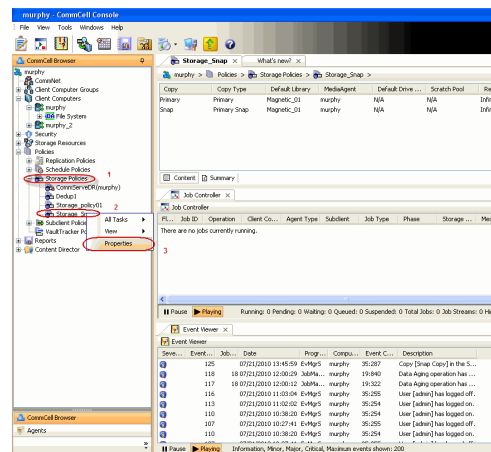
2.
 - Enter the copy name in the **Copy Name** field.
 - Select the **Library, MediaAgent, master Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



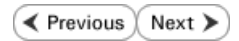
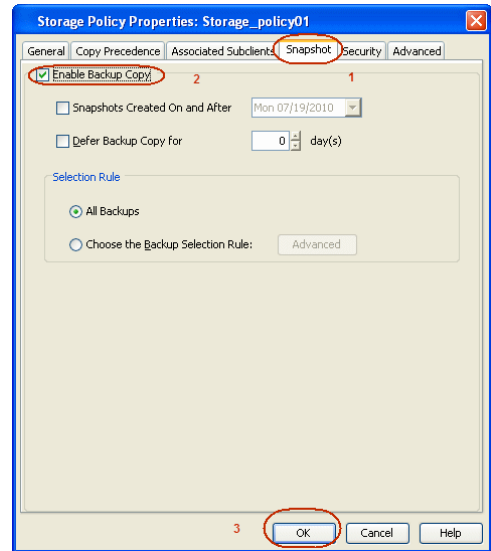
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



Storage Array Configuration

[◀ Previous](#) [Next ▶](#)

CHOOSE THE STORAGE ARRAY

HARDWARE STORAGE ARRAYS
3PAR
DELL COMPELLENT
DELL EQUALLOGIC
EMC CELERRA
EMC CLARIION, VNX
EMC SYMMETRIX
FUJITSU ETERNUS DX
HITACHI DATA SYSTEMS
HP EVA
IBM SVC
IBM XIV
LSI
NETAPP
NETAPP WITH SNAPVAULT/SNAPMIRROR
NIMBLE

[◀ Previous](#) [Next ▶](#)

SnapProtect™ Backup - 3PAR

◀ Previous Next ▶

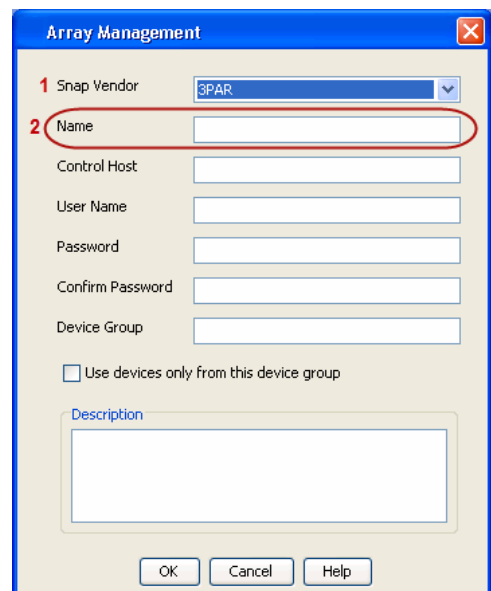
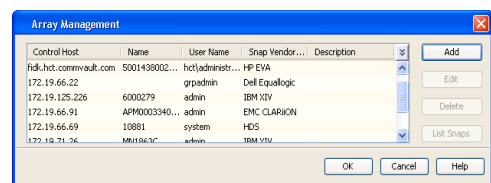
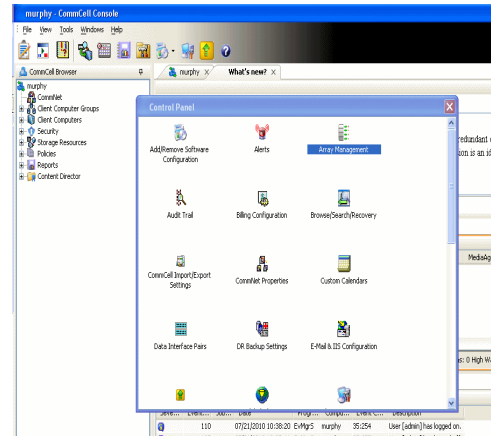
PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
 - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

where $\text{DevID.substr}(12,4)$ is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(12,4)$ is 0B95

After adding all the values, the resulting array name is 2FF70002AC00B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

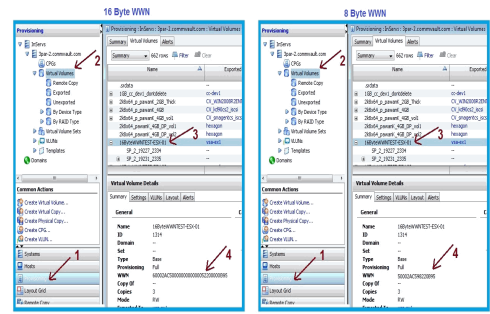
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(26,6)$ is 000B95

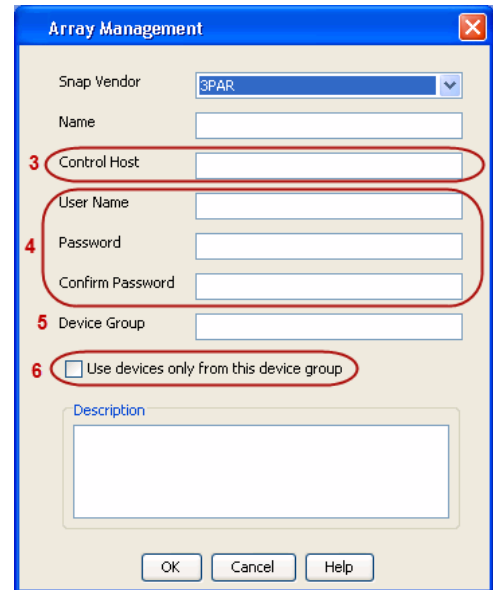
After adding all the values, the resulting array name is 2FF70002AC000B95.



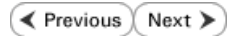
- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - Dell Compellent



PRE-REQUISITIES

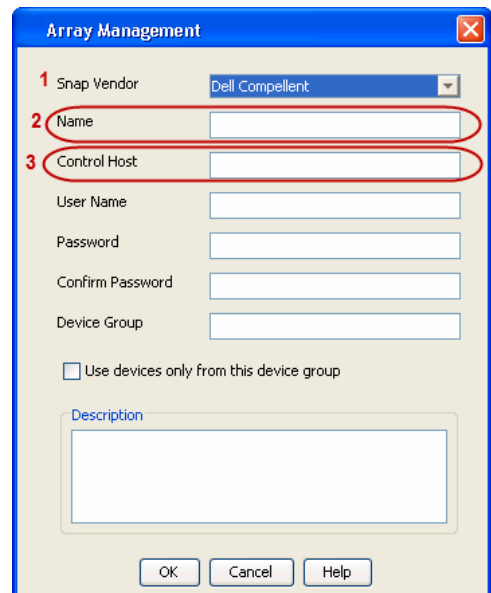
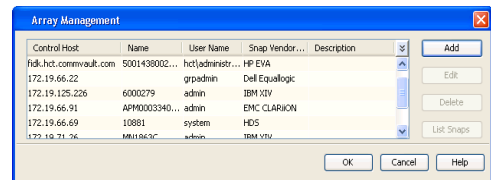
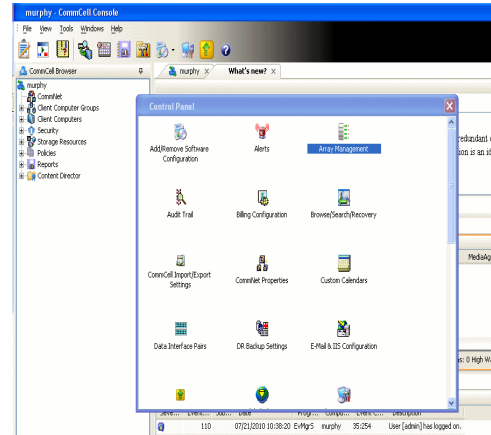
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

SETUP THE ARRAY INFORMATION

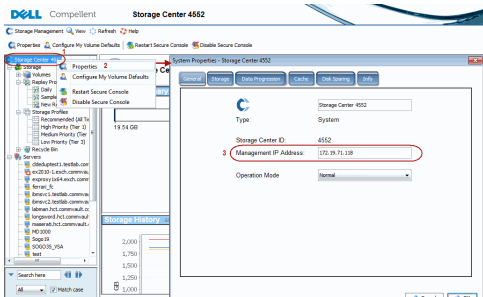
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **Dell Compellent** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** and **Control Host** fields.

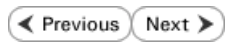
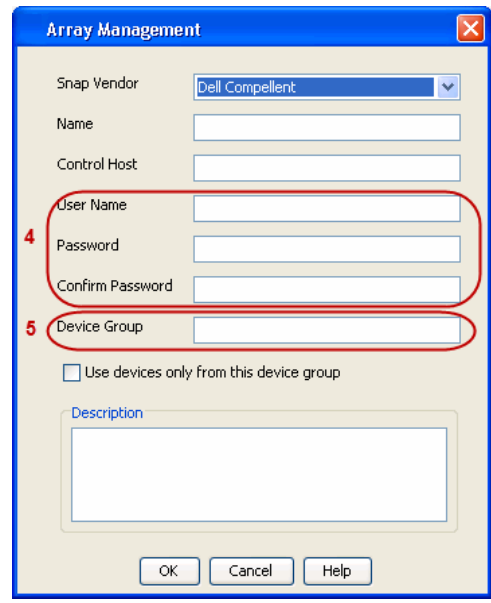
The Management IP address is also referred as the Storage Center IP address.



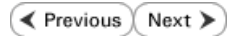
For reference purposes, the screenshot on the right shows the Storage Center Management Console of the Dell Compellent storage device displaying the Management IP address.



- 4.
- Enter the user access information of the application administrator in the **Username** and **Password** fields.
 - In the **Device Group** field, type *none* as this array does not use device groups for snapshot operations.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - Dell EqualLogic



PRE-REQUISITIES

WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

FIRMWARE VERSION

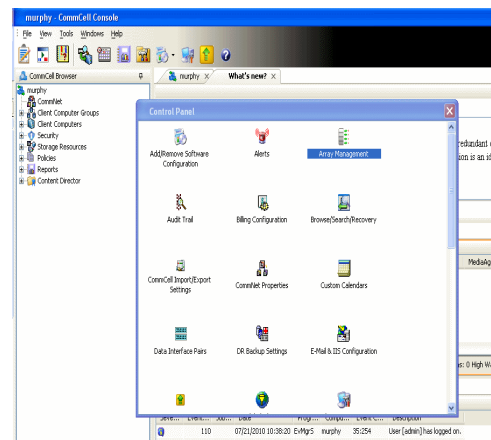
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

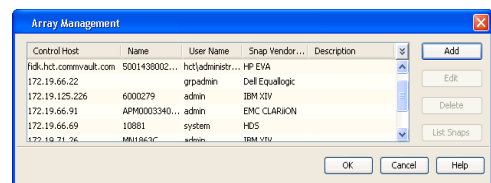
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



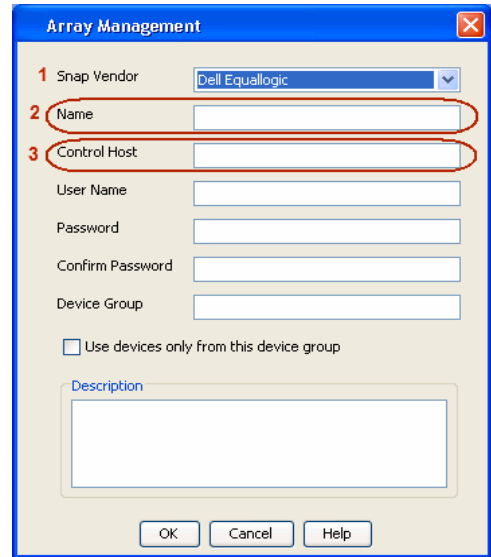
2. Click **Add**.



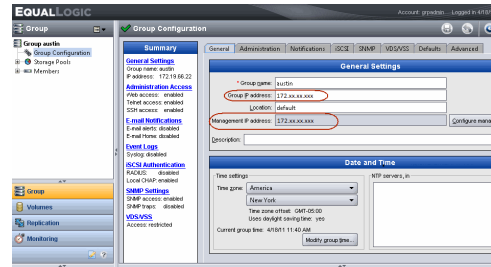
3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

No entry is required in the **Name** field if there is no Management IP address configured.

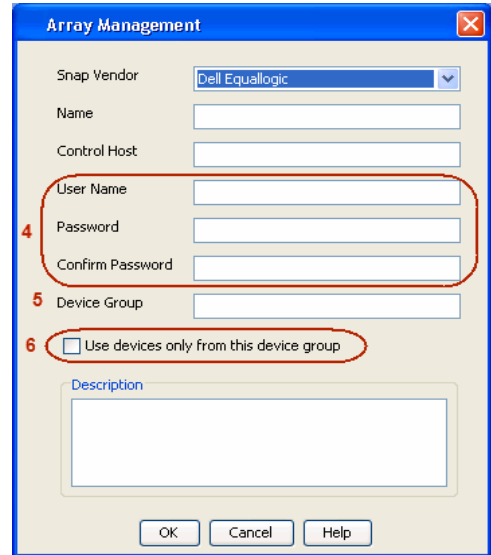
- Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
 - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
 - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
 - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous Next ▶

PRE-REQUISITES

LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

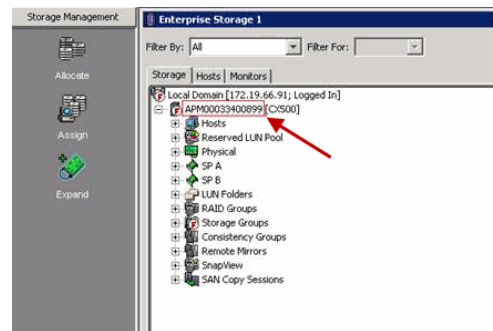
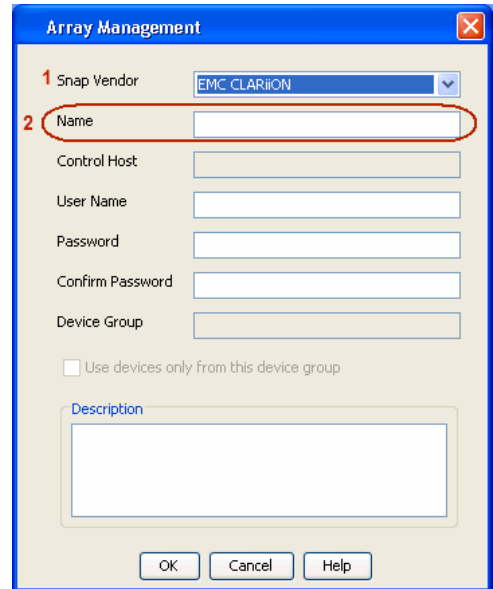
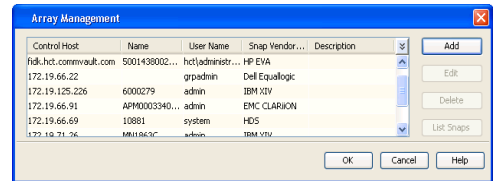
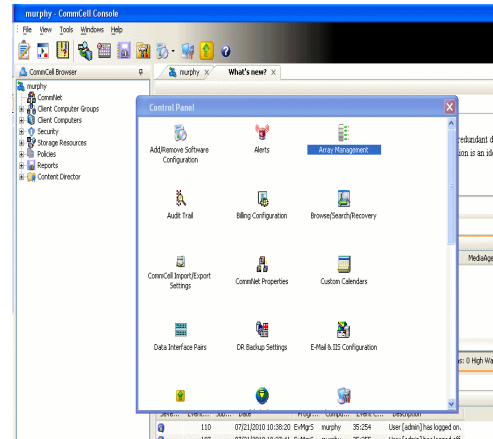
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
 - Specify the serial number of the array in the **Name** field.

For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.

- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



Array Management ✕

Snap Vendor:

Name:

Control Host:

User Name:

3 Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

SnapProtect™ Backup - EMC Symmetrix

◀ Previous Next ▶

PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

LOAD THE SYMMETRIX DATABASE

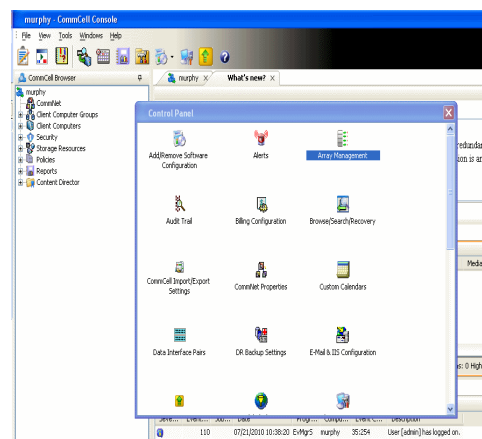
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

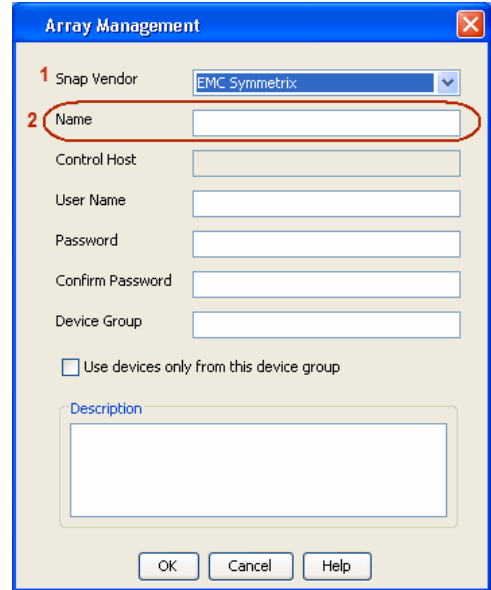
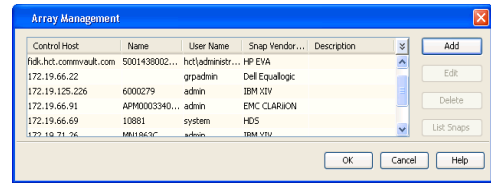
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

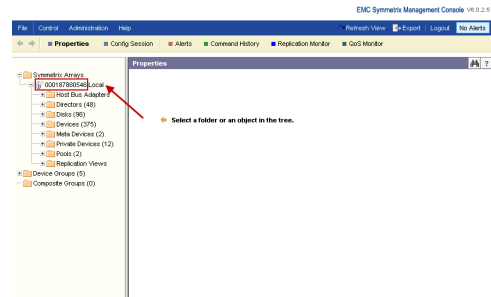


- Click **Add**.

3.
 - Select **EMC Symmetrix** from the **Snap Vendor** list.
 - Specify the **Symm ID** of the array in the **Name** field.

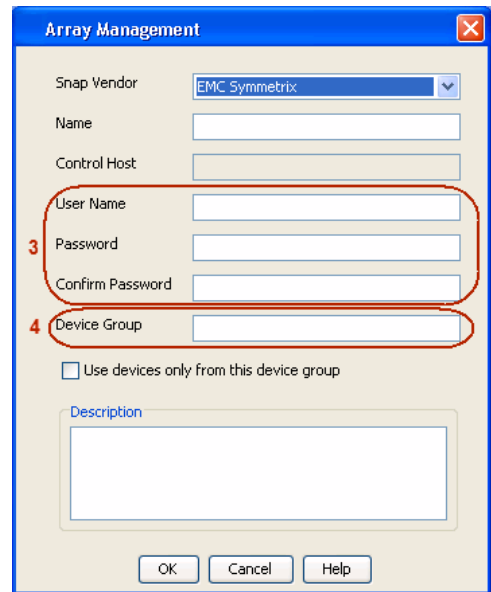


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.
If you do not specify a device group, the default device group will be used for snapshot operations.
 - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).



SnapProtect™ Backup - Hitachi Data Systems

◀ Previous Next ▶

PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
 - COW pools
 - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

ADDITIONAL REQUIREMENTS FOR VMWARE

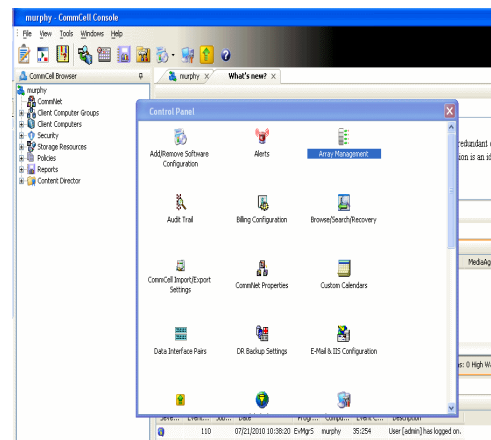
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server *iDataAgent* client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server *iDataAgent* client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

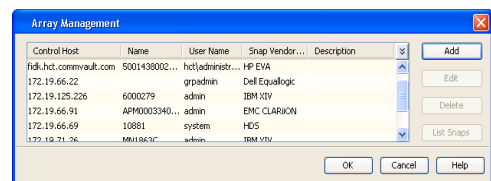
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

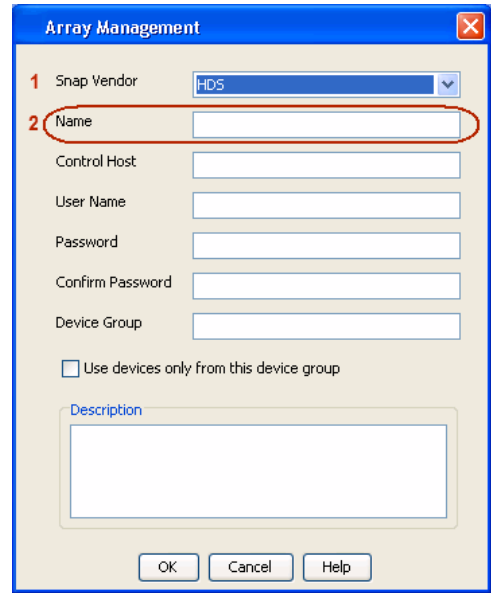
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



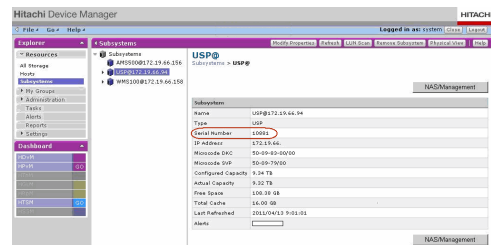
2. Click **Add**.



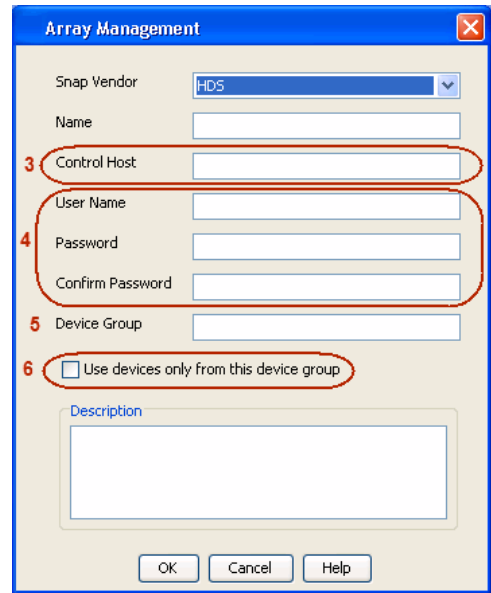
3.
 - Select **HDS** from the **Snap Vendor** list.
 - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



- 4.
- Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:
`<COW_POOL_ID>-<LABEL>` or `<LABEL>-<COW_POOL_ID>`
 where `<COW_POOL_ID>` (for COW job) should be a number. This parameter is required.
`<LABEL>` (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.
 - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - HP StorageWorks EVA

◀ Previous Next ▶

SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

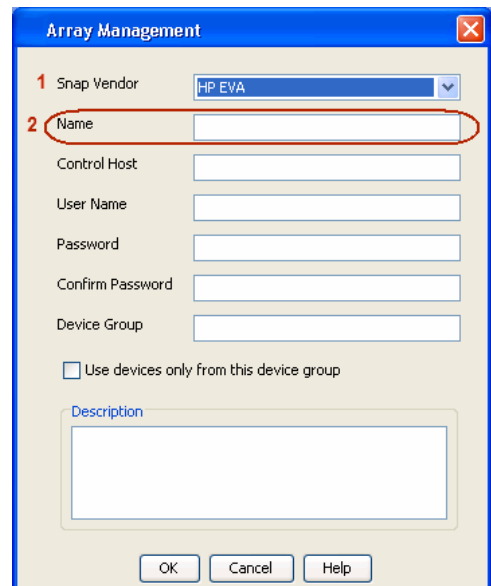
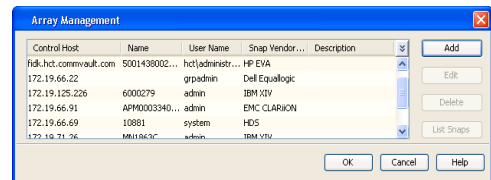
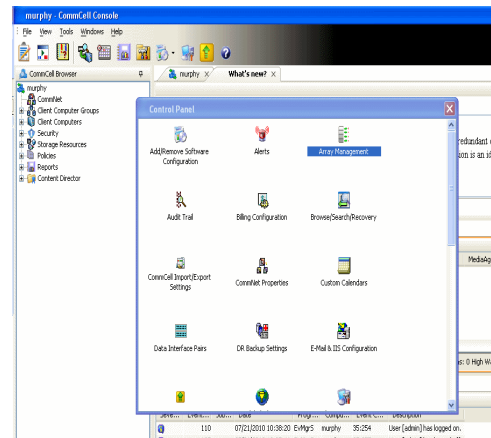
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the `C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin` folder to discover the HP-EVA arrays.
3. Use the `CLIRefreshTool.bat` tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the `C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin` folder.

SETUP THE ARRAY INFORMATION

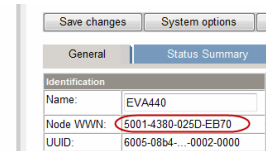
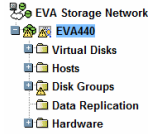
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
2. Click **Add**.
3.
 - Select **HP EVA** from the **Snap Vendor** list.
 - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

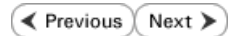
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



4.
 - Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous Next ▶

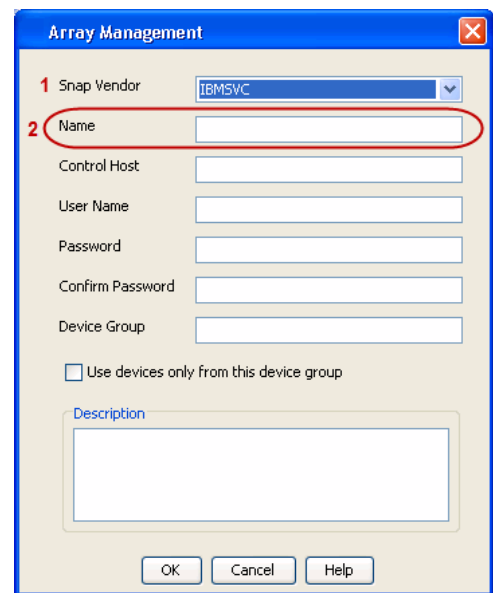
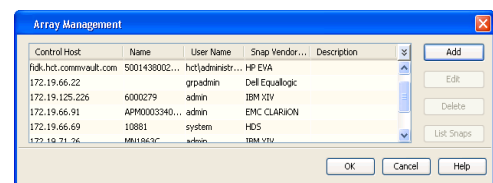
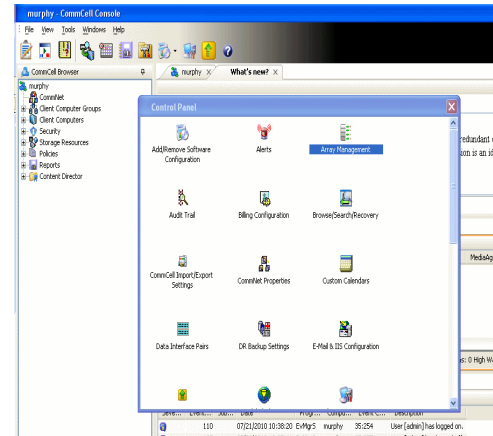
PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

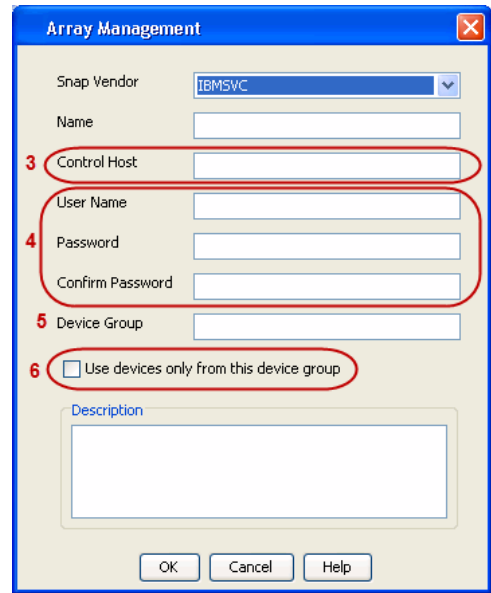
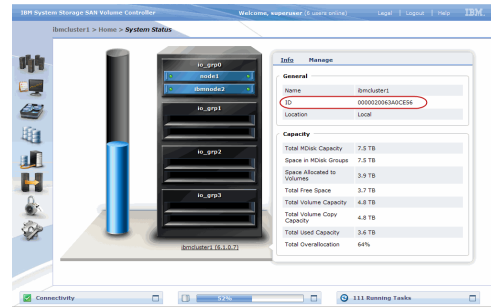
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM XIV

◀ Previous Next ▶

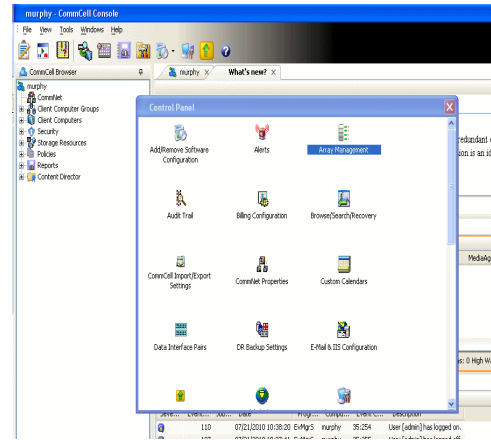
PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

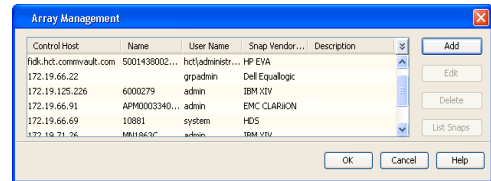
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

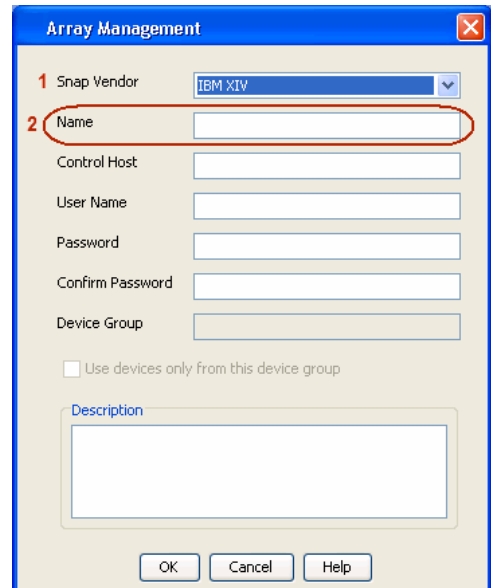
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

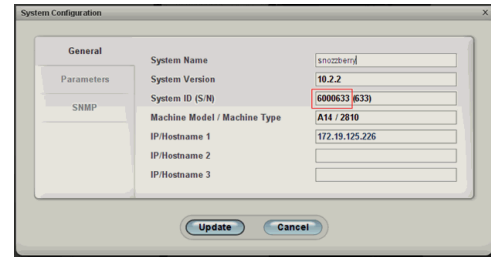


3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.

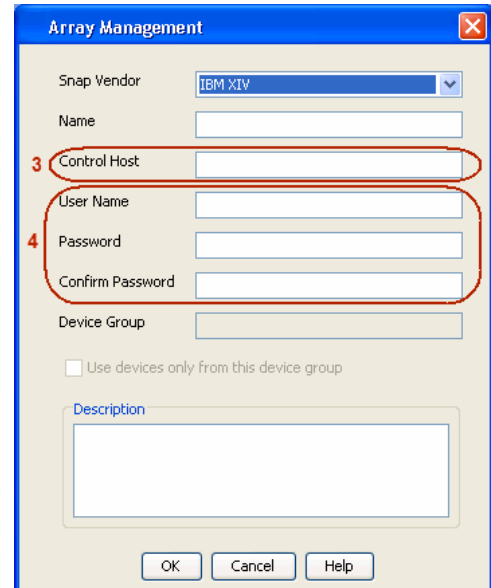


The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

- 4.
- Enter the IP address or host name of the array in the **Control Host** field.
 - Enter the user access information of the application administrator in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



The System Configuration dialog box shows the General tab. The System Name is 'snap24m1', System Version is '10.2.2', System ID (S/N) is '6000633 6333', and Machine Model / Machine Type is 'A14 / 2810'. IP/Hostname 1 is '172.19.125.226'. There are Update and Cancel buttons at the bottom.



The Array Management dialog box has a Snap Vendor dropdown set to 'IBM XIV'. The Name field is empty. The Control Host field is circled in red and labeled with a red '3'. The User Name, Password, and Confirm Password fields are grouped together in a red oval and labeled with a red '4'. The Device Group field is empty. There is a checkbox for 'Use devices only from this device group' which is unchecked. A Description text area is empty. There are OK, Cancel, and Help buttons at the bottom.

< Previous Next >

SnapProtect™ Backup - LSI

◀ Previous Next ▶

PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
 - SMIS server through TCP/IP network.
 - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

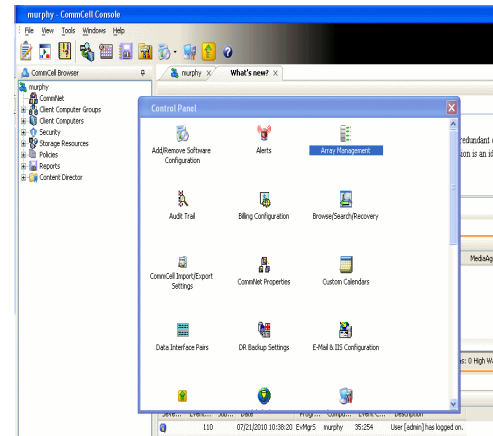
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

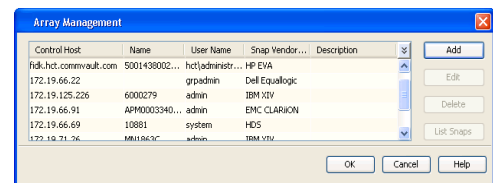
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

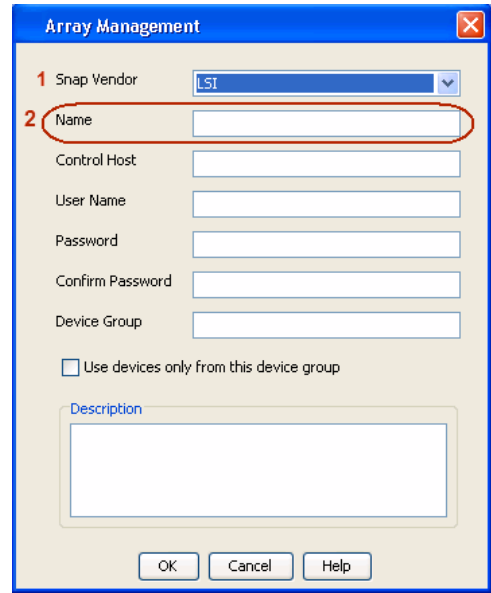
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

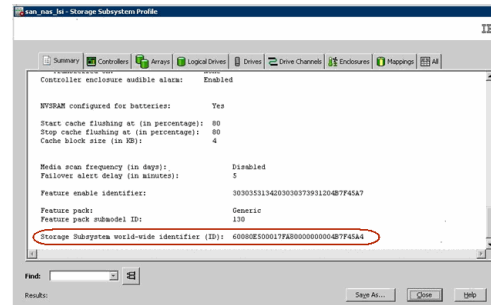


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

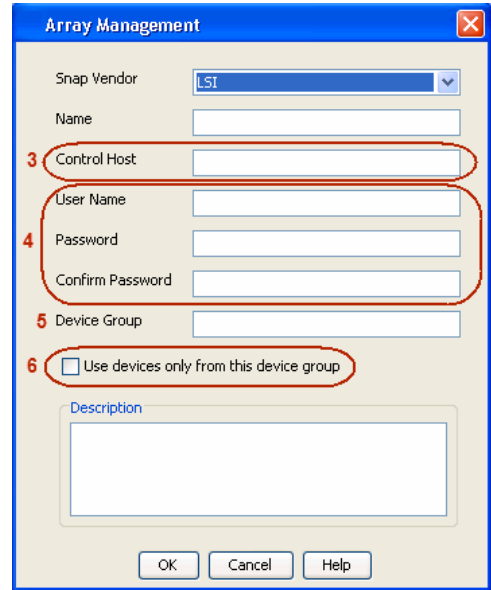
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



4.
 - Specify the name of the device manager server where the array was configured in the **Control Host** field.
 - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

If you specify None in the **Device Group** field but do have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - NetApp



PREREQUISITES

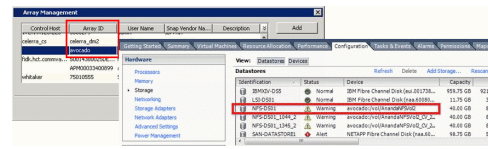
LICENSES

- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

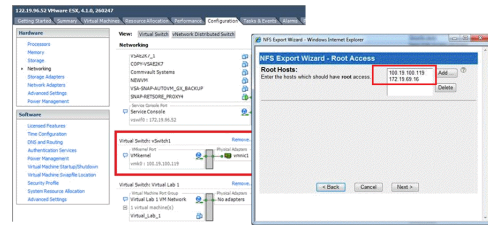
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.



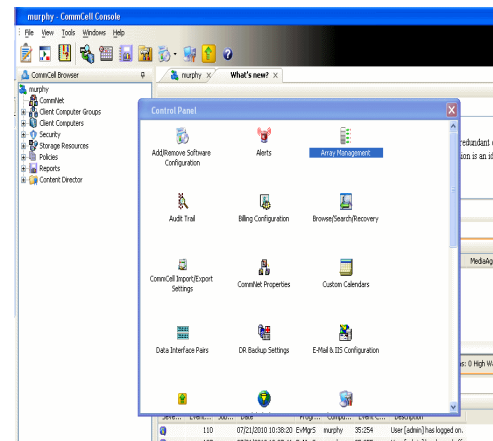
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



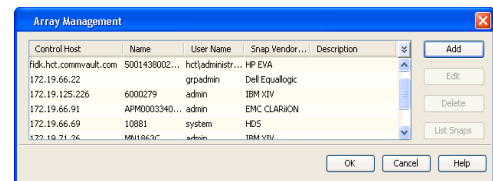
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the file server in the **Name** field.
 - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: []

Control Host: []

User Name: []

Password: []

Confirm Password: []

Device Group: []

Use devices only from this device group

Description: []

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous Next ▶

OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

PREREQUISITES

LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:


```
options snapvault.enable on
```
3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:


```
options snapvault.access host=secondary_filer1, secondary_filer2
```
4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:


```
options snapvault.access host=primary_filer1, primary_filer2
```

INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
 - Discover storage devices
 - Add Resource Pools to be used for the Vault/Mirror storage provisioning

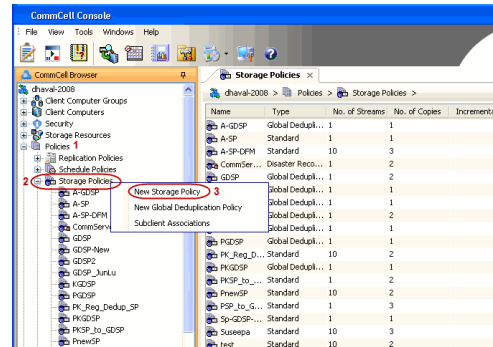
CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

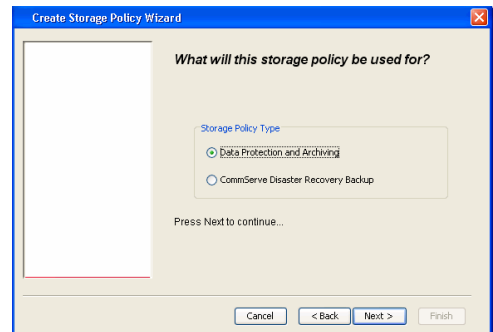
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

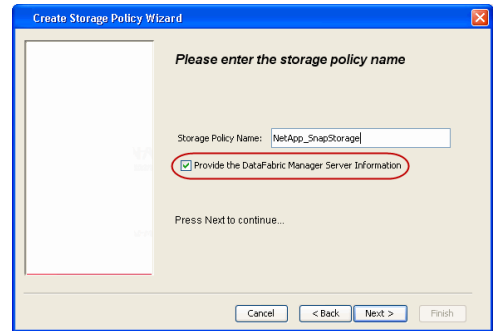
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



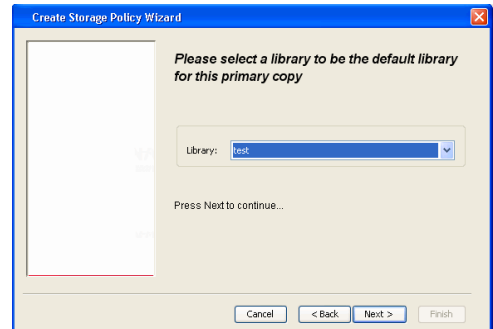
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.

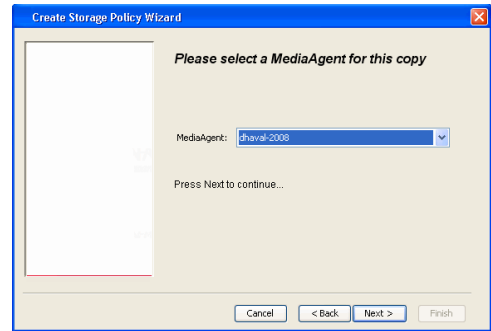
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

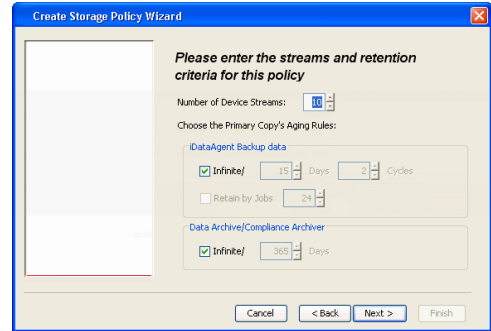


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

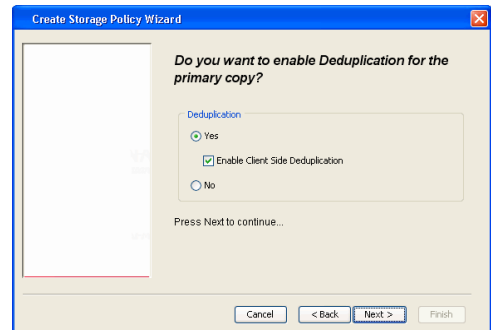
6. Click **Next**.



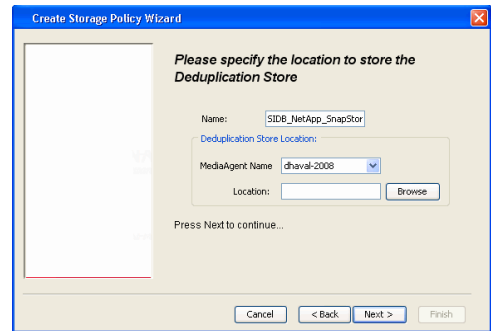
7. Click **Next**.



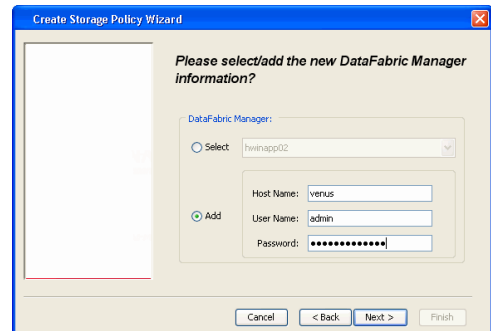
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

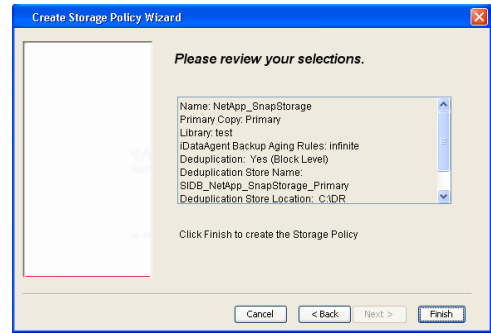


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



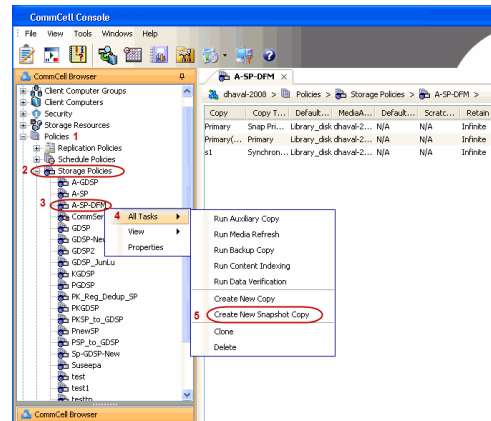


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

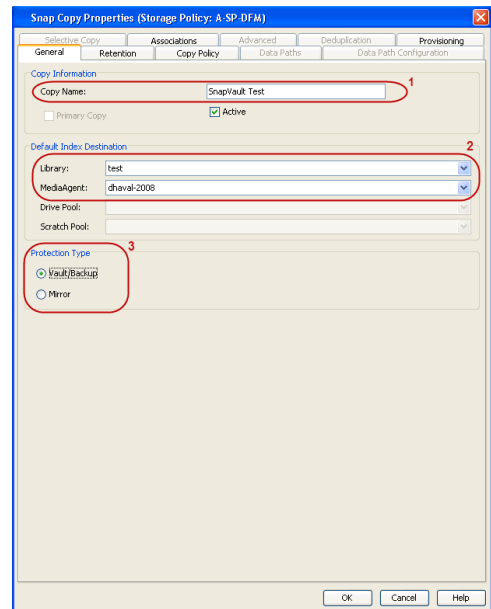
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
 - Enter the **Copy Name**.
 - Select the **Library** and **MediaAgent** from the drop-down list.
 - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

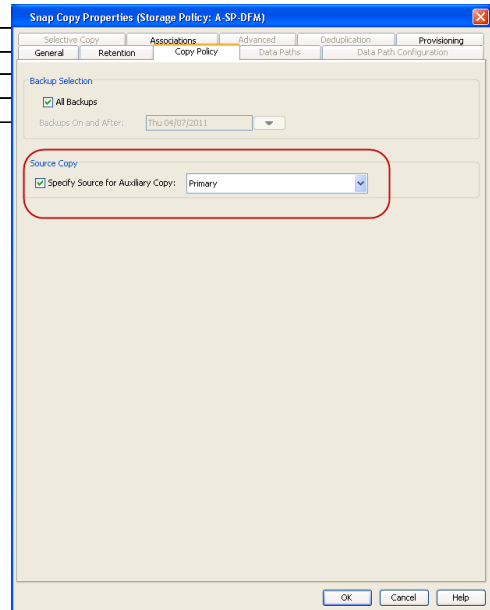


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

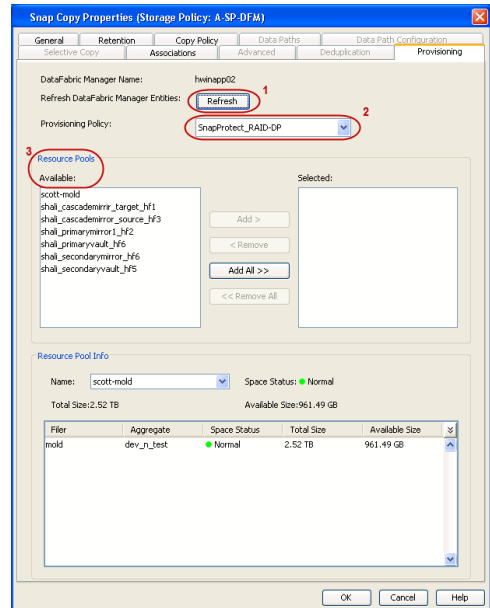
TOPOLOGY	SOURCE COPY
----------	-------------

Primary-Mirror	Primary
Primary-Mirror-Vault	Mirror
Primary-Vault	Primary
Primary-Vault-Mirror	Vault
Primary-Mirror-Mirror	Mirror



4.
 - Click the **Provisioning** tab.
 - Click **Refresh** to display the DFM entities.
 - Select the **Provisioning Policy** from the drop-down list.
 - Select the **Resource Pools** available from the list.
 - Click **OK**.

The secondary snapshot copy is created.



5. If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:

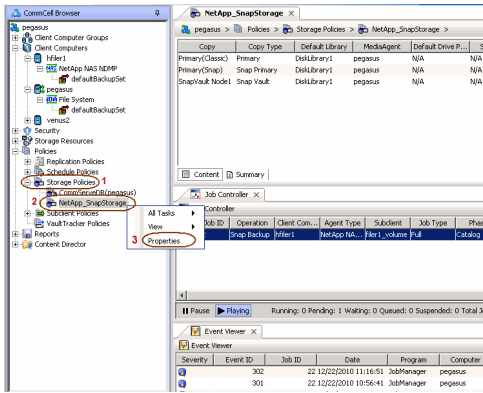

```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

It is recommended that you perform this operation on all nodes in the P-M-V topology.

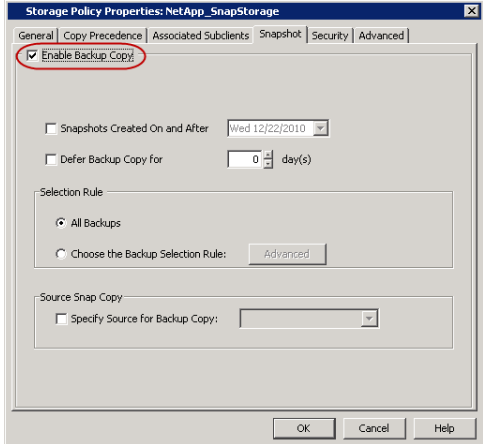
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

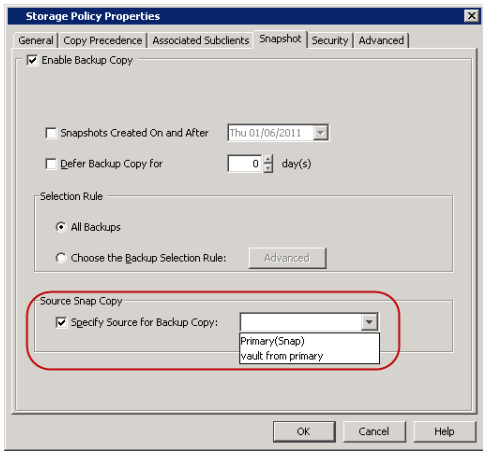
1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



3.
 - Select **Specify Source for Backup Copy**.
 - From the drop-down list, select the source copy to be used for performing the backup copy operation.



SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

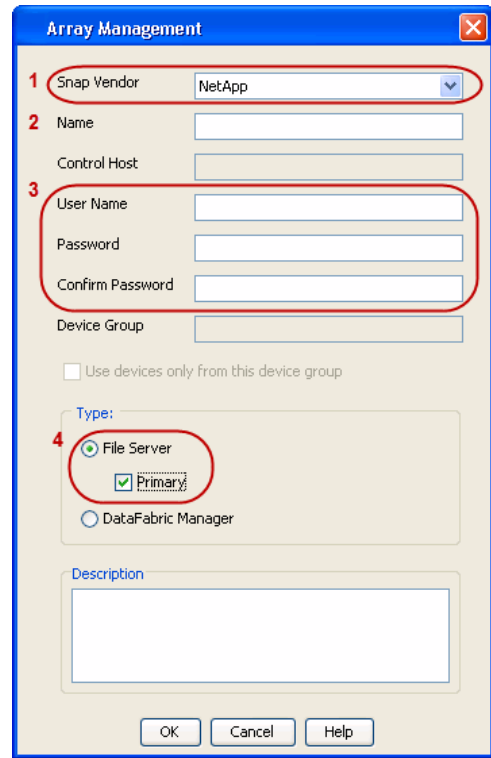
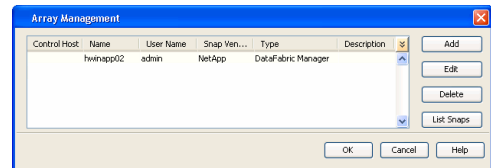
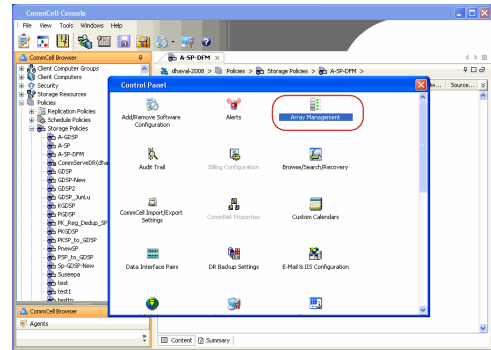
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

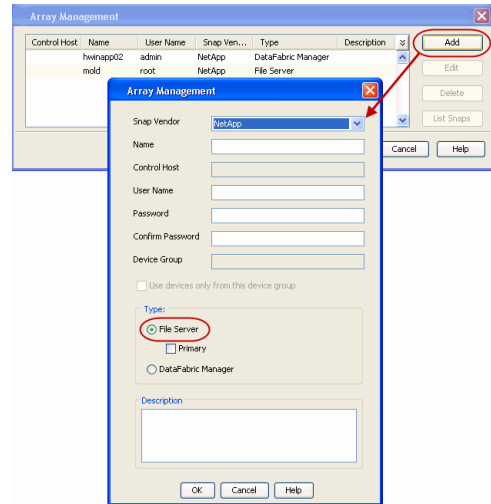
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

4.
 - Click **Add** again to enter the information for the secondary array.
 - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.





SEE ALSO

Import Wizard Tool

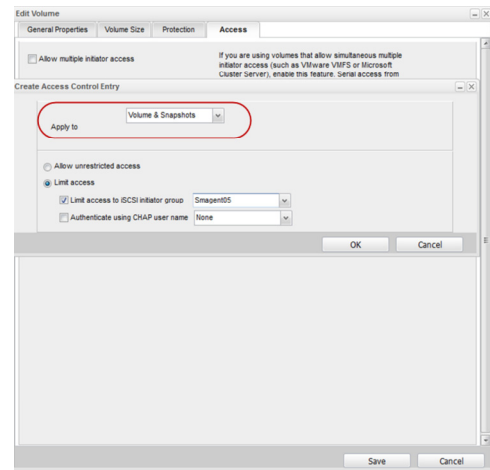
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

SnapProtect™ Backup - Nimble

◀ Previous Next ▶

PREREQUISITES

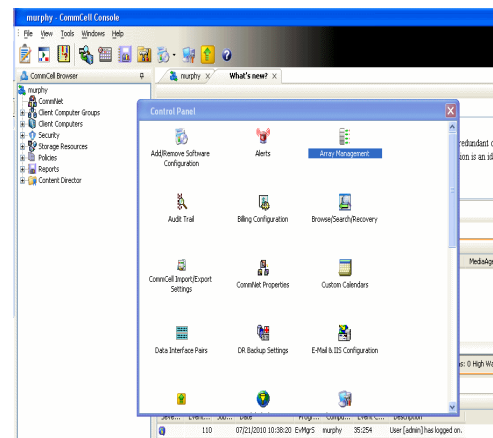
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry** to **Snapshots Only**.
- Ensure that a temporary LUN is allocated to all ESX Servers that are used for snapshot operations.



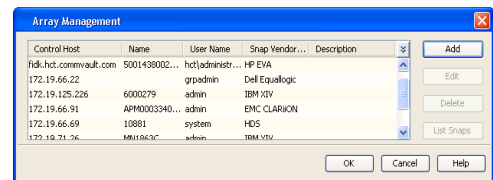
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **Nimble** from the **Snap Vendor** list.
 - Specify the Data IP Address of the array in the **Name** field.

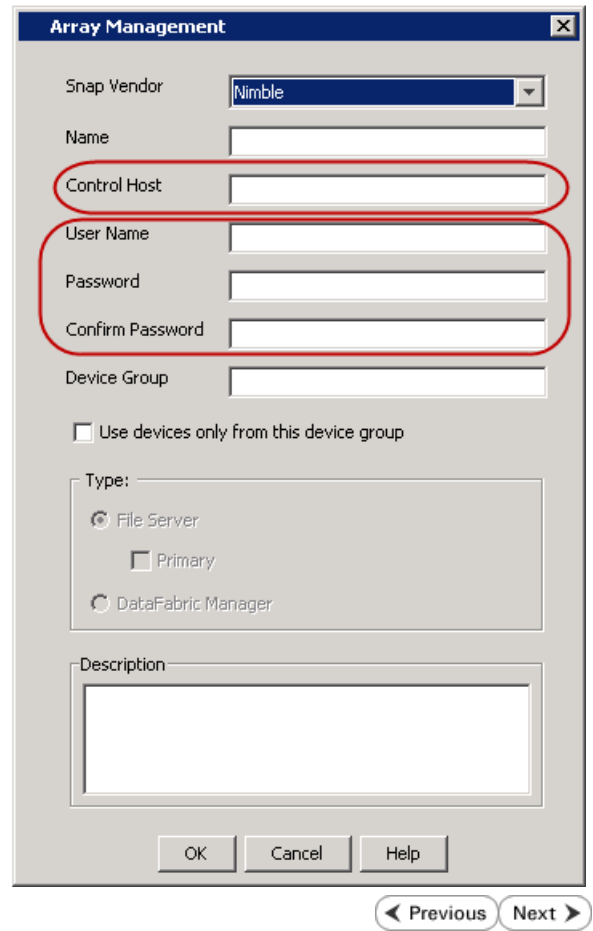
If you have more than one Data IP Address configured, you will need to add the array information for each of the configured Data IP addresses.

- Enter the Management IP Address of the array in the **Control Host** field.

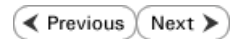
For reference purposes, the screenshot on the right shows the Data IP Address and Management IP for the Nimble storage device.

Name	Status	Type	Data IP Address	Subnet Mask	MTU	Bytes
eth1		Data only	172.19.108.100	255.255.252.0	Standard	1500
eth2		Data only	172.19.108.101	255.255.252.0	Standard	1500
eth3		Not configured			Standard	1500
eth4		Not configured			Standard	1500

4.
 - Enter the access information of a user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



Getting Started - VMware Backup

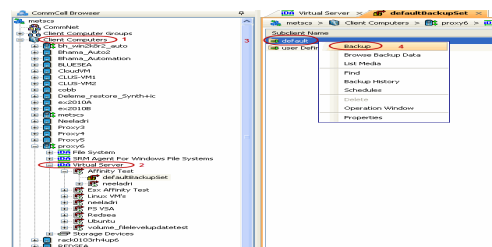


PERFORM A BACKUP

After configuring your Instance, Backup Set and Subclient, you are ready to perform your first backup.

The following section provides step-by-step instructions for running your first full backup of a single virtual machine immediately.

1.
 - From the CommCell Console, navigate to **Client Computers | Virtual Server**.
 - Right-click the **Subclient** and click **Backup**.



2.
 - Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.

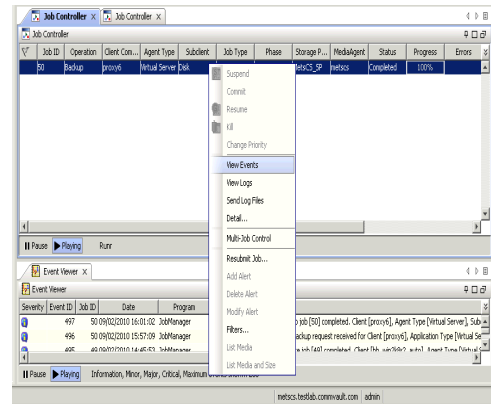
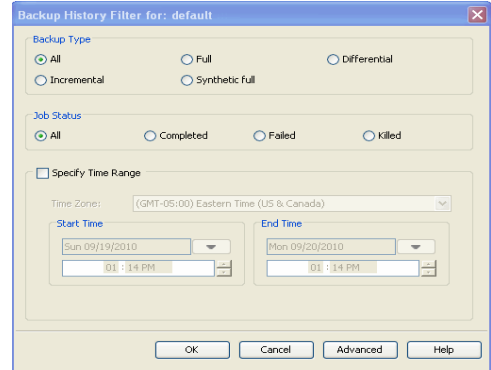
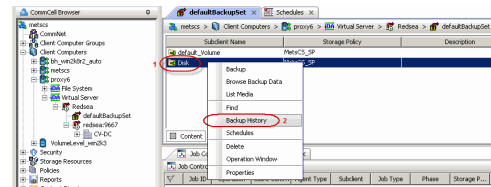
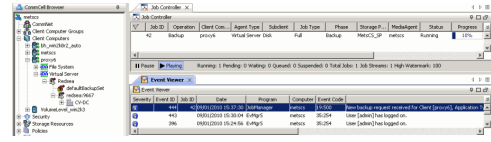
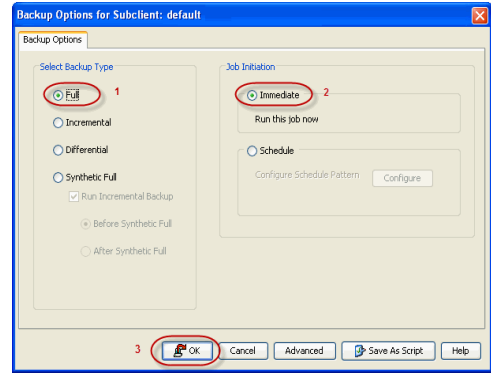
3. You can track the progress of the job from the **Job Controller** window of the CommCell console.

4. Once job is complete, view the details of job from the **Backup History**. Right-click the **Subclient** and select **Backup History**.

5. Click **OK**.

6. You can view the following details about the job by right-clicking the job:

- Items that failed during the job
- Items that succeeded during the job
- Details of the job
- Events of the job
- Log files of the job
- Media associated with the job



Getting Started - Vault/Mirror Copy

◀ Previous Next ▶

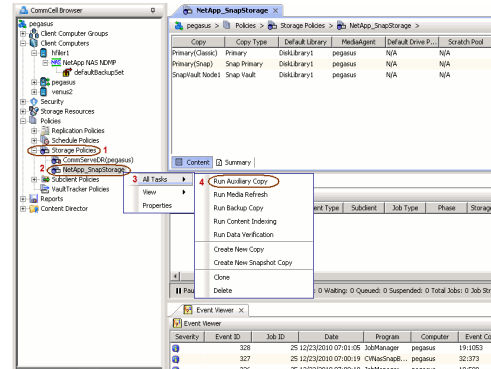
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

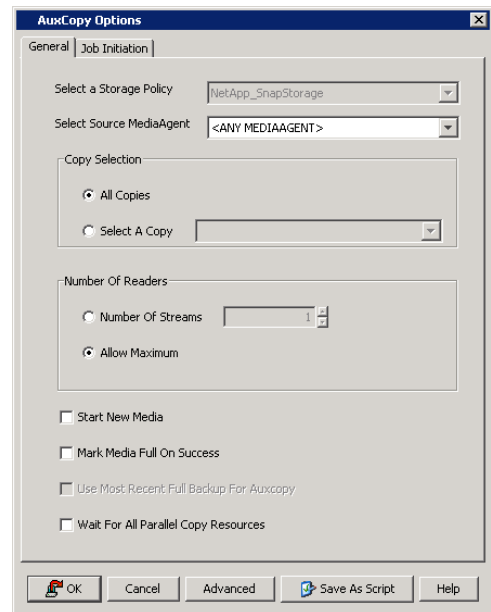
INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

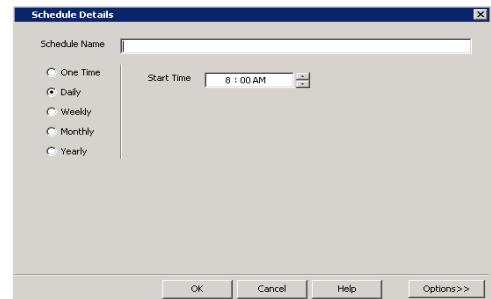


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- Enter the schedule name and select the appropriate scheduling options.
 - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.

◀ Previous Next ▶

Getting Started - VMware Snap Movement to Media

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

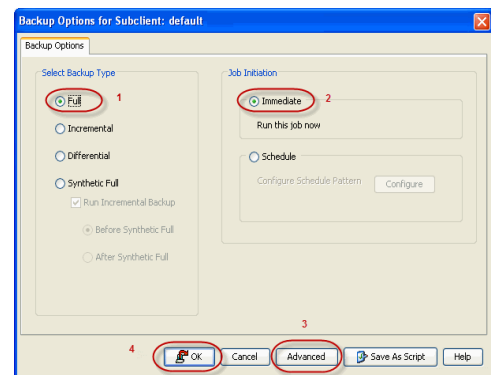
BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

INLINE BACKUP COPY

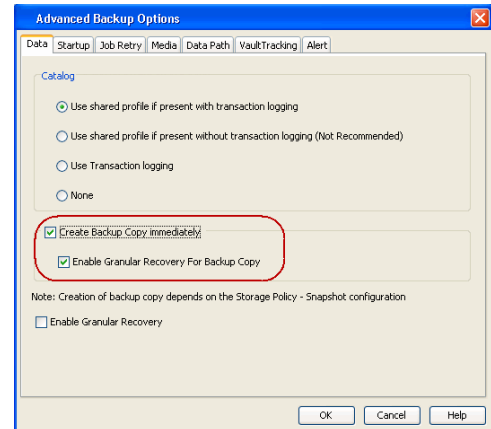
Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

- From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
 - Right click the default subclient and click **Backup**.
 - Select **Full** as backup type.
 - Click **Advanced**.



- Select **Create Backup Copy immediately** to create a backup copy.

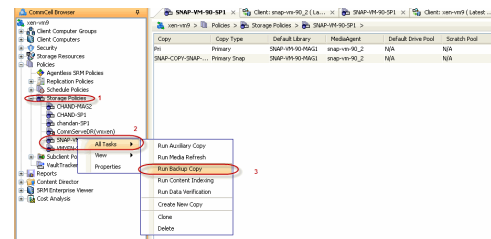
Enable Granular Recovery for Backup Copy is automatically selected. This option allows you to view the file/folder level details of the backup copy.
 - If you want to view the file/folder level details of the snapshot copy, select **Enable Granular Recovery**.
 - Click **OK**.



OFFLINE BACKUP COPY

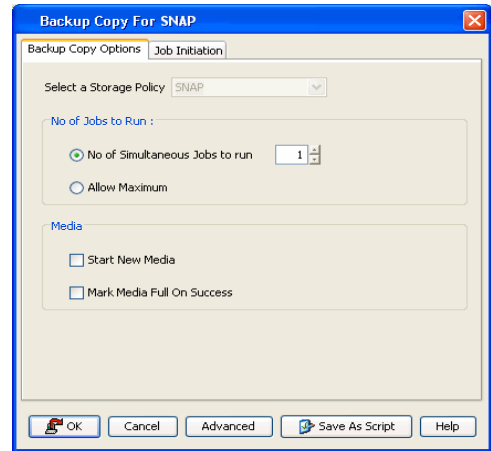
Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

- From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



- Select **Start new media** to copy the data to a different tape or optical media.
 - Select **Mark media full on Success** to mark the media that is used for this operation after the snapshot copy operation has successfully completed.

- Click **OK**.



Getting Started - VMware Restore



PERFORM A RESTORE

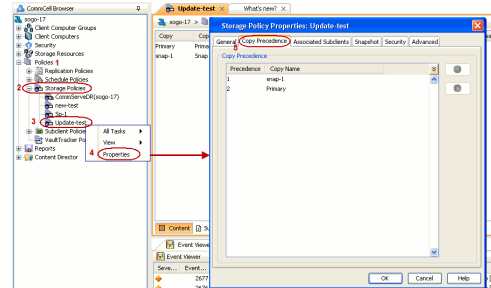
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections describe the steps involved in restoring a virtual machine to a different Virtual Center/ESX Server.

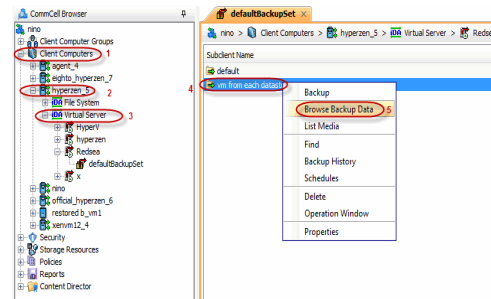
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.

You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.

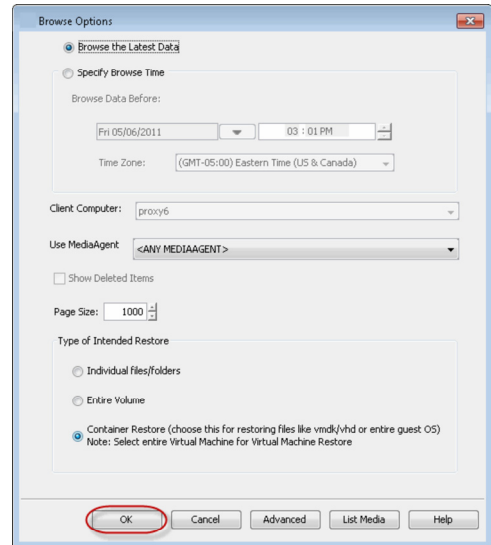
- Click **OK**.



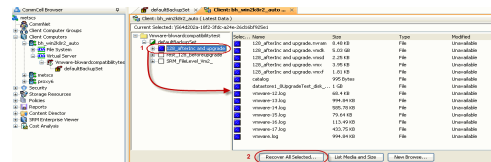
- From the CommCell Console, navigate to **<Client> | Virtual Server**.
 - Right-click the subclient that contains the data you want to restore and click **All Tasks | Browse Backup Data**.



- Select the MediaAgent that was used during the storage policy creation from the **Use MediaAgent** drop-down list. This MediaAgent should be the one you installed along with the Virtual Server agent.
 - Click **OK**.



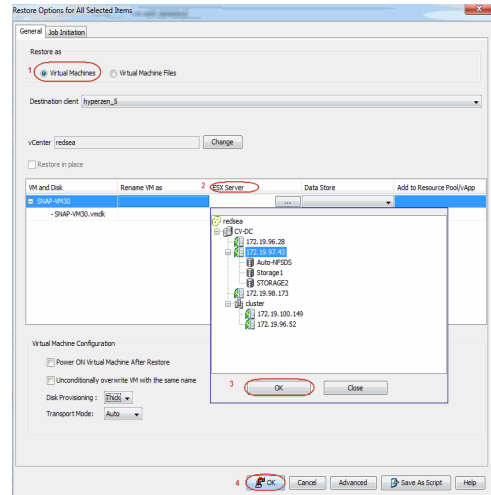
- Select the virtual machine under the backup set. Its entire contents will be automatically selected in the right pane.
 - Click **Recover All Selected**.



- Select the **Destination ESX Server** to which the virtual machine will be restored.

6. Select the **Datastore** to which the disk will be restored.

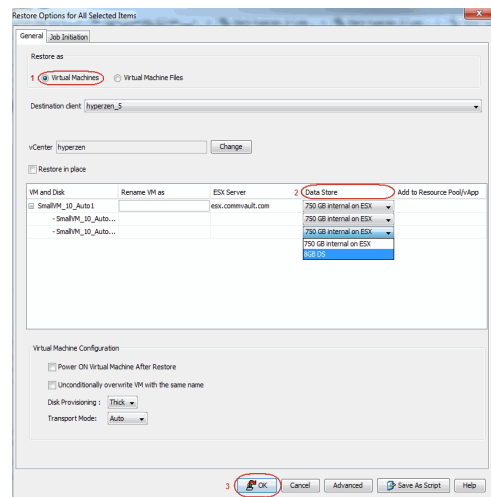
If the selected datastore does not meet the minimum requirements needed to restore the virtual machine, you can repeat this step until an acceptable datastore is found.



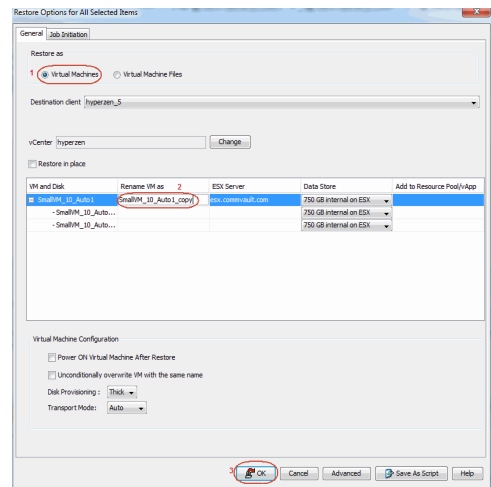
7. Enter the **VM Name** for the virtual machine.

Ensure that you provide a fully qualified name for the virtual machine. Entering an IP address will cause the restore operation to fail.

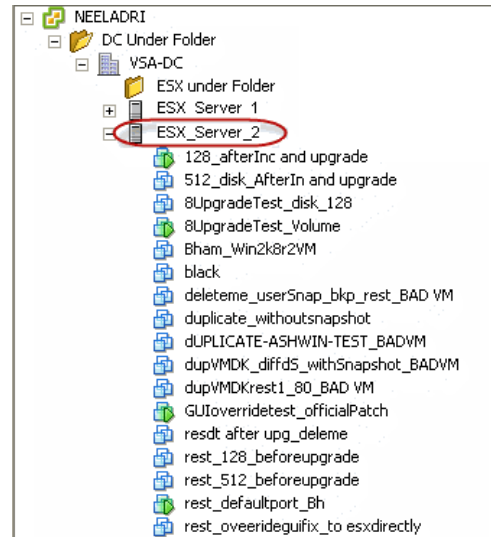
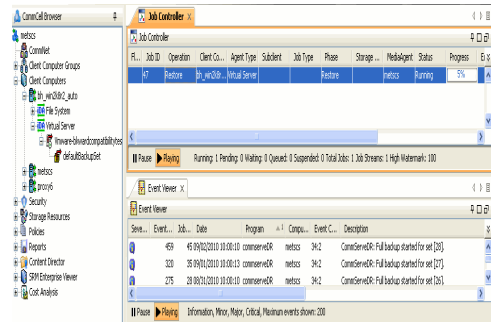
- Click **OK**.



8. You can monitor the progress of the restore job in the **Job Controller** window of the CommCell Console.



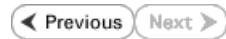
- Once the virtual machine is restored, it is automatically mounted to the virtual center/ESX Server you selected.



CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



Deployment - Microsoft Exchange Database Agent

Choose the appropriate installation procedure as described in the tables below.

EXCHANGE SERVER 2010

SERVER SETUP	INSTALLATION PROCEDURE
64-bit Exchange Server	Install the 64-bit Exchange Database Agent on Exchange Server 2010 or 2007

EXCHANGE SERVER 2007

SERVER SETUP	INSTALLATION PROCEDURE
64-bit Exchange Server	Install the 64-bit Exchange Database Agent on Exchange Server 2010 or 2007
64-bit Exchange Server - Cluster	Install the 64-bit Exchange Database Agent on Exchange Server 2010 or 2007 - Clustered Environment

EXCHANGE SERVER 2003

SERVER SETUP	INSTALLATION PROCEDURE
Exchange Server	Install the Exchange Database Agent on Exchange Server 2003
Exchange Server - Cluster	Install the Exchange Database Agent on Exchange Server 2003 - Clustered Environment

Getting Started - Install the 64-bit Exchange Database Agent on Exchange Server 2010 or 2007

◀ Previous Next ▶

Follow the steps given below to install Exchange Database iDataAgent on one of the following:

- 64-bit Exchange Server 2010
- 64-bit Exchange Server 2007

WHERE TO INSTALL

The Exchange Database iDataAgent can be installed directly onto the Exchange Server. This method is referred to as an on-host installation and is useful if you want to preserve hardware resources.

BEFORE YOU BEGIN

Download Software Packages

Download the latest software package to perform the install.

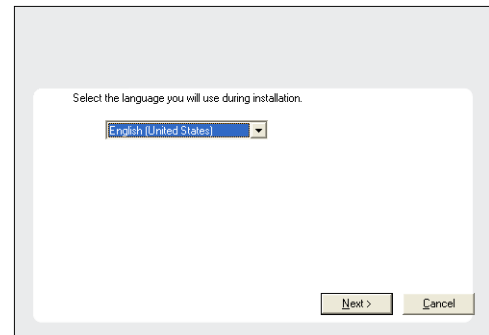
SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.

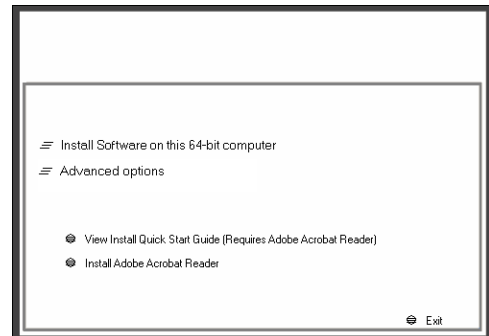
INSTALL THE EXCHANGE DATABASE iDATAAGENT

Use the following procedure to directly install the software from the installation package or a network drive.

1. Log on to the computer using an account with the following privileges:
 - Administrator of the local computer
 - Administrator of the Exchange Server
2. Run **Setup.exe** from the Software Installation Package.
3. Select the required language.
Click **Next**.



4. Select the option to **Install Calypso on this 64-bit computer**.
Your screen may look different from the example shown.



5. Select **I accept the terms in the license agreement**.
Click **Next**.

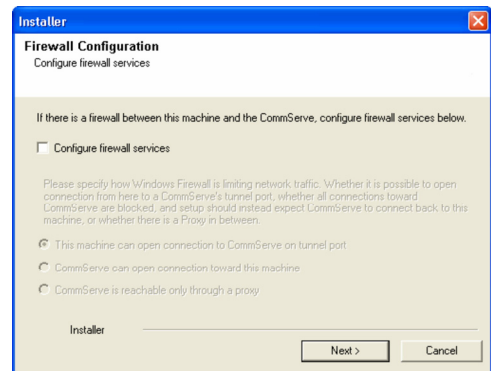
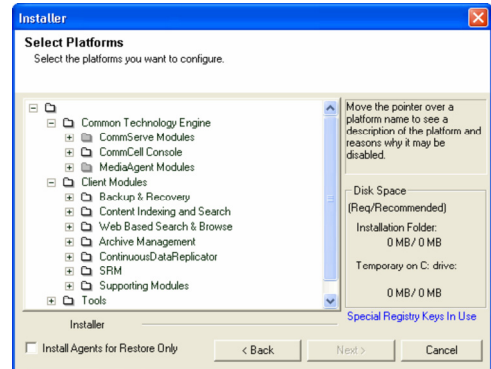
6.
 - Expand **Client Modules | Backup & Recovery | Exchange**, and select **Exchange Database /DataAgent**.
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
 - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
 - Click **Next**.



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

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

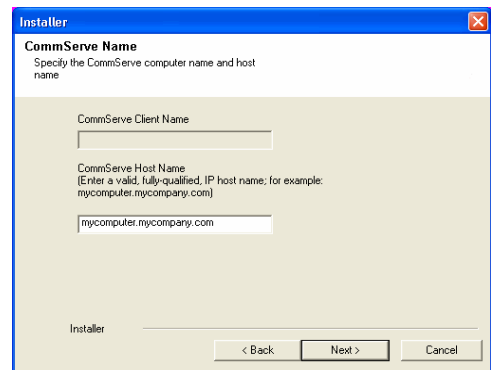
If firewall configuration is not required, click **Next**.



8. Enter the fully qualified domain name of the **CommServe Host Name**. Click **Next**.

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

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



9. Click **Next**.

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

Click **Next**.

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

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

11. Click **Next**.

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

12. Verify the default location for software installation.

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

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

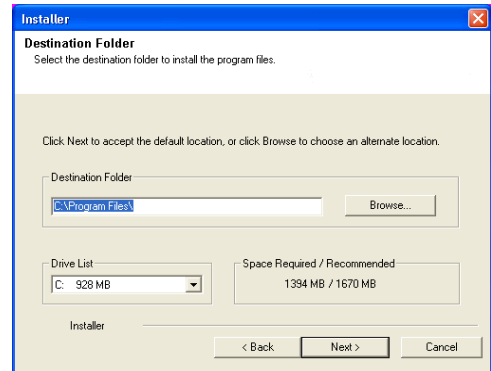
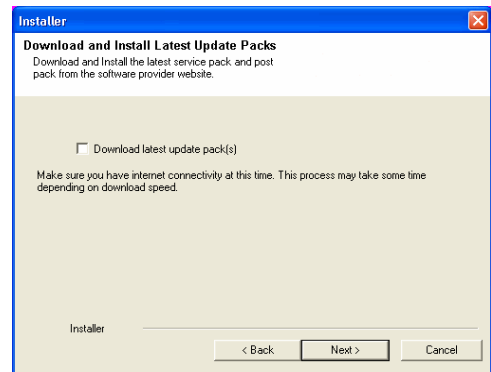
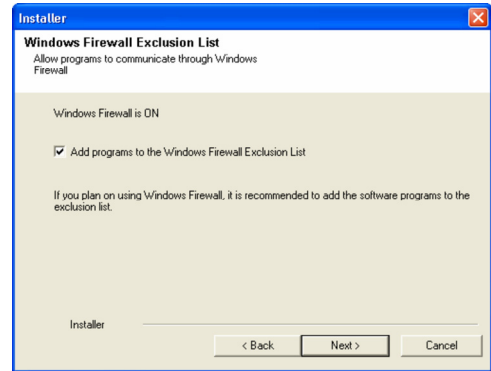
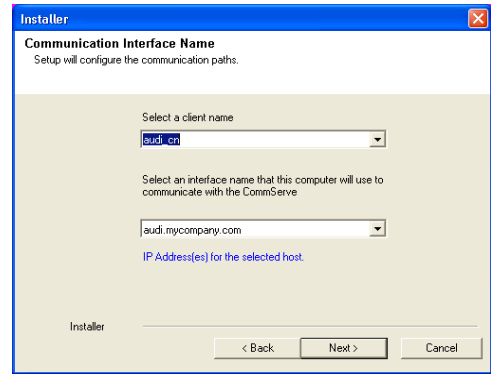
/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

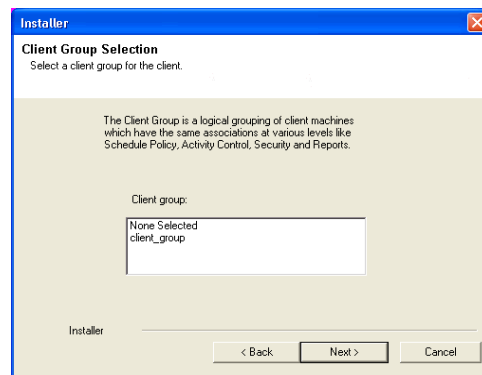
13. Select a Client Group from the list.

Click **Next**.

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

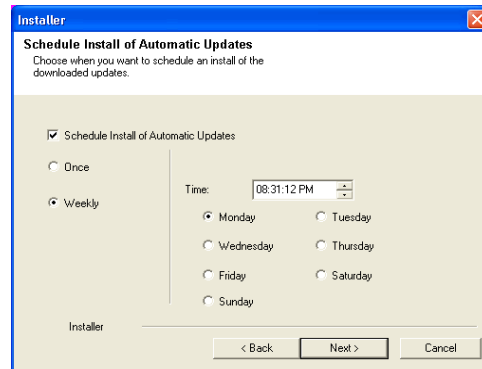


14. Click **Next**.

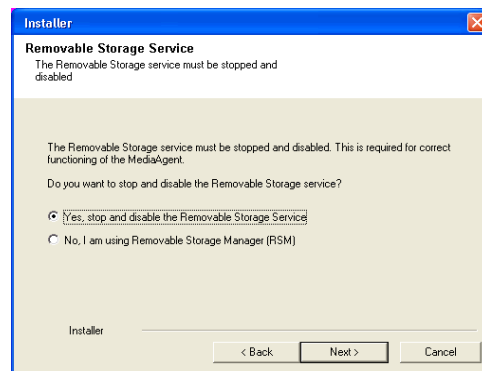


15. Select **Yes** to stop Removable Storage Services on the MediaAgent.
Click **Next**.

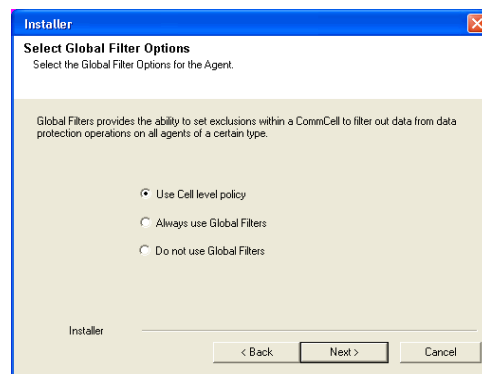
This prompt will not appear if Removable Storage Services are already disabled on the computer.



16. Click **Next**.



17. Select a **Storage Policy**.
Click **Next**.



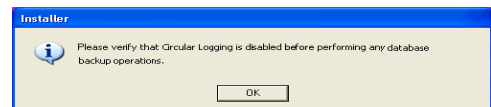
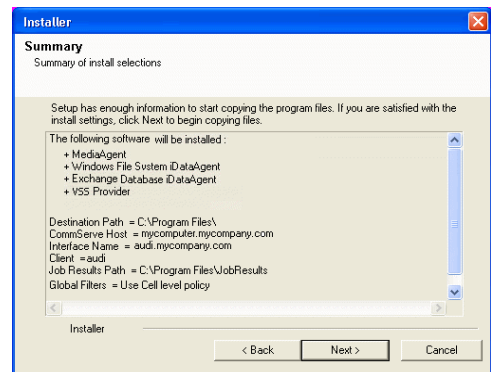
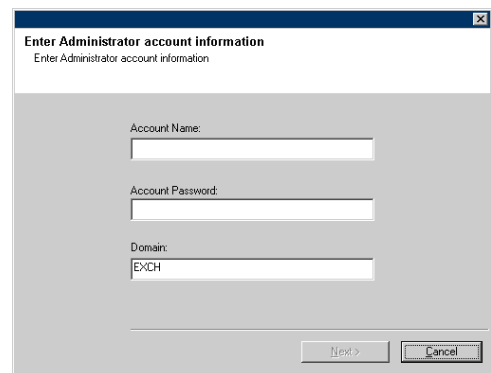
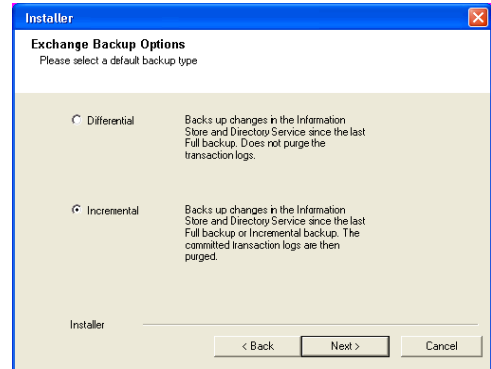
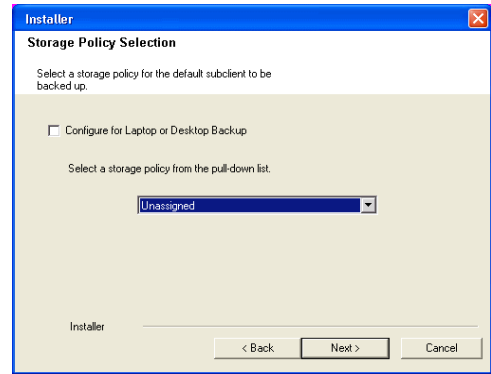
19. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.
 - **Differential** - Specifies that each non-full Exchange Database backup secures all data that has changed since the last full backup. Transaction logs are not purged.
 - **Incremental** - Specifies that each non-full Exchange Database backup secures only that data that has changed since the last backup of any type. Committed transaction logs are purged.

19. Enter the user credentials to access the Exchange Server to perform the backup operation.
 - The User Account must have Exchange Administrator privileges.
 - The installation detects the domain name. If necessary, you can modify the domain name by specifying Windows domain that the Exchange Server resides in.

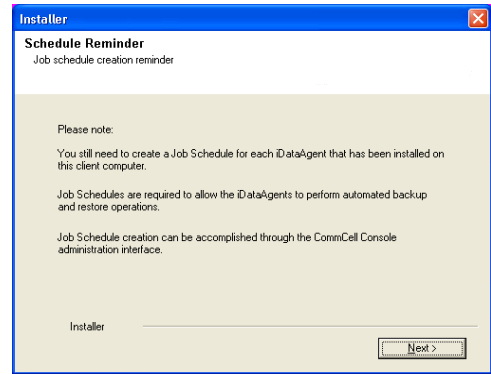
20. Click **Next**.

21. The install program displays a reminder to verify that Circular Logging is disabled before performing any database backup operations. To verify that Circular Logging is disabled:
 - From Exchange System Manager, navigate to and expand the server that the Database iDataAgent is being installed on.
 - Verify that the Circular Logging check box has not been selected for each Storage Group. If Circular Logging has been enabled for a Storage Group, disable it at this time.

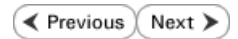
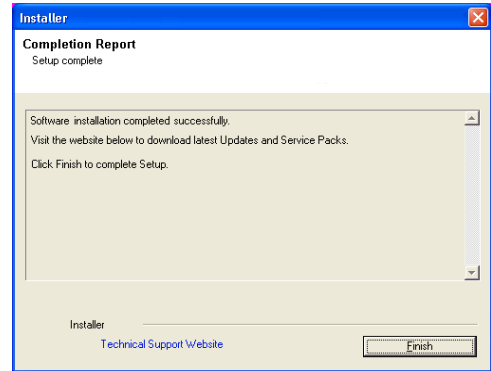
Click **OK**.



22. Click **Next**.



23. Click **Finish**.



Getting Started - Install the 64-bit Exchange Database Agent on Exchange Server 2007 - Clustered Environment

◀ Previous Next ▶

Follow the steps given below to install the 64-bit Exchange Database iDataAgent on Exchange Server 2007 in a clustered environment.

WHERE TO INSTALL

The Exchange Database iDataAgent can be installed directly onto the Exchange Server. This method is referred to as an on-host installation and is useful if you want to preserve hardware resources.

INSTALL THE EXCHANGE DATABASE iDATAAGENT

- Log on to the computer using an account with the following privileges:
 - Administrator of the local computer
 - Administrator of the Exchange Server
- Run **Setup.exe** from the Software Installation Package.
- Select the required language.
Click **Next**.

- Select the option to **Install Calypso on this 64-bit computer**.

NOTES:

- Your screen may look different from the example shown.

- Click **Next**.

- Click **OK**.

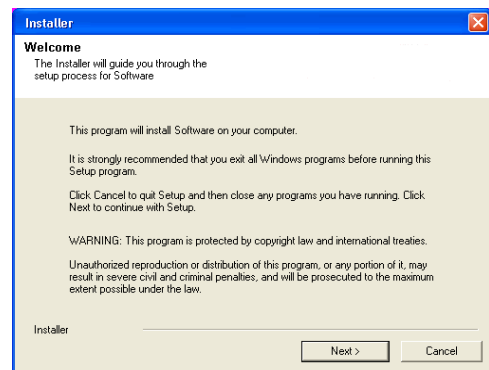
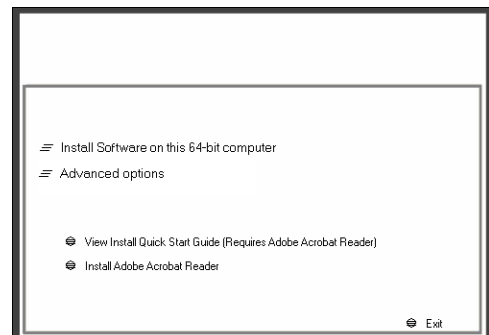
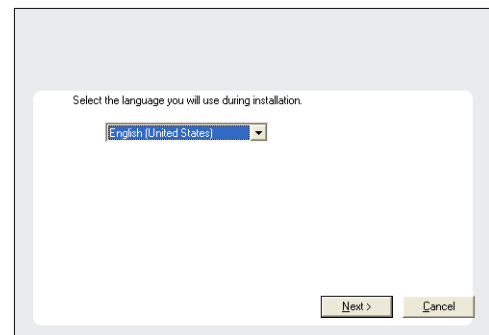
BEFORE YOU BEGIN

Download Software Packages

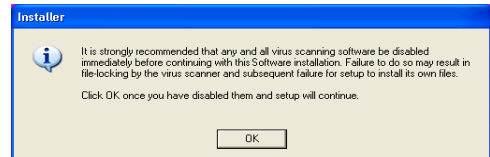
Download the latest software package to perform the install.

SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.



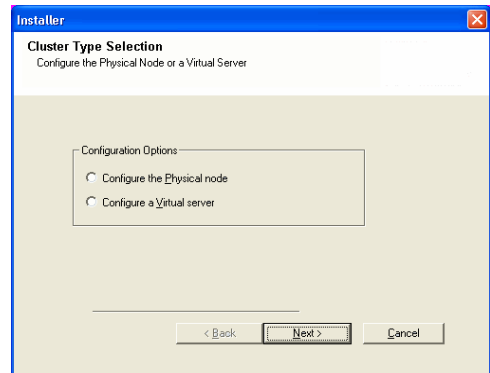
7. Select **I accept the terms in the license agreement**.
Click **Next**.



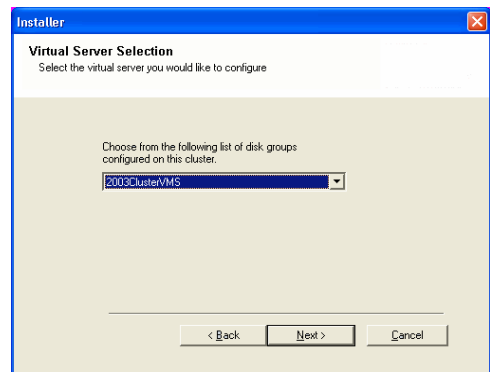
8. Select **Configure a Virtual Server**.
Click **Next**.



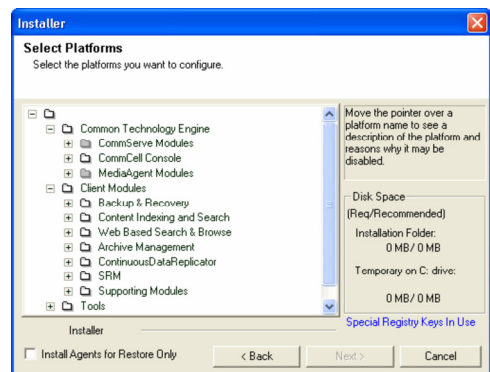
9. Select the disk group in which the virtual server resides.
Click **Next**.



10.
 - Expand **Client Modules | Backup & Recovery | Exchange**, and select **Exchange Database iDataAgent**.
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
 - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
 - Click **Next**.



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



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

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

12. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

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

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

13. Click **Next**.

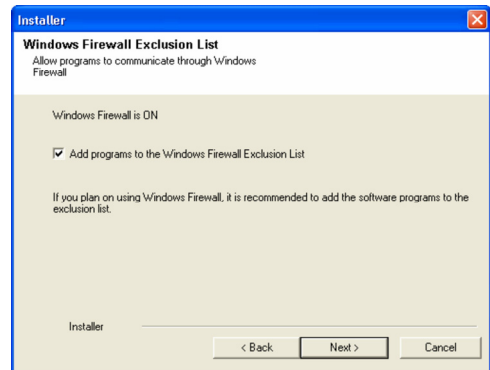
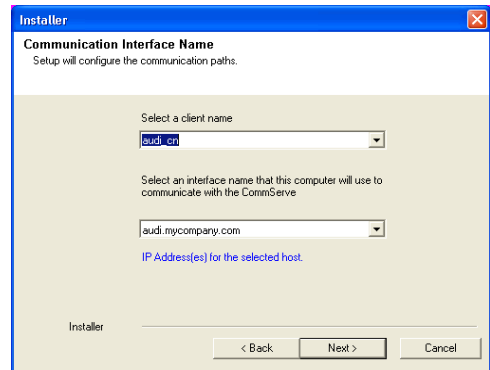
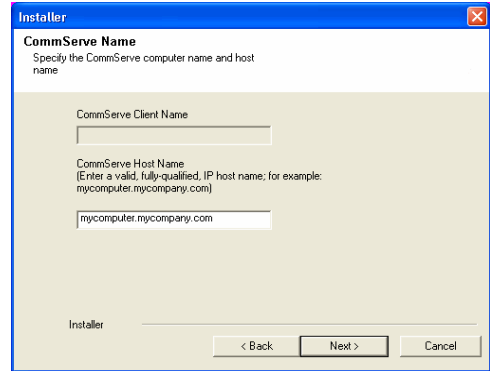
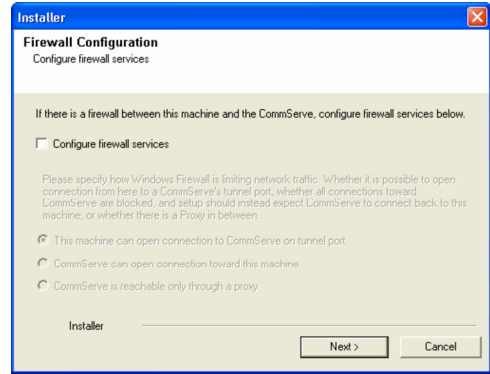
14. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

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

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

15. Click **Next**.



16. Verify the default location for software installation.

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

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

17. Select a Client Group from the list.

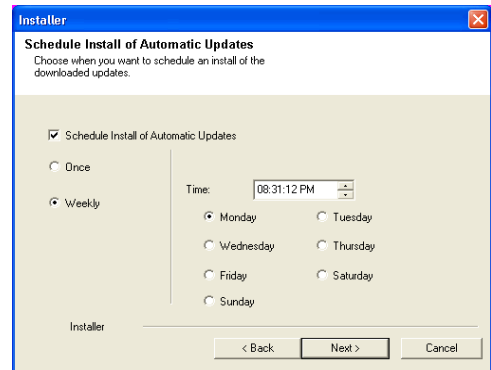
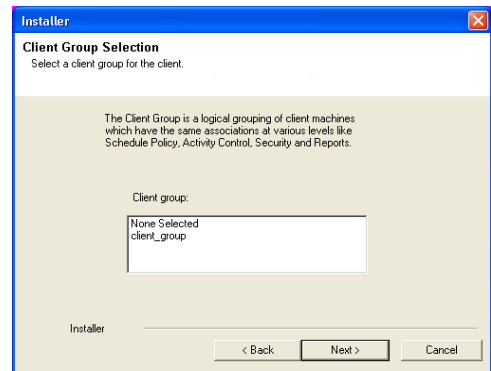
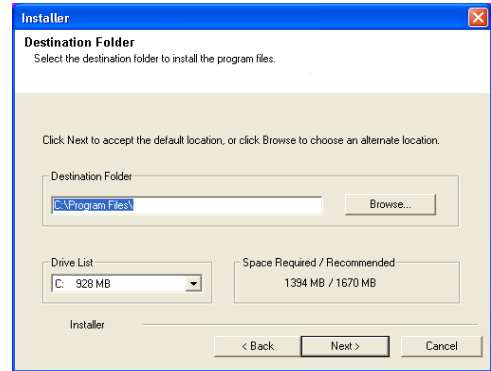
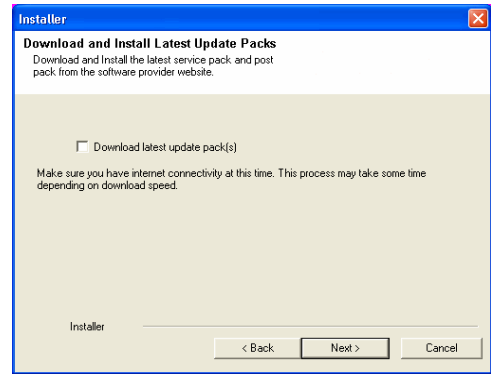
Click **Next**.

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

18. Click **Next**.

19. Select a **Storage Policy**.

Click **Next**.



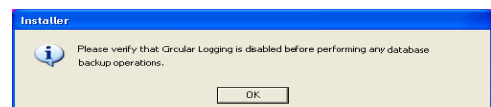
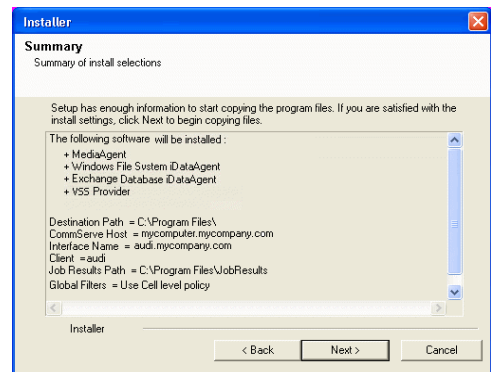
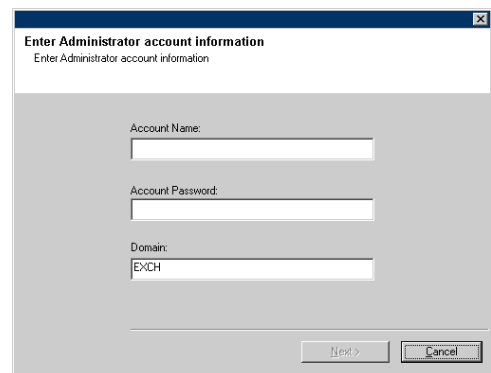
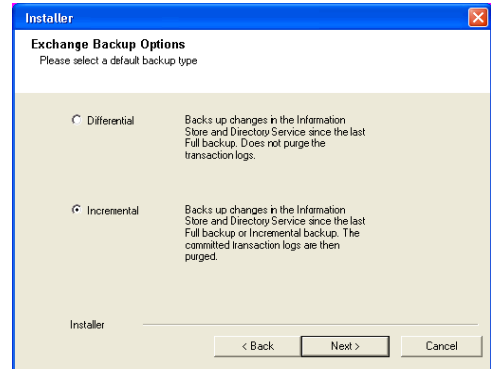
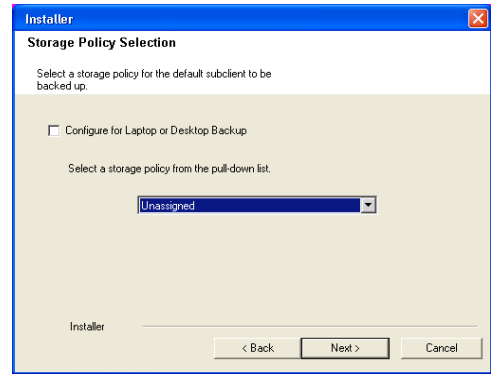
20. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.
- **Differential** - Specifies that each non-full Exchange Database backup secures all data that has changed since the last full backup. Transaction logs are not purged.
 - **Incremental** - Specifies that each non-full Exchange Database backup secures only that data that has changed since the last backup of any type. Committed transaction logs are purged.

21. Enter the user credentials to access the Exchange Server to perform the backup operation.
- The User Account must have Exchange Administrator privileges.
 - The installation detects the domain name. If necessary, you can modify the domain name by specifying Windows domain that the Exchange Server resides in.

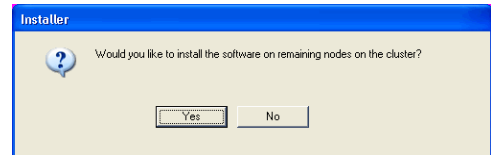
22. Click **Next**.

23. The install program displays a reminder to verify that Circular Logging is disabled before performing any database backup operations. To verify that Circular Logging is disabled:
- From Exchange System Manager, navigate to and expand the server that the Database iDataAgent is being installed on.
 - Verify that the Circular Logging check box has not been selected for each Storage Group. If Circular Logging has been enabled for a Storage Group, disable it at this time.

Click **OK**.

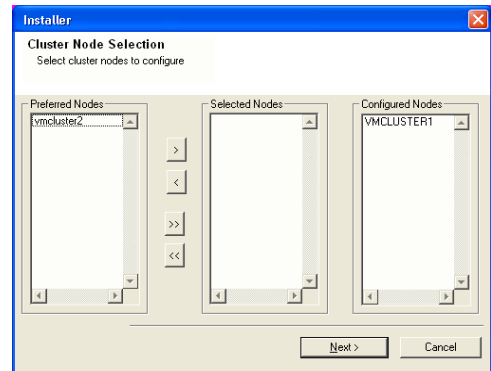


24. To install the software on the remaining nodes of the cluster, click **Yes**.
To complete the install for this node only, click **No**.



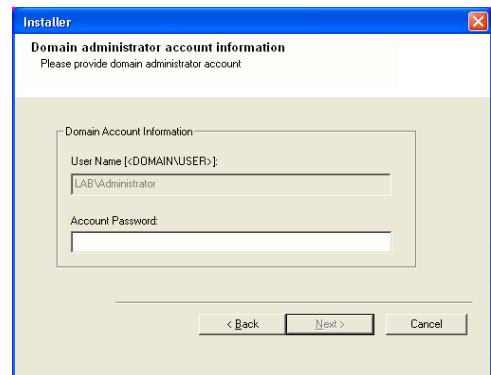
25. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.
Once you complete your selections, click **Next**.

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



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

Click **Next**.



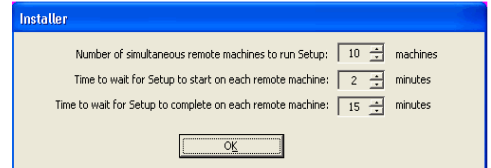
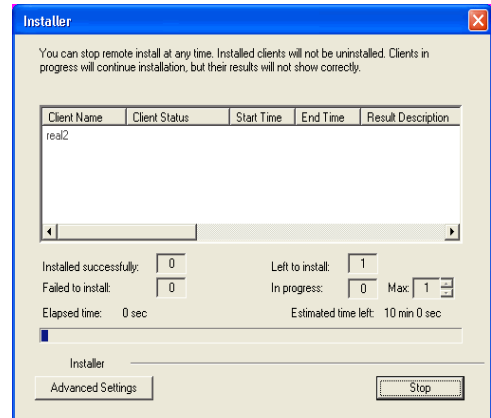
27. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

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.

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*.

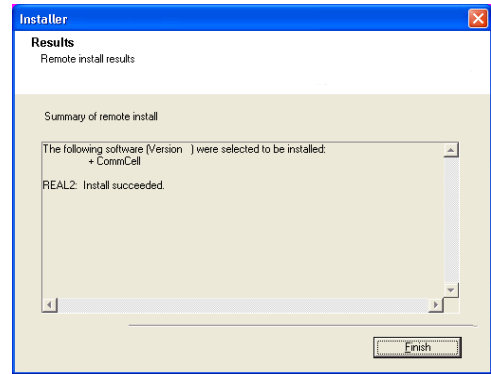


28. Read the summary for remote installation to verify that all selected nodes were installed successfully.

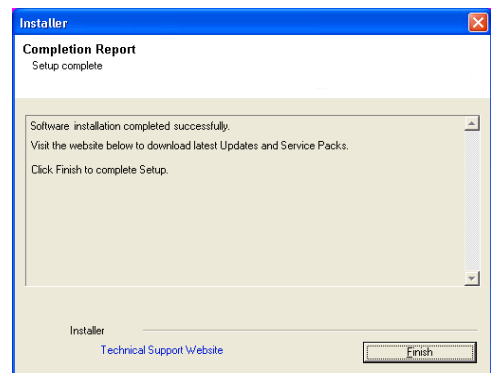
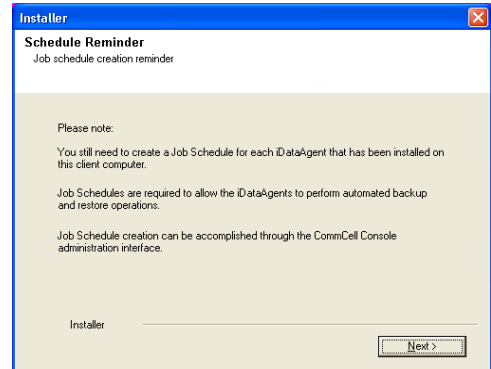
Click **Next**.

- 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.

29. Click **Next**.



30. Click **Finish**.



Getting Started - Install the Exchange Database Agent on Exchange Server 2003

◀ Previous Next ▶

Follow the steps given below to install the Exchange Database iDataAgent on Exchange Server 2003.

WHERE TO INSTALL

The Exchange Database iDataAgent can be installed directly onto the Exchange Server. This method is referred to as an on-host installation and is useful if you want to preserve hardware resources.

INSTALL THE EXCHANGE DATABASE iDATAAGENT

- Log on to the computer using an account with the following privileges:
 - Administrator of the local computer
 - Administrator of the Exchange Server
- Run **Setup.exe** from the Software Installation Package.
- Select the required language.
Click **Next**.

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

- Click **Next**.

- Click **OK**.

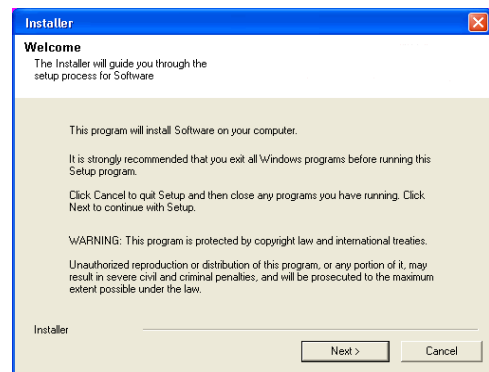
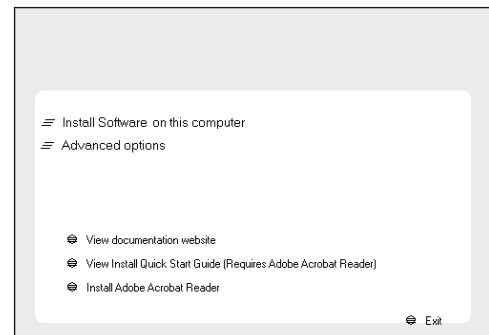
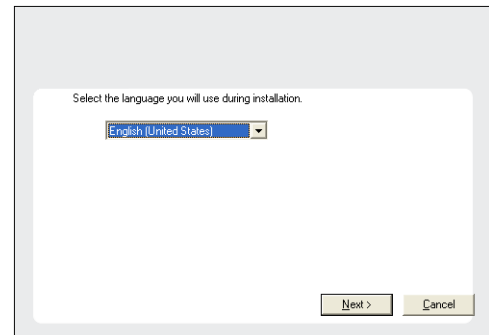
BEFORE YOU BEGIN

Download Software Packages

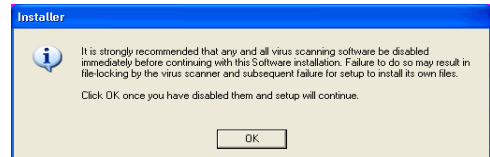
Download the latest software package to perform the install.

SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.



7. Select **I accept the terms in the license agreement**.
Click **Next**.



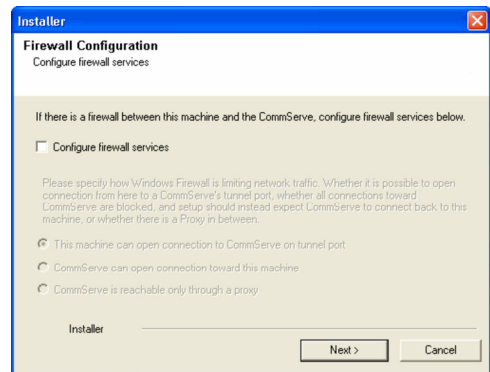
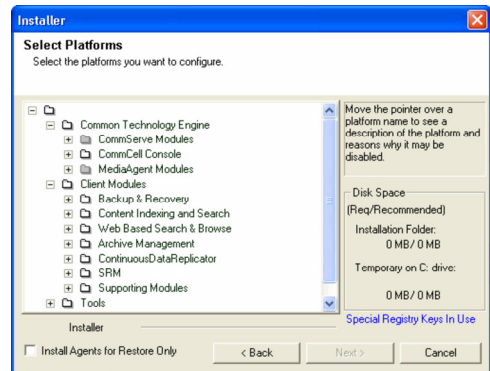
10.
 - Expand **Client Modules | Backup & Recovery | Exchange**, and select **Exchange Database /DataAgent**.
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
 - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
 - Click **Next**.



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

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

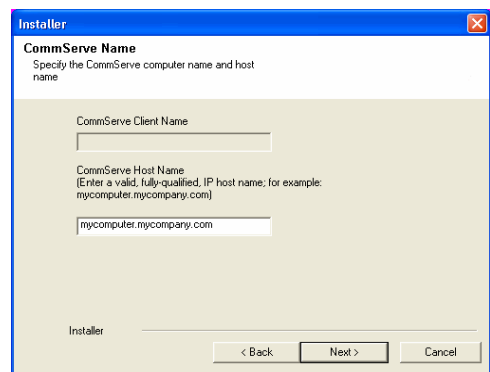
If firewall configuration is not required, click **Next**.



12. Enter the fully qualified domain name of the **CommServe Host Name**.
Click **Next**.

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

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



13. Click **Next**.

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

Click **Next**.

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

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

15. Click **Next**.

16. Verify the default location for software installation.

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

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

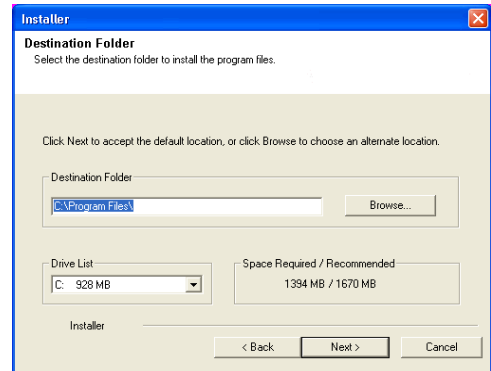
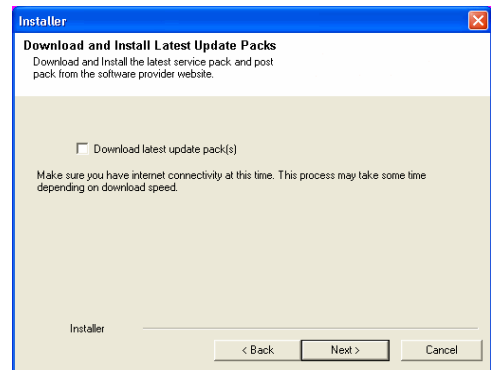
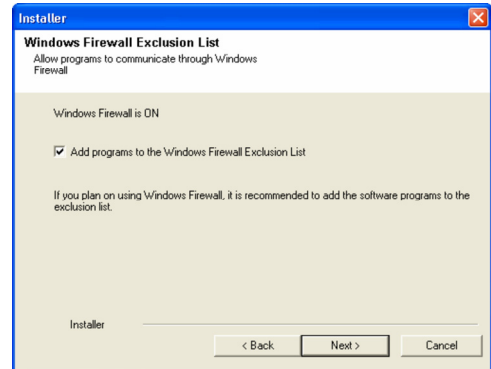
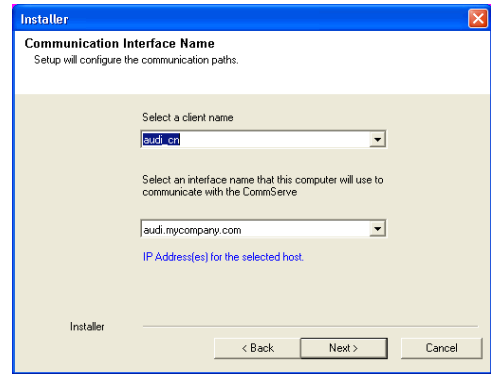
/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

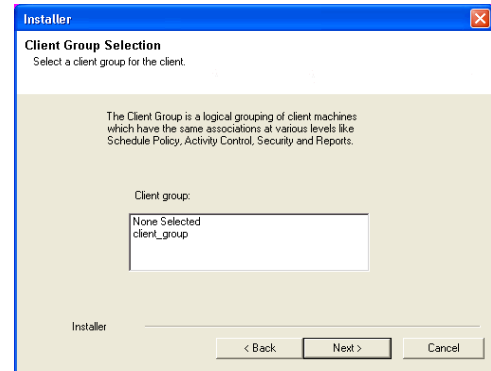
17. Select a Client Group from the list.

Click **Next**.

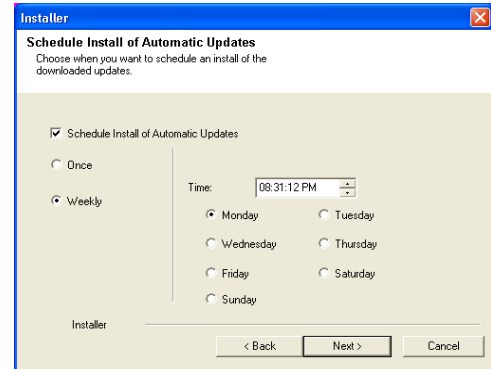
This screen will be displayed if Client Groups are configured in the CommCell Console.



18. Click **Next**.

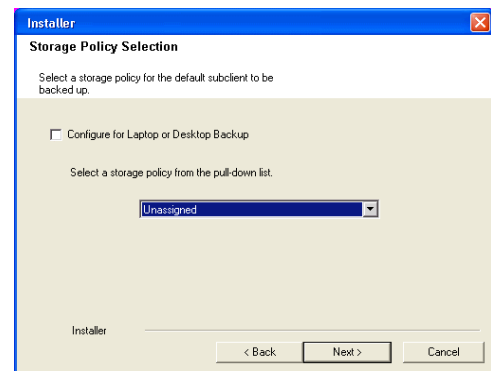


19. Select a **Storage Policy**.
Click **Next**.



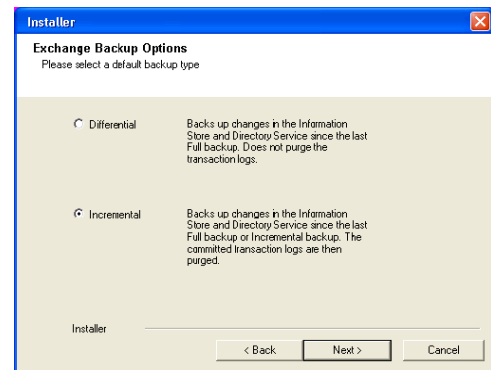
20. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.

- **Differential** - Specifies that each non-full Exchange Database backup secures all data that has changed since the last full backup. Transaction logs are not purged.
- **Incremental** - Specifies that each non-full Exchange Database backup secures only that data that has changed since the last backup of any type. Committed transaction logs are purged.

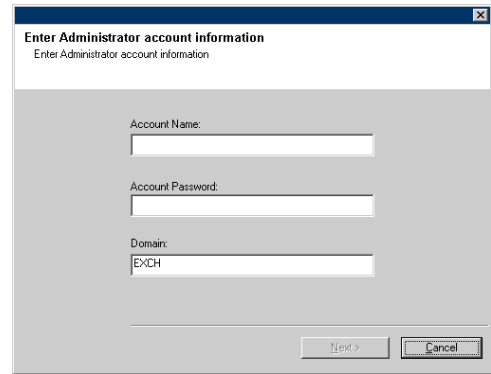


21. Enter the user credentials to access the Exchange Server to perform the backup operation.

- The User Account must have Exchange Administrator privileges.
- The installation detects the domain name. If necessary, you can modify the domain name by specifying Windows domain that the Exchange Server resides in.



22. Click **Next**.

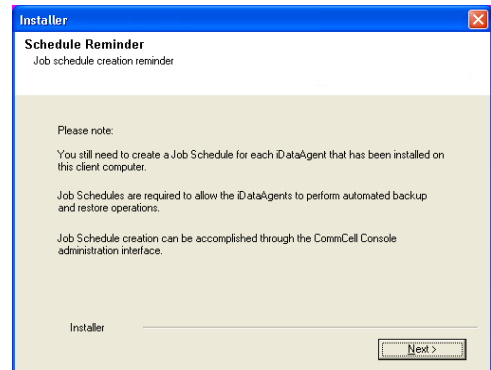
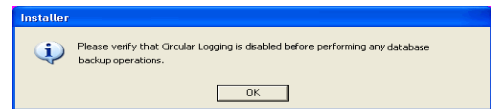
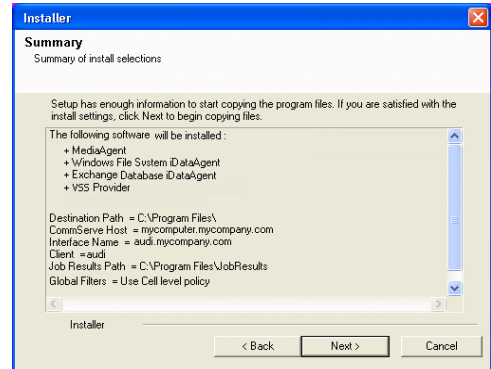


23. The install program displays a reminder to verify that Circular Logging is disabled before performing any database backup operations. To verify that Circular Logging is disabled:

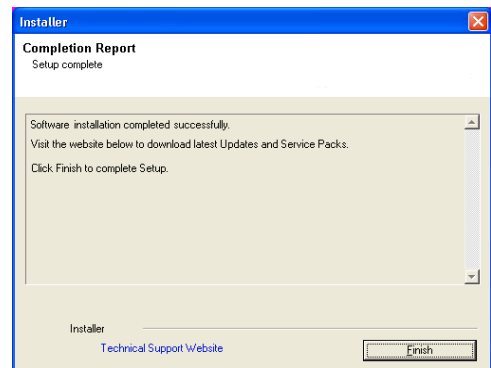
- From Exchange System Manager, navigate to and expand the server that the Database iDataAgent is being installed on.
- Verify that the Circular Logging check box has not been selected for each Storage Group. If Circular Logging has been enabled for a Storage Group, disable it at this time.

Click **OK**.

24. Click **Next**.



25. Click **Finish**.



Getting Started - Install the Exchange Database Agent on Exchange Server 2003 - Clustered Environment

◀ Previous Next ▶

Follow the steps given below to install the Exchange Database iDataAgent on Exchange Server 2003 in a clustered environment.

WHERE TO INSTALL

The Exchange Database iDataAgent can be installed directly onto the Exchange Server. This method is referred to as an on-host installation and is useful if you want to preserve hardware resources.

INSTALL THE EXCHANGE DATABASE iDATAAGENT

1. Log on to the computer using an account with the following privileges:
 - Administrator of the local computer
 - Administrator of the Exchange Server
2. Run **Setup.exe** from the Software Installation Package.
3. Select the required language.
Click **Next**.

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

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

5. Click **Next**.

6. Click **OK**.

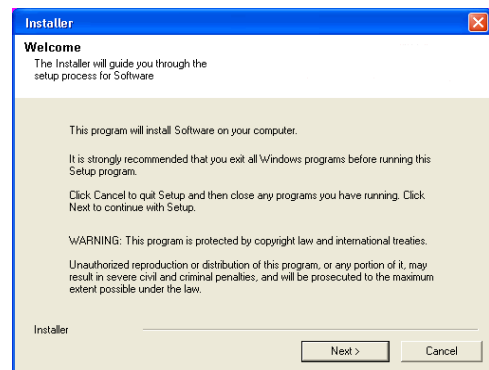
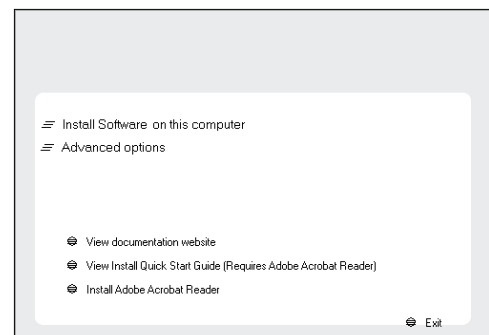
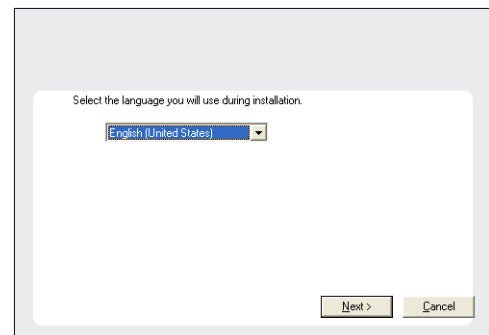
BEFORE YOU BEGIN

Download Software Packages

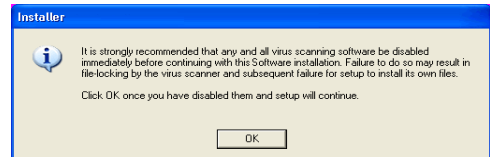
Download the latest software package to perform the install.

SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.



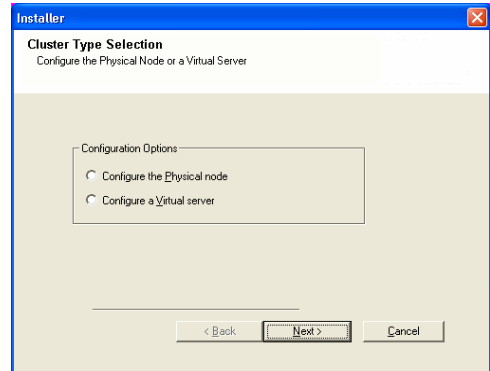
7. Select **I accept the terms in the license agreement**.
Click **Next**.



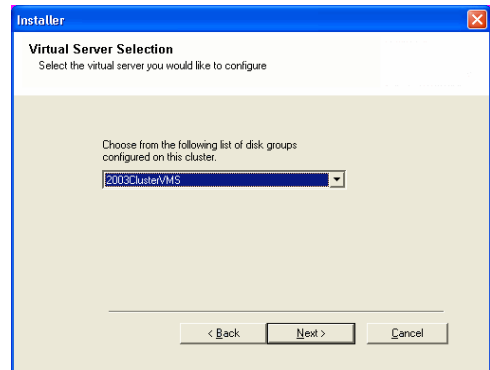
8. Select **Configure a Virtual Server**.
Click **Next**.



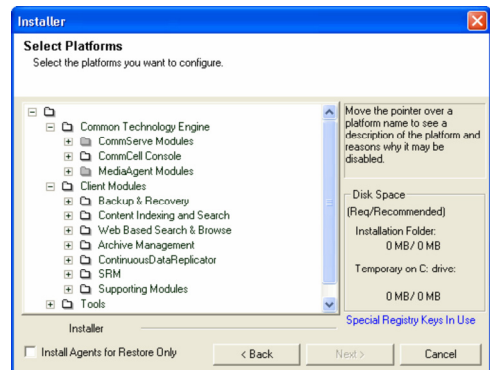
9. Select the disk group in which the virtual server resides.
Click **Next**.



10.
 - Expand **Client Modules | Backup & Recovery | Exchange**, and select **Exchange Database iDataAgent**.
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
 - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
 - Click **Next**.



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



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

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

12. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

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

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

13. Click **Next**.

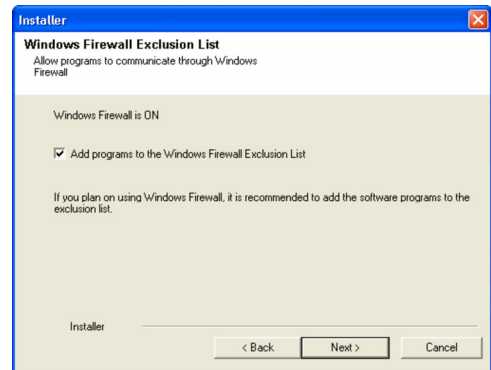
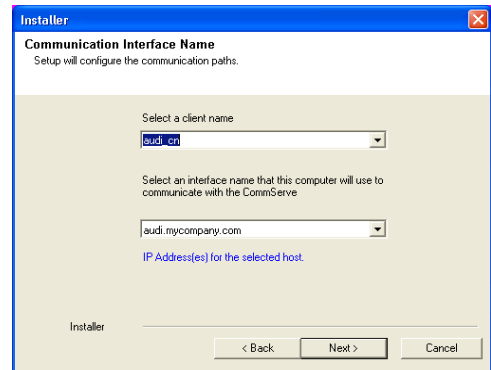
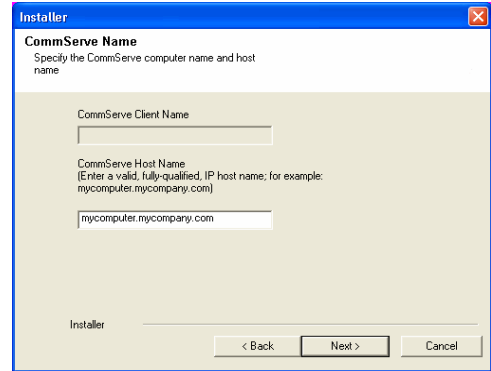
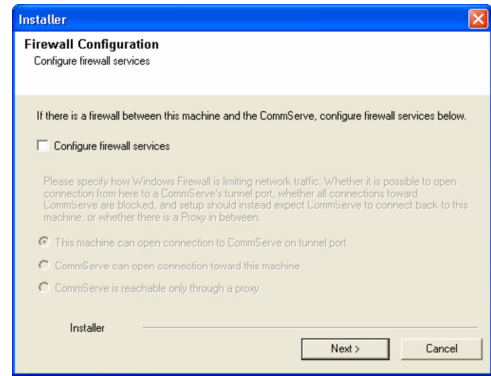
14. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

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

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

15. Click **Next**.



16. Verify the default location for software installation.

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

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

17. Select a Client Group from the list.

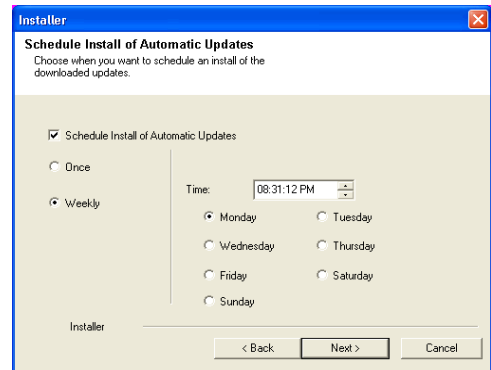
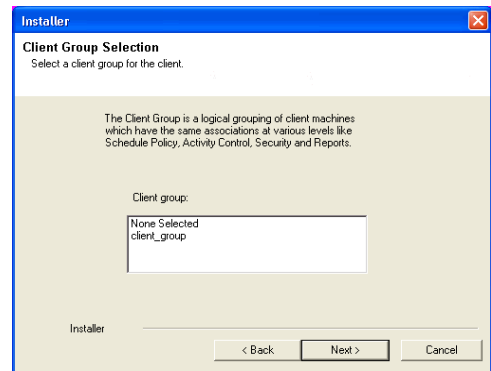
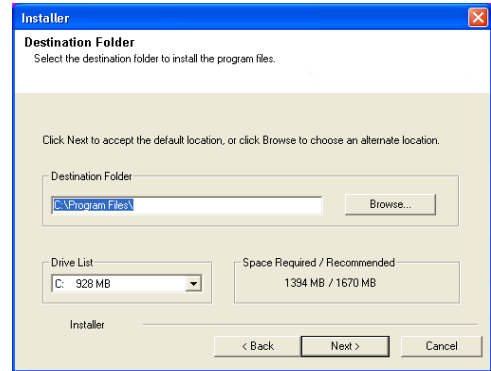
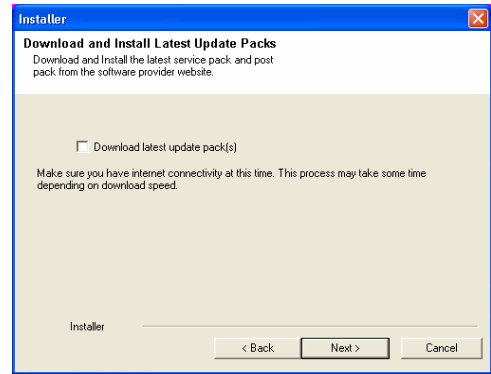
Click **Next**.

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

18. Click **Next**.

19. Select a **Storage Policy**.

Click **Next**.



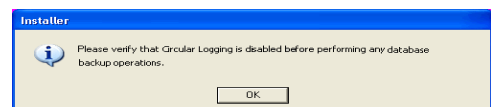
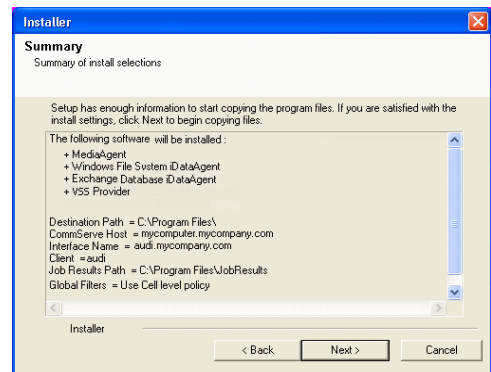
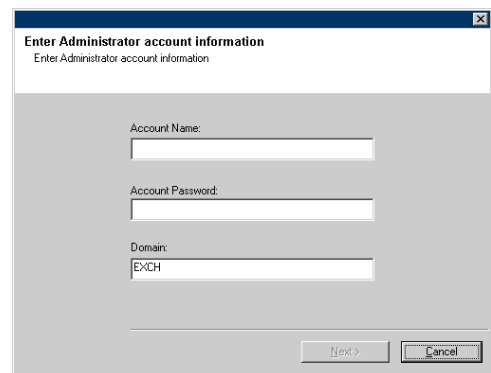
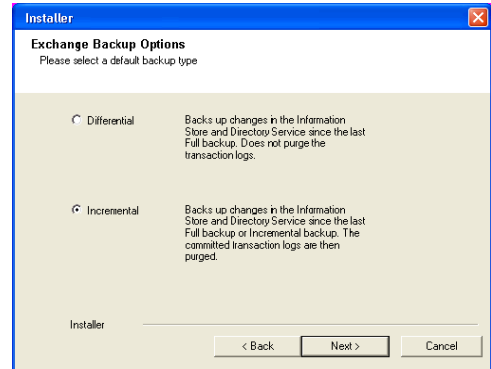
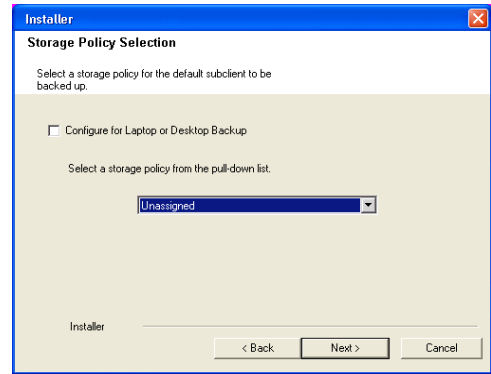
20. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.
- **Differential** - Specifies that each non-full Exchange Database backup secures all data that has changed since the last full backup. Transaction logs are not purged.
 - **Incremental** - Specifies that each non-full Exchange Database backup secures only that data that has changed since the last backup of any type. Committed transaction logs are purged.

21. Enter the user credentials to access the Exchange Server to perform the backup operation.
- The User Account must have Exchange Administrator privileges.
 - The installation detects the domain name. If necessary, you can modify the domain name by specifying Windows domain that the Exchange Server resides in.

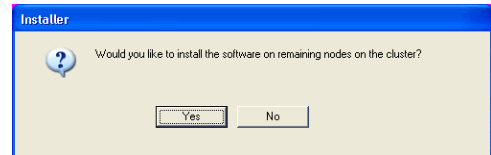
22. Click **Next**.

23. The install program displays a reminder to verify that Circular Logging is disabled before performing any database backup operations. To verify that Circular Logging is disabled:
- From Exchange System Manager, navigate to and expand the server that the Database iDataAgent is being installed on.
 - Verify that the Circular Logging check box has not been selected for each Storage Group. If Circular Logging has been enabled for a Storage Group, disable it at this time.

Click **OK**.

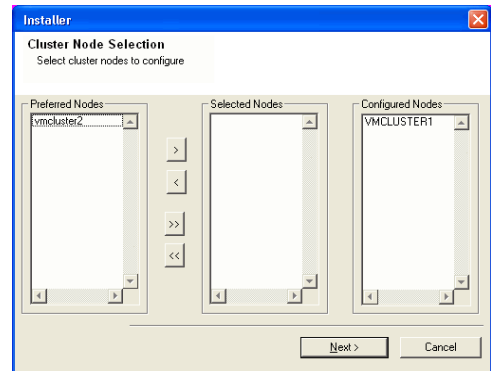


24. To install the software on the remaining nodes of the cluster, click **Yes**.
To complete the install for this node only, click **No**.



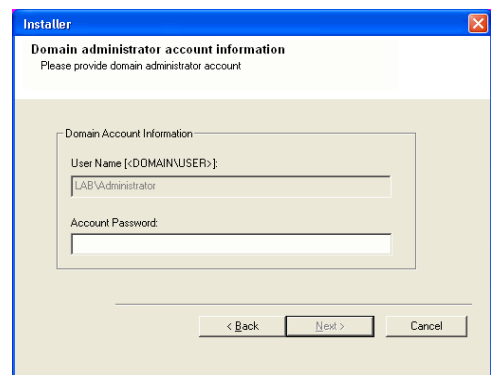
25. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.
Once you complete your selections, click **Next**.

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



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

Click **Next**.



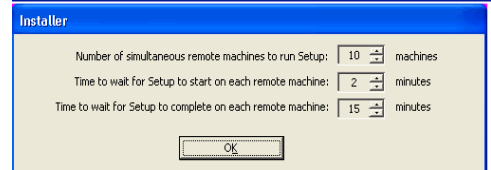
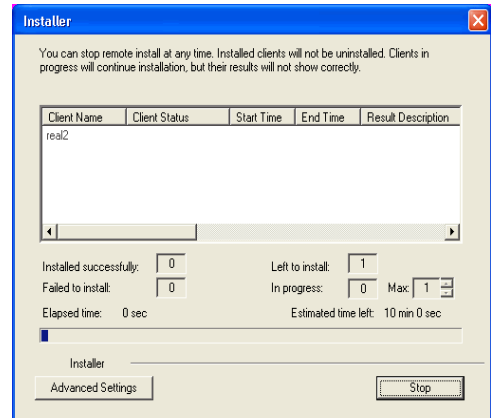
27. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

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.

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*.

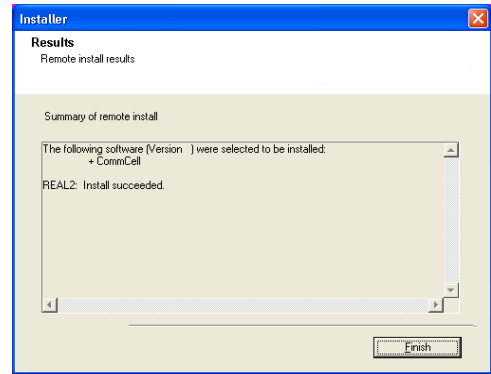


28. Read the summary for remote installation to verify that all selected nodes were installed successfully.

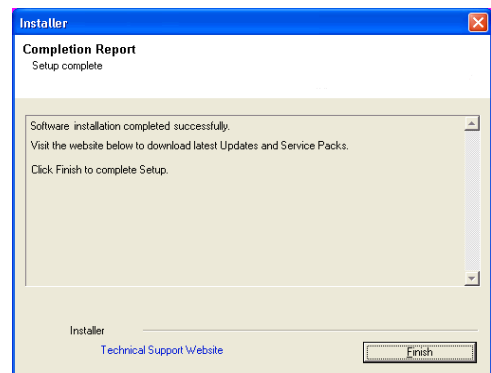
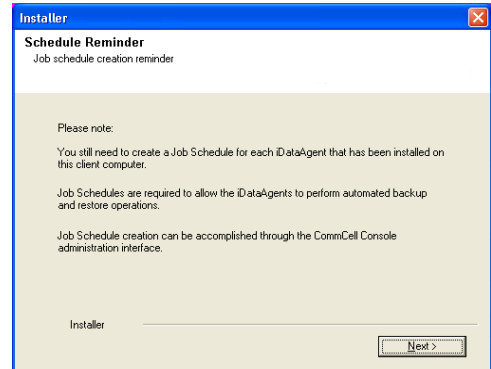
Click **Next**.

- 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.

29. Click **Next**.



30. Click **Finish**.



Getting Started - Microsoft Exchange Database Configuration

< Previous Next >

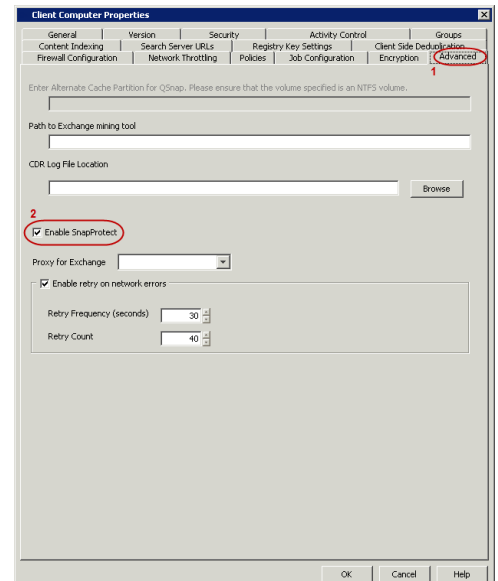
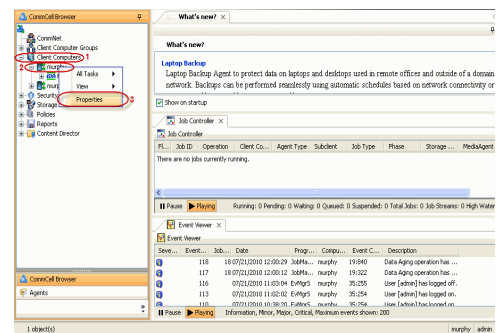
PRE-REQUISITES

- When using a proxy configuration, installation of the Exchange management tools on the proxy is required. Also, ensure that the version of the management tools is the same as the version of the Exchange server.
- When performing Integrity Check on Exchange 2010 DAG subclients, it is required to use a proxy. You can use one of the following as the proxy:
 - DAG member server
 - Separate computer with connectivity to the Exchange Server and with the ability to mount the snapshots
- Prior to performing a SnapProtect backup, ensure that all the available hotfixes for Virtual Disk Service (VDS) and VSS are applied.
- When performing SnapProtect backup for a Windows Cluster, a proxy server must be used for performing backup and restore operations.
- SnapProtect backup on Windows supports basic disks.

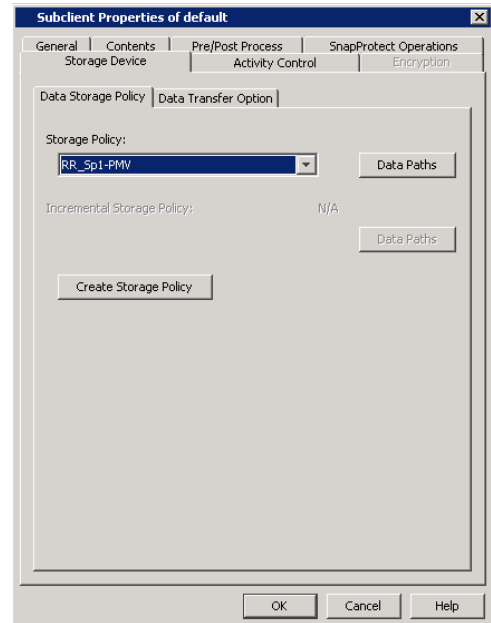
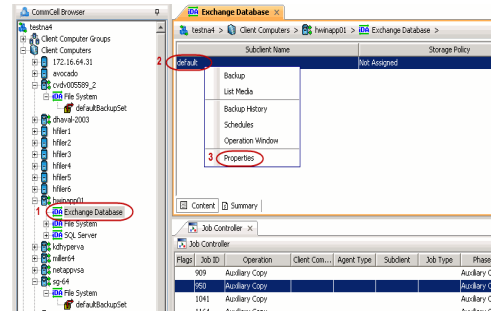
CONFIGURATION

Once installed, the Microsoft Exchange Database iDataAgent requires some additional configuration before running your first SnapProtect backup. Follow the steps given below to complete the configuration for this Agent.

- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.
- Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.
- From the CommCell Browser, navigate to **<Client>** | **Exchange Database**.
 - Right-click the subclient in the right pane and click **Properties**.



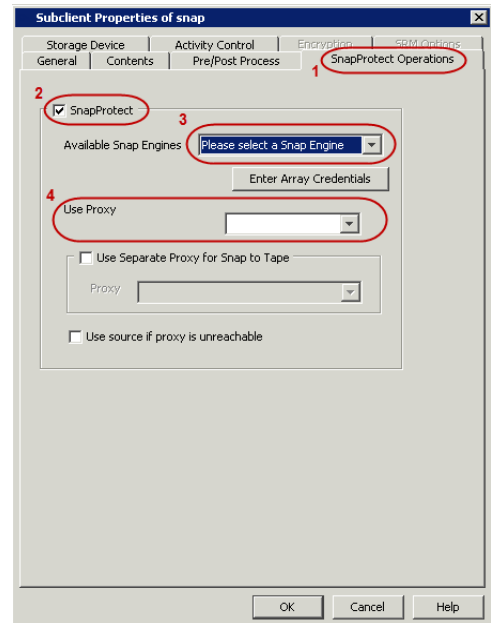
4.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.



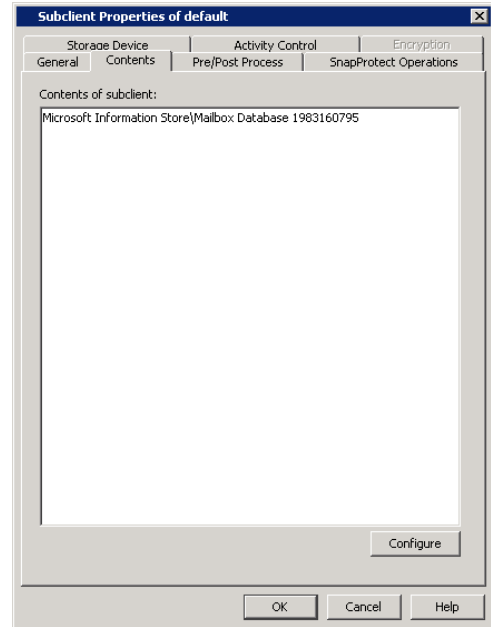
5.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy operations will be performed.

When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent. Select the MediaAgent from the **Proxy** list.



6.
 - Click the **Content** tab.
 - Click **Configure** to add or modify the content for the subclient.
 - Click **OK**.



SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

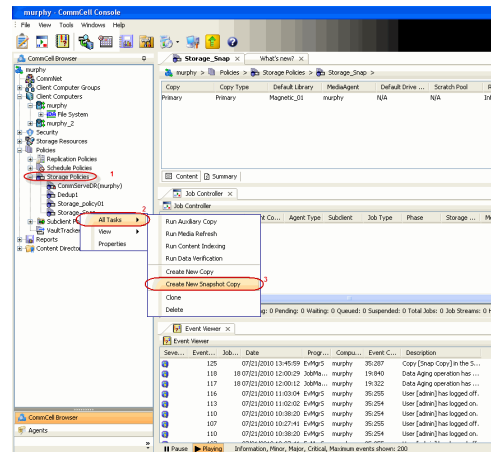
Click **Next** to Continue.

CREATE A SNAPSHOT COPY

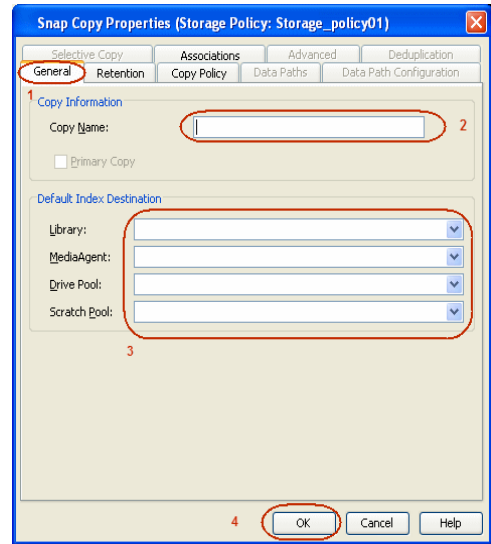


Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.



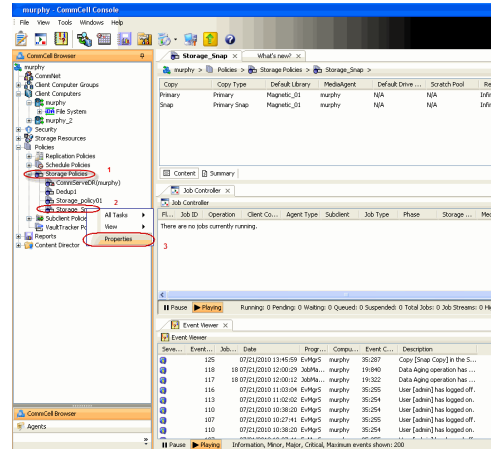
2.
 - Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



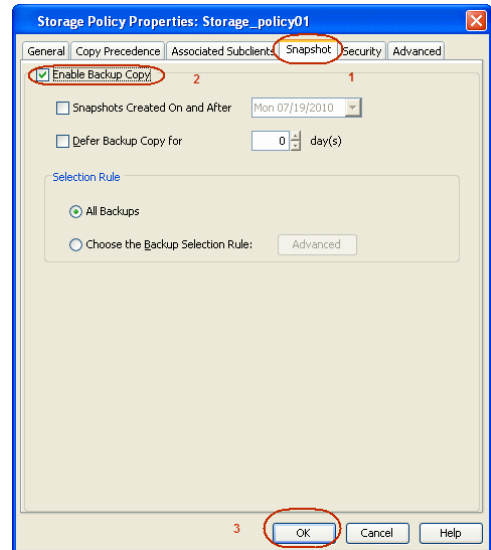
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



- Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



Storage Array Configuration

◀ Previous Next ▶

CHOOSE THE STORAGE ARRAY

HARDWARE STORAGE ARRAYS	SOFTWARE STORAGE ARRAY
3PAR	DATA REPLICATOR
DELL COMPELLENT	
DELL EQUALLOGIC	
EMC CLARIION, VNX	
EMC SYMMETRIX	
FUJITSU ETERNUS DX	
HITACHI DATA SYSTEMS	
HP EVA	
IBM SVC	
IBM XIV	
LSI	
NETAPP	
NETAPP WITH SNAPVAULT/SNAPMIRROR	
NIMBLE	

◀ Previous Next ▶

SnapProtect™ Backup - 3PAR

◀ Previous Next ▶

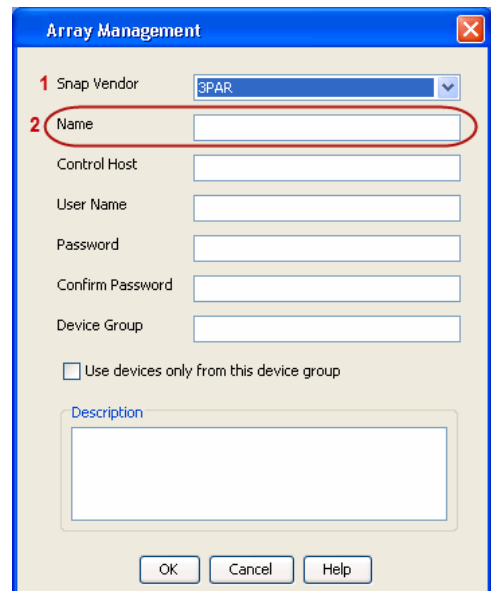
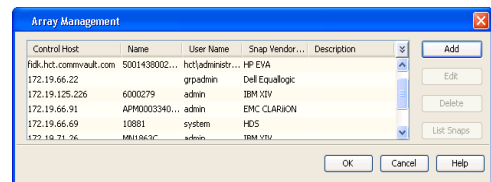
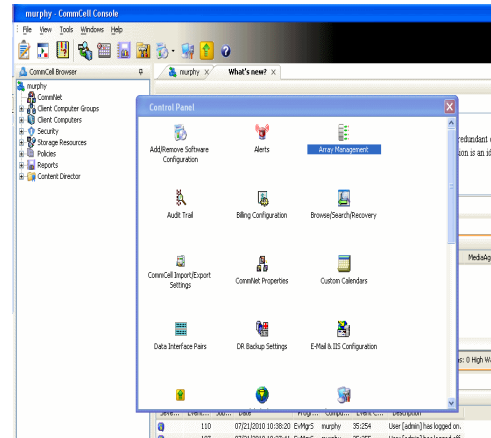
PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
 - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

where $\text{DevID.substr}(12,4)$ is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(12,4)$ is 0B95

After adding all the values, the resulting array name is 2FF70002AC00B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

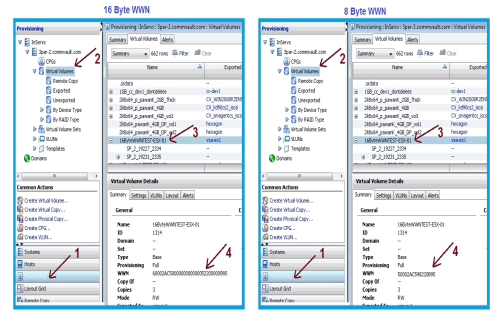
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(26,6)$ is 000B95

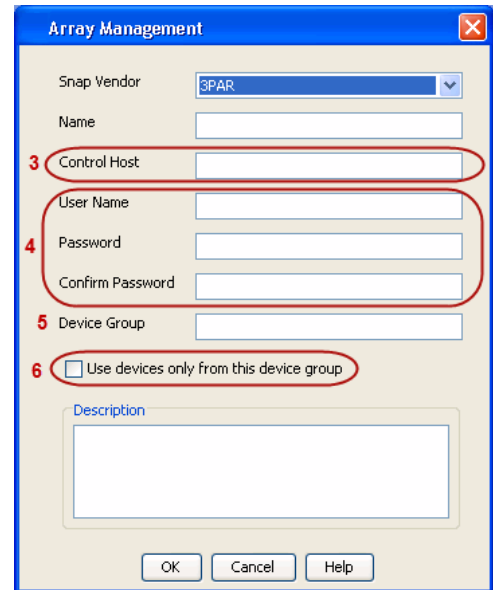
After adding all the values, the resulting array name is 2FF70002AC000B95.



- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - Dell Compellent

◀ Previous Next ▶

PRE-REQUISITIES

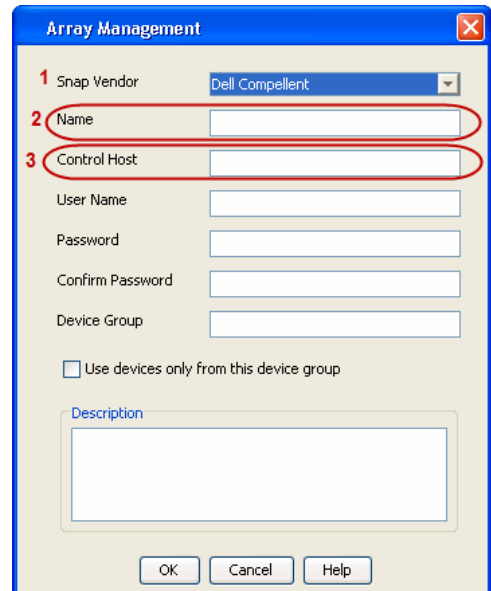
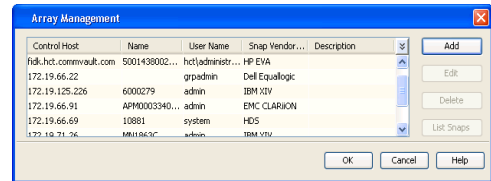
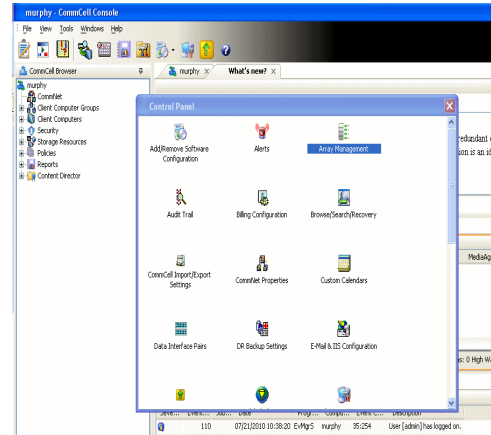
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

SETUP THE ARRAY INFORMATION

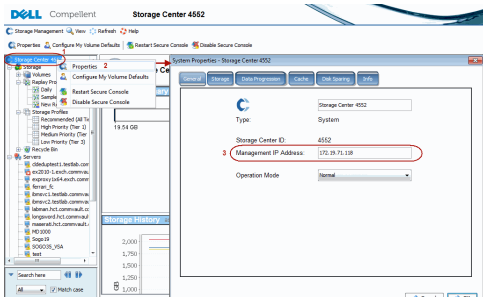
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **Dell Compellent** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** and **Control Host** fields.

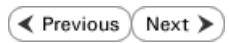
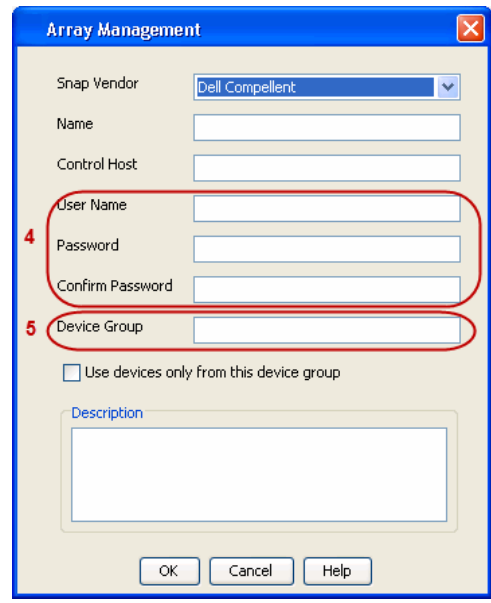
The Management IP address is also referred as the Storage Center IP address.



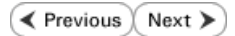
For reference purposes, the screenshot on the right shows the Storage Center Management Console of the Dell Compellent storage device displaying the Management IP address.



- 4.
- Enter the user access information of the application administrator in the **Username** and **Password** fields.
 - In the **Device Group** field, type *none* as this array does not use device groups for snapshot operations.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - Dell EqualLogic



PRE-REQUISITIES

WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

FIRMWARE VERSION

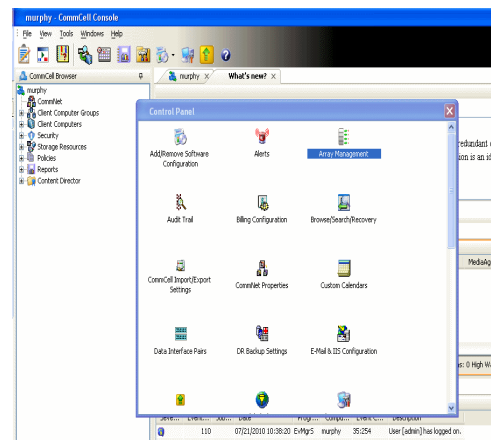
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

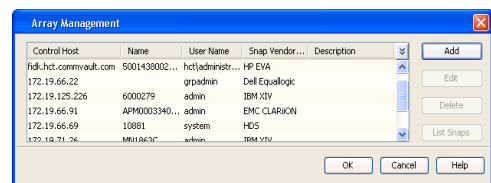
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



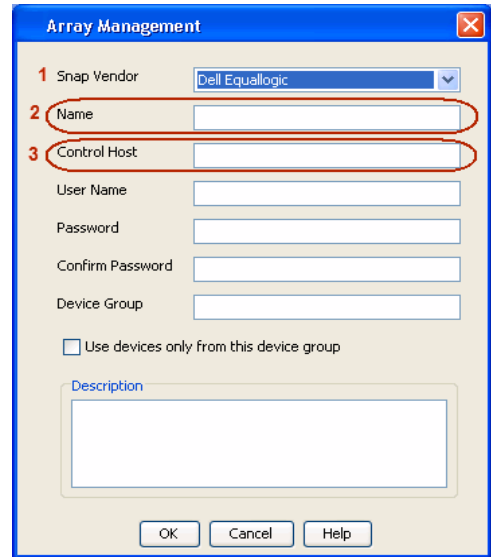
2. Click **Add**.



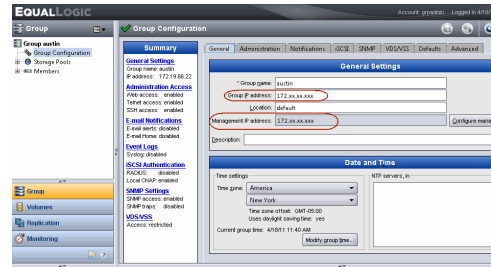
3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

No entry is required in the **Name** field if there is no Management IP address configured.

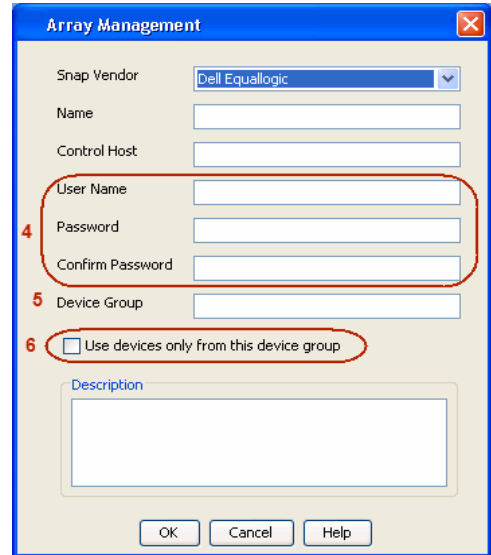
- Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
 - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
 - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
 - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous Next ▶

PRE-REQUISITES

LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

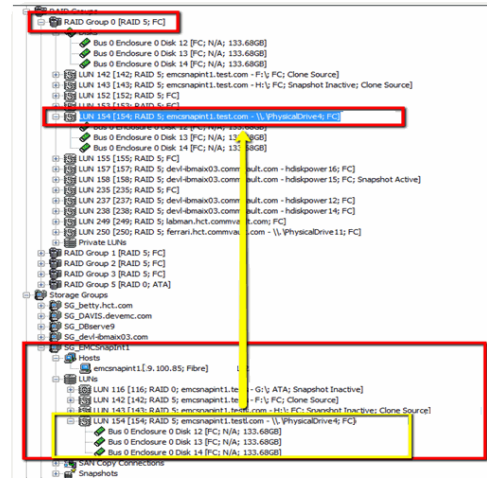
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

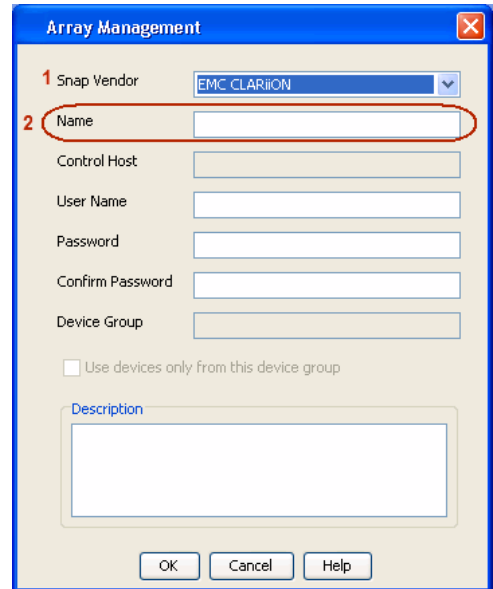
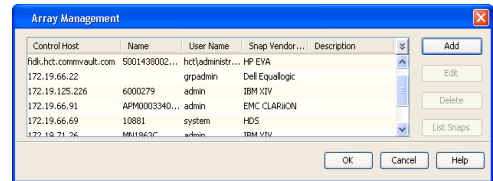
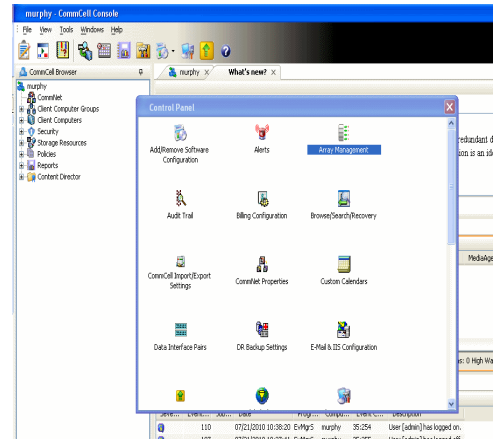
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

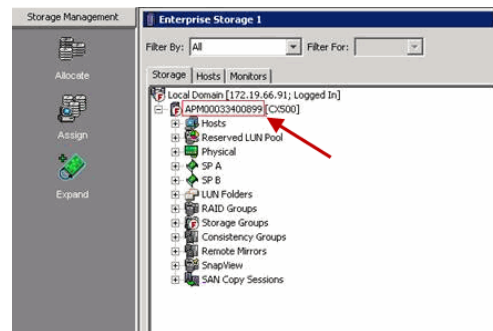
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
 - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.



- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

Array Management [Close]

Snap Vendor:

Name:

Control Host:

User Name:

3 Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - EMC Symmetrix

◀ Previous Next ▶

PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

LOAD THE SYMMETRIX DATABASE

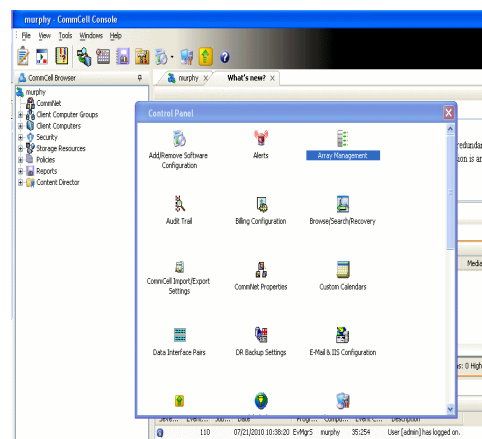
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

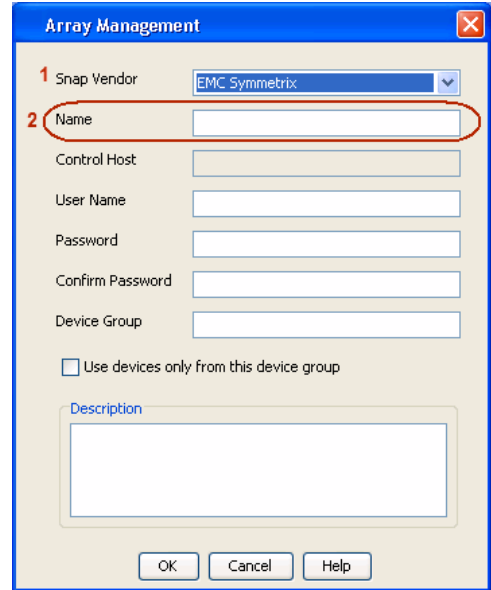
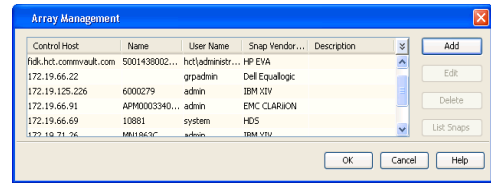
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

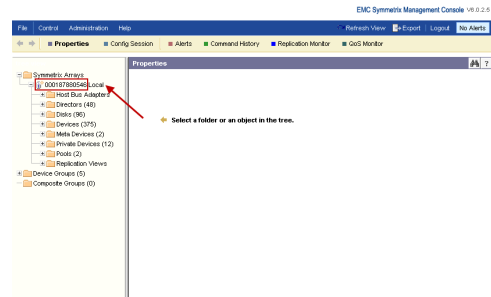


2. Click **Add**.

3.
 - Select **EMC Symmetrix** from the **Snap Vendor** list.
 - Specify the **Symm ID** of the array in the **Name** field.

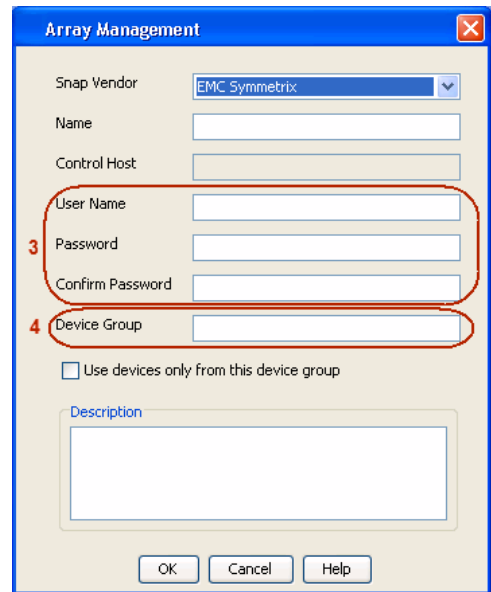


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.
If you do not specify a device group, the default device group will be used for snapshot operations.
 - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).



SnapProtect™ Backup - Fujitsu ETERNUS DX

◀ Previous Next ▶

PRE-REQUISITES

- Local Copy license for Snap and Clone.
- Thin Provisioning license.
- Ensure that all members in the Fujitsu array are running firmware version V10L22-1000 or higher.
- Enable SMI-S on the storage array.
- Create a Host Affinity group for the proxy computer.
- If using SnapOPC, ensure to create a SDV and SDPV volumes.

CONFIGURE DESTINATION VOLUMES

- Source and destination volumes should be pre-paired before performing any snapshot operation. For EC snapshots (clone), pre-paired sessions should be in active state.
- To pre-pair source and destination volumes, install the ETERNUS SF Express Manager software version 14.2A or higher.
- Forbid Advanced Copy and Encrypted volumes are not supported.
- Depending on the type of snapshot being used, review the following for the creation of destination volumes:

FOR SNAP SNAPSHOTS

If pre-paired sessions are not available, SnapOPC snapshots use any available SDV volumes as their destination volumes. If you need to create a new SDV volume, ensure that the SDV volume is of equal size to the source volume.

FOR CLONE SNAPSHOTS

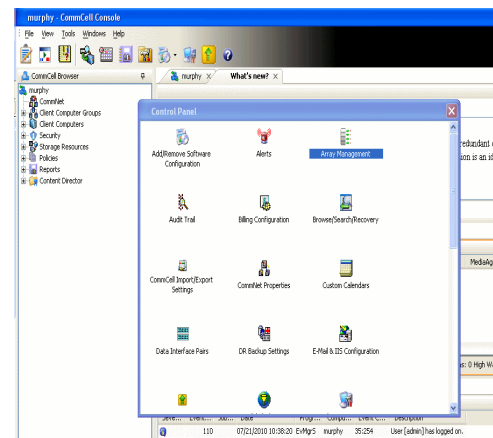
If pre-paired sessions are not available, destination volumes are automatically created for clone snapshots. If a non-existing device group is specified during array configuration in the CommCell Console, a destination volume is created based on the source volume type. However, if a valid device group is specified, the following destination volumes are created depending on the device group type:

- A Thin Provisioning volume is created if the device group is a Thin Provisioning pool.
- A standalone volume is created if the device group is a RAID group.

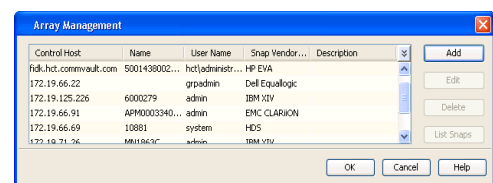
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

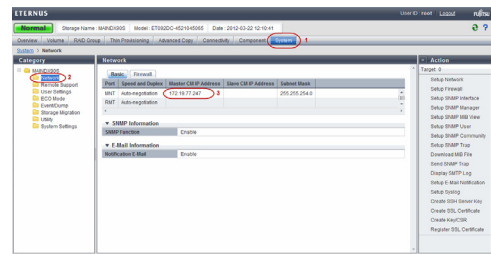
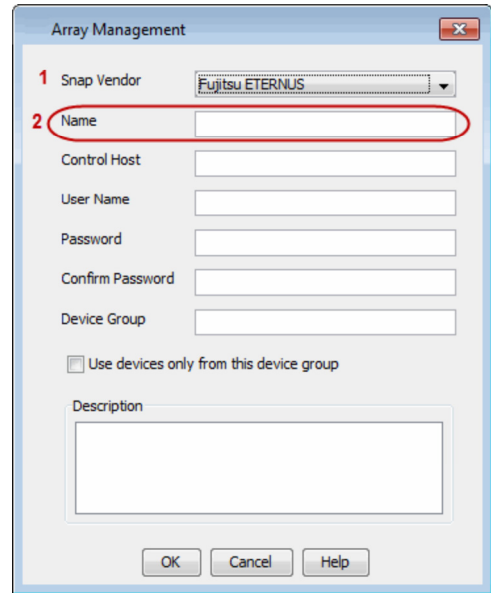


2. Click **Add**.

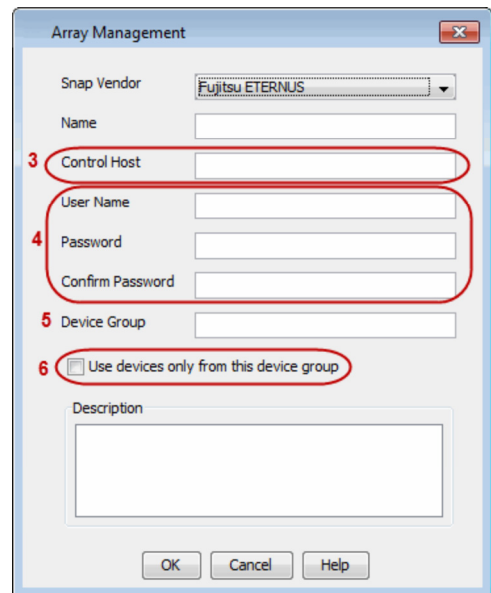


3.
 - Select **Fujitsu ETERNUS** from the **Snap Vendor** list.
 - Specify the CM IP Address of the array in the **Name** field.

For reference purposes, the screenshot on the right shows the CM IP Address for the Fujitsu storage device.



4.
 - Enter the CM IP Address of the array in the **Control Host** field.
 - Enter the access information of a user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the RAID group or Thin Provisioning group created on the array to be used for clone operations. Device groups are not applicable for Snap snapshots.
 - Select the **Use devices only from this device group** option to use only the snapshot devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - Hitachi Data Systems

◀ Previous Next ▶

PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
 - COW pools
 - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

ADDITIONAL REQUIREMENTS FOR VMWARE

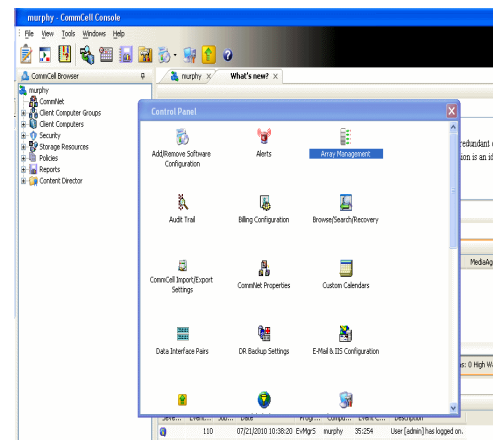
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server *iDataAgent* client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server *iDataAgent* client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

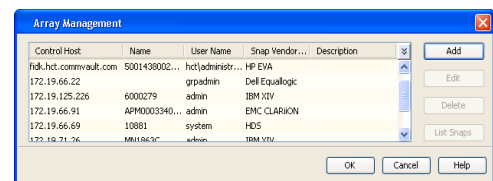
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

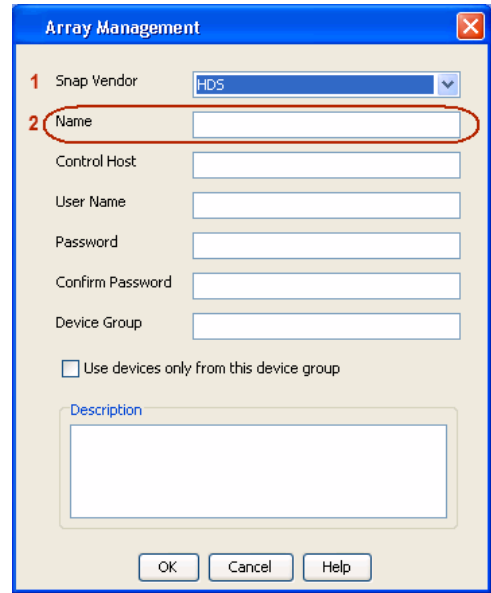
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



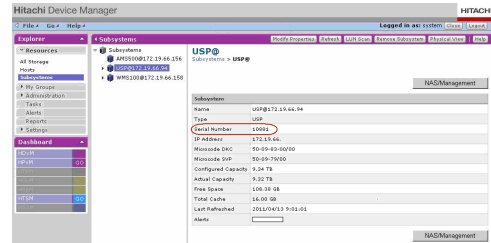
2. Click **Add**.



3.
 - Select **HDS** from the **Snap Vendor** list.
 - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



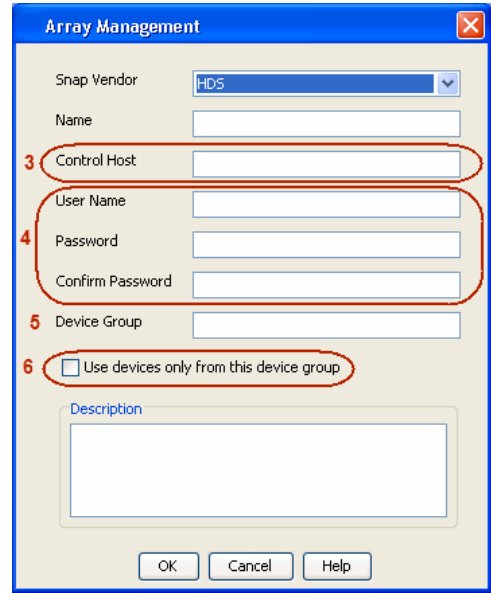
4.
 - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:

<COW_POOL_ID>-<LABEL> or <LABEL>-<COW_POOL_ID>

where <COW_POOL_ID> (for COW job) should be a number. This parameter is required.

<LABEL> (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - HP StorageWorks EVA

◀ Previous Next ▶

SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

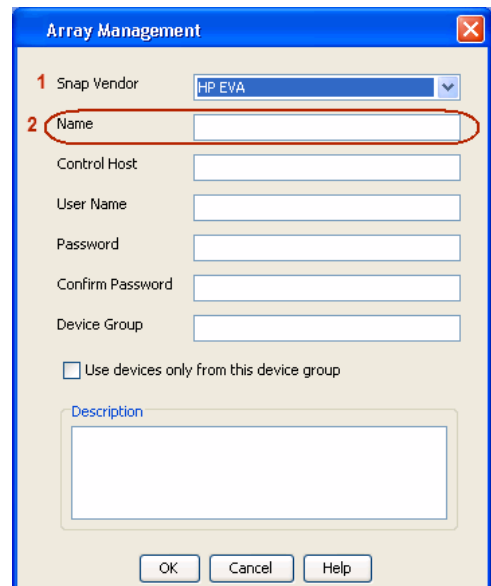
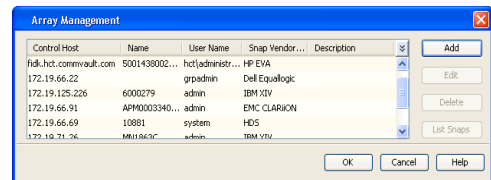
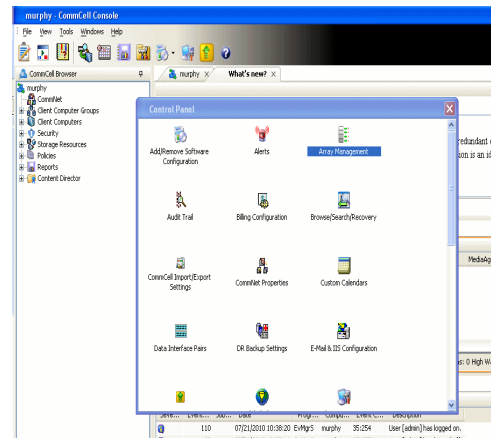
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin folder to discover the HP-EVA arrays.
3. Use the CLIRefreshTool.bat tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin folder.

SETUP THE ARRAY INFORMATION

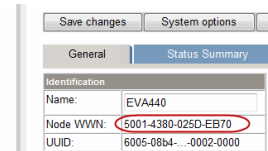
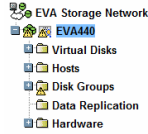
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
2. Click **Add**.
3.
 - Select **HP EVA** from the **Snap Vendor** list.
 - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

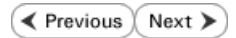
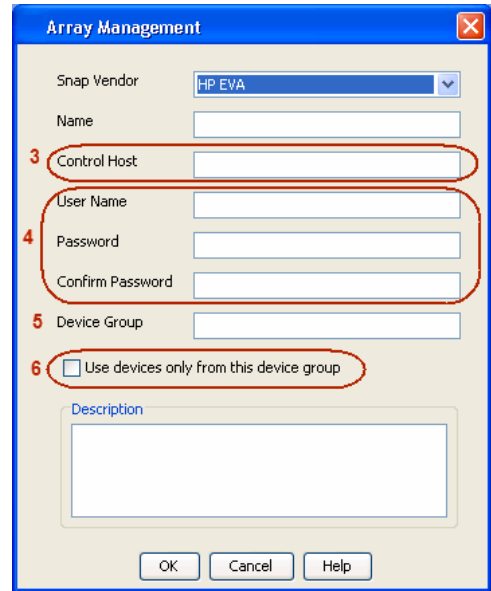
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



- 4. Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous Next ▶

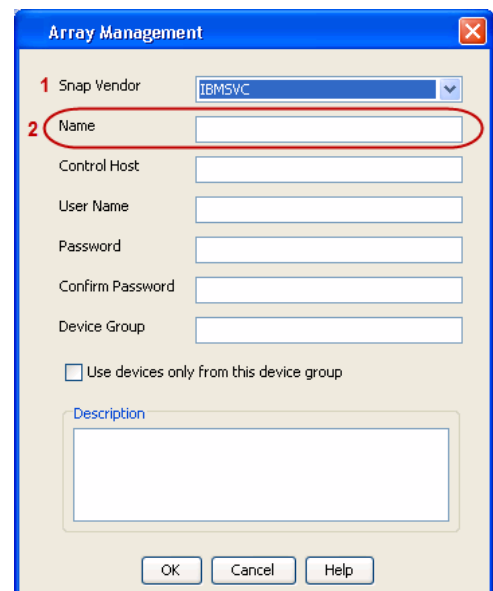
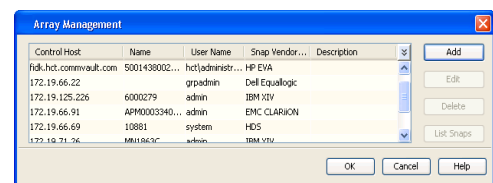
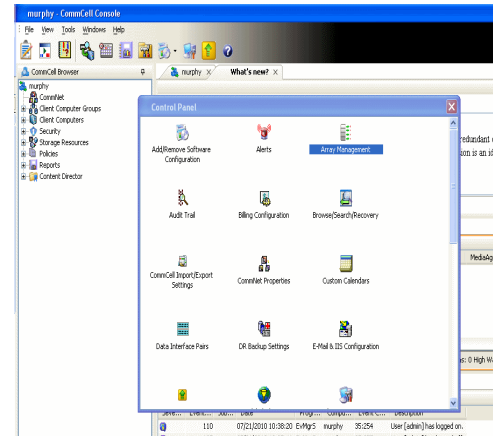
PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

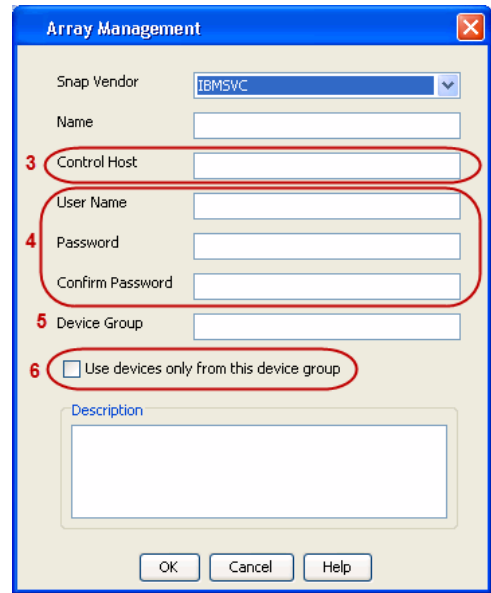
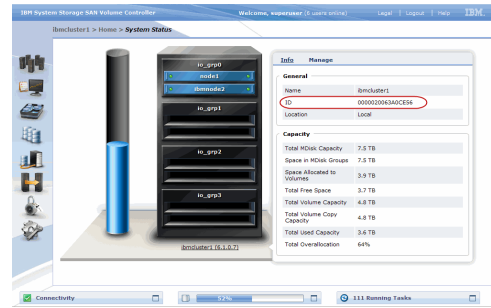
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



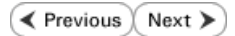
The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM XIV



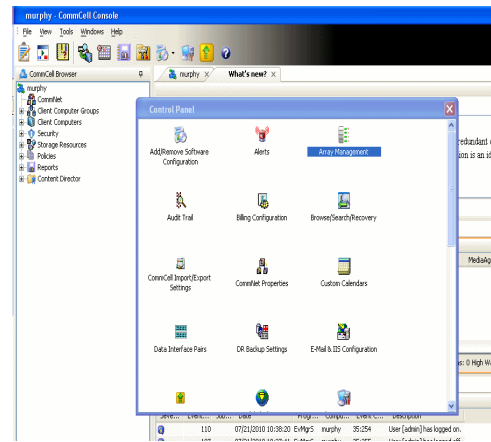
PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

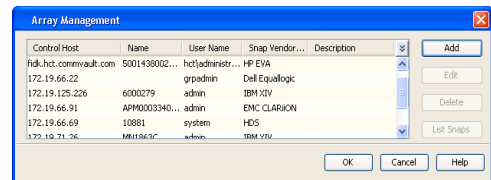
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

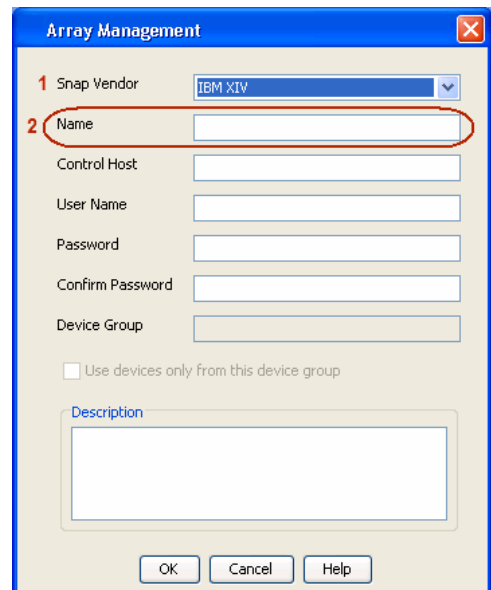
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

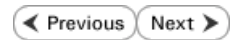
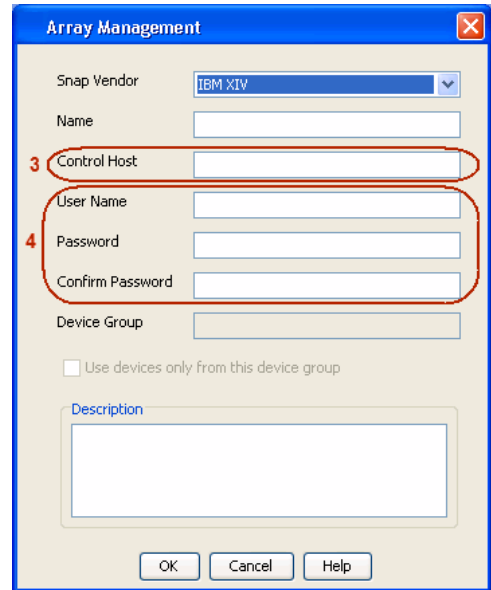
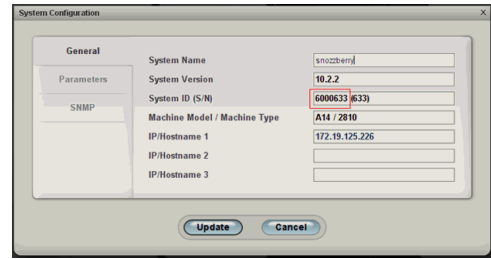


3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

- 4.
- Enter the IP address or host name of the array in the **Control Host** field.
 - Enter the user access information of the application administrator in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - LSI

◀ Previous Next ▶

PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
 - SMIS server through TCP/IP network.
 - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

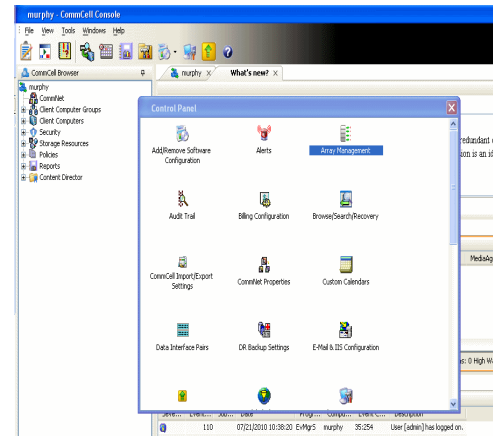
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

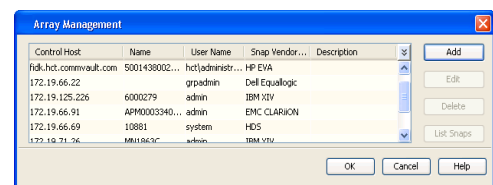
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

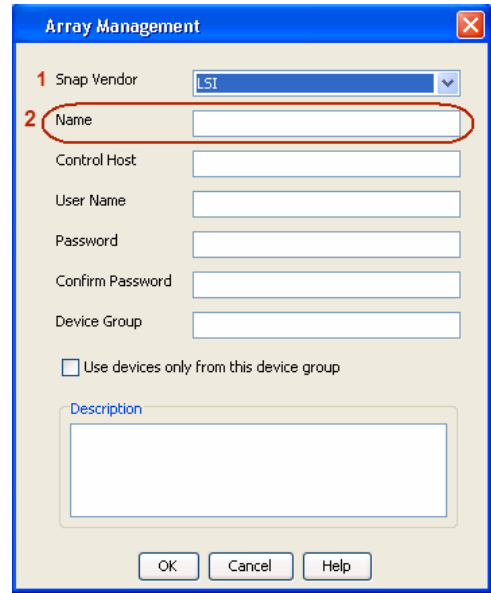
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

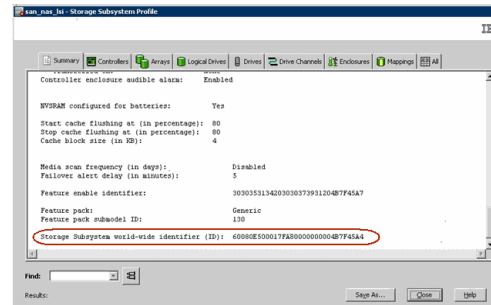


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

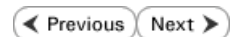
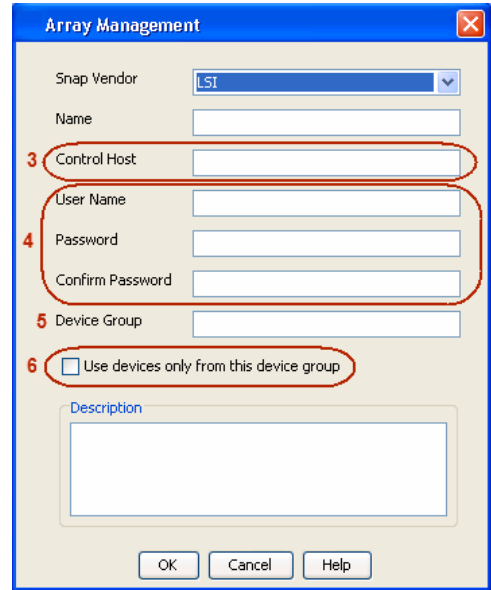
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



4.
 - Specify the name of the device manager server where the array was configured in the **Control Host** field.
 - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

If you specify None in the **Device Group** field but do not have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - NetApp

PREREQUISITES

LICENSES

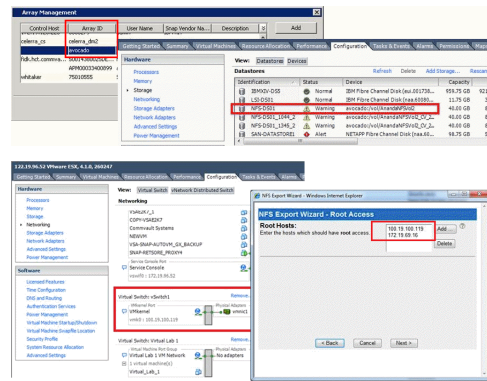
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.

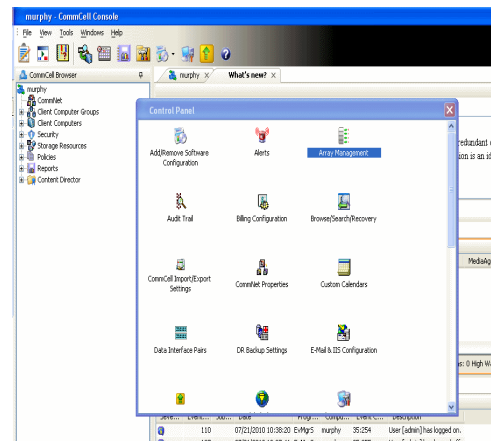
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



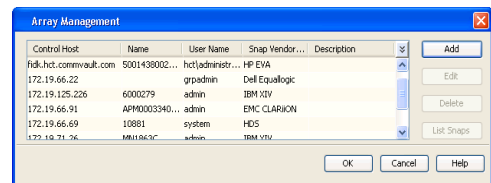
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the file server in the **Name** field.
 - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: []

Control Host: []

User Name: []

Password: []

Confirm Password: []

Device Group: []

Use devices only from this device group

Description: []

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous Next ▶

OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

PREREQUISITES

LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:

```
options snapvault.enable on
```

3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:

```
options snapvault.access host=secondary_filer1, secondary_filer2
```

4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:

```
options snapvault.access host=primary_filer1, primary_filer2
```

INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
 - Discover storage devices
 - Add Resource Pools to be used for the Vault/Mirror storage provisioning

CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

CREATE STORAGE POLICY

Use the following steps to create a storage policy.

1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.

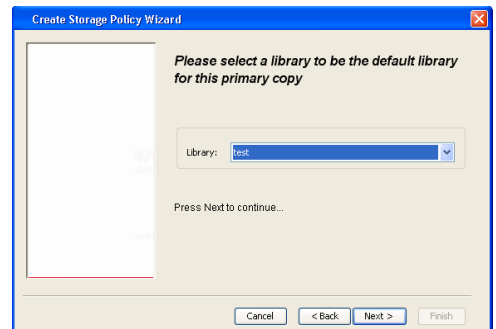
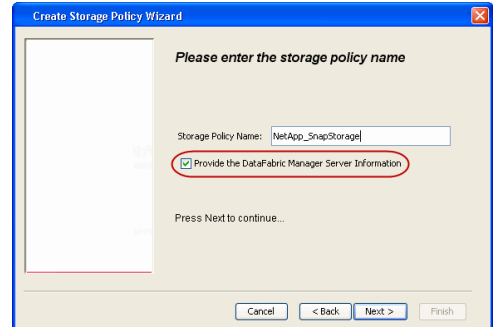
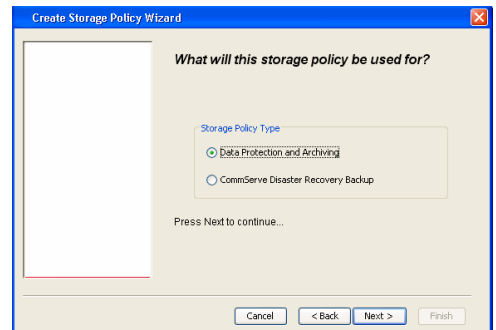
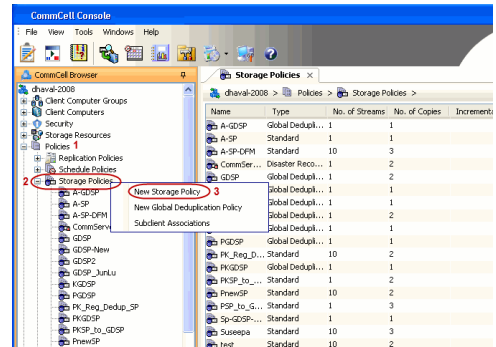
2. Click **Next**.

3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.

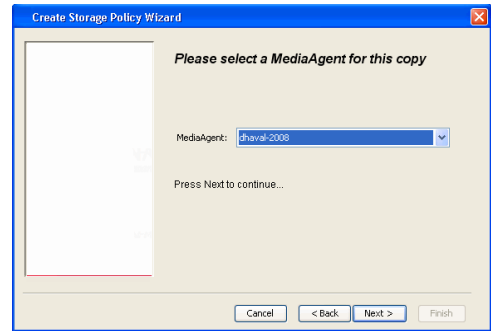
4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.

It is recommended that the selected disk library uses a LUN from the File server.
 - Click **Next**.

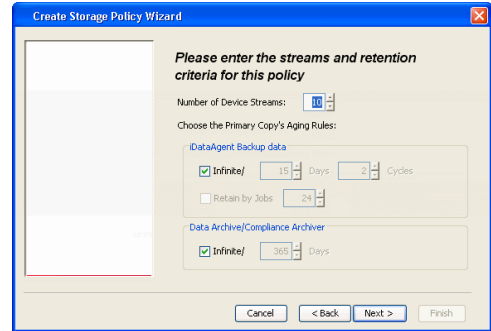
5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.



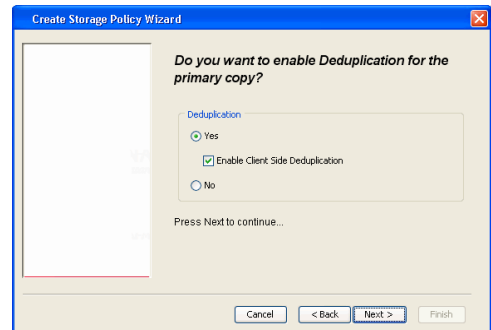
6. Click **Next**.



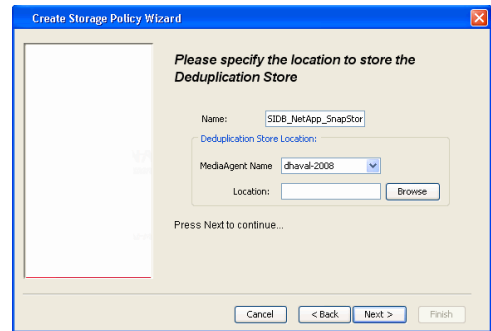
7. Click **Next**.



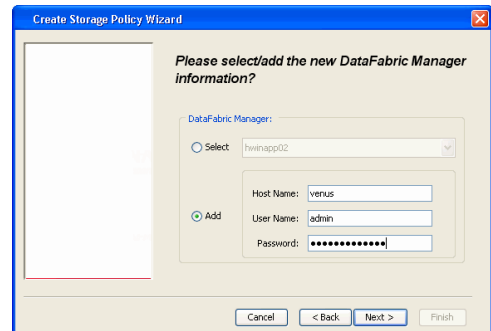
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

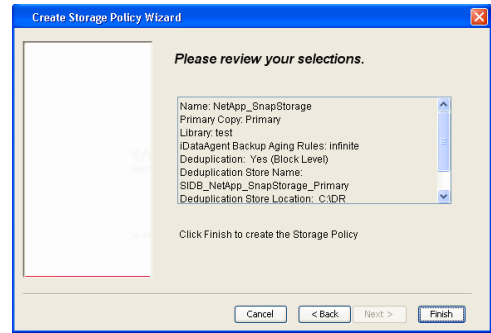


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



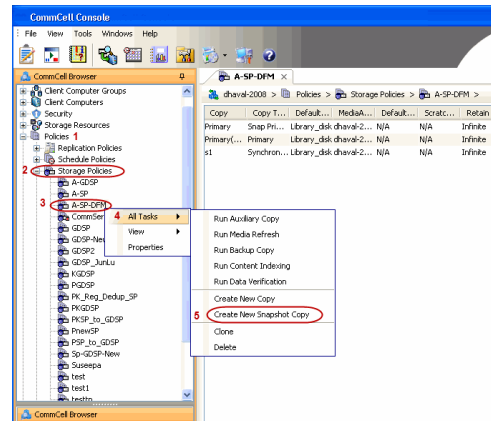


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

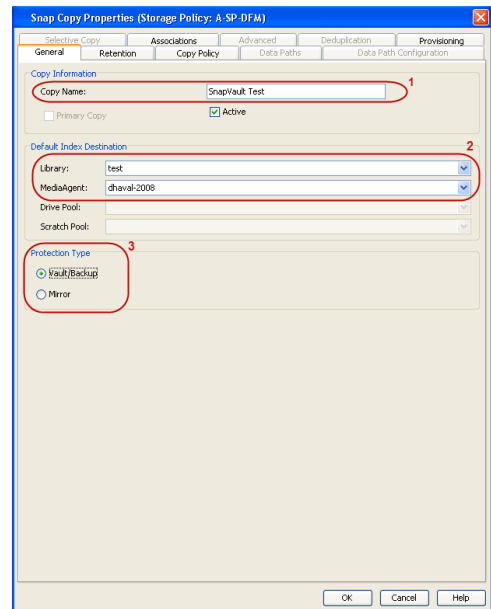
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
 - Enter the **Copy Name**.
 - Select the **Library** and **MediaAgent** from the drop-down list.
 - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

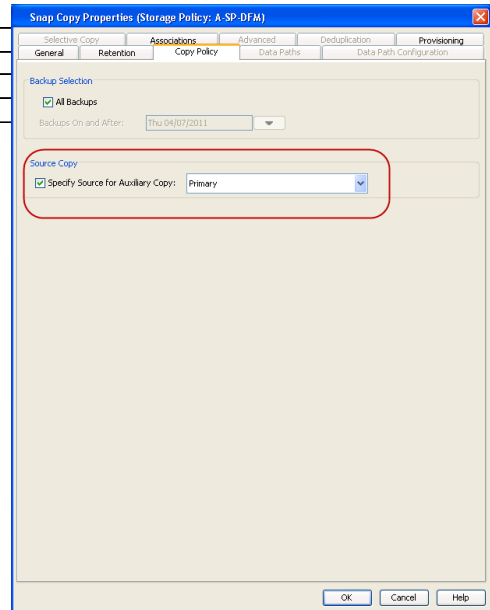


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

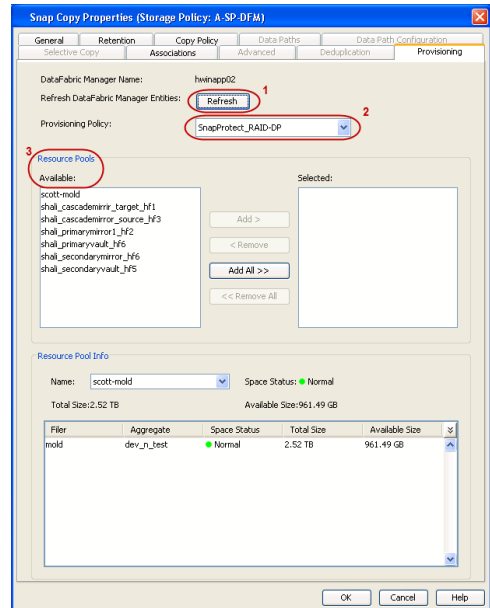
TOPOLOGY	SOURCE COPY
----------	-------------

Primary-Mirror	Primary
Primary-Mirror-Vault	Mirror
Primary-Vault	Primary
Primary-Vault-Mirror	Vault
Primary-Mirror-Mirror	Mirror



4.
 - Click the **Provisioning** tab.
 - Click **Refresh** to display the DFM entities.
 - Select the **Provisioning Policy** from the drop-down list.
 - Select the **Resource Pools** available from the list.
 - Click **OK**.

The secondary snapshot copy is created.



5. If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:


```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

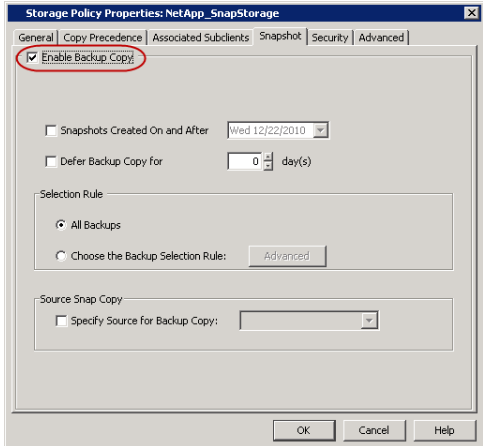
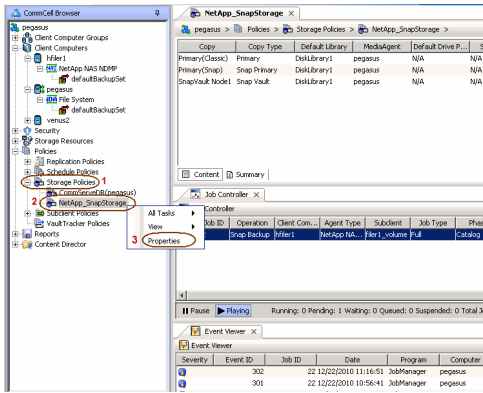
It is recommended that you perform this operation on all nodes in the P-M-V topology.

CONFIGURE BACKUP COPY

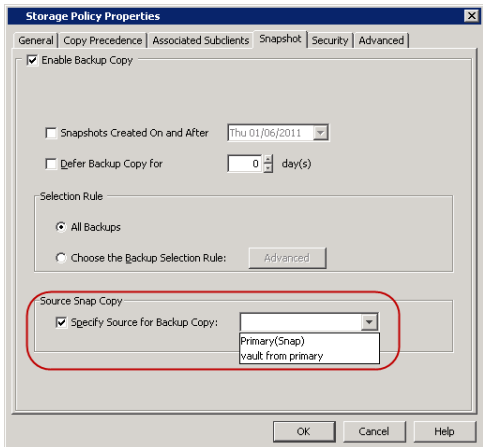
Follow the steps given below to configure Backup Copy for moving snapshots to media.

1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.

2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



3.
 - Select **Specify Source for Backup Copy**.
 - From the drop-down list, select the source copy to be used for performing the backup copy operation.

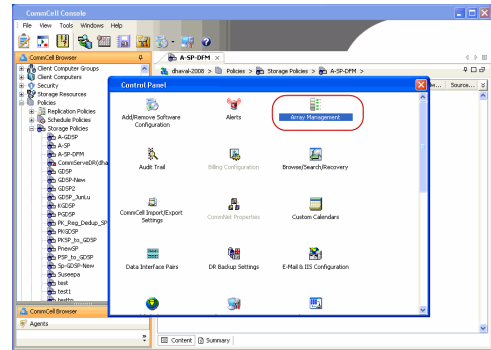


SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

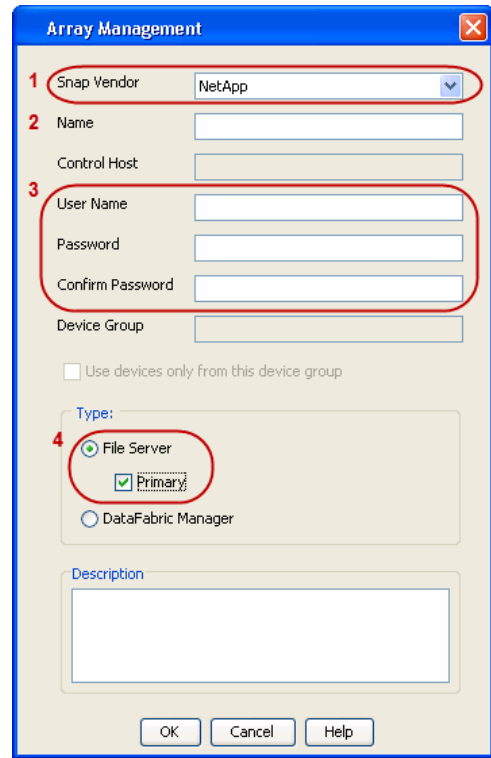
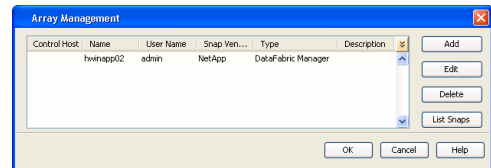


3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

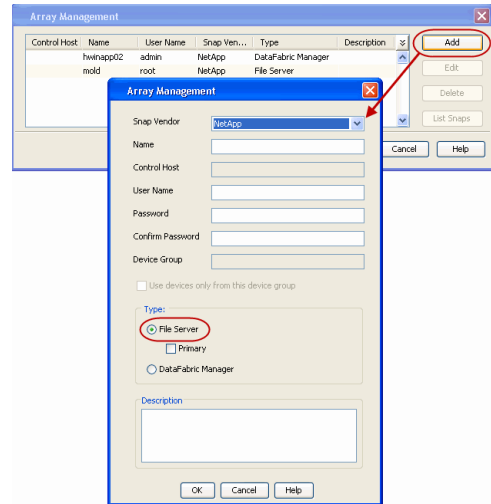
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



4.
 - Click **Add** again to enter the information for the secondary array.
 - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



SEE ALSO

Import Wizard Tool

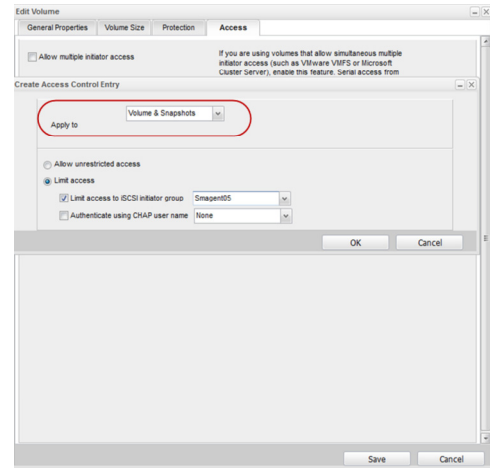
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

SnapProtect™ Backup - Nimble

◀ Previous Next ▶

PREREQUISITES

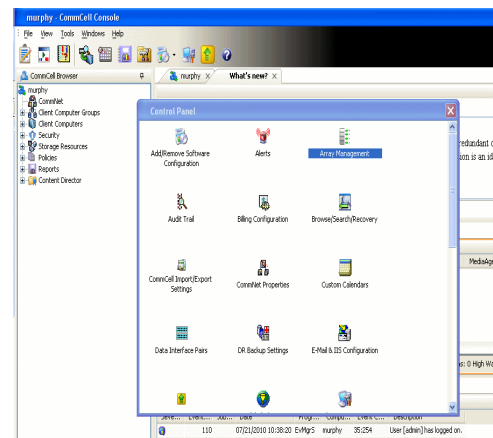
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry** to **Snapshots Only**.
- Ensure that a temporary LUN is allocated to all ESX Servers that are used for snapshot operations.



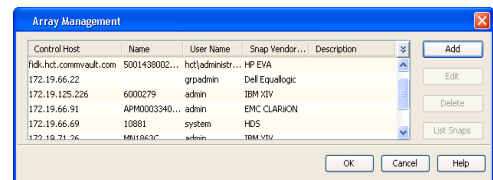
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **Nimble** from the **Snap Vendor** list.
 - Specify the Data IP Address of the array in the **Name** field.

If you have more than one Data IP Address configured, you will need to add the array information for each of the configured Data IP addresses.

- Enter the Management IP Address of the array in the **Control Host** field.

For reference purposes, the screenshot on the right shows the Data IP Address and Management IP for the Nimble storage device.

Name	Status	Type	Data IP Address	Subnet Mask	MTU	Bytes
eth1		Data only	172.19.108.100	255.255.252.0	Standard	1500
eth2		Data only	172.19.108.101	255.255.252.0	Standard	1500
eth3		Not configured			Standard	1500
eth4		Not configured			Standard	1500

4.
 - Enter the access information of a user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

< Previous Next >

SnapProtect™ Backup - Data Replicator

< Previous Next >

PRE-REQUISITES

INSTALLATION

- The use of Data Replicator with the SnapProtect backup requires MediaAgent, File System iDataAgent, and ContinuousDataReplicator on the source, destination, and proxy computers.

The use of a proxy server to perform SnapProtect operations is supported when a hardware storage array is used for performing the SnapProtect backup.

- The operating system of the MediaAgent to be used for SnapProtect backup must be either the same or higher version than the source computer.

STORAGE POLICY REQUIREMENTS

The Primary Snap Copy to be used for creating the snapshot copy must be a disk library.

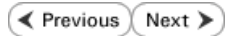
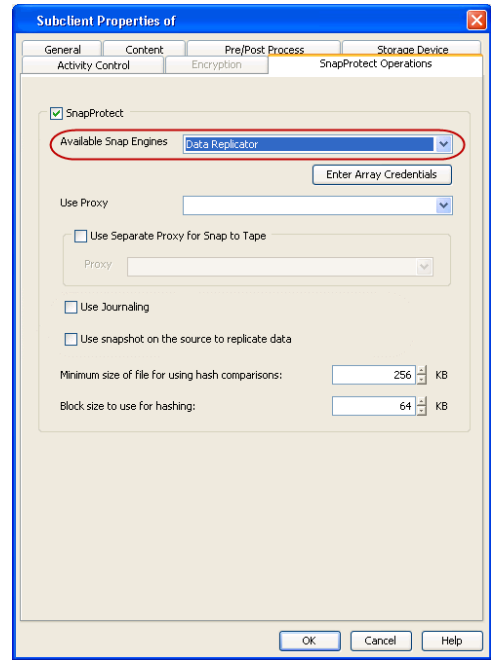
If the Storage Policy or the disk library being used by the subclient is updated, the subclient should be recreated.

SETUP THE ARRAY

1.
 - From the CommCell Console, navigate to <Client> | <Agent>.
 - Right-click the subclient and click **Properties**.
2.
 - Click the **SnapProtect Operations** tab.
 - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down

list.

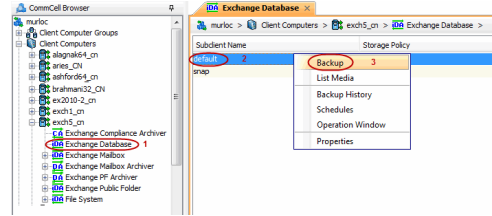
- Click **OK**.



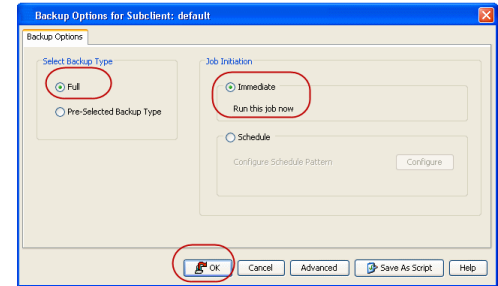
Getting Started - Exchange Database iDataAgent Backup

PERFORM A BACKUP

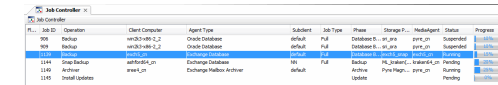
1. Ensure that Circular Logging has been disabled on the Exchange Server.
2.
 - From the CommCell Console, navigate to **Client Computers | <Client> | Exchange Database**.
 - Right-click the **default subclient** and click **Backup**.



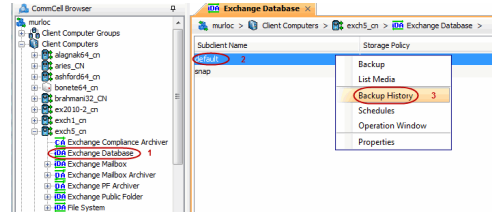
3.
 - Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.



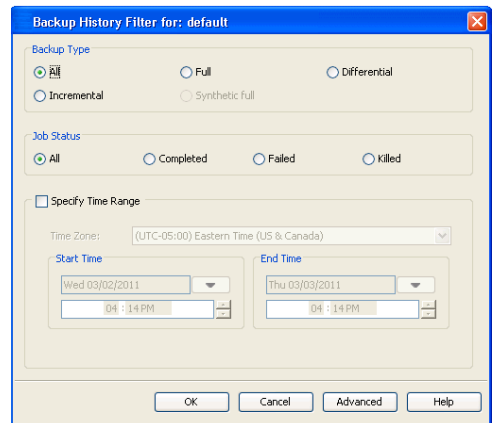
4. You can track the progress of the job from the **Job Controller** window of the CommCell console.



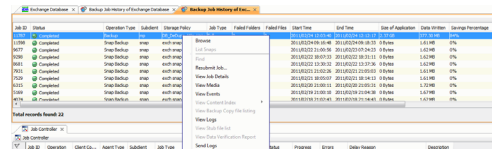
5. Once job is complete, view the details of job from the **Backup History**. Right-click the **Subclient** and select **Backup History**.



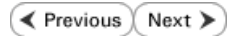
6. Click **OK**.



7. Right-click the job to:
 - View job details, such as the number of mailboxes backed up.
 - View media associated with the job.
 - View events associated with the job.
 - Resubmit the job.
 - View messages that were backed up.
 - Send the log file that is associated with the job.



Getting Started - Vault/Mirror Copy



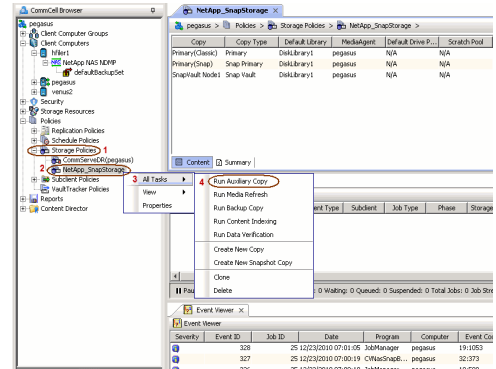
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** > to Continue.

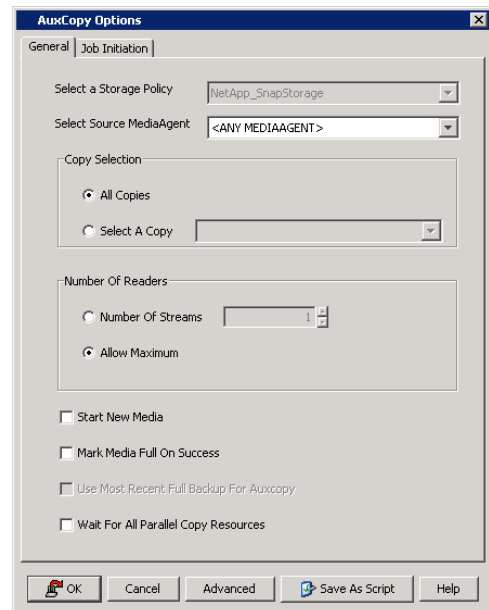
INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

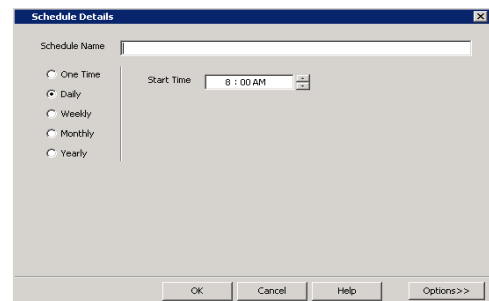


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.

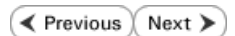


- Enter the schedule name and select the appropriate scheduling options.
 - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.



Getting Started - Snap Movement to Media

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

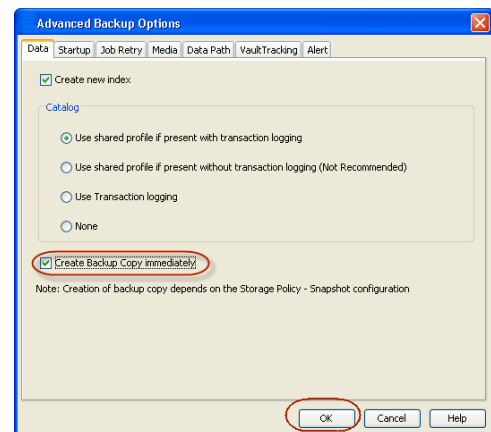
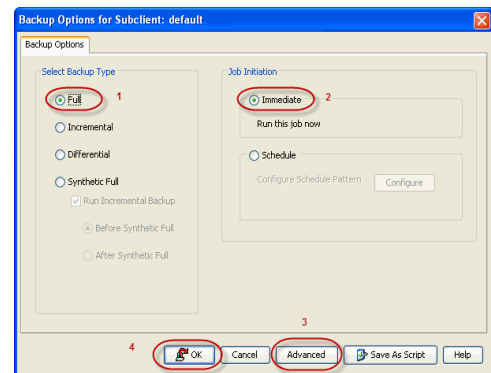
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

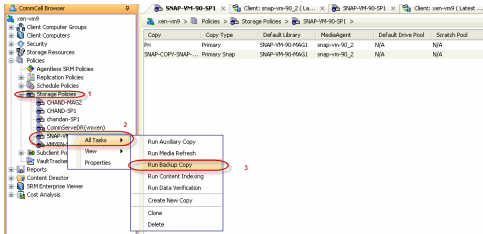
- From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
 - Right click the default subclient and click **Backup**.
 - Select **Full** as backup type.
 - Click **Advanced**.
- Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



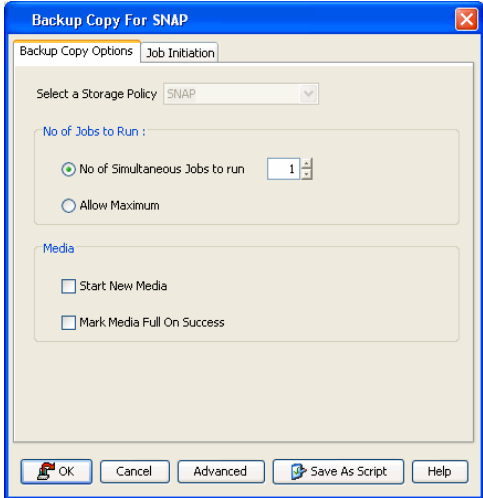
OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

- From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



Getting Started - Microsoft Exchange Database Restore

◀ Previous Next ▶

PERFORM A RESTORE

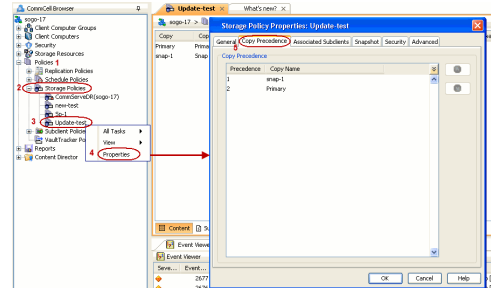
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring a single database to a different client computer.

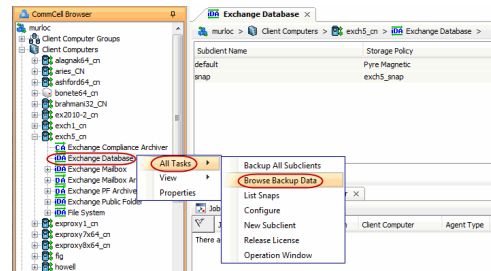
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.

You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.

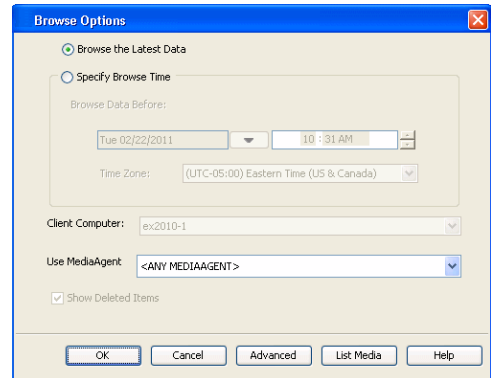
 - Click **OK**.



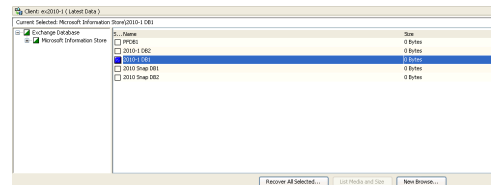
- From the CommCell Console, navigate to **Client Computers | <Client> | Exchange Database**.
 - Right-click the Agent and then click **All Tasks | Browse Backup Data**.



- Select a Windows MediaAgent from the **Use MediaAgent** drop-down list.
 - Click **OK**.

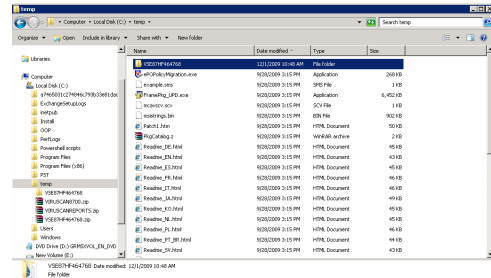
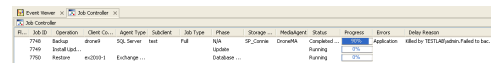
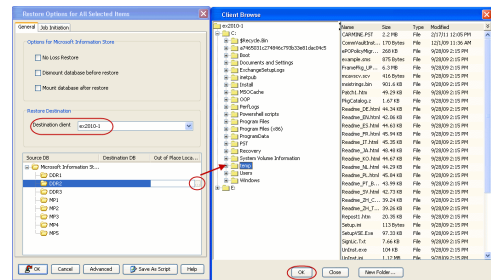


- Select the Microsoft Information Store in the left pane. Select a database in the right pane.
 - Click **Recover All Selected**.



- Select the name of the client computer from the **Destination Client** list.
 - This client should not be the same client on which the database originally resided.
 - Click **...** under **Out of Place** Location column.
 - Select a folder on the destination client and click **OK**.
 - Click **OK**.

6. You can monitor the progress of the restore job in the **Job Controller**.
7. The database is restored to the directory and client that was specified.



CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



Getting Started Deployment On a UNIX Computer - Oracle iDataAgent



WHERE TO INSTALL

Install the software directly on the Unix computer that you wish to protect and has the application data.

RELATED TOPICS

Download Software Packages

Download the latest software package to perform the install.

SnapProtect Support - Platforms

Verify that the computer in which you wish to install the software satisfies the minimum requirements.

INSTALL THE ORACLE iDATAAGENT

Use the following procedure to directly install the software from the installation package or a network drive.

1. Logon to the client computer as **root**.
2. 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:

```
./cvpkgadd
```

3. The product banner and other information is displayed.
Press **Enter**.
4. Read the license agreement. Type **y** and press **Enter**.
5. Press **Enter**.

6. Press **Enter**.

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 interface name that you wish to use as default, and then press **Enter**.

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

8. Press **Enter**.

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
- 2) Advance options
- 3) Exit this menu

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.

You now have a choice of performing a regular Calypso install on the physical host or installing Calypso on a virtual machine for operation within a cluster.

Most users should select "Install on a physical machine" here.

- 1) Install on a physical machine
- 2) Install on a virtual machine
- 3) Exit

Your choice: [1]

We found one network interface available on your machine. We will associate it with the physical machine being installed, and it will also be used by the CommServe to connect 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 check the interface name below, and make connections if necessary:

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

Please specify the client name for this machine.

9. Type the number associated with the **Oracle iDataAgent, Unix File System iDataAgent, and MediaAgent**.

Press **Enter**.

10. A confirmation screen will mark your choice with an "**X**".

Type **d** for **Done**, and press **Enter**.

11. Press **Enter**.

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

- Select **Download from the software provider website** to download the latest software scripts. Make sure you have internet access.
- Select **Use the one in the installation media** to install the software scripts from the package or share from which the installation is currently being 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.

13. Press **Enter**.

14. Press **Enter** to accept the default path.

- If you want to specify a different path, type the path and then press **Enter**.
- If you want to install the software binaries to an NFS shared drive, specify the directory on which you have mounted the NFS file system and then press **Enter**.

In order to make sure that the client computer has `read/write` access to NFS shared drive, review the steps described in *Installing Software Binaries to an NFS Shared Drive*.

Do not use the following characters when specifying the path:

!@#\$\$%^&*():?\
 \

15. Press **Enter** to accept the default location.

- Enter a path to modify the default location and press **Enter**.
- All the modules installed on the computer will store the log files in this directory.

16. Type **Yes** and press **Enter**.

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]

Install Calypso on physical machine 172.19.99.62

Please select the Calypso module(s) that you would like to install.

```
[ ] 1) MediaAgent [1301] [CVGxMA]
[ ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]
[ ] 3) Oracle iDataAgent [1204] [CVGxOrIDA]

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

Enter number(s)/one of "a,n,r,q,d,>,<,>?" here:3

Install Calypso on physical machine 172.19.99.62

Please select the Calypso module(s) that you would like to install.

```
[X] 1) MediaAgent [1301] [CVGxMA]
[X] 2) UNIX File System iDataAgent [1101] [CVGxIDA]
[X] 3) Oracle iDataAgent [1204] [CVGxOrIDA]

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

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

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]

Please specify where you want us to install Calypso binaries.

It must be a local directory and there should be at least 176MB 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]

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]

Most of Software processes run with root privileges, but some are launched by databases and inherit database access rights. To make sure that registry and log files can be written to by both kinds of processes we can either make

17. Type the **Group name** and then press **Enter**.

such files world-writeable or we can grant write access only to processes belonging to a particular group, e.g. a "calypso" or a "oinstall" group.

We highly recommend now that you create a new user group and enter its name in the next setup screen. If you choose not to assign a dedicated group to Software processes, you will need to specify the access permissions later.

If you're planning to backup Oracle DB you should use "oinstall" group.

Would you like to assign a specific group to Software?
[yes]

Please enter the name of the group which will be assigned to all Software files and on behalf of which all Software 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 "oinstall" group here.

Group name: oinstall

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 "oinstall".

18. This prompt is relevant only when you install on Solaris. Press **Enter** to accept the default value for **Number of Streams**.

You can type the **Number of Streams** that you plan to run at the same time and then press **Enter**.

Number of Streams

IMPORTANT : Please read install document "Configure Kernel Parameters - Unix/Macintosh" from "Books Online" before you start configuring kernel parameters. Please enter the total number of streams that you plan to run at the same time. We need to make sure that you have enough semaphores and shared memory segments configured in /etc/system.

Number of streams [10]

19. Press **Enter** if you do not want the changes to be updated automatically.

- If you want the changes to be made automatically, type **Yes** and then press **Enter**.
- You will come across this prompt when you install the software on the earlier versions of Solaris.

We now need to modify the /etc/system configuration file on this computer. It is done to make sure that there will be enough shared memory and semaphores available for Calypso programs. Please review the changes below and answer "yes" if you want us to apply them to the /etc/system file. Otherwise, the installation will proceed, the changes will be saved to some other file, and you will have to apply them manually.

```
set shmsys:shminfo_shmmni=8570 (was 7930)
set shmsys:shminfo_shmseg=8420 (was 7780)
set semsys:seminfo_semmns=10320 (was 9680)
set semsys:seminfo_semmni=8570 (was 7930)
set semsys:seminfo_semmsl=8570 (was 7930)
```

Do you want us to apply these changes now? [no]

Changes saved into /etc/system.gal.1744

Press <ENTER> to continue.

20. Press **Enter**.

You will see this prompt if you have accepted the default **no** and pressed **Enter** in the above step.

21. Press **Enter**.

You will see this prompt if you have accepted the default **no** and pressed **Enter** in step 19.

Although a 'no' answer can be selected to this question during install, the user should make sure the min requirements (below) for shared memory are met, otherwise the backups may fail (the message in logs is 'could not start the pipeline').

```
set shmsys:shminfo_shmmax=4199304
set shmsys:shminfo_shmmin=1
set semsys:shminfo_shmmni=640
set semsys:shminfo_shmseg=640
set semsys:seminfo_semmns=640
set semsys:seminfo_semmni=640
set semsys:seminfo_semmsl=640
set maxusers=256
```

Press <ENTER> to continue.

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

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

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

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 : [8400]

Port Number for EvMgrC: [8402]

23. If you do not wish to configure the firewall services, press **Enter**.

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

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

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

24. Type the fully qualified CommServe host name and press **Enter**.
Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.

25. Press **Enter**.

26. Type the number associated with the Client Group and press **Enter**.

NOTES

- This screen will be displayed only if Client Groups are configured for the CommCell.

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

28. Enter the number associated with the storage policy you want use and press **Enter**.

29. Type **3** to the **Exit** option and press **Enter**.
The installation is now complete.

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

CommServe Host Name: mycommserve.company.com

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.

- 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(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.

[] 1) Unix

[] 2) DR

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

Enter number(s)/one of "a,n,r,q,d,>,<," here: 1

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.

[X] 1) Unix

[] 2) DR

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

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

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

1) SP_StandAloneLibrary2_2

2) SP_Library3_3

3) SP_MagLibrary4_4

Storage Policy: [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

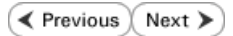
2) Install Calypso on a virtual machine

3) Exit

Your choice: [1] 3



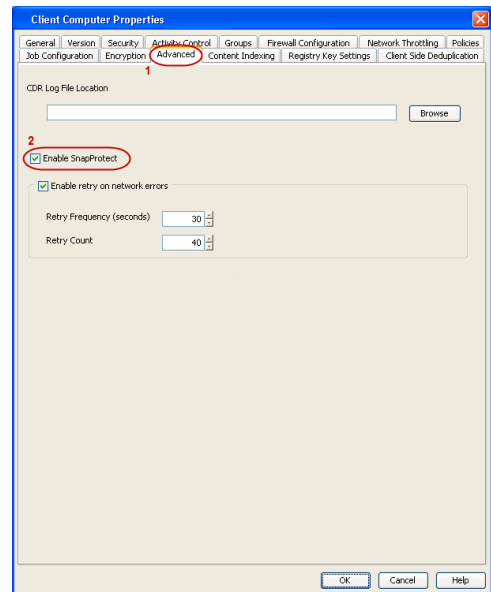
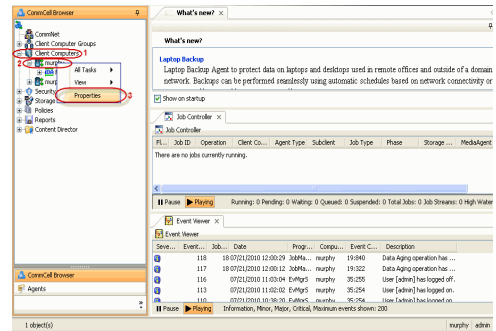
Getting Started - Oracle Configuration



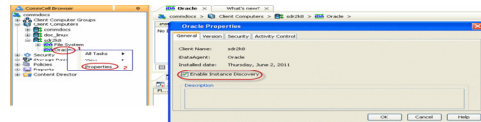
CONFIGURATION

The following sections provide the necessary steps required to create and configure the components for a first SnapProtect backup of an Oracle database.

- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.
- Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.



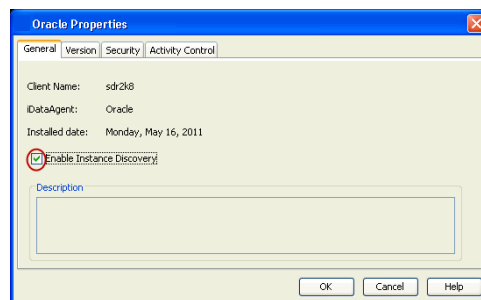
- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click **Oracle** and then click **Properties**.



- Select the **Enable Instance Discovery** checkbox.
 - Click **OK**.

If the instances are discovered automatically, go to step 7.

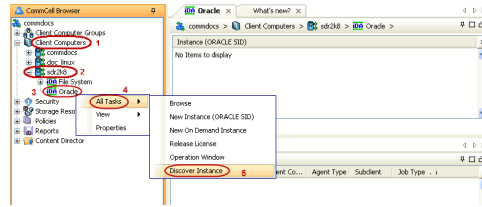
If the instances are not discovered automatically, follow the step given below to manually discover the instances.



- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click **Oracle**, point to **All Tasks** and then click **Discover Instance**.

6. Click **Yes**.

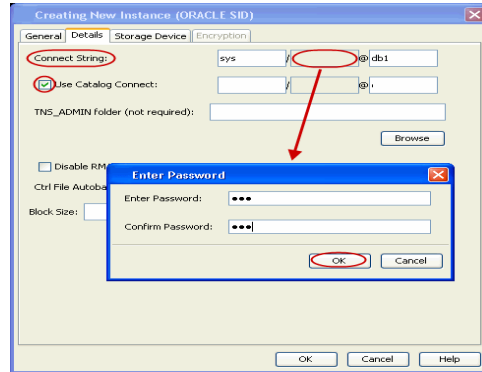
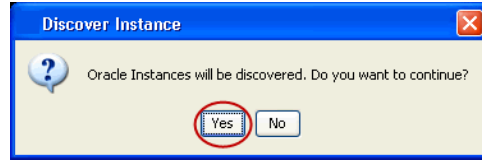
If your Oracle database uses an ASM instance and the instance is in a different Oracle Home, you may have to manually add the instance as the discovery operation may not find it. When configuring the instance, verify the database status shows as STARTED.



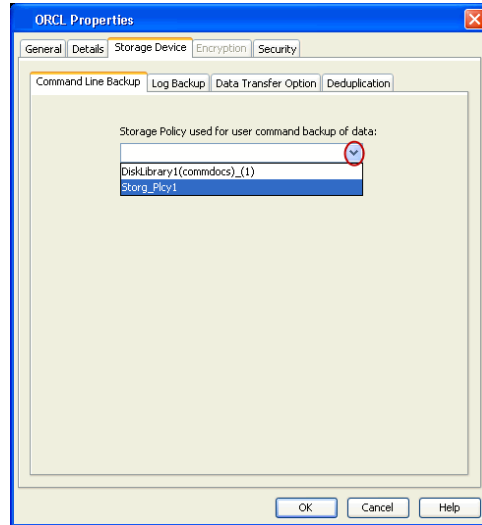
- 7.
- From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
 - Right-click the **<Instance>** and then click **Properties**.

8. Skip this step if you are not using a proxy computer.

- Click the **Details** tab.
- In the **Use Catalog Connect** field, type the user name to connect to the Recovery Catalog database.
- Click the grayed box in **Use Catalog Connect**.
- In the **Password** field, type the password for the user to connect to the Recovery Catalog database.
- In the **Confirm Password** box, re-type the password for the user.
- Click **OK**.

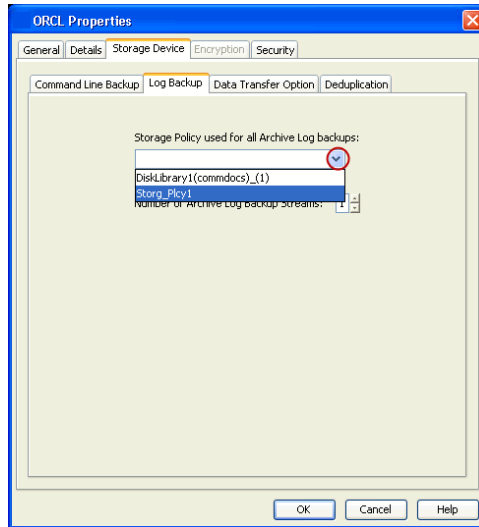


- 9.
- Click the **Storage Device** tab.
 - In the **Storage Policy used for user command backup of data** box, select a storage policy name.

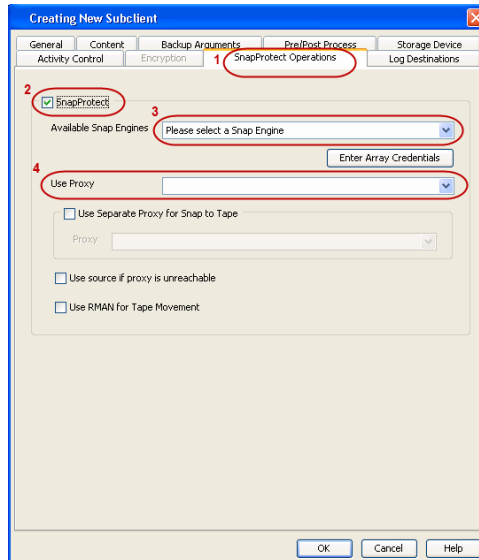
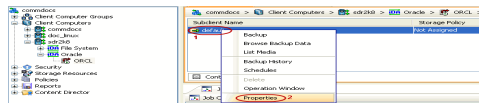


- 10.
- Click the **Logs Backup** tab.
 - In the **Storage Policy used for all Archive Log backups** box, select a storage policy name.
 - Click **OK**.

11.
 - From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle | <Instance>**.
 - Right-click the default subclient and then click **Properties**.

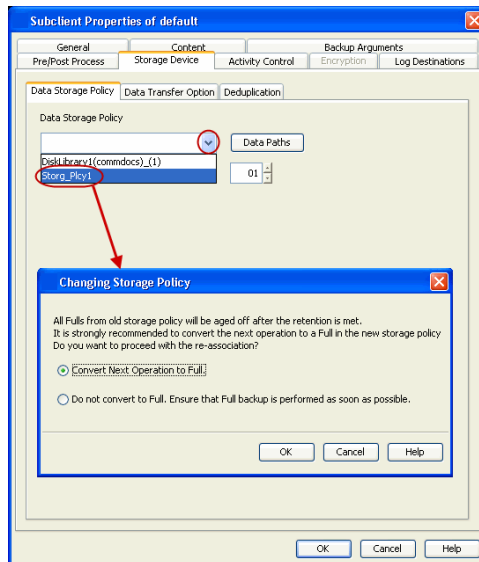


12.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where backup copy operations will be performed.
 - When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.
 - For clustered environments, ensure the proxy you want to select is not part of a cluster setup.



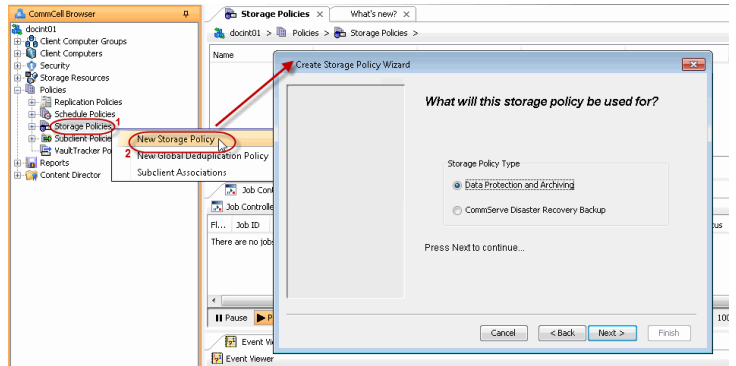
13.
 - Click the **Storage Device** tab.
 - In the **Data Storage Policy** list, select a Storage Policy name.
 - Click **OK** to convert the next backup as a full backup.
 - Click **OK**.

Click **Next** ➤ to continue. If you do not have Storage Policy created, follow the step given below to create a storage policy.



14. Create a Storage Policy:

1. Click **Create Storage Policy**.
2. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
 - o Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.
 - o Enter the name in the **Storage Policy Name** box and click **Next**.
 - o From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.
Ensure that you select a library attached to a MediaAgent operating in the current release.
 - o From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.
 - o For the device streams and the retention criteria information, click **Next** to accept default values.
 - o Select **Yes** to enable deduplication for the primary copy.
 - o From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.
Type the name of the folder in which the deduplication database must be located in the Deduplication Store Location or click the Browse button to select the folder and then click **Next**.
 - o Review the details and click **Finish** to create the Storage Policy.



SKIP THIS SECTION IF NOT USING SOLARIS.

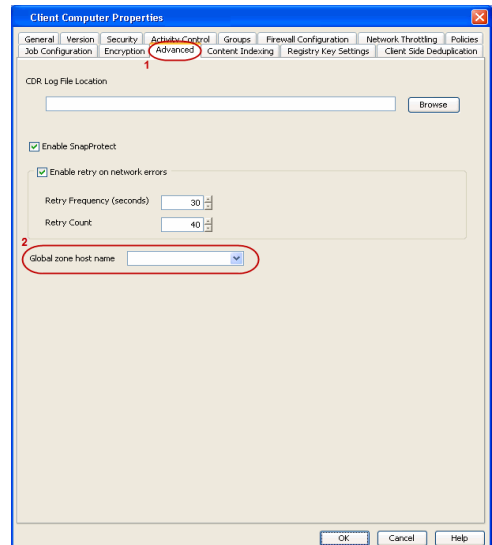
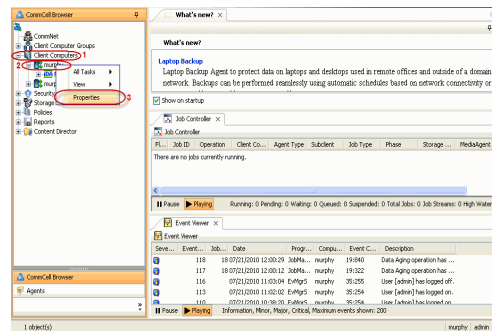
Click **Next** to Continue.

ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE



Follow the steps given below to enable SnapProtect backups on each of the non-global zone clients containing the application data.

1.
 - From the CommCell Console, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.
2.
 - Click **Advanced** tab.
 - Select the **Global Zone host name** from the drop-down list.
 - Click **OK**.
 - We support disks on a global zone mounted using loopback File System on a non global zone.
 - This option need not be enabled if you are using a NFS share. This is because when using NFS mount paths, the operations are limited to the non-global zone and does not use the global zone.



- Repeat the above steps on all the non-global zone clients containing the application data.

SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

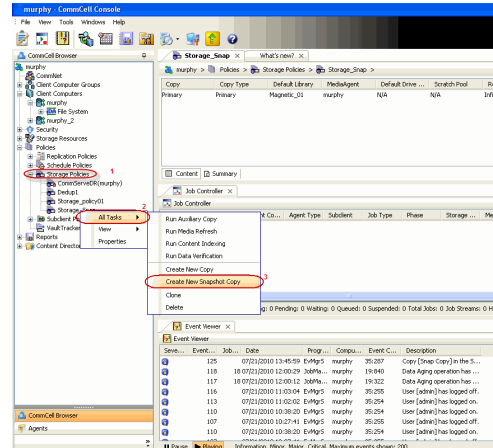
Click **Next** ➤ to Continue.

Next ➤

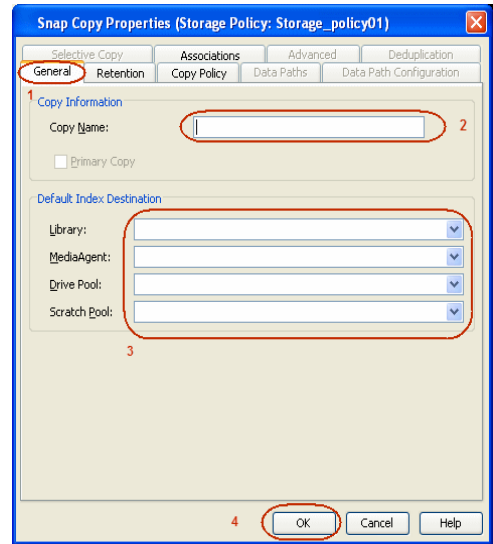
CREATE A SNAPSHOT COPY

Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.



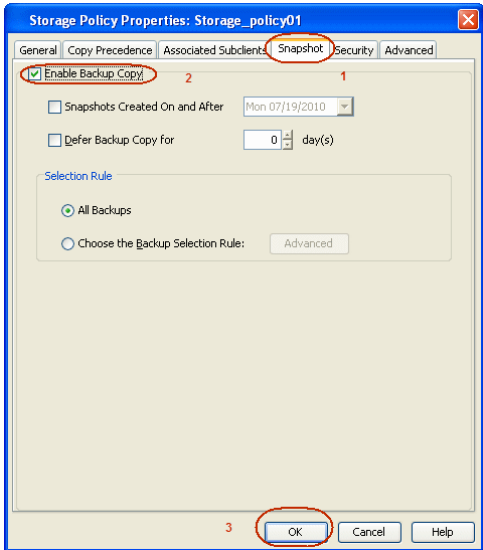
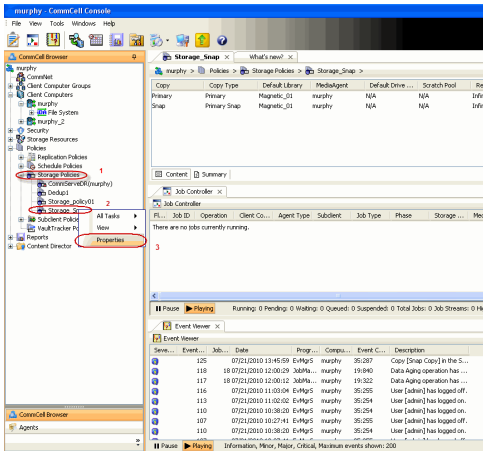
- Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



Storage Array Configuration

◀ Previous Next ▶

CHOOSE THE STORAGE ARRAY

HARDWARE STORAGE ARRAYS	SOFTWARE STORAGE ARRAY
3PAR	DATA REPLICATOR
DELL COMPELLENT	
DELL EQUALLOGIC	
EMC CLARIION, VNX	
EMC SYMMETRIX	
FUJITSU ETERNUS DX	
HITACHI DATA SYSTEMS	
HP EVA	
IBM SVC	
IBM XIV	
LSI	
NETAPP	
NETAPP WITH SNAPVAULT/SNAPMIRROR	

◀ Previous Next ▶

SnapProtect™ Backup - 3PAR

◀ Previous Next ▶

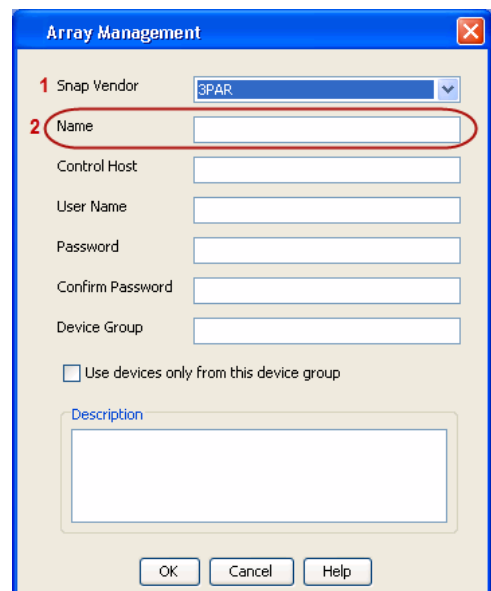
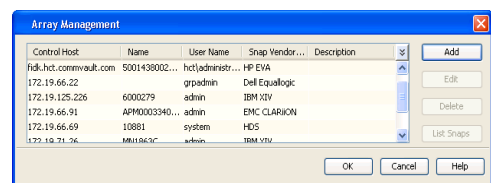
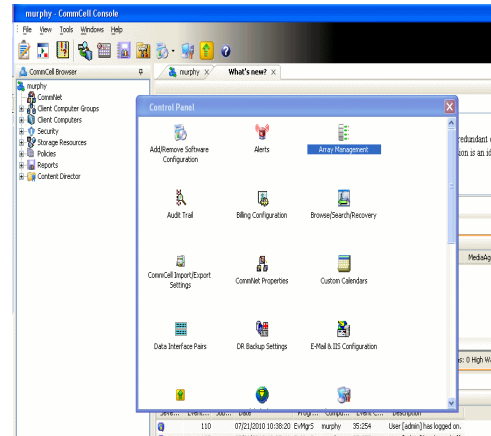
PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
 - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

where $\text{DevID.substr}(12,4)$ is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(12,4)$ is 0B95

After adding all the values, the resulting array name is 2FF70002AC000B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

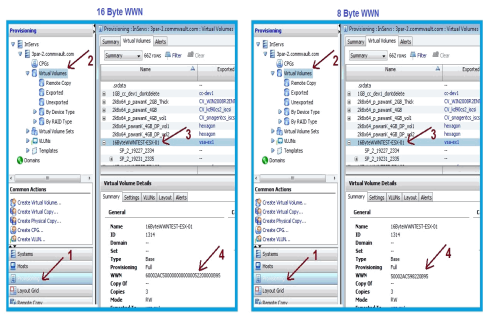
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(26,6)$ is 000B95

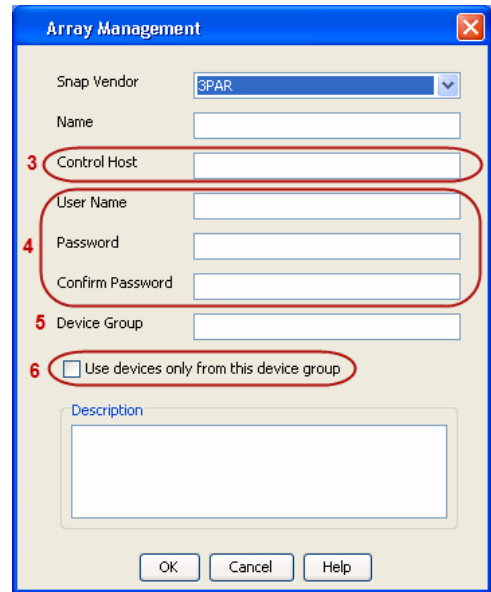
After adding all the values, the resulting array name is 2FF70002AC000B95.



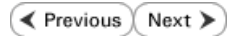
- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - Dell EqualLogic



PRE-REQUISITIES

WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

FIRMWARE VERSION

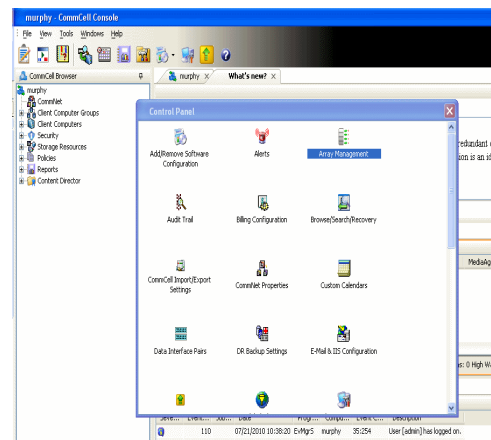
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

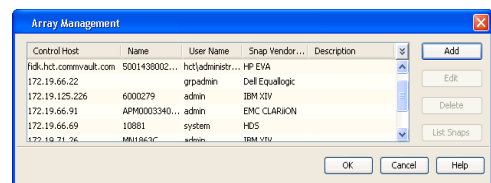
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



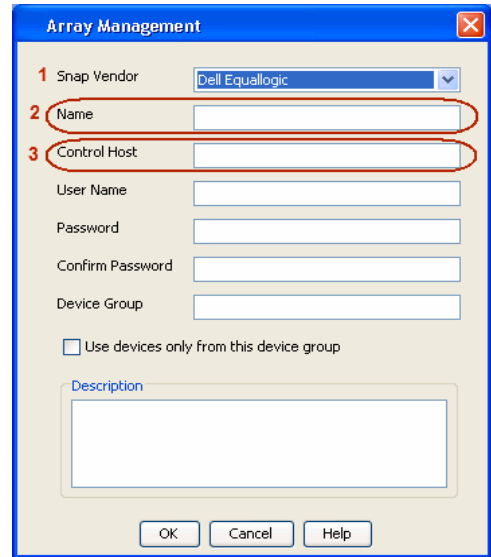
2. Click **Add**.



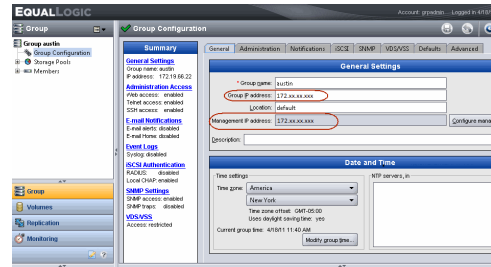
3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

No entry is required in the **Name** field if there is no Management IP address configured.

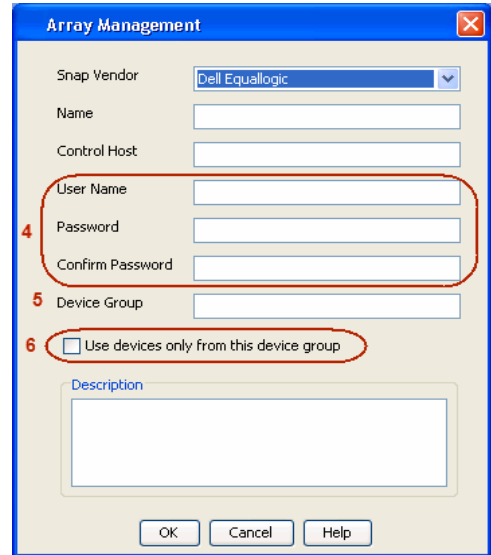
- Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
 - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
 - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
 - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous Next ▶

PRE-REQUISITES

LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

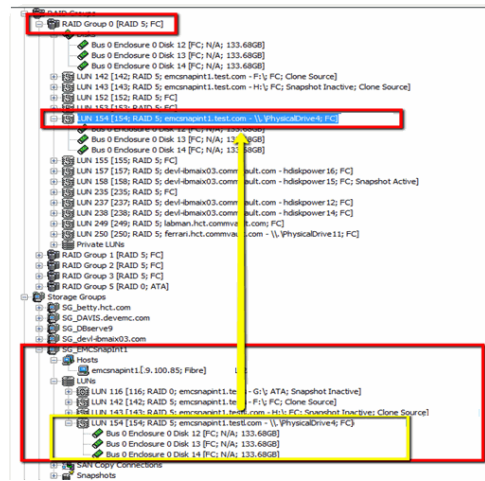
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

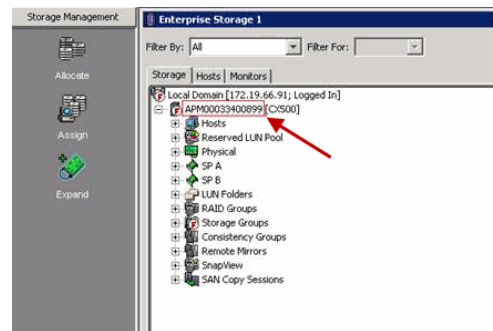
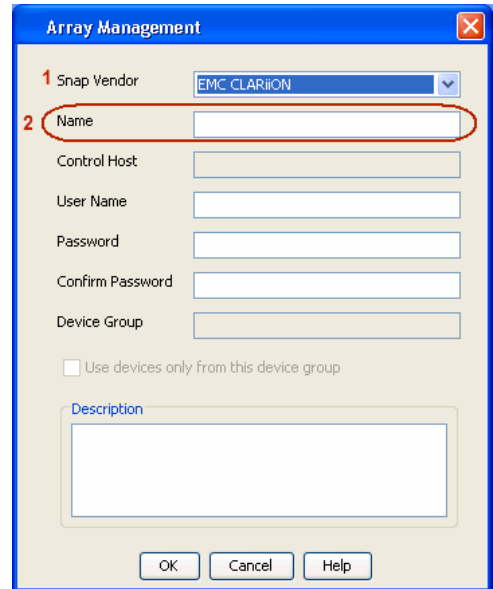
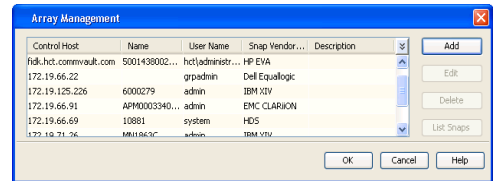
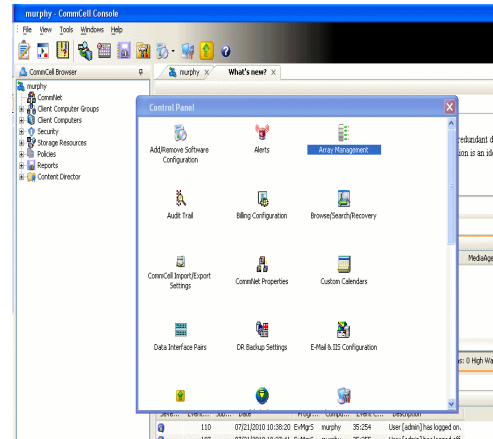
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
 - Specify the serial number of the array in the **Name** field.

For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.

- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



Array Management [Close]

Snap Vendor:

Name:

Control Host:

User Name:

3 Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - EMC Symmetrix

◀ Previous Next ▶

PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

LOAD THE SYMMETRIX DATABASE

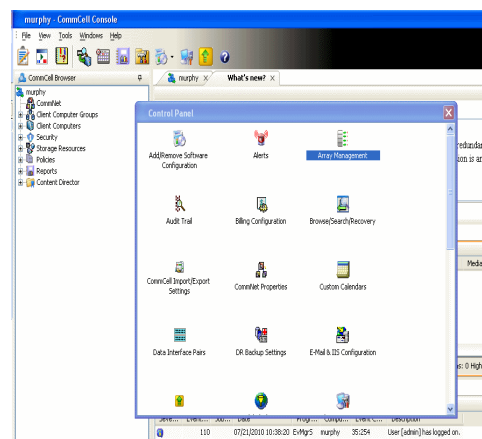
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

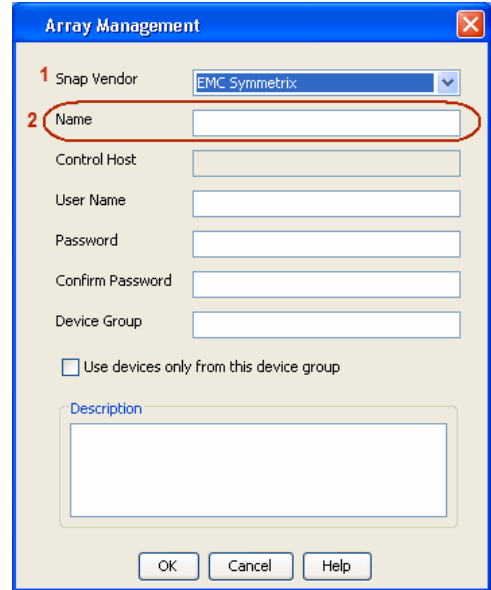
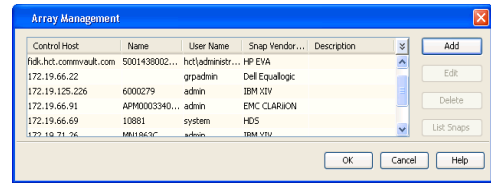
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

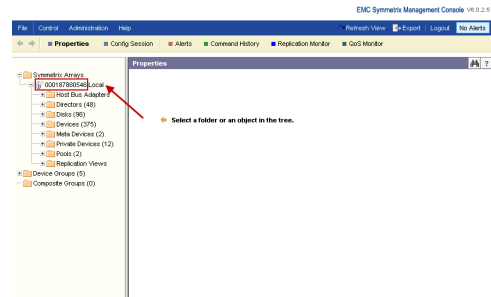


- Click **Add**.

3.
 - Select **EMC Symmetrix** from the **Snap Vendor** list.
 - Specify the **Symm ID** of the array in the **Name** field.

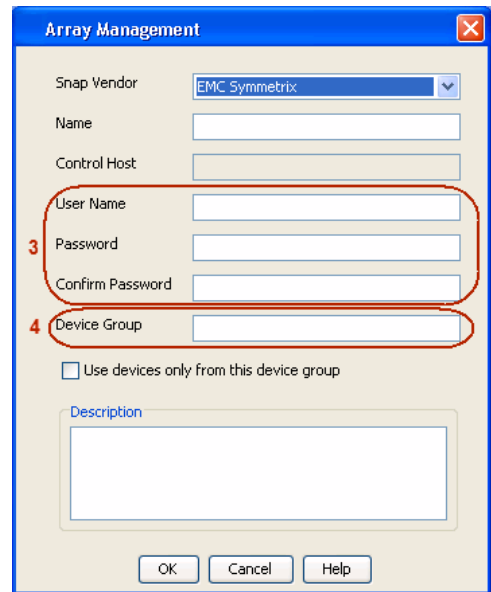


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.
If you do not specify a device group, the default device group will be used for snapshot operations.
 - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).



SnapProtect™ Backup - Hitachi Data Systems

◀ Previous Next ▶

PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
 - COW pools
 - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

ADDITIONAL REQUIREMENTS FOR VMWARE

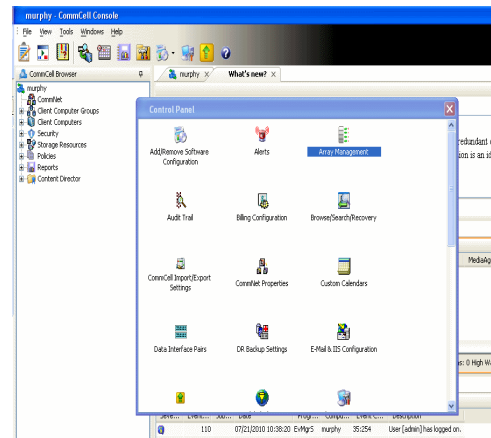
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server *iDataAgent* client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server *iDataAgent* client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

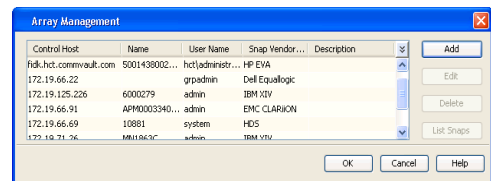
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

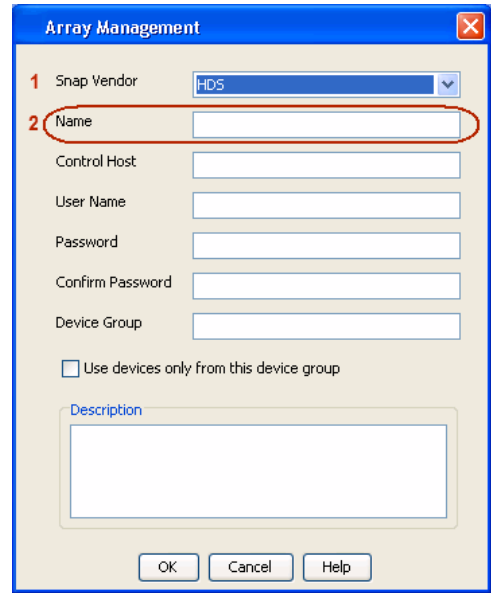
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



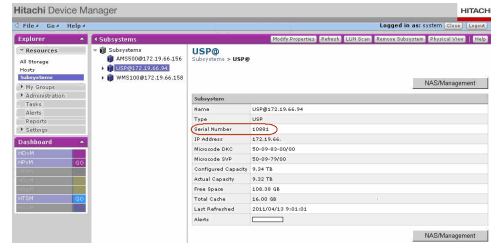
2. Click **Add**.



3.
 - Select **HDS** from the **Snap Vendor** list.
 - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



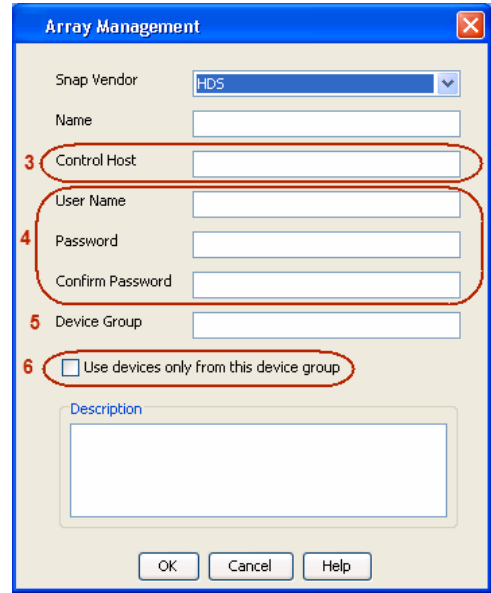
- 4.
- Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:

<COW_POOL_ID>-<LABEL> or <LABEL>-<COW_POOL_ID>

where <COW_POOL_ID> (for COW job) should be a number. This parameter is required.

<LABEL> (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - HP StorageWorks EVA

◀ Previous Next ▶

SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

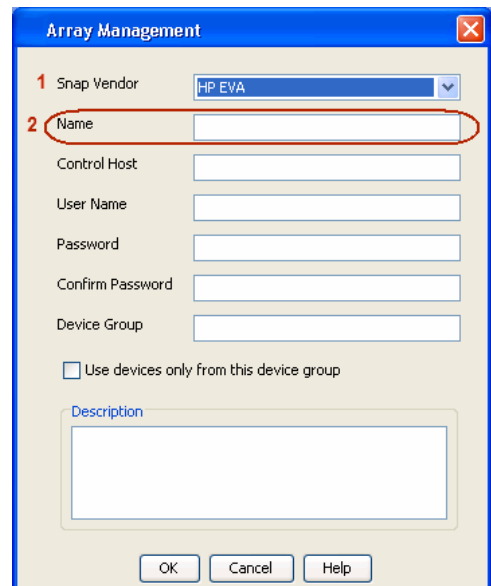
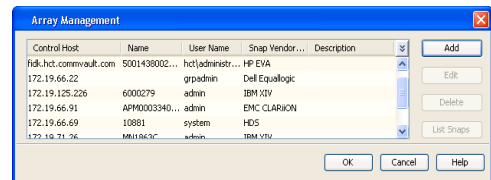
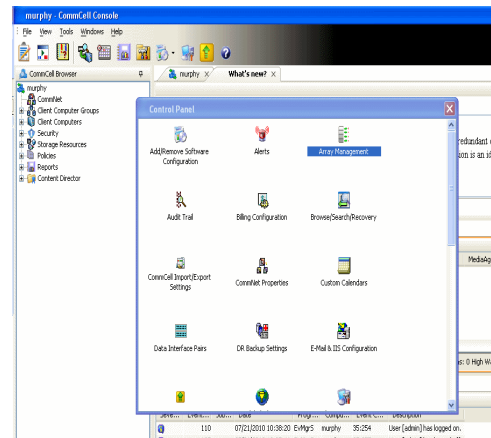
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin folder to discover the HP-EVA arrays.
3. Use the CLIRefreshTool.bat tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin folder.

SETUP THE ARRAY INFORMATION

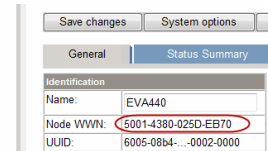
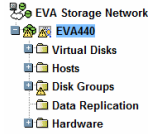
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
2. Click **Add**.
3.
 - Select **HP EVA** from the **Snap Vendor** list.
 - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

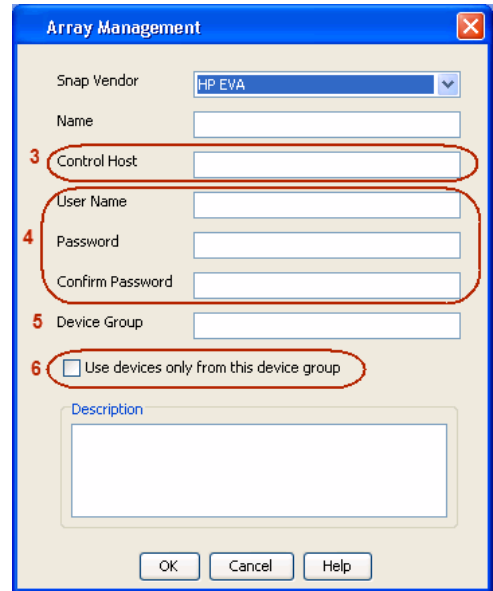
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



- 4. Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous Next ▶

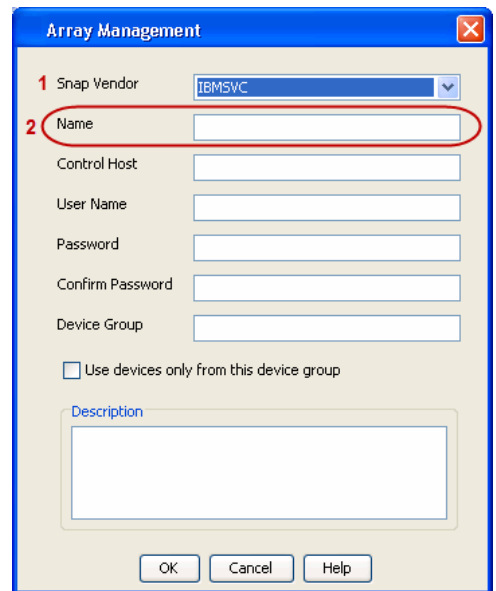
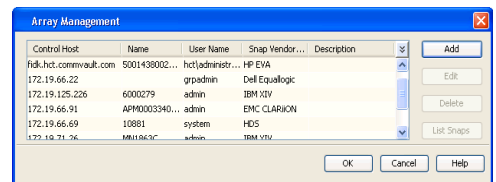
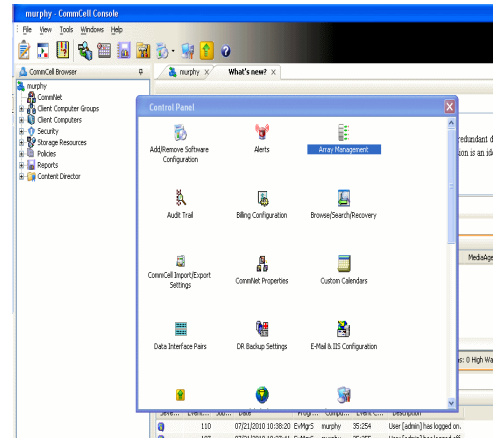
PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

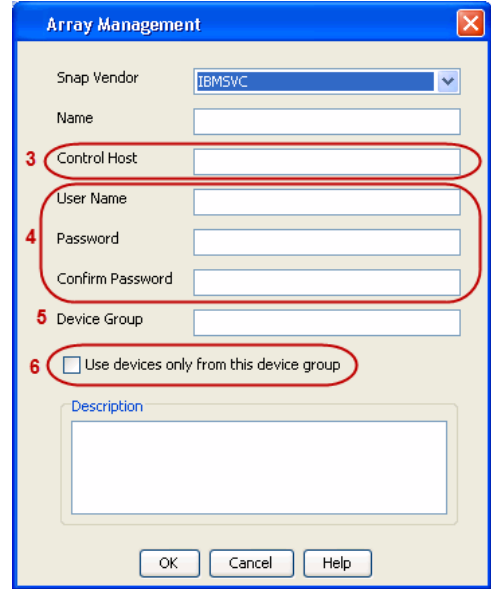
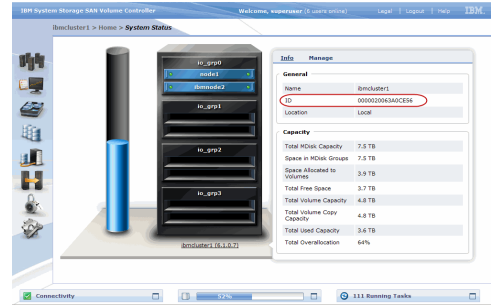
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM XIV



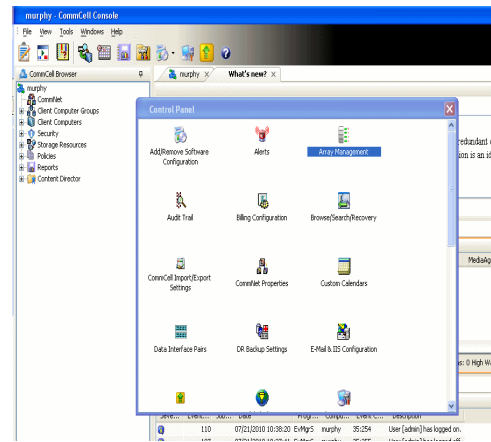
PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

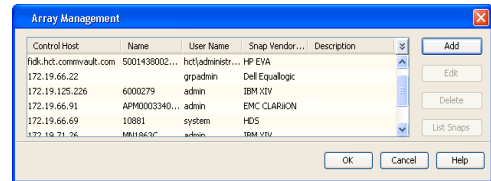
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

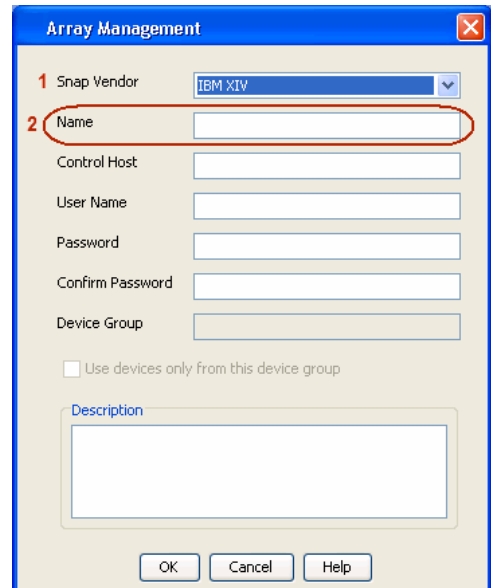
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



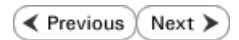
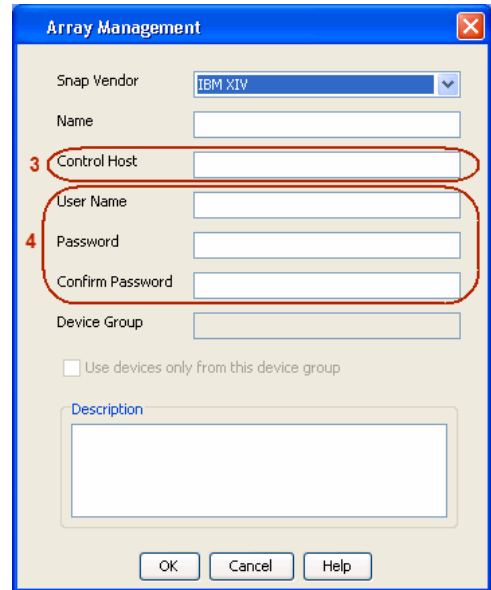
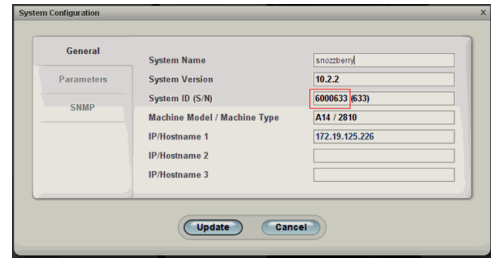
3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

4.

- Enter the IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the application administrator in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - LSI

◀ Previous Next ▶

PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
 - SMIS server through TCP/IP network.
 - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

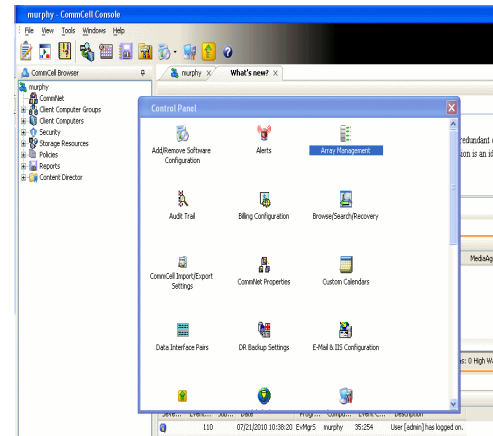
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

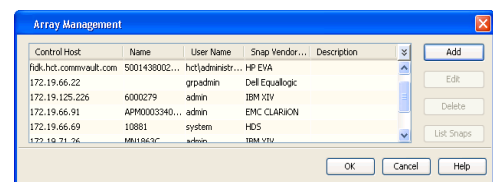
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

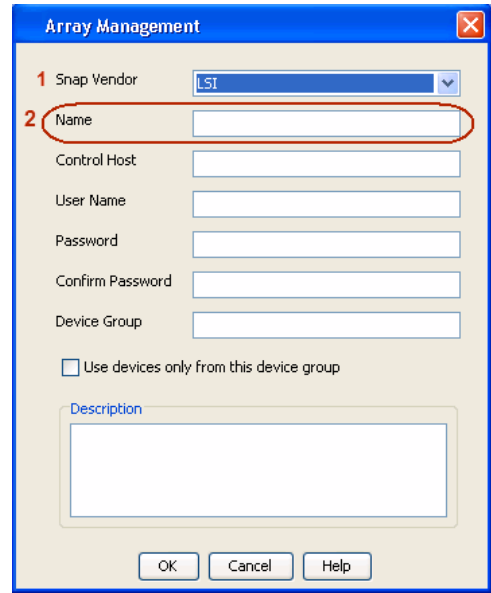
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

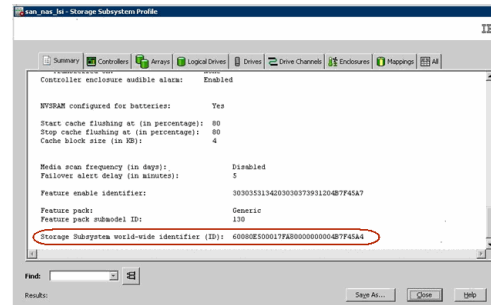


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

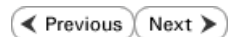
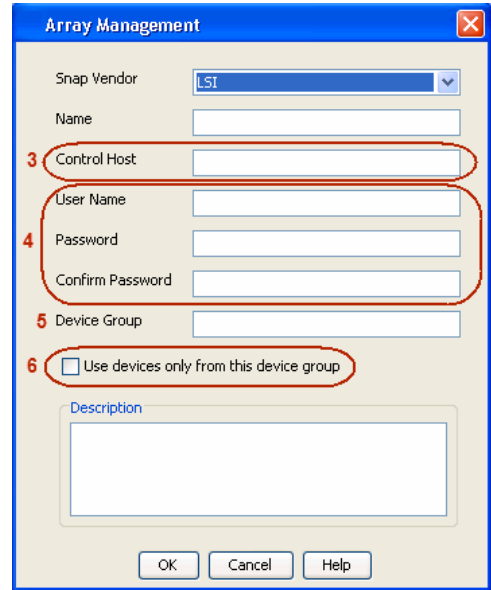
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



4.
 - Specify the name of the device manager server where the array was configured in the **Control Host** field.
 - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

If you specify None in the **Device Group** field but do not have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - NetApp



PREREQUISITES

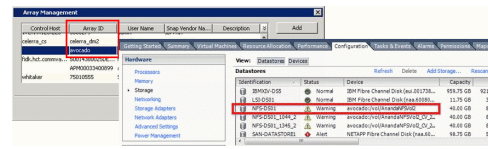
LICENSES

- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

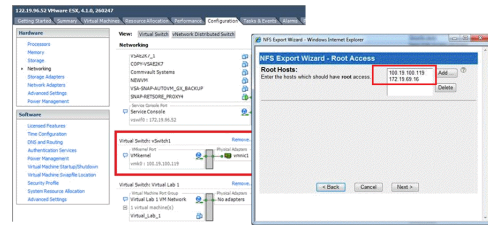
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.



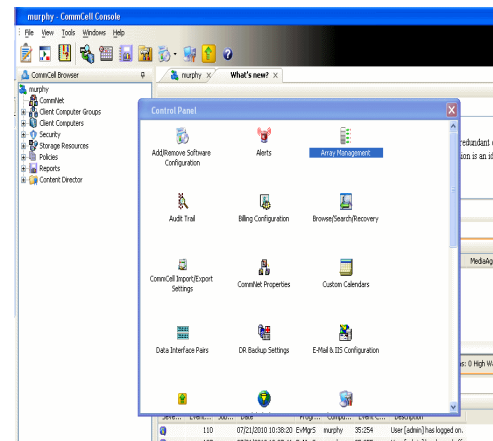
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



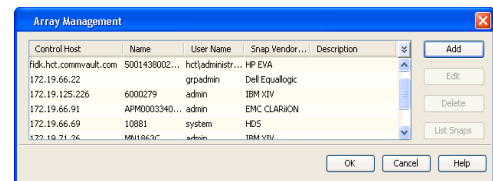
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the file server in the **Name** field.
 - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: []

Control Host: []

User Name: []

Password: []

Confirm Password: []

Device Group: []

Use devices only from this device group

Description: []

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous Next ▶

OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

PREREQUISITES

LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:

```
options snapvault.enable on
```

3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:

```
options snapvault.access host=secondary_filer1, secondary_filer2
```

4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:

```
options snapvault.access host=primary_filer1, primary_filer2
```

INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
 - Discover storage devices
 - Add Resource Pools to be used for the Vault/Mirror storage provisioning

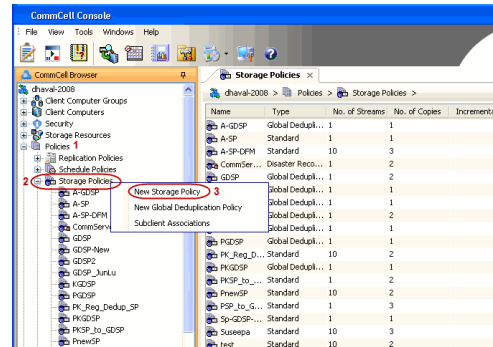
CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

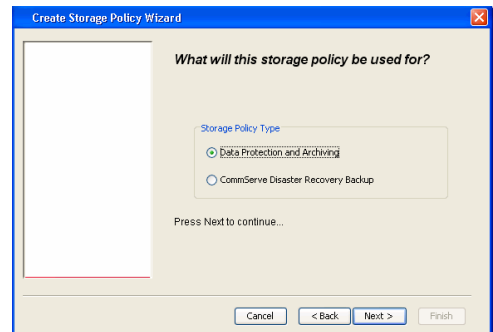
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

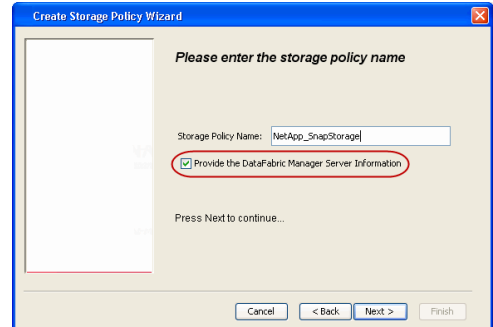
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



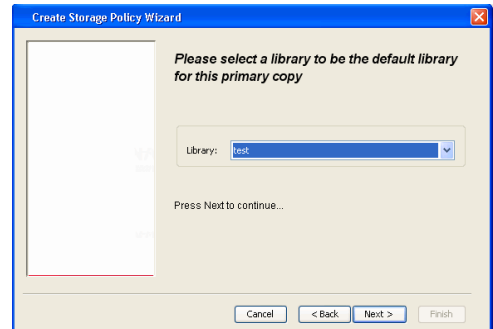
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.

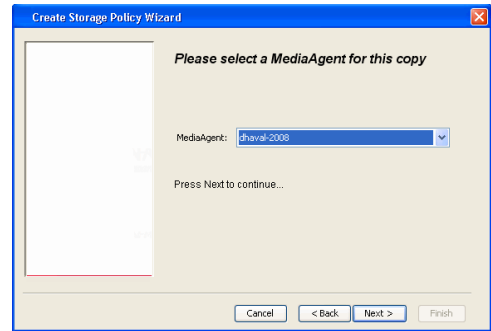
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

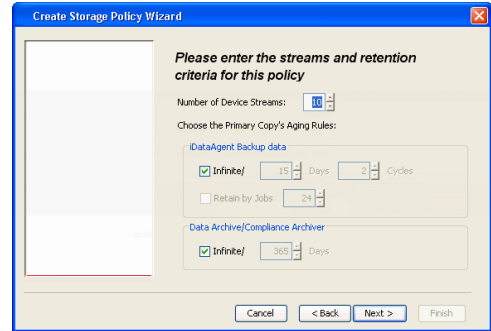


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

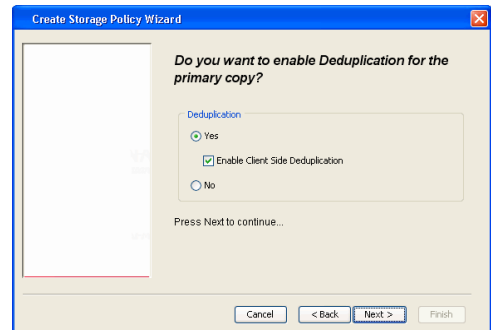
6. Click **Next**.



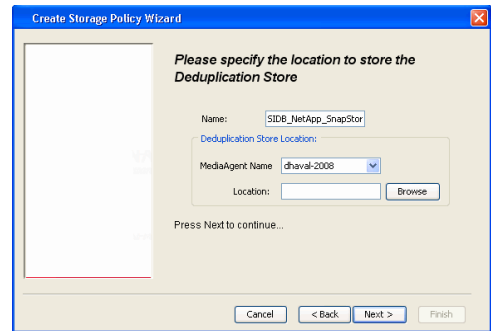
7. Click **Next**.



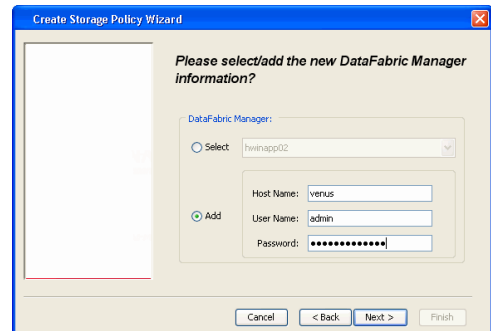
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

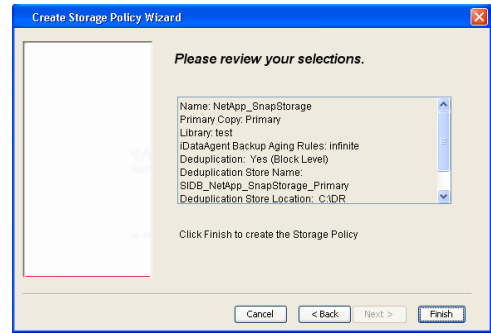


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



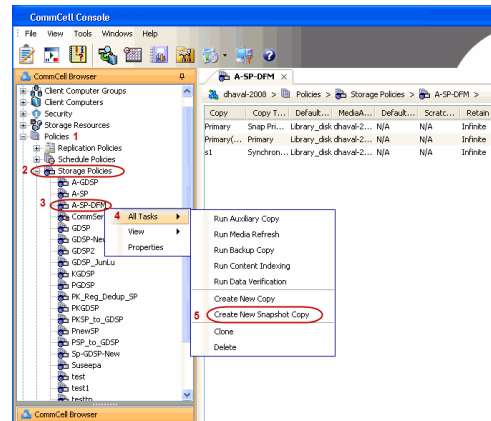


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

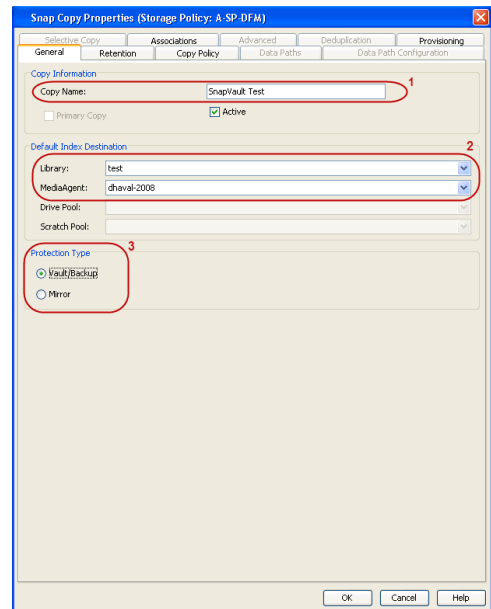
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
 - Enter the **Copy Name**.
 - Select the **Library** and **MediaAgent** from the drop-down list.
 - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

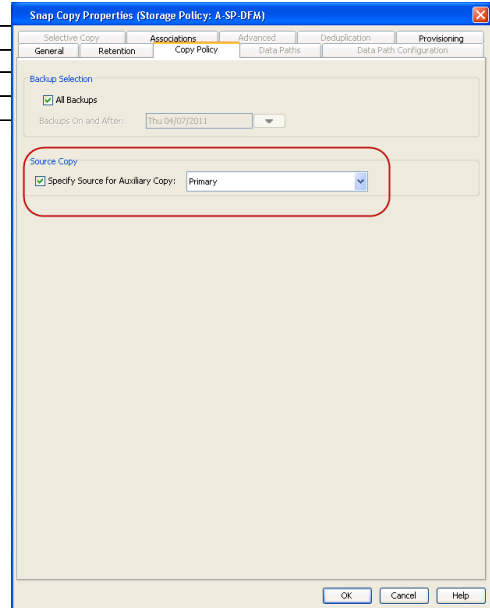


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

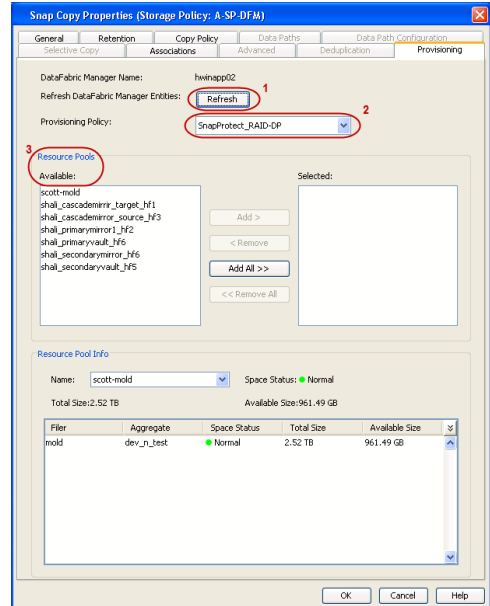
TOPOLOGY	SOURCE COPY
----------	-------------

Primary-Mirror	Primary
Primary-Mirror-Vault	Mirror
Primary-Vault	Primary
Primary-Vault-Mirror	Vault
Primary-Mirror-Mirror	Mirror



4.
 - Click the **Provisioning** tab.
 - Click **Refresh** to display the DFM entities.
 - Select the **Provisioning Policy** from the drop-down list.
 - Select the **Resource Pools** available from the list.
 - Click **OK**.

The secondary snapshot copy is created.



5. If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:


```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

It is recommended that you perform this operation on all nodes in the P-M-V topology.

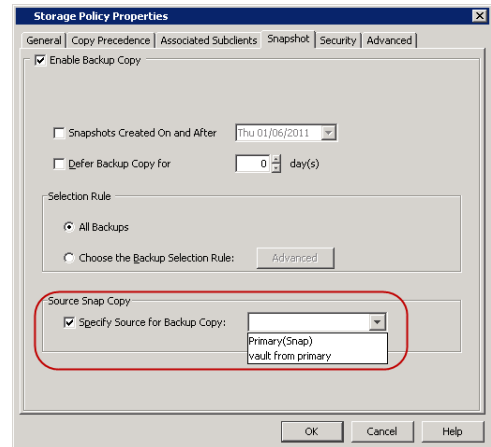
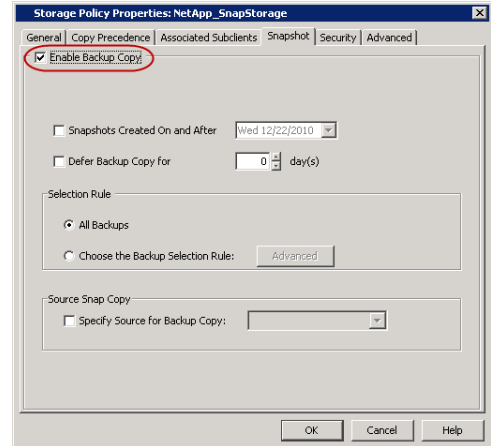
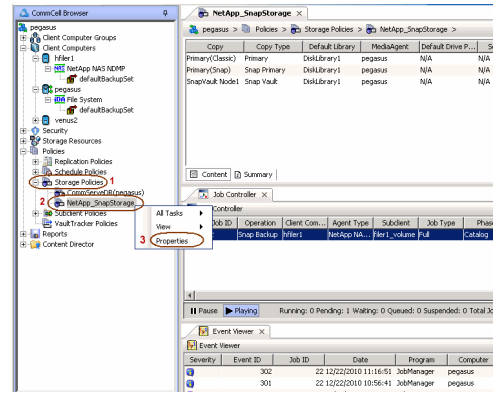
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.

2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.

3.
 - Select **Specify Source for Backup Copy**.
 - From the drop-down list, select the source copy to be used for performing the backup copy operation.

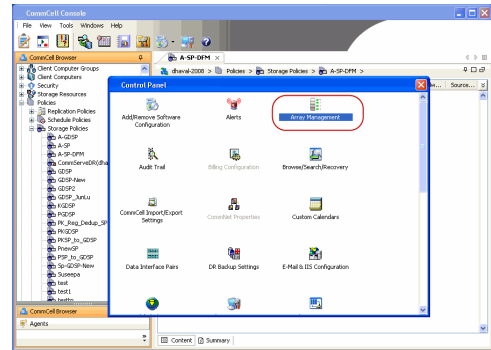


SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

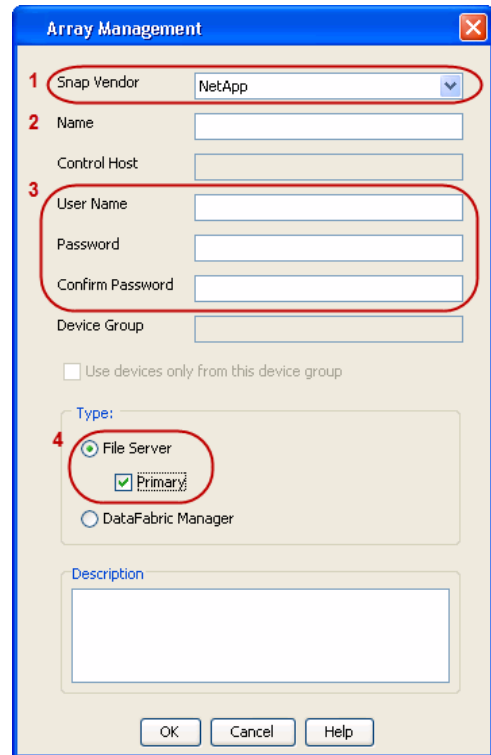
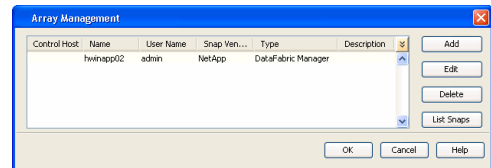


3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

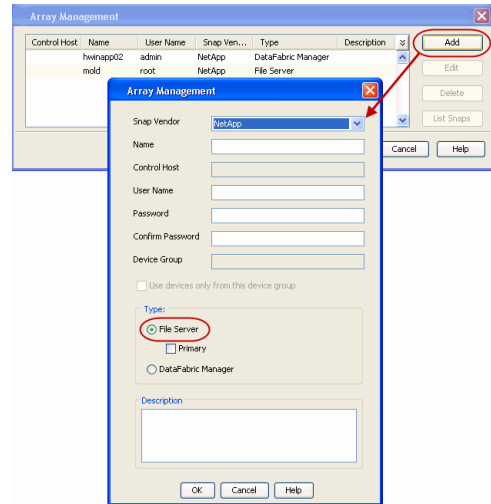
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



4.
 - Click **Add** again to enter the information for the secondary array.
 - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



SEE ALSO

Import Wizard Tool

Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

SnapProtect™ Backup - Data Replicator

◀ Previous Next ▶

PRE-REQUISITES

INSTALLATION

- The use of Data Replicator with the SnapProtect backup requires MediaAgent, File System iDataAgent, and ContinuousDataReplicator on the source, destination, and proxy computers.

The use of a proxy server to perform SnapProtect operations is supported when a hardware storage array is used for performing the SnapProtect backup.

- The operating system of the MediaAgent to be used for SnapProtect backup must be either the same or higher version than the source computer.

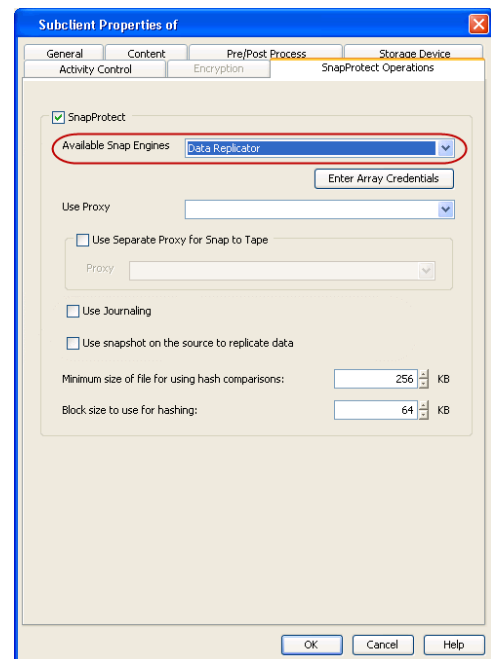
STORAGE POLICY REQUIREMENTS

The Primary Snap Copy to be used for creating the snapshot copy must be a disk library.

If the Storage Policy or the disk library being used by the subclient is updated, the subclient should be recreated.

SETUP THE ARRAY

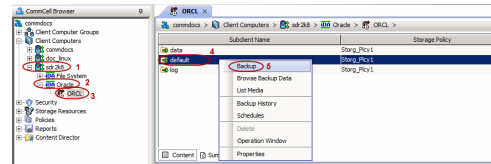
- From the CommCell Console, navigate to **<Client> | <Agent>**.
 - Right-click the subclient and click **Properties**.
- Click the **SnapProtect Operations** tab.
 - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down list.
 - Click **OK**.



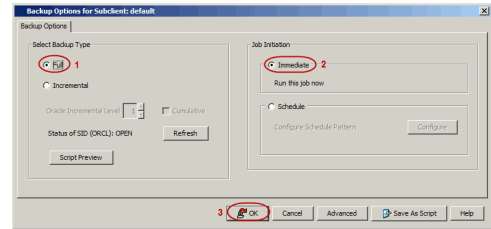
◀ Previous Next ▶

Getting Started Backup - Oracle iDataAgent

- From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **Oracle** | **<Instance>**.
 - Right-click the default subclient and click **Backup**.



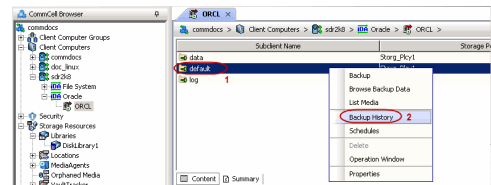
- Click **Full** as backup type and then click **Immediate**.
 - Click **OK**.



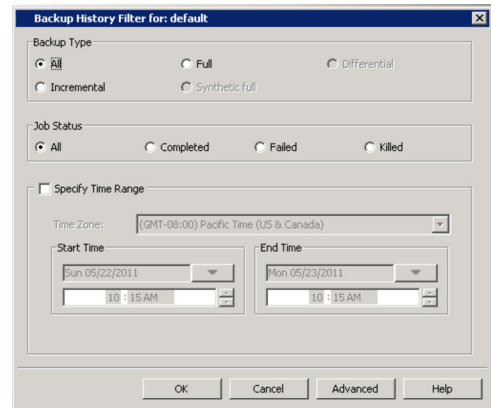
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



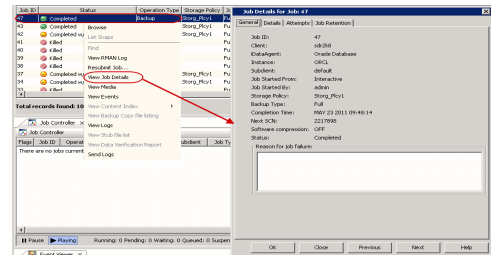
- Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.



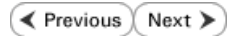
- Click **OK**.



- Right-click the job to:
 - Browse the database that was backed up.
 - View RMAN Logs.
 - Resubmit the job.
 - View job details.
 - View media associated with the job.
 - View events associated with the job.
 - View or send the log file that is associated with the job.



Getting Started - Vault/Mirror Copy



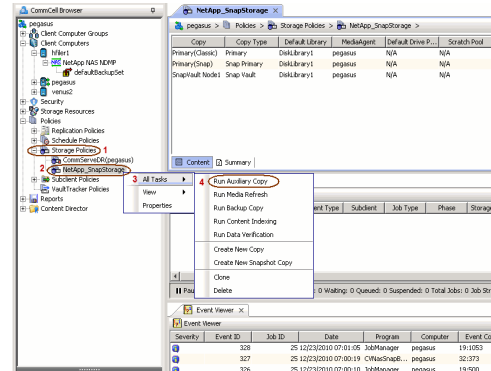
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** > to Continue.

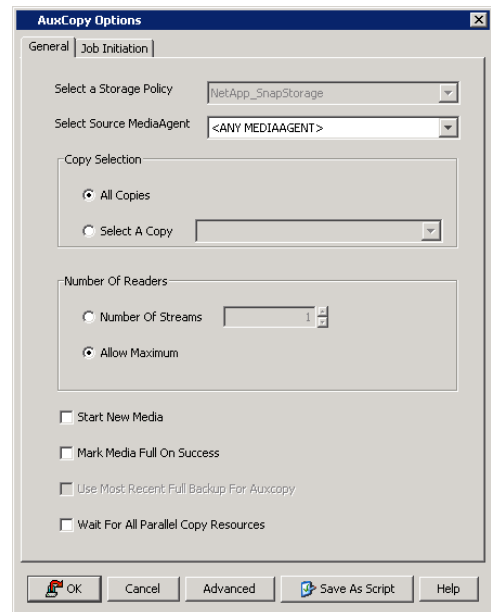
INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

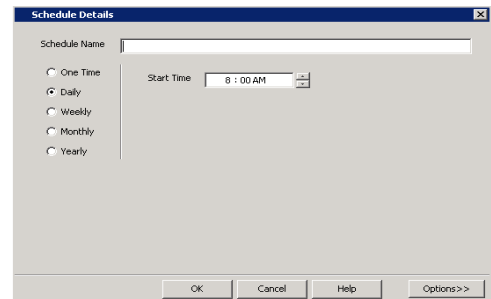


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.

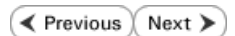


- Enter the schedule name and select the appropriate scheduling options.
 - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.



Getting Started - Snap Movement to Media

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

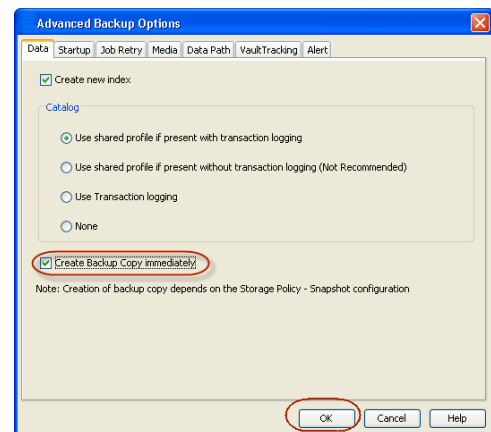
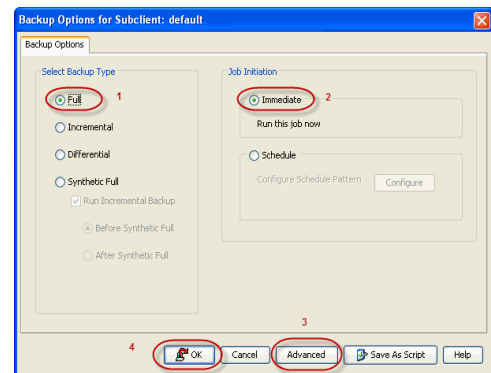
INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

1.
 - From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
 - Right click the default subclient and click **Backup**.
 - Select **Full** as backup type.
 - Click **Advanced**.

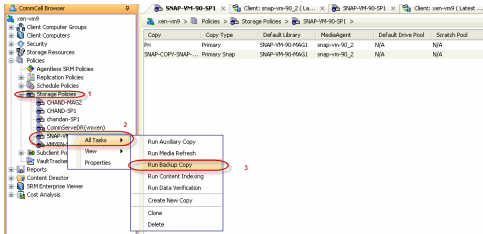
2.
 - Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



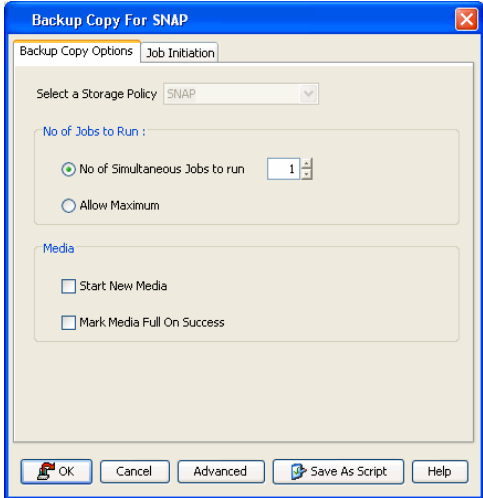
OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

1.
 - From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



Getting Started - Oracle Restore

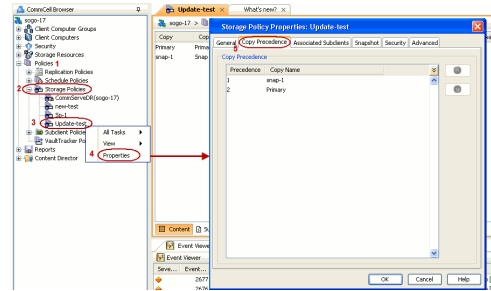


PERFORM A RESTORE

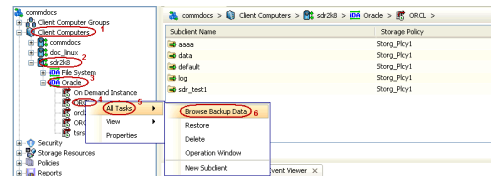
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring a database.

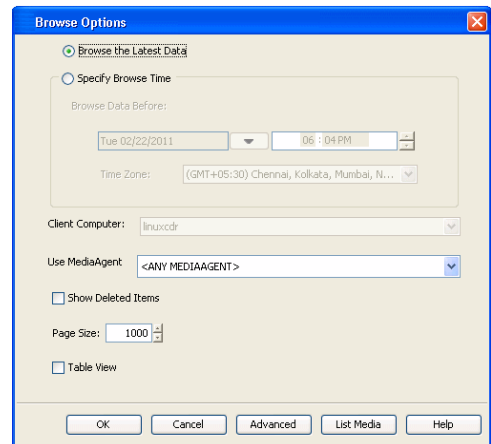
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
 - Click **OK**.



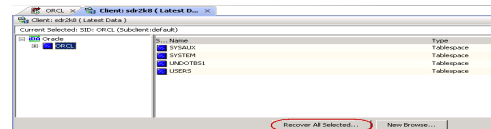
- From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
 - Right-click the **<Instance>**, point to **All Tasks**, and then click **Browse Backup Data**.



- Click **OK**.



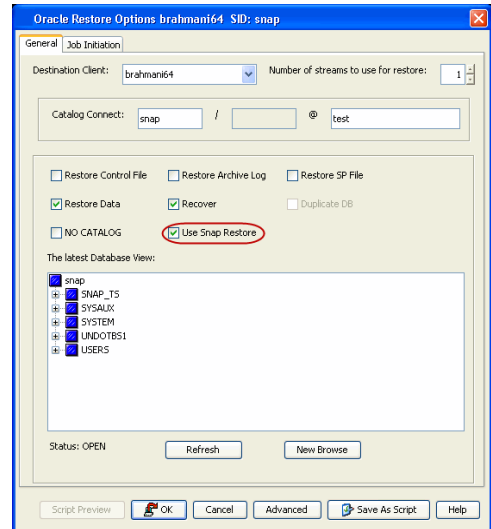
- In the right pane of the Browse window, click the **<Instance>** and select all the entities.
 - Click **Recover All Selected**.



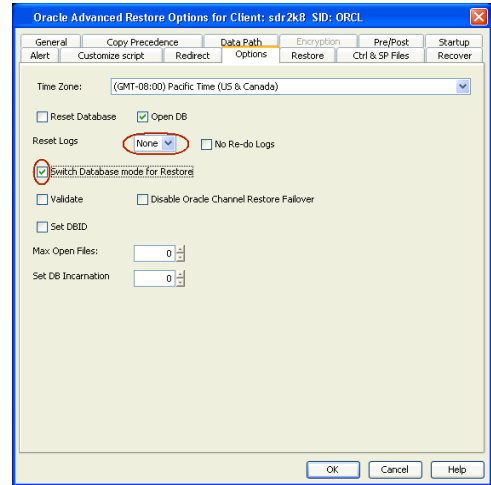
- Select the **Use Snap Restore** checkbox.
If you are restoring from a backup copy, clear the checkbox.
 - Click **Advanced**.

Verify that the Status of the database is displayed as **STARTED**; if necessary click the **Refresh** button to refresh the status.

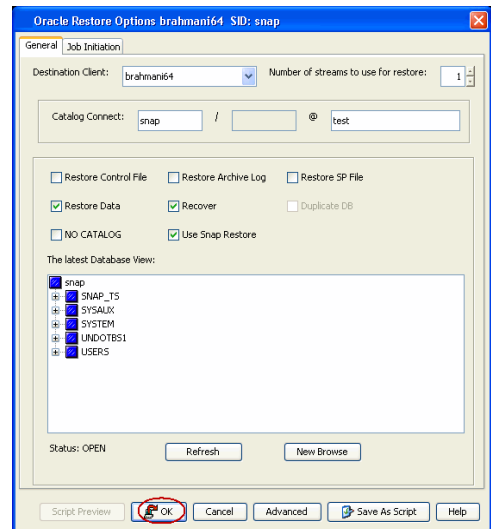
6.
 - Click the **Options** tab.
 - In the **Reset Logs** box, select **None**.
 - Select the **Switch Database mode for Restore** checkbox.
 - Click **OK**.



7. Click **OK**.

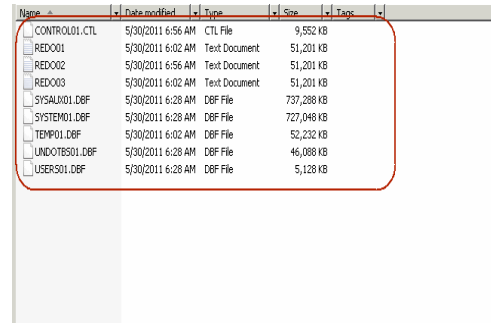


7. You can monitor the progress of the restore job in the **Job Controller**.



Job ID	Operation	Client Co.	Agent Type	Subagent	Job Type	Phase	Storage	PackageID	Status	Progress	Errors	Delta Reason	Description
8064	Install Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8065	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8066	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8067	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8068	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8069	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8070	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8071	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8072	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8073	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8074	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8075	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8076	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8077	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8078	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8079	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			
8080	Restore Snap	brahman164	Windows File Archiver	Snapshot	Full	Running	Snapshot	WMSnap	Running	100%			

8. Once the database is restored, verify that the restored database and log files are available in the original location.

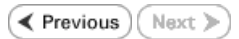


Name	Date modified	Type	Size	Tags
CONTROL01.CTL	5/30/2011 6:56 AM	CTL File	9,552 KB	
RED001	5/30/2011 6:02 AM	Text Document	51,201 KB	
RED002	5/30/2011 6:56 AM	Text Document	51,201 KB	
RED003	5/30/2011 6:02 AM	Text Document	51,201 KB	
SYSALW01.DBF	5/30/2011 6:28 AM	DBF File	737,288 KB	
SYSTEM01.DBF	5/30/2011 6:28 AM	DBF File	727,048 KB	
TEMP01.DBF	5/30/2011 6:02 AM	DBF File	52,232 KB	
UNDOTBS01.DBF	5/30/2011 6:28 AM	DBF File	46,088 KB	
USERS01.DBF	5/30/2011 6:28 AM	DBF File	5,128 KB	

CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



Getting Started - Microsoft SQL Server Deployment

◀ Previous Next ▶

WHERE TO INSTALL

Install the software on a computer on which SQL Server resides.

BEFORE YOU BEGIN

Download Software Packages

Download the latest software package to perform the install.

SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.

INSTALL THE MICROSOFT SQL SERVER /DATAAGENT

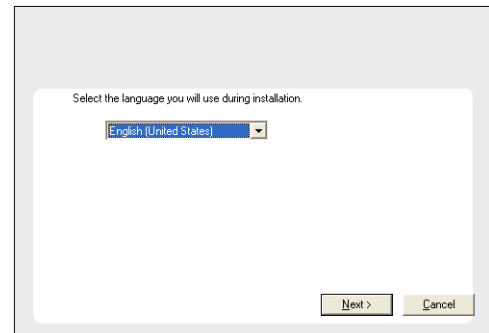
Use the following procedure to directly install the software from the installation package or a network drive.

1. Log on to the client computer as Administrator or as a member of the Administrator group on that computer.
2. Run **Setup.exe** from the **Software Installation Package**.

If you are installing on Windows Server Core editions, navigate to Software Installation Package through command line, and then run **Setup.exe**.

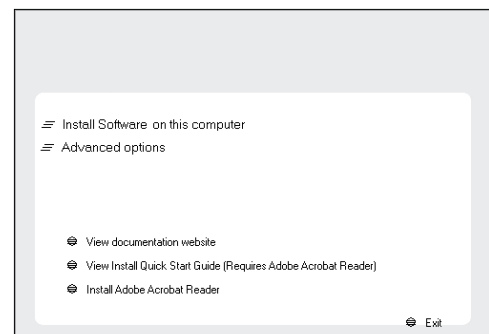
3. Select the required language.

Click **Next**.



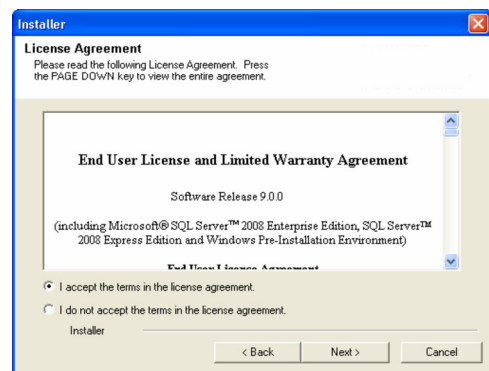
4. Select the option to install software on this computer.

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



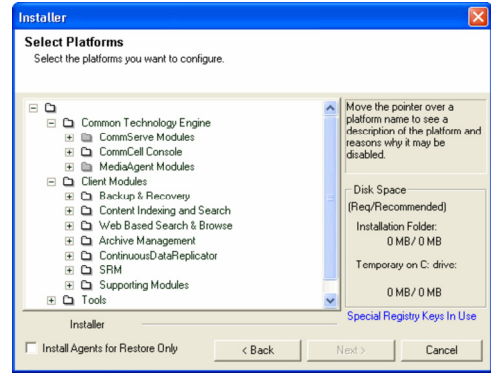
5. Select **I accept the terms in the license agreement**.

Click **Next**.



6.
 - Expand **Client Modules** | **Backup & Recovery** | **Database** and select **SQL Server iDataAgent**.

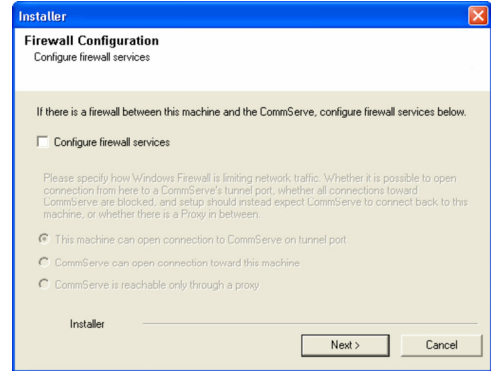
- Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
- Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
- Click **Next**.



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

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

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

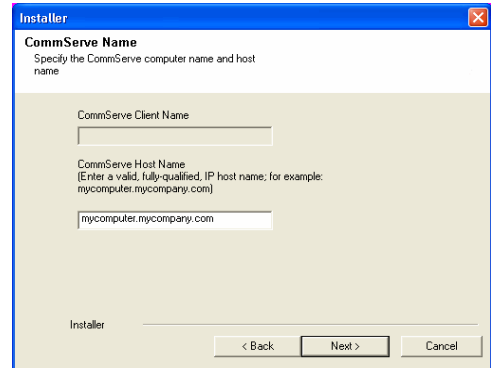


8. Enter the fully qualified domain name of the **CommServe Host Name**.

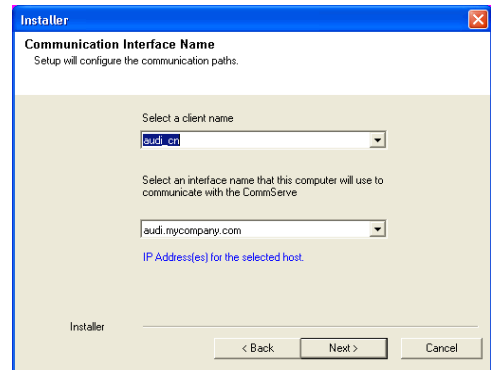
Click **Next**.

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

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



9. Click **Next**.



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

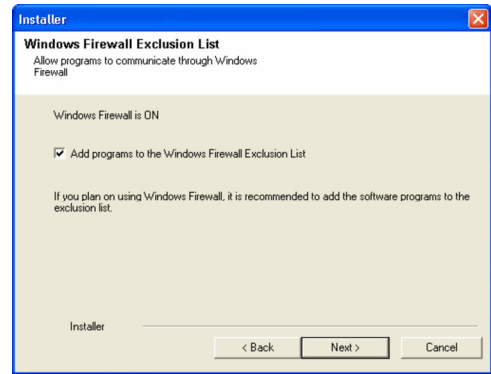
Click **Next**.

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

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

11. Click **Next**.

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



12. Verify the default location for software installation.

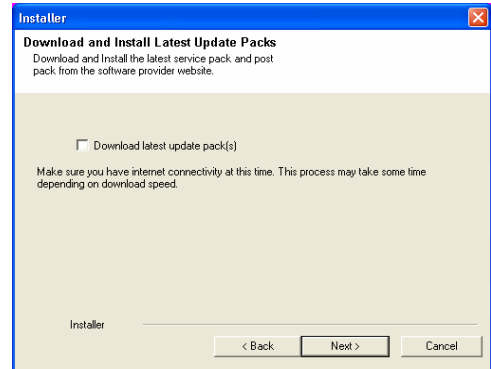
Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

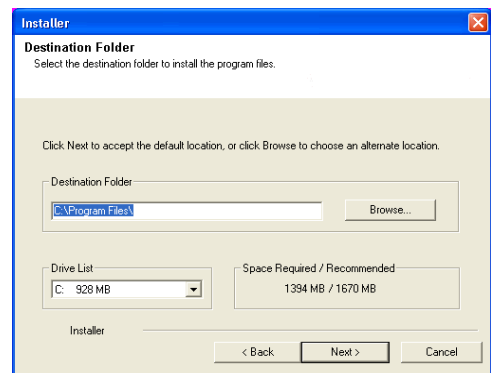
It is recommended that you use alphanumeric characters only.



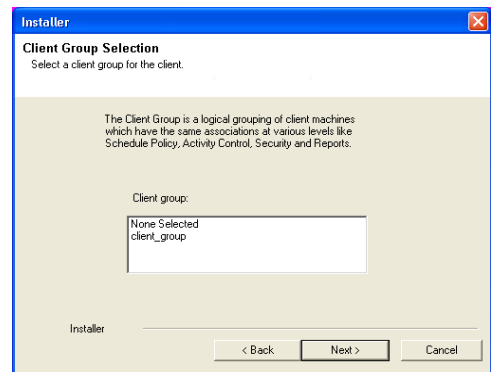
13. Select a Client Group from the list.

Click **Next**.

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



14. Click **Next**.



15. Select **Yes** to stop Removable Storage Services on the MediaAgent.
Click **Next**.

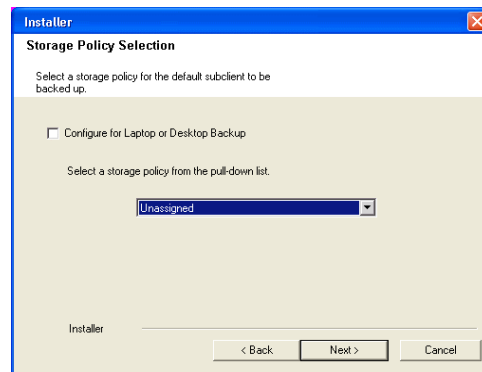
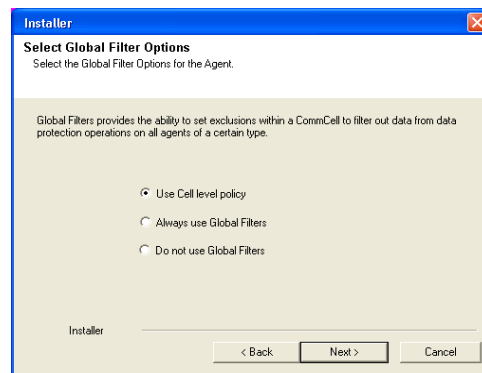
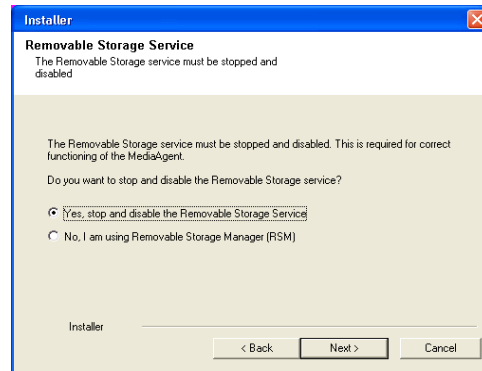
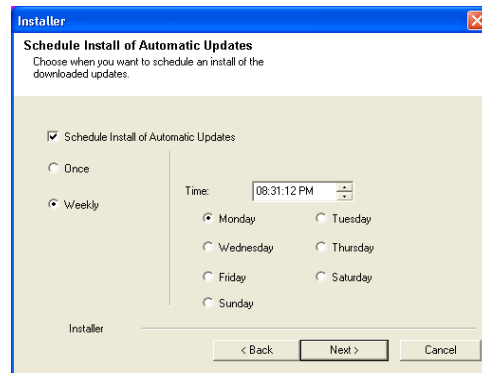
This prompt will not appear if Removable Storage Services are already disabled on the computer.

16. Click **Next**.

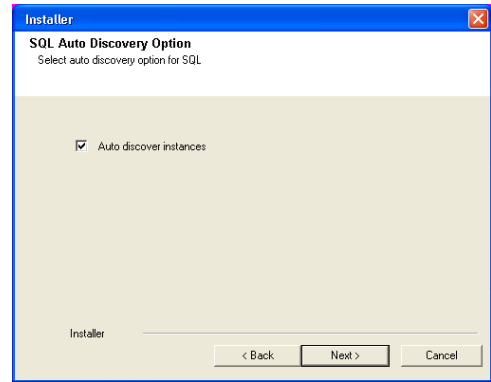
17. Select a **Storage Policy**.
Click **Next**.

18. Click **Next**.

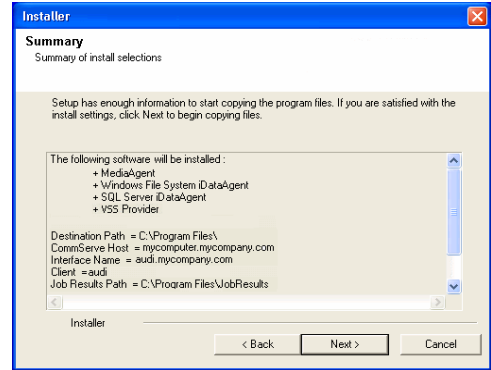
When **Auto Discover Instances** is enabled, new instances are automatically discovered every 24 hours.



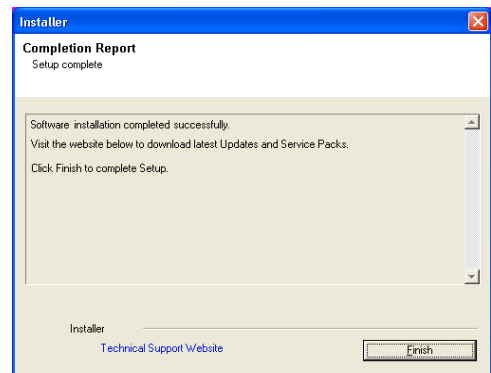
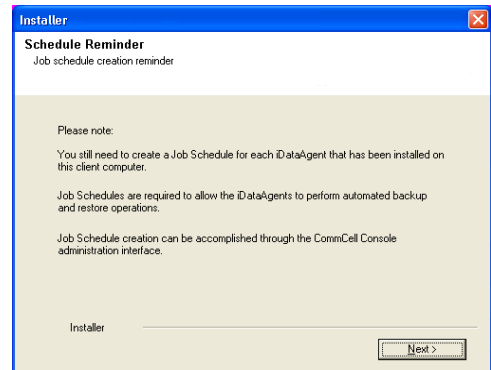
19. Click **Next**.



20. Click **Next**.



21. Click **Finish**.



Getting Started - Microsoft SQL Server Configuration



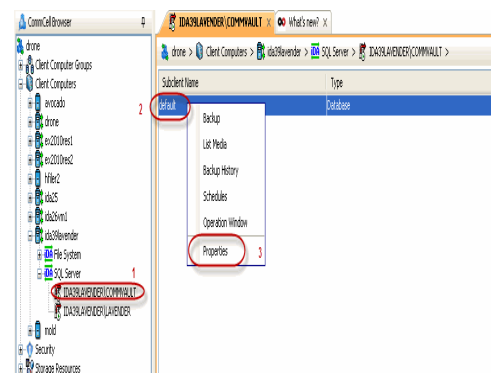
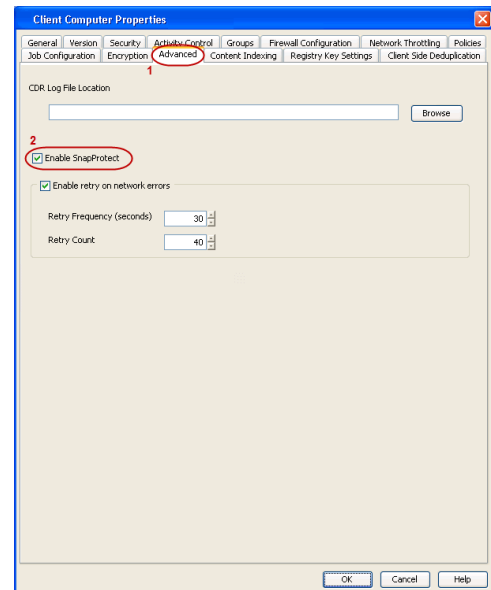
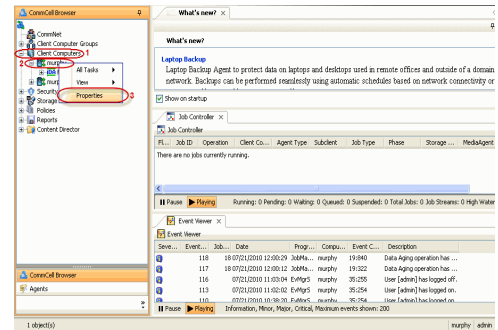
PRE-REQUISITES

- Prior to performing a SnapProtect backup, ensure that all the available hotfixes for Virtual Disk Service (VDS) and VSS are applied.
- When performing SnapProtect backup for a Windows Cluster, a proxy server must be used for performing backup and restore operations.
- SnapProtect backup on Windows supports basic disks.

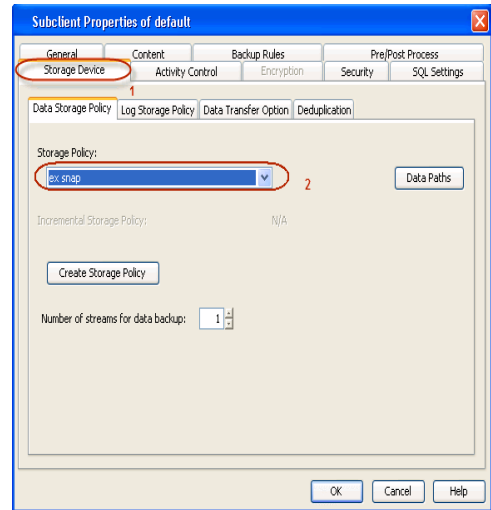
CONFIGURATION

Once the SQL Server *iDataAgent* has been installed, a SQL Server instance is automatically created. The following section provides the necessary steps required to associate a database to the subclient to perform your first SnapProtect backup.

- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.
- Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.
- From the CommCell Browser, navigate to **<Client>** | **SQL Server**.
 - Right-click the default subclient and click **Properties**.



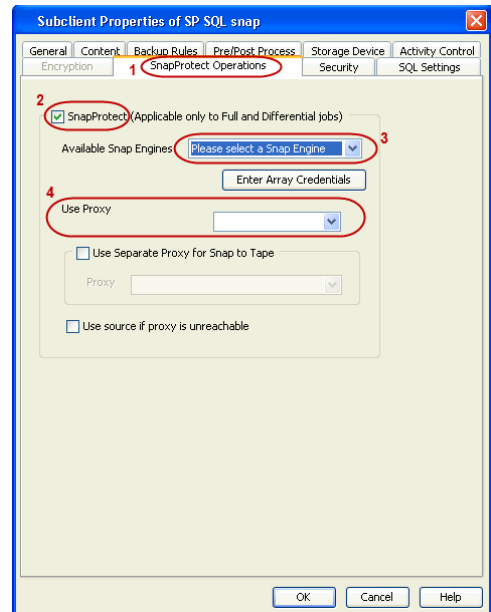
4.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.



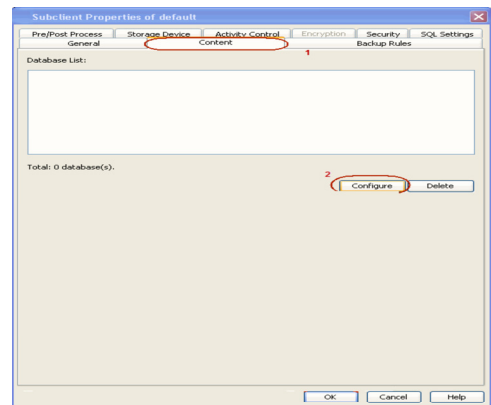
5.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy operations will be performed.

When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent. Select the MediaAgent from the **Proxy** list.



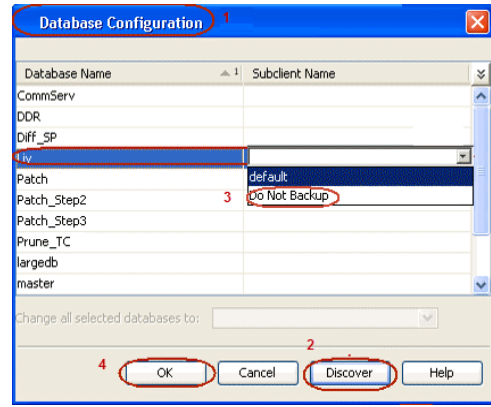
6.
 - Select the **Content** tab.
 - Click **Configure** to discover and associate databases to the subclient.



7.
 - Click **Discover**.
 - Select a database to be backed up from the **Database Name** column.
 - Databases that you want to exclude from backups can be assigned to **Do Not Backup** subclient. This data will never be backed up without manually initiating a backup.

You can select a range of databases and use **Change all selected databases to** drop-down list to assign a single subclient to all the databases.

- Click **OK**.
- Click **OK** from the **Subclient Properties** window.



SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

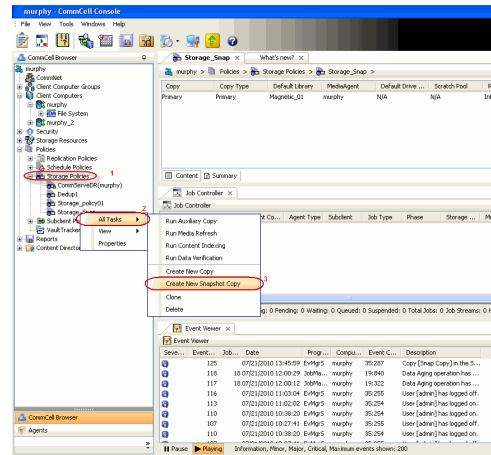
Click **Next** ➤ to Continue.

CREATE A SNAPSHOT COPY

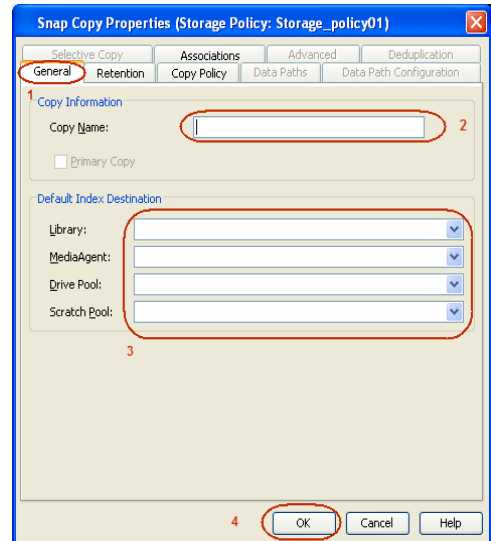


Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.



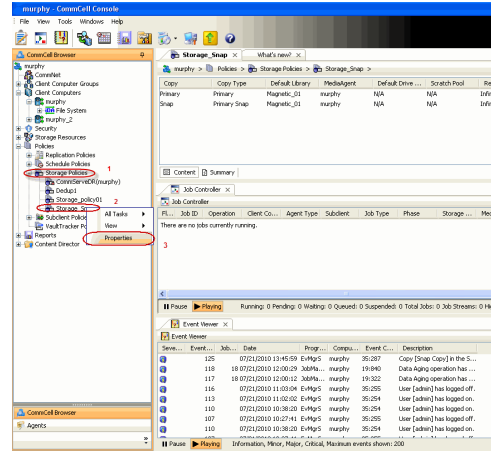
- Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



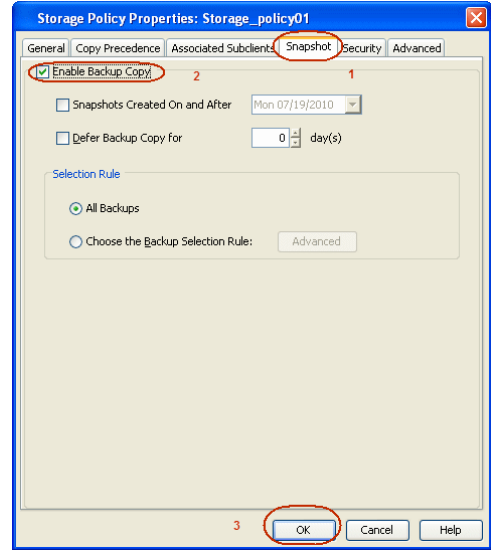
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



- Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



Storage Array Configuration

◀ Previous Next ▶

CHOOSE THE STORAGE ARRAY

HARDWARE STORAGE ARRAYS	SOFTWARE STORAGE ARRAY
3PAR	DATA REPLICATOR
DELL COMPELLENT	
DELL EQUALLOGIC	
EMC CLARIION, VNX	
EMC SYMMETRIX	
FUJITSU ETERNUS DX	
HITACHI DATA SYSTEMS	
HP EVA	
IBM SVC	
IBM XIV	
LSI	
NETAPP	
NETAPP WITH SNAPVAULT /SNAPMIRROR	
NIMBLE	

◀ Previous Next ▶

SnapProtect™ Backup - 3PAR

◀ Previous Next ▶

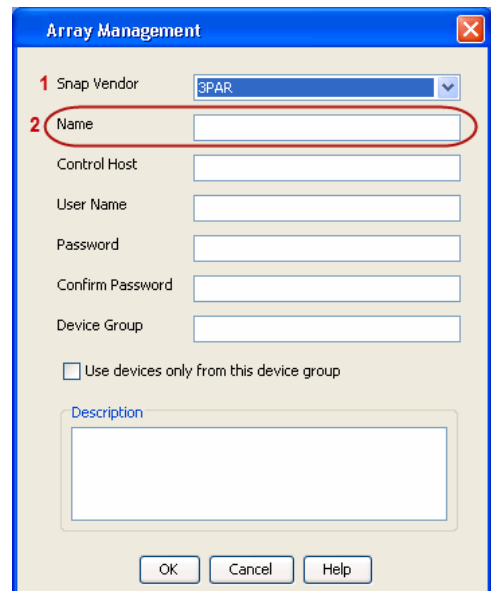
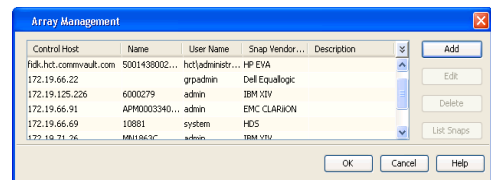
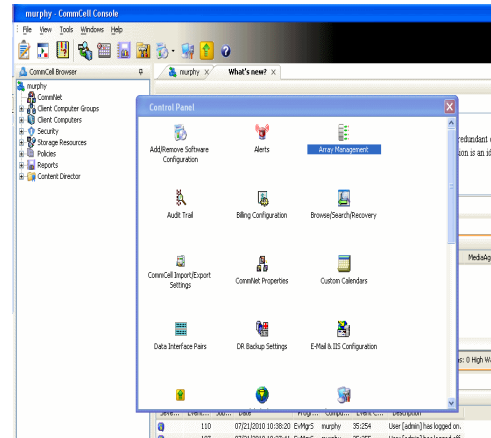
PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
 - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

where $\text{DevID.substr}(12,4)$ is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(12,4)$ is 0B95

After adding all the values, the resulting array name is 2FF70002AC00B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

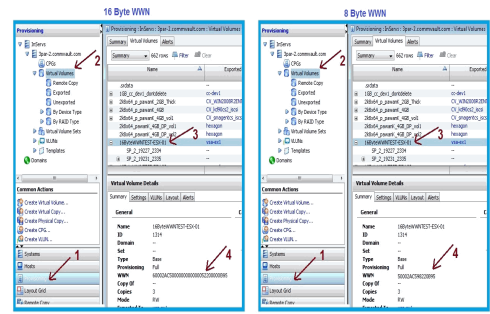
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(26,6)$ is 000B95

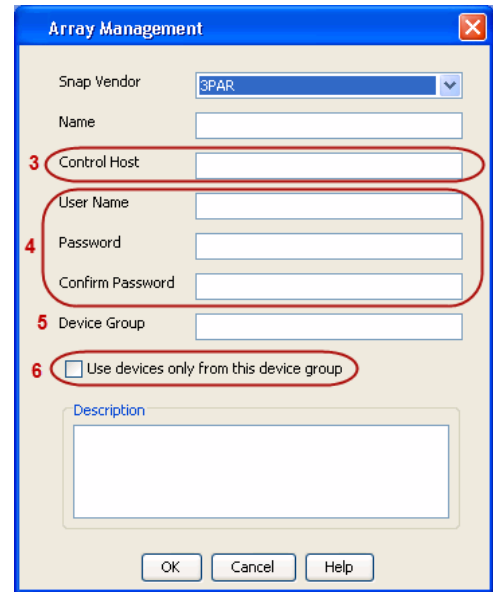
After adding all the values, the resulting array name is 2FF70002AC000B95.



- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - Dell Compellent

◀ Previous Next ▶

PRE-REQUISITIES

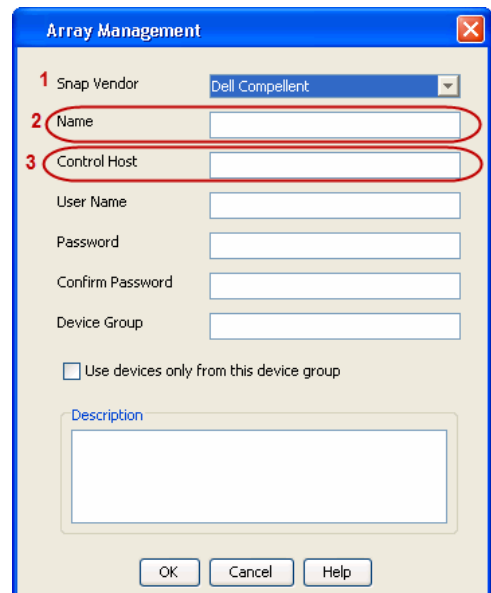
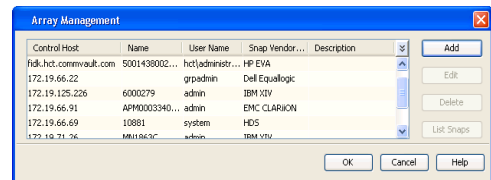
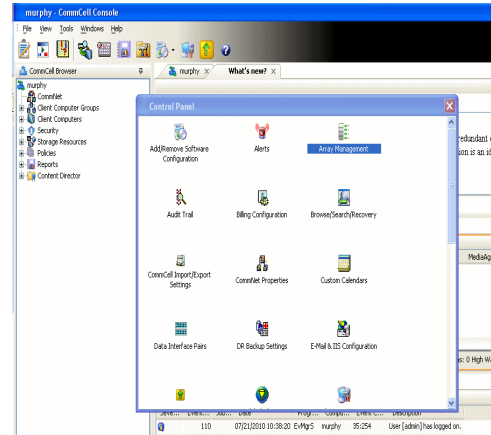
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **Dell Compellent** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** and **Control Host** fields.

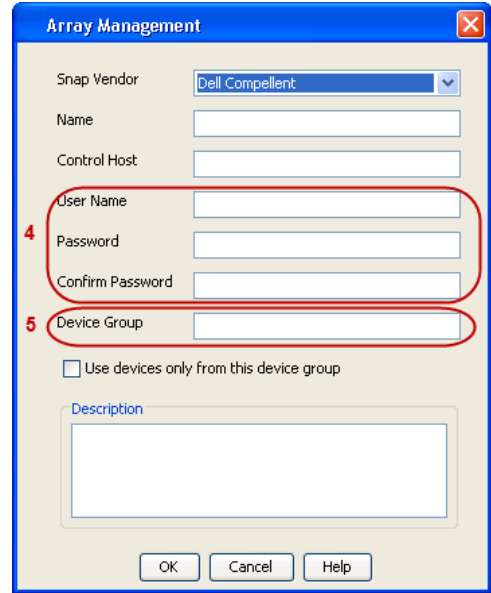
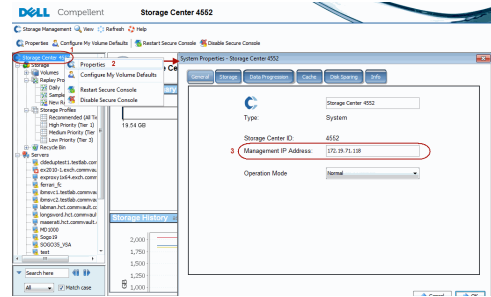
The Management IP address is also referred as the Storage Center IP address.



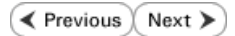
For reference purposes, the screenshot on the right shows the Storage Center Management Console of the Dell Compellent storage device displaying the Management IP address.

4.

- Enter the user access information of the application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, type *none* as this array does not use device groups for snapshot operations.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - Dell EqualLogic



PRE-REQUISITIES

WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

FIRMWARE VERSION

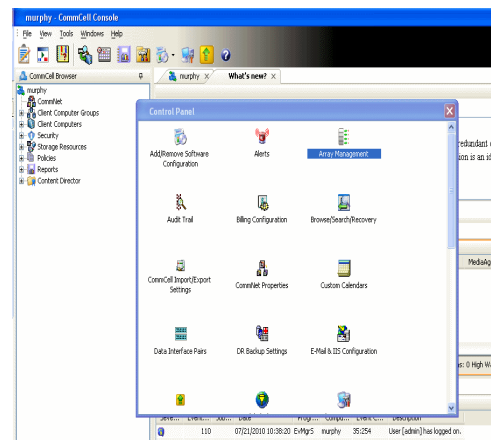
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

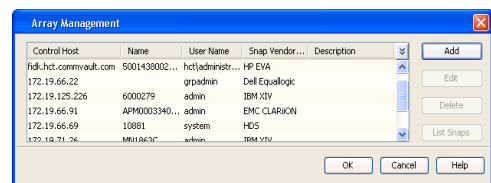
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

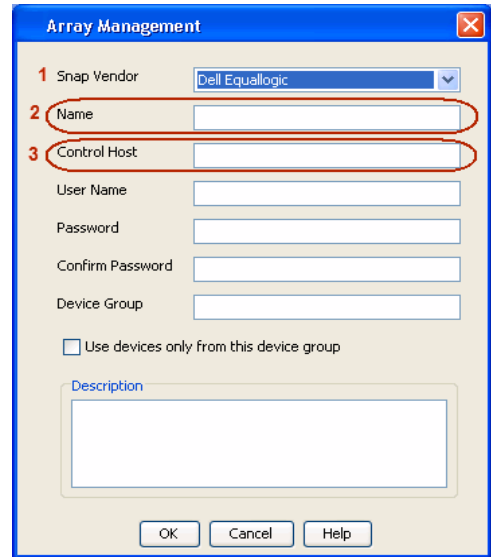


2. Click **Add**.

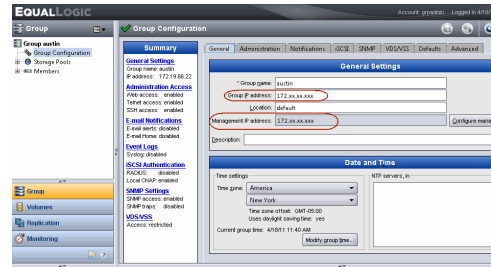


3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

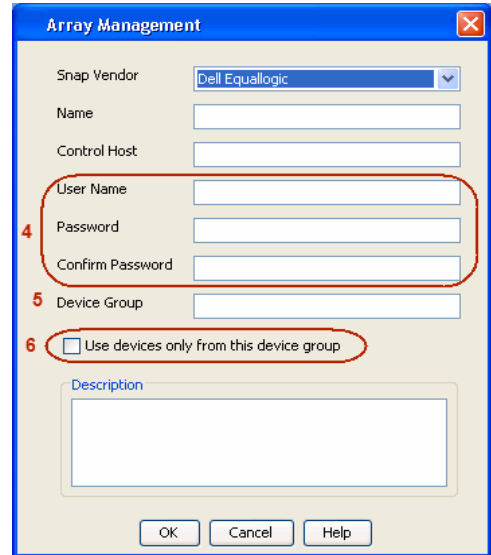
No entry is required in the **Name** field if there is no Management IP address configured.
 - Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
 - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
 - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
 - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous Next ▶

PRE-REQUISITES

LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

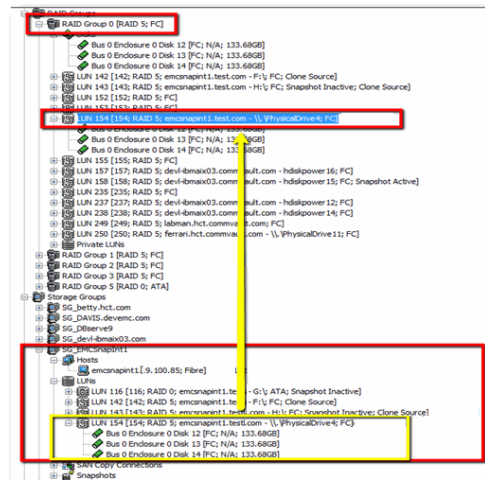
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

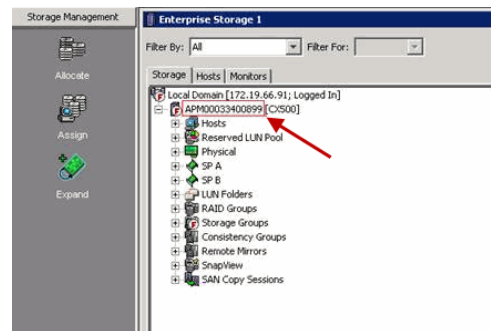
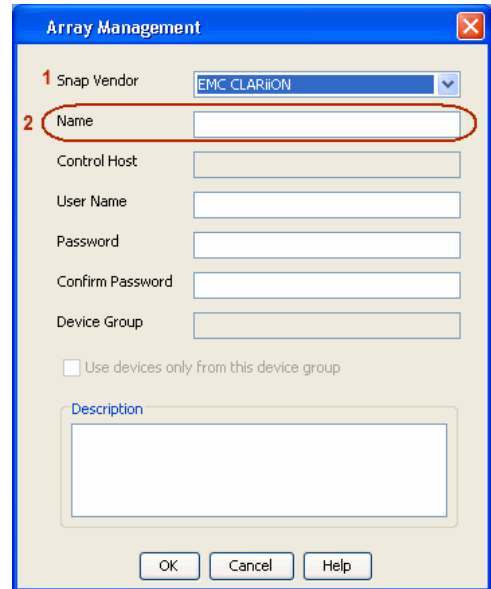
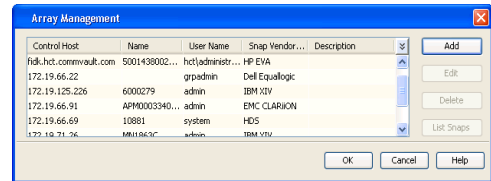
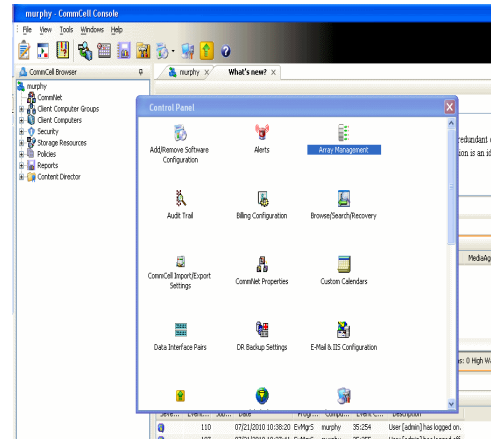
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
 - Specify the serial number of the array in the **Name** field.

For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.

- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



Array Management ✕

Snap Vendor:

Name:

Control Host:

User Name:

3 Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - EMC Symmetrix

◀ Previous Next ▶

PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

LOAD THE SYMMETRIX DATABASE

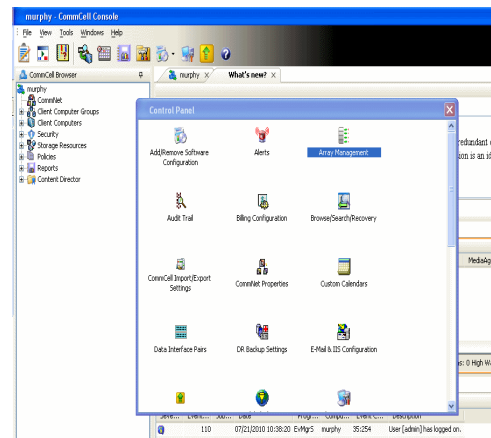
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

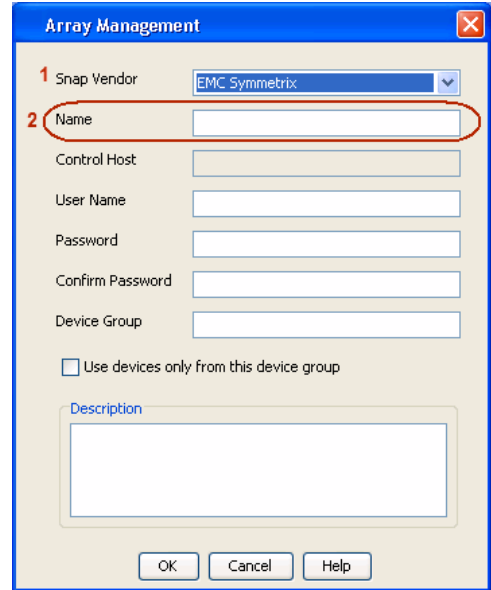
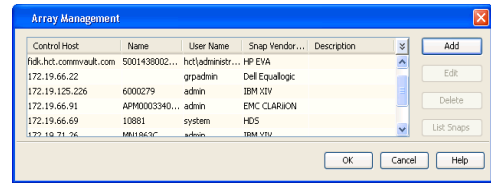
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

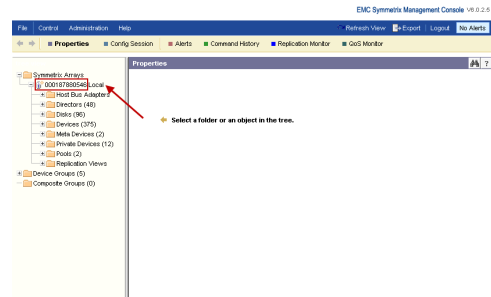


2. Click **Add**.

3.
 - Select **EMC Symmetrix** from the **Snap Vendor** list.
 - Specify the **Symm ID** of the array in the **Name** field.

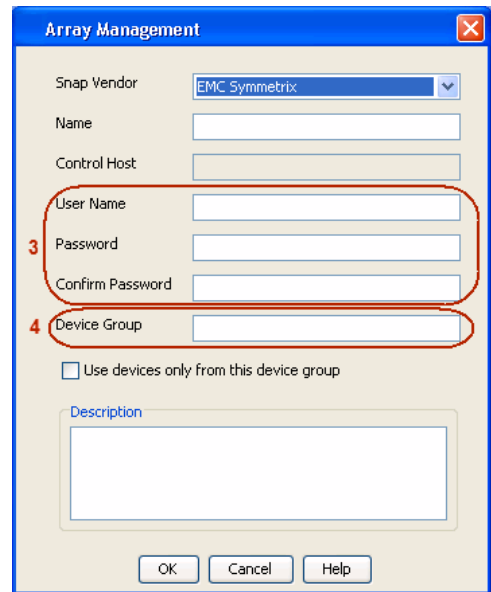


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.
If you do not specify a device group, the default device group will be used for snapshot operations.
 - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).



SnapProtect™ Backup - Fujitsu ETERNUS DX

◀ Previous Next ▶

PRE-REQUISITES

- Local Copy license for Snap and Clone.
- Thin Provisioning license.
- Ensure that all members in the Fujitsu array are running firmware version V10L22-1000 or higher.
- Enable SMI-S on the storage array.
- Create a Host Affinity group for the proxy computer.
- If using SnapOPC, ensure to create a SDV and SDPV volumes.

CONFIGURE DESTINATION VOLUMES

- Source and destination volumes should be pre-paired before performing any snapshot operation. For EC snapshots (clone), pre-paired sessions should be in active state.
- To pre-pair source and destination volumes, install the ETERNUS SF Express Manager software version 14.2A or higher.
- Forbid Advanced Copy and Encrypted volumes are not supported.
- Depending on the type of snapshot being used, review the following for the creation of destination volumes:

FOR SNAP SNAPSHOTS

If pre-paired sessions are not available, SnapOPC snapshots use any available SDV volumes as their destination volumes. If you need to create a new SDV volume, ensure that the SDV volume is of equal size to the source volume.

FOR CLONE SNAPSHOTS

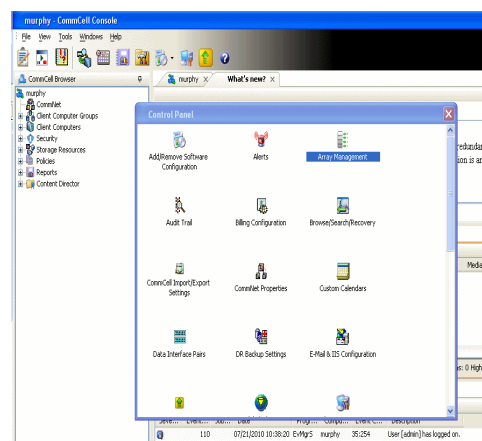
If pre-paired sessions are not available, destination volumes are automatically created for clone snapshots. If a non-existing device group is specified during array configuration in the CommCell Console, a destination volume is created based on the source volume type. However, if a valid device group is specified, the following destination volumes are created depending on the device group type:

- A Thin Provisioning volume is created if the device group is a Thin Provisioning pool.
- A standalone volume is created if the device group is a RAID group.

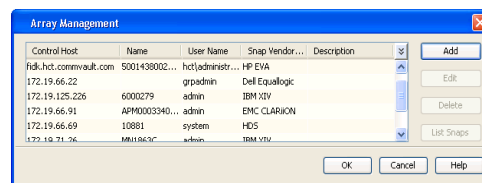
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

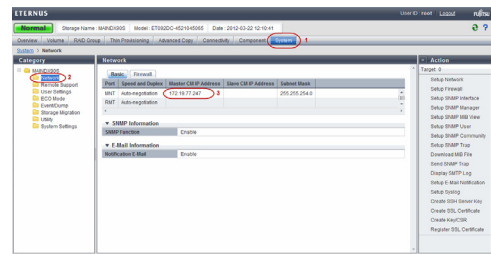
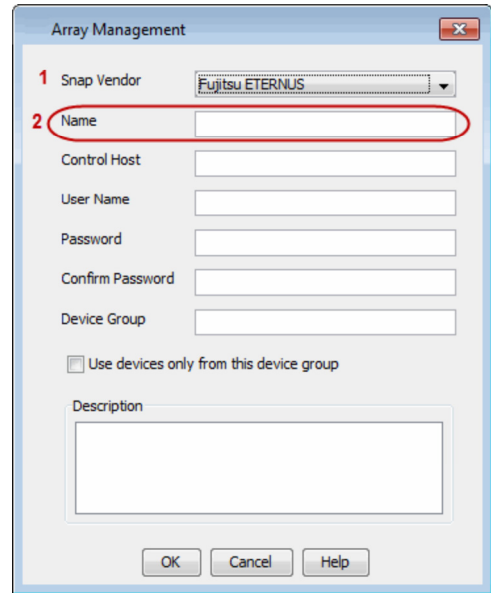


2. Click **Add**.

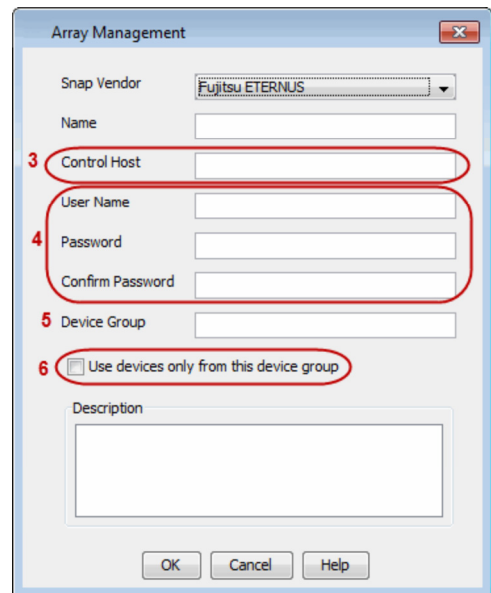


3.
 - Select **Fujitsu ETERNUS** from the **Snap Vendor** list.
 - Specify the CM IP Address of the array in the **Name** field.

For reference purposes, the screenshot on the right shows the CM IP Address for the Fujitsu storage device.



4.
 - Enter the CM IP Address of the array in the **Control Host** field.
 - Enter the access information of a user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the RAID group or Thin Provisioning group created on the array to be used for clone operations. Device groups are not applicable for Snap snapshots.
 - Select the **Use devices only from this device group** option to use only the snapshot devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - Hitachi Data Systems

◀ Previous Next ▶

PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
 - COW pools
 - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

ADDITIONAL REQUIREMENTS FOR VMWARE

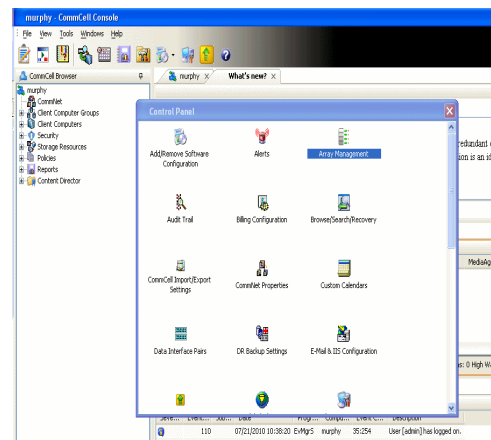
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server iDataAgent client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server iDataAgent client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

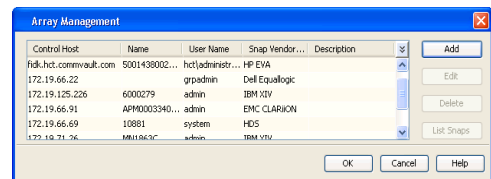
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

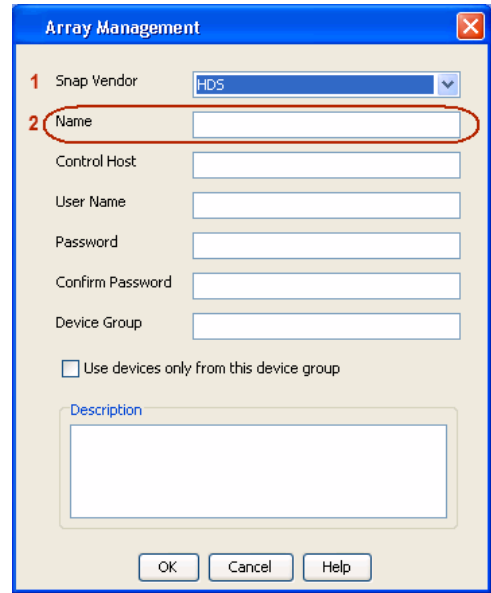
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



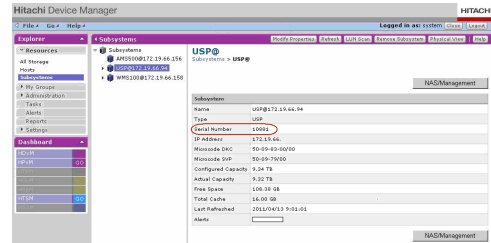
2. Click **Add**.



3.
 - Select **HDS** from the **Snap Vendor** list.
 - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



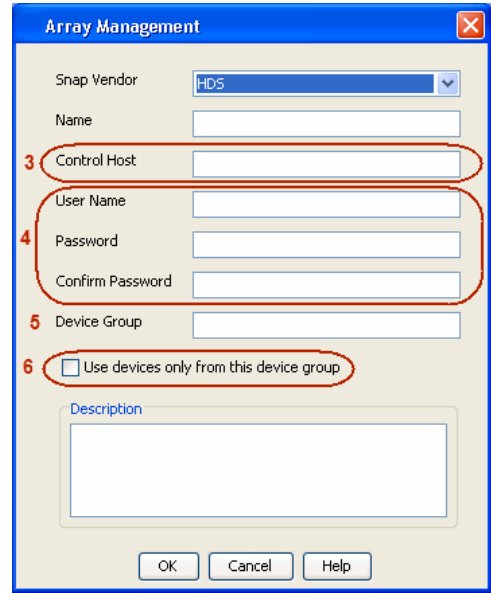
4.
 - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:

<COW_POOL_ID>-<LABEL> or <LABEL>-<COW_POOL_ID>

where <COW_POOL_ID> (for COW job) should be a number. This parameter is required.

<LABEL> (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - HP StorageWorks EVA

◀ Previous Next ▶

SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

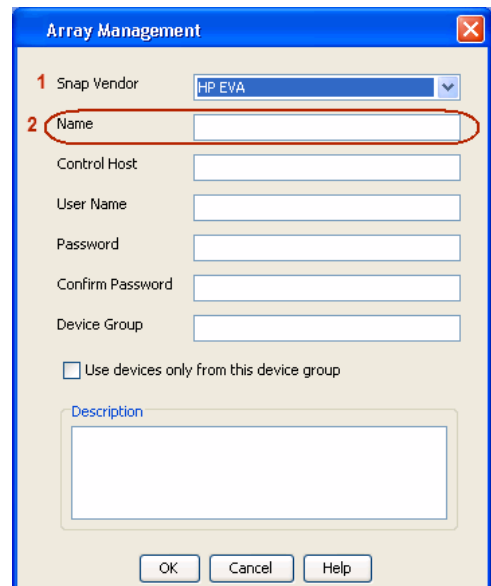
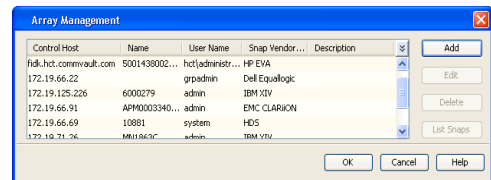
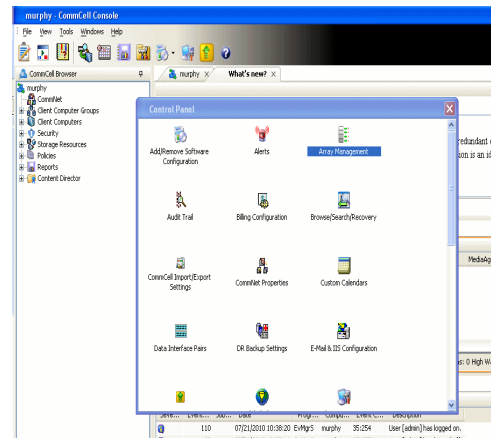
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin folder to discover the HP-EVA arrays.
3. Use the CLIRefreshTool.bat tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin folder.

SETUP THE ARRAY INFORMATION

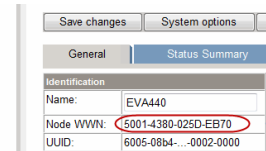
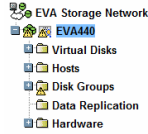
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
2. Click **Add**.
3.
 - Select **HP EVA** from the **Snap Vendor** list.
 - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

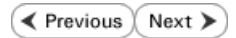
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



4.
 - Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous Next ▶

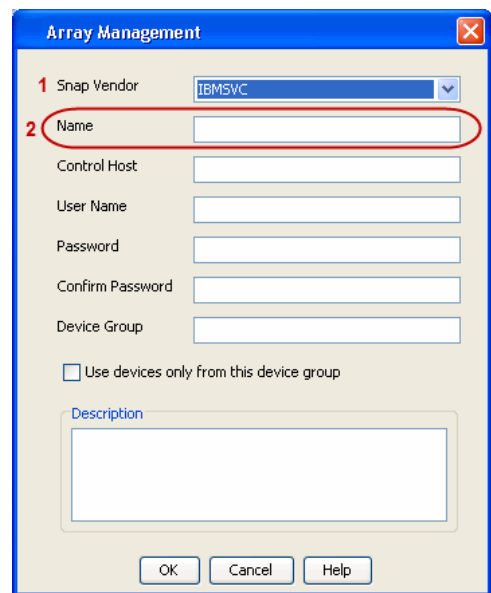
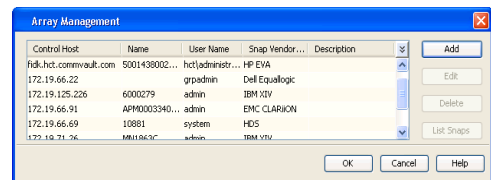
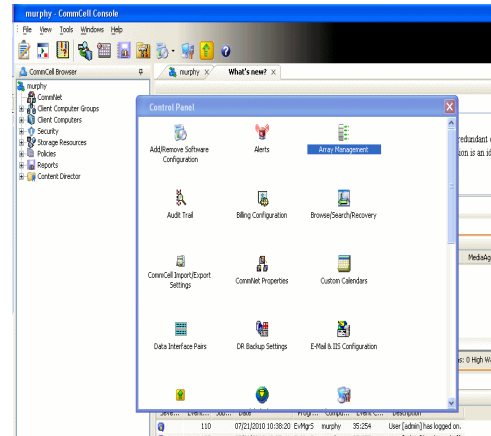
PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

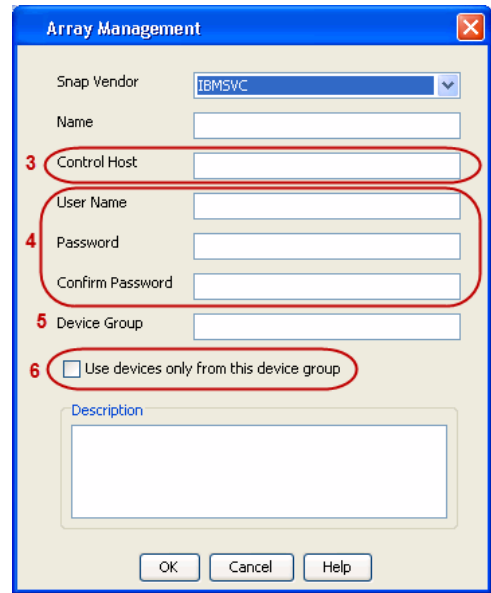
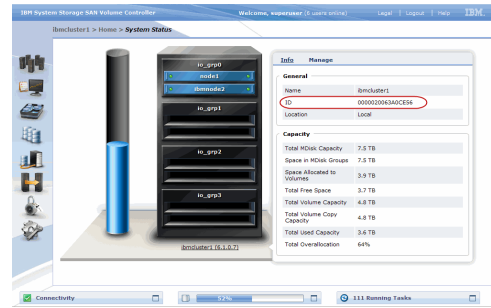
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM XIV



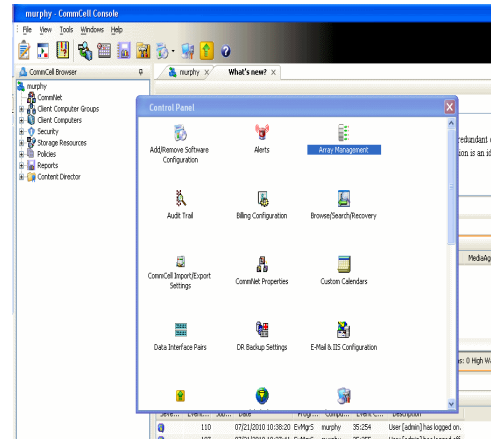
PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

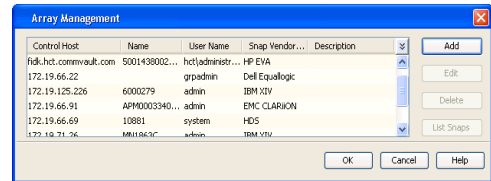
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

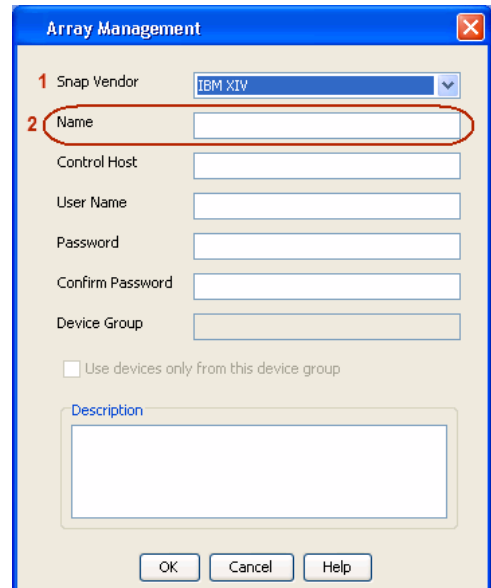
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

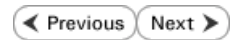
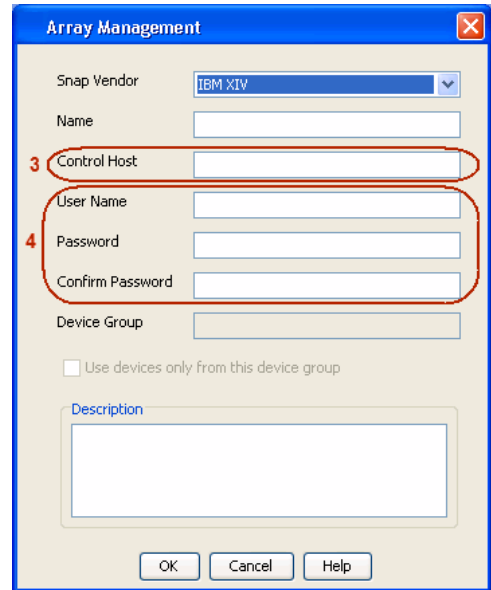
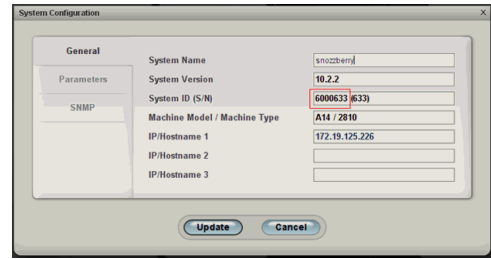


3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

- 4.
- Enter the IP address or host name of the array in the **Control Host** field.
 - Enter the user access information of the application administrator in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - LSI

◀ Previous Next ▶

PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
 - SMIS server through TCP/IP network.
 - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

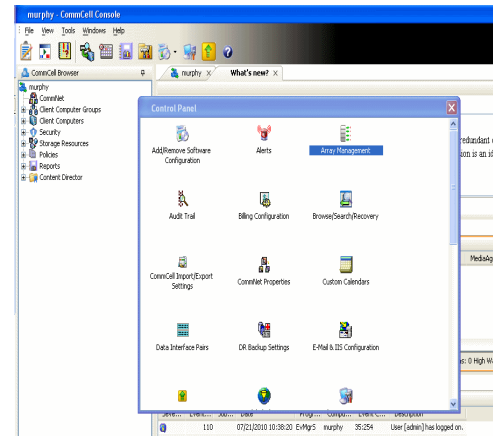
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

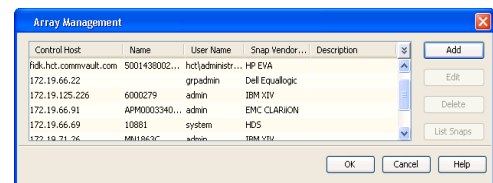
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

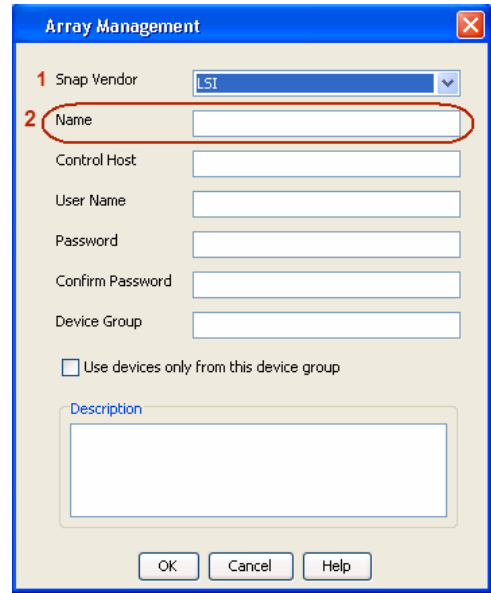
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

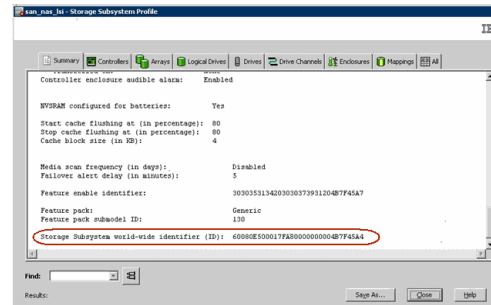


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

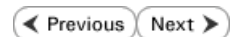
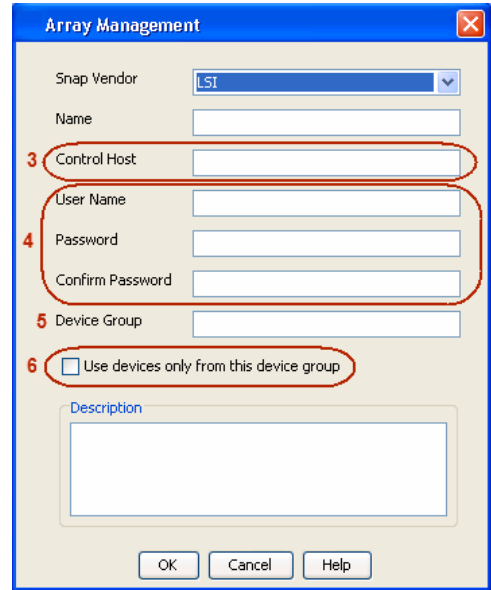
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



4.
 - Specify the name of the device manager server where the array was configured in the **Control Host** field.
 - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

If you specify None in the **Device Group** field but do not have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - NetApp



PREREQUISITES

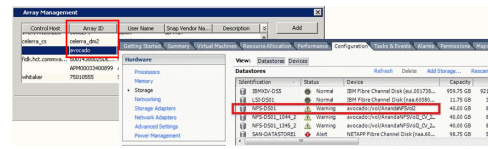
LICENSES

- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

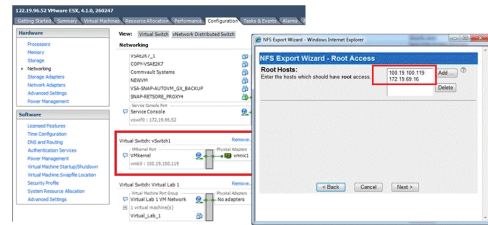
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.



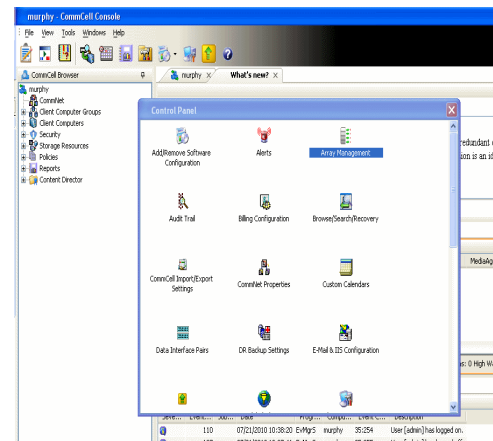
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



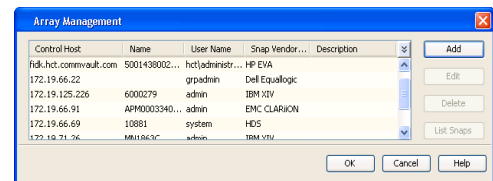
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the file server in the **Name** field.
 - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: []

Control Host: []

User Name: []

Password: []

Confirm Password: []

Device Group: []

Use devices only from this device group

Description: []

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous Next ▶

OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

PREREQUISITES

LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:


```
options snapvault.enable on
```
3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:


```
options snapvault.access host=secondary_filer1, secondary_filer2
```
4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:


```
options snapvault.access host=primary_filer1, primary_filer2
```

INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
 - Discover storage devices
 - Add Resource Pools to be used for the Vault/Mirror storage provisioning

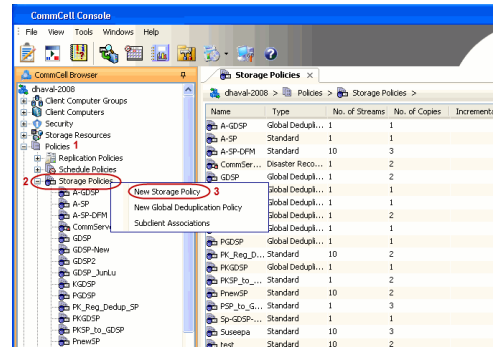
CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

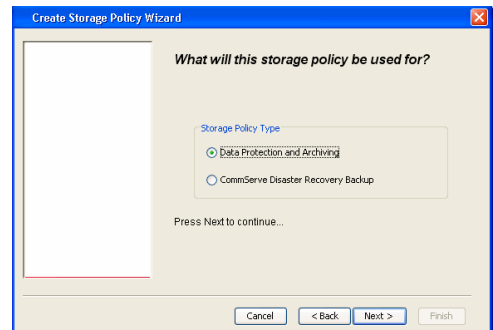
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

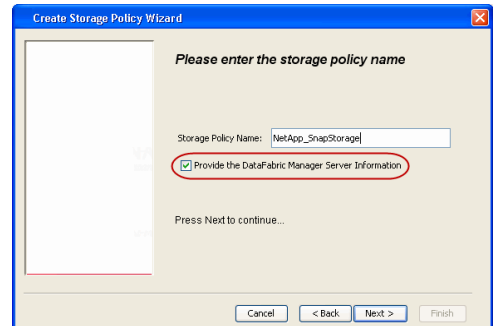
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



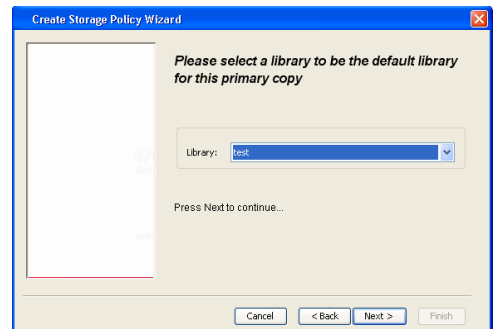
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.

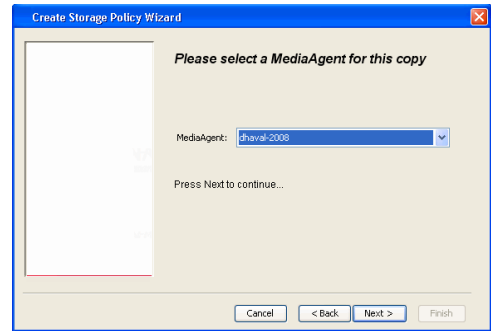
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

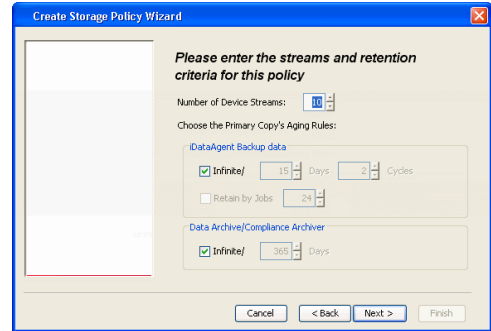


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

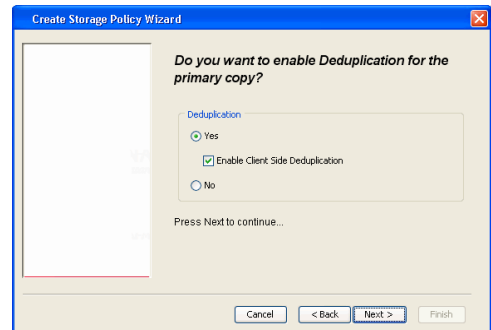
6. Click **Next**.



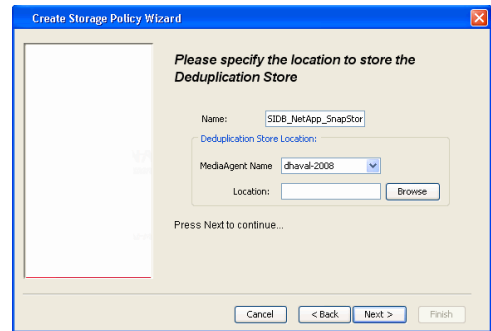
7. Click **Next**.



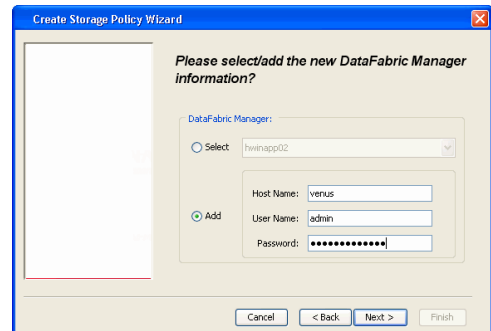
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

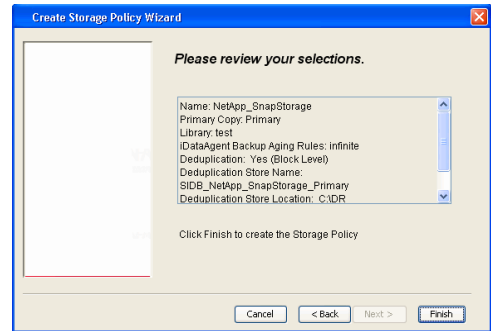


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



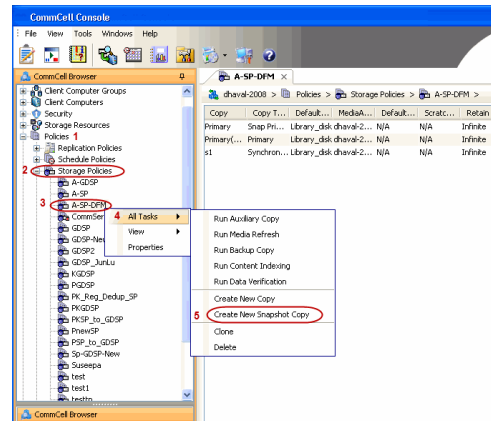


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

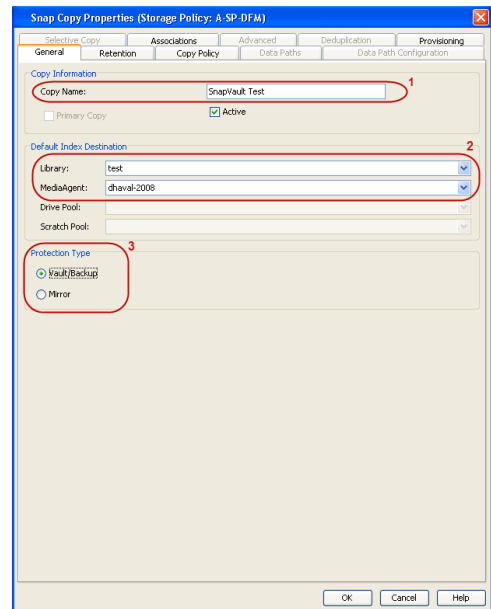
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
 - Enter the **Copy Name**.
 - Select the **Library** and **MediaAgent** from the drop-down list.
 - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

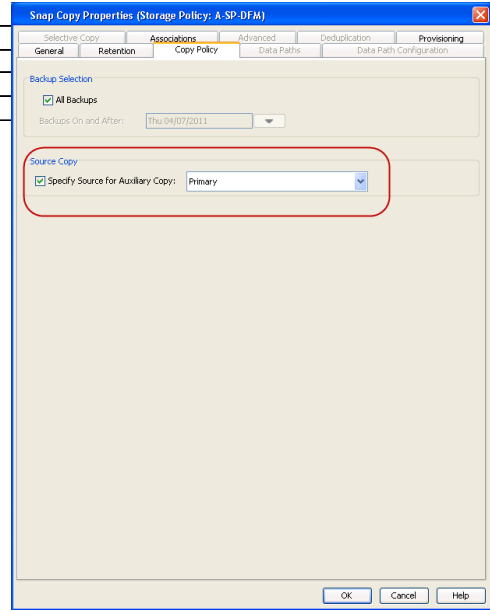


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

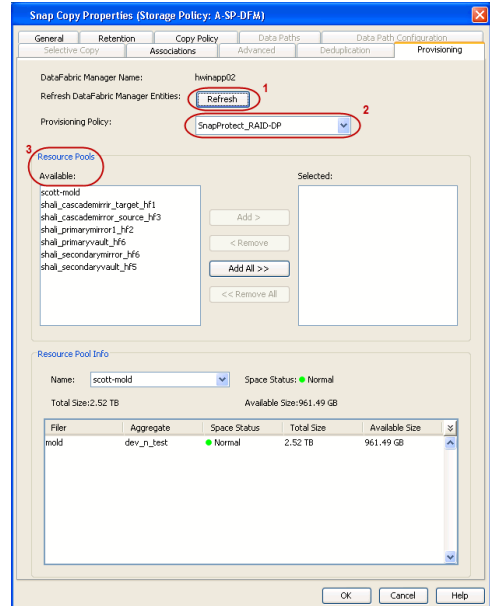
TOPOLOGY	SOURCE COPY
----------	-------------

Primary-Mirror	Primary
Primary-Mirror-Vault	Mirror
Primary-Vault	Primary
Primary-Vault-Mirror	Vault
Primary-Mirror-Mirror	Mirror



- Click the **Provisioning** tab.
 - Click **Refresh** to display the DFM entities.
 - Select the **Provisioning Policy** from the drop-down list.
 - Select the **Resource Pools** available from the list.
 - Click **OK**.

The secondary snapshot copy is created.



- If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:


```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

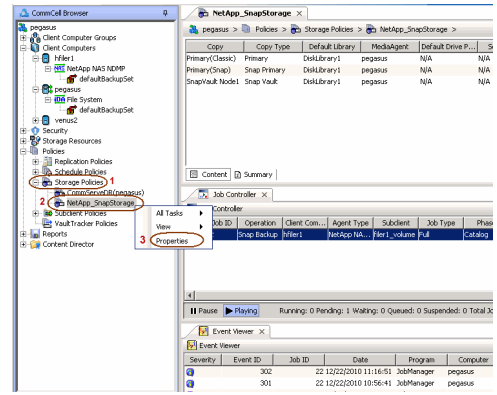
It is recommended that you perform this operation on all nodes in the P-M-V topology.

CONFIGURE BACKUP COPY

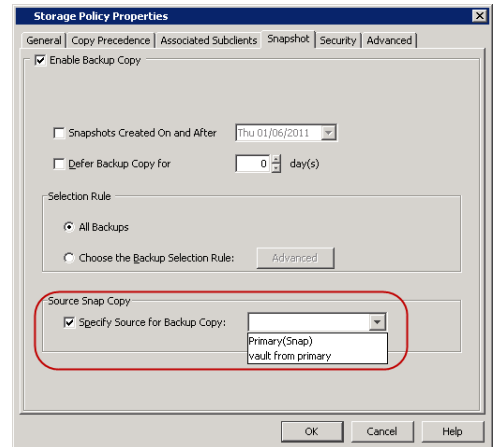
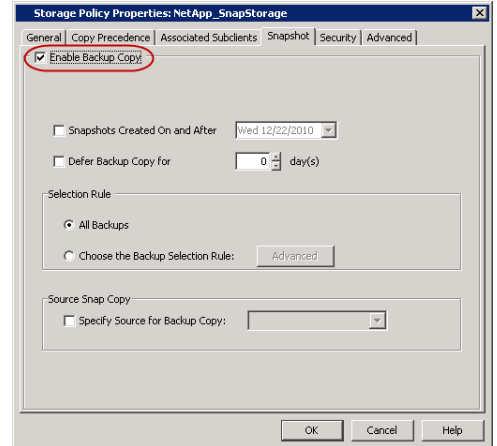
Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.

2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



3.
 - Select **Specify Source for Backup Copy**.
 - From the drop-down list, select the source copy to be used for performing the backup copy operation.



SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

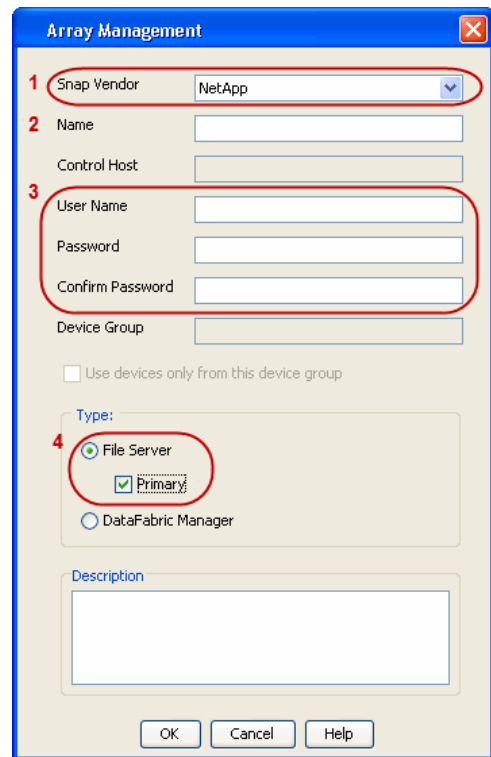
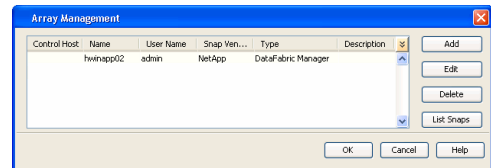
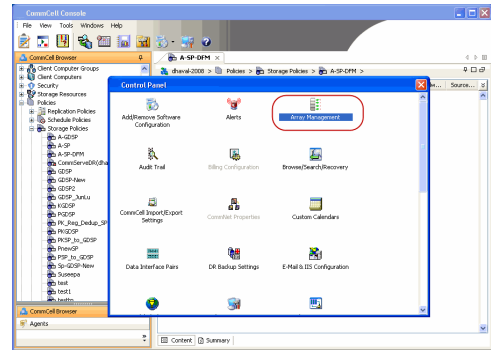
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

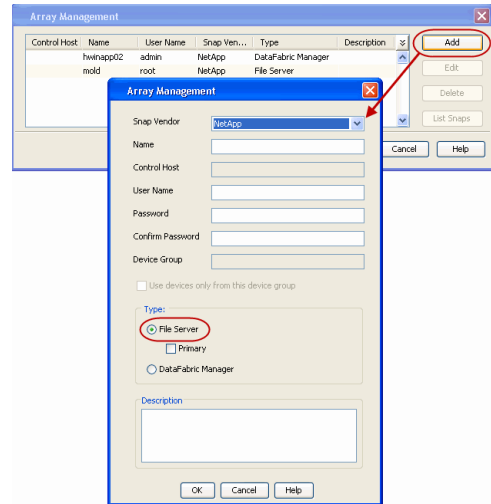
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

4.
 - Click **Add** again to enter the information for the secondary array.
 - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.





SEE ALSO

Import Wizard Tool

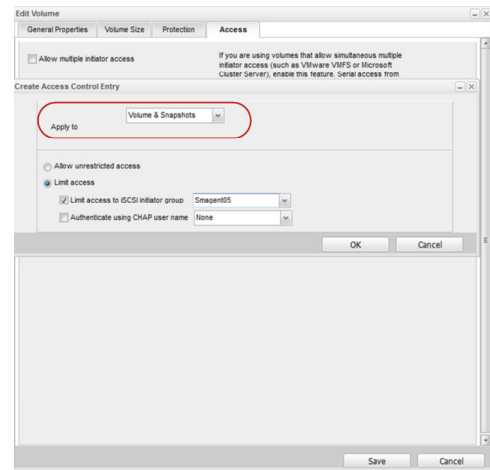
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

SnapProtect™ Backup - Nimble

◀ Previous Next ▶

PREREQUISITES

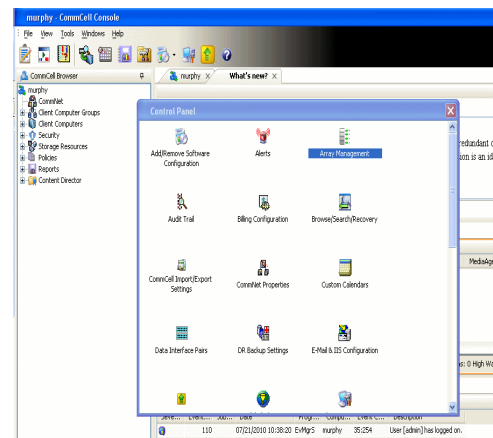
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry** to **Snapshots Only**.
- Ensure that a temporary LUN is allocated to all ESX Servers that are used for snapshot operations.



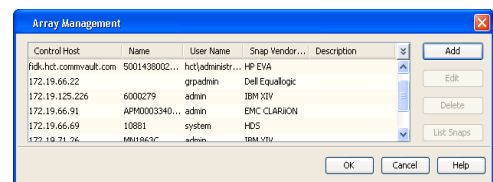
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **Nimble** from the **Snap Vendor** list.
 - Specify the Data IP Address of the array in the **Name** field.

If you have more than one Data IP Address configured, you will need to add the array information for each of the configured Data IP addresses.

- Enter the Management IP Address of the array in the **Control Host** field.

For reference purposes, the screenshot on the right shows the Data IP Address and Management IP for the Nimble storage device.

Name	Status	Type	Data IP Address	Subnet Mask	MTU	Bytes
eth1	Enabled	Data only	172.19.108.100	255.255.252.0	Standard	1500
eth2	Enabled	Data only	172.19.108.101	255.255.252.0	Standard	1500
eth3	Disabled	Not configured			Standard	1500
eth4	Disabled	Not configured			Standard	1500

4.
 - Enter the access information of a user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

SnapProtect™ Backup - Data Replicator

< Previous Next >

PRE-REQUISITES

INSTALLATION

- The use of Data Replicator with the SnapProtect backup requires MediaAgent, File System iDataAgent, and ContinuousDataReplicator on the source, destination, and proxy computers.

The use of a proxy server to perform SnapProtect operations is supported when a hardware storage array is used for performing the SnapProtect backup.

- The operating system of the MediaAgent to be used for SnapProtect backup must be either the same or higher version than the source computer.

STORAGE POLICY REQUIREMENTS

The Primary Snap Copy to be used for creating the snapshot copy must be a disk library.

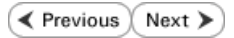
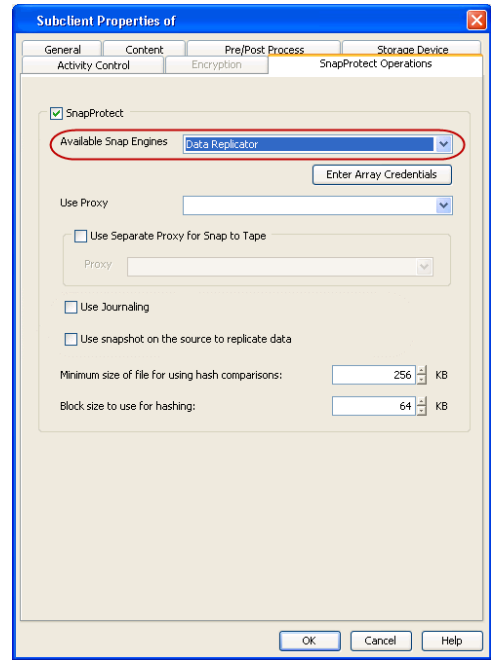
If the Storage Policy or the disk library being used by the subclient is updated, the subclient should be recreated.

SETUP THE ARRAY

1.
 - From the CommCell Console, navigate to <Client> | <Agent>.
 - Right-click the subclient and click **Properties**.
2.
 - Click the **SnapProtect Operations** tab.
 - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down

list.

- Click **OK**.



Getting Started Backup - SQL Server *iDataAgent*

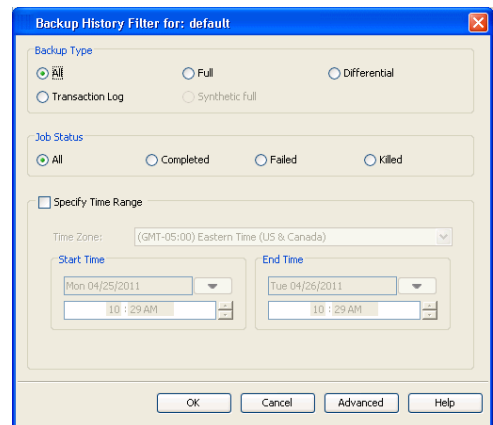
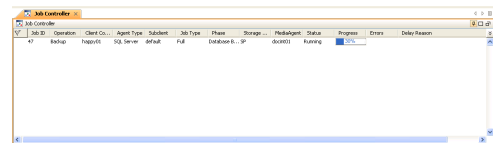
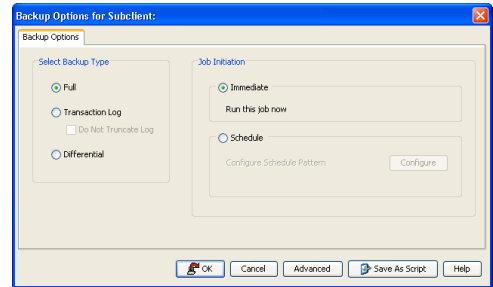
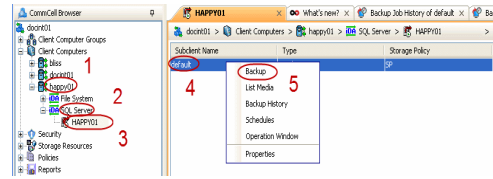
1.
 - From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **SQL Server** | **<Instance>**.
 - Right-click the default subclient and click **Backup**.

2.
 - Click **Full** as backup type and then click **Immediate**.
 - Click **OK**.

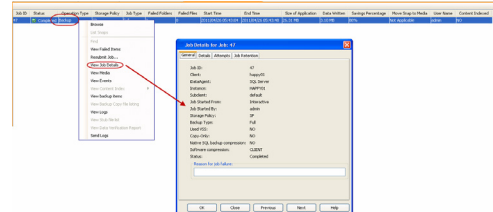
3. You can track the progress of the job from the **Job Controller** window of the CommCell console.

4. Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.

5. Click **OK**.



6. Right-click the job to:
 - Browse the databases that were backed up.
 - View items that failed, if any, during the job.
 - Resubmit the job.
 - View job details.
 - View media associated with the job.
 - View events associated with the job.
 - View backup items (you can view the database files that were backed up e.g., .mdf, .ldf).
 - View or send the log file that is associated with the job.



Getting Started - Vault/Mirror Copy

◀ Previous Next ▶

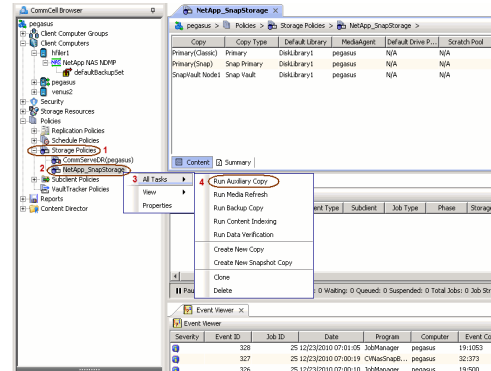
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

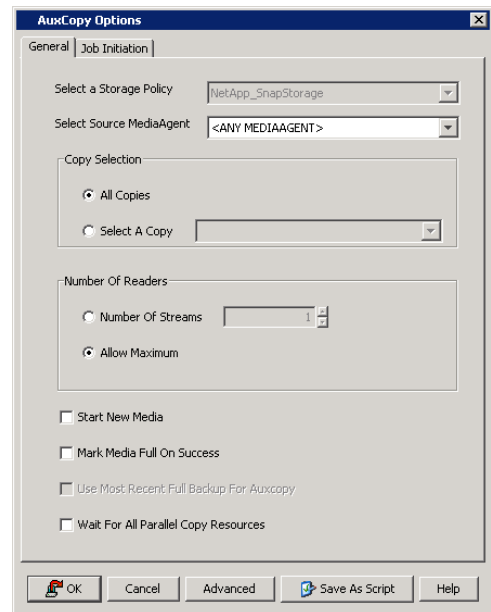
INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

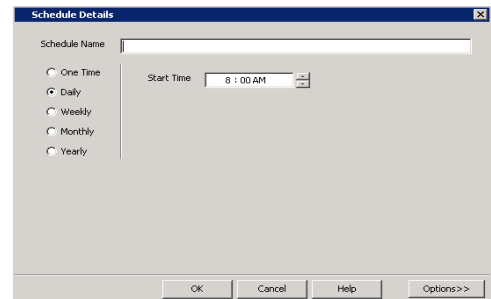


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- Enter the schedule name and select the appropriate scheduling options.
 - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.

◀ Previous Next ▶

Getting Started - Snap Movement to Media

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

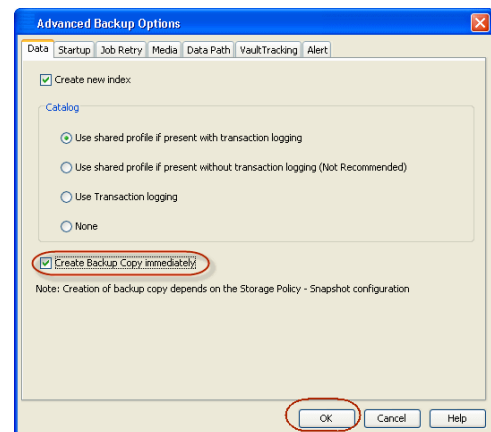
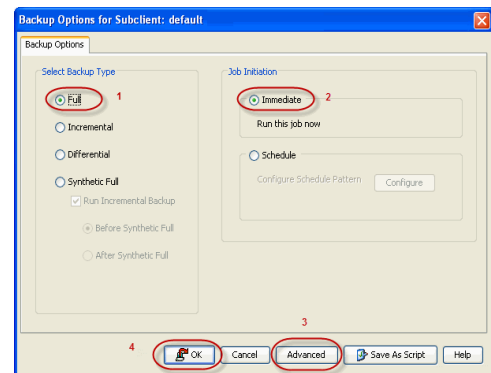
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

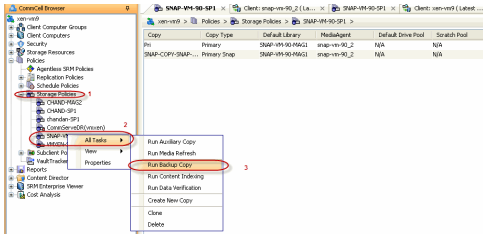
- From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
 - Right click the default subclient and click **Backup**.
 - Select **Full** as backup type.
 - Click **Advanced**.
- Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



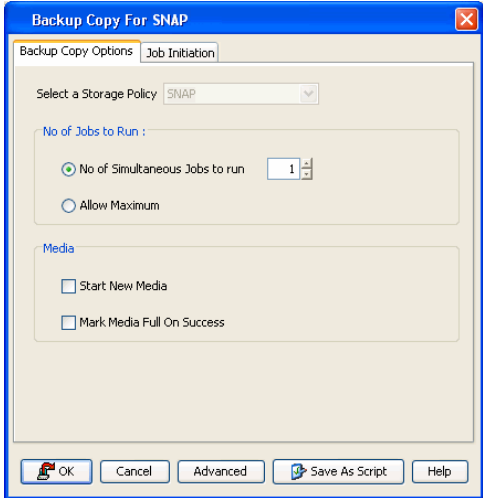
OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

- From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



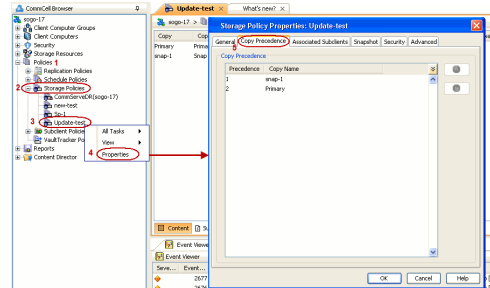
Getting Started - Microsoft SQL Server Restore

PERFORM A RESTORE

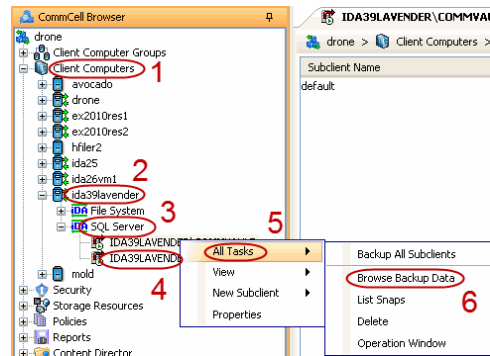
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring a database to a different location on the same destination server.

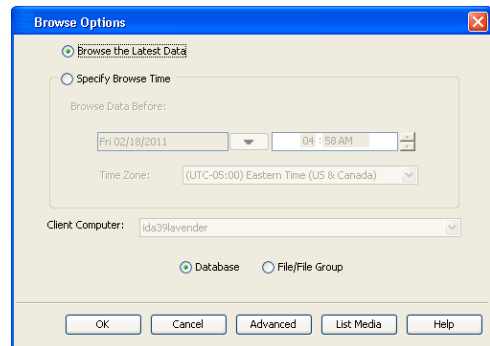
1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
 - Click **OK**.



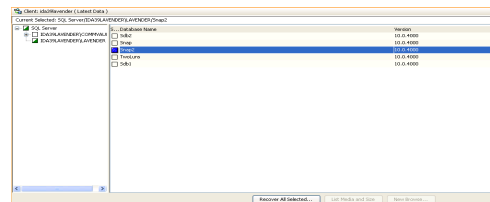
2.
 - From the CommCell Browser, navigate to **Client Computers | <Client> | SQL Server**.
 - Right-click the instance and then click **All Tasks | Browse Backup Data**.



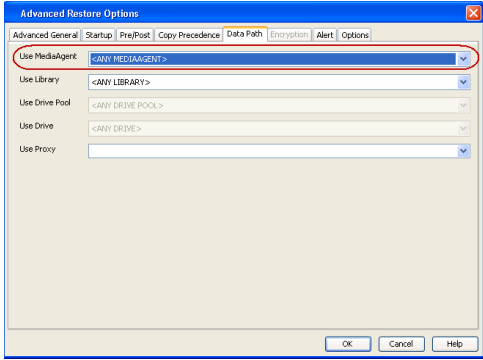
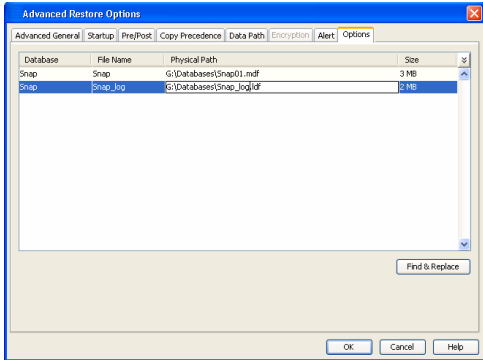
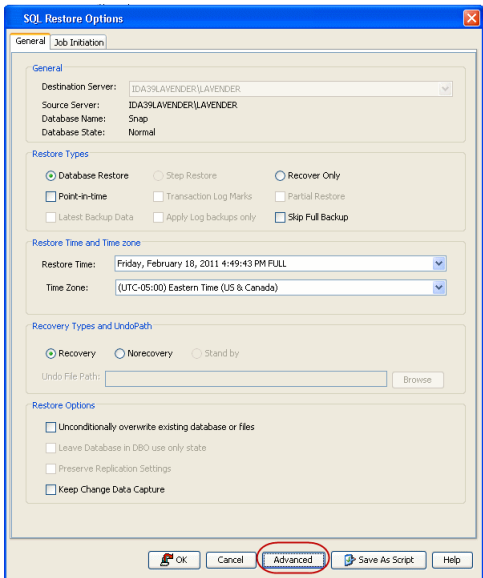
3. Click **OK**.



4.
 - Click the instance node in the left pane. Select the database you want to restore in the right pane.
 - Click **Recover All Selected**.



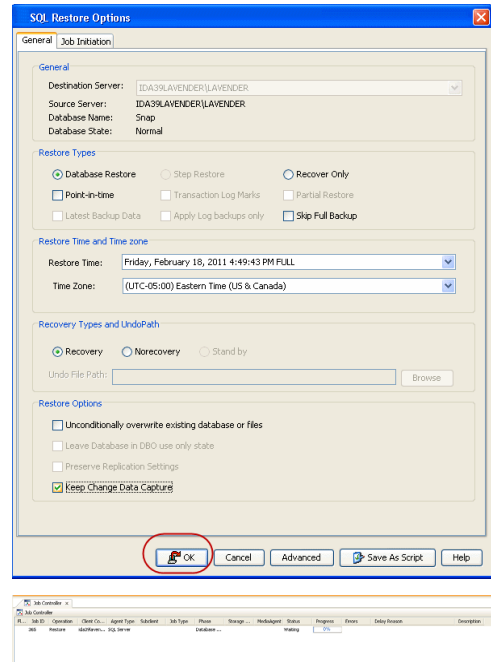
5. Click **Advanced**.



6.
 - Click the **Options** tab.
 - Rename the database name under the **Database** column.
 - Change the path of the database and log files under the **Physical Path** column.
 - Click **OK**.

7.
 - Click the **Data Path** tab.
 - Select a Windows MediaAgent from the **Use MediaAgent** drop-down list.
 - Click **OK**.

8. Click **OK**.



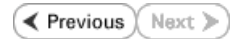
9. You can monitor the progress of the restore job in the **Job Controller**.

10. The database and the log files are restored to the location specified in step 6.

CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



Getting Started - NAS Configuration



PRE-REQUISITES

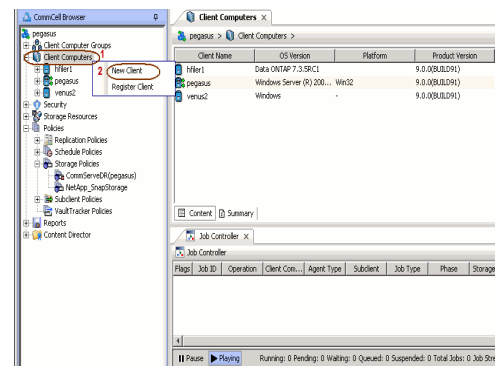
- Prior to performing a SnapProtect backup, ensure that all the available hotfixes for Virtual Disk Service (VDS) and VSS are applied.
- When performing SnapProtect backup for a Windows Cluster, a proxy server must be used for performing backup and restore operations.
- SnapProtect backup on Windows supports basic disks.

CONFIGURATION

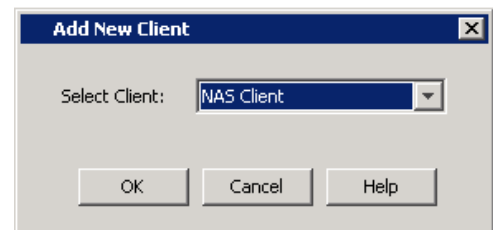
The software for the NAS *iDataAgent* is installed automatically as part of the MediaAgent installation. However, the client is not automatically created in the CommCell Console.

Follow the steps given below to create and configure the NAS client for a first SnapProtect backup. If the data you want to backup resides on a vFiler, configure the vFiler as the NAS client.

1. From the CommCell Browser, right-click the **Client Computers** node and click **New Client**.



2.
 - Select **NAS Client** from the drop-down list.
 - Click **OK**.



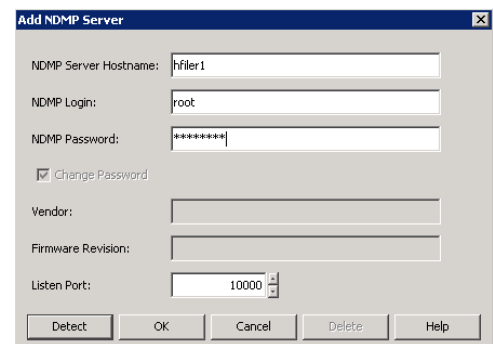
3.
 - Provide the File Server details to add the **NDMP Server**.
For any ONTAP version, do not provide the host name or IP address of the management port (e.g., e0M). Use the host name or IP address of a data port (e.g., e0A, e0B).

- Click **Detect**.
- Click **OK**.

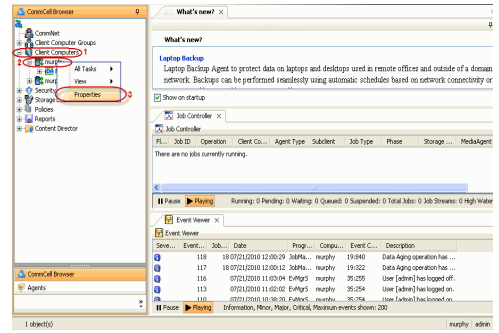
A new client is created and listed under the Client Computers node. The default subclient is created automatically.

Any NAS storage device that will be used for backing up secondary storage data (Vault, Mirror or backup copy) must be configured as a **NAS Client** in the CommCell with the same name that is used by the DFM server to communicate to the secondary NAS file server.

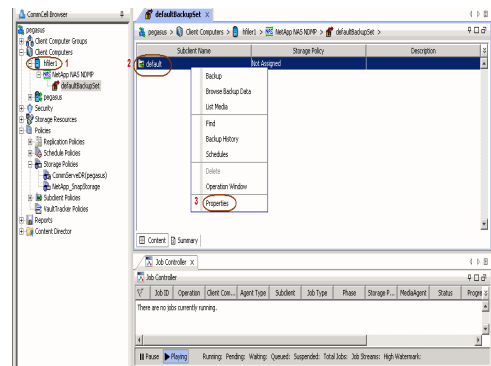
4. From the CommCell Browser, right-click the NAS client just created and select **Properties**.



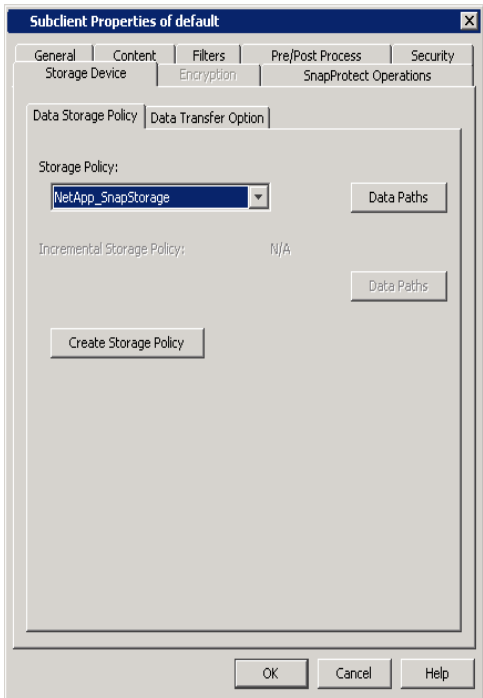
5.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.



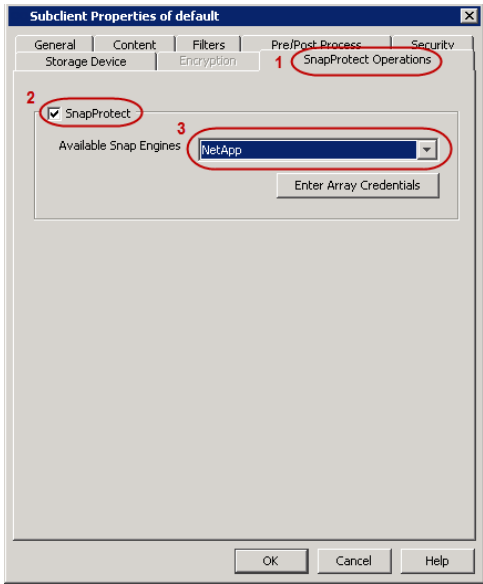
6.
 - From the CommCell Browser, right-click the subclient.
 - Click **Properties**.



7.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.

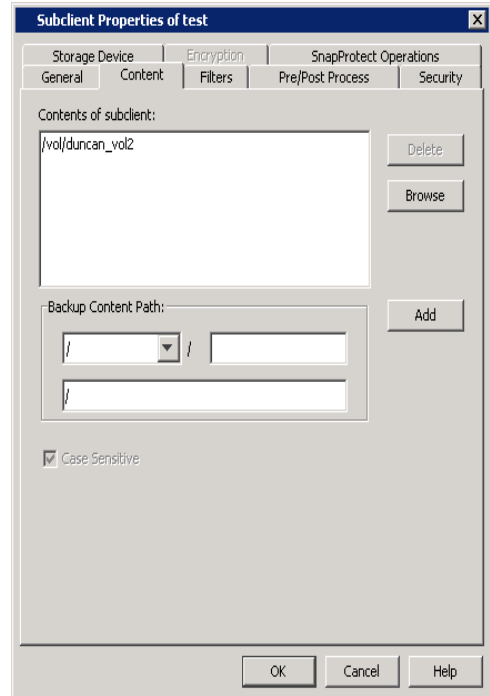


- 8.
- Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select **NetApp** from the **Available Snap Engine** drop-down list.



- 9.
- Click the **Content** tab.
 - Click **Browse** and specify the content for the subclient.
It is recommended that you add full volume as the subclient content and not a sub directory or a qtree.
 - Click **OK**.

The subclient content must contain data that resides on the storage device volume; do not include local drives as subclient content. If you added a vFiler as a client, do not include the root volume.



SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

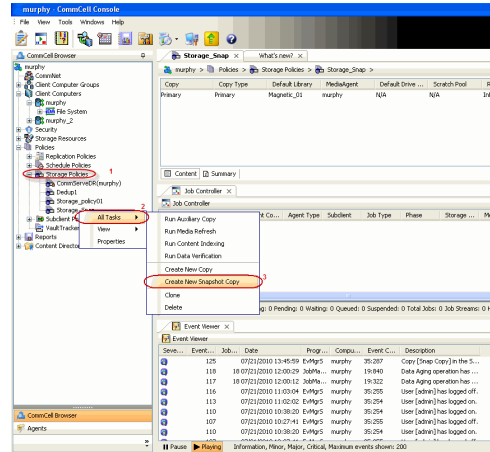
Click **Next** ➤ to Continue.

CREATE A SNAPSHOT COPY

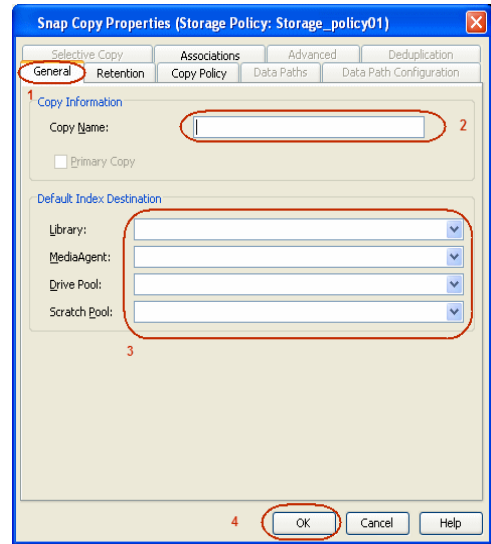


Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.



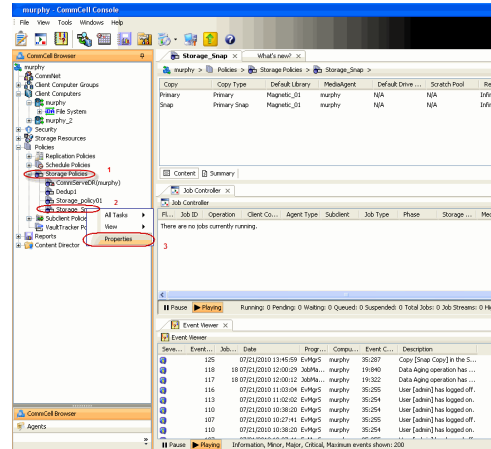
2.
 - Enter the copy name in the **Copy Name** field.
 - Select the **Library, MediaAgent, master Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



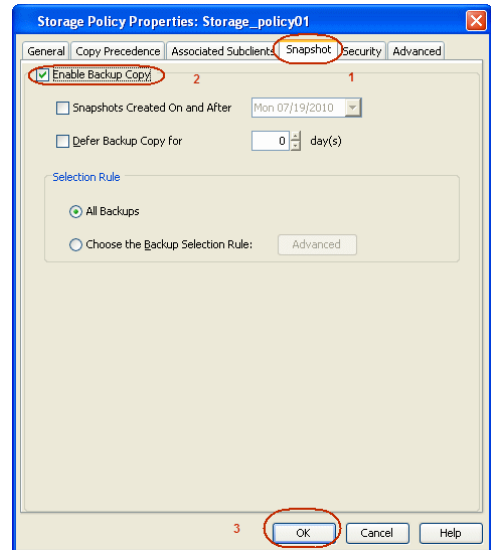
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



SnapProtect™ Backup - NetApp



PREREQUISITES

LICENSES

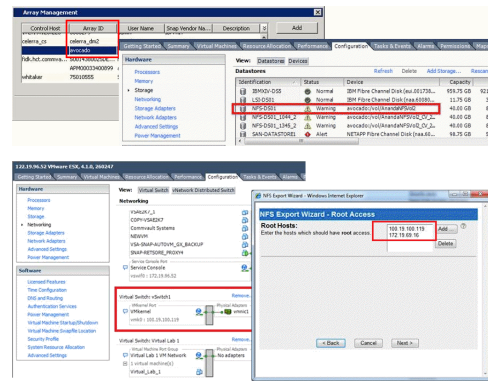
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.

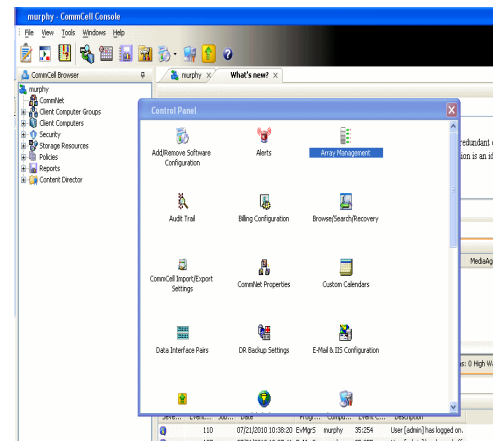
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



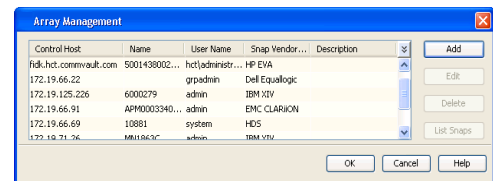
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the file server in the **Name** field.
 - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: [Text Box]

Control Host: [Text Box]

User Name: [Text Box]

Password: [Text Box]

Confirm Password: [Text Box]

Device Group: [Text Box]

Use devices only from this device group

Description: [Text Area]

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous Next ▶

OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

PREREQUISITES

LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:

```
options snapvault.enable on
```

3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:

```
options snapvault.access host=secondary_filer1, secondary_filer2
```

4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:

```
options snapvault.access host=primary_filer1, primary_filer2
```

INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
 - Discover storage devices
 - Add Resource Pools to be used for the Vault/Mirror storage provisioning

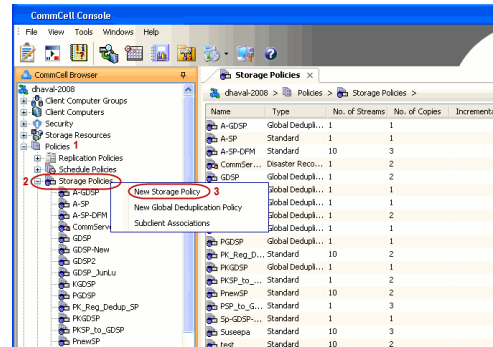
CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

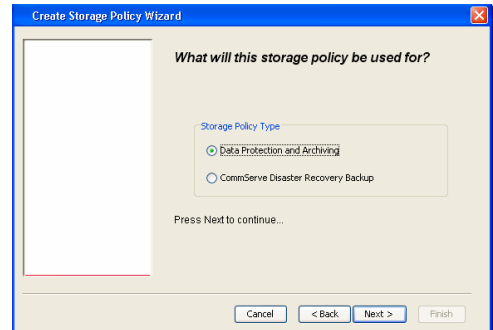
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



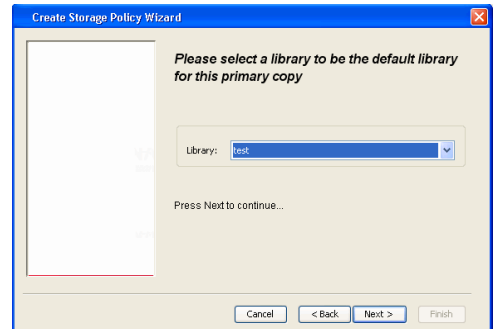
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.

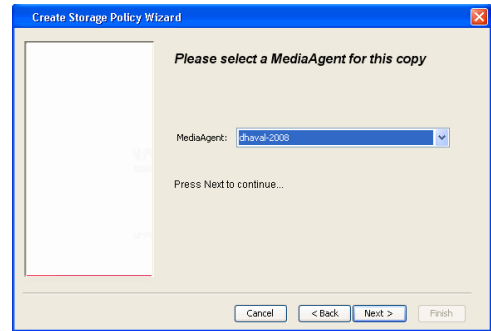
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

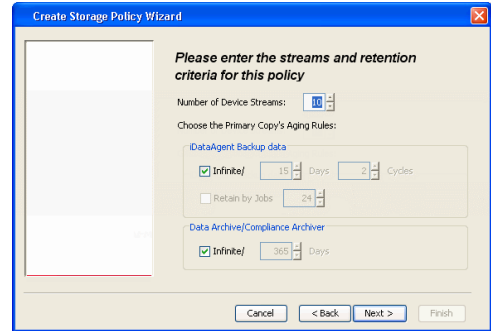


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

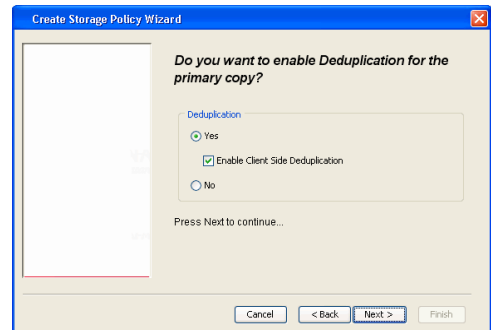
6. Click **Next**.



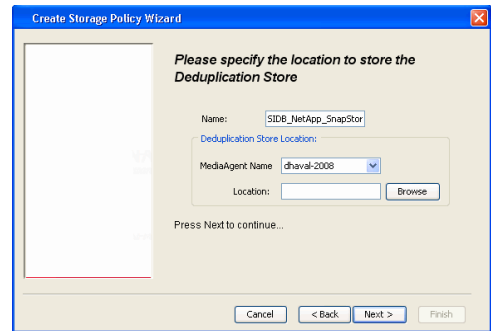
7. Click **Next**.



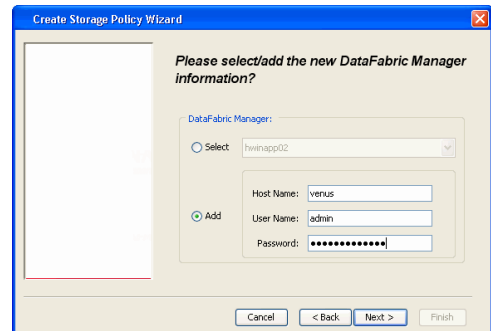
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

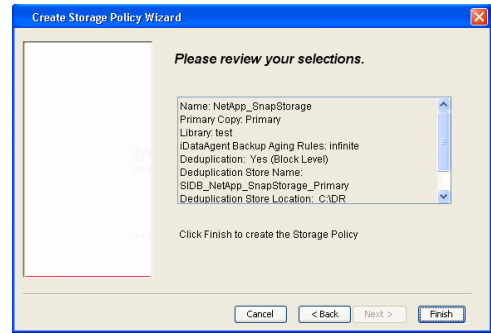


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



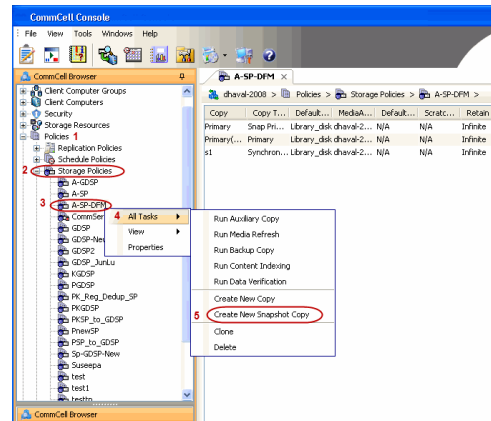


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

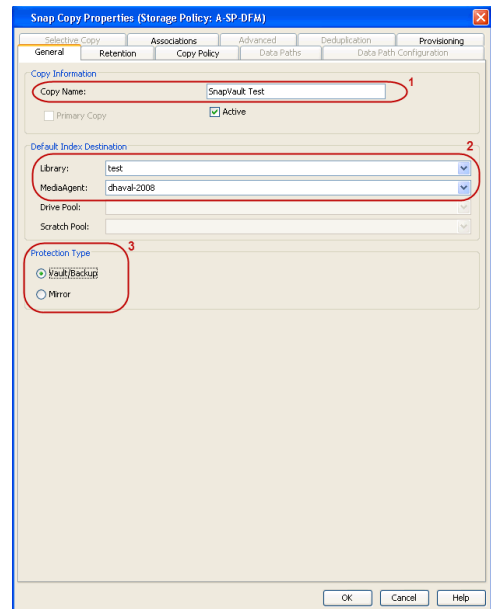
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
 - Enter the **Copy Name**.
 - Select the **Library** and **MediaAgent** from the drop-down list.
 - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

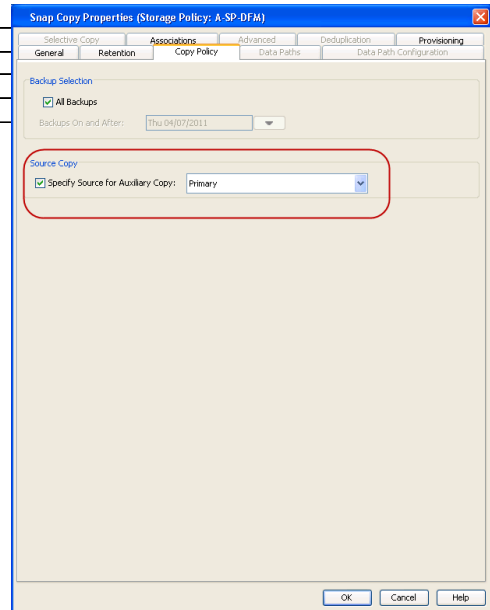


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

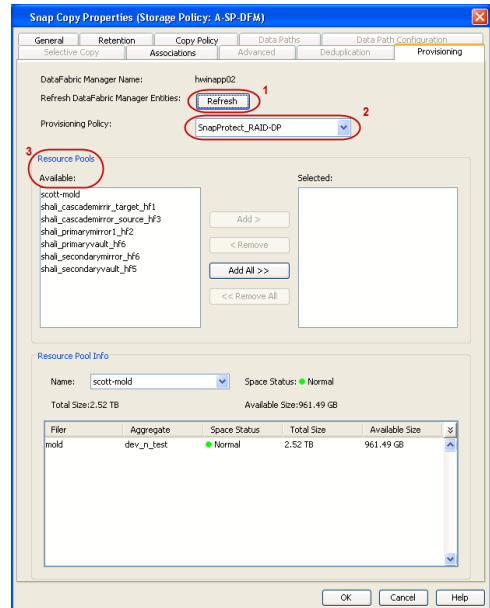
TOPOLOGY	SOURCE COPY
----------	-------------

Primary-Mirror	Primary
Primary-Mirror-Vault	Mirror
Primary-Vault	Primary
Primary-Vault-Mirror	Vault
Primary-Mirror-Mirror	Mirror



- Click the **Provisioning** tab.
 - Click **Refresh** to display the DFM entities.
 - Select the **Provisioning Policy** from the drop-down list.
 - Select the **Resource Pools** available from the list.
 - Click **OK**.

The secondary snapshot copy is created.



- If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:


```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

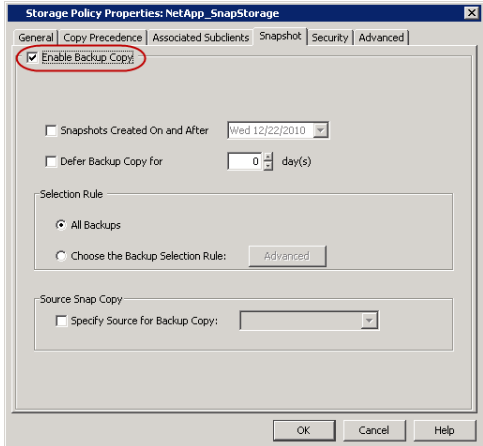
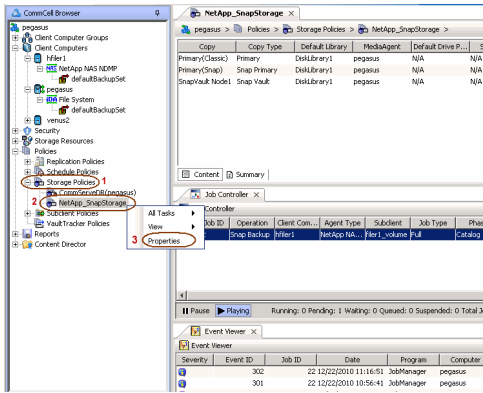
It is recommended that you perform this operation on all nodes in the P-M-V topology.

CONFIGURE BACKUP COPY

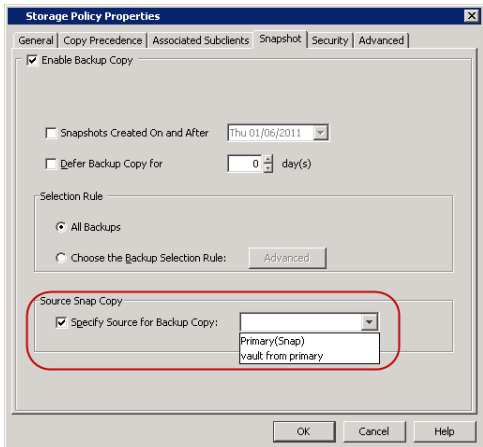
Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.

2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



3.
 - Select **Specify Source for Backup Copy**.
 - From the drop-down list, select the source copy to be used for performing the backup copy operation.

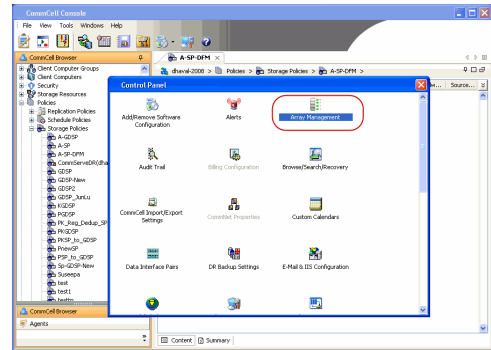


SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

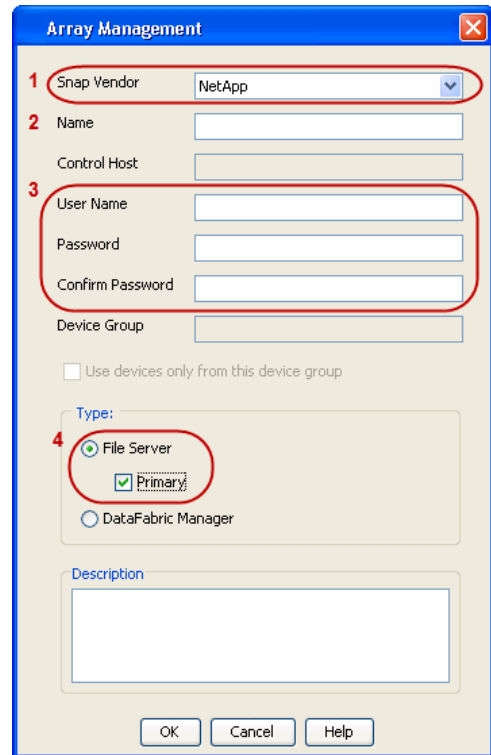
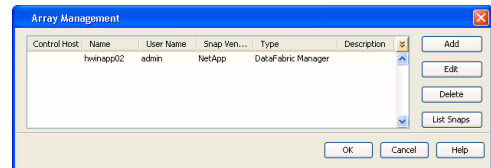


3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

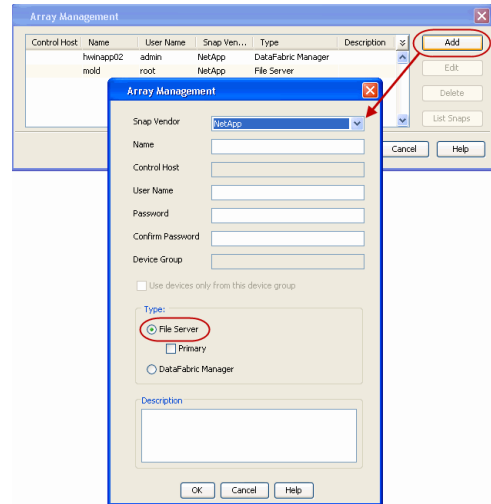
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



4.
 - Click **Add** again to enter the information for the secondary array.
 - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



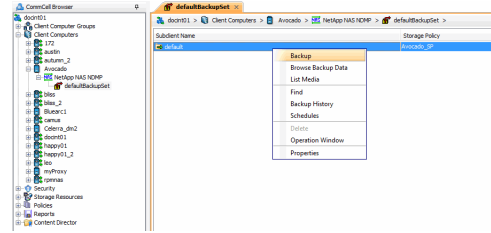
SEE ALSO

Import Wizard Tool

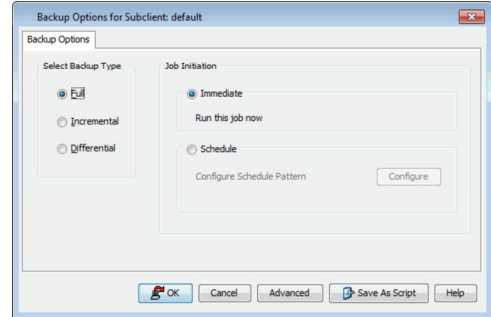
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

Getting Started - NAS iDataAgent Backup

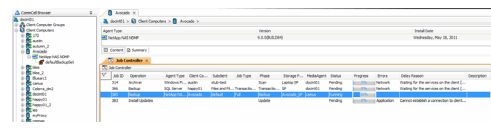
- From the CommCell Console, navigate to <Client> | <File Server> NAS NDMP | defaultBackupSet.
 - Right-click the **Subclient** and click **Backup**.



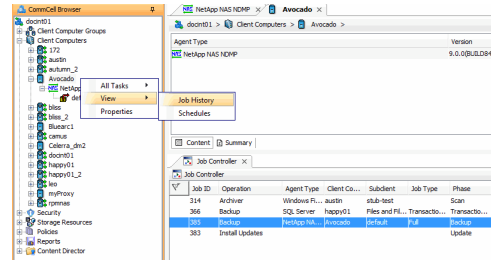
- Select **Full** as backup type.
If you are backing up vFiler data and the physical file server (where the vFiler resides) has not been specified in Array Management, click **Advanced**. From the **Advanced Backup Options** dialog box, click the **Skip Catalog phase for SnapProtect** option as indexing is not supported for vFiler backups.
 - Click **OK**.



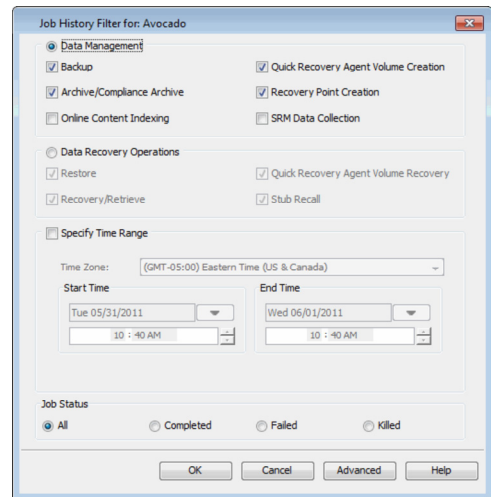
- You can track the progress of the job from the **Job Controller** window.



- Once job is complete, view the details of job from the **Job History**. Right-click the client computer, click **View** | **Job History**.

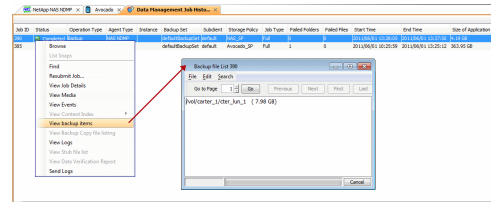


- Click **OK**.



- Right-click the job to:
 - Browse the NAS data that was backed up.
 - Resubmit the job.
 - View the job details.
 - View media associated with the job.
 - View events associated with the job.

- View backup items (displays the NAS data that was backed up).
- View or send the log file associated with the job.



Getting Started - Vault/Mirror Copy



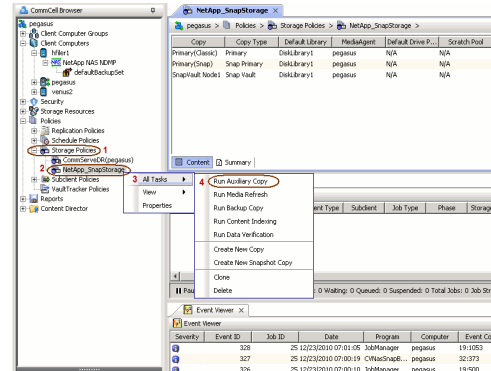
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** > to Continue.

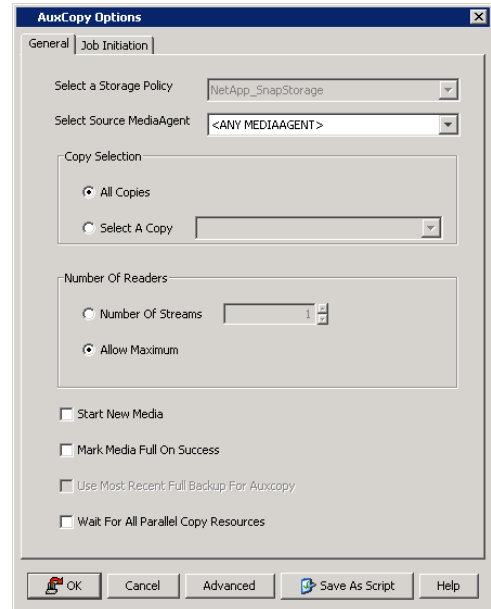
INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

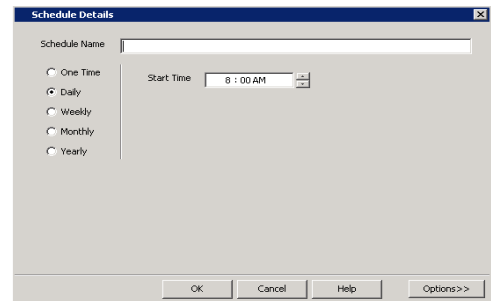


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.

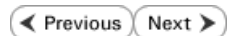


- Enter the schedule name and select the appropriate scheduling options.
 - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.



Getting Started - Snap Movement to Media

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

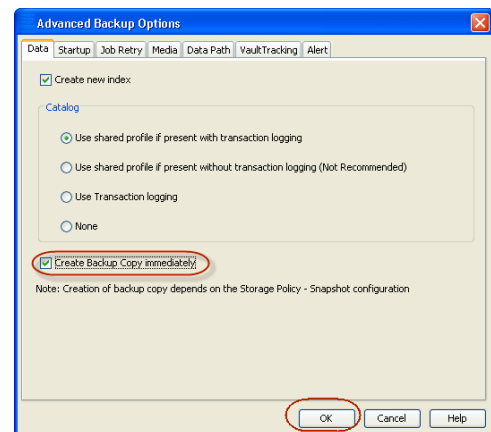
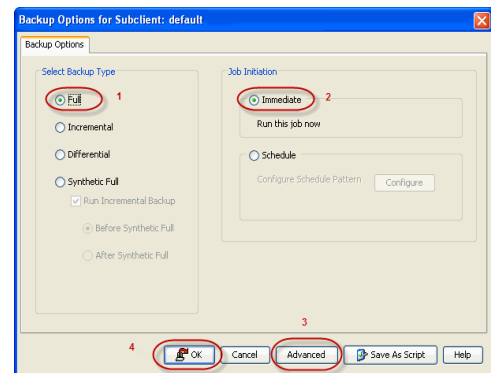
INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

1.
 - From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
 - Right click the default subclient and click **Backup**.
 - Select **Full** as backup type.
 - Click **Advanced**.

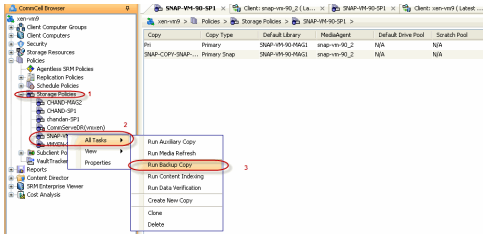
2.
 - Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



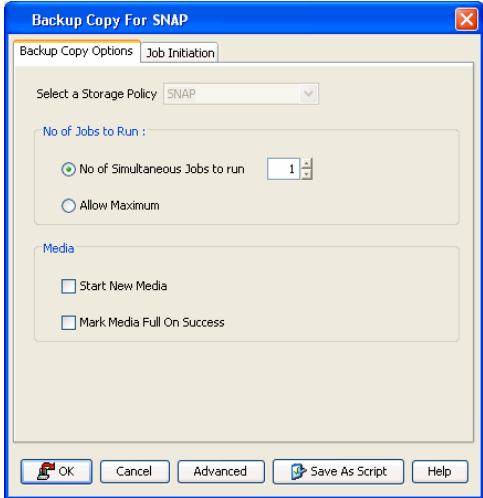
OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

1.
 - From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



Getting Started - NAS Restore

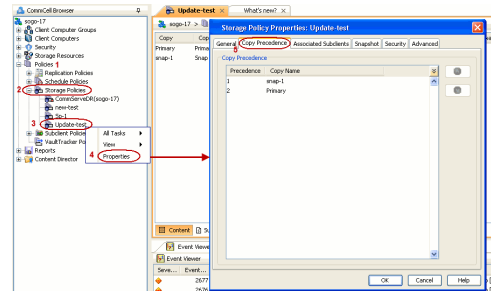


PERFORM A RESTORE

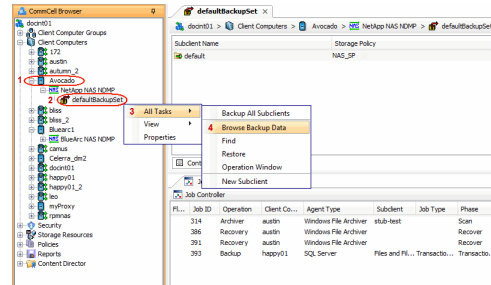
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring the data of a volume to a different location in the file server. If you are restoring from a vFile backup, click the **Previous** button above to follow the steps to create a backup copy, and restore your vFile data from the backup copy.

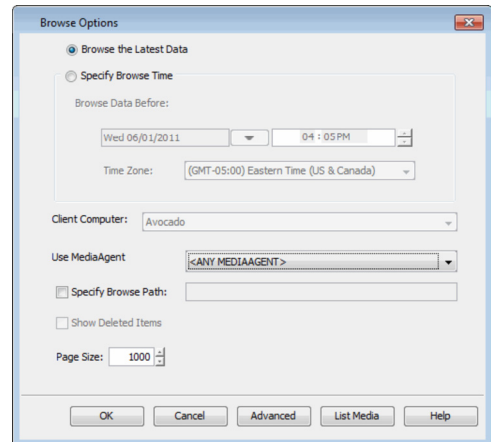
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - Select the backup copy and set the copy precedence as 1.
 - Click **OK**.



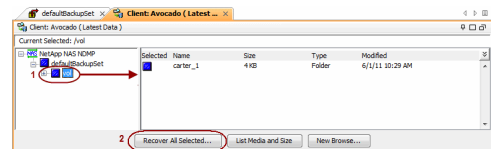
- From the CommCell Console, navigate to **<Client> | <File Server> NAS NDMP**.
 - Right-click the backup set and click **All Tasks | Browse Backup Data**.



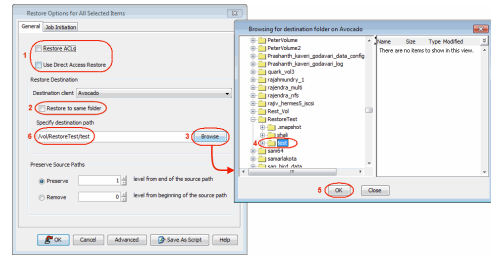
- Click **OK**.



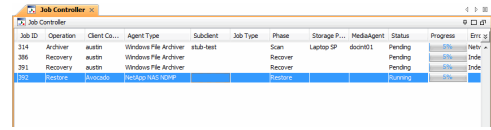
- Expand the backup set node in the left pane. Select the volume containing the data you want to restore.
 - Click **Recover All Selected**.



- Clear the **Restore ACLS** and **Use Direct Access Restore** checkboxes. Selecting these options are not applicable when restoring data from a snapshot.
 - Clear the **Restore to same folder** checkbox.
 - Specify the destination path by clicking **Browse**.
 - Click **Preserve** or **Remove** source paths to specify whether the restore operation will keep or remove the specified number of levels from the beginning or end of the source path.
 - Click **OK**.



6. You can track the progress of the job from the **Job Controller** window.



CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



Getting Started - Microsoft Hyper-V Deployment

◀ Previous Next ▶

WHERE TO INSTALL

Install the software directly on the Hyper-V Server.

BEFORE YOU BEGIN

Download Software Packages

Download the latest software package to perform the install.

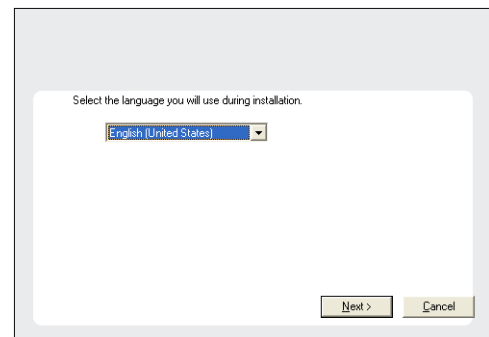
SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.

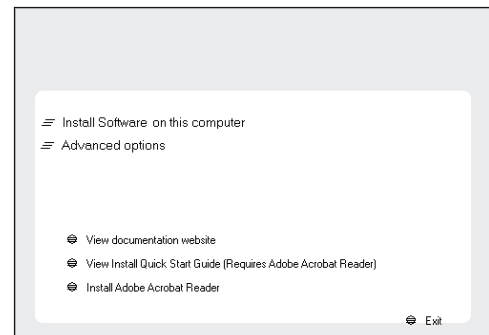
INSTALL THE VIRTUAL SERVER iDATAAGENT (HYPER-V)

The Virtual Server iDataAgent is used to protect Hyper-V virtual machine data. Use the following procedure to directly install the software from the installation package or a network drive.

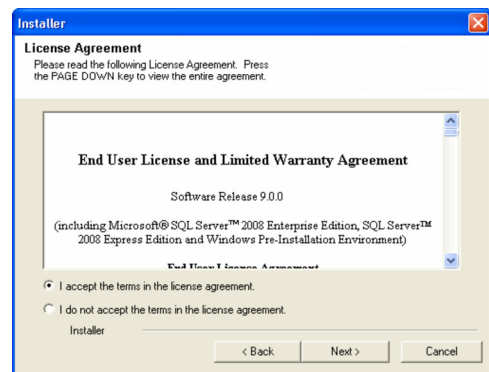
1. Run **Setup.exe** from the Software Installation Package.
2. Select the required language.
Click **Next**.



3. Select the option to **Install Calypso on this 64-bit computer**.
Your screen may look different from the example shown.

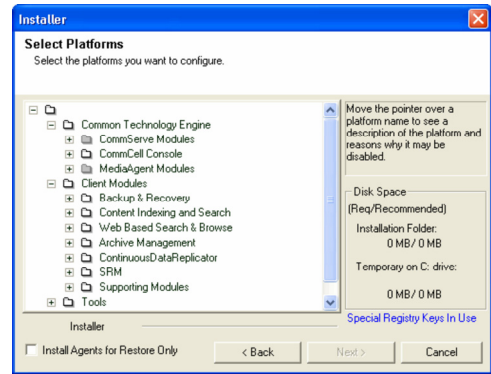


4. Select **I accept the terms in the license agreement**.
Click **Next**.

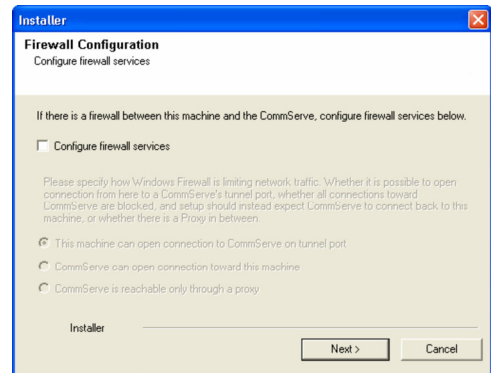
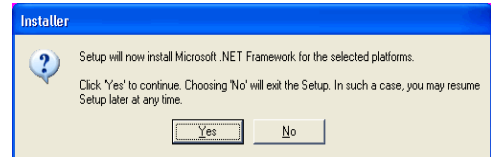


5.
 - Expand **Client Modules | Backup & Recovery | File System**, and select **Virtual Server Agent**.
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
 - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
 - Click **Next**.

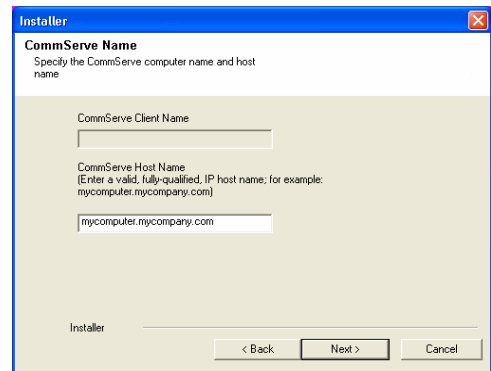
6. Click **YES** to install Microsoft .NET Framework package.
 - This prompt is displayed only when Microsoft .NET Framework is not installed.
 - Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.
7. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.
 For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.
 If firewall configuration is not required, click **Next**.



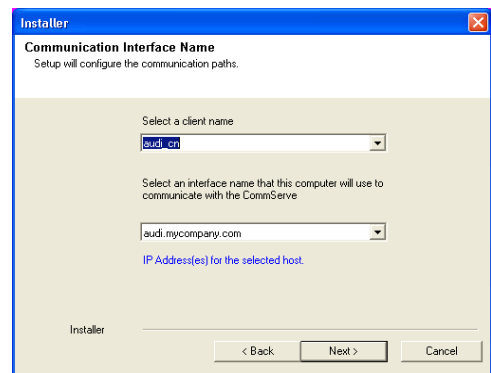
8. Enter the fully qualified domain name of the **CommServe Host Name**.
 Click **Next**.
 Do not use space and the following characters when specifying a new name for the CommServe Host Name:
`\ | ` ~ ! @ # $ % ^ & * () + = < > / ? , [] { } ; : ; " ' " "`



9. Click **Next**.



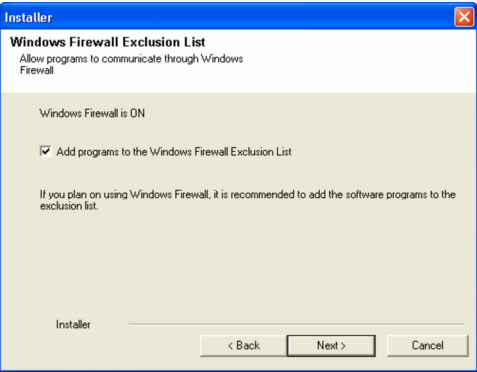
10. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.



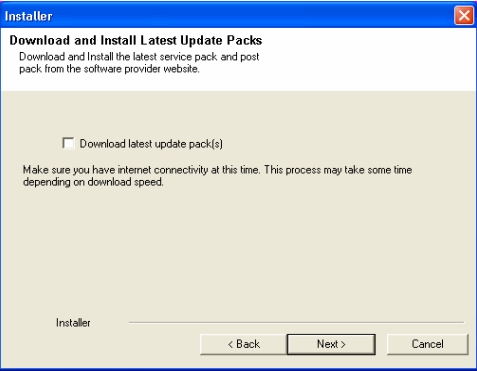
Click **Next**.

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

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



11. Click **Next**.



12. Verify the default location for software installation.

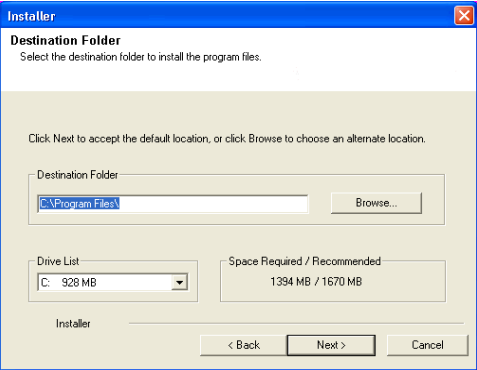
Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

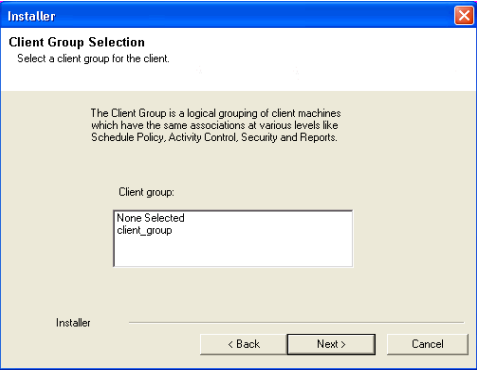
It is recommended that you use alphanumeric characters only.



13. Select a Client Group from the list.

Click **Next**.

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



14. Click **Next**.

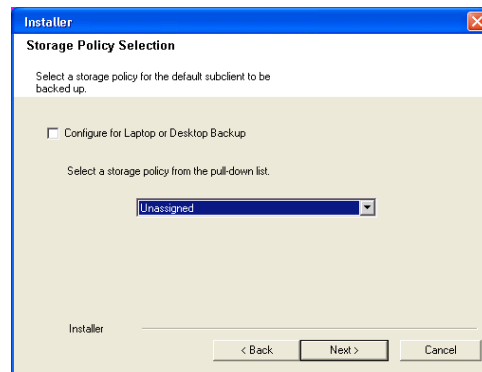
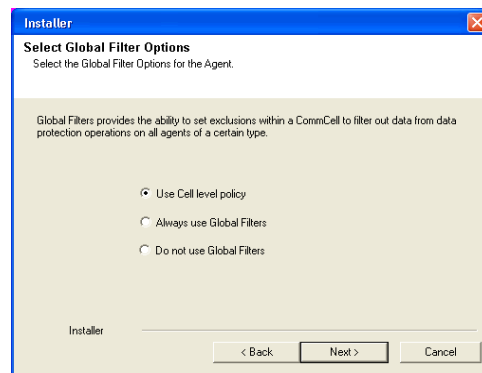
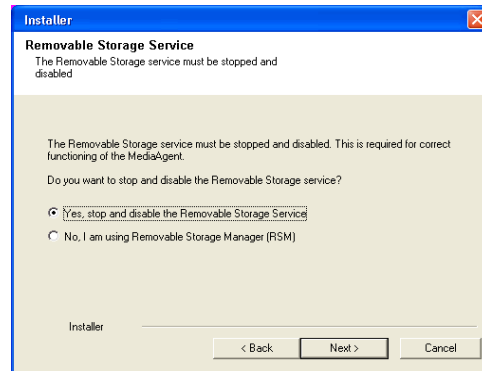
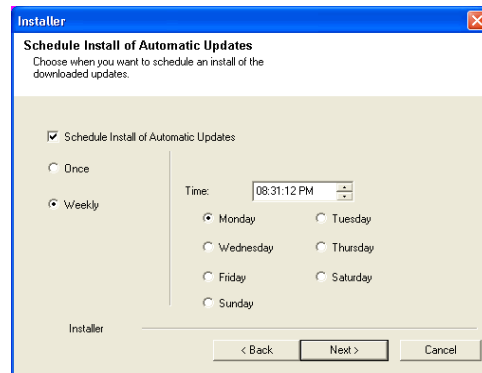
- 15. Select **Yes** to stop Removable Storage Services on the MediaAgent.
Click **Next**.

This prompt will not appear if Removable Storage Services are already disabled on the computer.

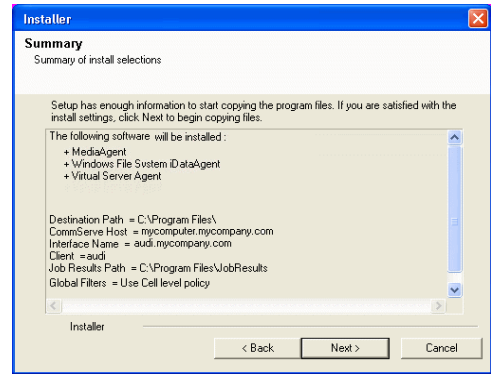
- 16. Click **Next**.

- 17. Select a **Storage Policy**.
Click **Next**.

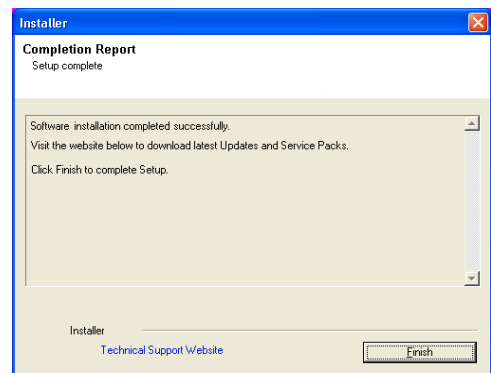
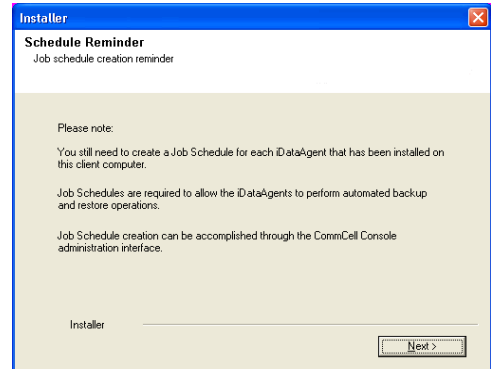
- 18. Click **Next**.



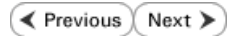
19. Click **Next**.



20. Click **Finish**.



Getting Started - Microsoft Hyper-V Configuration



CONFIGURATION

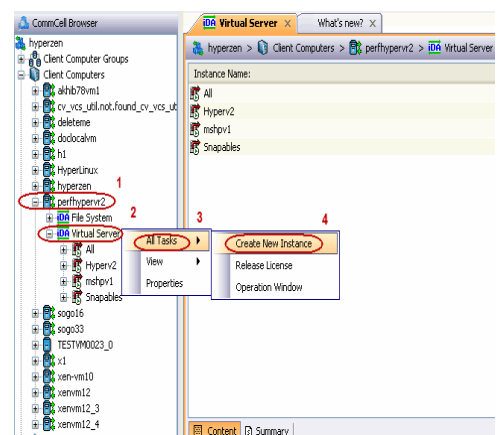
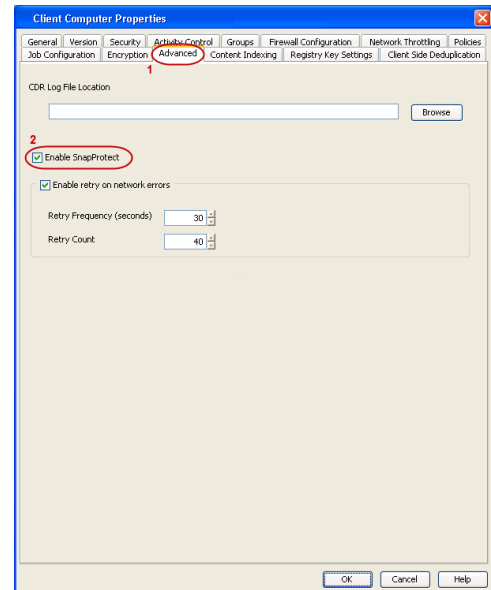
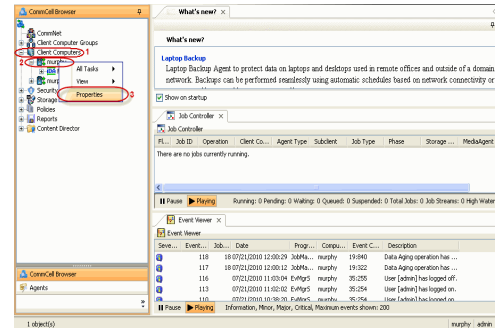
Once the Virtual Server *iDataAgent* has been installed, configure an Instance, a Backup Set and a Subclient to facilitate backups. The following sections provide the necessary steps required to create and configure these components for a first SnapProtect backup of a single virtual machine.

1.
 - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.

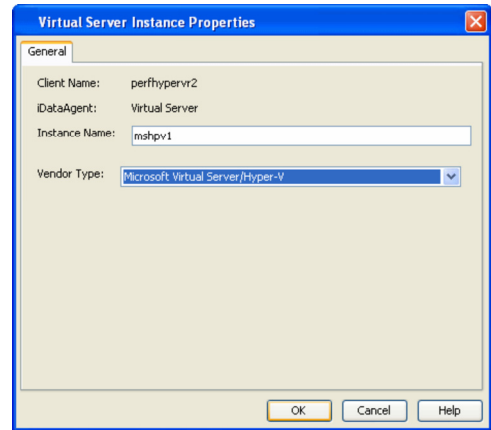
2.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.

3.
 - From the CommCell Browser, navigate to **<Client>** | **Virtual Server**.
 - Right-click the **Virtual Server** agent and click **All Tasks** | **Create New Instance**.

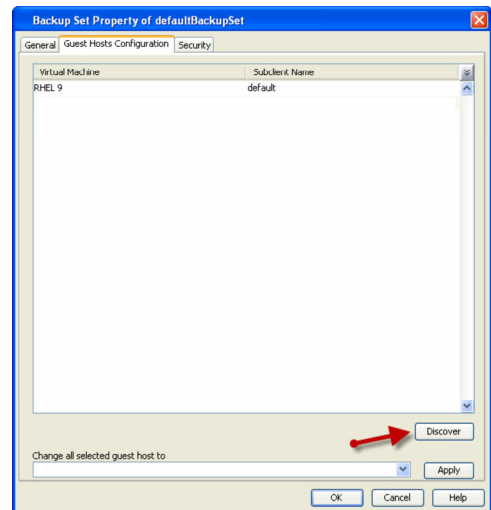
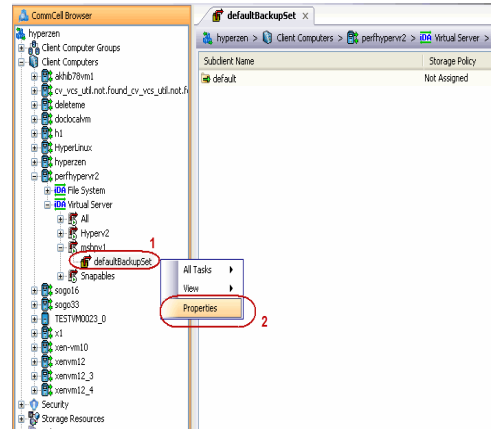
4.
 - Enter the **Instance Name**.
 - Select **Microsoft Virtual Server/Hyper-V** from **Vendor Type** menu.
 - Click **OK**.



5.
 - From the CommCell Browser, right-click the **Default Backup Set**.
 - Click **Properties**.

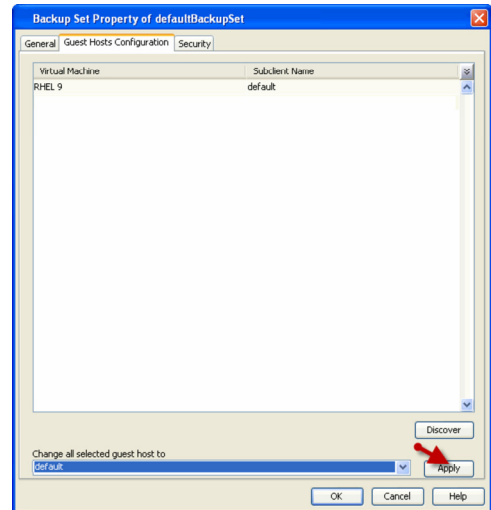


6. Click **Discover**, on the **Guest Hosts Configuration** tab. Discovery process might take several minutes to complete.

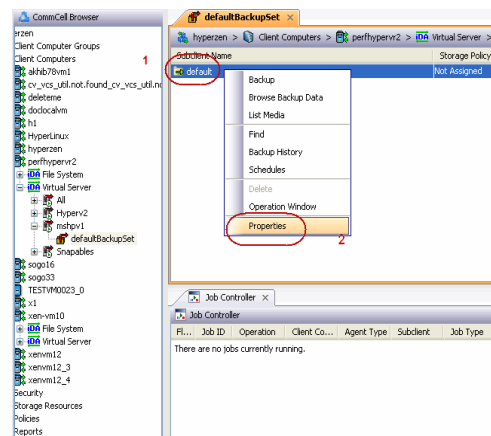


7.
 - Select the default subclient from **Change all selected guest hosts to** list.
 - Click **Apply**.
 - Click **OK**.

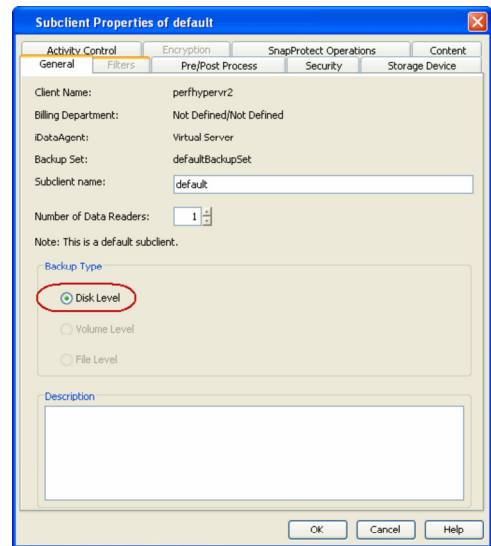
8.
 - From the CommCell Browser, navigate to the default subclient.
 - Click **Properties**.



9. Ensure **Disk-Level** from **Backup Type** is selected.



10.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.

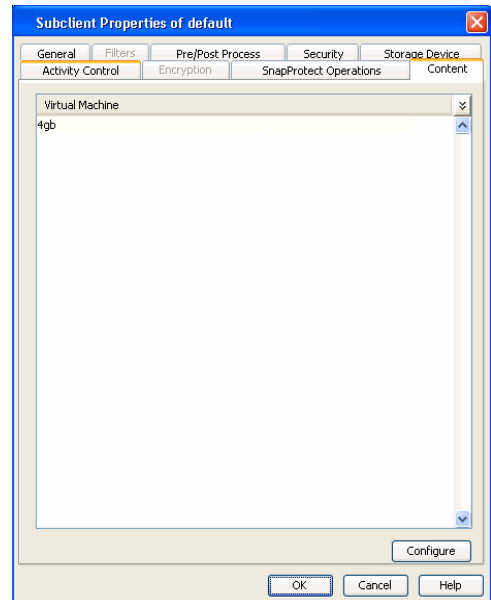
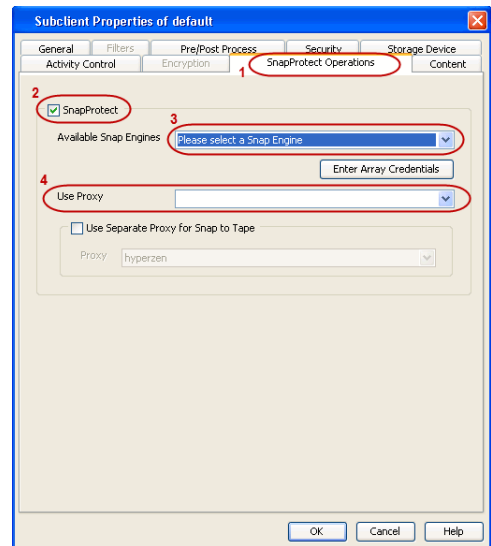
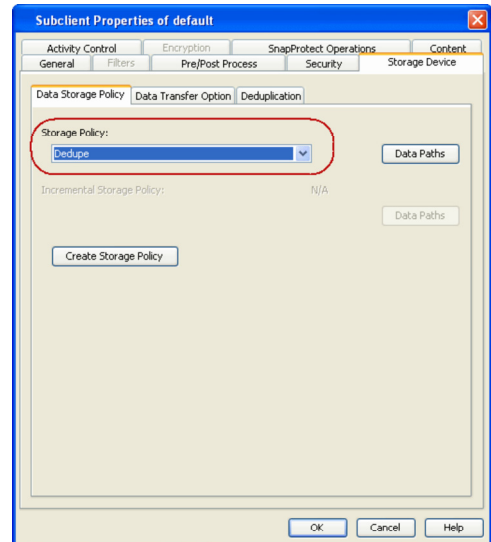


11.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy operations will be performed.

When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent. Select the MediaAgent from the **Proxy** list.

12.
 - Click the **Content** tab.
 - Click **Configure** if you need to configure an additional virtual machine for the subclient.
 - Click **OK**.



SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

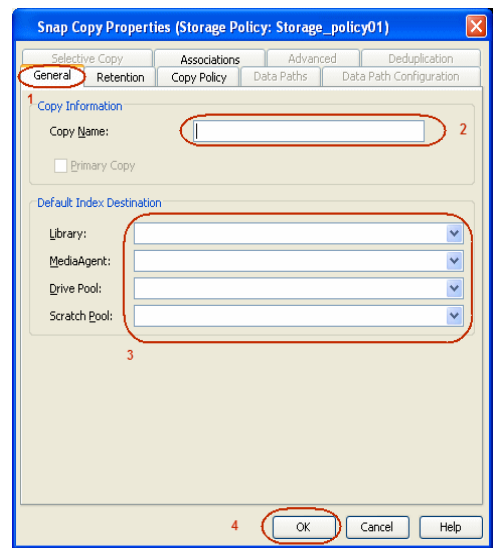
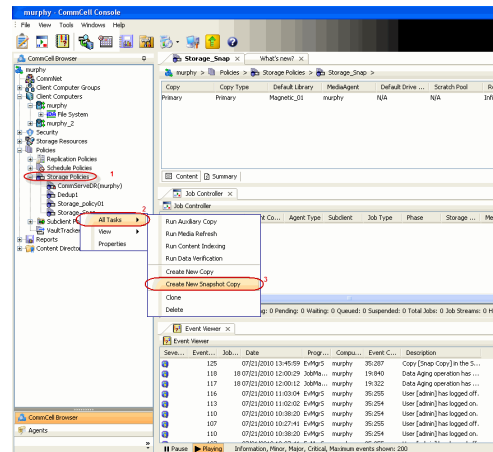
Click **Next** to Continue.



CREATE A SNAPSHOT COPY

Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

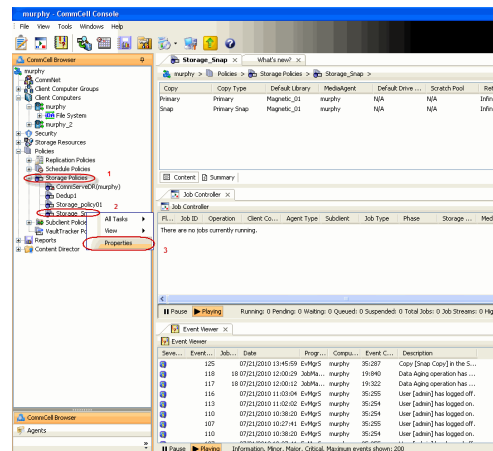
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.
- Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



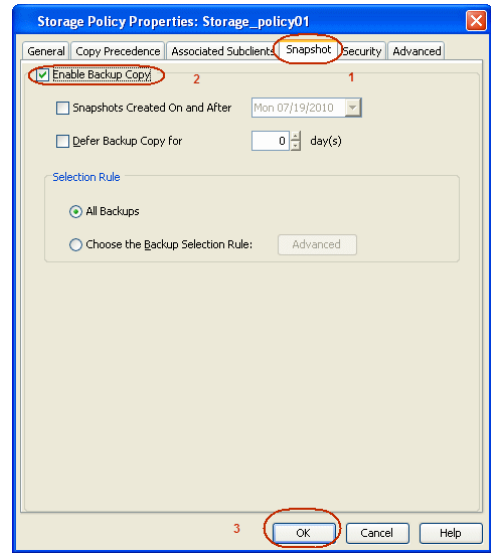
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
- Click the **Snapshot** tab.



- Select **Enable Backup Copy** option to enable movement of snapshots to media.
- Click **OK**.



Storage Array Configuration

[◀ Previous](#) [Next ▶](#)

CHOOSE THE STORAGE ARRAY

HARDWARE STORAGE ARRAYS
NETAPP
NETAPP WITH SNAPVAULT/SNAPMIRROR

[◀ Previous](#) [Next ▶](#)

SnapProtect™ Backup - NetApp



PREREQUISITES

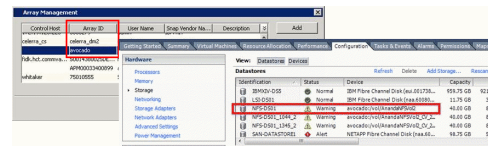
LICENSES

- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

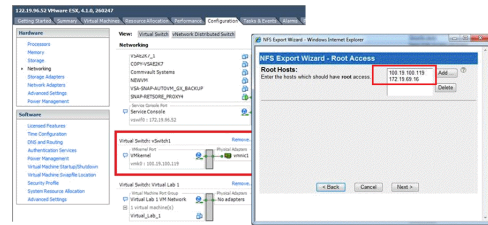
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.



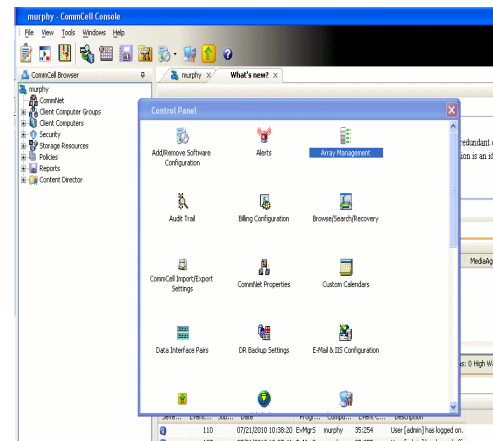
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



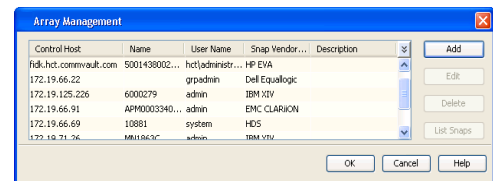
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the file server in the **Name** field.
 - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: []

Control Host: []

User Name: []

Password: []

Confirm Password: []

Device Group: []

Use devices only from this device group

Description: []

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous Next ▶

OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

PREREQUISITES

LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:


```
options snapvault.enable on
```
3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:


```
options snapvault.access host=secondary_filer1, secondary_filer2
```
4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:


```
options snapvault.access host=primary_filer1, primary_filer2
```

INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
 - Discover storage devices
 - Add Resource Pools to be used for the Vault/Mirror storage provisioning

CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

CREATE STORAGE POLICY

Use the following steps to create a storage policy.

1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.

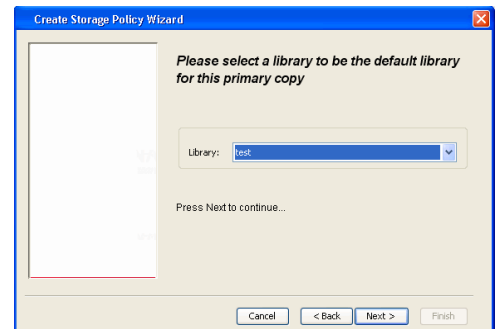
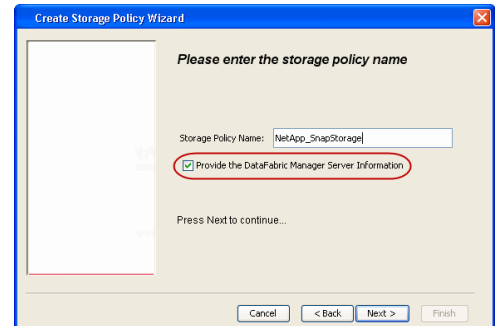
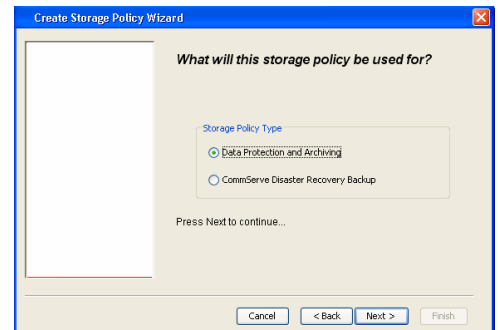
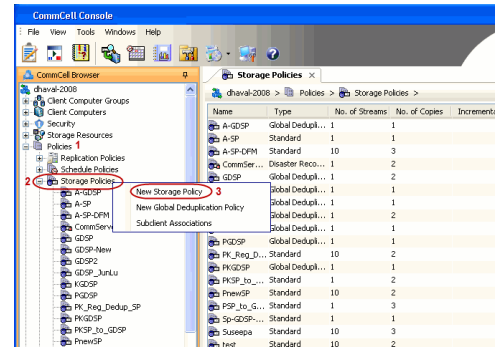
2. Click **Next**.

3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.

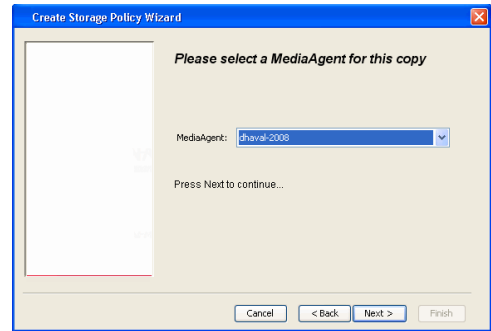
4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.

It is recommended that the selected disk library uses a LUN from the File server.
 - Click **Next**.

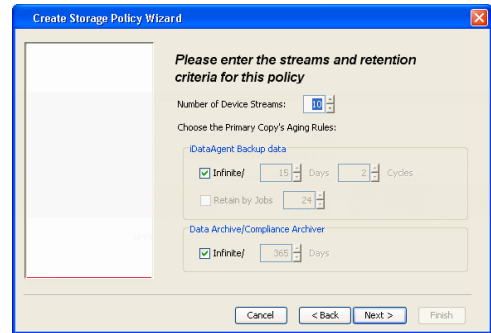
5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.



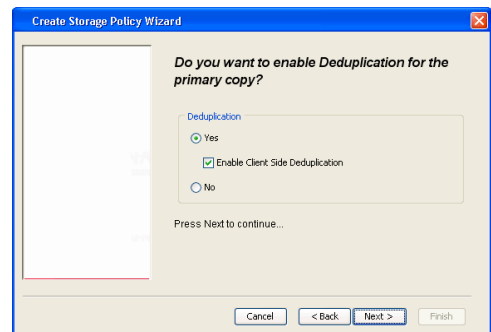
6. Click **Next**.



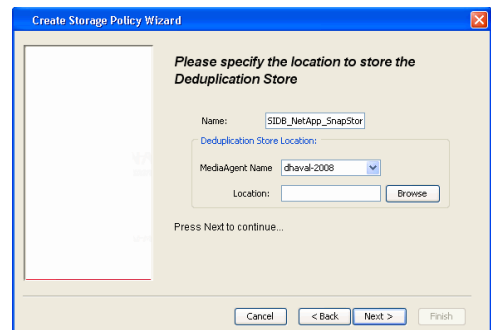
7. Click **Next**.



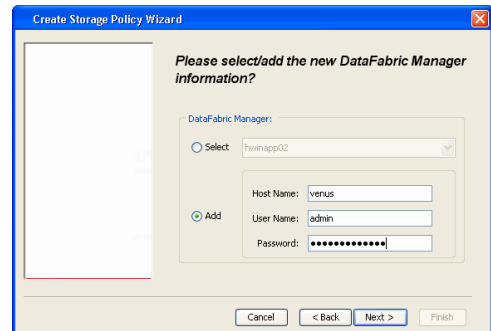
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

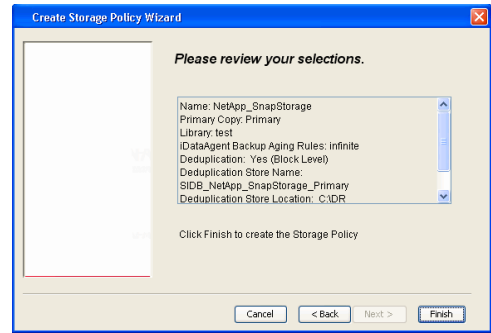


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



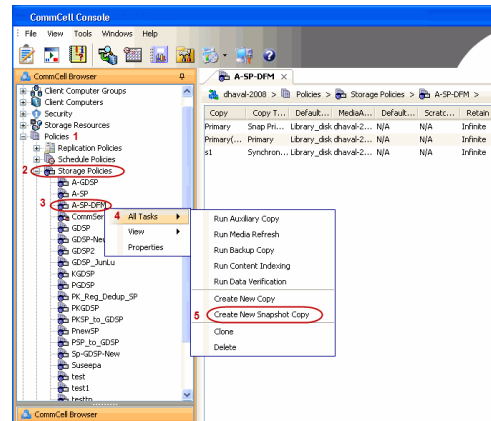


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

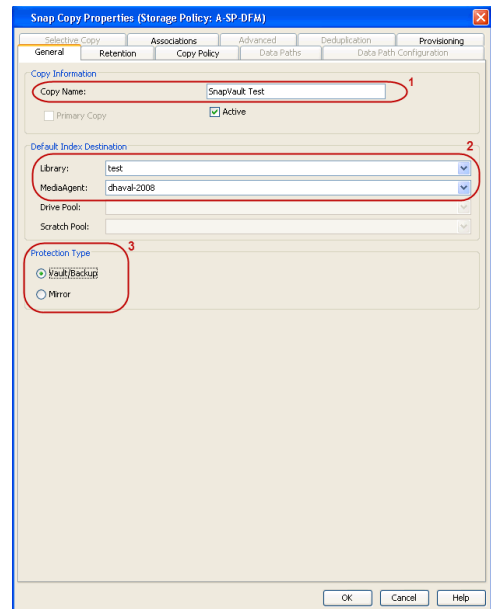
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
 - Enter the **Copy Name**.
 - Select the **Library** and **MediaAgent** from the drop-down list.
 - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

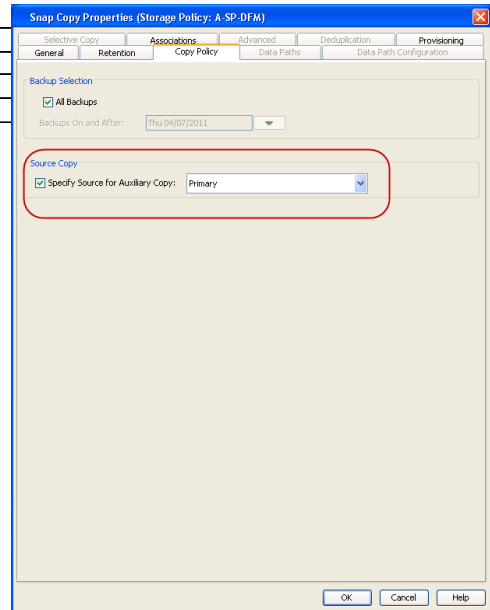


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

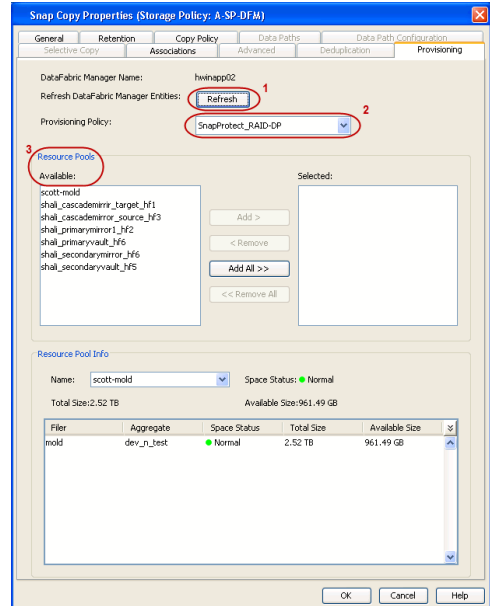
TOPOLOGY	SOURCE COPY
----------	-------------

Primary-Mirror	Primary
Primary-Mirror-Vault	Mirror
Primary-Vault	Primary
Primary-Vault-Mirror	Vault
Primary-Mirror-Mirror	Mirror



- Click the **Provisioning** tab.
 - Click **Refresh** to display the DFM entities.
 - Select the **Provisioning Policy** from the drop-down list.
 - Select the **Resource Pools** available from the list.
 - Click **OK**.

The secondary snapshot copy is created.



- If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:

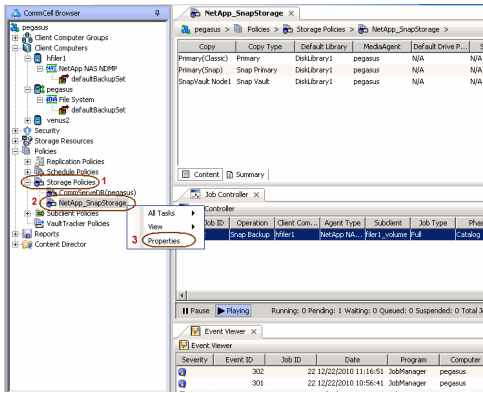

```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

It is recommended that you perform this operation on all nodes in the P-M-V topology.

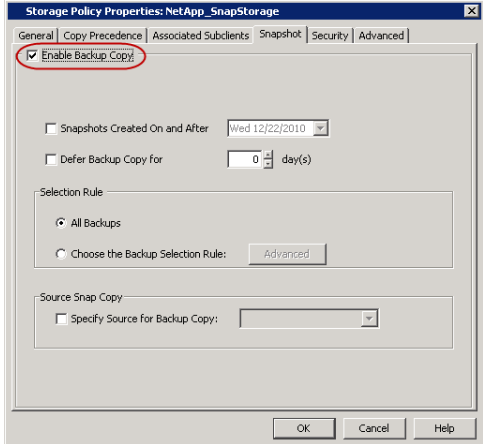
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

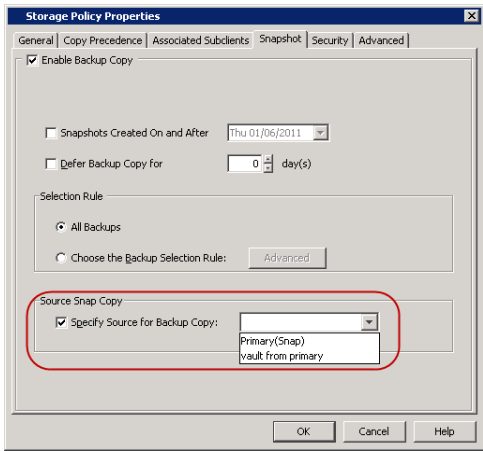
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.



3.
 - Select **Specify Source for Backup Copy**.
 - From the drop-down list, select the source copy to be used for performing the backup copy operation.



SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

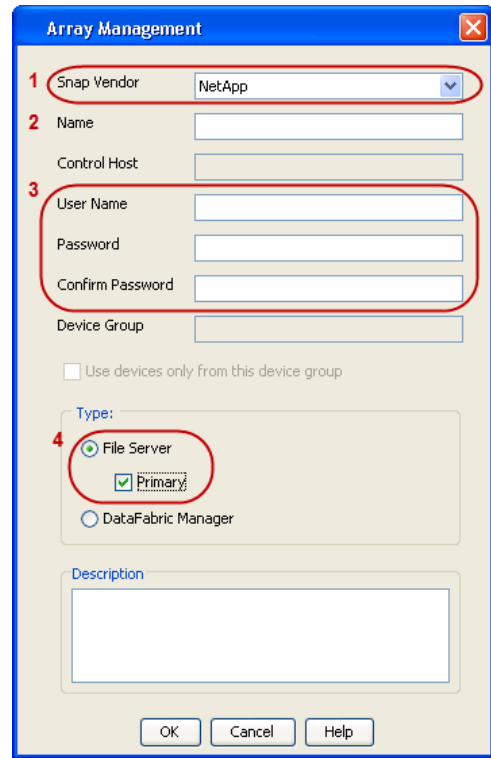
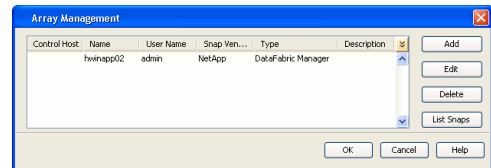
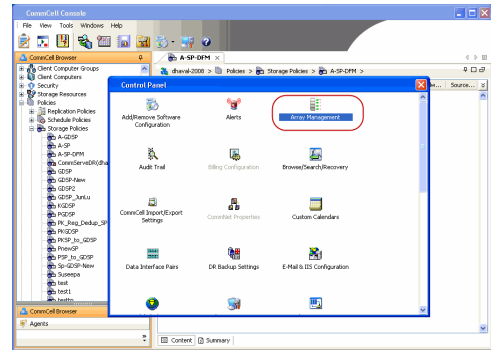
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

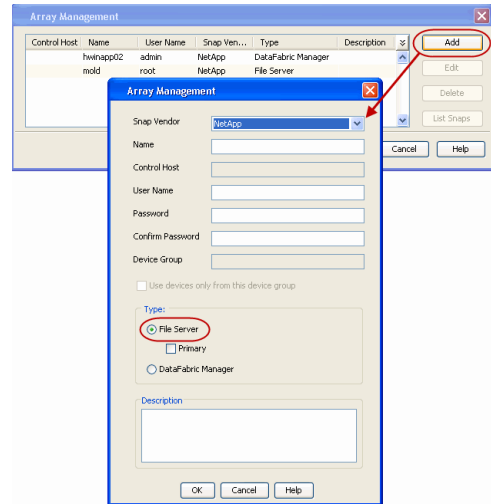
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

4.
 - Click **Add** again to enter the information for the secondary array.
 - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.





SEE ALSO

Import Wizard Tool

Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

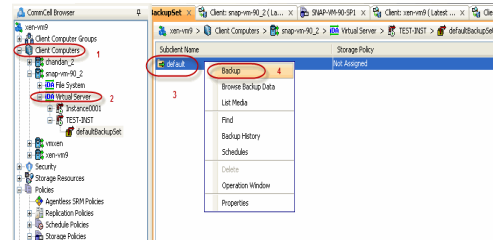
Getting Started - Microsoft Hyper-V Backup

PERFORM A BACKUP

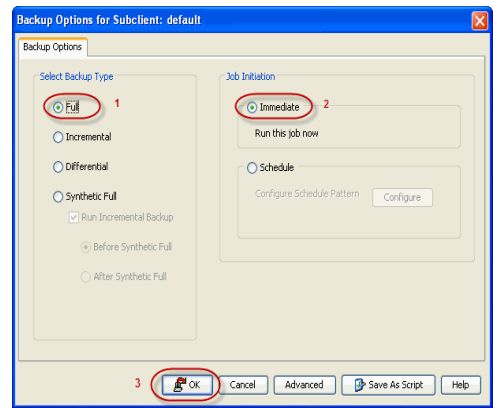
After configuring the Instance, BackupSet, and Subclient you are ready to perform your first backup.

The following section provides step-by-step instructions for running your first full backup of a single virtual machine immediately.

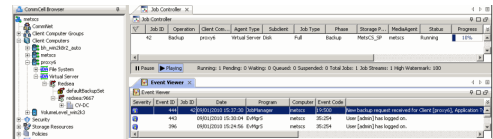
- From the CommCell Console, navigate to **Client Computers | Virtual Server**
 - Right-click the **Subclient** and click **Backup**.



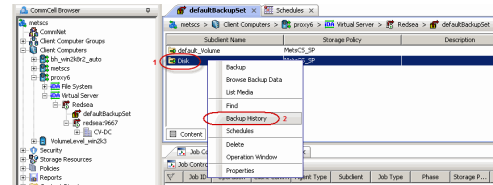
- Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.



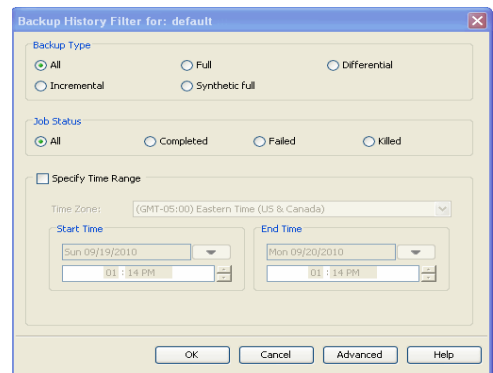
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



- Once job is complete, view the details of job from the **Backup History**. Right-click the **Subclient** and select **Backup History**.

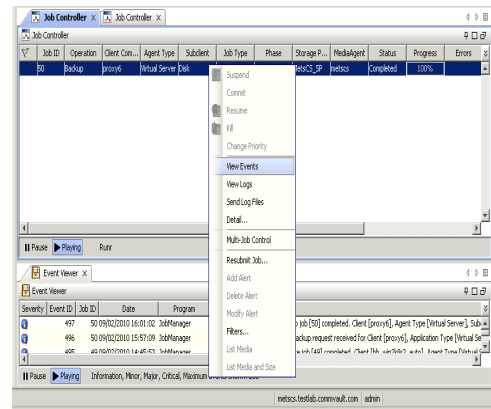


- Click **OK**.



- You can view the following details about the job by right-clicking the job:
 - Items that failed during the job
 - Items that succeeded during the job

- Details of the job
- Events of the job
- Log files of the job
- Media associated with the job



◀ Previous Next ▶

Getting Started - Vault/Mirror Copy



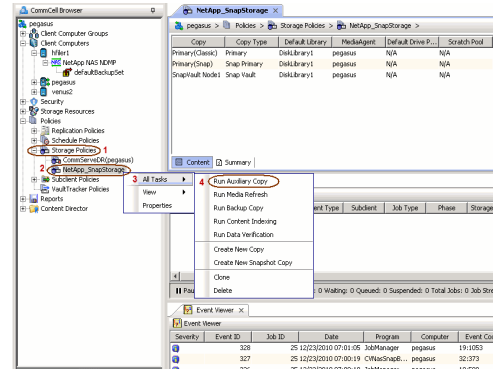
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** > to Continue.

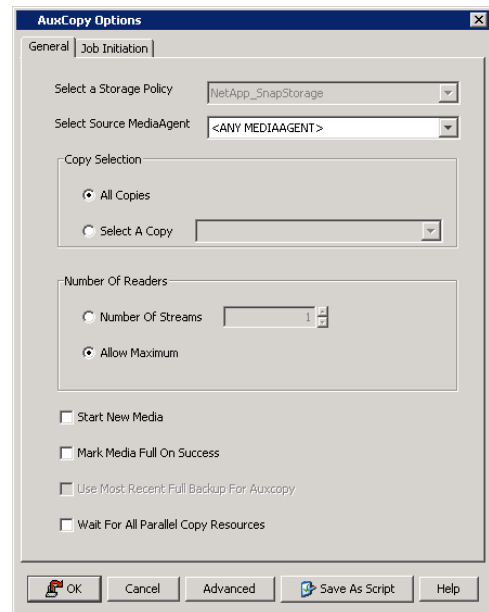
INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

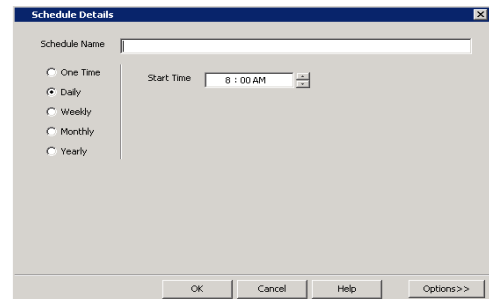


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.

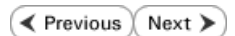


- Enter the schedule name and select the appropriate scheduling options.
 - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.



Getting Started - Snap Movement to Media

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

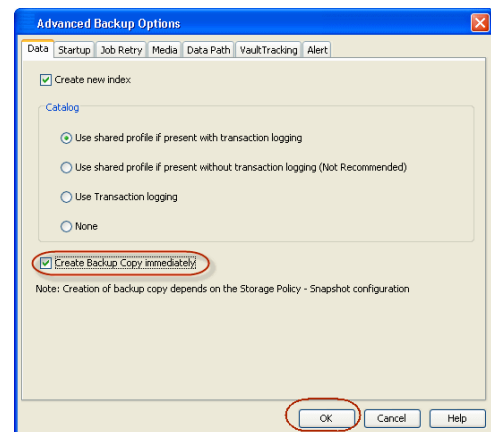
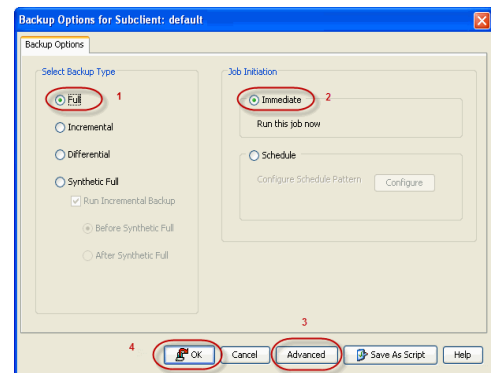
INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

1.
 - From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
 - Right click the default subclient and click **Backup**.
 - Select **Full** as backup type.
 - Click **Advanced**.

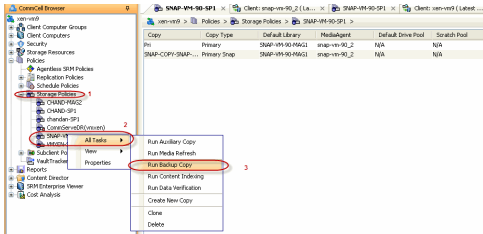
2.
 - Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



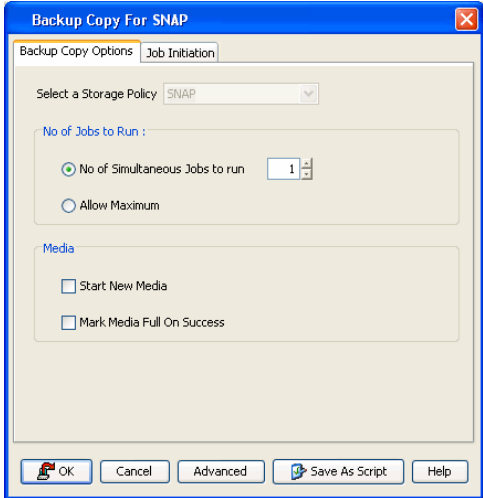
OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

1.
 - From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



Getting Started - Microsoft Hyper-V Restore

PERFORM A RESTORE

As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections describe the steps involved in restoring a virtual machine.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.

You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.

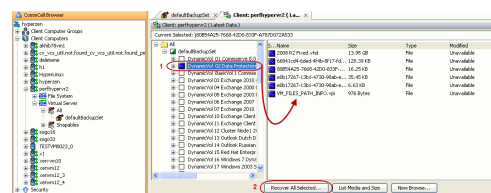
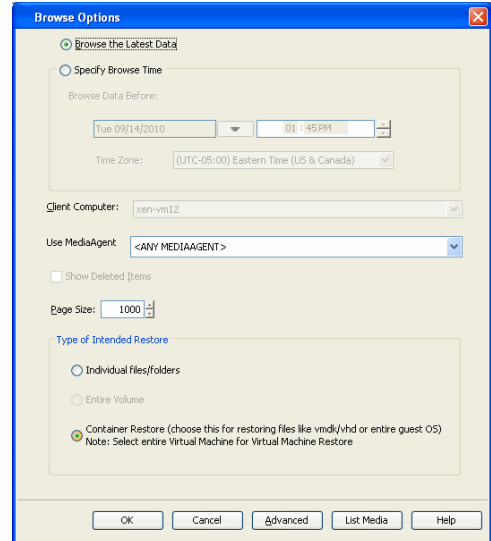
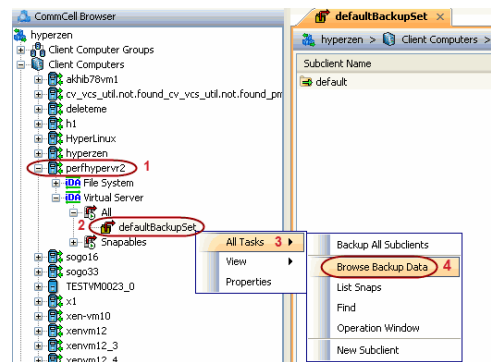
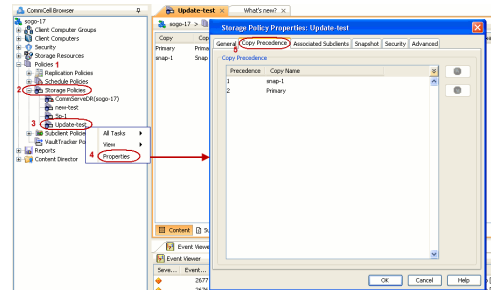
- Click **OK**.

- From the CommCell Console, navigate to **<Client> | Virtual Server**.
 - Right-click the backup set that contains the data you want to restore and click **All Tasks | Browse Backup Data**.

- Click **OK**.

- Select the virtual machine under the backup set. Its entire contents will be automatically selected in the right pane.
 - Click **Recover All Selected**.

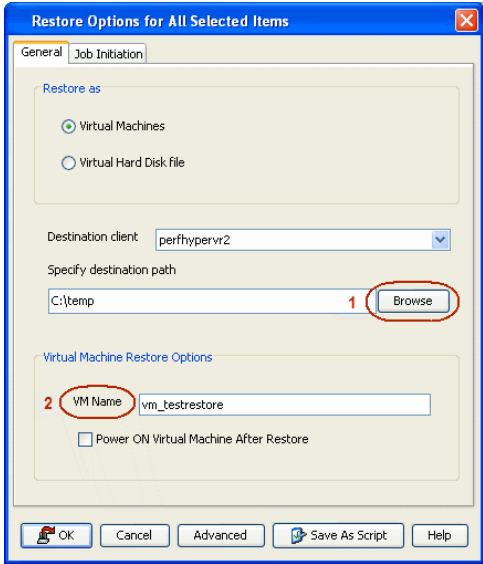
- Click **Browse** to locate the desired **Destination Path** in the currently selected



Destination Client.

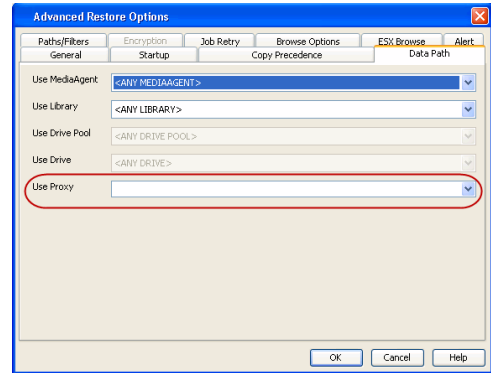
- Enter the **VM Name** for the virtual machine.

Ensure that you provide a fully qualified name for the virtual machine. Entering an IP address will cause the restore operation to fail.

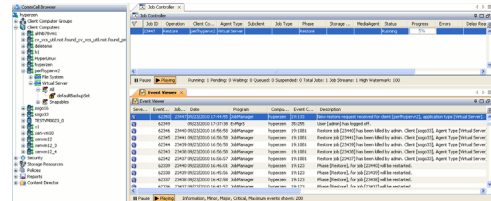


- Hyper-V Live migration cluster restores require the use of a proxy to mount the snapshots. If you have a Hyper-V cluster, do the following:

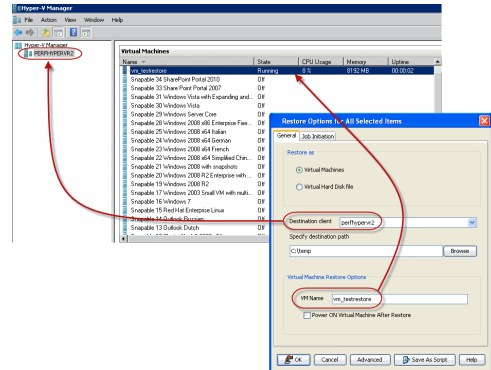
- Click **Advanced**.
- Select the **Data Path** tab.
- Select a proxy from the **Use Proxy** dropdown to mount the snapshot.
- Click **OK**.
- Click **OK** from the **Restore Options** dialog box.



- You can monitor the progress of the restore job in the **Job Controller** window of the CommCell Console.



- Once the virtual machine is restored, it is automatically mounted to the Hyper-V Server of the specified client computer.



CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.

Getting Started - SAP for Oracle iDataAgent Deployment in a Non-Global Zone



WHERE TO INSTALL

Install the software on each of the non-global zones where you have application data.

It is recommended to install the software on the global zone to protect non-changing or static data on non-global zones. If the data is dynamic or contains application data, install the software on the non-global zone.

INSTALL THE SAP FOR ORACLE iDATAAGENT

Use the following procedure to directly install the software from the installation package or a network drive.

- Logon to the client computer as **root** or as a sudo user.
If you are installing the software using a sudo user account, make sure that sudo user account is configured on this computer. For more information, see FAQ - Install.

- Mount the installation disc on the non-global zone.

```
mkdir <Non-Global Zone root location>/<Non-Global Zone local directory>
```

```
mount -F lofs <Global zone software Install Disc mount point> <Non-Global Zone root location>/<Non-Global Zone local directory>
```

Connect to Non-Global Zone terminal

- Run the following command from the Software Installation Package:

```
./cvpkgadd
```

- The product banner and other information is displayed.

Press **Enter**.

- Read the license agreement. Type **y** and press **Enter**.

- Press **Enter**.

- Press **Enter**.

- 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 interface name that you wish to use as default, and then press **Enter**.

The interface names and IP addresses depend on the computer in which

BEFORE YOU BEGIN

Download Software Packages

Download the latest software package to perform the install.

SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.

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
- 2) Advance options
- 3) Exit this menu

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.

You now have a choice of performing a regular Calypso install on the physical host or installing Calypso on a virtual machine for operation within a cluster.

Most users should select "Install on a physical machine" here.

- 1) Install on a physical machine
- 2) Install on a virtual machine
- 3) Exit

Your choice: [1]

We found one network interface available on your machine. We will associate it with the physical machine being installed, and it will also be used by the CommServe to connect 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.

the software is installed and may be different from the example shown.

9. Press **Enter**.

10. Type the number associated with the **SAP for Oracle iDataAgent, Unix File System iDataAgent**, and the **MediaAgent**.

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

12. Press **Enter**.

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

- Select **Download from the software provider website** to download the latest software scripts. Make sure you have internet access.
- Select **Use the one in the installation media** to install the software scripts from the package or share from which the installation is currently being 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.

14. Press **Enter**.

15. Press **Enter** to accept the default path.

- If you want to specify a different path, type the path and then press **Enter**.
- If you want to install the software binaries to an NFS shared drive, specify the directory on which you have mounted the NFS file system and then press **Enter**.

Please check the interface name below, and make connections if necessary:

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]

Please select the Calypso module(s) that you would like to install.

```
[ ] 1) UNIX File System iDataAgent [1101] [CVGxIDA]
[ ] 2) MediaAgent [1301] [CVGxMA]
[ ] 3) ProxyHost iDataAgent [1102] [CVGxProxyIDA]
[ ] 4) Documentum iDataAgent [1126] [CVGxDctmIDA]
[ ] 5) Oracle iDataAgent [1204] [CVGxOrIDA]
[ ] 6) SAP for Oracle [1205] [CVGxOrSAP]
[ ] 7) SAP for MaxDB [1206] [CVGxSAPMAXDB]
[ ] 8) Informix iDataAgent [1201] [CVGxIfIDA]
[ ] 9) Sybase iDataAgent [1202] [CVGxSybIDA]
[ ] 10) DB2 iDataAgent [1207] [CVGxDB2]
[ ] 11) MySQL iDataAgent [1208] [CVGxMySQL]
[ ] 12) PostGres iDataAgent [1209] [CVGxPostGres]
[ ] 13) Lotus Notes Database iDataAgent [1051]
[CVGxLndbIDA]
>) >>>>>>>>>> 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: 1 2 6
```

Please select the Calypso module(s) that you would like to install.

```
[X] 1) UNIX File System iDataAgent [1101] [CVGxIDA]
[X] 2) MediaAgent [1301] [CVGxMA]
[ ] 3) ProxyHost iDataAgent [1102] [CVGxProxyIDA]
[ ] 4) Documentum iDataAgent [1126] [CVGxDctmIDA]
[ ] 5) Oracle iDataAgent [1204] [CVGxOrIDA]
[X] 6) SAP for Oracle [1205] [CVGxOrSAP]
[ ] 7) SAP for MaxDB [1206] [CVGxSAPMAXDB]
[ ] 8) Informix iDataAgent [1201] [CVGxIfIDA]
[ ] 9) Sybase iDataAgent [1202] [CVGxSybIDA]
[ ] 10) DB2 iDataAgent [1207] [CVGxDB2]
[ ] 11) MySQL iDataAgent [1208] [CVGxMySQL]
[ ] 12) PostGres iDataAgent [1209] [CVGxPostGres]
[ ] 13) Lotus Notes Database iDataAgent [1051]
[CVGxLndbIDA]
>) >>>>>>>>>> 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: d
```

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]

Please specify where you want us to install Calypso binaries.

It must be a local directory and there should be at least 176MB 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".

In order to make sure that the client computer has `read/write` access to NFS shared drive, review the steps described in `Installing Software Binaries to an NFS Shared Drive`.

Do not use the following characters when specifying the path:

`!@#$%^&*():/?\`

16. Press **Enter** to accept the default location.

- Enter a path to modify the default location and press **Enter**.
- All the modules installed on the computer will store the log files in this directory.

17. Type **Yes** and press **Enter**.

18. Type the **Group name** and then press **Enter**.

19. This prompt is relevant only when you install on Solaris. Press **Enter** to accept the default value for **Number of Streams**.

You can type the **Number of Streams** that you plan to run at the same time and then press **Enter**.

20. Press **Enter** if you do not want the changes to be updated automatically.

- If you want the changes to be made automatically, type **Yes** and then press **Enter**.
- You will come across this prompt when you install the software on the earlier versions of Solaris.

21. Press **Enter**.

You will see this prompt if you have accepted the default **no** and pressed **Enter** in the above step.

22. Press **Enter**.

You will see this message if you have accepted the default answer and pressed **Enter** in step 20.

Installation Directory: [/opt]

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]

Most of Software processes run with root privileges, but some are launched by databases and inherit database access rights. To make sure that registry and log files can be written to by both kinds of processes we can either make such files world-writeable or we can grant write access only to processes belonging to a particular group, e.g. a "calypso" or a "dba" group.

We highly recommend now that you create a new user group and enter its name in the next setup screen. If you choose not to assign a dedicated group to Software processes, you will need to specify the access permissions later.

If you're planning to backup Oracle DB you should use "dba" group.

Would you like to assign a specific group to Software?
[yes]

Please enter the name of the group which will be assigned to all Software files and on behalf of which all Software 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 "oinstall" group here.

Group name: oinstall

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 "oinstall".

Number of Streams

IMPORTANT : Please read install document "Configure Kernel Parameters - Unix/Macintosh" from "Books Online" before you start configuring kernel parameters. Please enter the total number of streams that you plan to run at the same time. We need to make sure that you have enough semaphores and shared memory segments configured in /etc/system.

Number of streams [10]

We now need to modify the /etc/system configuration file on this computer. It is done to make sure that there will be enough shared memory and semaphores available for Calypso programs. Please review the changes below and answer "yes" if you want us to apply them to the /etc/system file. Otherwise, the installation will proceed, the changes will be saved to some other file, and you will have to apply them manually.

set shmsys:shminfo_shmmni=8570 (was 7930)

set shmsys:shminfo_shmseg=8420 (was 7780)

set semsys:seminfo_semmns=10320 (was 9680)

set semsys:seminfo_semmni=8570 (was 7930)

set semsys:seminfo_semmsl=8570 (was 7930)

Do you want us to apply these changes now? [no]

Changes saved into /etc/system.gal.1744

Press <ENTER> to continue.

Although a 'no' answer can be selected to this question during install, the user should make sure the min requirements (below) for shared memory are met, otherwise the backups may fail (the message in logs is 'could not start the pipeline').

set shmsys:shminfo_shmmax=4199304

set shmsys:shminfo_shmmni=1

set semsys:shminfo_shmmni=640

set semsys:shminfo_shmseg=640

set semsys:seminfo_semmns=640

23. 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**.
24. If you do not wish to configure the firewall services, press **Enter**.

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

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.
25. Type the fully qualified CommServe host name and press **Enter**.

Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.
26. Press **Enter**.
27. Type the appropriate number to select the **Client Group** and press **Enter**.

This screen will be displayed only if Client Groups are configured for the CommCell
28. A confirmation screen will mark your choice with an "**X**".
Type **d** for **Done**, and press **Enter**.
29. Enter the number associated with the storage policy you want use and press **Enter**.
30. Type the path of the **SAPEXE** directory and then press **Enter**.
31. Type **3** to the **Exit** option and press **Enter**.
The installation is now complete.
- ```

set semsys:seminfo_semmni=640
set semsys:seminfo_semmsl=640
set maxusers=256
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 : [8400]
Port Number for EvMgrC: [8402]

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

Please specify hostname of the CommServe below. Make sure the hostname is fully qualified, resolvable by the name services configured on this machine.
CommServe Host Name: mycommserve.company.com

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.

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(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.
[] 1) Unix
[] 2) DR
[a=all n=none r=reverse q=quit d=done >=next <=previous ? =help]

Enter number(s)/one of "a,n,r,q,d,>,<," here: 1

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.
[X] 1) Unix
[] 2) DR
[a=all n=none r=reverse q=quit d=done >=next <=previous ? =help]

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

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

1) SP_StandAloneLibrary2_2
2) SP_Library3_3
3) SP_MagLibrary4_4

Storage Policy: [1]

Please specify the location of SAPEXE directory.
SAPEXE:

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

```

angel.company.com.

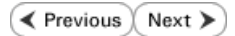
Now you have a choice of either adding another package to the existing installation or configure Calypso on a virtual machine for use in a cluster.

- 1) Add another package to angel.company.com
- 2) Install Calypso on a virtual machine
- 3) Exit

Your choice: [3]



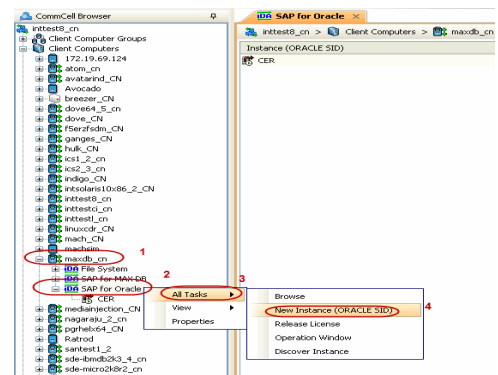
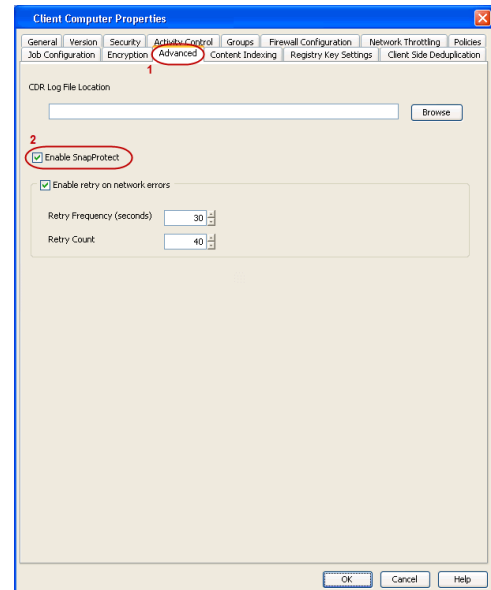
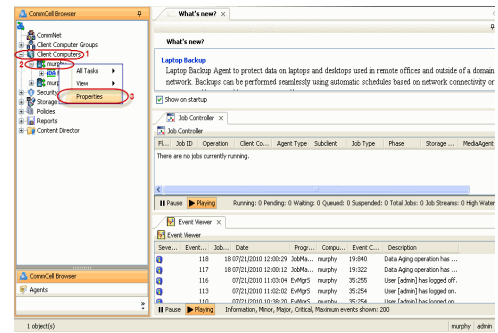
# Getting Started - SAP for Oracle Configuration



## CONFIGURATION

Once the SAP for Oracle *iDataAgent* has been installed, configure an Instance to facilitate backups. Each instance references an Oracle database. Also it is recommended to create separate subclients for data and log backups. The following sections provide the necessary steps required to create and configure these components for a first SnapProtect backup of an Oracle database.

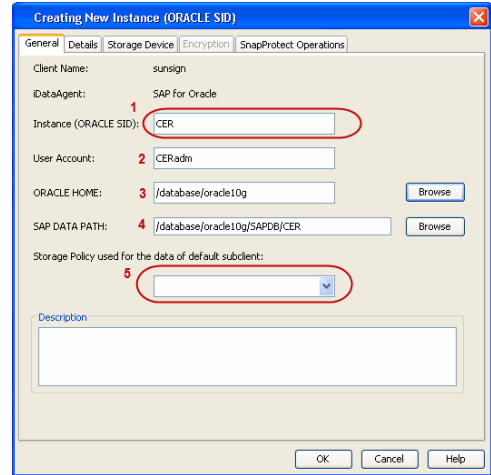
1.
  - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
  - Right-click the client and select **Properties**.
  
2.
  - Click on the **Advanced** tab.
  - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
  - Click **OK**.
  
3.
  - From the CommCell Browser, navigate to **<Client>** | **SAP for Oracle**.
  - Right-click **SAP for Oracle** and click **All Tasks** | **New Instance (ORACLE SID)**.
  
4.
  - Enter the **Instance Name**.
  - Enter the user name in **User Account** to access the Oracle application on a Unix client.  
Use `<SID_name>adm,` in order to perform backup and restore operations from CommCell Console for the associated instance.





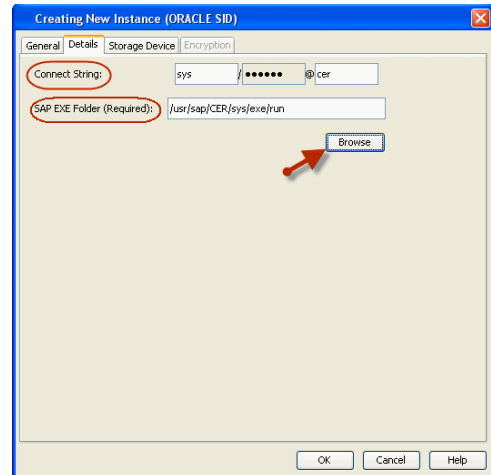
Make sure that the user has administrator privileges to access the Oracle application.

- **Browse** or enter the path to the Oracle application files in **Oracle Home**.
- **Browse** or enter the path to the Oracle data and control files in **SAP DATA PATH**.
- Select a **Storage Policy** from the drop down list.



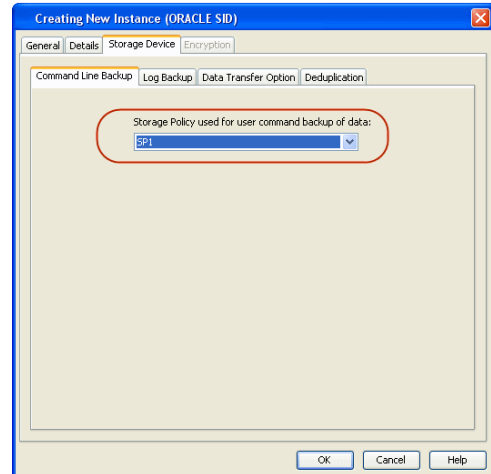
5. Click **Details** tab and add the following information:

- Enter the target database connect string in **Connect String**.
- **Browse** or enter the path to the SAP EXE folder in **SAP EXE Folder (Required)**.



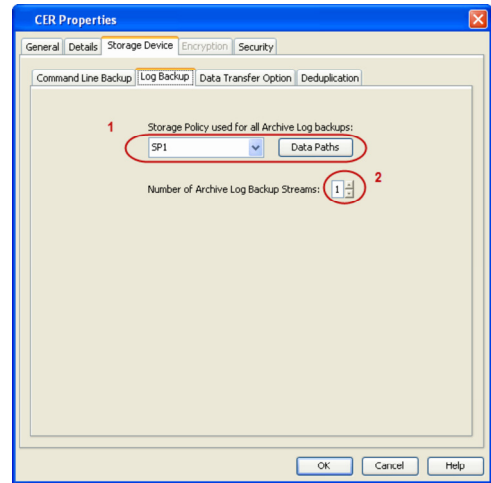
6. • Click **Storage Device** tab.

- Select a **Storage Policy used for user command backup of data** from the drop down list.

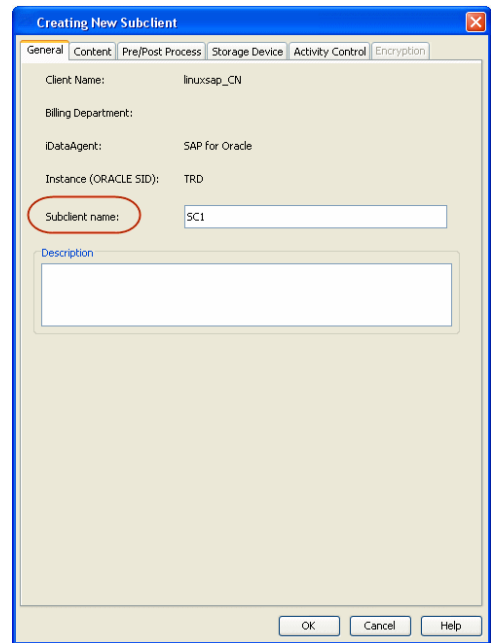
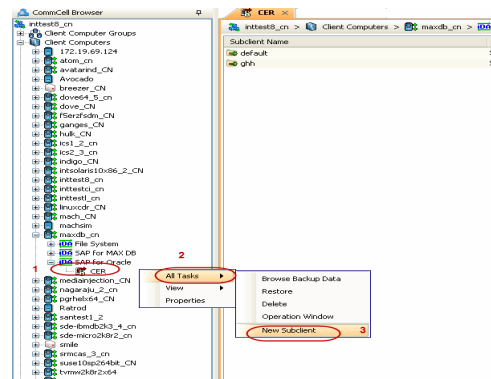


- 7.
- Click **Log Backup** tab.
  - Select a **Storage Policy used for all Archive Log backups** from the drop down list.
  - Click **OK**.

8.
  - From the CommCell Browser, navigate to **<Client> | SAP for Oracle**.
  - Right-click the **<Instance>** and click **All Tasks | New Subclient**.



9. In the **Subclient Name** field, type a name.

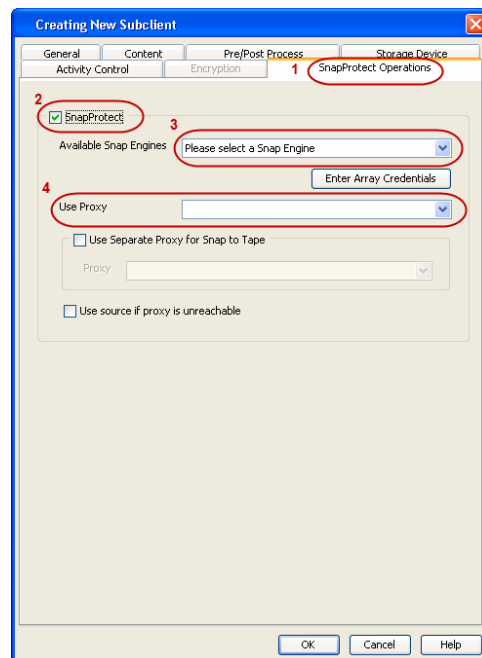


10.
  - Click the **SnapProtect Operations** tab.
  - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
  - Select the storage array from the **Available Snap Engine** drop-down list.
  - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy operations will be performed.

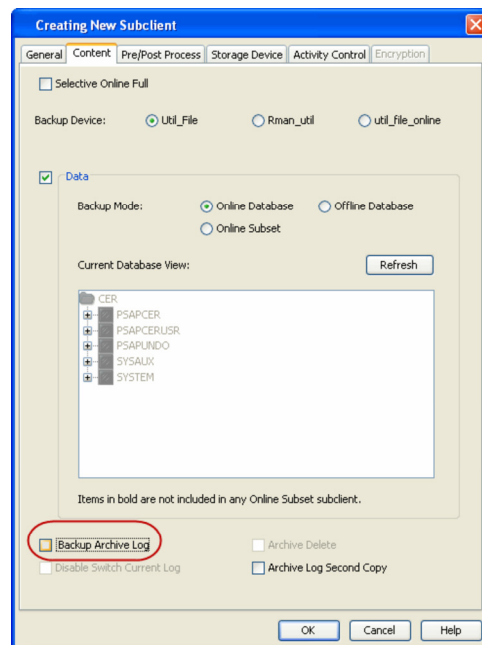
When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent.

Select the MediaAgent from the **Proxy** list.

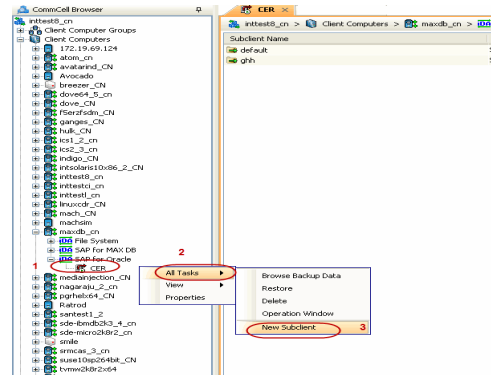
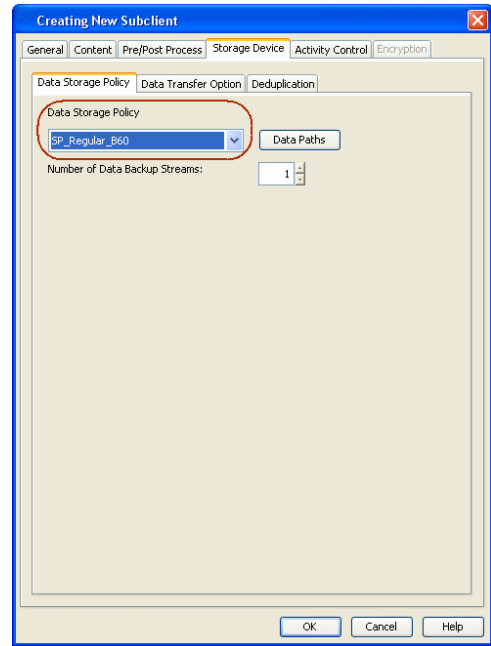


11. Click the **Content** tab and clear the check box for **Backup Archive Log**.

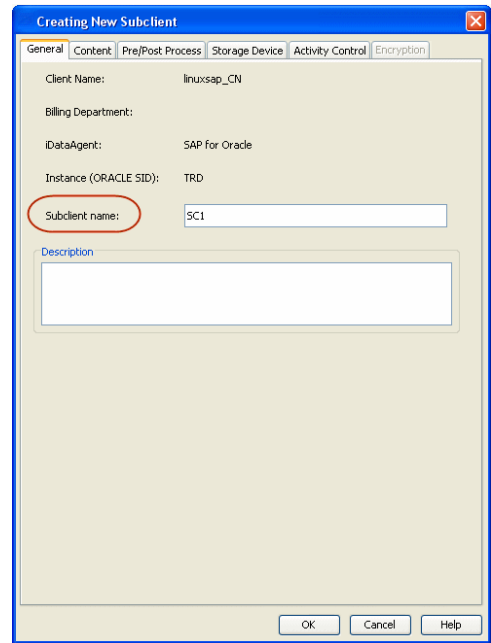


12.
  - Click the **Storage Device** tab.
  - Select a **Data Storage Policy** from the drop down list.
  - Click **OK**.

13.
  - From the CommCell Browser, navigate to <Client> | SAP for Oracle.
  - Right-click the <Instance> and click **All Tasks | New Subclient**.

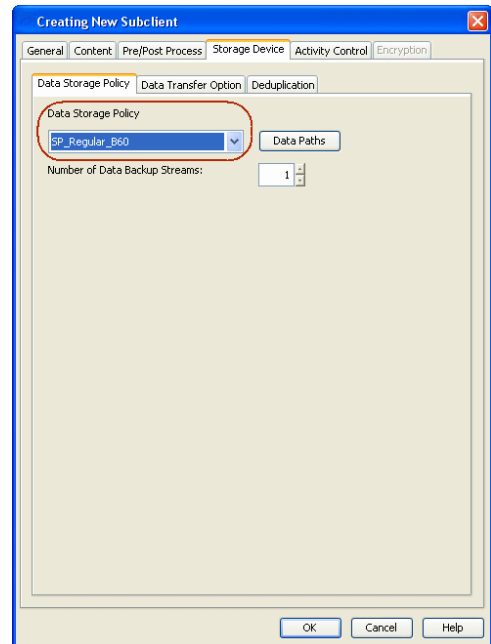
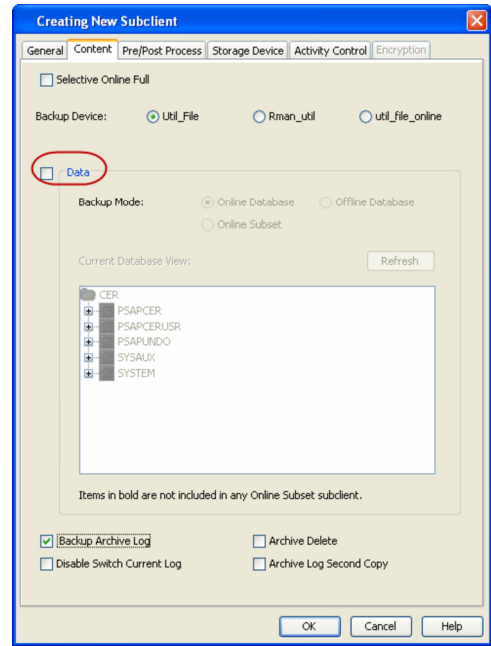


14. In the **Subclient Name** field, type a name.



15. Click the **Content** tab and clear the check box for **Data**.

16.
  - Click the **Storage Device** tab.
  - Select a **Data Storage Policy** from the drop down list.
  - Click **OK**.



## SKIP THIS SECTION IF NOT USING SOLARIS.

Click **Next** > to Continue.

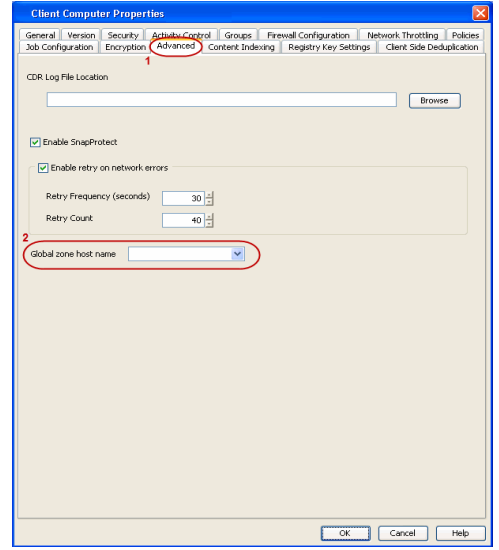
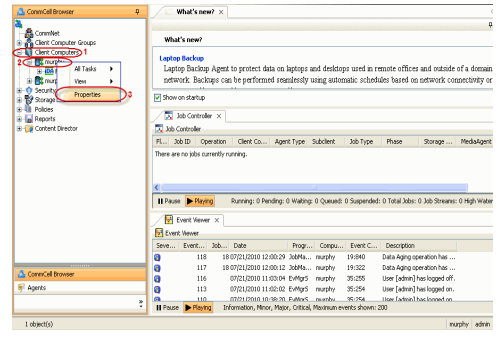
## ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE

**Next** >

Follow the steps given below to enable SnapProtect backups on each of the non-global zone clients containing the application data.

1.
  - From the CommCell Console, navigate to **Client Computers** | <Client>.
  - Right-click the client and select **Properties**.

- Click **Advanced** tab.
  - Select the **Global Zone host name** from the drop-down list.
  - Click **OK**.
    - We support disks on a global zone mounted using loopback File System on a non global zone.
    - This option need not be enabled if you are using a NFS share. This is because when using NFS mount paths, the operations are limited to the non-global zone and does not use the global zone.



- Repeat the above steps on all the non-global zone clients containing the application data.

## SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

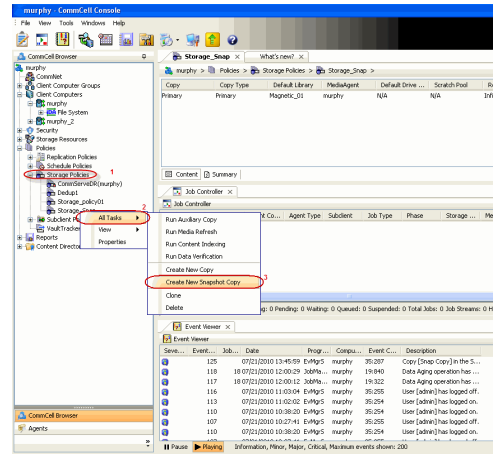
Click **Next** to Continue.

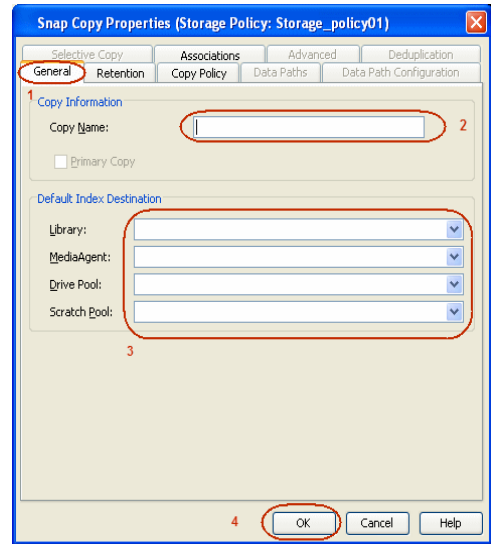
## CREATE A SNAPSHOT COPY



Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.
- Enter the copy name in the **Copy Name** field.
  - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
  - Click **OK**.

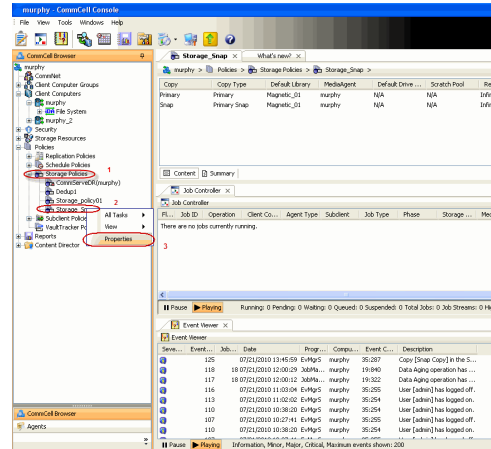




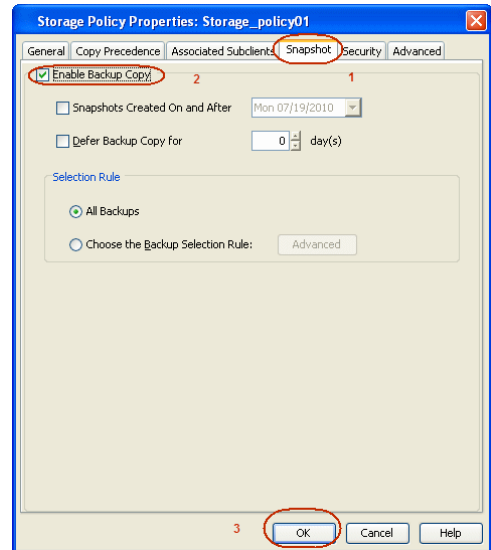
## CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Browser, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.



- Click the **Snapshot** tab.
  - Select **Enable Backup Copy** option to enable movement of snapshots to media.
  - Click **OK**.



# Storage Array Configuration

◀ Previous   Next ▶

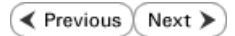
## CHOOSE THE STORAGE ARRAY

| HARDWARE STORAGE ARRAYS          | SOFTWARE STORAGE ARRAY |
|----------------------------------|------------------------|
| 3PAR                             | DATA REPLICATOR        |
| DELL COMPELLENT                  |                        |
| DELL EQUALLOGIC                  |                        |
| EMC CLARIION, VNX                |                        |
| EMC SYMMETRIX                    |                        |
| FUJITSU ETERNUS DX               |                        |
| HITACHI DATA SYSTEMS             |                        |
| HP EVA                           |                        |
| IBM SVC                          |                        |
| IBM XIV                          |                        |
| LSI                              |                        |
| NETAPP                           |                        |
| NETAPP WITH SNAPVAULT/SNAPMIRROR |                        |

◀ Previous   Next ▶



# SnapProtect™ Backup - 3PAR



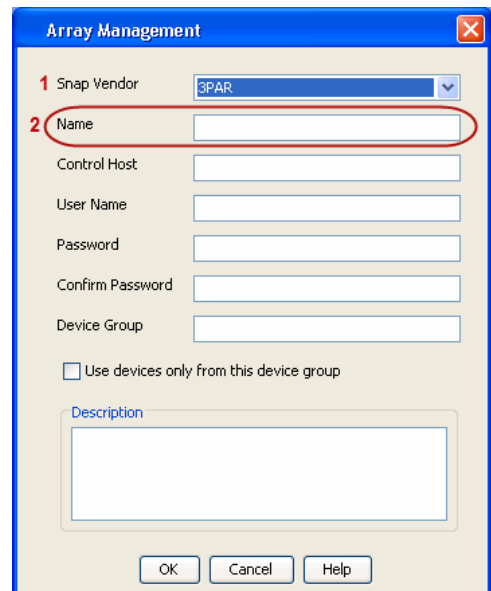
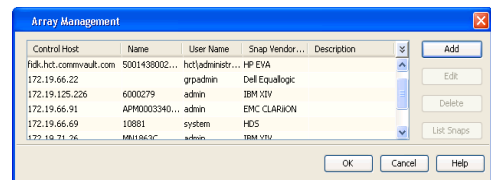
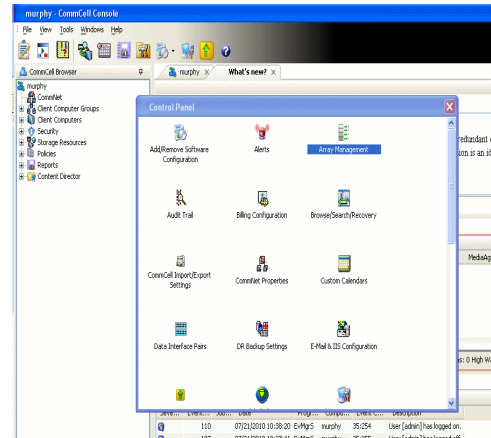
## PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
  - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where  $\text{DevID.substr}(4,3)$  is the next 3 digits after the fourth digit from the WWN number

where  $\text{DevID.substr}(12,4)$  is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$  is 2AC and  $\text{DevID.substr}(12,4)$  is 0B95

After adding all the values, the resulting array name is 2FF70002AC00B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where  $\text{DevID.substr}(4,3)$  is the next 3 digits after the fourth digit from the WWN number

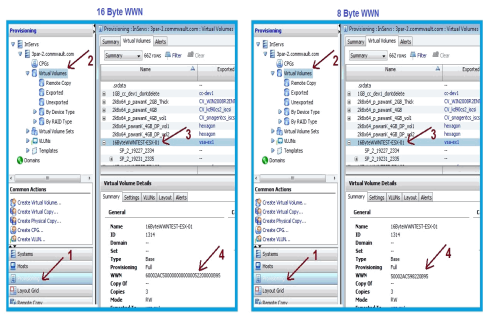
where  $\text{DevID.substr}(26,6)$  is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$  is 2AC and  $\text{DevID.substr}(26,6)$  is 000B95

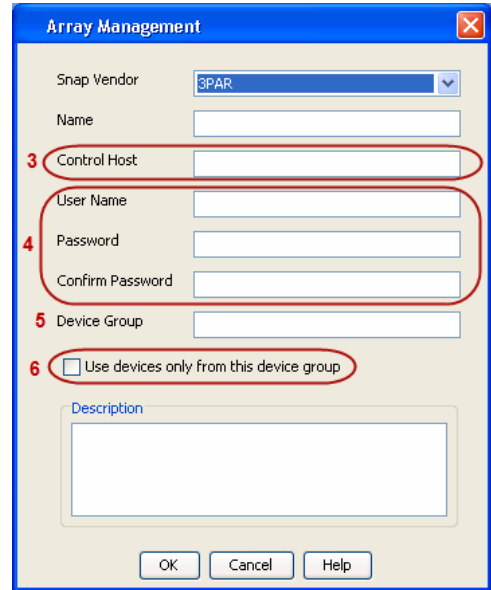
After adding all the values, the resulting array name is 2FF70002AC000B95.



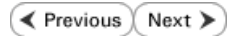
- Enter the IP address of the array in the **Control Host** field.
  - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - Dell EqualLogic



## PRE-REQUISITIES

### WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

### UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

### FIRMWARE VERSION

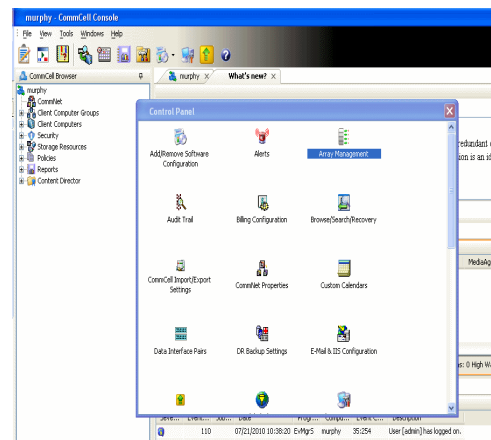
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
  - Create a new group administration account in the firmware, and set the desired permissions for this account.
  - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

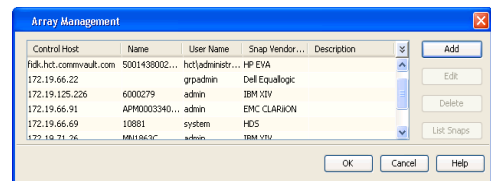
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



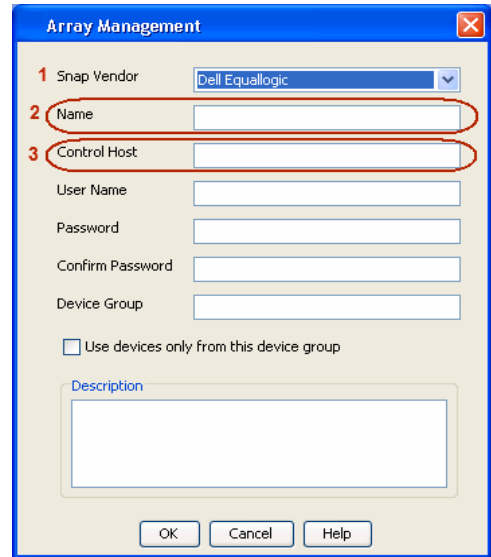
2. Click **Add**.



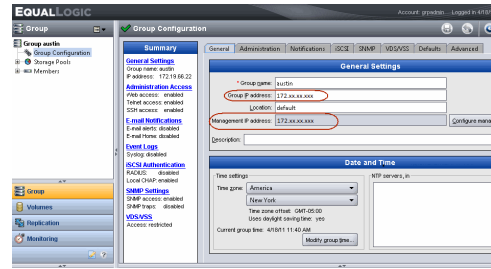
3.
  - Select **Dell Equallogic** from the **Snap Vendor** list.
  - Specify the Management IP address in the **Name** field.

No entry is required in the **Name** field if there is no Management IP address configured.

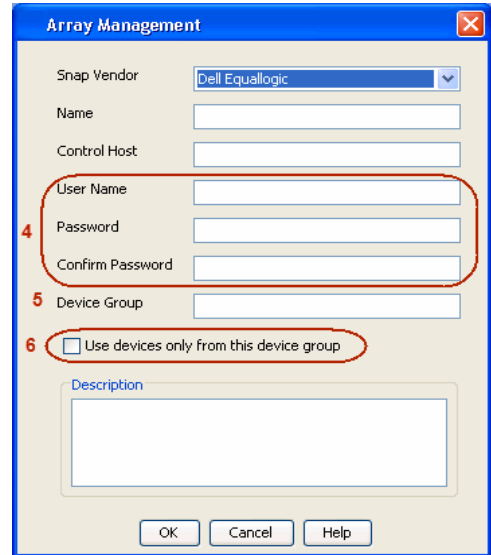
- Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
  - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
  - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
  - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.



# SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous   Next ▶

## PRE-REQUISITES

### LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

### ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.  
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.  
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

## SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG\_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



## AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

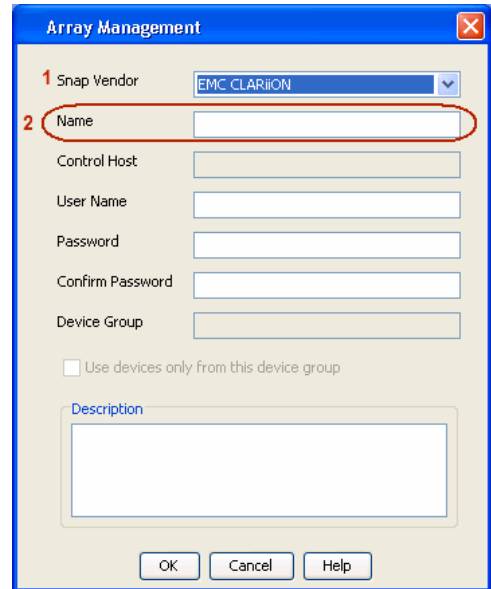
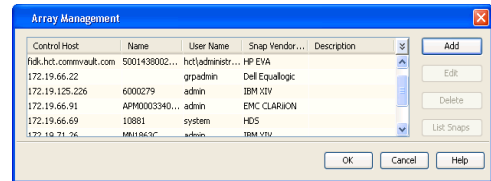
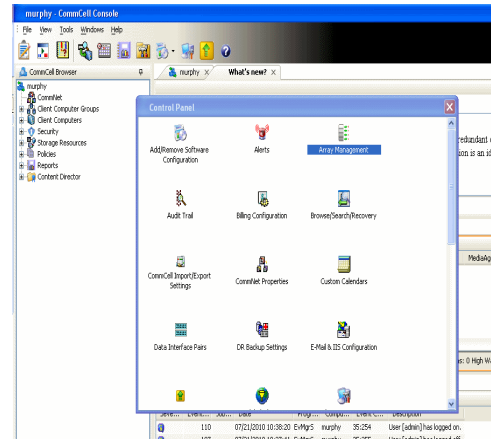
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

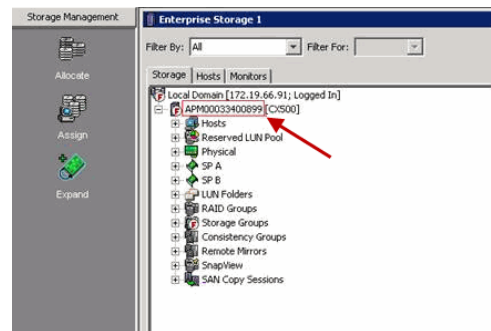
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
  - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.



- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.

**Array Management** [Close]

Snap Vendor:

Name:

Control Host:

User Name:

**3** Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

OK Cancel Help

◀ Previous Next ▶



# SnapProtect™ Backup - EMC Symmetrix

◀ Previous    Next ▶

## PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

## SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

## CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

## LOAD THE SYMMETRIX DATABASE

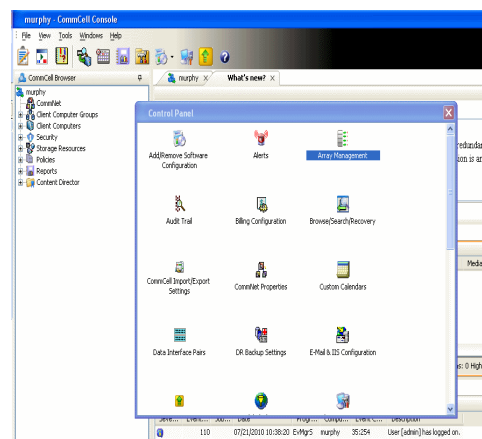
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

## SETUP THE ARRAY INFORMATION

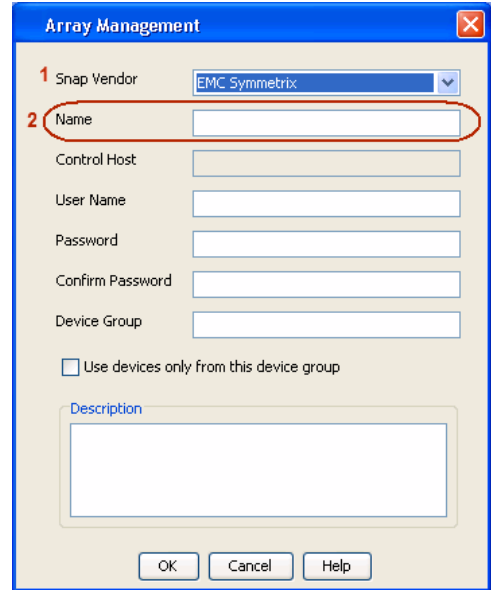
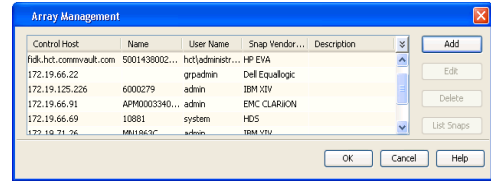
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

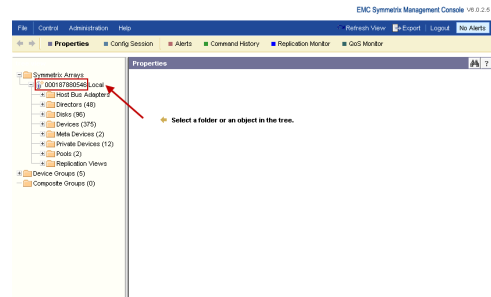


2. Click **Add**.

3.
  - Select **EMC Symmetrix** from the **Snap Vendor** list.
  - Specify the **Symm ID** of the array in the **Name** field.

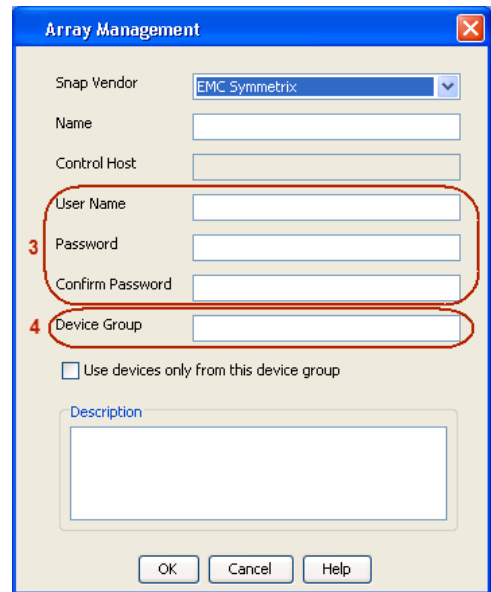


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
  - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.  
If you do not specify a device group, the default device group will be used for snapshot operations.
  - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).



# SnapProtect™ Backup - Hitachi Data Systems



## PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
  - COW pools
  - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

## ADDITIONAL REQUIREMENTS FOR VMWARE

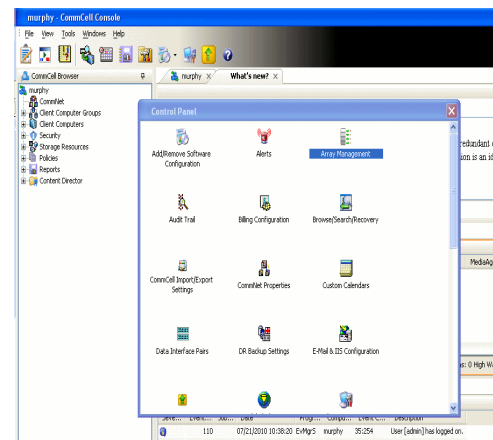
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server iDataAgent client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server iDataAgent client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

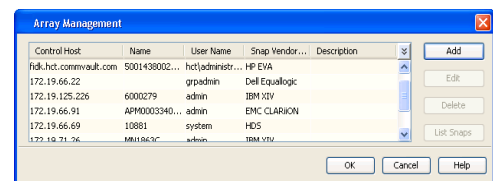
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

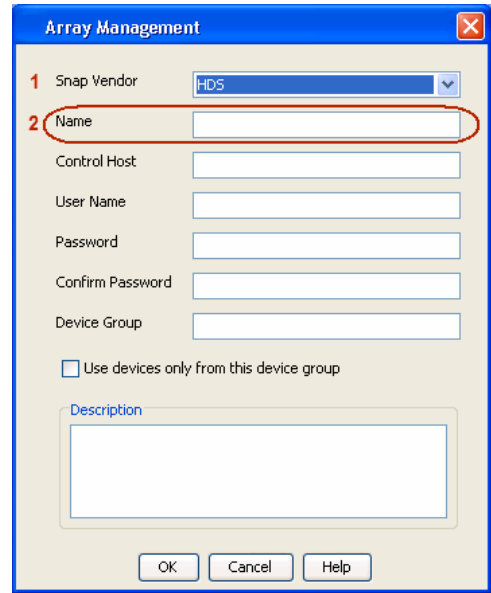
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



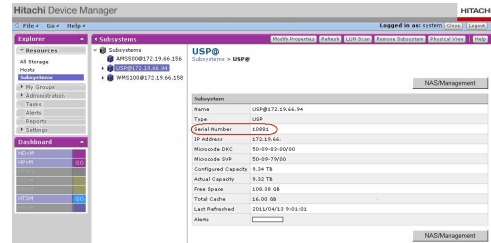
2. Click **Add**.



3.
  - Select **HDS** from the **Snap Vendor** list.
  - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



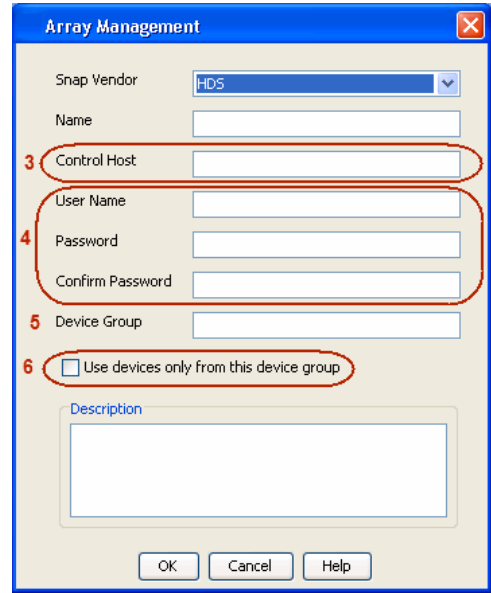
4.
  - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
  - Enter the user access information in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:

<COW\_POOL\_ID>-<LABEL> or <LABEL>-<COW\_POOL\_ID>

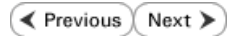
where <COW\_POOL\_ID> (for COW job) should be a number. This parameter is required.

<LABEL> (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - HP StorageWorks EVA



## SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

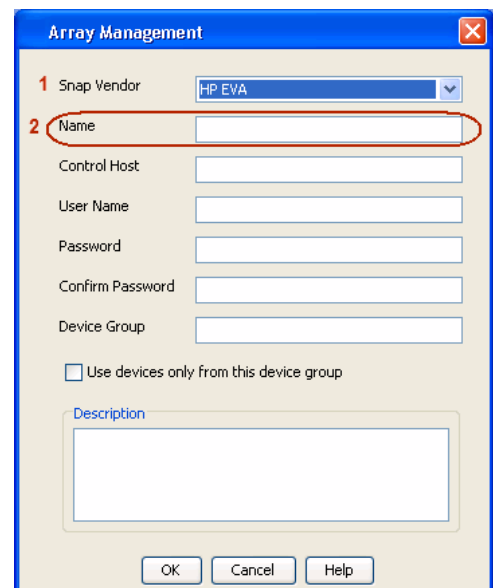
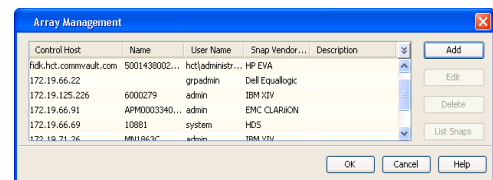
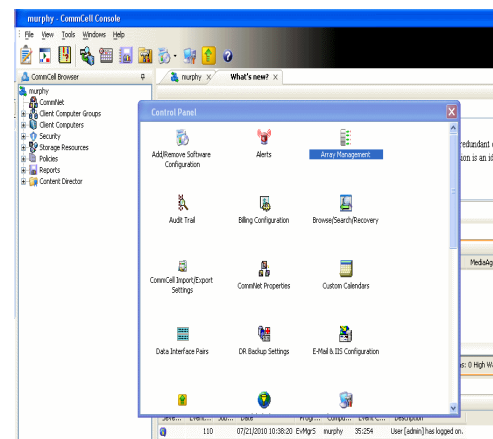
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin folder to discover the HP-EVA arrays.
3. Use the CLIRefreshTool.bat tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin folder.

## SETUP THE ARRAY INFORMATION

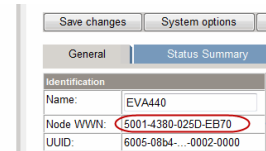
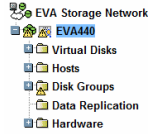
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
2. Click **Add**.
3.
  - Select **HP EVA** from the **Snap Vendor** list.
  - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

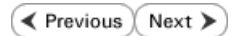
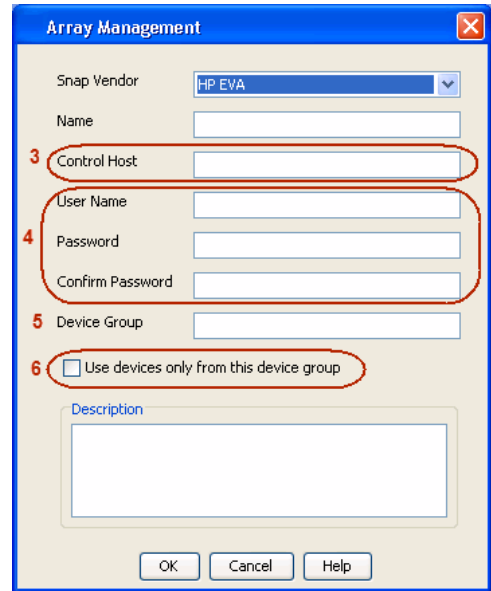
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



- 4.
- Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous   Next ▶

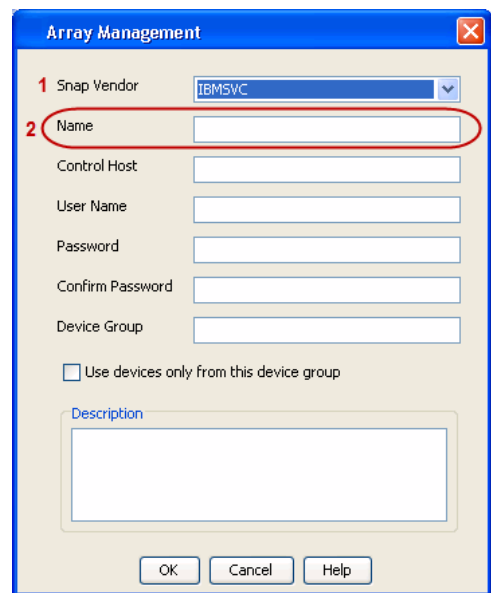
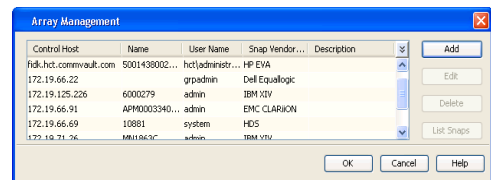
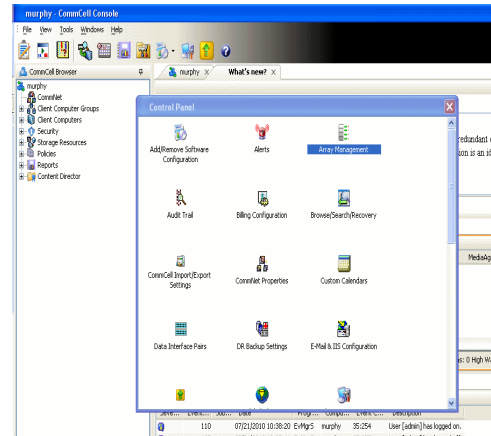
## PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

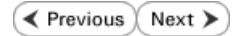
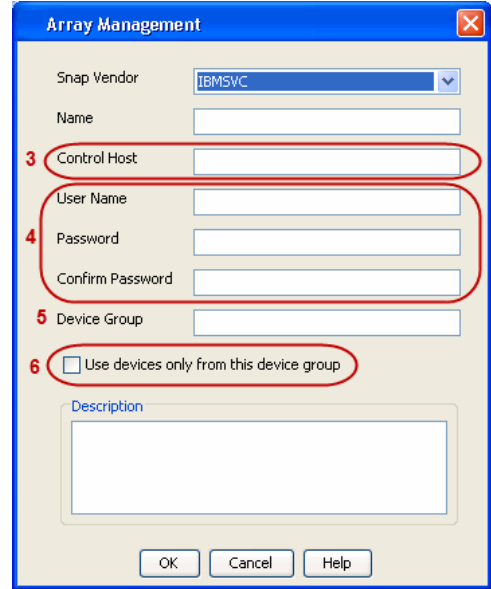
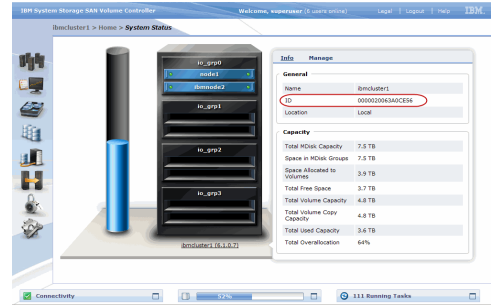
- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
  - Specify the 16-digit ID of the storage device in the **Name** field.



The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

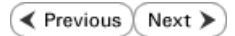
4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.  
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.





# SnapProtect™ Backup - IBM XIV



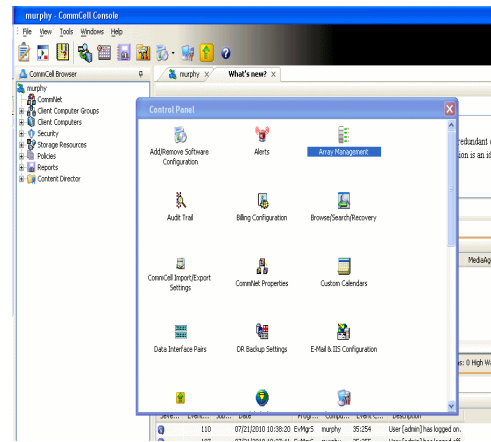
## PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

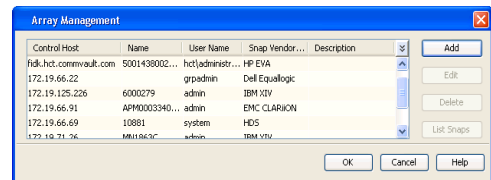
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

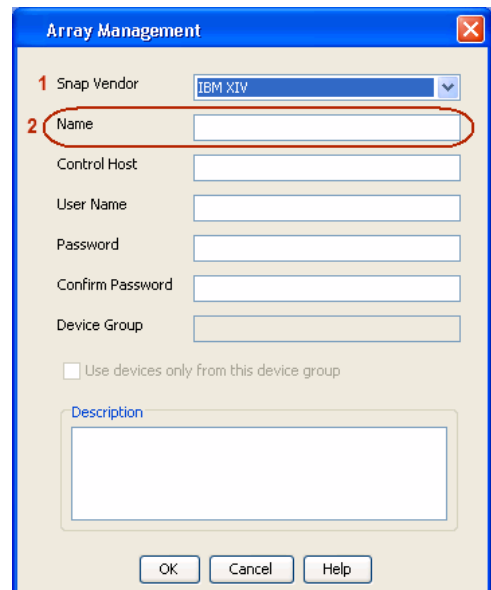
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

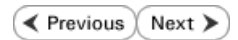
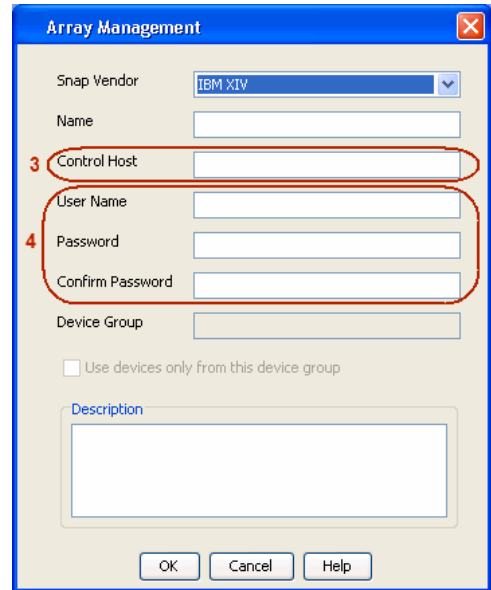
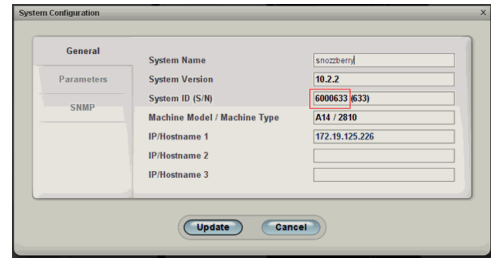


3.
  - Select **IBM XIV** from the **Snap Vendor** list.
  - Specify the 7-digit serial number for the array in the **Name** field.



The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

- 4.
- Enter the IP address or host name of the array in the **Control Host** field.
  - Enter the user access information of the application administrator in the **Username** and **Password** fields.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.



# SnapProtect™ Backup - LSI

◀ Previous    Next ▶

## PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
  - SMIS server through TCP/IP network.
  - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

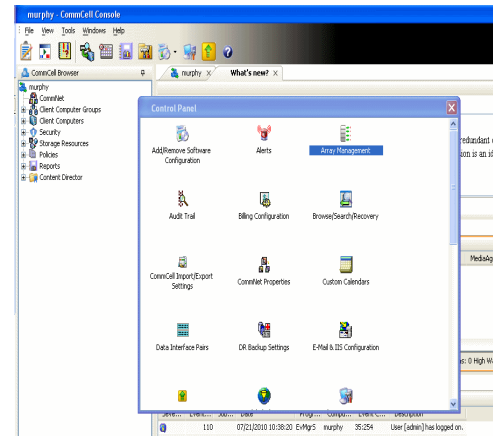
## ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

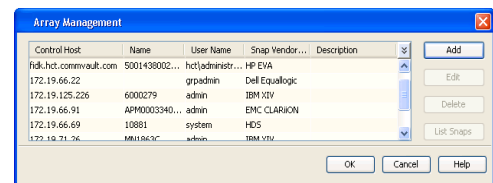
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

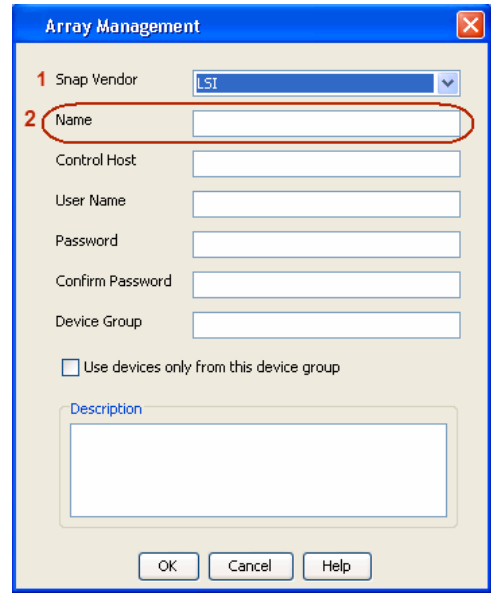
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

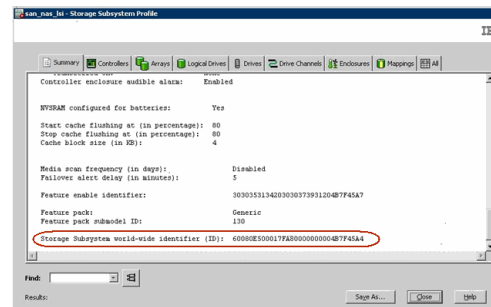


3.
  - Select **LSI** from the **Snap Vendor** list.
  - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

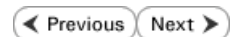
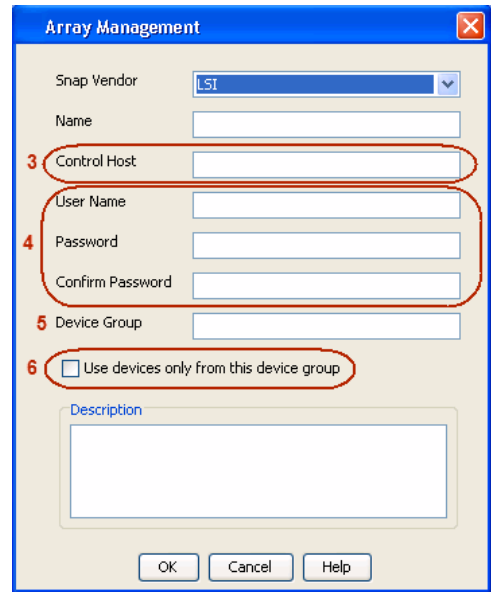
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



4.
  - Specify the name of the device manager server where the array was configured in the **Control Host** field.
  - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

If you specify None in the **Device Group** field but do have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.





name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: [ ]

Control Host: [ ]

User Name: [ ]

Password: [ ]

Confirm Password: [ ]

Device Group: [ ]

Use devices only from this device group

Description: [ ]

OK Cancel Help

◀ Previous Next ▶

# SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous   Next ▶

## OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

## PREREQUISITES

### LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

### ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

## SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:
 

```
options snapvault.enable on
```
3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:
 

```
options snapvault.access host=secondary_filer1, secondary_filer2
```
4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:
 

```
options snapvault.access host=primary_filer1, primary_filer2
```

## INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
  - Discover storage devices
  - Add Resource Pools to be used for the Vault/Mirror storage provisioning

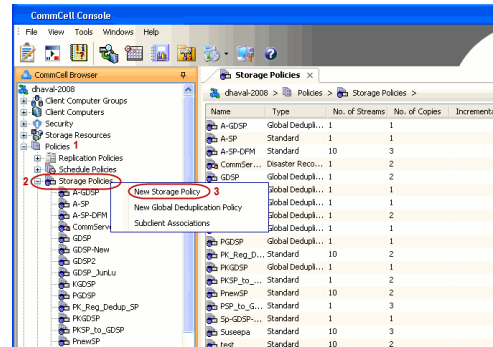
## CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

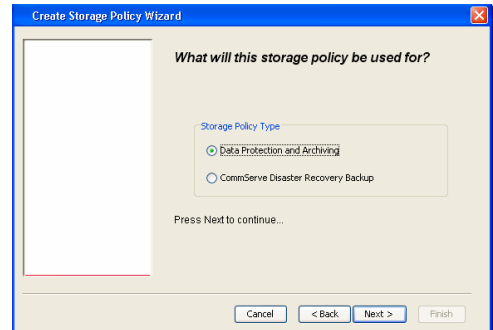
## CREATE STORAGE POLICY

Use the following steps to create a storage policy.

1.
  - From the CommCell Browser, navigate to **Policies**.
  - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



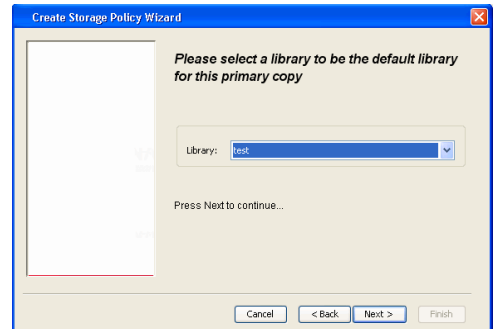
3.
  - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
  - Select **Provide the DataFabric Manager Server Information**.
  - Click **Next**.



4.
  - In the **Library** list, select the default library to which the Primary Copy should be associated.

It is recommended that the selected disk library uses a LUN from the File server.

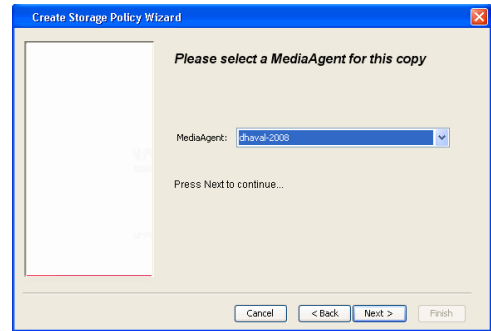
- Click **Next**.



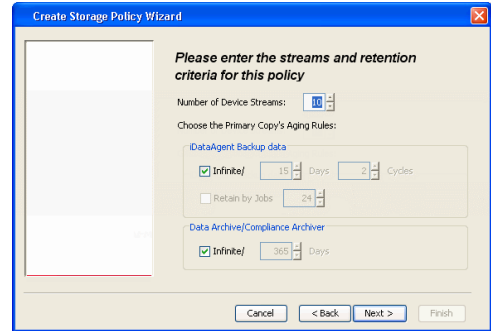
5.
  - Select a MediaAgent from the **MediaAgent** list.
  - Click **Next**.



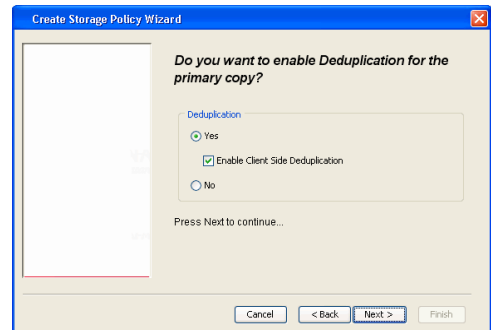
6. Click **Next**.



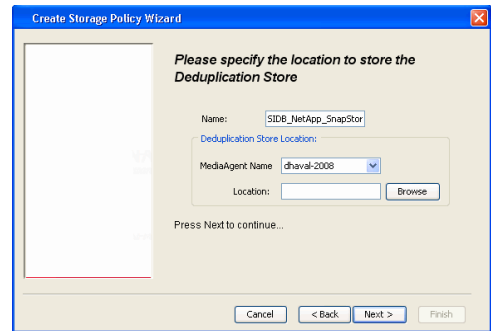
7. Click **Next**.



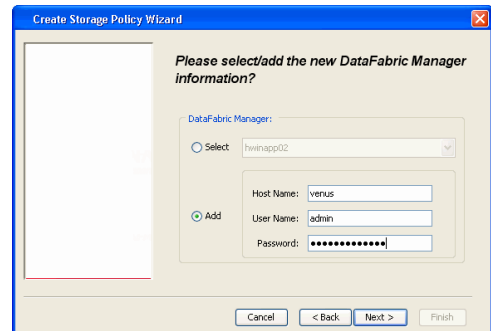
- 8.
- Verify **Name** and **MediaAgent Name**.
  - Click **Browse** to specify location for **Deduplication Store**.
  - Click **Next**.

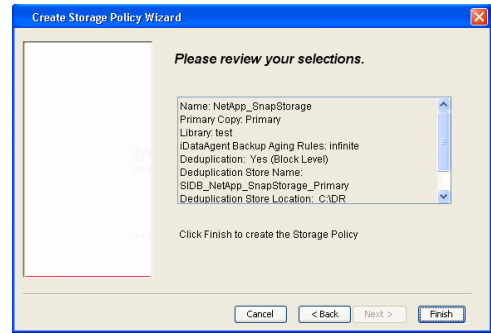


- 9.
- Provide the DataFabric Manager server information.
    - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
    - If you want to add a new DataFabric Manager Server, click **Add**.
  - Click **Next**.



10. Click **Finish**.



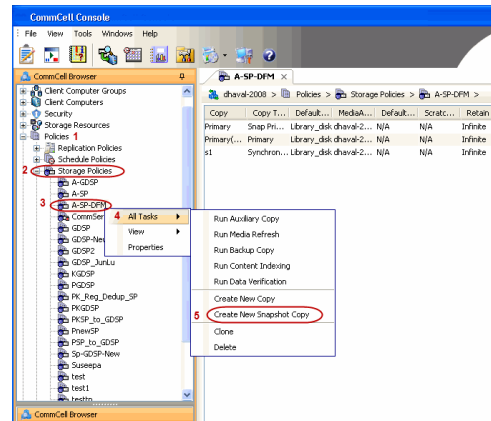


11. The new Storage Policy creates the following:
  - **Primary Snap Copy**, used for local snapshot storage
  - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

### CREATE A SECONDARY SNAPSHOT COPY

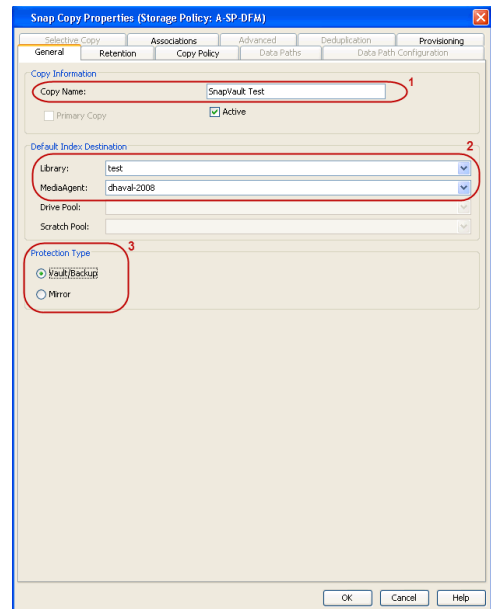
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
  - From the CommCell Browser, navigate to **Policies | Storage Policies**.
  - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
  - Enter the **Copy Name**.
  - Select the **Library** and **MediaAgent** from the drop-down list.
  - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

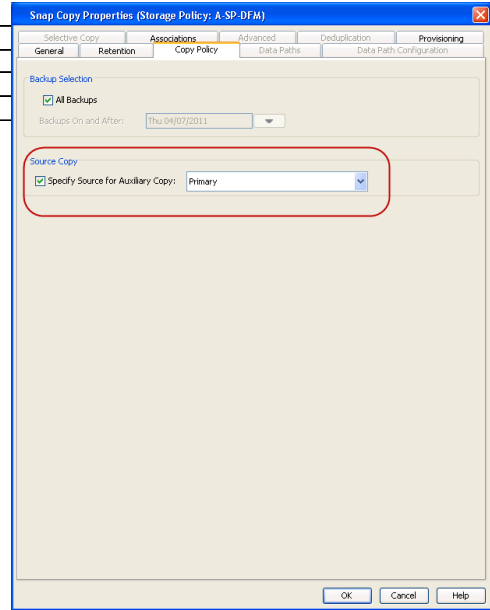


3.
  - Click the **Copy Policy** tab.
  - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

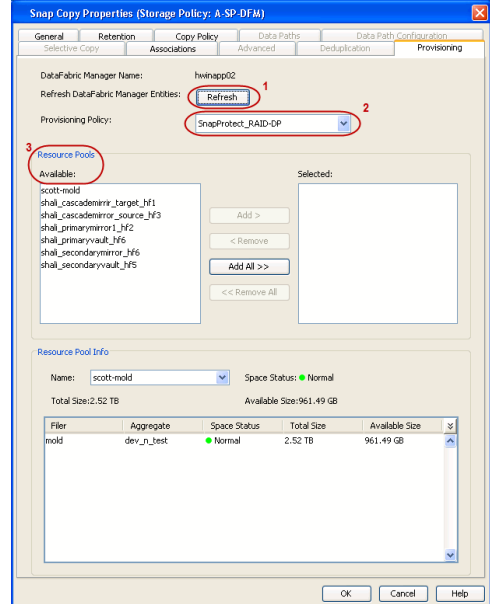
| TOPOLOGY | SOURCE COPY |
|----------|-------------|
|----------|-------------|

|                       |         |
|-----------------------|---------|
| Primary-Mirror        | Primary |
| Primary-Mirror-Vault  | Mirror  |
| Primary-Vault         | Primary |
| Primary-Vault-Mirror  | Vault   |
| Primary-Mirror-Mirror | Mirror  |



- Click the **Provisioning** tab.
  - Click **Refresh** to display the DFM entities.
  - Select the **Provisioning Policy** from the drop-down list.
  - Select the **Resource Pools** available from the list.
  - Click **OK**.

The secondary snapshot copy is created.



- If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:
 

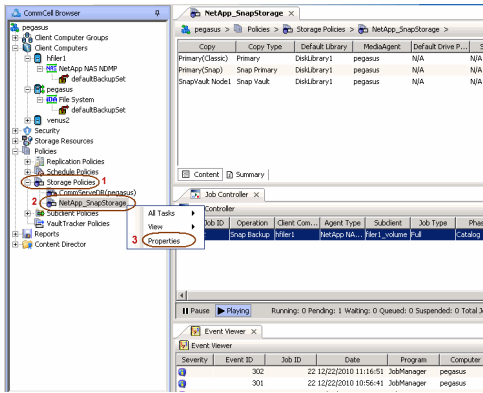
```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

It is recommended that you perform this operation on all nodes in the P-M-V topology.

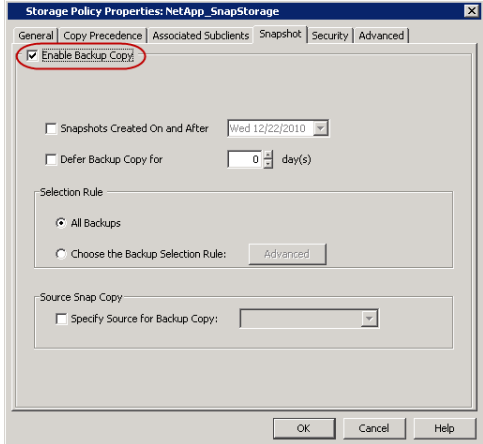
## CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

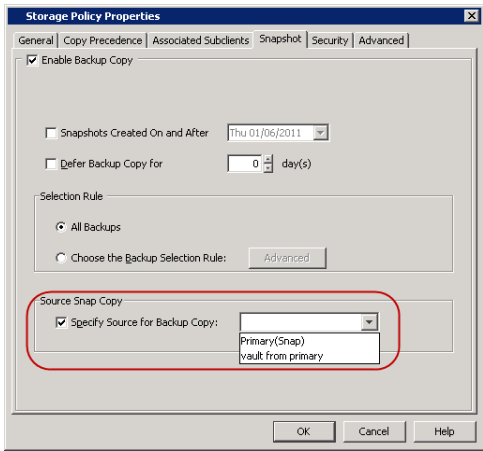
- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.



- Click the **Snapshot** tab.
  - Select **Enable Backup Copy** option to enable movement of snapshots to media.
  - Click **OK**.



- Select **Specify Source for Backup Copy**.
  - From the drop-down list, select the source copy to be used for performing the backup copy operation.

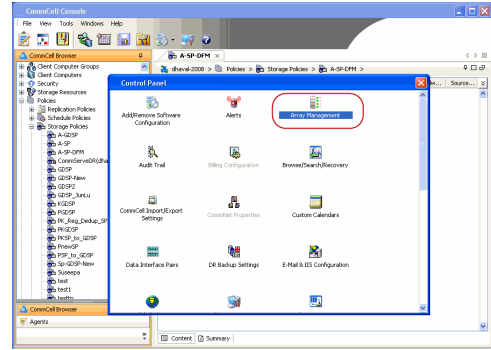


**SETUP THE ARRAY INFORMATION**

The following steps describe the instructions to set up the primary and secondary arrays.

- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

2. Click **Add**.

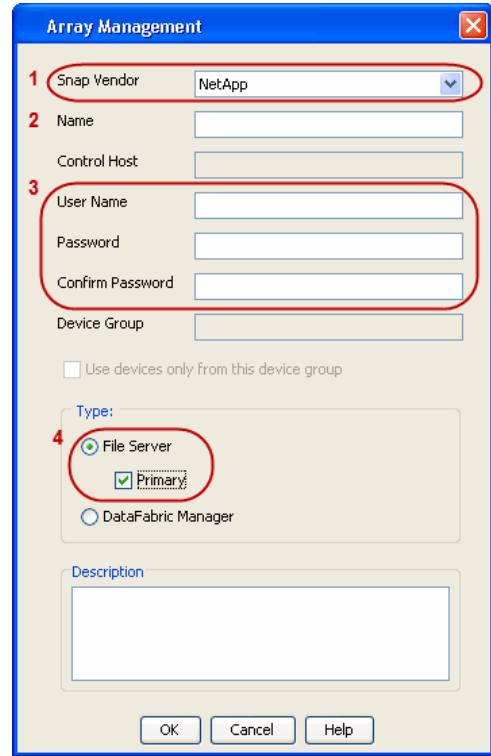
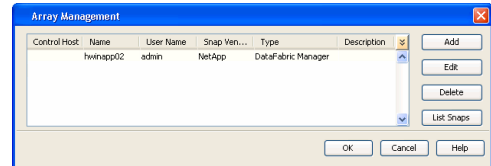


3.
  - Select **NetApp** from the **Snap Vendor** list.
  - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

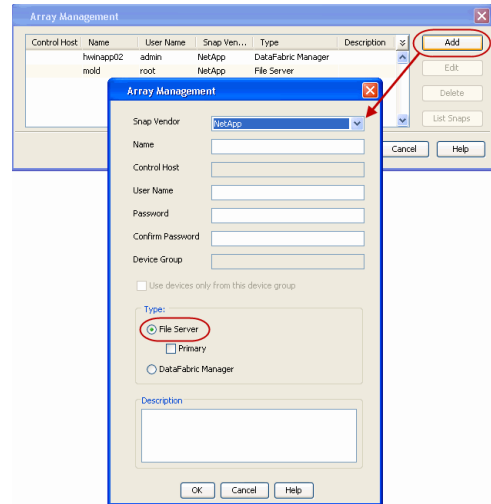
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



4.
  - Click **Add** again to enter the information for the secondary array.
  - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



## SEE ALSO

### Import Wizard Tool

Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

# SnapProtect™ Backup - Data Replicator

◀ Previous   Next ▶

## PRE-REQUISITES

### INSTALLATION

- The use of Data Replicator with the SnapProtect backup requires MediaAgent, File System iDataAgent, and ContinuousDataReplicator on the source, destination, and proxy computers.

The use of a proxy server to perform SnapProtect operations is supported when a hardware storage array is used for performing the SnapProtect backup.

- The operating system of the MediaAgent to be used for SnapProtect backup must be either the same or higher version than the source computer.

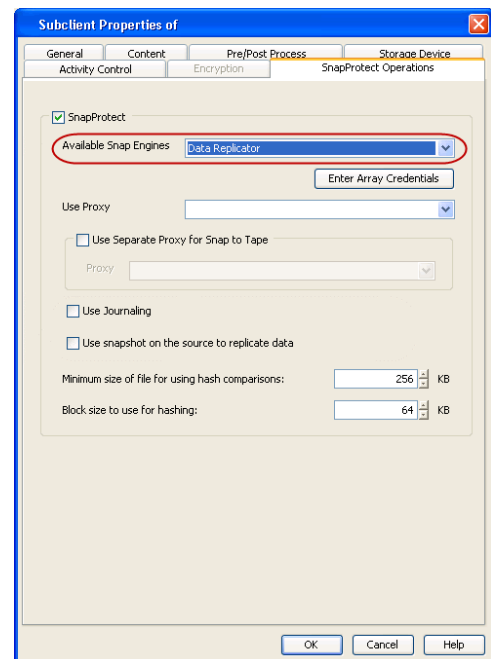
### STORAGE POLICY REQUIREMENTS

The Primary Snap Copy to be used for creating the snapshot copy must be a disk library.

If the Storage Policy or the disk library being used by the subclient is updated, the subclient should be recreated.

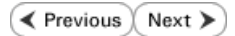
## SETUP THE ARRAY

- From the CommCell Console, navigate to <Client> | <Agent>.
  - Right-click the subclient and click **Properties**.
- Click the **SnapProtect Operations** tab.
  - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down list.
  - Click **OK**.



◀ Previous   Next ▶

# Getting Started - SAP for Oracle Backup

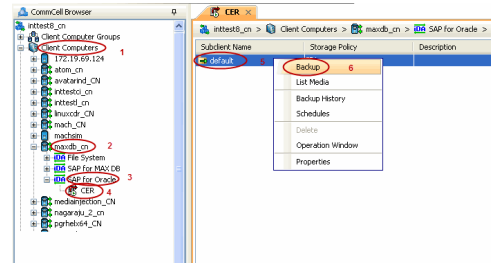


After configuring your instance, and subclient, you are ready to perform your first backup.

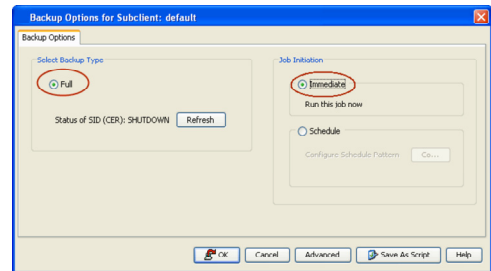
## PERFORM A BACKUP

The following section provides step-by-step instructions for running your first full backup:

- From the CommCell Console, navigate to **Client Computers** | **<Client>** | **SAP for Oracle** | **<Instance>**
  - Right-click the **Subclient** and click **Backup**.

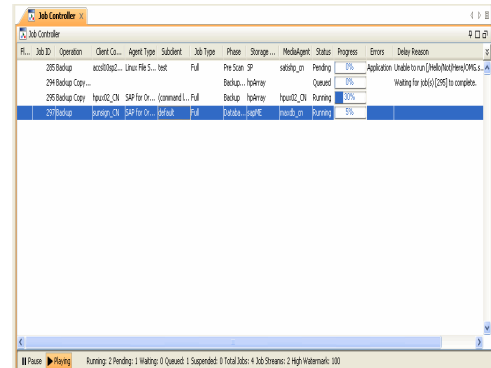


- Select **Full** as backup type and **Immediate** to run the job immediately.
  - Click **OK**.

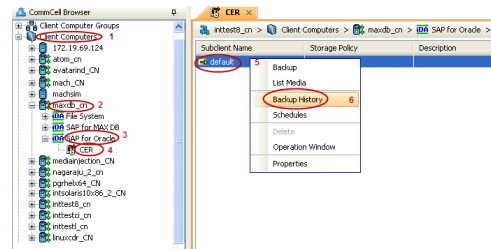


- You can track the progress of the job from the **Job Controller** window of the CommCell console.

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.



- Once job is complete, view the details of job from the **Backup History**. Right-click the **Subclient** and select **Backup History**.

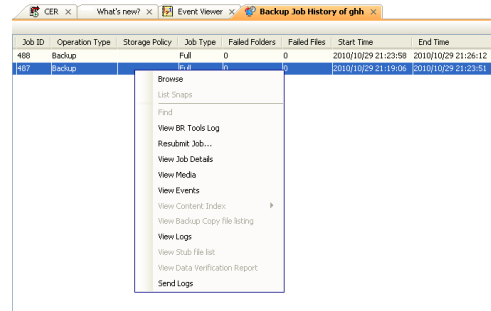
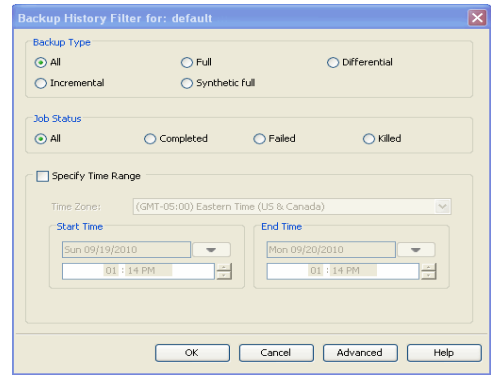


- Click **OK**.



6. You can view the following details about the job by right-clicking the job:

- Items that failed during the job
- Items that succeeded during the job
- Details of the job
- Events of the job
- Log files of the job
- Media associated with the job



# Getting Started - Vault/Mirror Copy



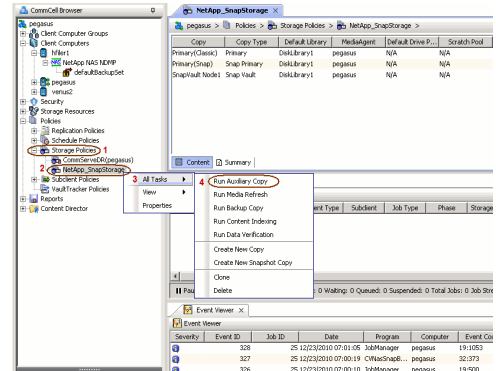
## SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** > to Continue.

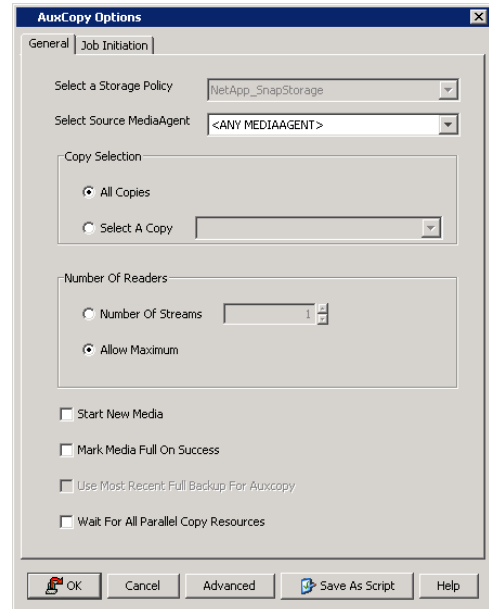
### INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

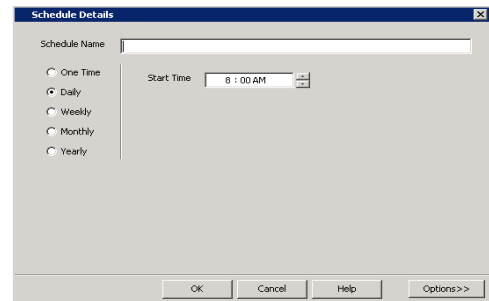


- Select the desired options and click the **Job Initiation** tab.
  - Select **Schedule** to configure the schedule pattern and click **Configure**.

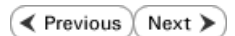


- Enter the schedule name and select the appropriate scheduling options.
  - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.



# Getting Started - Snap Movement to Media

◀ Previous   Next ▶

## SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

### BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

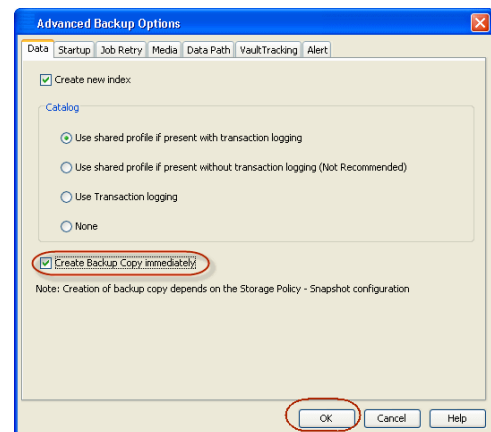
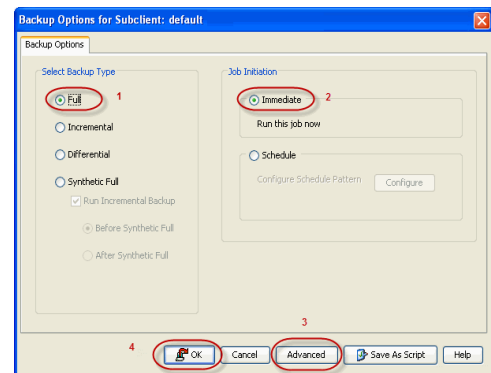
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

#### INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

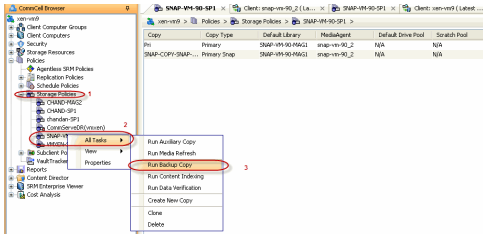
1.
  - From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
  - Right click the default subclient and click **Backup**.
  - Select **Full** as backup type.
  - Click **Advanced**.
  
2.
  - Select **Create Backup Copy immediately** to create a backup copy.
  - Click **OK**.



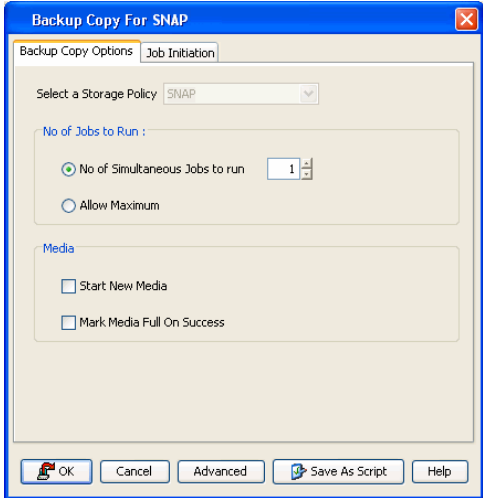
#### OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

1.
  - From the CommCell Console, navigate to **Policies** | **Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



# Getting Started - SAP for Oracle Restore

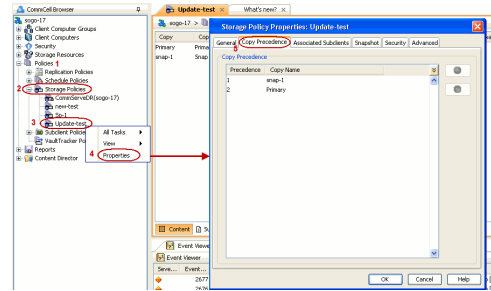


## PERFORM A RESTORE

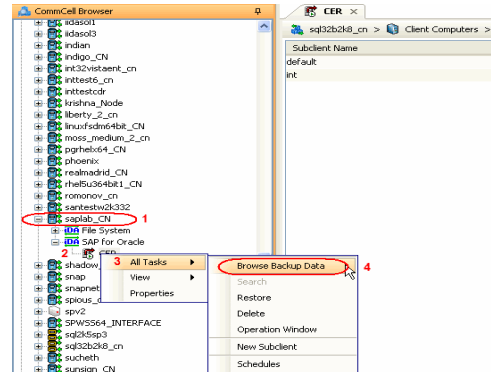
It is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following section comprehends the steps involved in restoring your entire database.

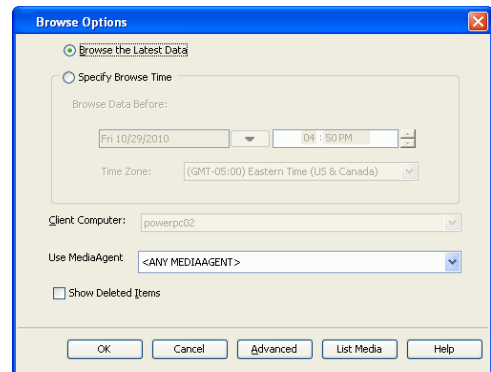
- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.
  - Click the **Copy Precedence** tab.
  - By default, the snapshot copy is set to 1 and is used for the operation.  
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
  - Click **OK**.



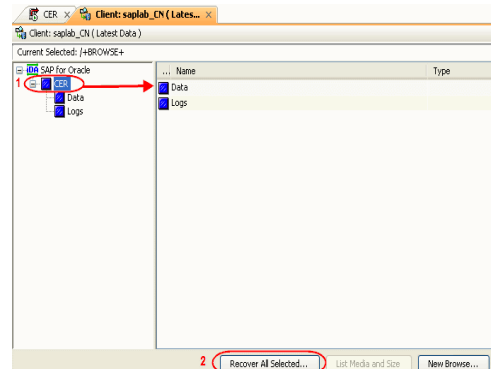
- From the CommCell Console, navigate to **<Client> | SAP for Oracle**.
  - Right-click the instance that contains the data you want to restore and click **All Tasks | Browse Backup Data**.



- Click **OK**.

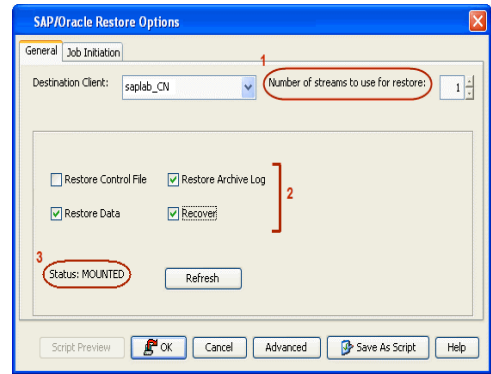


- Select the instance node in the left pane. The data and logs will be automatically selected in the right pane.
  - Click **Recover All Selected**.



- Choose the **Number of streams to use for restore**.

- Select the following options to restore the database.
  - **Restore Archive Log**
  - **Restore Data**
  - **Recover**
- Verify that the Status of the database is displayed as **MOUNTED**; if necessary click **Refresh** to get the latest status.
- Click **OK**.

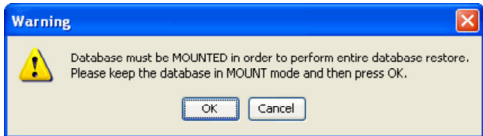


If the database is not mounted, a warning dialog appears to remind you to set the database in MOUNT mode.

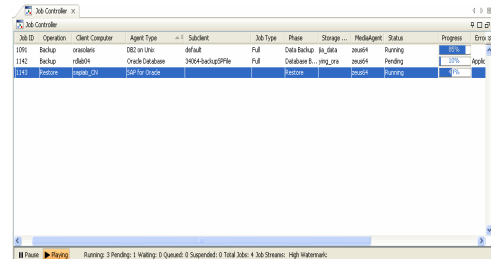
To mount the database, enter the following commands in the machine hosting the database:

```
[root]# export ORACLE_SID=<instance name>
[root]# sqlplus "/ as sysdba"
[root]# shutdown immediate;
[root]# startup mount;
```

Once the database is mounted, click **OK**.



6. You can monitor the progress of the restore job in the **Job Controller**.



7. The database is restored to the directory where it resides.

**CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.**

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.

# Getting Started - DB2 iDataAgent Deployment



Use the following steps to install the DB2 iDataAgent on a Unix computer.

## WHERE TO INSTALL

Install the software directly on the Unix computer that you wish to protect and has the application data.

## INSTALL THE DB2 iDATAAGENT

Use the following procedure to directly install the software from the installation package or a network drive.

1. Logon to the client computer as **root**.

2. 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:

```
./cvpkgadd
```

3. The product banner and other information is displayed.

Press **Enter**.

4. Read the license agreement. Type **y** and press **Enter**.

5. Press **Enter**.

6. Press **Enter**.

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 interface name that you wish to use as default, and then press **Enter**.

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

## RELATED TOPICS

### Download Software Packages

Download the latest software package to perform the install.

### SnapProtect Support - Platforms

Verify that the computer in which you wish to install the software satisfies the minimum requirements.

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
- 2) Advance options
- 3) Exit this menu

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.

You now have a choice of performing a regular Calypso install on the physical host or installing Calypso on a virtual machine for operation within a cluster.

Most users should select "Install on a physical machine" here.

- 1) Install on a physical machine
- 2) Install on a virtual machine
- 3) Exit

Your choice: [1]

We found one network interface available on your machine. We will associate it with the physical machine being installed, and it will also be used by the CommServe to connect 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 check the interface name below, and make connections if necessary:

8. Press **Enter**.
9. Type the number associated with the **DB2 iDataAgent, Media Agent, and Unix File System iDataAgent**.
10. A confirmation screen will mark your choice with an "**X**". Type **d** for **Done**, and press **Enter**.
11. Press **Enter**.
12. Type the appropriate number to install the latest software scripts and press **Enter**.
- Select **Download from the software provider website** to download the latest software scripts. Make sure you have internet access.
  - Select **Use the one in the installation media** to install the software scripts from the package or share from which the installation is currently being 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.
13. Press **Enter**.
14. Press **Enter** to accept the default path.
- If you want to specify a different path, type the path and then press **Enter**.
  - If you want to install the software binaries to an NFS shared drive, specify the directory on which you have mounted the NFS file system and then press **Enter**.
- In order to make sure that the client computer has *read/write* access to NFS shared drive, review the steps described in *Installing Software Binaries to an NFS Shared Drive*.
- Do not use the following characters when specifying the path:
- ```
!@#$$%^&*():/?\
```
15. Press **Enter** to accept the default location.
- Enter a path to modify the default location and press **Enter**.
 - All the modules installed on the computer will store the log files in this directory.

```
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]
```

```
Install Calypso on physical machine 172.19.99.62
```

```
Please select the Calypso module(s) that you would like to install.
```

```
[ ] 1) MediaAgent [1301] [CVGxMA]
```

```
[ ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]
```

```
[ ] 3) DB2 iDataAgent [1207] [CVGxDB2]
```

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

```
Enter number(s)/one of "a,n,r,q,d,>,<,>?" here:3
```

```
Install Calypso on physical machine 172.19.99.62
```

```
Please select the Calypso module(s) that you would like to install.
```

```
[X ] 1) MediaAgent [1301] [CVGxMA]
```

```
[X ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]
```

```
[X ] 3) DB2 iDataAgent [1207] [CVGxDB2]
```

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

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

```
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]
```

```
Please specify where you want us to install Calypso binaries.
```

```
It must be a local directory and there should be at least 176MB 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]
```

```
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]
```


16. Type **Yes** and press **Enter**.

Most of Software processes run with root privileges, but some are launched by databases and inherit database access rights. To make sure that registry and log files can be written to by both kinds of processes we can either make such files world-writeable or we can grant write access only to processes belonging to a particular group, e.g. a "calypso" or a "dba" group.

We highly recommend now that you create a new user group and enter its name in the next setup screen. If you choose not to assign a dedicated group to Software processes, you will need to specify the access permissions later.

If you're planning to backup Oracle DB you should use "dba" group.

Would you like to assign a specific group to Software?
[yes]

17. Type the **Group name** and then press **Enter**.

Please enter the name of the group which will be assigned to all Software files and on behalf of which all Software 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: mydb2

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".

18. This prompt is relevant only when you install on Solaris.

Number of Streams

Press **Enter** to accept the default value for **Number of Streams**.

You can type the **Number of Streams** that you plan to run at the same time and then press **Enter**.

IMPORTANT : Please read install document "Configure Kernel Parameters - Unix/Macintosh" from "Books Online" before you start configuring kernel parameters. Please enter the total number of streams that you plan to run at the same time. We need to make sure that you have enough semaphores and shared memory segments configured in /etc/system.

Number of streams [10]

We now need to modify the /etc/system configuration file on this computer. It is done to make sure that there will be enough shared memory and semaphores available for Calypso programs. Please review the changes below and answer "yes" if you want us to apply them to the /etc/system file. Otherwise, the installation will proceed, the changes will be saved to some other file, and you will have to apply them manually.

```
set shmsys:shminfo_shmmni=8570 (was 7930)
set shmsys:shminfo_shmseg=8420 (was 7780)
set semsys:seminfo_semms=10320 (was 9680)
set semsys:seminfo_semms=8570 (was 7930)
set semsys:seminfo_semmsl=8570 (was 7930)
```

Do you want us to apply these changes now? [no]

19. Press **Enter** if you do not want the changes to be updated automatically.

NOTES:

- If you want the changes to be made automatically, type **Yes** and then press **Enter**.
- You will come across this prompt when you install the software on the earlier versions of Solaris.

Changes saved into /etc/system.gal.1744

20. Press **Enter**.

You will see this prompt if you have accepted the default **no** and pressed **Enter** in the above step.

Press <ENTER> to continue.

21. Press **Enter**.

You will see this prompt if you have accepted the default **no** and pressed **Enter** in step 19.

Although a 'no' answer can be selected to this question during install, the user should make sure the min requirements (below) for shared memory are met, otherwise the backups may fail (the message in logs is 'could not start the pipeline').

```
set shmsys:shminfo_shmmax=4199304
set shmsys:shminfo_shmmni=1
set semsys:shminfo_shmmni=640
set semsys:shminfo_shmseg=640
set semsys:seminfo_semms=640
set semsys:seminfo_semms=640
set semsys:seminfo_semmsl=640
set maxusers=256
```

Press <ENTER> to continue.

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

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

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

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 : [8400]

Port Number for EvMgrC: [8402]

23. If you do not wish to configure the firewall services, press **Enter**.

Is there a firewall between this client and the CommServe?

- If this computer is separated from the CommServe by firewall(s), type **Yes** and then press **Enter**.
- For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.
24. Type the fully qualified CommServe host name and press **Enter**.
- Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.
25. Type the number associated with the Client Group and press **Enter**.
- NOTES**
- This screen will be displayed only if Client Groups are configured for the CommCell.
26. A confirmation screen will mark your choice with an "X". Type **d** for done with the selection, and press **Enter** to continue.
27. Enter the number associated with the storage policy you want use and press **Enter**.
28. Type the path for storing the DB2 archive files and then press Enter
- NOTE**
- If the path that you enter does not exist, you will be asked if you want to create this path. In such a case, accept the yes default and then press Enter.
29. Type the path to the DB2 Audit Error Directory and then press **Enter**.
- NOTE**
- If the path that you enter does not exist, you will be asked if you want to create this path. In such a case, accept the **yes** default and then press **Enter**.
30. Type the path for storing the DB2 Retrieve files and then press **Enter**.
- NOTES**
- If the path that you enter does not exist, you will be asked if you want to create this path. In such a case, accept the **yes** and then press **Enter**.
31. If you want to integrate the software with DB2 now, accept yes and press **Enter**. If you want to do this later, type **No** and press **Enter**.
32. Specify the DB2 Instance User name that was selected when the DB2 instance was installed. This is the first bit of information required to integrate the product with the appropriate DB2 server.
- Type this name or accept the default and then press **Enter**.
33. Press **Enter**.
34. Press **Enter**.
35. Type **3** to the **Exit** option and press **Enter**.

[no]

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

CommServe Host Name: mycommserve.company.com

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.

[] 1) Unix

[] 2) DR

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

Enter number(s)/one of "a,n,r,q,d,>,<," here: 1

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.

[X] 1) Unix

[] 2) DR

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

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

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

1) SP_StandAloneLibrary2_2

2) SP_Library3_3

3) SP_MagLibrary4_4

Storage Policy: [1]

Please enter path to the DB2 Archive Directory.

DB2 Archive Directory: /BU_area/db2/log

Please enter path to the DB2 Audit Error Directory.

DB2 Logs Directory: /BU_area/db2/log1

Please enter path to the DB2 Retrieve Directory.

DB2 Retrieve Directory: /BU_area/db2/ret

In order to complete integration of Calypso with DB2, we need to create links to some Calypso binaries in each of the DB2 instance directories. We can either do it now, or if you prefer, you can run /space/opt/calypso /iDataAgent/Db2_install.sh script later yourself.

Would you like us to integrate Calypso with DB2 now? [yes]

To integrate Calypso with a DB2 server we need to create a set of links under lib subdirectory of the DB2 installation directory.

Please specify the DB2 Instance User Name that was selected when DB2 Instance was installed.

DB2 Instance User Name: [db2inst1]

Calypso links will be created in /BU_area/db2as/sql/lib.

Press <ENTER> to continue ...

Would you like to configure another DB2 instance?

Configure? [no]

Certain Calypso packages can be associated with a virtual IP, or in other words, installed on a "virtual machine"

The installation is now complete.

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] 3



Getting Started - DB2 Configuration



CONFIGURATION

Once the DB2 *iDataAgent* is installed, configure an Instance and a Backup Set to facilitate backups. Each Backup Set references a DB2 database. Also it is recommended to create separate subclients for data backups and archive log backups.

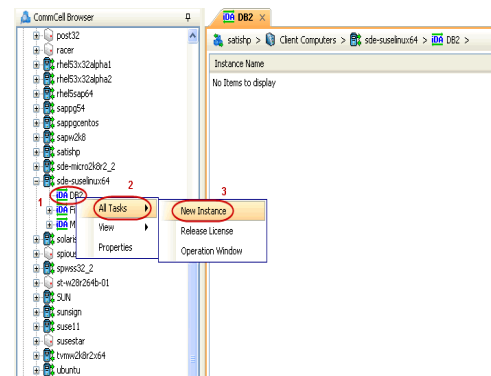
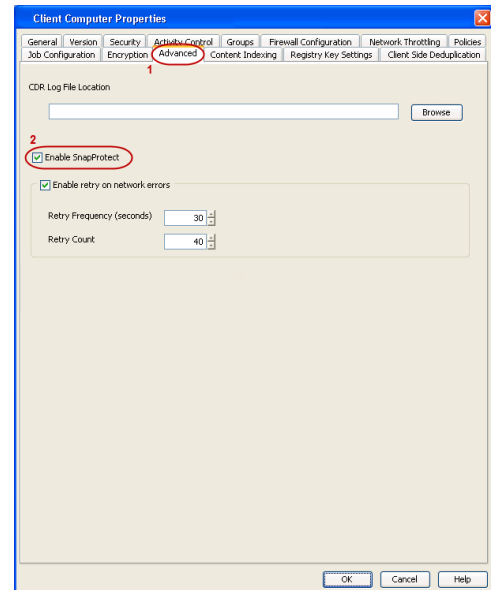
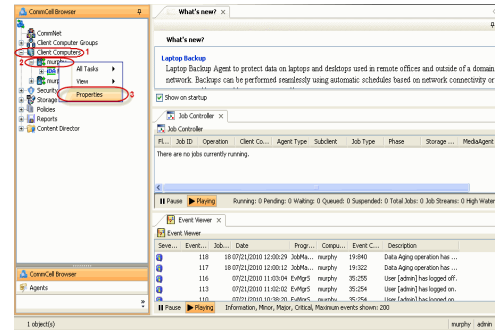
The following sections provide the necessary steps required to create and configure these components for a first SnapProtect backup of the DB2 database.

1.
 - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.

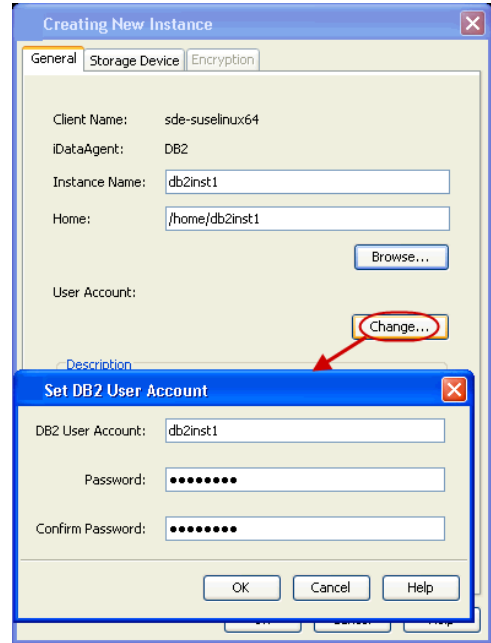
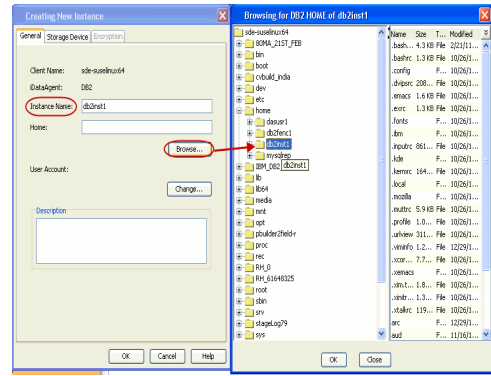
2.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.

3.
 - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click **DB2** and click **All Tasks** | **New Instance**.

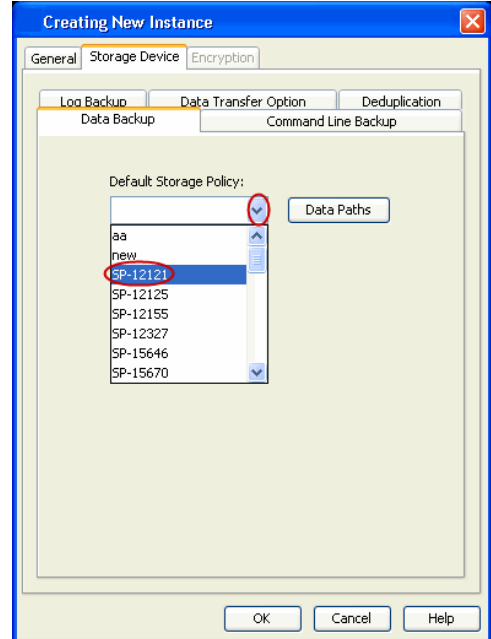
4.
 - In the **Instance Name** field, type a name.
 - In the **Home** field, click **Browse** and select the path to the DB2 application files.



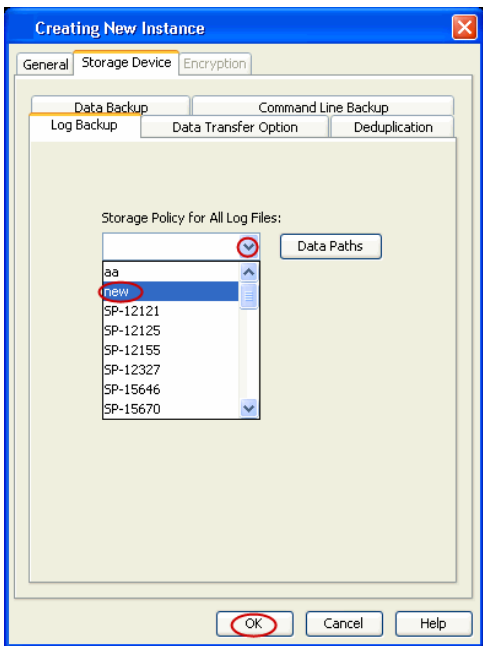
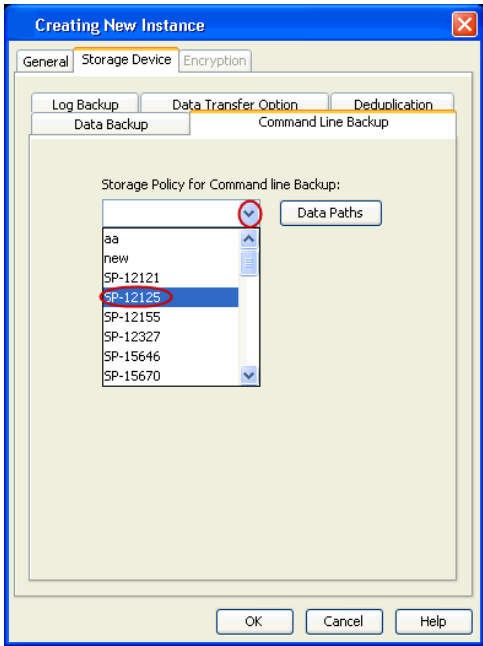
5.
 - Click **Change**.
 - In the **User Account** field, type the user name to access the DB2 application.
 - In the **Password** field, type the password for the user.
 - In the **Confirm Password** field, re-type the password for the user.
 - Click **OK**.



6.
 - Click the **Storage Device** tab.
 - In the **Default Storage Policy** box, select a storage policy name for data backups.

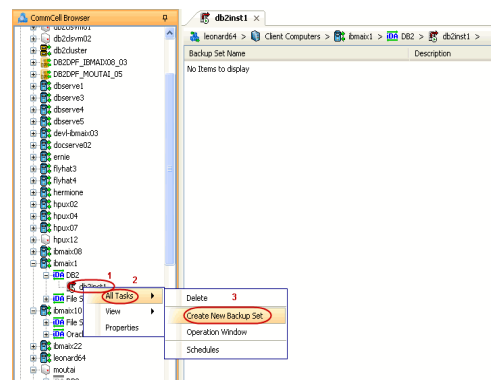


7.
 - Click the **Command Line Backup** tab.
 - In the **Storage Policy for Command Line Backup** box, select a storage policy name.



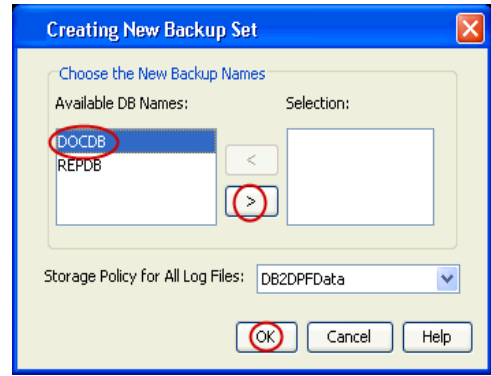
8.
 - Click the **Logs Backup** tab.
 - In the **Storage Policy for All Log Files** box, select a storage policy name for log backups.
 - Click **OK**.

9.
 - From the CommCell Browser, navigate to **Client Computers | <Client> | DB2**.
 - Right-click the **<Instance>** and click **All Tasks | Create New Backup Set**.

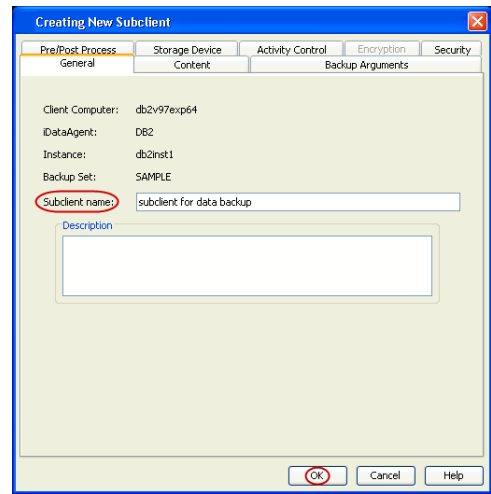
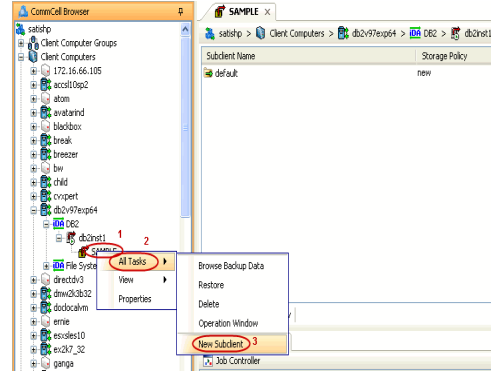


10.
 - Under **Available DB Names**, click the database name, and then click the arrow button to move the database name to the **Selection** box.
 - Click **OK**.

11.
 - From the CommCell Browser, navigate to the **<Instance>**.
 - Right-click the **<Backup Set>** and click **All Tasks | New Subclient**.

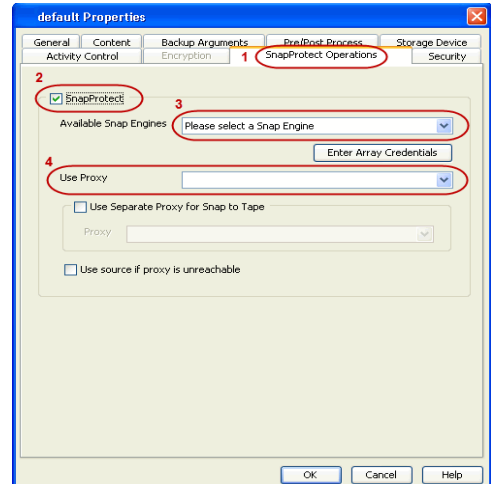


12. In the **Subclient Name** field, type a name.



13.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where backup copy operation will be performed.

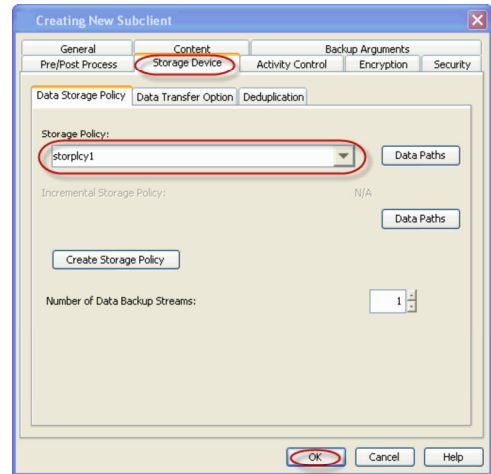
When performing IntelliSnap backup copy using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.



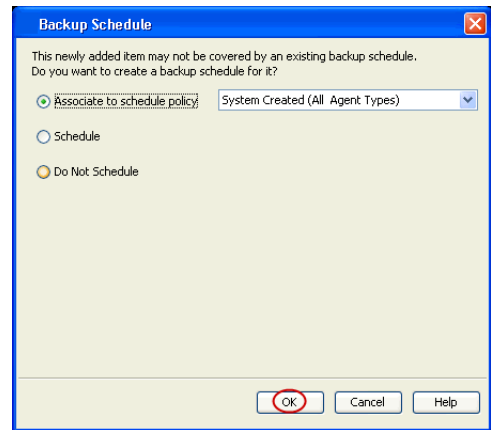
14.
 - Click the **Storage Device** tab.
 - In the **Data Storage Policy** list, select the same storage policy used for data backups in **Step 6**.

The subclient should use the same storage policy set for data backups at the instance level in order to prevent job failure.

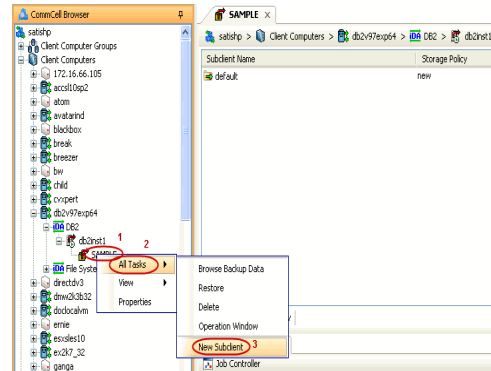
- Click **OK**.



15. Click **OK**.

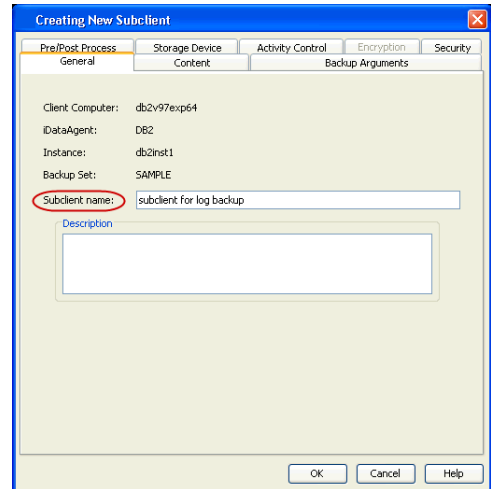


16.
 - From the CommCell Browser, navigate to the **<Instance>**.
 - Right-click the **<Backup Set>** and click **All Tasks | New Subclient**.

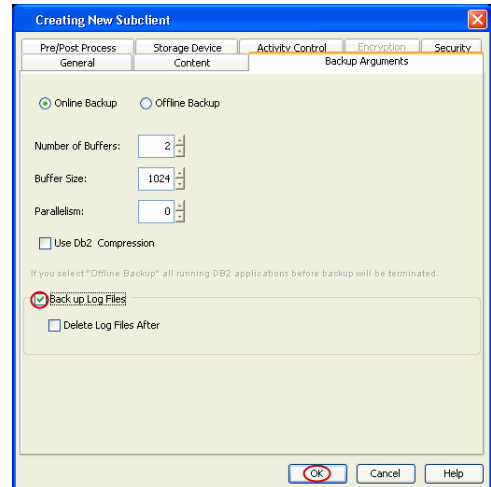
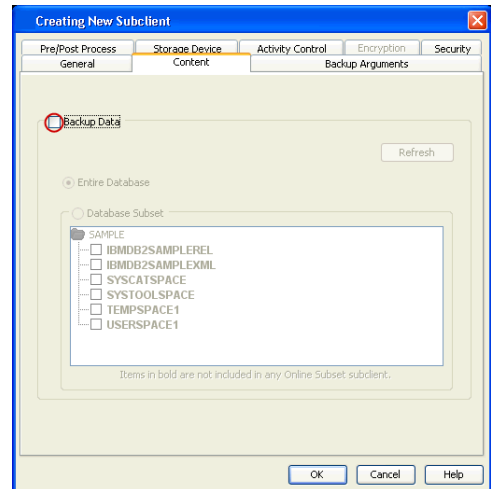


17. In the **Subclient Name** field, type a name.

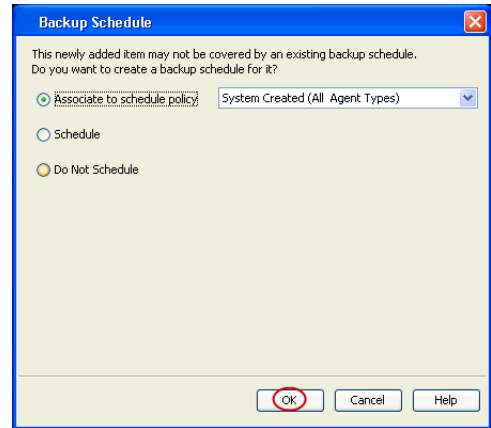
- 18.
- Click the **Content** tab.
 - Clear the **Backup Data** checkbox.



- 19.
- Click the **Backup Arguments** tab.
 - Click the **Back up Log Files** checkbox.
 - Click **OK**.



20. Click **OK**.



SKIP THIS SECTION IF NOT USING SOLARIS.

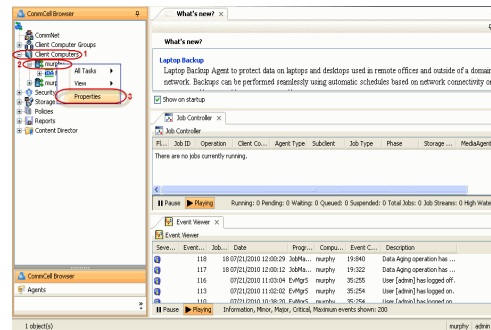
Click **Next** ► to Continue.

ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE

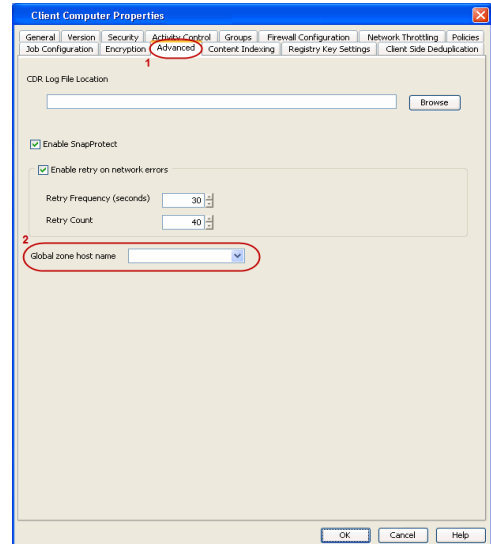


Follow the steps given below to enable SnapProtect backups on each of the non-global zone clients containing the application data.

- From the CommCell Console, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.



- Click **Advanced** tab.
 - Select the **Global Zone host name** from the drop-down list.
 - Click **OK**.
 - We support disks on a global zone mounted using loopback File System on a non global zone.
 - This option need not be enabled if you are using a NFS share. This is because when using NFS mount paths, the operations are limited to the non-global zone and does not use the global zone.



- Repeat the above steps on all the non-global zone clients containing the application data.

SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

Click **Next** ► to Continue.

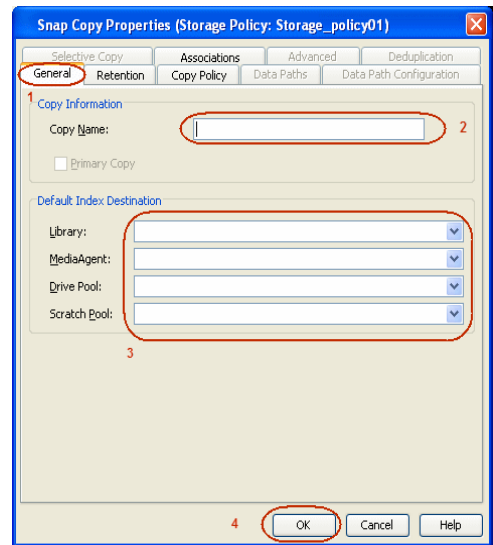
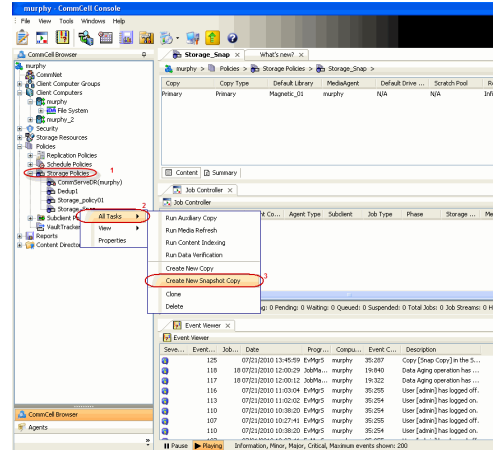
CREATE A SNAPSHOT COPY



Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

1.
 - From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.

2.
 - Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.

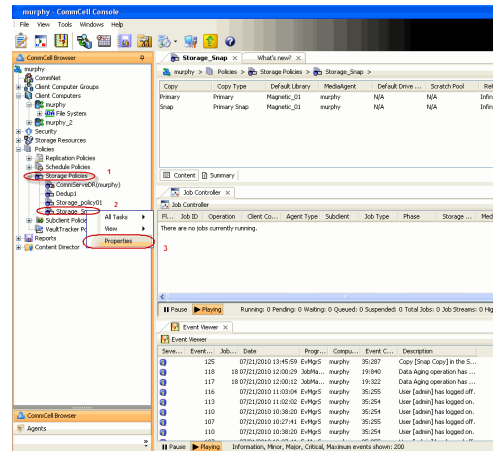


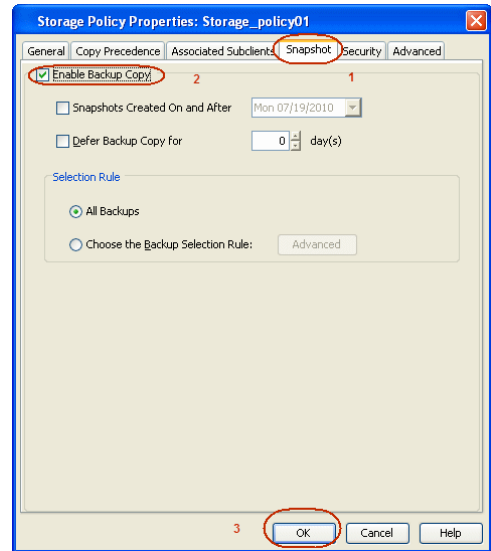
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.

2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.





Storage Array Configuration

[< Previous](#) [Next >](#)

CHOOSE THE STORAGE ARRAY

HARDWARE STORAGE ARRAYS
3PAR
DELL COMPELLENT
DELL EQUALLOGIC
EMC CLARIION, VNX
EMC SYMMETRIX
FUJITSU ETERNUS DX
HITACHI DATA SYSTEMS
HP EVA
IBM SVC
IBM XIV
LSI
NETAPP
NETAPP WITH SNAPVAULT/SNAPMIRROR

[< Previous](#) [Next >](#)

SnapProtect™ Backup - 3PAR

◀ Previous Next ▶

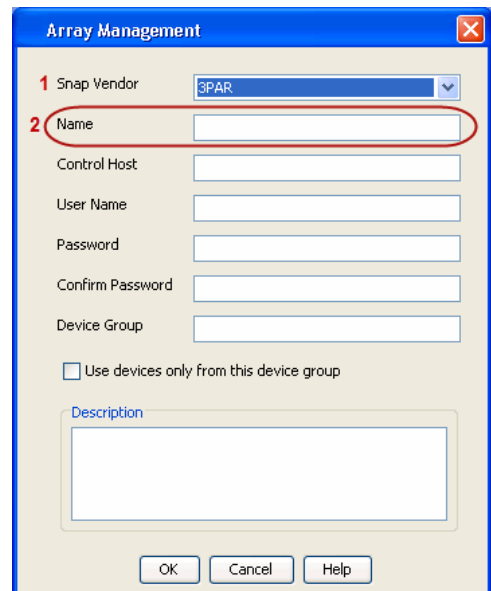
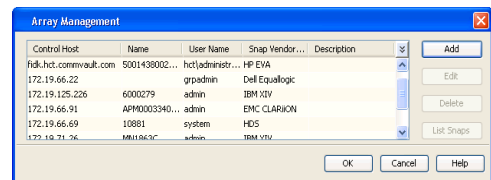
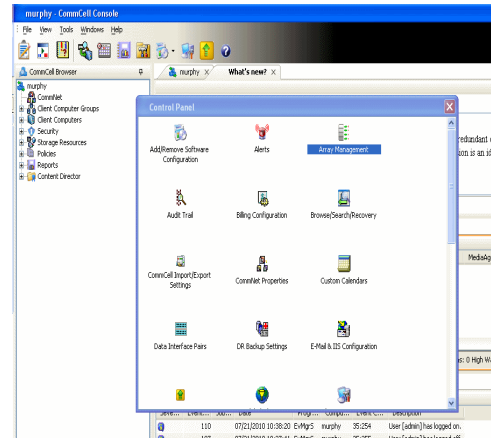
PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
 - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

where $\text{DevID.substr}(12,4)$ is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(12,4)$ is 0B95

After adding all the values, the resulting array name is 2FF70002AC000B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where $\text{DevID.substr}(4,3)$ is the next 3 digits after the fourth digit from the WWN number

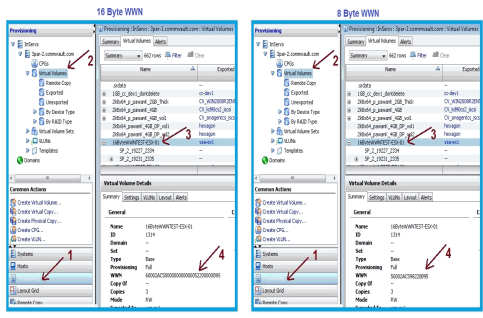
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(26,6)$ is 000B95

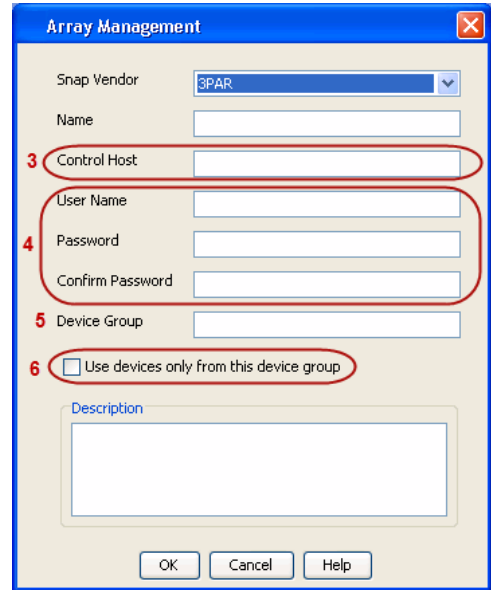
After adding all the values, the resulting array name is 2FF70002AC000B95.



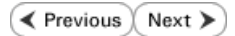
- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - Dell EqualLogic



PRE-REQUISITIES

WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

FIRMWARE VERSION

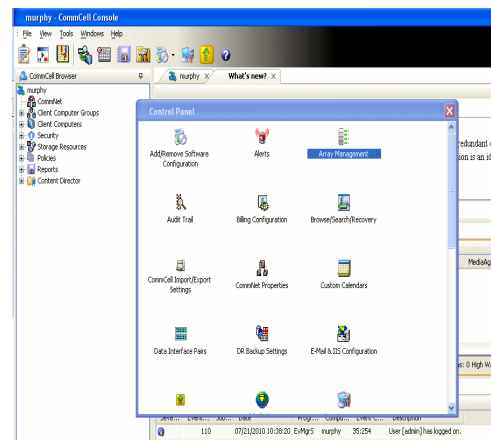
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

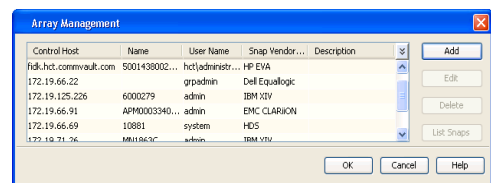
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

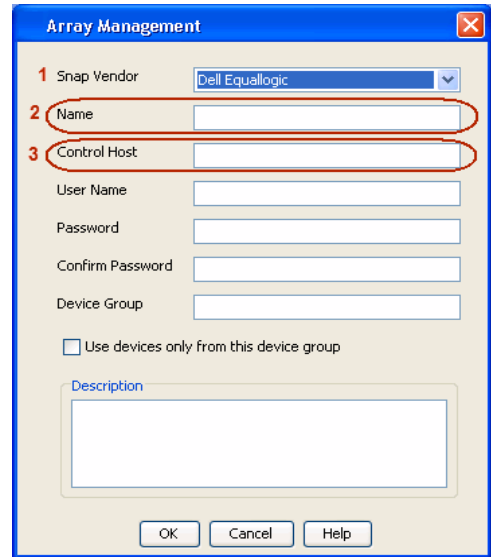


2. Click **Add**.

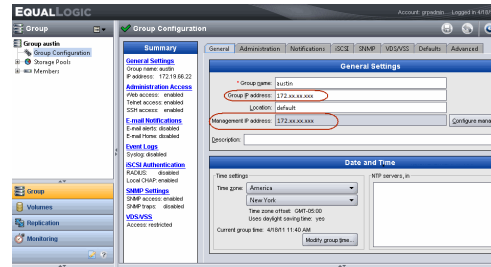


3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

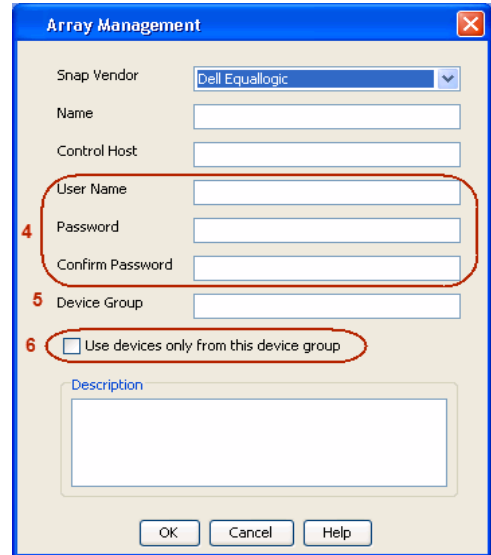
No entry is required in the **Name** field if there is no Management IP address configured.
 - Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
 - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
 - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
 - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous Next ▶

PRE-REQUISITES

LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

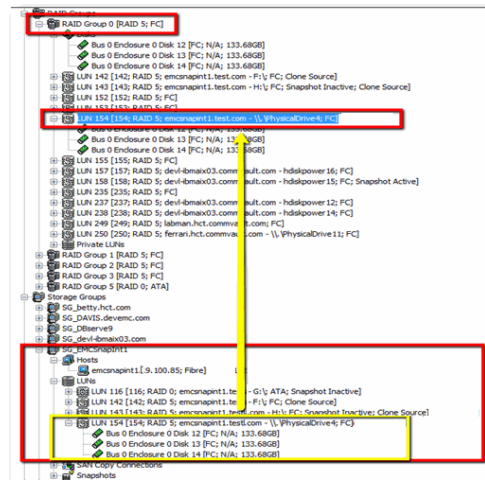
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

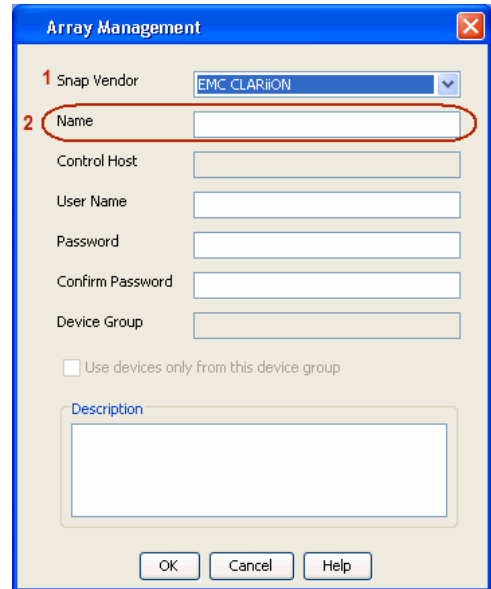
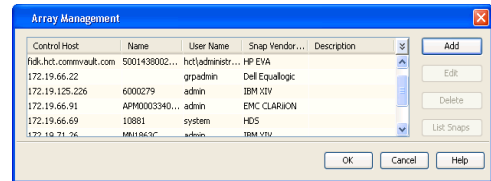
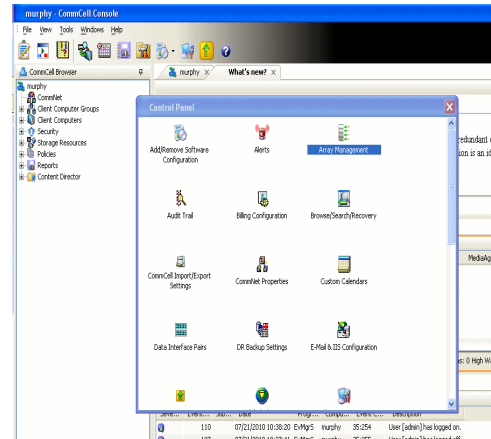
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

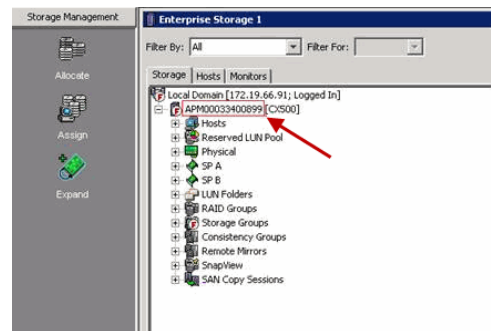
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
 - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.



- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

Array Management ✕

Snap Vendor:

Name:

Control Host:

User Name:

3 Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

SnapProtect™ Backup - EMC Symmetrix

◀ Previous Next ▶

PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

LOAD THE SYMMETRIX DATABASE

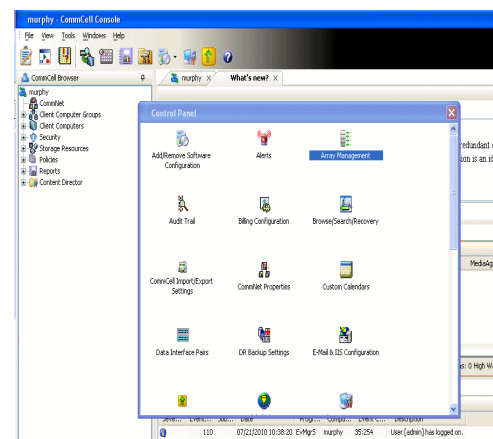
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

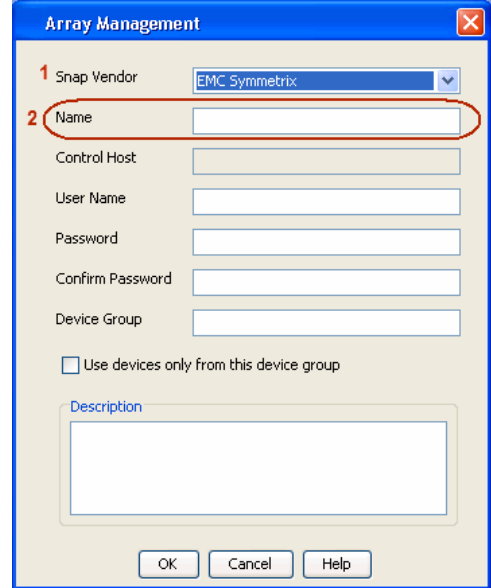
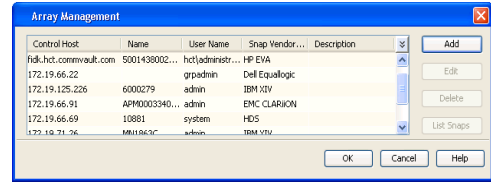
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

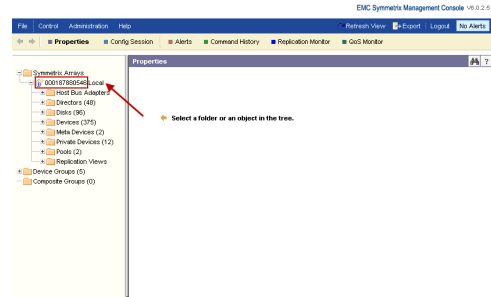


- Click **Add**.

3.
 - Select **EMC Symmetrix** from the **Snap Vendor** list.
 - Specify the **Symm ID** of the array in the **Name** field.

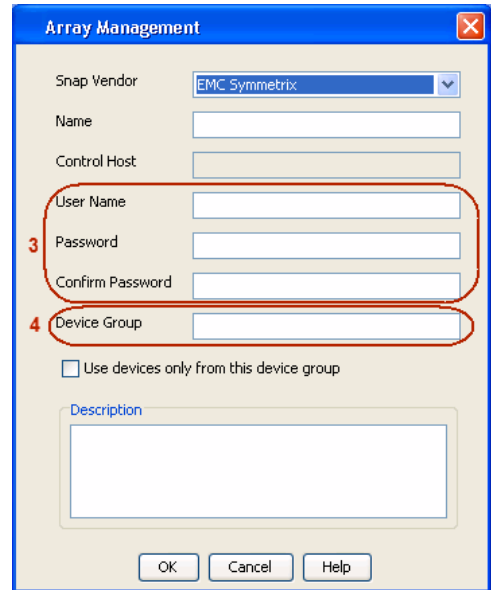


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.
If you do not specify a device group, the default device group will be used for snapshot operations.
 - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).



SnapProtect™ Backup - Hitachi Data Systems

◀ Previous Next ▶

PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
 - COW pools
 - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

ADDITIONAL REQUIREMENTS FOR VMWARE

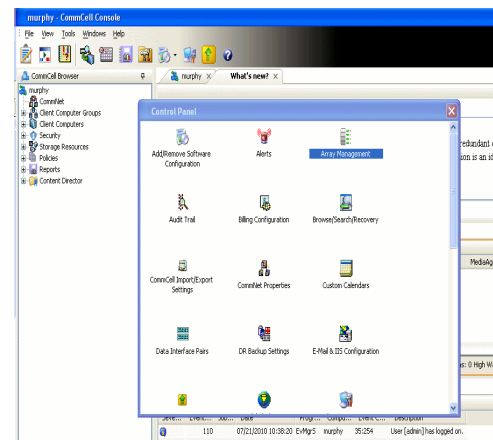
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server *iDataAgent* client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server *iDataAgent* client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

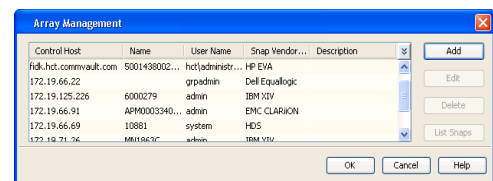
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

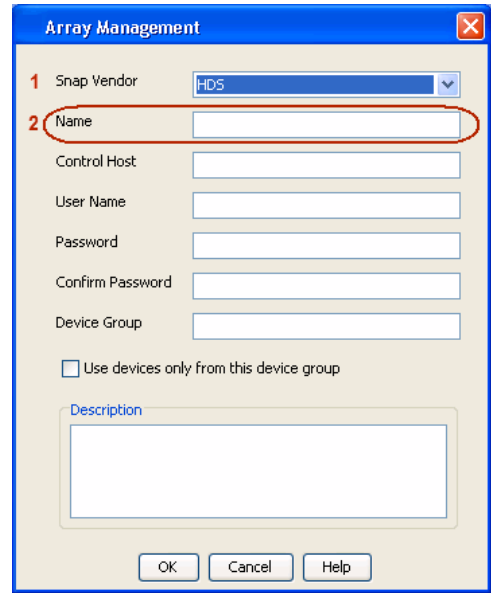
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



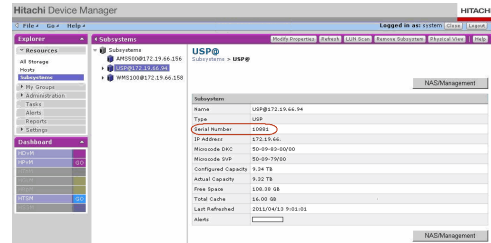
2. Click **Add**.



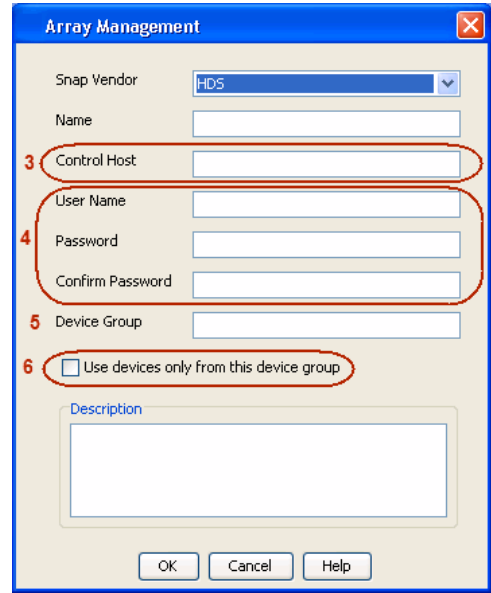
3.
 - Select **HDS** from the **Snap Vendor** list.
 - Specify the serial number of the array in the **Name** field.



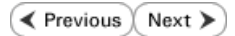
For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



4.
 - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:
`<COW_POOL_ID>-<LABEL>` or `<LABEL>-<COW_POOL_ID>`
 where `<COW_POOL_ID>` (for COW job) should be a number. This parameter is required.
`<LABEL>` (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.
 - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



SnapProtect™ Backup - HP StorageWorks EVA



SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

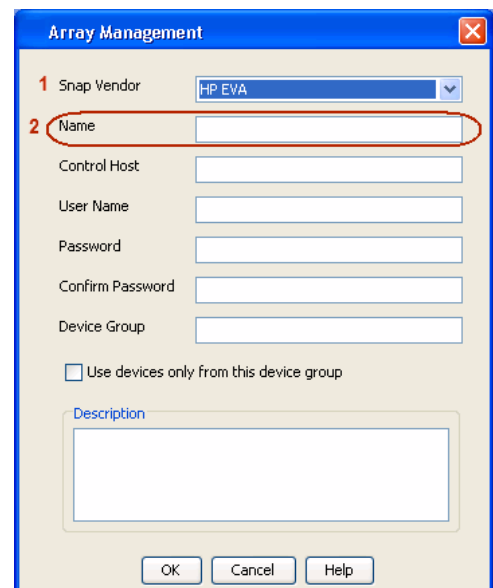
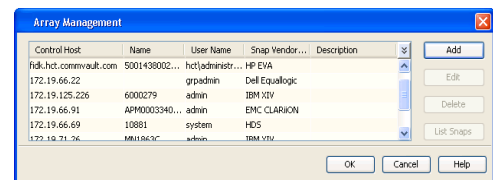
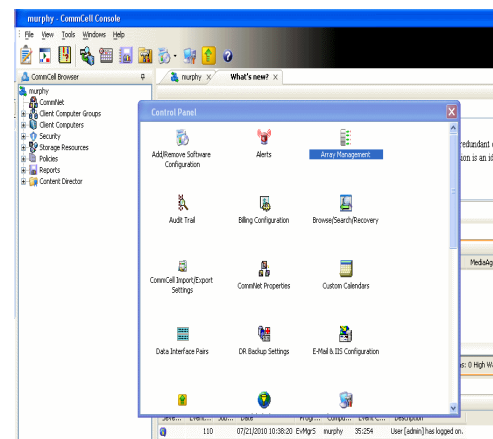
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin folder to discover the HP-EVA arrays.
3. Use the CLIRefreshTool.bat tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin folder.

SETUP THE ARRAY INFORMATION

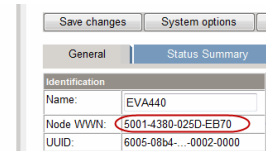
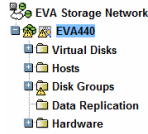
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
2. Click **Add**.
3.
 - Select **HP EVA** from the **Snap Vendor** list.
 - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



4.
 - Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous Next ▶

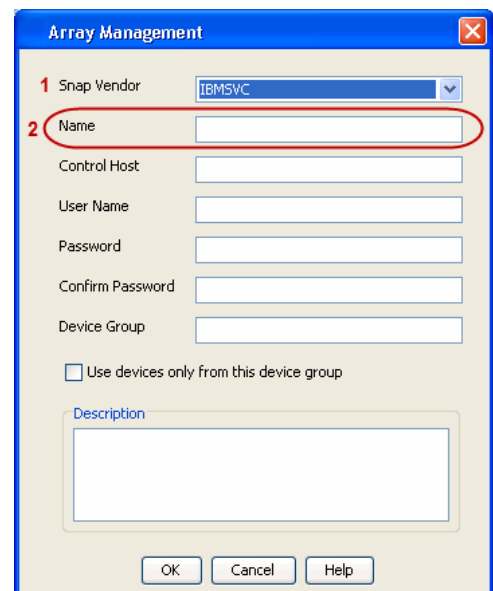
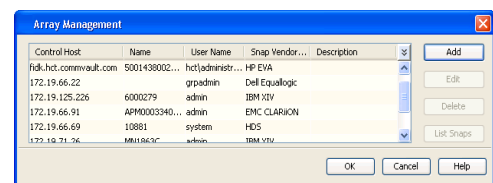
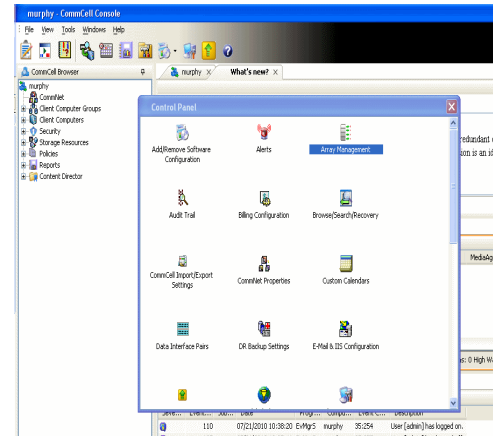
PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

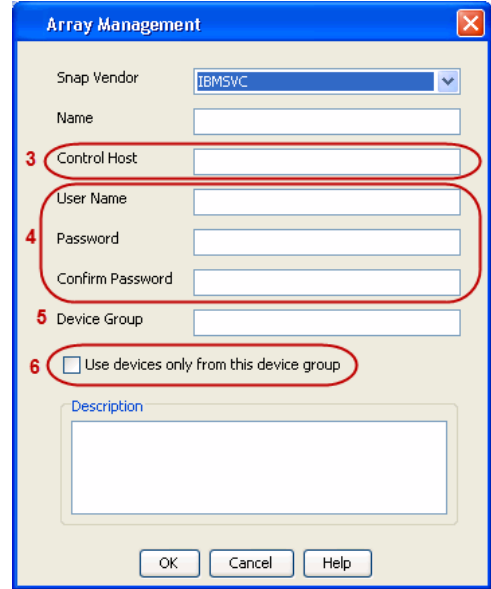
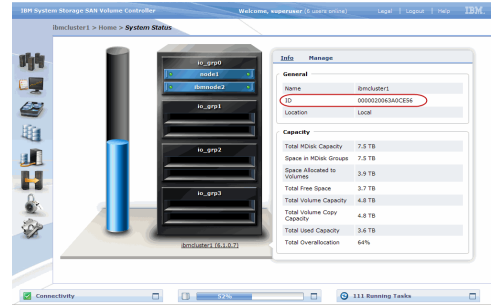
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - IBM XIV



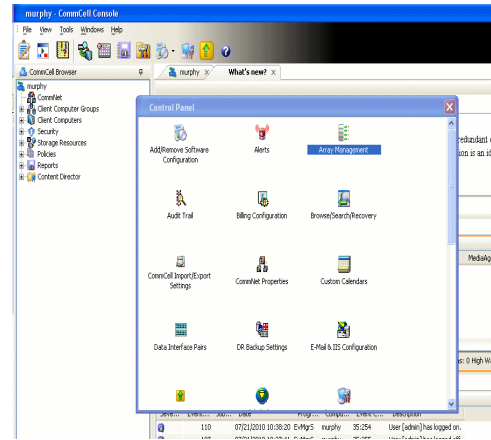
PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

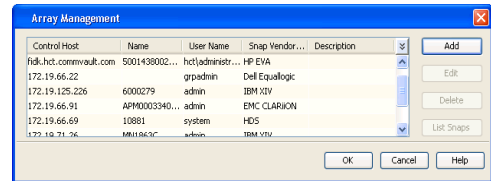
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

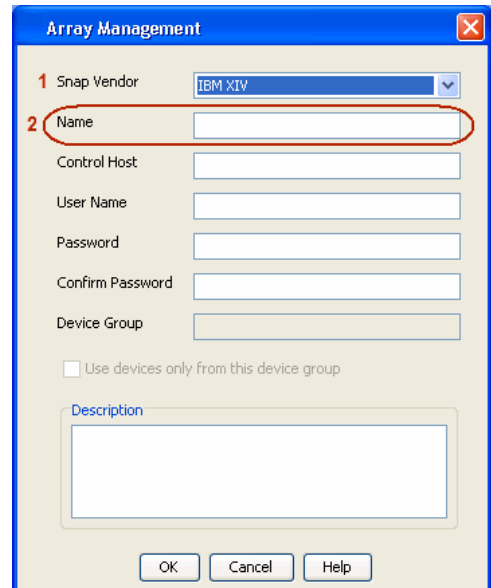
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

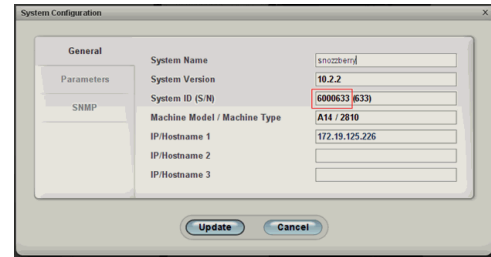


3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.

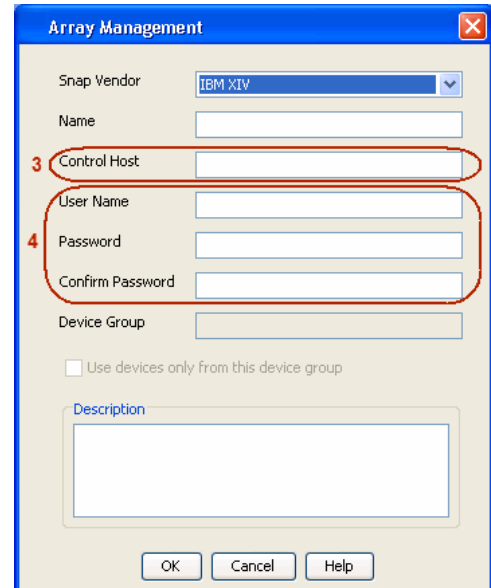


The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

- 4.
- Enter the IP address or host name of the array in the **Control Host** field.
 - Enter the user access information of the application administrator in the **Username** and **Password** fields.
 - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
 - Click **OK** to save the information.



The System Configuration dialog box shows the General tab. The System Name is 'snap24m1', System Version is '10.2.2', System ID (S/N) is '6000633 633', and Machine Model / Machine Type is 'A14 / 2810'. IP/Hostname 1 is '172.19.125.226'. There are Update and Cancel buttons at the bottom.



The Array Management dialog box has a Snap Vendor dropdown set to 'IBM XIV'. The Name field is empty. The Control Host field is circled in red and labeled with a red '3'. The User Name, Password, and Confirm Password fields are grouped together in a red oval and labeled with a red '4'. The Device Group field is empty. There is a checkbox for 'Use devices only from this device group' which is unchecked. A Description text area is empty. There are OK, Cancel, and Help buttons at the bottom.

< Previous Next >

SnapProtect™ Backup - LSI

◀ Previous Next ▶

PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
 - SMIS server through TCP/IP network.
 - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

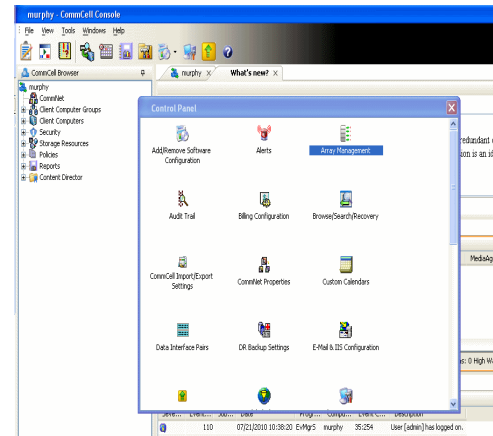
ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

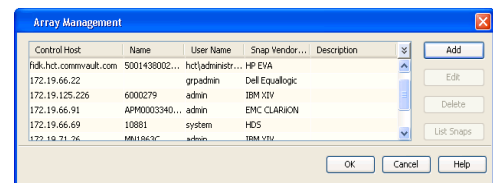
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

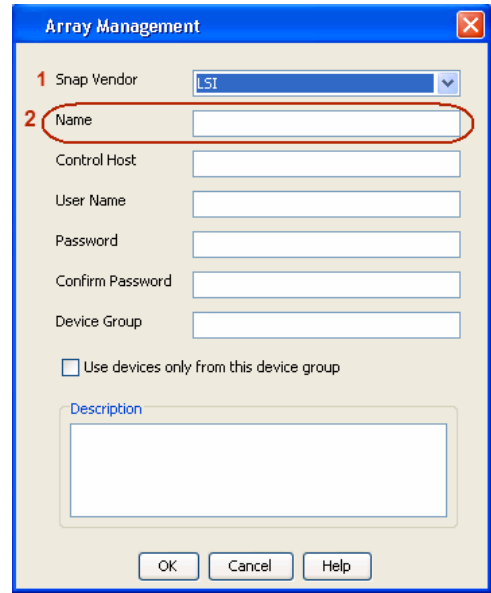
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

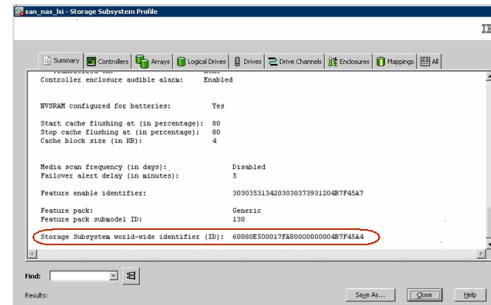


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

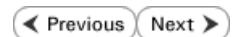
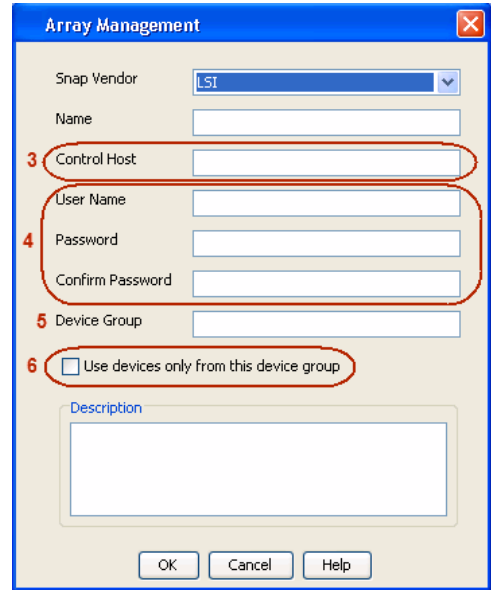
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



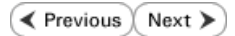
4.
 - Specify the name of the device manager server where the array was configured in the **Control Host** field.
 - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

If you specify None in the **Device Group** field but do not have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



SnapProtect™ Backup - NetApp



PREREQUISITES

LICENSES

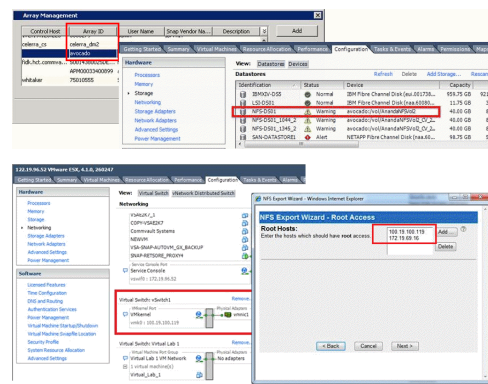
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.

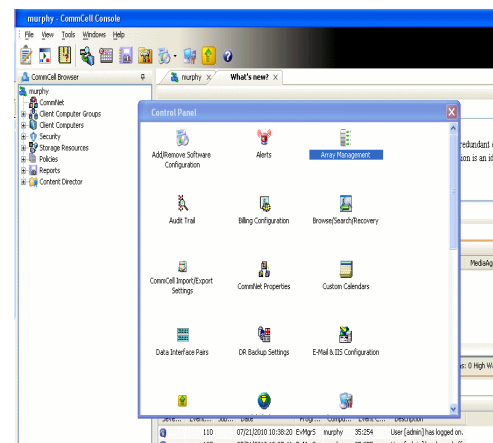
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



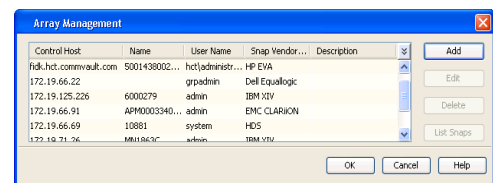
SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the file server in the **Name** field.
 - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: [Text Box]

Control Host: [Text Box]

User Name: [Text Box]

Password: [Text Box]

Confirm Password: [Text Box]

Device Group: [Text Box]

Use devices only from this device group

Description: [Text Area]

OK Cancel Help

◀ Previous Next ▶

SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous Next ▶

OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

PREREQUISITES

LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:

```
options snapvault.enable on
```

3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:

```
options snapvault.access host=secondary_filer1, secondary_filer2
```

4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:

```
options snapvault.access host=primary_filer1, primary_filer2
```

INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
 - Discover storage devices
 - Add Resource Pools to be used for the Vault/Mirror storage provisioning

CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

CREATE STORAGE POLICY

Use the following steps to create a storage policy.

1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.

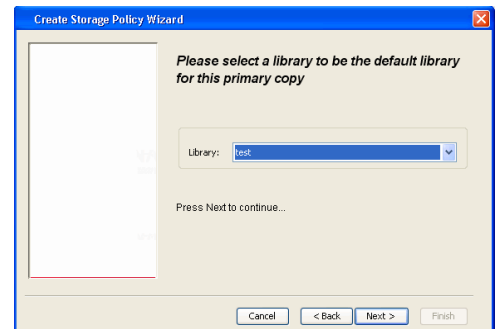
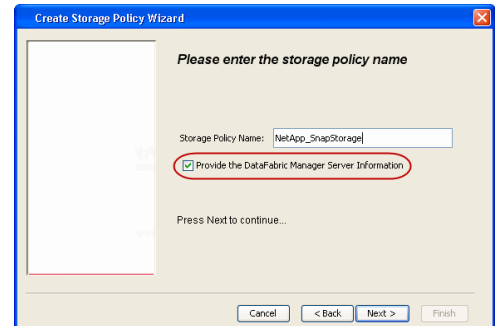
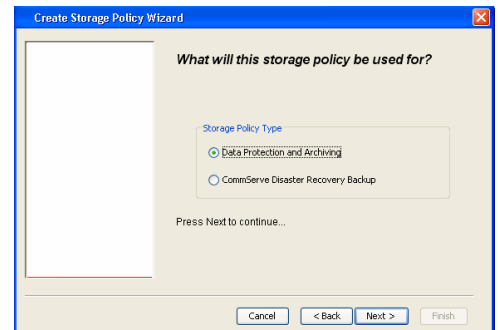
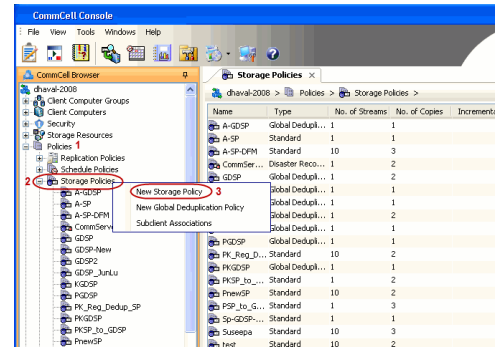
2. Click **Next**.

3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.

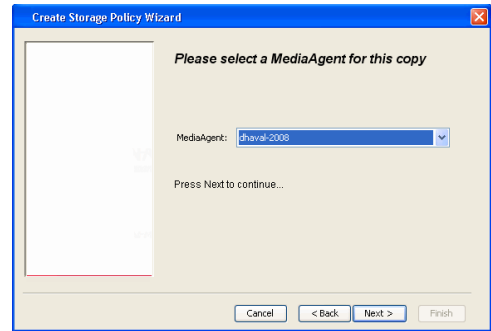
4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.

It is recommended that the selected disk library uses a LUN from the File server.
 - Click **Next**.

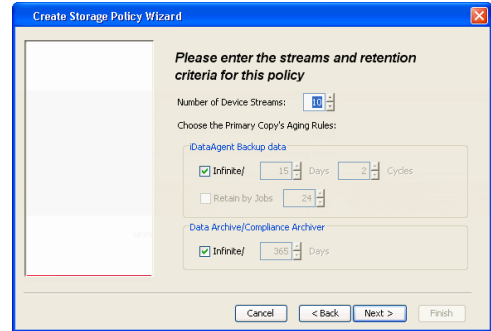
5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.



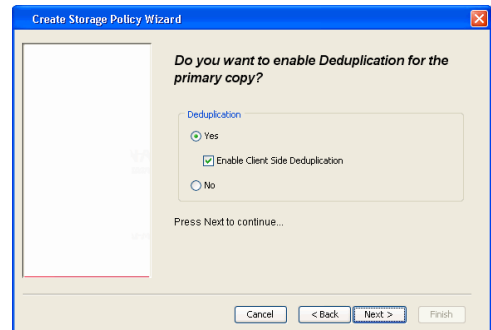
6. Click **Next**.



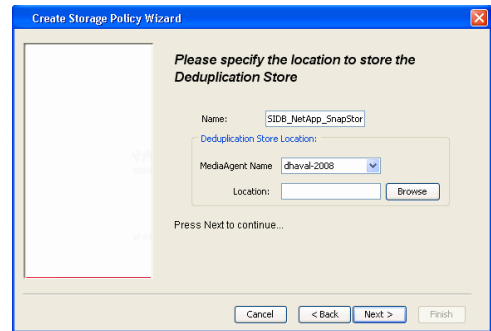
7. Click **Next**.



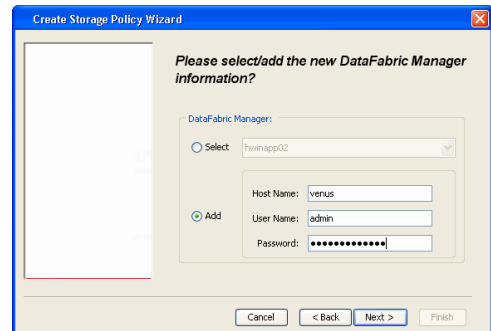
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

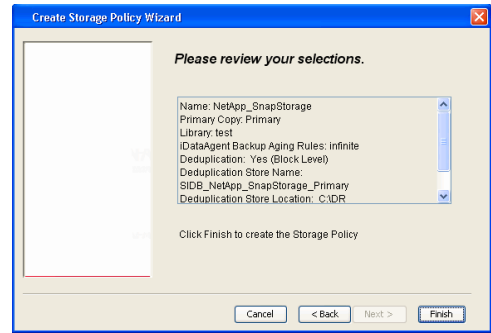


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



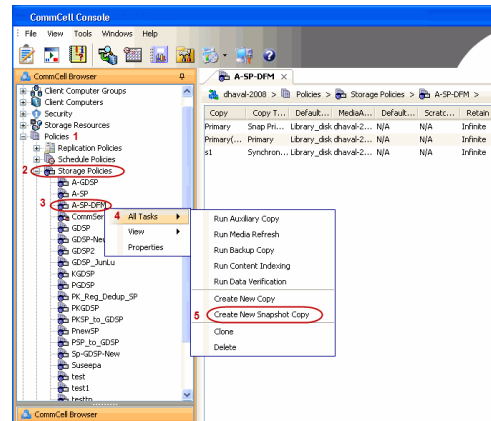


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

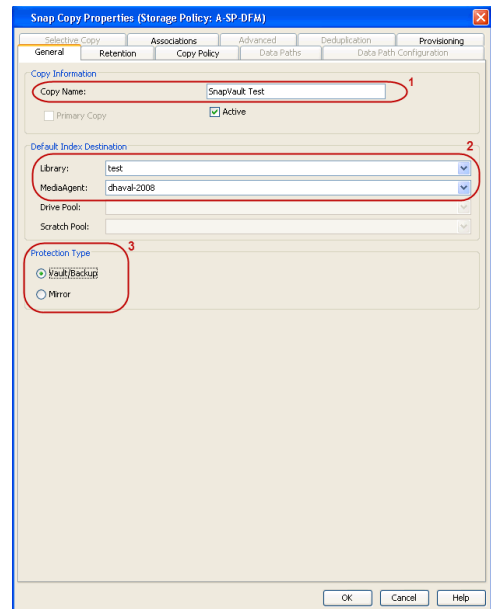
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
 - From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
 - Enter the **Copy Name**.
 - Select the **Library** and **MediaAgent** from the drop-down list.
 - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

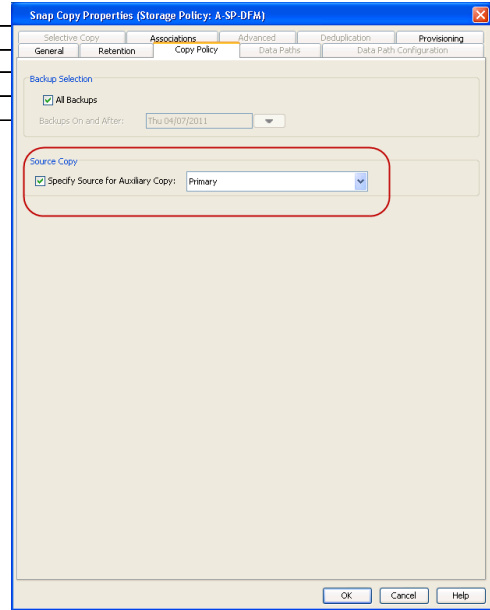


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

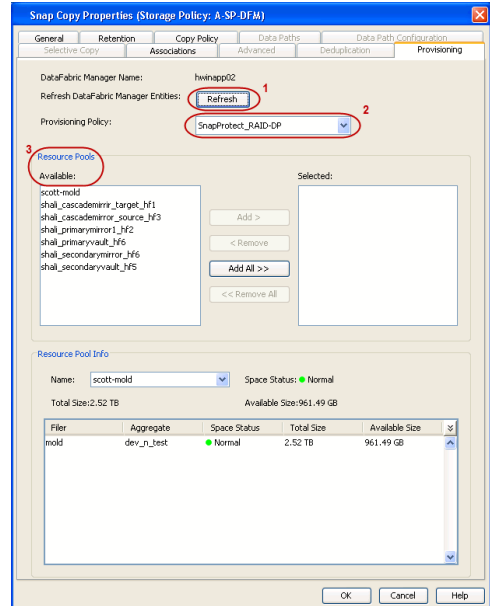
TOPOLOGY	SOURCE COPY
----------	-------------

Primary-Mirror	Primary
Primary-Mirror-Vault	Mirror
Primary-Vault	Primary
Primary-Vault-Mirror	Vault
Primary-Mirror-Mirror	Mirror



- Click the **Provisioning** tab.
 - Click **Refresh** to display the DFM entities.
 - Select the **Provisioning Policy** from the drop-down list.
 - Select the **Resource Pools** available from the list.
 - Click **OK**.

The secondary snapshot copy is created.



- If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:


```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

It is recommended that you perform this operation on all nodes in the P-M-V topology.

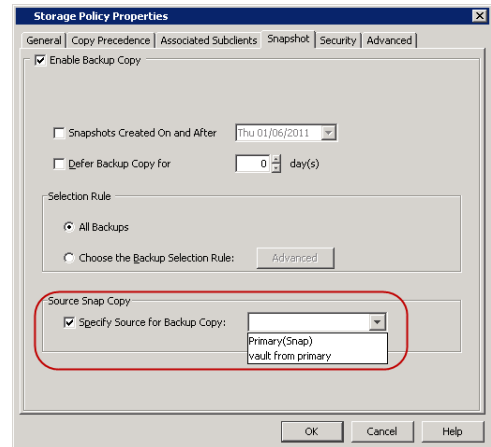
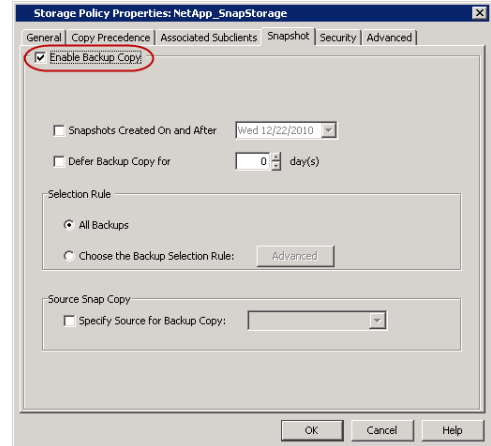
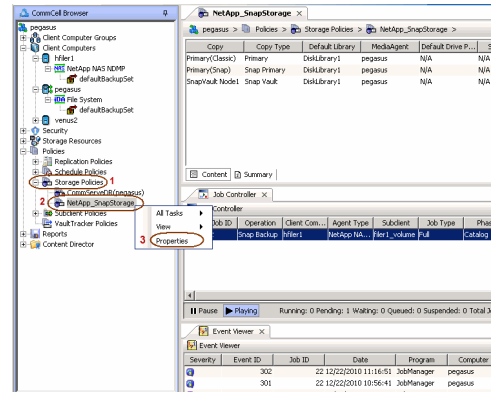
CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.

2.
 - Click the **Snapshot** tab.
 - Select **Enable Backup Copy** option to enable movement of snapshots to media.
 - Click **OK**.

3.
 - Select **Specify Source for Backup Copy**.
 - From the drop-down list, select the source copy to be used for performing the backup copy operation.

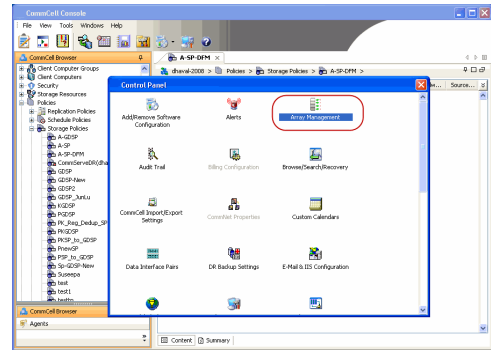


SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

2. Click **Add**.

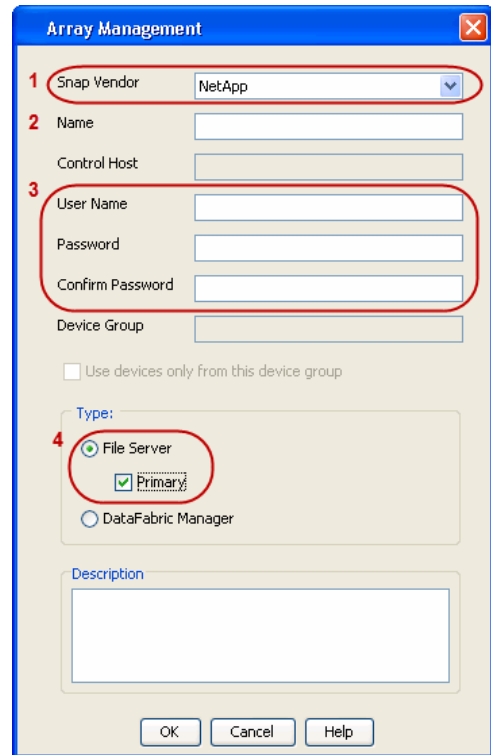
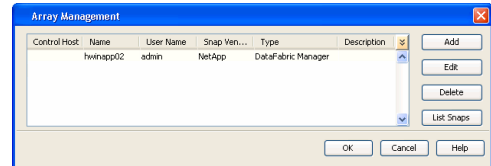


3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

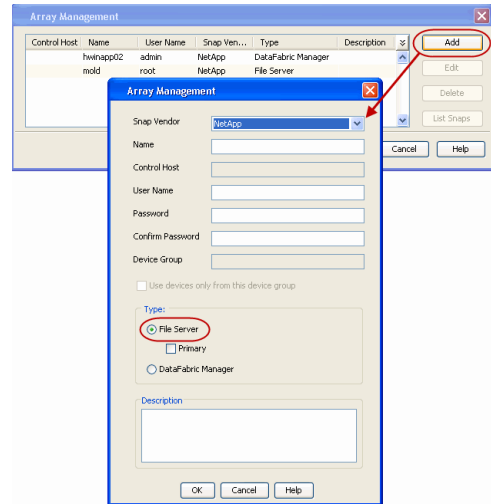
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



4.
 - Click **Add** again to enter the information for the secondary array.
 - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



SEE ALSO

Import Wizard Tool

Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

Getting Started - DB2 Backup

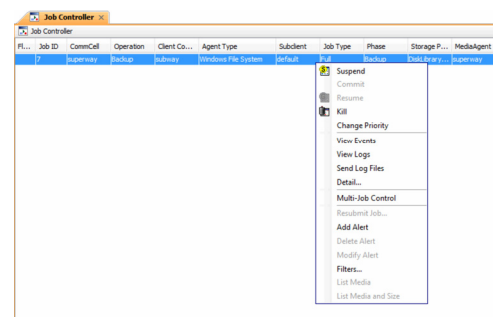
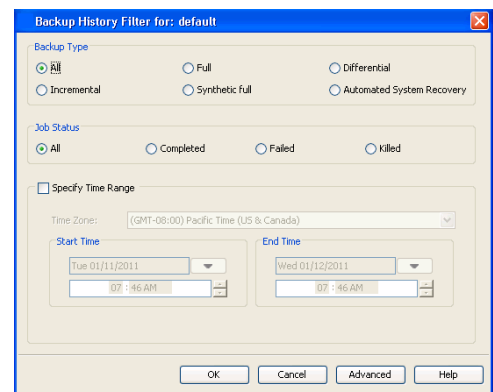
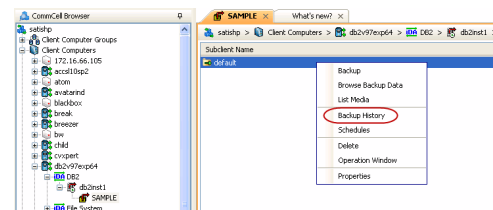
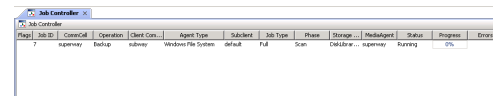
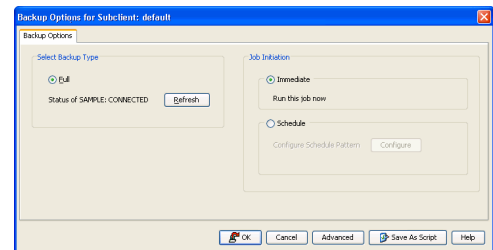
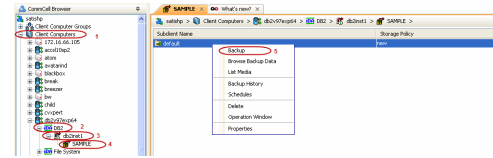


PERFORM A BACKUP

Once the storage policy is configured, you are ready to perform your first backup.

The following section provides step-by-step instructions for performing your first backup:

- From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **DB2** | **<Instance>**
 - Right-click the subclient and click **Backup**.
- Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.
- You can track the progress of the job from the **Job Controller**.
- Once job is complete, view the details of job from the **Backup History**. Right-click the **Subclient** and select **Backup History**.
- Click **OK**.
- You can view the following details about the job by right-clicking the job:
 - Items that failed during the job
 - Items that succeeded during the job
 - Details of the job
 - Events of the job
 - Log files of the job
 - Media associated with the job



Getting Started - Vault/Mirror Copy

◀ Previous Next ▶

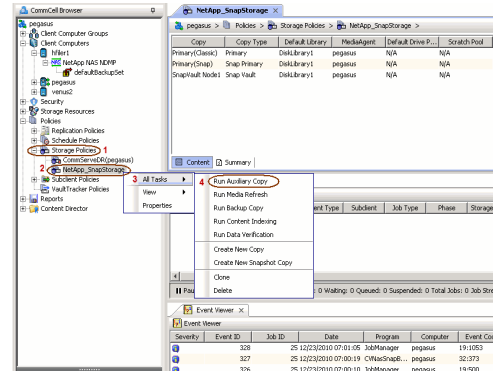
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

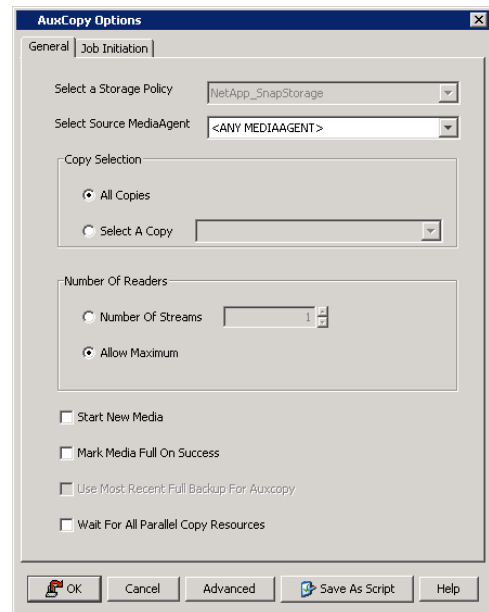
INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

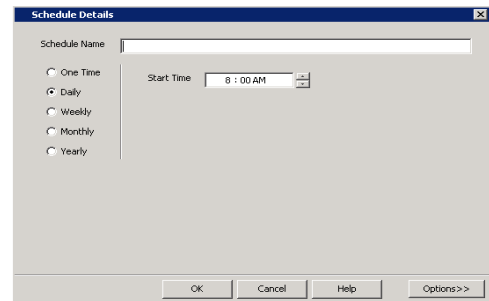


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- Enter the schedule name and select the appropriate scheduling options.
 - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.

◀ Previous Next ▶

Getting Started - Snap Movement to Media

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

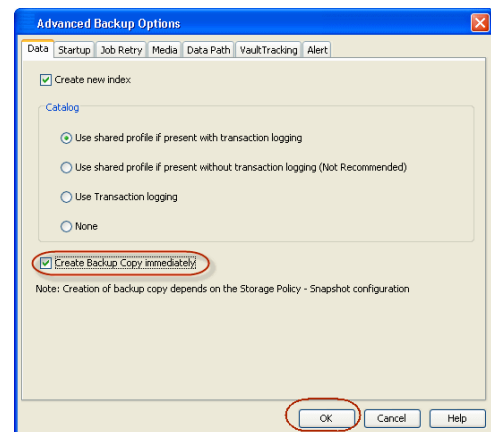
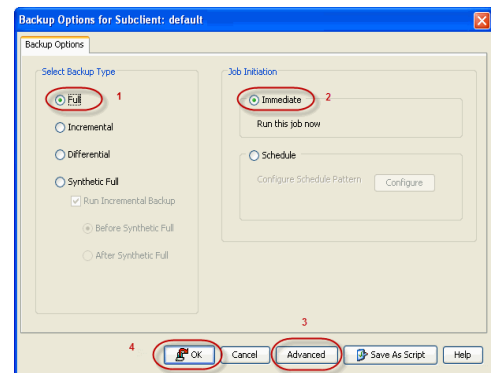
INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

1.
 - From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
 - Right click the default subclient and click **Backup**.
 - Select **Full** as backup type.
 - Click **Advanced**.

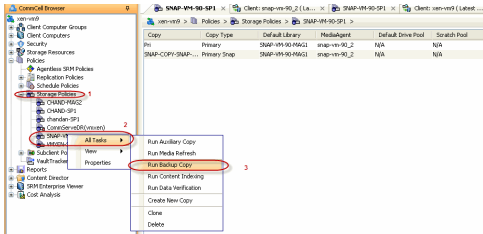
2.
 - Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



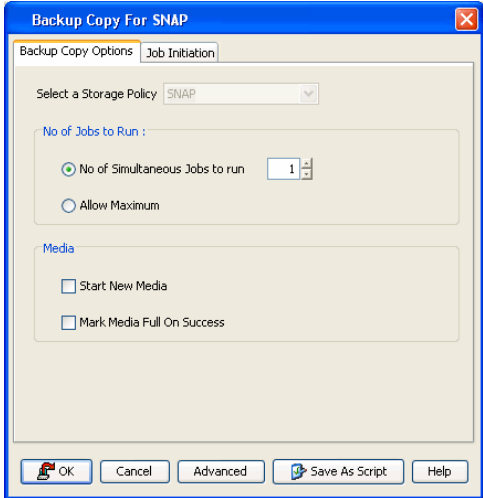
OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

1.
 - From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



Getting Started - DB2 Restore

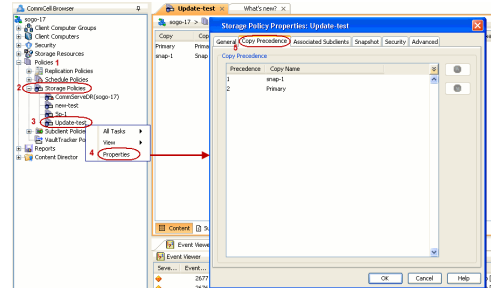


PERFORM A RESTORE

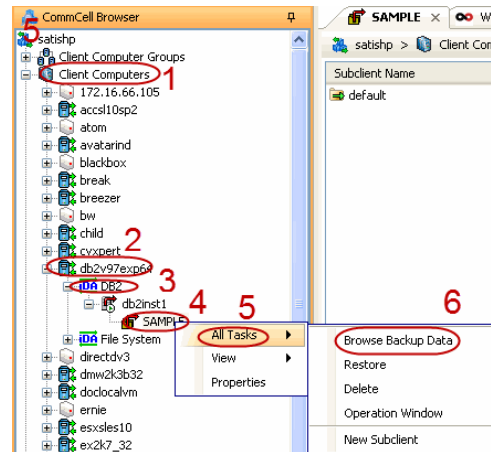
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring the entire database to a different computer.

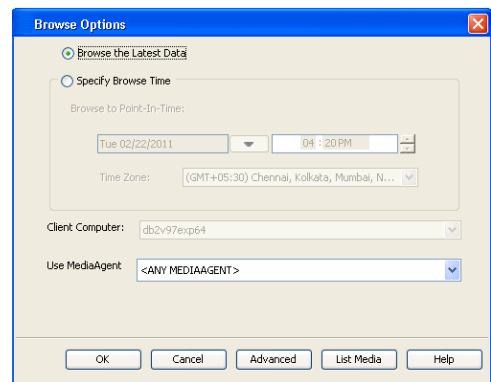
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
 - Click **OK**.



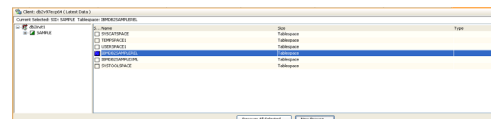
- From the CommCell Browser, navigate to **Client Computers | <Client> | DB2**.
 - Right-click the backup set and then click **All Tasks | Browse Backup Data**.



- Click **OK**.

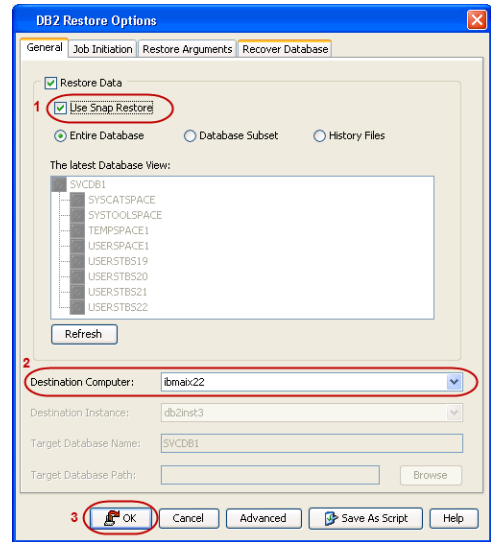


- Select the entire database in the left pane.
 - Click **Recover All Selected**.
- Select the **Use Snap Restore** checkbox to restore the database to a different computer.
 - Select the **Destination Computer** in which to restore the entire database.

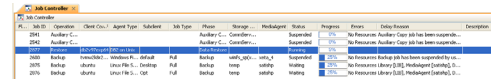


Ensure that the source and destination computers have the same directory structure and user/group IDs of the DB2 instance you are restoring.

- Click **OK**.



6. You can monitor the progress of the restore job in the **Job Controller**.



CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



Getting Started - Unix File System Deployment



Use the following steps to install the File System iDataAgent on a Linux computer.

WHERE TO INSTALL

Install the software directly on the Linux computer that you wish to protect.

BEFORE YOU BEGIN

Download Software Packages

Download the latest software package to perform the install.

SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.

INSTALL THE UNIX FILE SYSTEM /DATAAGENT

Use the following procedure to directly install the software from the installation package or a network drive.

- Logon to the client computer as **root** or as a sudo user.
If you are installing the software using a sudo user account, make sure that sudo user account is configured on this computer. For more information, see FAQ - Install.
- 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:
./cvpkgadd
- The product banner and other information is displayed.
Press **Enter**.
- Read the license agreement. Type **y** and press **Enter**.
- Press **Enter**.
- Press **Enter**.
- 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 interface name that you wish to use as default, and then press **Enter**.

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

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
- 2) Advance options
- 3) Exit this menu

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.

You now have a choice of performing a regular Calypso install on the physical host or installing Calypso on a virtual machine for operation within a cluster.

Most users should select "Install on a physical machine" here.

- 1) Install on a physical machine
- 2) Install on a virtual machine
- 3) Exit

Your choice: [1]

We found one network interface available on your machine. We will associate it with the physical machine being installed, and it will also be used by the CommServe to connect 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 check the interface name below, and make connections if necessary:

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

8. Press **Enter**.
9. Type the number associated with the **Unix File System iDataAgent and MediaAgent**. Press **Enter**.
10. A confirmation screen will mark your choice with an "X". Type **d** for **Done**, and press **Enter**.
11. Press **Enter**.
12. Type the appropriate number to install the latest software scripts and press **Enter**.
- Select **Download from the software provider website** to download the latest software scripts. Make sure you have internet access.
 - Select **Use the one in the installation media** to install the software scripts from the package or share from which the installation is currently being 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.
13. Press **Enter**.
14. Press **Enter** to accept the default path.
- If you want to specify a different path, type the path and then press **Enter**.
 - If you want to install the software binaries to an NFS shared drive, specify the directory on which you have mounted the NFS file system and then press **Enter**.
- In order to make sure that the client computer has `read/write` access to NFS shared drive, review the steps described in `Installing Software Binaries to an NFS Shared Drive`.
- Do not use the following characters when specifying the path:
- ```
!@#$$%^&*():/?\
```
15. Press **Enter** to accept the default location.
- Enter a path to modify the default location and press **Enter**.
  - All the modules installed on the computer will store the log files in this directory.
16. Press **Enter**.

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]

Install Calypso on physical machine angel

Please select the Calypso module(s) that you would like to install.

[ ] 1) MediaAgent [1301] [CVGxMA]

[ ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]

[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

Install Calypso on physical machine 172.19.99.62

Please select the Calypso module(s) that you would like to install.

[X] 1) UNIX File System iDataAgent [1101] [CVGxIDA]

[X] 2) MediaAgent [1301] [CVGxMA]

[ ] 3) ProxyHost iDataAgent [1102] [CVGxProxyIDA]

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

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

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]

Please specify where you want us to install Calypso binaries.

It must be a local directory and there should be at least 176MB 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]

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]

Most of Software processes run with root privileges, but some are launched by databases and inherit database access rights. To make sure that registry and log files can be written to by both kinds of processes we can either make

- such files world-writeable or we can grant write access only to processes belonging to a particular group, e.g. a "calypso" or a "dba" group.
- We highly recommend now that you create a new user group and enter its name in the next setup screen. If you choose not to assign a dedicated group to Software processes, you will need to specify the access permissions later.
- If you're planning to backup Oracle DB you should use "dba" group.
- Would you like to assign a specific group to Software?  
[yes]
- Please enter the name of the group which will be assigned to all Software files and on behalf of which all Software 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: skyl
- 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 "skyl".
- 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 : [8400]
- Port Number for EvMgrC: [8402]
- Is there a firewall between this client and the CommServe?  
[no]
- If this computer is separated from the CommServe by firewall(s), type **Yes** and then press **Enter**.
- For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.
- Please specify hostname of the CommServe below. Make sure the hostname is fully qualified, resolvable by the name services configured on this machine.
- CommServe Host Name: mycommserve.company.com
- 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.
- 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(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.
- [ ] 1) Unix  
[ ] 2) DR
- [a=all n=none r=reverse q=quit d=done >=next <=previous ? =help]
- Enter number(s)/one of "a,n,r,q,d,>,<," here: 1
- 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.
- [X ] 1) Unix  
[ ] 2) DR
- [a=all n=none r=reverse q=quit d=done >=next <=previous ?
17. Type the **Group name** and then press **Enter**.
18. 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**.
19. If you do not wish to configure the firewall services, press **Enter**.
20. Type the fully qualified CommServe host name and press **Enter**.  
Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.
21. Press **Enter**.
22. Type the appropriate number to select the **Client Group** and press **Enter**.  
This screen will be displayed only if Client Groups are configured for the CommCell
23. A confirmation screen will mark your choice with an "**X**".  
Type **d** for **Done**, and press **Enter**.

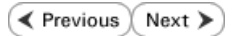
24. Enter the number associated with the storage policy you want use and press **Enter**.

25. Type **3** and press **Enter**.  
The installation is now complete.

```
=help]
Enter number(s)/one of "a,n,r,q,d,>,<,>?" here: d
Please select one storage policy for this IDA from the
list below:
1) SP_StandAloneLibrary2_2
2) SP_Library3_3
3) SP_MagLibrary4_4
Storage Policy: [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
angel.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 angel.company.com
2) Install Calypso on a virtual machine
3) Exit
Your choice: [3]
```



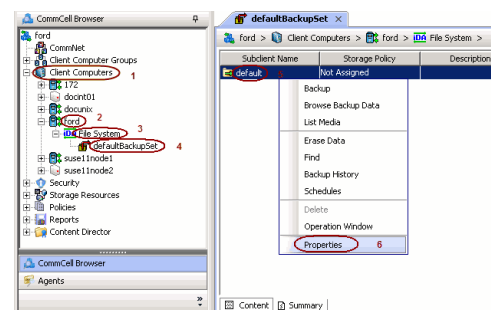
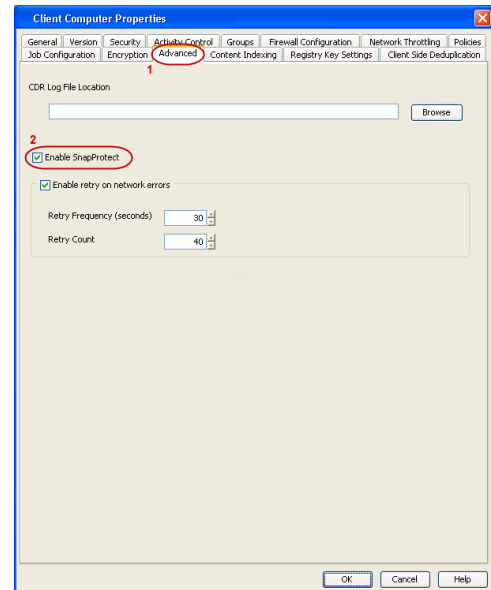
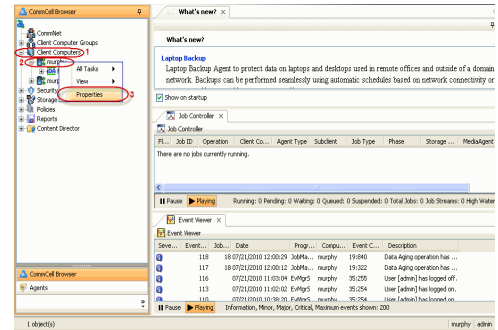
# Getting Started - Unix File System Configuration

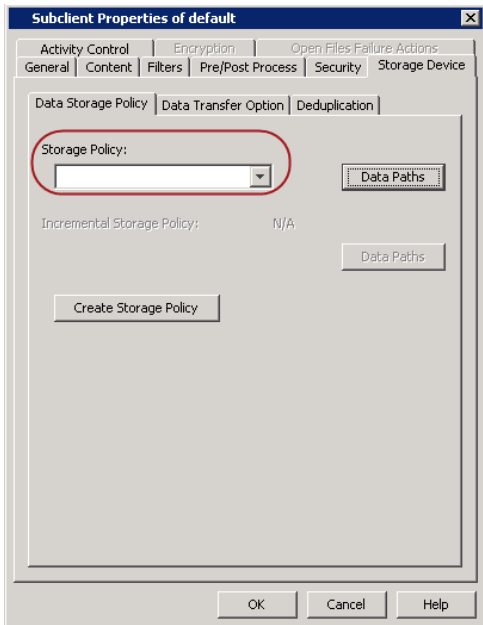


## CONFIGURATION

Once installed, the Linux File System *rdDataAgent* requires some additional configuration before running your first SnapProtect backup. Follow the steps given below to complete the configuration for this Agent.

1.
  - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
  - Right-click the client and select **Properties**.
  
2.
  - Click on the **Advanced** tab.
  - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
  - Click **OK**.
  
3.
  - From the CommCell Browser, navigate to **<Client>** | **File System**.
  - Right click the default subclient and click **Properties**.
  
4.
  - Click the **Storage Device** tab.
  - In the **Storage Policy** box, select the storage policy name.

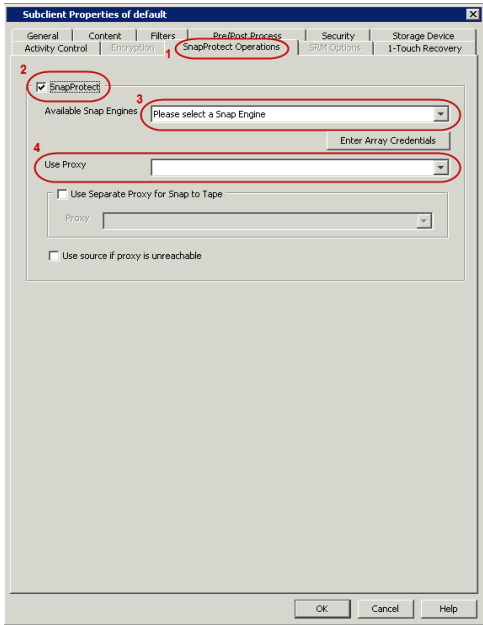




5.
  - Click the **SnapProtect Operations** tab.
  - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
  - Select the storage array from the **Available Snap Engine** drop-down list.
  - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy operations will be performed.

When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent. Select the MediaAgent from the **Proxy** list.

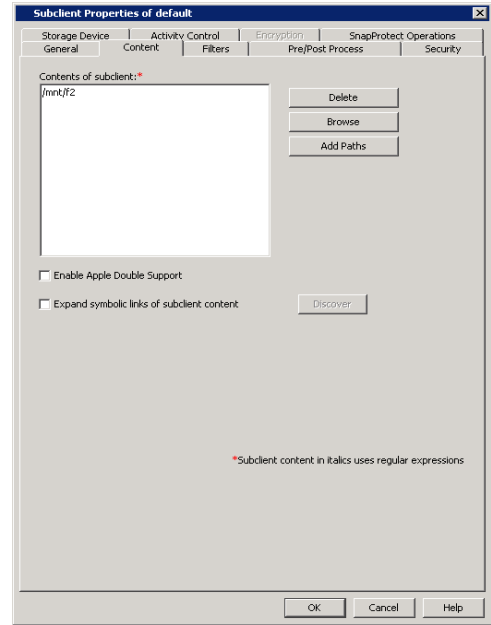


6.
  - Click the **Content** tab.
  - Click **Browse** and specify the content for the subclient.
  - Click **OK**.

The subclient content must contain data that resides on the storage device volume; do not include local drives as subclient content.

The root folder (/) or a folder belonging to the root volume should not be added as subclient content.





## SKIP THIS SECTION IF NOT USING SOLARIS.

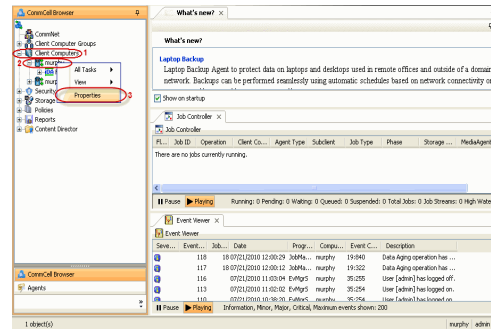
Click **Next** ➤ to Continue.

## ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE

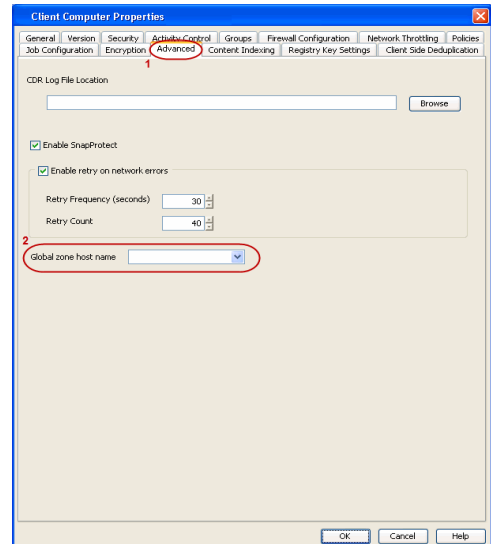
**Next** ➤

Follow the steps given below to enable SnapProtect backups on each of the non-global zone clients containing the application data.

- From the CommCell Console, navigate to **Client Computers** | **<Client>**.
  - Right-click the client and select **Properties**.



- Click **Advanced** tab.
  - Select the **Global Zone host name** from the drop-down list.
  - Click **OK**.
  - We support disks on a global zone mounted using loopback File System on a non global zone.
  - This option need not be enabled if you are using a NFS share. This is because when using NFS mount paths, the operations are limited to the non-global zone and does not use the global zone.



- Repeat the above steps on all the non-global zone clients containing the application

data.

## SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

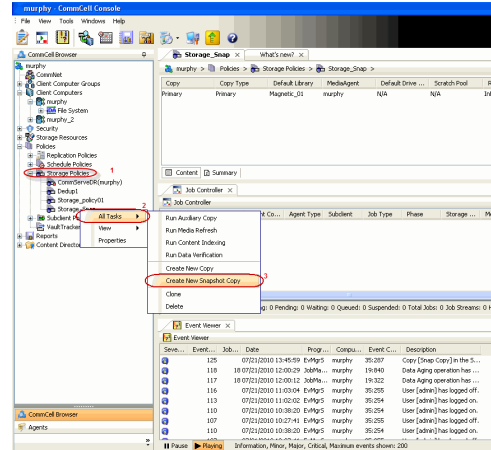
Click **Next** to Continue.

Next

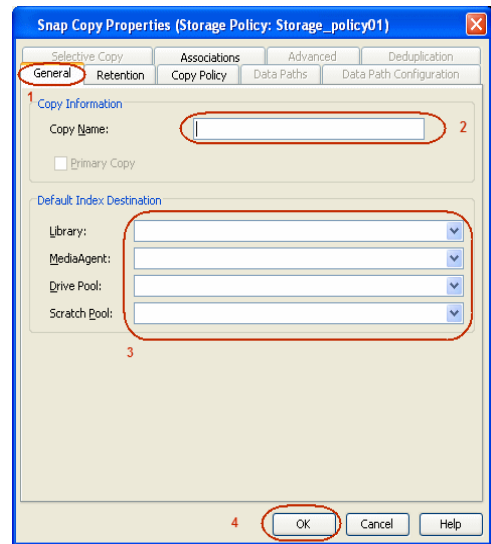
### CREATE A SNAPSHOT COPY

Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.



- Enter the copy name in the **Copy Name** field.
  - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
  - Click **OK**.

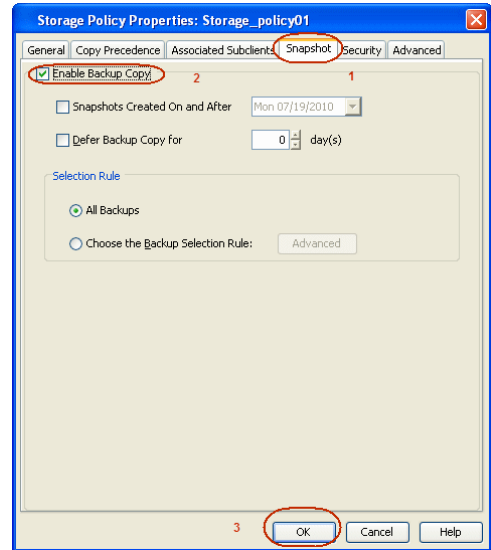
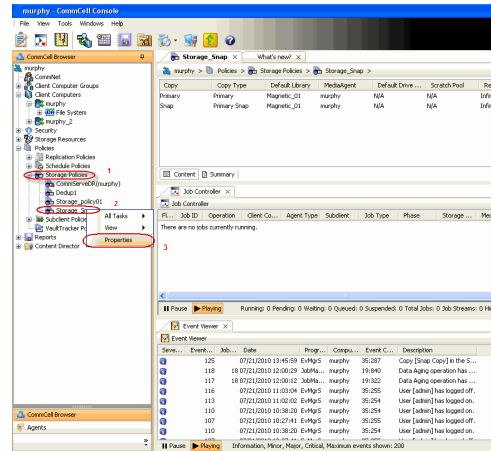


### CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

- From the CommCell Browser, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.

2.
  - Click the **Snapshot** tab.
  - Select **Enable Backup Copy** option to enable movement of snapshots to media.
  - Click **OK**.



# Storage Array Configuration

◀ Previous Next ▶

## CHOOSE THE STORAGE ARRAY

| HARDWARE STORAGE ARRAYS          | SOFTWARE STORAGE ARRAY |
|----------------------------------|------------------------|
| 3PAR                             | DATA REPLICATOR        |
| DELL COMPELLENT                  |                        |
| DELL EQUALLOGIC                  |                        |
| EMC CLARIION, VNX                |                        |
| EMC SYMMETRIX                    |                        |
| FUJITSU ETERNUS DX               |                        |
| HITACHI DATA SYSTEMS             |                        |
| HP EVA                           |                        |
| IBM SVC                          |                        |
| IBM XIV                          |                        |
| LSI                              |                        |
| NETAPP                           |                        |
| NETAPP WITH SNAPVAULT/SNAPMIRROR |                        |

◀ Previous Next ▶

# SnapProtect™ Backup - 3PAR

◀ Previous   Next ▶

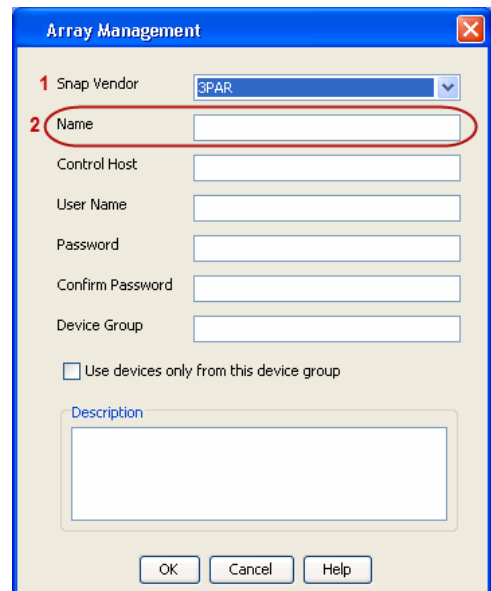
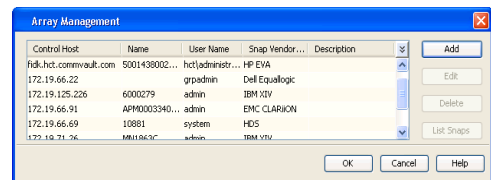
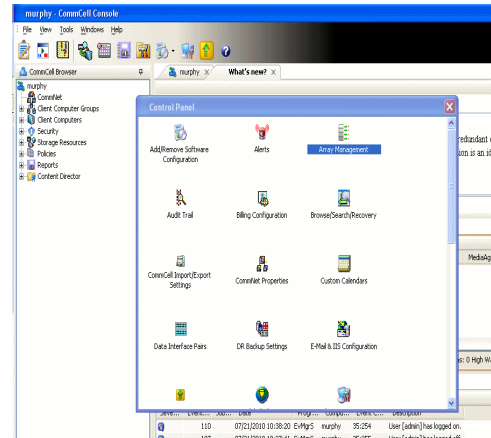
## PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
  - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where  $\text{DevID.substr}(4,3)$  is the next 3 digits after the fourth digit from the WWN number

where  $\text{DevID.substr}(12,4)$  is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$  is 2AC and  $\text{DevID.substr}(12,4)$  is 0B95

After adding all the values, the resulting array name is 2FF70002AC000B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where  $\text{DevID.substr}(4,3)$  is the next 3 digits after the fourth digit from the WWN number

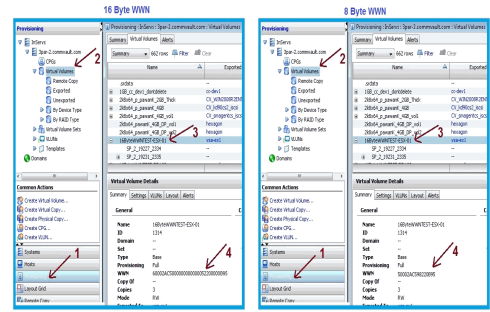
where  $\text{DevID.substr}(26,6)$  is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$  is 2AC and  $\text{DevID.substr}(26,6)$  is 000B95

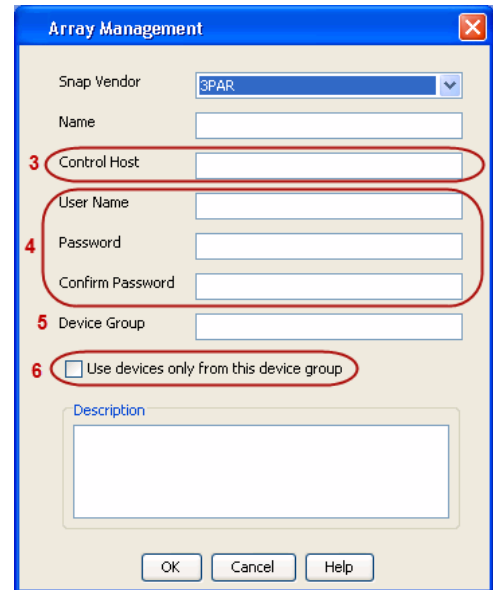
After adding all the values, the resulting array name is 2FF70002AC000B95.



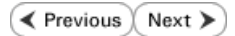
- Enter the IP address of the array in the **Control Host** field.
  - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - Dell EqualLogic



## PRE-REQUISITIES

### WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

### UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

### FIRMWARE VERSION

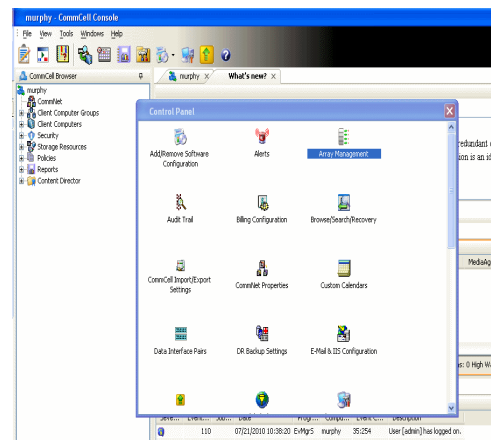
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
  - Create a new group administration account in the firmware, and set the desired permissions for this account.
  - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

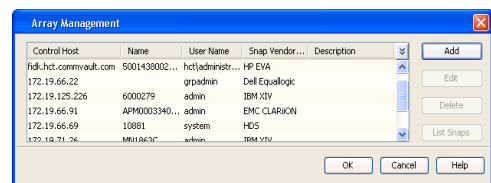
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

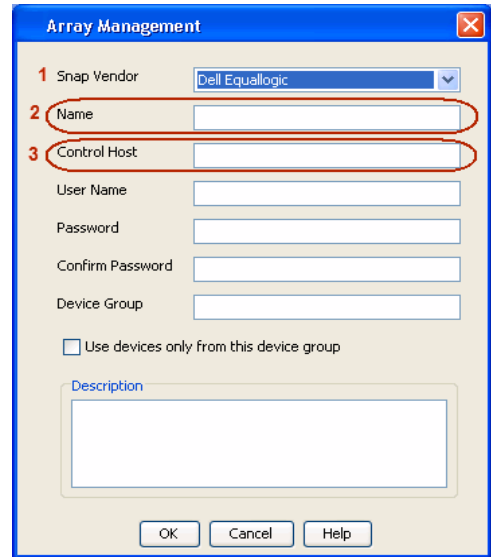


2. Click **Add**.

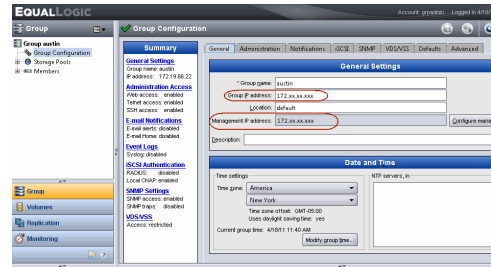


3.
  - Select **Dell Equallogic** from the **Snap Vendor** list.
  - Specify the Management IP address in the **Name** field.
 

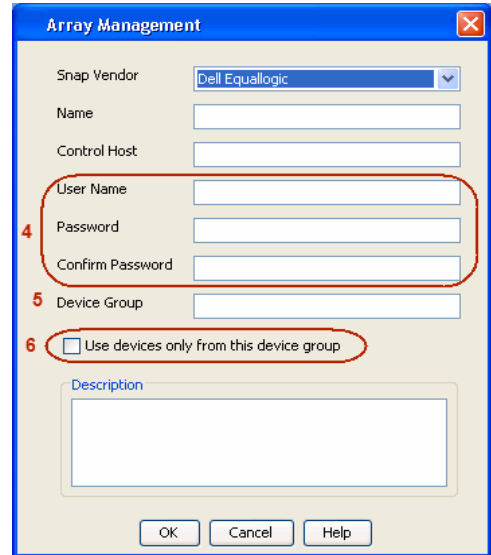
No entry is required in the **Name** field if there is no Management IP address configured.
  - Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
  - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
  - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
  - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.





# SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous   Next ▶

## PRE-REQUISITES

### LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

### ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.  
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.  
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

## SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

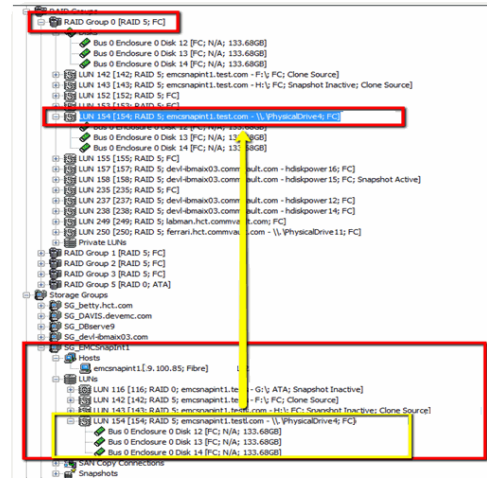
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG\_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



## AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

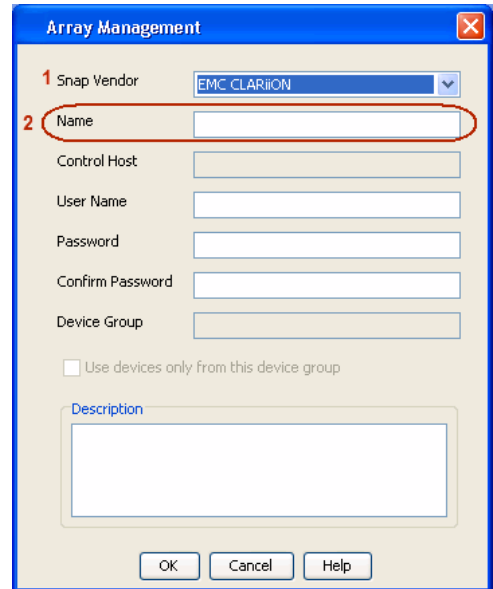
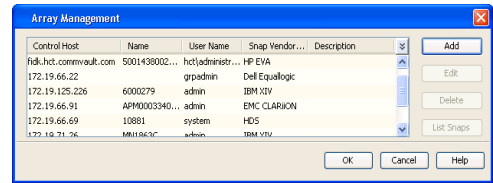
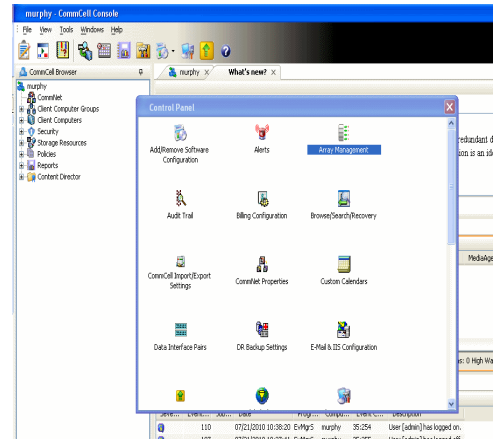
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

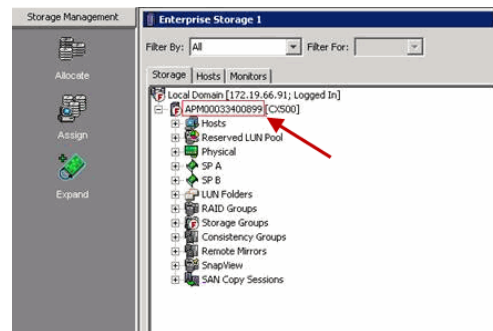
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
  - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.



- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.

**Array Management** ✕

Snap Vendor:

Name:

Control Host:

User Name:

**3** Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

OK Cancel Help

◀ Previous Next ▶

# SnapProtect™ Backup - EMC Symmetrix

◀ Previous    Next ▶

## PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

## SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

## CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

## LOAD THE SYMMETRIX DATABASE

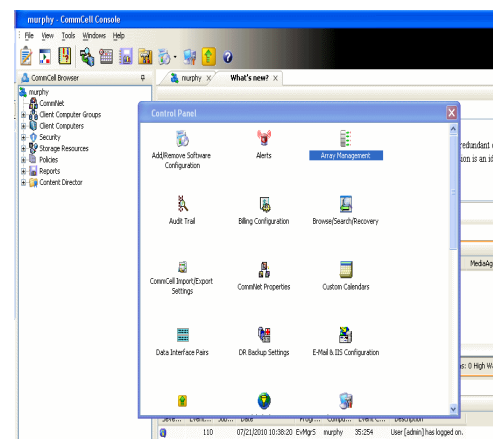
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

## SETUP THE ARRAY INFORMATION

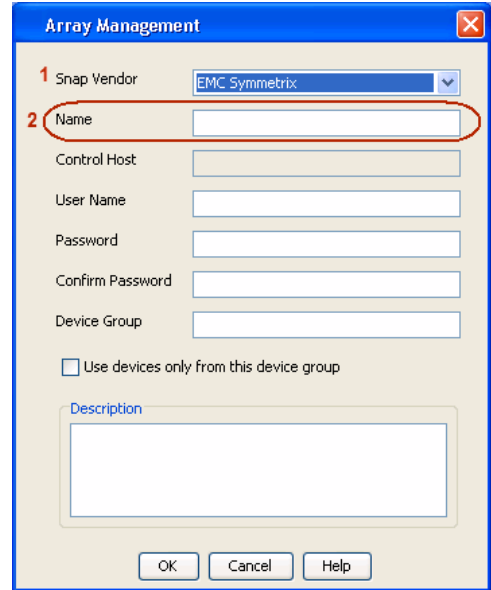
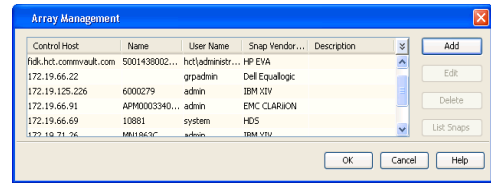
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

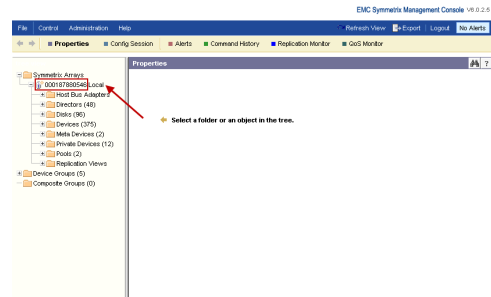


2. Click **Add**.

3.
  - Select **EMC Symmetrix** from the **Snap Vendor** list.
  - Specify the **Symm ID** of the array in the **Name** field.

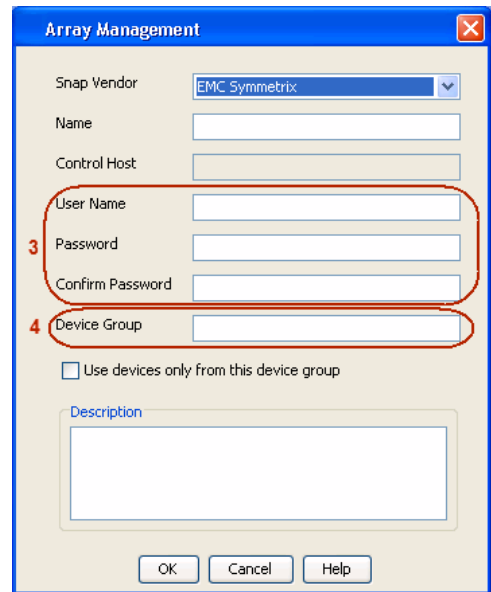


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
  - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.  
If you do not specify a device group, the default device group will be used for snapshot operations.
  - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).



# SnapProtect™ Backup - Hitachi Data Systems

◀ Previous Next ▶

## PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
  - COW pools
  - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

## ADDITIONAL REQUIREMENTS FOR VMWARE

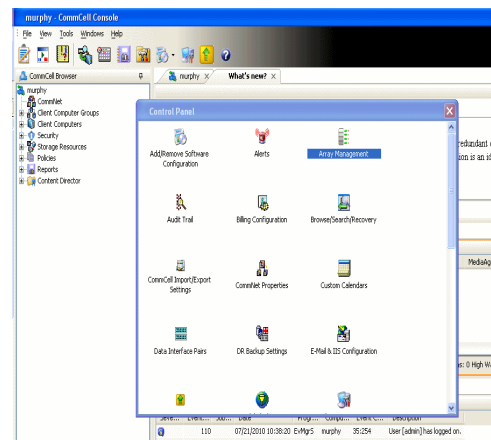
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server *iDataAgent* client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server *iDataAgent* client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

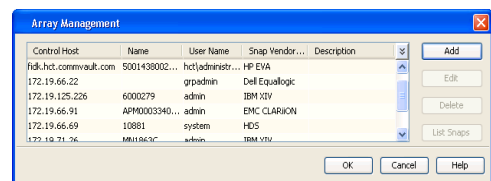
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

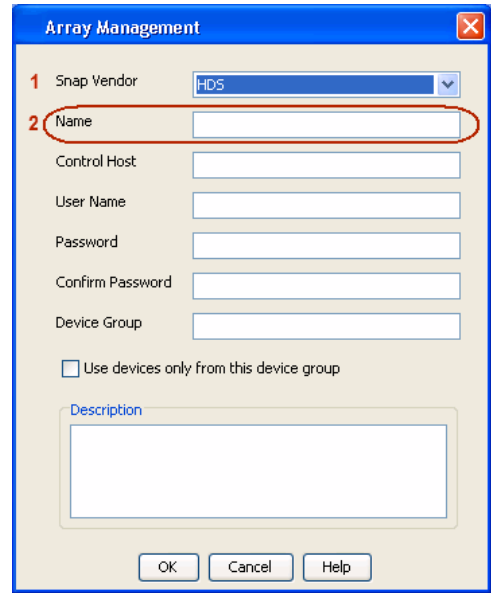
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



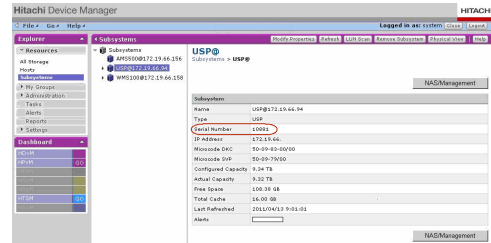
2. Click **Add**.



3.
  - Select **HDS** from the **Snap Vendor** list.
  - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



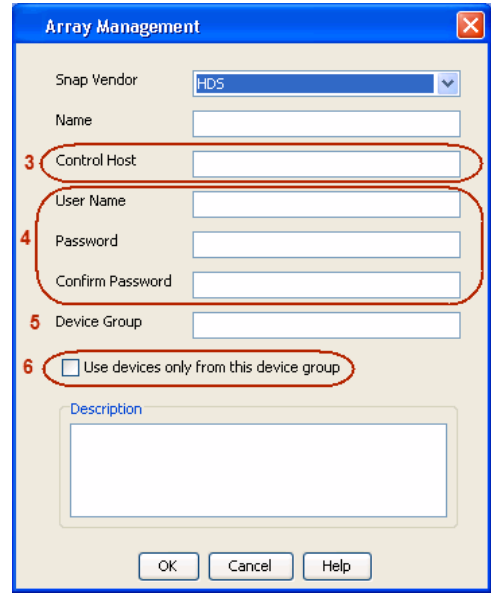
4.
  - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
  - Enter the user access information in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:

<COW\_POOL\_ID>-<LABEL> or <LABEL>-<COW\_POOL\_ID>

where <COW\_POOL\_ID> (for COW job) should be a number. This parameter is required.

<LABEL> (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.





# SnapProtect™ Backup - HP StorageWorks EVA

◀ Previous   Next ▶

## SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

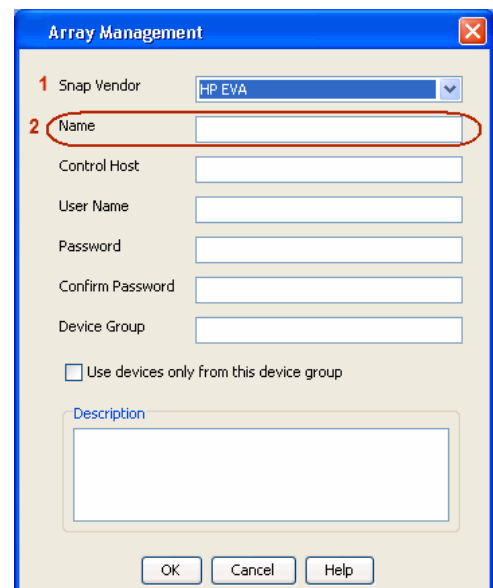
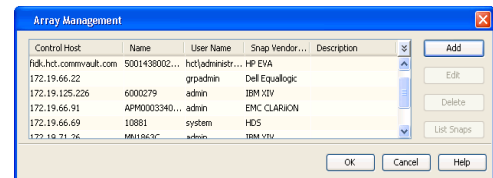
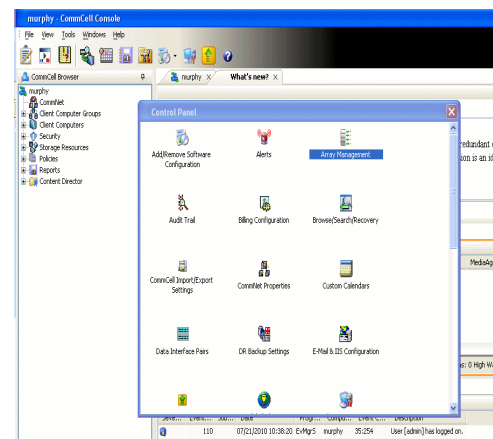
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin folder to discover the HP-EVA arrays.
3. Use the CLIRefreshTool.bat tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin folder.

## SETUP THE ARRAY INFORMATION

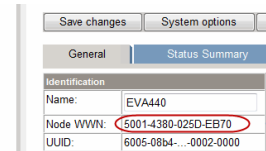
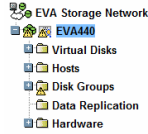
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
2. Click **Add**.
3.
  - Select **HP EVA** from the **Snap Vendor** list.
  - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

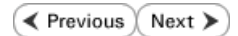
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



4.
  - Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous   Next ▶

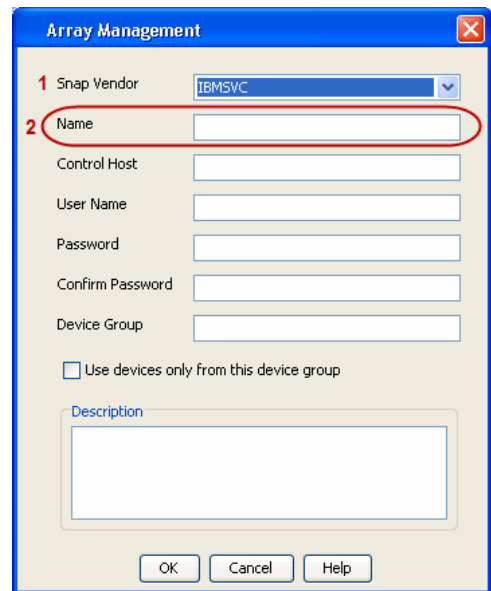
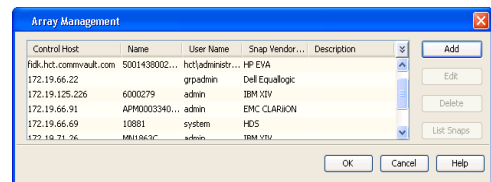
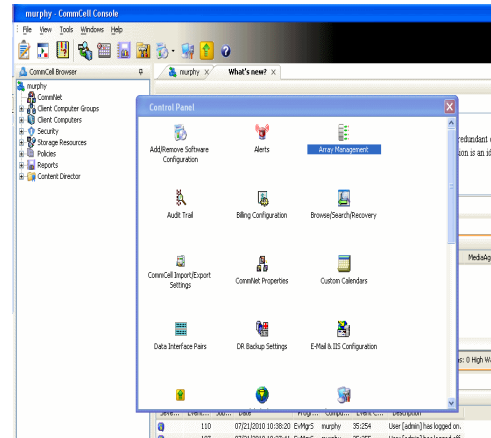
## PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

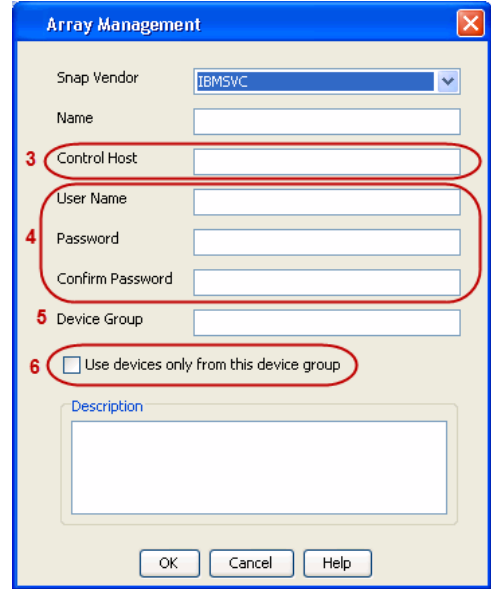
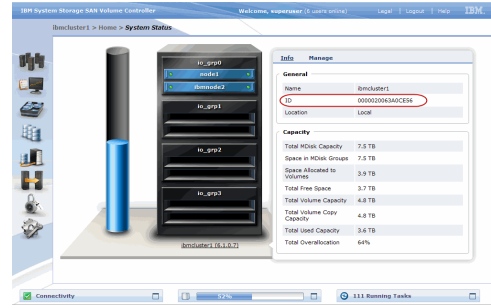
- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
  - Specify the 16-digit ID of the storage device in the **Name** field.



The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.  
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - IBM XIV

◀ Previous Next ▶

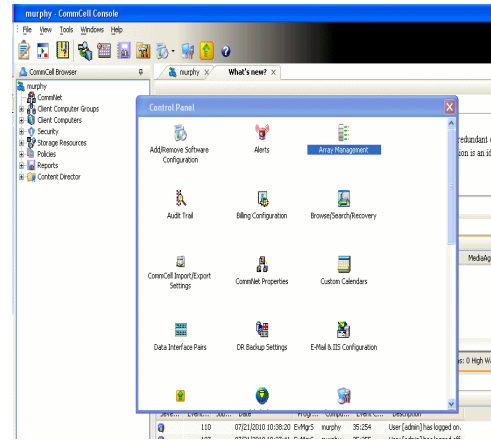
## PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

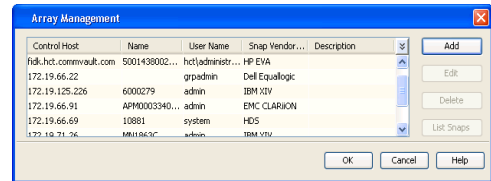
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

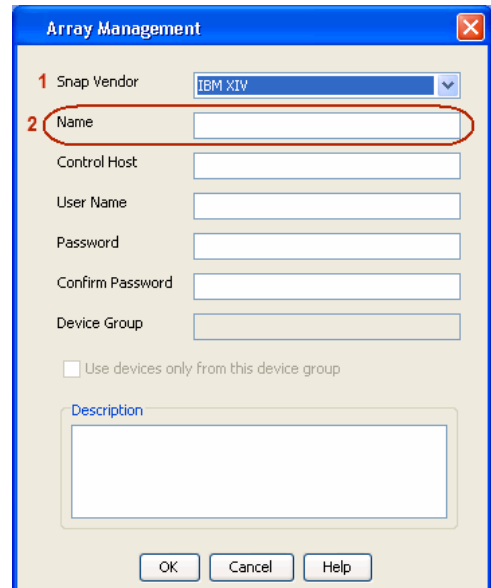
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.



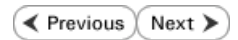
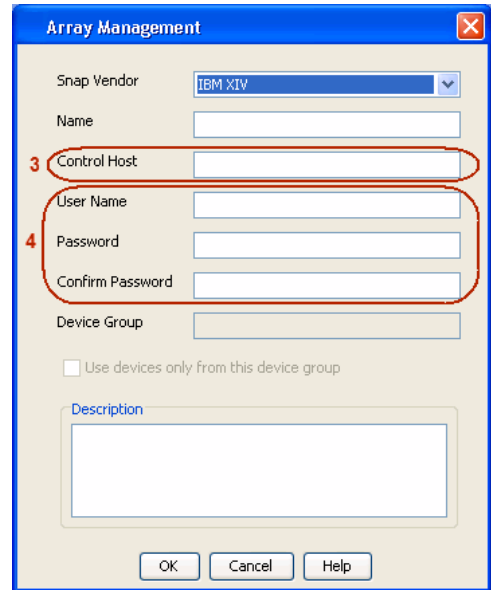
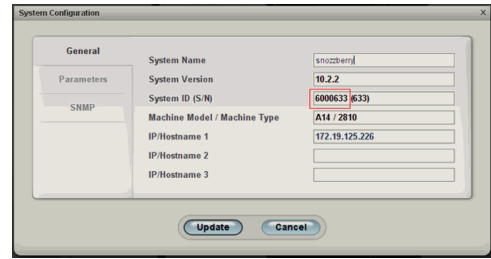
3.
  - Select **IBM XIV** from the **Snap Vendor** list.
  - Specify the 7-digit serial number for the array in the **Name** field.



The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

4.

- Enter the IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the application administrator in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - LSI

◀ Previous    Next ▶

## PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
  - SMIS server through TCP/IP network.
  - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

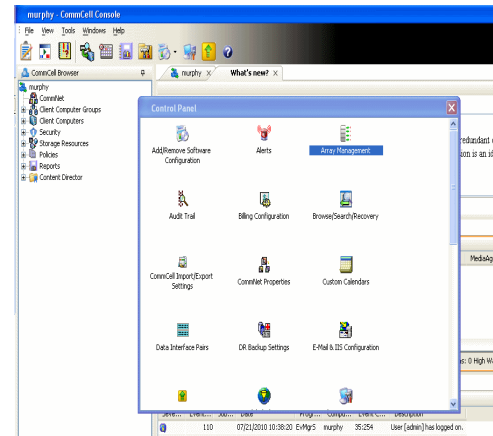
## ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

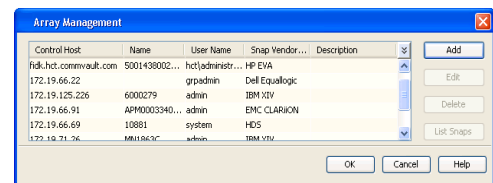
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

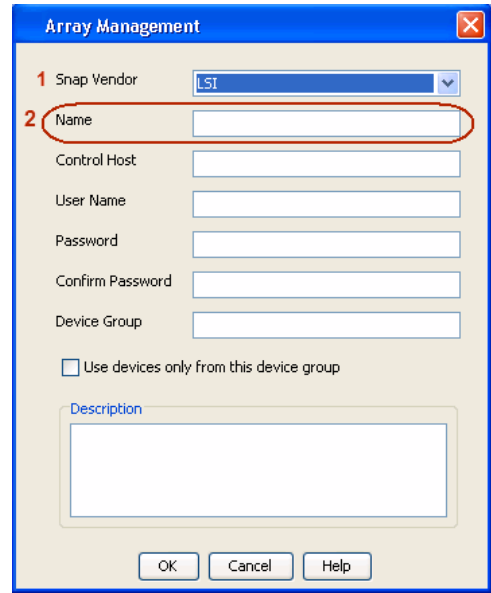
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

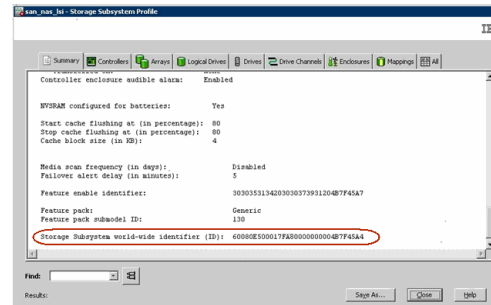


3.
  - Select **LSI** from the **Snap Vendor** list.
  - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

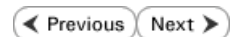
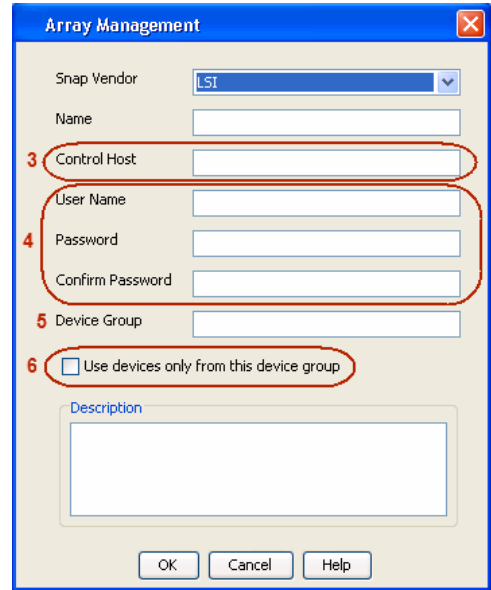
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



4.
  - Specify the name of the device manager server where the array was configured in the **Control Host** field.
  - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

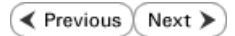
If you specify None in the **Device Group** field but do have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.





# SnapProtect™ Backup - NetApp



## PREREQUISITES

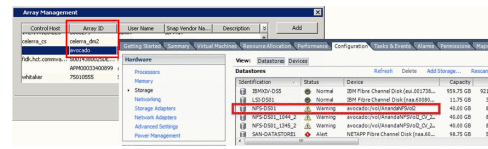
### LICENSES

- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

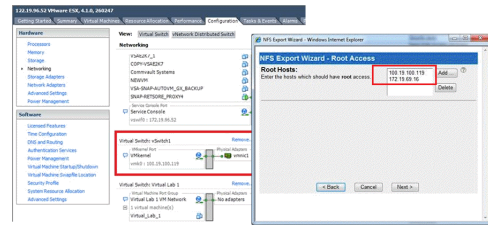
## ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.



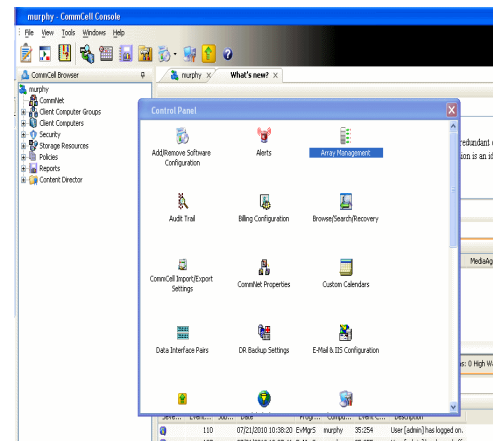
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



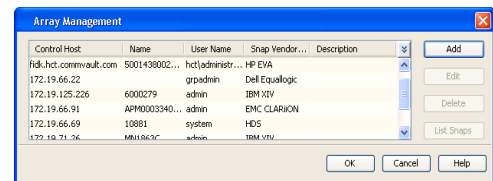
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.



3.
  - Select **NetApp** from the **Snap Vendor** list.
  - Specify the name of the file server in the **Name** field.
  - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: [ ]

Control Host: [ ]

User Name: [ ]

Password: [ ]

Confirm Password: [ ]

Device Group: [ ]

Use devices only from this device group

Description: [ ]

OK Cancel Help

◀ Previous Next ▶

# SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous   Next ▶

## OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

## PREREQUISITES

### LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

### ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

## SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:

```
options snapvault.enable on
```

3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:

```
options snapvault.access host=secondary_filer1, secondary_filer2
```

4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:

```
options snapvault.access host=primary_filer1, primary_filer2
```

## INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see [Setup the DataFabric Manager Server](#).
- The following must be configured:
  - Discover storage devices
  - Add Resource Pools to be used for the Vault/Mirror storage provisioning

## CONFIGURATION

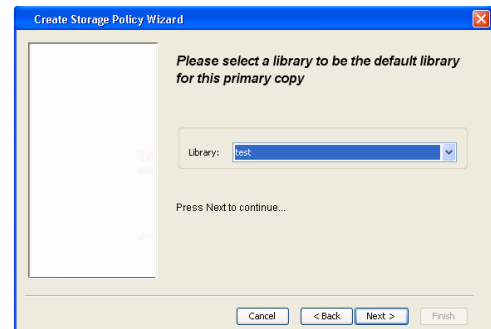
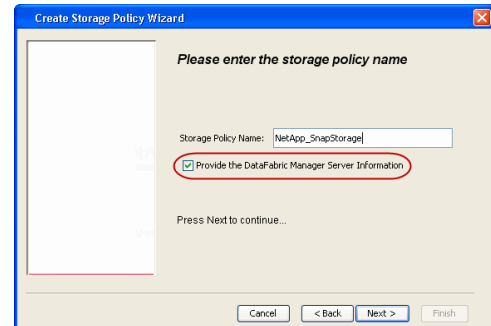
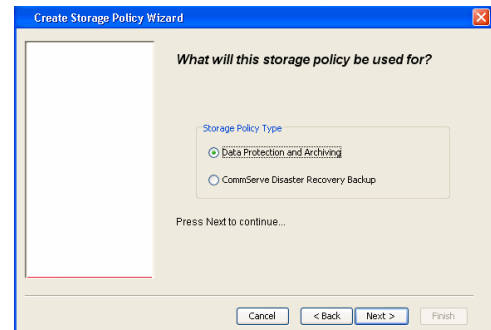
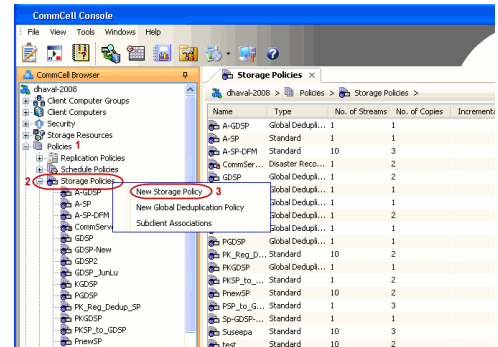
Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

## CREATE STORAGE POLICY

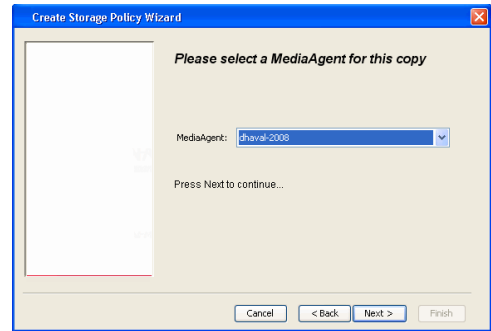
Use the following steps to create a storage policy.

1.
  - From the CommCell Browser, navigate to **Policies**.
  - Right-click the **Storage Policies** node and click **New Storage Policy**.
  
2. Click **Next**.
  
3.
  - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
  - Select **Provide the DataFabric Manager Server Information**.
  - Click **Next**.
  
4.
  - In the **Library** list, select the default library to which the Primary Copy should be associated.
 

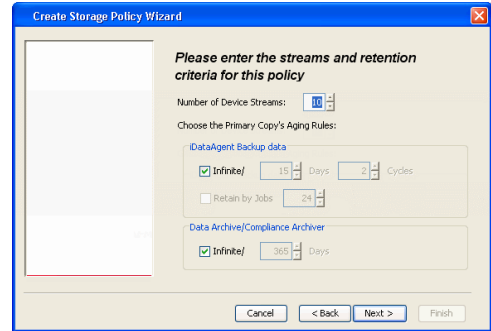
It is recommended that the selected disk library uses a LUN from the File server.
  - Click **Next**.
  
5.
  - Select a MediaAgent from the **MediaAgent** list.
  - Click **Next**.



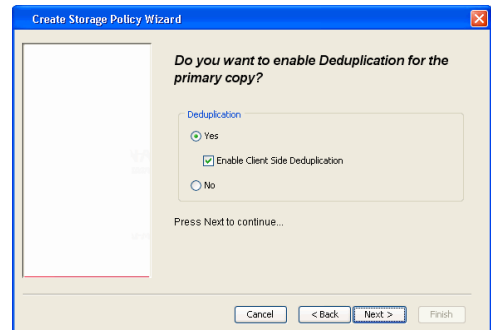
6. Click **Next**.



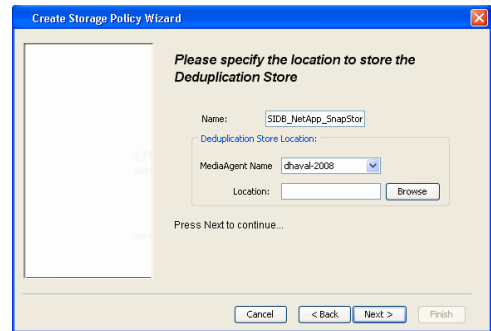
7. Click **Next**.



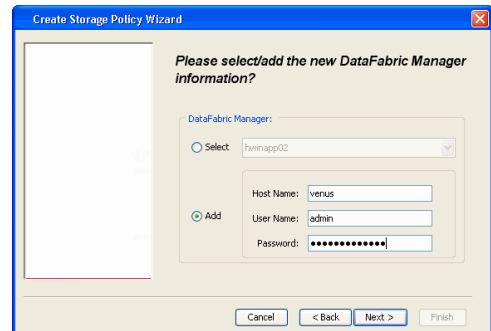
- 8.
- Verify **Name** and **MediaAgent Name**.
  - Click **Browse** to specify location for **Deduplication Store**.
  - Click **Next**.

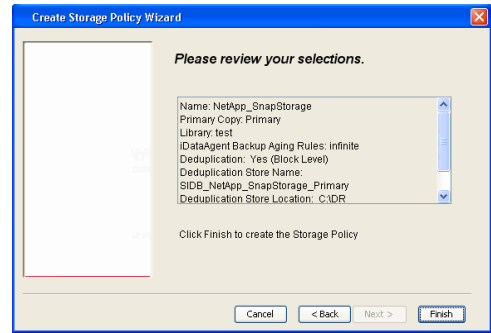


- 9.
- Provide the DataFabric Manager server information.
    - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
    - If you want to add a new DataFabric Manager Server, click **Add**.
  - Click **Next**.



10. Click **Finish**.



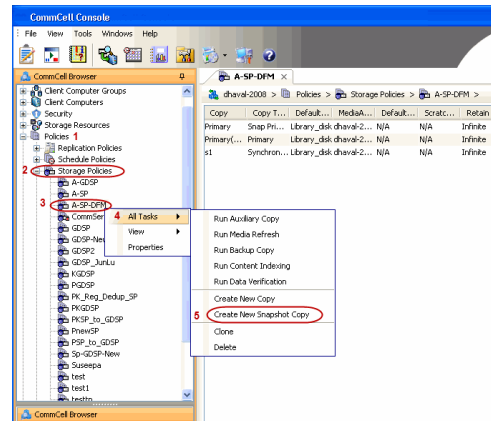


11. The new Storage Policy creates the following:
  - **Primary Snap Copy**, used for local snapshot storage
  - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

### CREATE A SECONDARY SNAPSHOT COPY

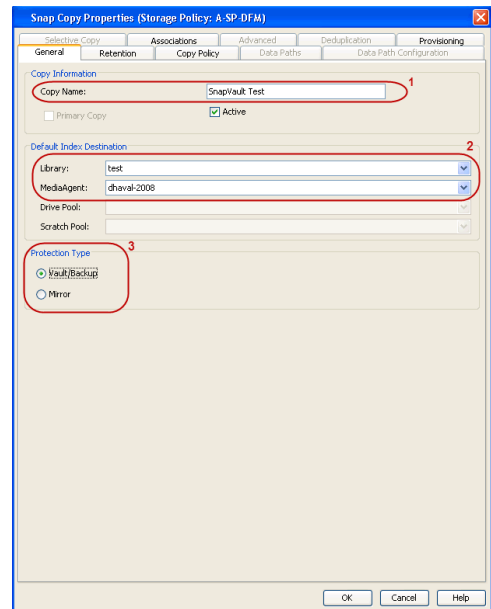
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
  - From the CommCell Browser, navigate to **Policies | Storage Policies**.
  - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
  - Enter the **Copy Name**.
  - Select the **Library** and **MediaAgent** from the drop-down list.
  - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

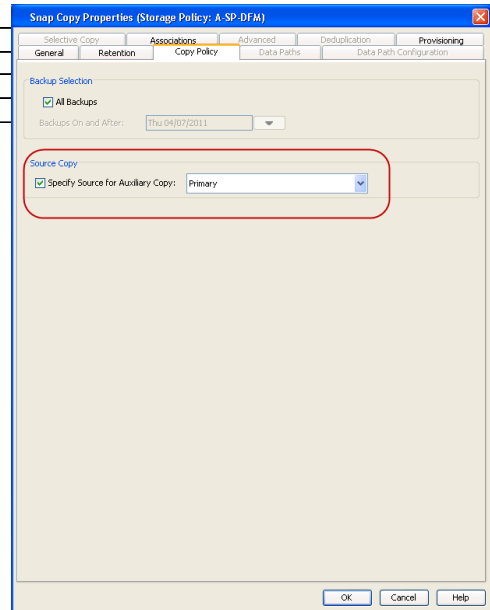


3.
  - Click the **Copy Policy** tab.
  - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

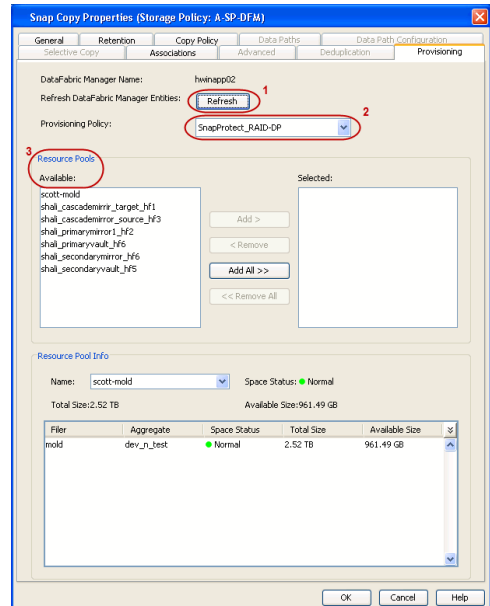
| TOPOLOGY | SOURCE COPY |
|----------|-------------|
|----------|-------------|

|                       |         |
|-----------------------|---------|
| Primary-Mirror        | Primary |
| Primary-Mirror-Vault  | Mirror  |
| Primary-Vault         | Primary |
| Primary-Vault-Mirror  | Vault   |
| Primary-Mirror-Mirror | Mirror  |



4.
  - Click the **Provisioning** tab.
  - Click **Refresh** to display the DFM entities.
  - Select the **Provisioning Policy** from the drop-down list.
  - Select the **Resource Pools** available from the list.
  - Click **OK**.

The secondary snapshot copy is created.



5. If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:
 

```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

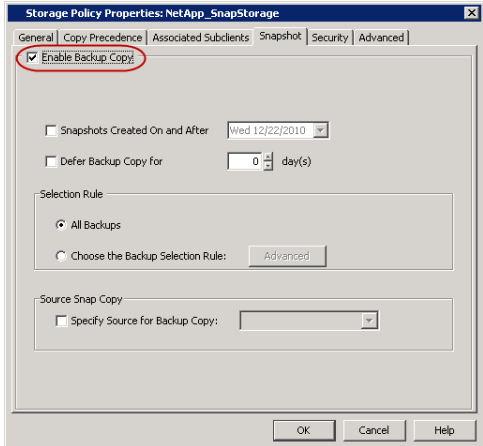
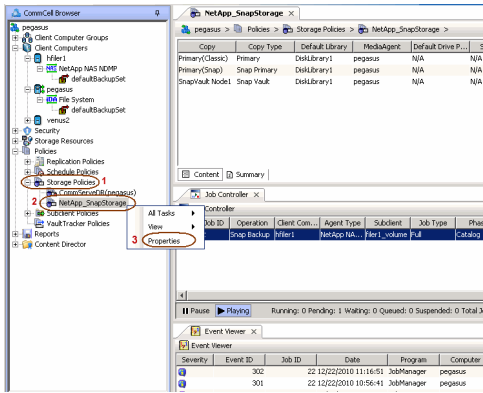
It is recommended that you perform this operation on all nodes in the P-M-V topology.

## CONFIGURE BACKUP COPY

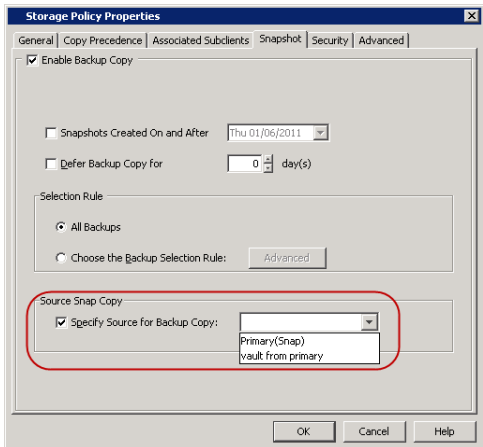
Follow the steps given below to configure Backup Copy for moving snapshots to media.

1.
  - From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.

2.
  - Click the **Snapshot** tab.
  - Select **Enable Backup Copy** option to enable movement of snapshots to media.
  - Click **OK**.



3.
  - Select **Specify Source for Backup Copy**.
  - From the drop-down list, select the source copy to be used for performing the backup copy operation.



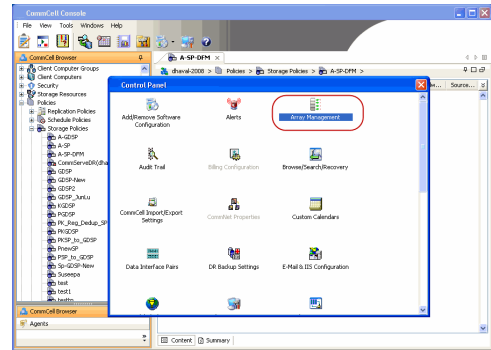
## SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

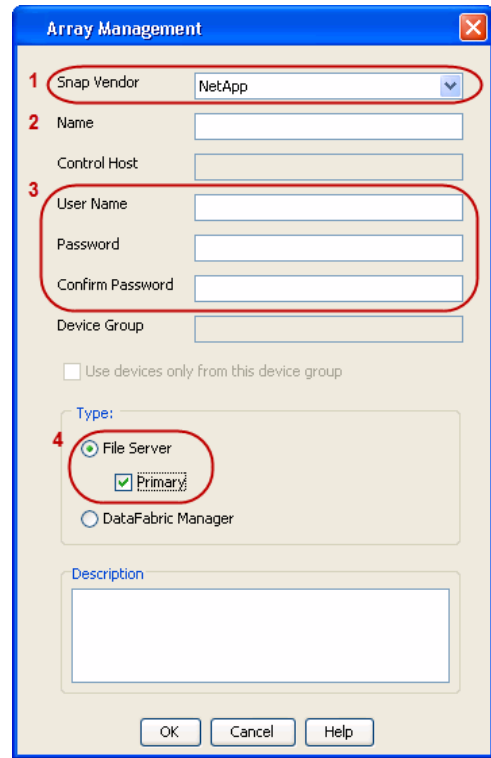
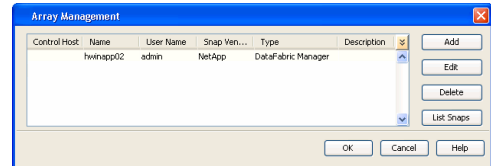


3.
  - Select **NetApp** from the **Snap Vendor** list.
  - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

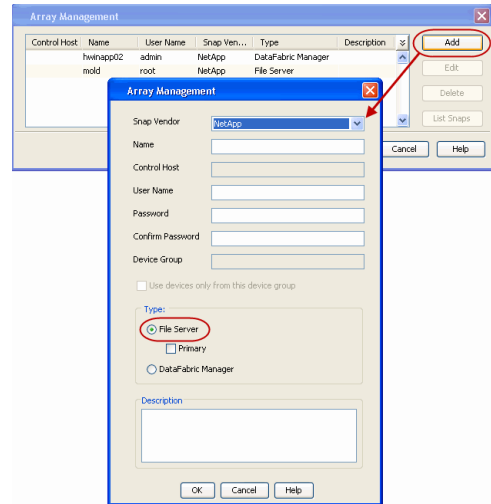
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



4.
  - Click **Add** again to enter the information for the secondary array.
  - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



## SEE ALSO

### Import Wizard Tool

Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

# SnapProtect™ Backup - Data Replicator

◀ Previous   Next ▶

## PRE-REQUISITES

### INSTALLATION

- The use of Data Replicator with the SnapProtect backup requires MediaAgent, File System iDataAgent, and ContinuousDataReplicator on the source, destination, and proxy computers.

The use of a proxy server to perform SnapProtect operations is supported when a hardware storage array is used for performing the SnapProtect backup.

- The operating system of the MediaAgent to be used for SnapProtect backup must be either the same or higher version than the source computer.

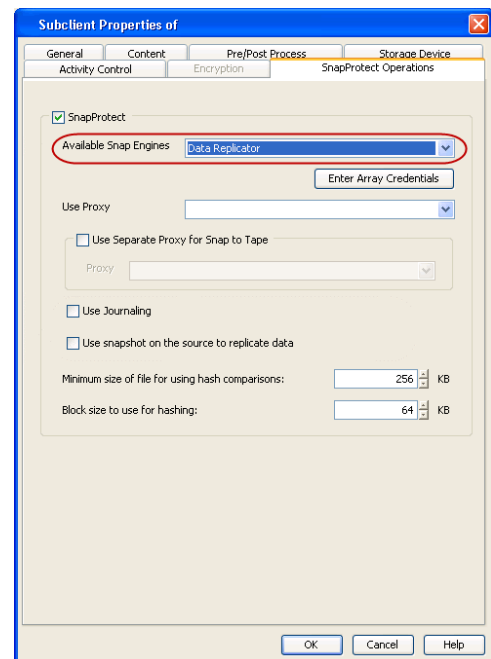
### STORAGE POLICY REQUIREMENTS

The Primary Snap Copy to be used for creating the snapshot copy must be a disk library.

If the Storage Policy or the disk library being used by the subclient is updated, the subclient should be recreated.

## SETUP THE ARRAY

- From the CommCell Console, navigate to <Client> | <Agent>.
  - Right-click the subclient and click **Properties**.
- Click the **SnapProtect Operations** tab.
  - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down list.
  - Click **OK**.



◀ Previous   Next ▶

# Getting Started - Linux File System Backup

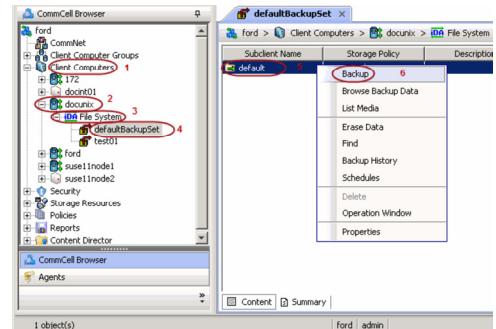
◀ Previous   Next ▶

## PERFORM A BACKUP

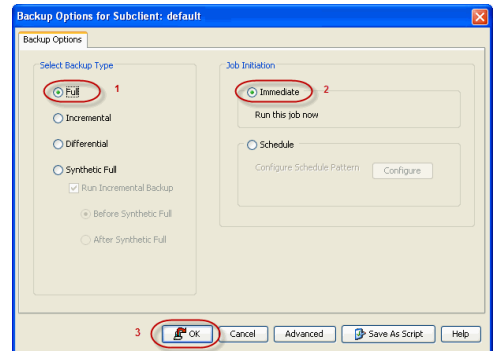
Once the storage policy is configured, you are ready to perform your first backup.

The following section provides step-by-step instructions for performing your first backup:

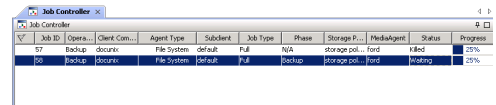
- From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.
  - Right-click the default subclient and click **Backup**.



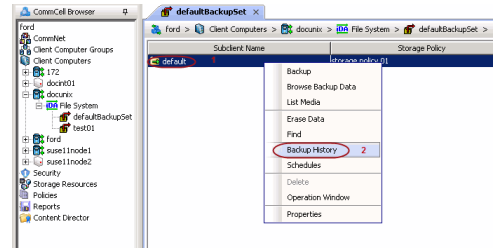
- Click **Full** as backup type and then click **Immediate**.
  - Click **OK**.



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



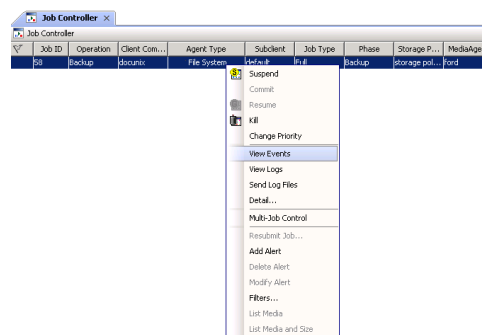
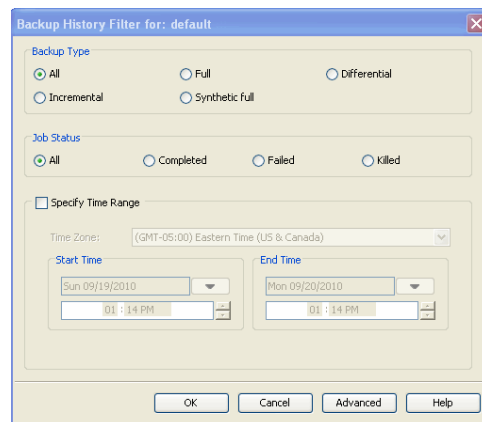
- Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.



- Click **OK**.

6. You can view the following details about the job by right-clicking the job:

- Items that failed during the job
- Items that succeeded during the job
- Details of the job
- Events of the job
- Log files of the job
- Media associated with the job



# Getting Started - Vault/Mirror Copy

◀ Previous   Next ▶

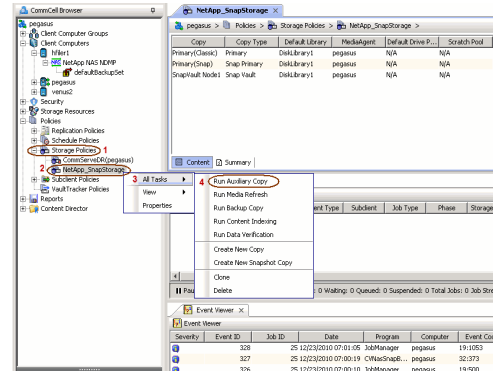
## SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

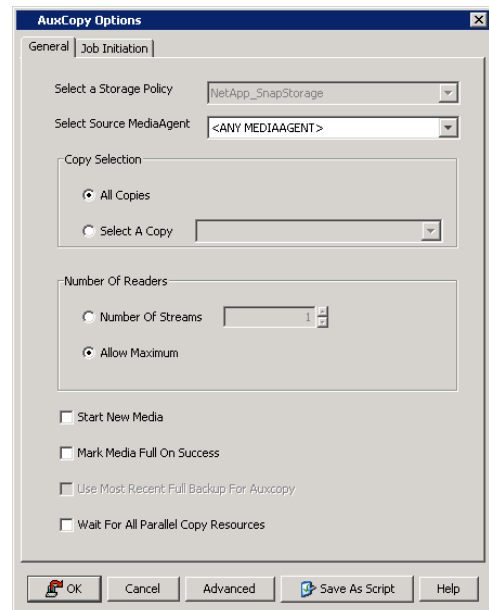
### INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

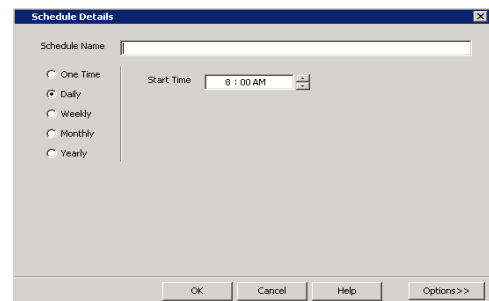


- Select the desired options and click the **Job Initiation** tab.
  - Select **Schedule** to configure the schedule pattern and click **Configure**.



- Enter the schedule name and select the appropriate scheduling options.
  - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.

◀ Previous   Next ▶

# Getting Started - Snap Movement to Media

◀ Previous   Next ▶

## SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

### BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

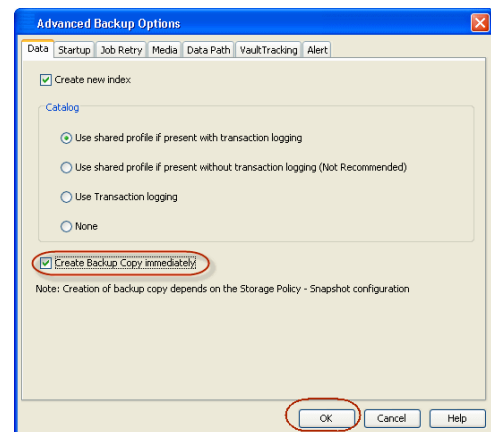
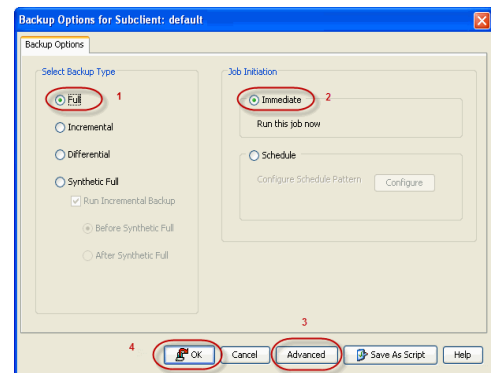
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

#### INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

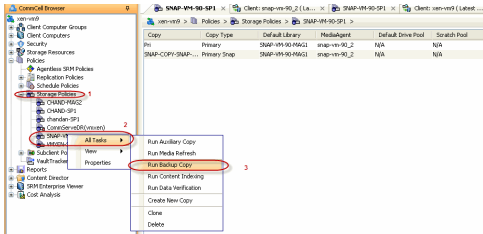
1.
  - From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
  - Right click the default subclient and click **Backup**.
  - Select **Full** as backup type.
  - Click **Advanced**.
  
2.
  - Select **Create Backup Copy immediately** to create a backup copy.
  - Click **OK**.



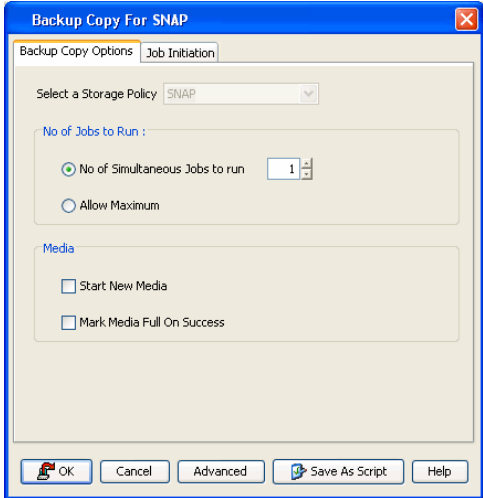
#### OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

1.
  - From the CommCell Console, navigate to **Policies** | **Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.





# Getting Started - Unix File System Restore



## PERFORM A RESTORE

As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring the backup data.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.
  - Click the **Copy Precedence** tab.
  - By default, the snapshot copy is set to 1 and is used for the operation.

You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.

- Click **OK**.

- From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.
  - Right-click the default subclient and then click **Browse Backup Data**.

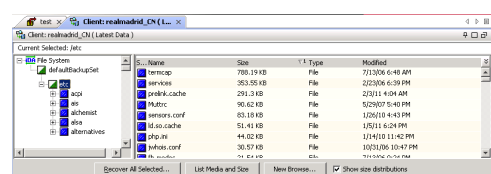
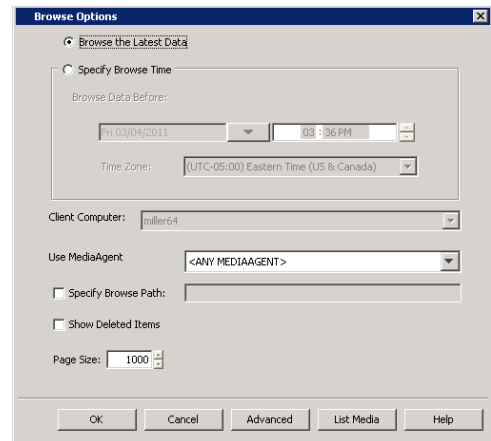
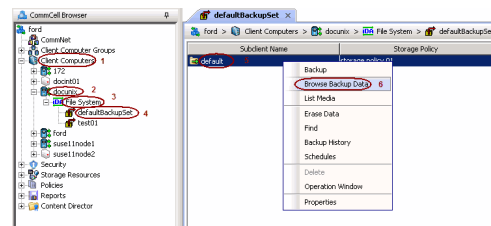
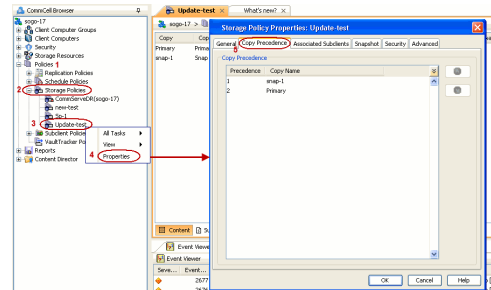
- Click **OK**.

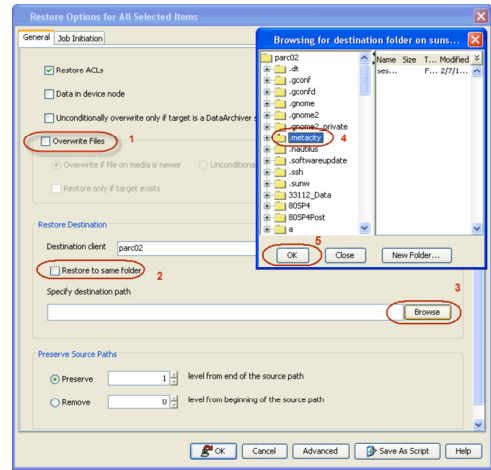
- Expand the **defaultBackupSet** and navigate to **etc** folder.
  - Select the **etc** folder.
  - Click **Recover All Selected**.

If you attempt to restore a running executable file, the application may crash and core dump.

- Clear the **Overwrite Files** and **Restore to same folder** options.
  - Specify the destination path by clicking **Browse** button.
  - This will ensure that the existing files are not overwritten.
  - Click **OK**.

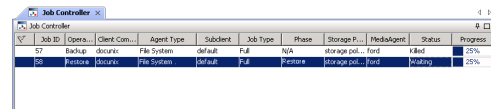
Restored data retains its original permissions. The ACLs are restored after the permissions are restored. Do not restore ACLs to any directory that has the "sticky bit" on.





6. You can monitor the progress of the restore job in the **Job Controller**.

7. Once the File System is restored, verify that the restored files/folders are available in the restore destination

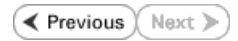


```
[parc02] # ls /.metacity
etc
```

**CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.**

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



# Getting Started - Windows File System Deployment

◀ Previous   Next ▶

## WHERE TO INSTALL

Install the software on a client computer that you want to protect.

## BEFORE YOU BEGIN

### Download Software Packages

Download the latest software package to perform the install.

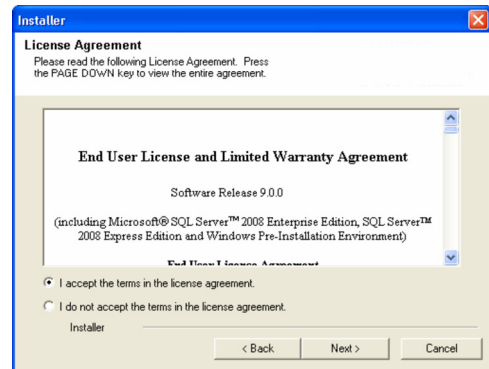
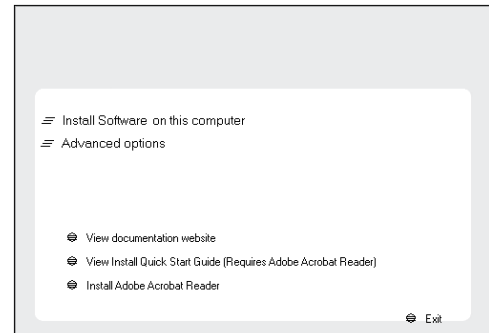
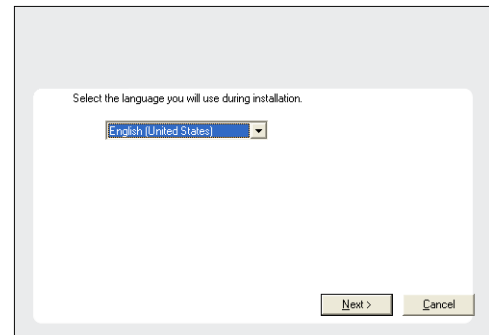
### SnapProtect Support - Platforms

Make sure that the computer in which you wish to install the software satisfies the minimum requirements.

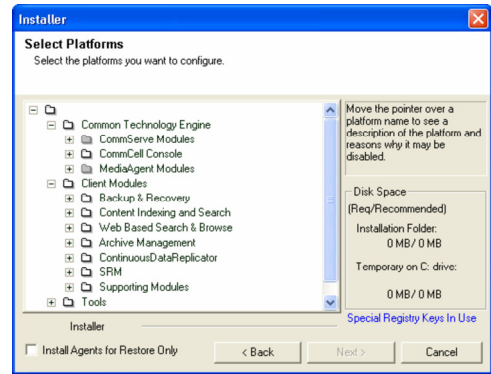
## INSTALL THE WINDOWS FILE SYSTEM iDATAAGENT

Use the following procedure to directly install the software from the installation package or a network drive.

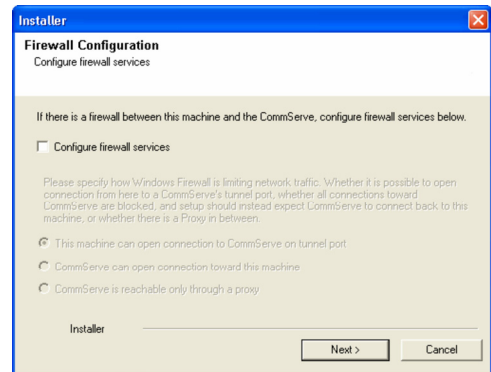
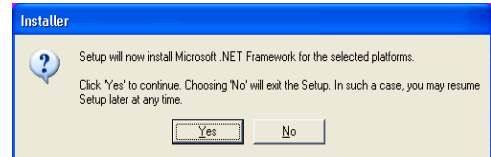
1. Run **Setup.exe** from the **Software Installation Package**.
2. Select the required language.  
Click **Next**.
3. Select the option to install software on this computer.  
  
The options that appear on this screen depend on the computer in which the software is being installed.
4. Select **I accept the terms in the license agreement**.  
Click **Next**.
5.
  - Expand **Client Modules | Backup & Recovery | File System** and select **Windows File System iDataAgent**.
  - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
  - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
  - Click **Next**.



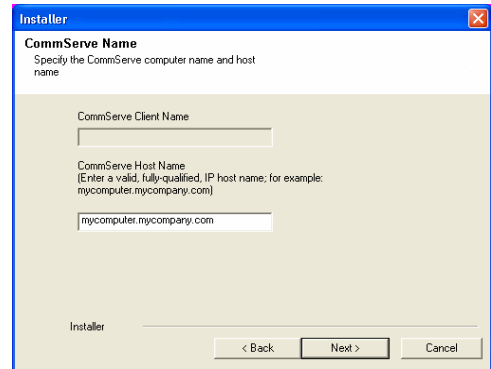
6. Click **YES** to install Microsoft .NET Framework package.
  - This prompt is displayed only when Microsoft .NET Framework is not installed.
  - Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.
7. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.  
 For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.  
 If firewall configuration is not required, click **Next**.



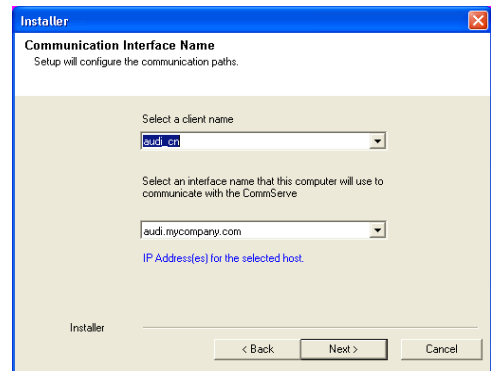
8. Enter the fully qualified domain name of the **CommServe Host Name**.  
 Click **Next**.  
 Do not use space and the following characters when specifying a new name for the CommServe Host Name:  
`\ | ` ~ ! @ # $ % ^ & * ( ) + = < > / ? , [ ] { } ; : ; " ' " "`



9. Click **Next**.



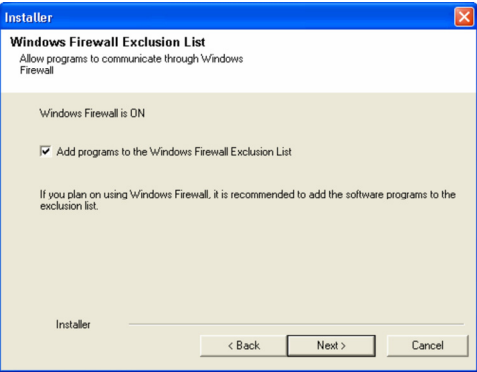
10. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.



Click **Next**.

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

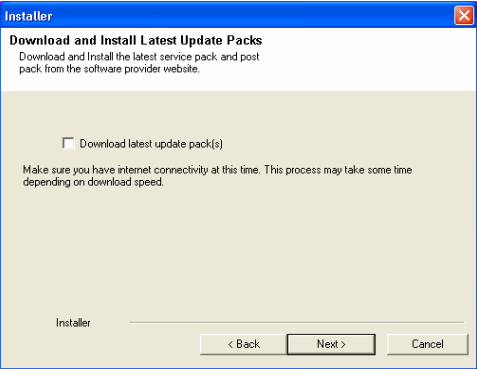
It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.



11. Click **Next**.

**NOTES**

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



12. Verify the default location for software installation.

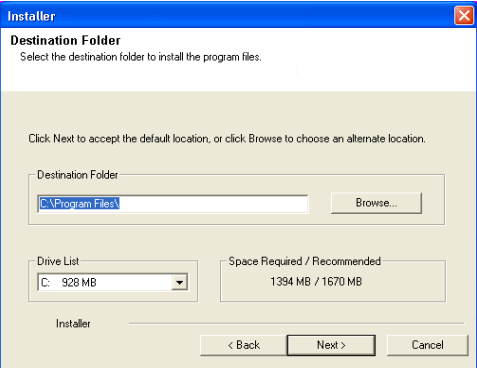
Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not install the software on a system drive or mount point that will be used as content for SnapProtect backup operations.
- Do not use the following characters when specifying the destination path:

/ : \* ? " < > | #

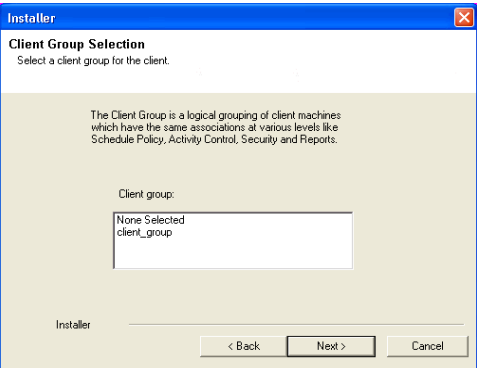
It is recommended that you use alphanumeric characters only.



13. Select a Client Group from the list.

Click **Next**.

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



14. Click **Next**.

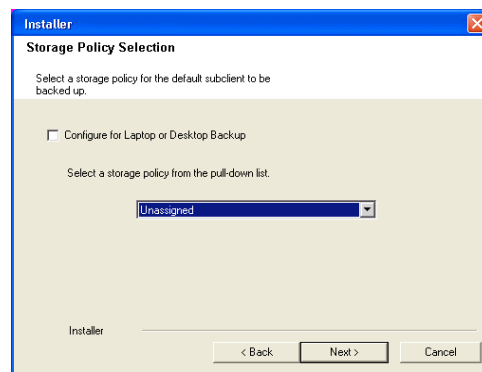
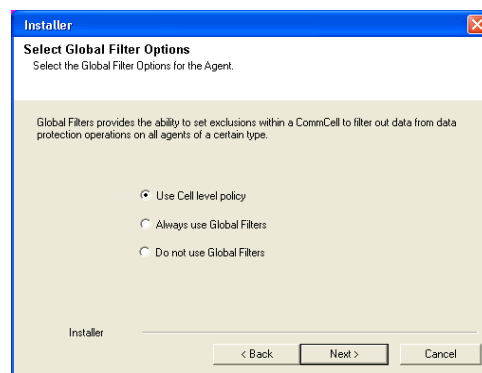
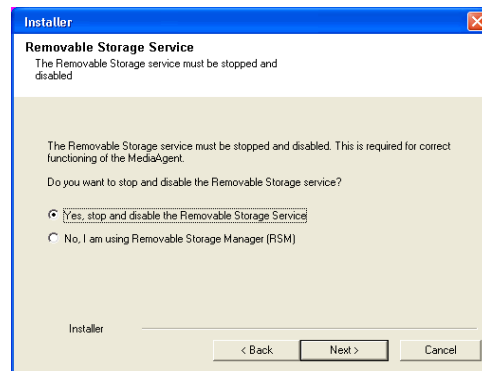
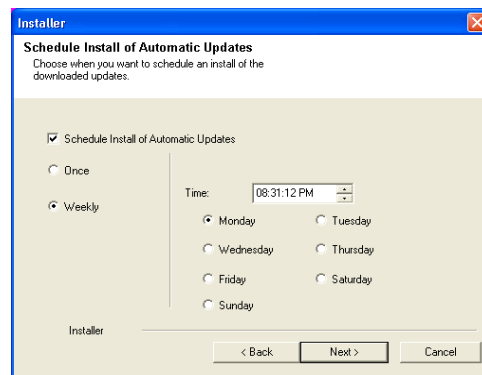
15. Select **Yes** to stop Removable Storage Services on the MediaAgent.  
Click **Next**.

This prompt will not appear if Removable Storage Services are already disabled on the computer.

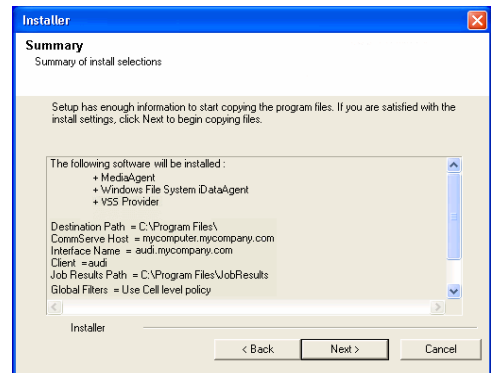
16. Click **Next**.

17. Select a **Storage Policy**.  
Click **Next**.

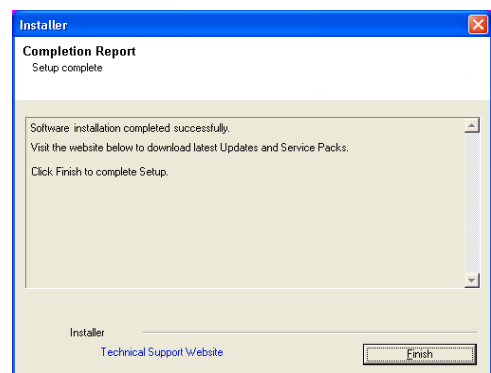
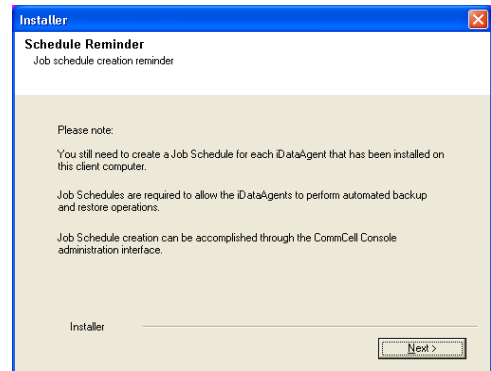
18. Click **Next**.



19. Click **Next**.



20. Click **Finish**.



# Getting Started - Windows File System Configuration

◀ Previous Next ▶

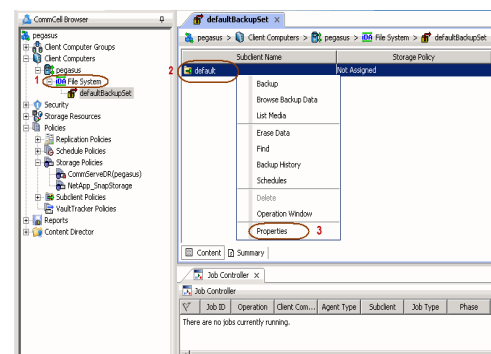
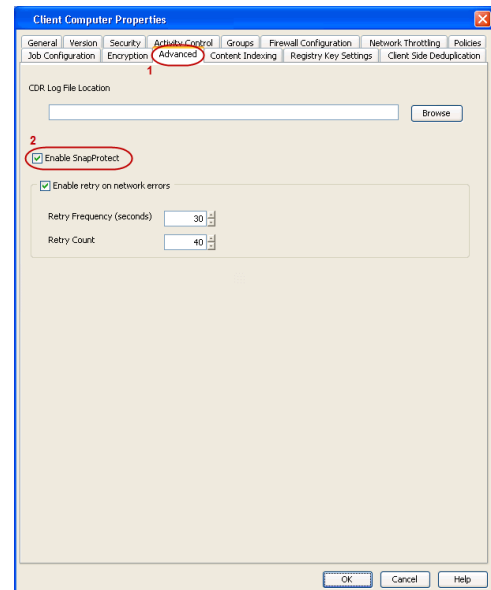
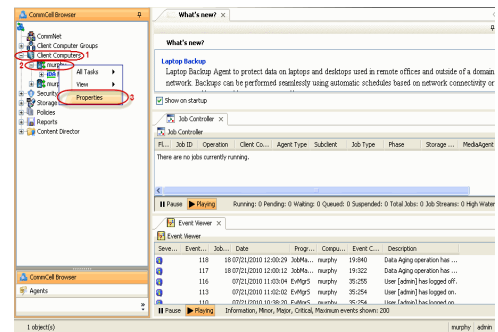
## PRE-REQUISITES

- Prior to performing a SnapProtect backup, ensure that all the available hotfixes for Virtual Disk Service (VDS) and VSS are applied.
- When performing SnapProtect backup for a Windows Cluster, a proxy server must be used for performing backup and restore operations.
- SnapProtect backup on Windows supports basic disks.

## CONFIGURATION

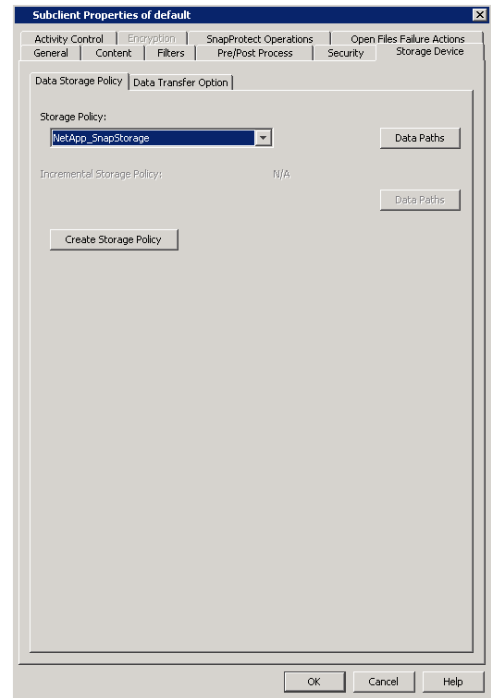
Once installed, the Windows File System *FileAgent* requires some additional configuration before running your first SnapProtect backup. Follow the steps given below to complete the configuration for this Agent.

- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
  - Right-click the client and select **Properties**.
- Click on the **Advanced** tab.
  - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
  - Click **OK**.
- From the CommCell Console, navigate to **<Client>** | **File System**.
  - Right-click the subclient and click **Properties**.
- Click the **Storage Device** tab.





- In the **Storage Policy** box, select the storage policy name.

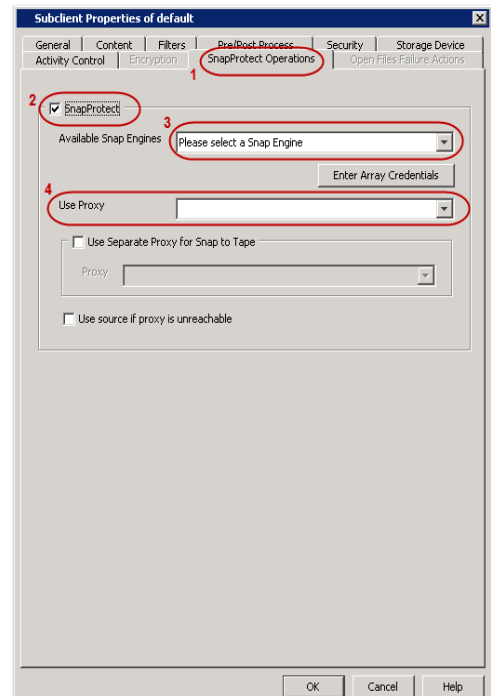


- 5.
- Click the **SnapProtect Operations** tab.
  - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
  - Select the storage array from the **Available Snap Engine** drop-down list.
  - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy operations will be performed.

When performing SnapProtect backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

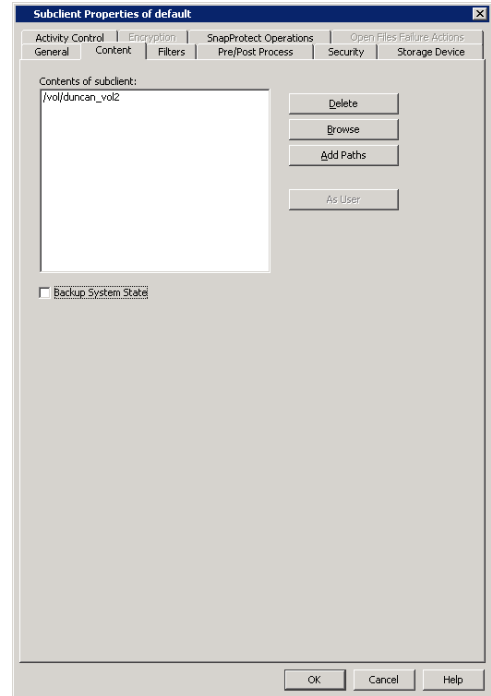
- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent.

Select the MediaAgent from the **Proxy** list.



- 6.
- Click the **Content** tab.
  - Click **Browse** and specify the content for the subclient.
  - Click **OK**.

The subclient content must contain data that resides on the storage device volume; do not include local drives or UNC paths as subclient content.



## SKIP THIS SECTION IF YOU ALREADY CREATED A SNAPSHOT COPY.

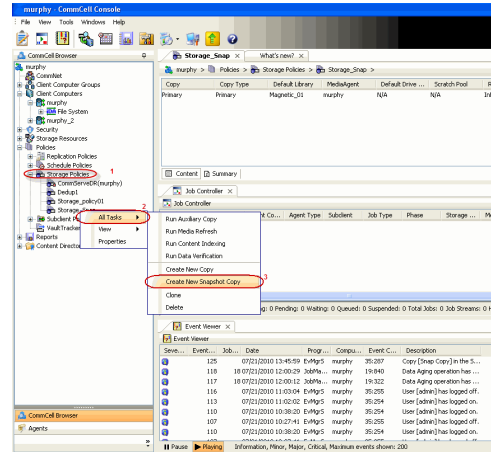
Click **Next** to Continue.

### CREATE A SNAPSHOT COPY

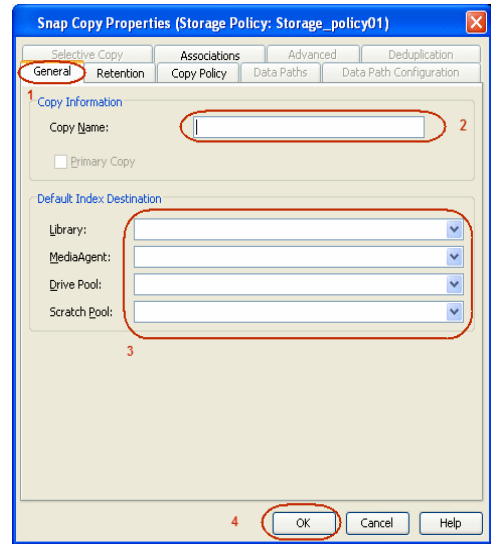


Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

1.
  - From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.



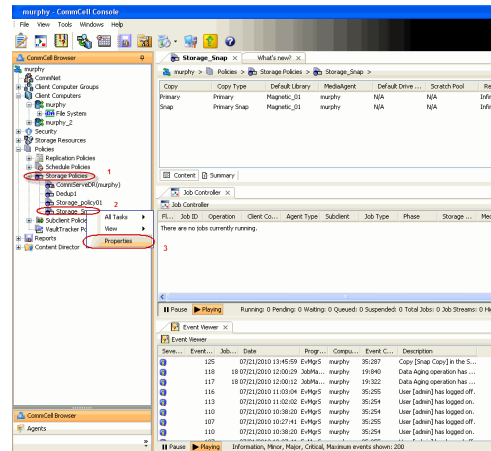
2.
  - Enter the copy name in the **Copy Name** field.
  - Select the **Library, MediaAgent, master Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
  - Click **OK**.



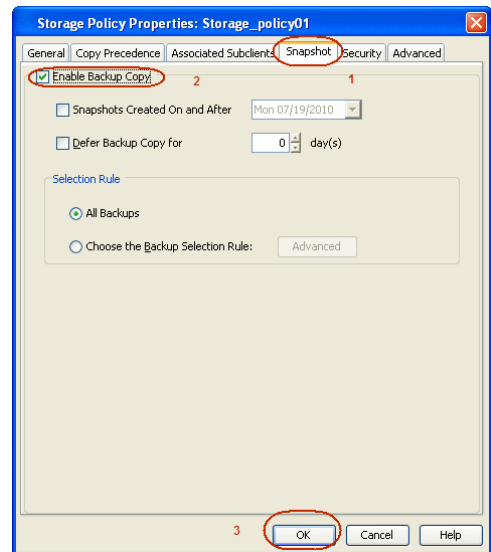
## CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

1.
  - From the CommCell Browser, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.



2.
  - Click the **Snapshot** tab.
  - Select **Enable Backup Copy** option to enable movement of snapshots to media.
  - Click **OK**.



# Storage Array Configuration

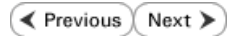
◀ Previous Next ▶

## CHOOSE THE STORAGE ARRAY

| HARDWARE STORAGE ARRAYS          | SOFTWARE STORAGE ARRAY |
|----------------------------------|------------------------|
| 3PAR                             | DATA REPLICATOR        |
| DELL COMPELLENT                  |                        |
| DELL EQUALLOGIC                  |                        |
| EMC CLARIION, VNX                |                        |
| EMC SYMMETRIX                    |                        |
| FUJITSU ETERNUS DX               |                        |
| HITACHI DATA SYSTEMS             |                        |
| HP EVA                           |                        |
| IBM SVC                          |                        |
| IBM XIV                          |                        |
| LSI                              |                        |
| NETAPP                           |                        |
| NETAPP WITH SNAPVAULT/SNAPMIRROR |                        |
| NIMBLE                           |                        |

◀ Previous Next ▶

# SnapProtect™ Backup - 3PAR



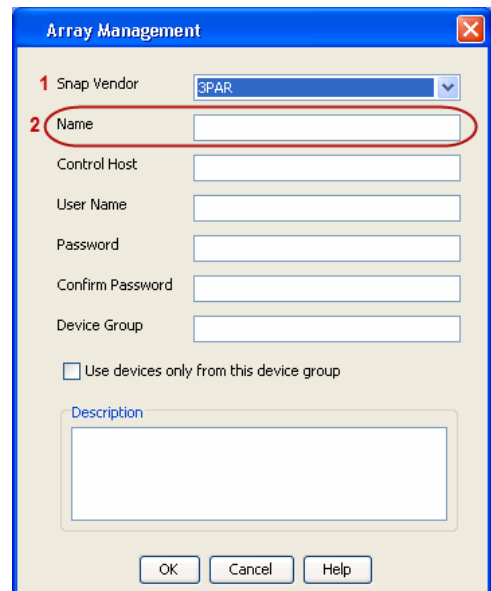
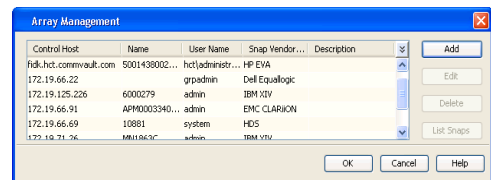
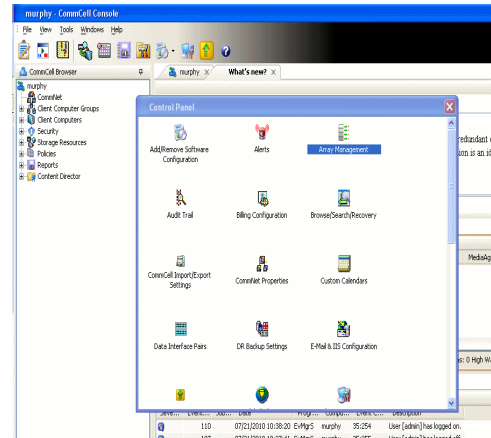
## PRE-REQUISITES

- 3PAR Snap and 3PAR Clone licenses.
- Thin Provisioning (4096G) and Virtual Copy licenses.
- Ensure that all members in the 3PAR array are running firmware version 2.3.1 (MU4) or higher.

## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **3PAR** from the **Snap Vendor** list.
  - Specify the 16-digit number obtained from the device ID of a 3PAR volume in the **Name** field.



Follow the steps given below to calculate the array name for the 3PAR storage device:

1. From the 3PAR Management console, click the **Provisioning** tab and navigate to the **Virtual Volumes** node. Click any volume in the **Provisioning** window
2. From the **Virtual Volume Details** section, click the **Summary** tab and write

down the **WWN** number. This is the device ID of the selected volume.

- From the **Virtual Volume Details** section, click the **Summary** tab and write down the **WWN** number.

This is the device ID of the selected volume.

This WWN may be 8-Byte number (having 16 Hex digits) or 16 Byte number (having 32 Hex digits).

- Use the following formula to calculate the array name:

- For 8 Byte WWN (16 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

where  $\text{DevID.substr}(4,3)$  is the next 3 digits after the fourth digit from the WWN number

where  $\text{DevID.substr}(12,4)$  is the next 4 digits after the twelfth digit from the WWN number

For example: if the WWN number is 50002AC0012B0B95 (see screenshot given below for 8 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + 00 + \text{DevID.substr}(12,4)$$

$\text{DevID.substr}(4,3)$  is 2AC and  $\text{DevID.substr}(12,4)$  is 0B95

After adding all the values, the resulting array name is 2FF70002AC000B95.

- For 16 Byte WWN (32 Hex digit WWN)

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

where  $\text{DevID.substr}(4,3)$  is the next 3 digits after the fourth digit from the WWN number

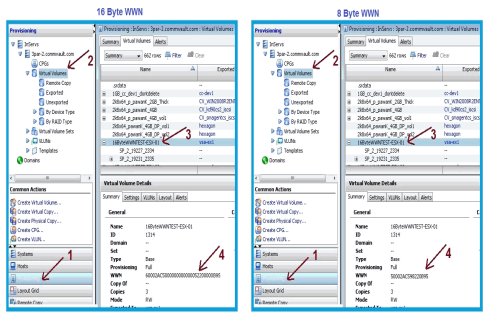
where  $\text{DevID.substr}(26,6)$  is the next 6 digits after the twenty sixth digit from the WWN number

For example: if the WWN number is 60002AC5000000000000052200000B95 (see screenshot given below for 16 Byte WWN), using the following formula:

$$2FF7000 + \text{DevID.substr}(4,3) + \text{DevID.substr}(26,6)$$

$\text{DevID.substr}(4,3)$  is 2AC and  $\text{DevID.substr}(26,6)$  is 000B95

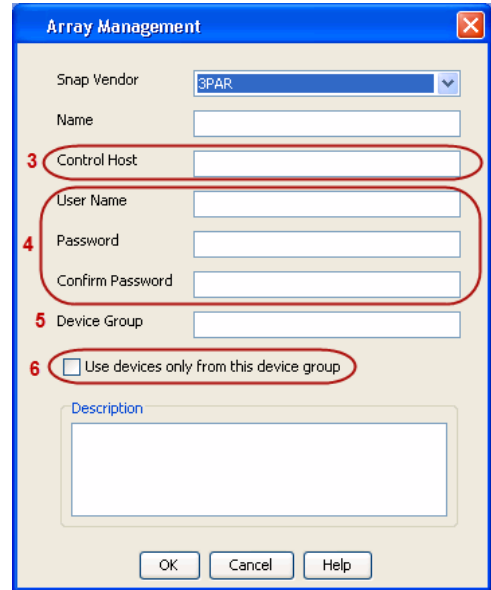
After adding all the values, the resulting array name is 2FF70002AC000B95.



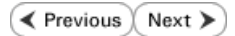
- Enter the IP address of the array in the **Control Host** field.
  - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the CPG group created on the array to be used for snapshot operations.

If you do not specify a CPG group, the default CPG group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - Dell Compellent



## PRE-REQUISITIES

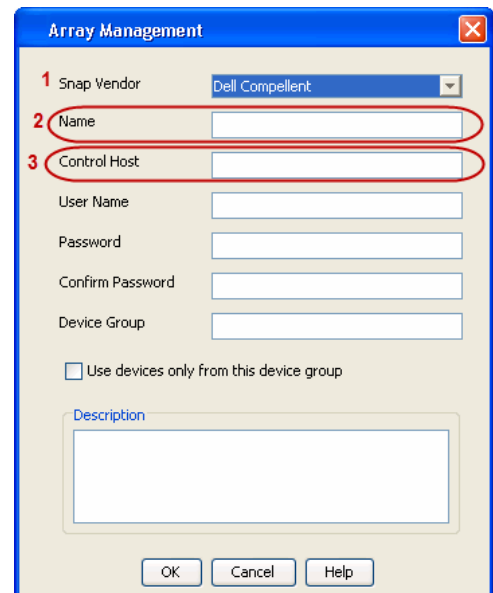
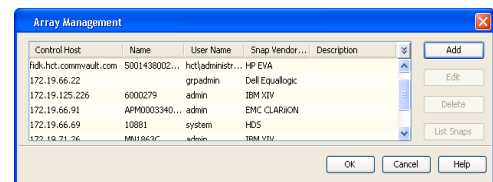
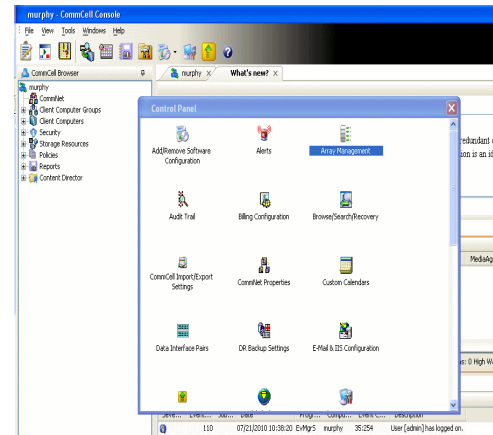
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

## SETUP THE ARRAY INFORMATION

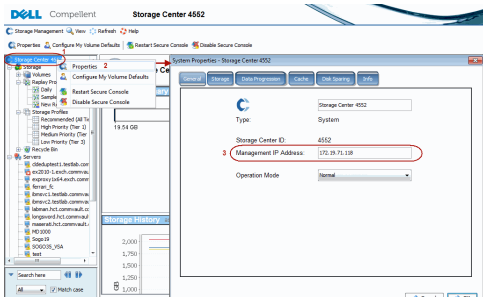
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **Dell Compellent** from the **Snap Vendor** list.
  - Specify the Management IP address in the **Name** and **Control Host** fields.

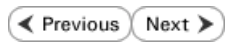
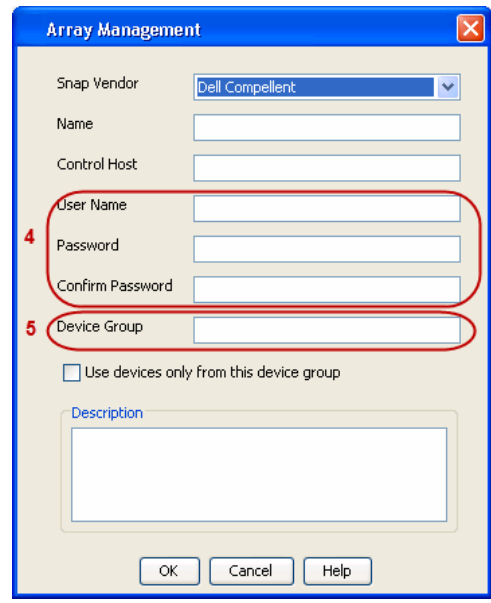
The Management IP address is also referred as the Storage Center IP address.



For reference purposes, the screenshot on the right shows the Storage Center Management Console of the Dell Compellent storage device displaying the Management IP address.

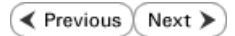


- 4.
- Enter the user access information of the application administrator in the **Username** and **Password** fields.
  - In the **Device Group** field, type *none* as this array does not use device groups for snapshot operations.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.





# SnapProtect™ Backup - Dell EqualLogic



## PRE-REQUISITIES

### WINDOWS

Microsoft iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

### UNIX

iSCSI Initiator to be configured on the client and proxy computers to access the Dell EqualLogic disk array.

### FIRMWARE VERSION

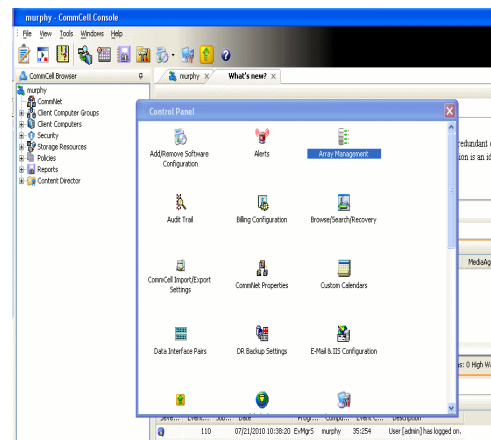
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
  - Create a new group administration account in the firmware, and set the desired permissions for this account.
  - If you plan to use the existing administration accounts from version prior to 4.2.0, reset the password for these accounts. The password can be the same as the original.

If you do not reset the password, snapshot creation will fail.

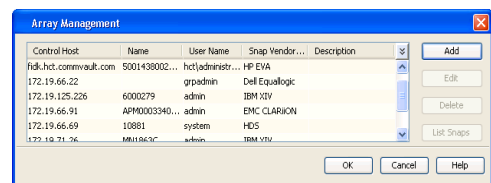
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



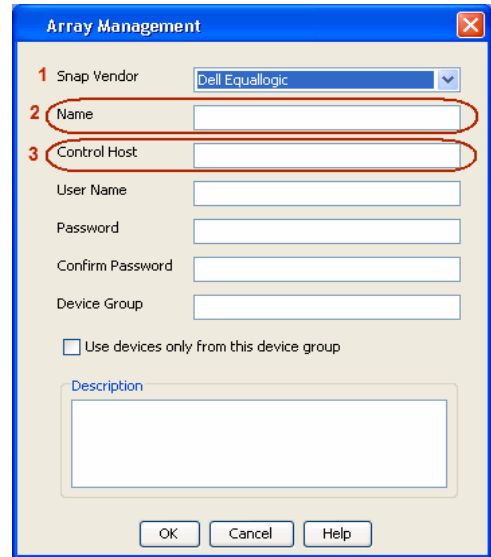
2. Click **Add**.



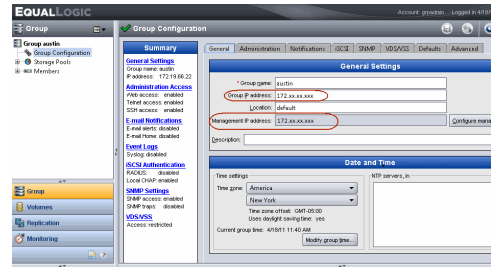
3.
  - Select **Dell Equallogic** from the **Snap Vendor** list.
  - Specify the Management IP address in the **Name** field.

No entry is required in the **Name** field if there is no Management IP address configured.

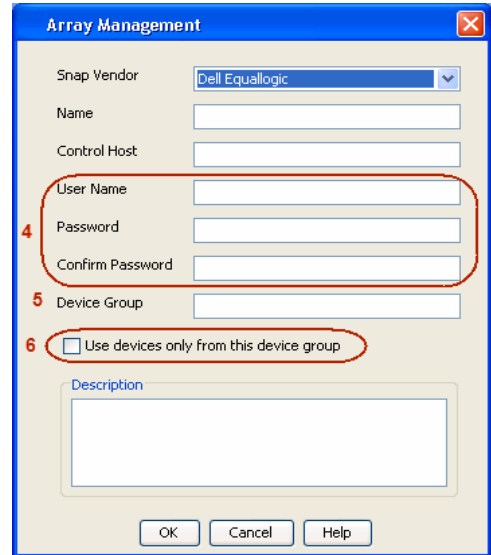
- Specify the Group IP address in the **Control Host** field.



For reference purposes, the screenshot on the right shows the Management IP address and Group IP address for the Dell Equallogic storage device.



4.
  - Enter the user access information of the Group Administrator user in the **Username** and **Password** fields.
  - For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones in the **Device Group** field.
  - Select the **Use devices only from this device group** option to use only the snapshot devices available in the storage pool specified above.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.



# SnapProtect™ Backup - EMC Clariion, VNX

◀ Previous    Next ▶

## PRE-REQUISITES

### LICENSES

- Clariion SnapView and AccessLogix licenses for Snap and Clone.
- SYMAPI Feature: BASE/Symmetrix license required to discover Clariion storage systems.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

### ARRAY SOFTWARE

- EMC Solutions Enabler (6.5.1 or higher) installed on the client and proxy computers.  
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and NaviAgent installed on the client and proxy computers.
- If AccessLogix is not enabled, go to the Navisphere GUI, right-click **EMC Clariion Storage System** and click Properties. From the **Data Access** tab, select **Enable AccessLogix**.
- Clariion storage system should have run successfully through the Navisphere Storage-System Initialization Utility prior to running any Navisphere functionality.
- Ensure enough reserved volumes are configured for SnapView/Snap to work properly.

For EMC VNX:

- EMC Solutions Enabler (7.2 or higher) installed on the client and proxy computers.  
Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
- Navisphere CLI and Navisphere/Unisphere Host Agent installed on the client and proxy computers.
- VNX storage system should have run successfully through the Unisphere Storage-System Initialization Utility prior to running any Unisphere functionality.

## SETUP THE EMC CLARIION

Perform the following steps to provide the required storage for SnapProtect operations:

1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

For example, as shown in the image on the right, the **Clariion ID** of **APM00033400899** has the following configuration:

- a **RAID Group 0** provisioned as a RAID-5 group (Fiber Channel drives)
- LUNs are mapped to Storage Group **SG\_EMCSnapInt1** with LUN ID of **#154** present to client computer **emcsnapint1**.

The example shows the serial number of LUN 154:

- **RAID Group:** RAID Group 0, containing 3 physical disks
- **Storage Group:** currently visible to a single client computer
- LUN is shown as a Fiber Channel device
- The devices under LUN 154 reside on RAID Group 0 which has RAID-5 configuration.



## AUTHENTICATE CALYPSO USER INFORMATION FOR THE NAVIAGENT

Follow the steps below to specify the authorization information for EMC Solutions Enabler and Navisphere CLI to ensure administrator access to the Navisphere server.

1. To set the authorize information, run the `symcfg` authorization command for both the storage processors. For example:

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPA IP> -username admin -password password
```

```
/opt/emc/SYMCLI/V6.5.3/bin# ./symcfg authorization add -host <clariion SPB IP> -username admin -password password
```

2. Run the following command to ensure that the Clariion database is successfully loaded.

```
symcfg discover -clariion -file AsstDiscoFile
```

where `AsstDiscoFile` is the fully qualified path of a user-created file containing the host name or IP address of each targeted Clariion array. This file should contain one array per line.

3. Create a Navisphere user account on the storage system. For example:

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPA IP> -Scope 0 -User admin -Password password
```

```
/opt/Navisphere/bin# ./naviseccli -AddUserSecurity -Address <clariion SPB IP> -Scope 0 -User admin -Password password
```

4. Restart the NaviAgent service.
5. Run `snapview` command from the command line to ensure that the setup is ready.

On Unix computers, you might need to add the Calypso user to the `agent.config` file.

Before running any commands ensure that the EMC commands are verified against EMC documentation for a particular product and version.

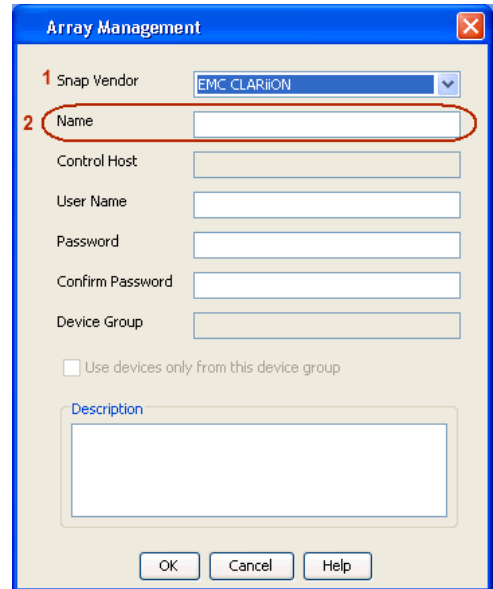
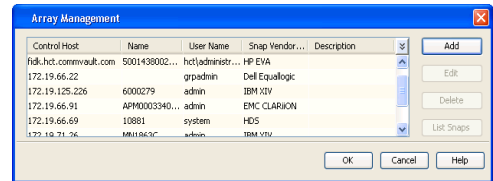
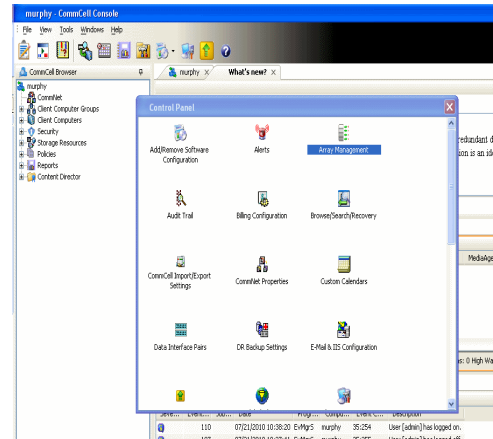
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

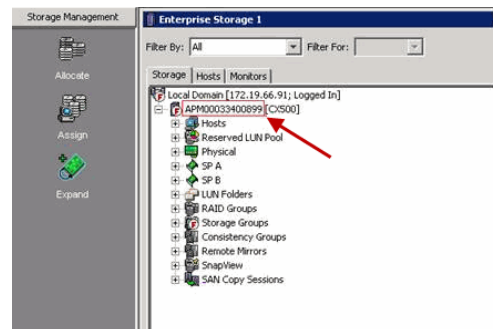
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

2. Click **Add**.

- 3.
- Select **EMC CLARiiON** from the **Snap Vendor** list for both Clariion and VNX arrays.
  - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the EMC Clariion storage device.



- 4.
- Enter the access information of a Navisphere user with administrative privileges in the **Username** and **Password** fields.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.

**Array Management** [Close]

Snap Vendor:

Name:

Control Host:

User Name:

**3** Password:

Confirm Password:

Device Group:

Use devices only from this device group

Description:

OK Cancel Help

◀ Previous Next ▶

# SnapProtect™ Backup - EMC Symmetrix

◀ Previous    Next ▶

## PRE-REQUISITES

- EMC Solutions Enabler (6.4 or higher) installed on the client and proxy computers.

Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.

- SYMAPI Feature: BASE /Symmetrix licenses for Snap, Mirror and Clone.

You can use the following command to check the licenses on the host computer:

```
C:\SYMAPI\Config> type symapi_licenses.dat
```

- By default, all functionality is already enabled in the EMC Symmetrix hardware layer. However, a Hardware Configuration File (IMPL) must be enabled before using the array. Contact an EMC Representative to ensure TimeFinder and SRDF functionalities have been configured.

## SETUP THE EMC SYMMETRIX

For SnapProtect to function appropriately, LUN Masking records/views must be visible from the host where the backup will take place:

- For DMX, the Masking and Mapping record for vcmdb must be accessible on the host executing the backup.
- For VMAX, the Masking view must be created for the host executing the backup.

## CONFIGURE SYMMETRIX GATEKEEPERS

Gatekeepers need to be defined on all MediaAgents in order to allow the Symmetrix API to communicate with the array. Use the following command on each MediaAgent computer:

```
symgate define -sid <Symmetrix array ID> dev <Symmetrix device name>
```

where <Symmetrix device name> is a numbered and un-formatted Symmetrix device (e.g., 00C) which has the MPIO policy set as `FAILOVER` in the MPIO properties of the gatekeeper device.

## LOAD THE SYMMETRIX DATABASE

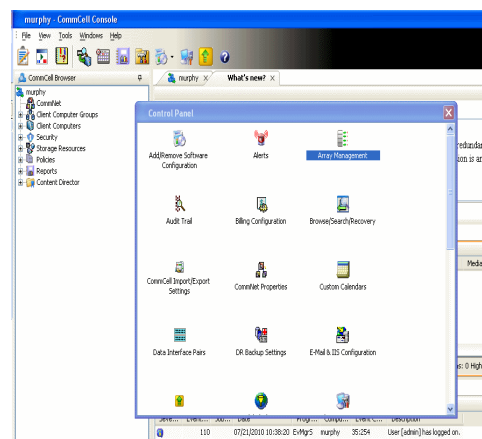
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

## SETUP THE ARRAY INFORMATION

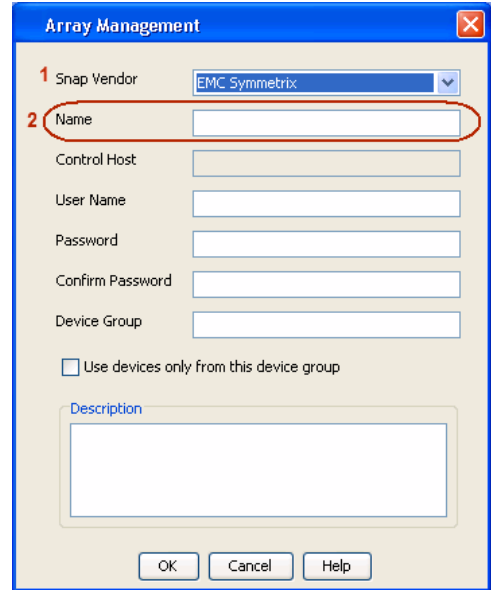
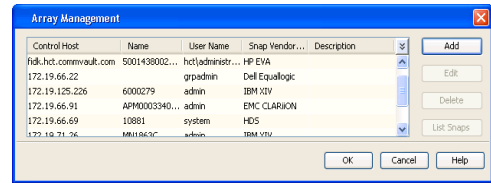
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

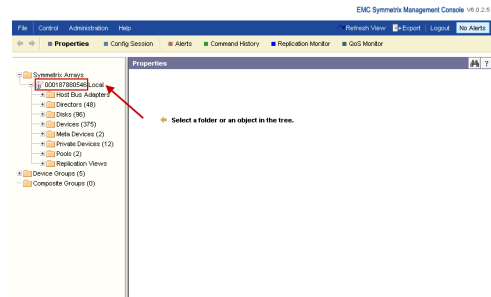


- Click **Add**.

3.
  - Select **EMC Symmetrix** from the **Snap Vendor** list.
  - Specify the **Symm ID** of the array in the **Name** field.

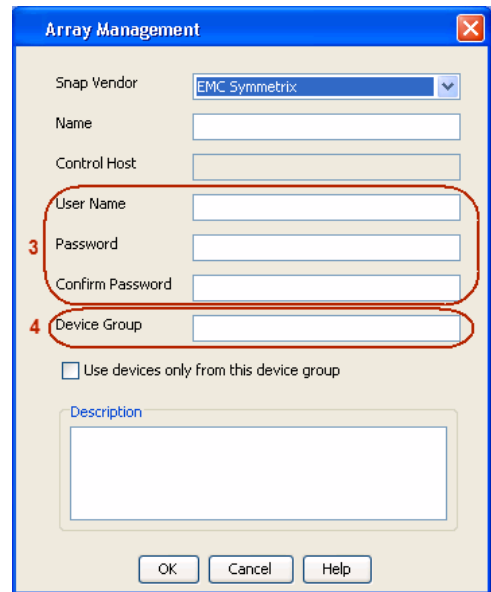


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



4.
  - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. The use of Group Name Service (GNS) is supported.  
If you do not specify a device group, the default device group will be used for snapshot operations.
  - Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.

To understand how the software selects the target devices during SnapProtect operations, click [here](#).





# SnapProtect™ Backup - Fujitsu ETERNUS DX

◀ Previous Next ▶

## PRE-REQUISITES

- Local Copy license for Snap and Clone.
- Thin Provisioning license.
- Ensure that all members in the Fujitsu array are running firmware version V10L22-1000 or higher.
- Enable SMI-S on the storage array.
- Create a Host Affinity group for the proxy computer.
- If using SnapOPC, ensure to create a SDV and SDPV volumes.

## CONFIGURE DESTINATION VOLUMES

- Source and destination volumes should be pre-paired before performing any snapshot operation. For EC snapshots (clone), pre-paired sessions should be in active state.
- To pre-pair source and destination volumes, install the ETERNUS SF Express Manager software version 14.2A or higher.
- Forbid Advanced Copy and Encrypted volumes are not supported.
- Depending on the type of snapshot being used, review the following for the creation of destination volumes:

### FOR SNAP SNAPSHOTS

If pre-paired sessions are not available, SnapOPC snapshots use any available SDV volumes as their destination volumes. If you need to create a new SDV volume, ensure that the SDV volume is of equal size to the source volume.

### FOR CLONE SNAPSHOTS

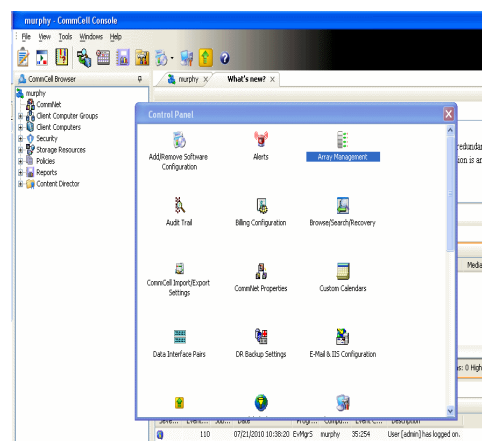
If pre-paired sessions are not available, destination volumes are automatically created for clone snapshots. If a non-existing device group is specified during array configuration in the CommCell Console, a destination volume is created based on the source volume type. However, if a valid device group is specified, the following destination volumes are created depending on the device group type:

- A Thin Provisioning volume is created if the device group is a Thin Provisioning pool.
- A standalone volume is created if the device group is a RAID group.

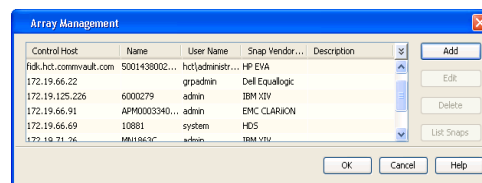
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

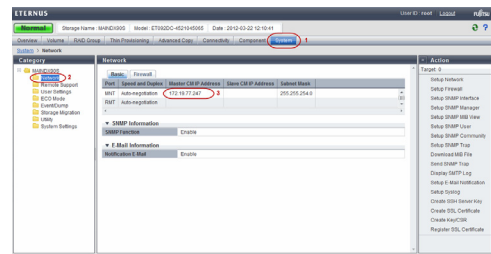
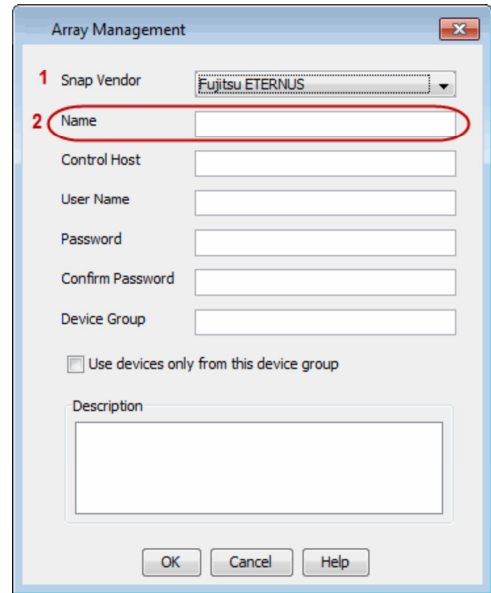


2. Click **Add**.

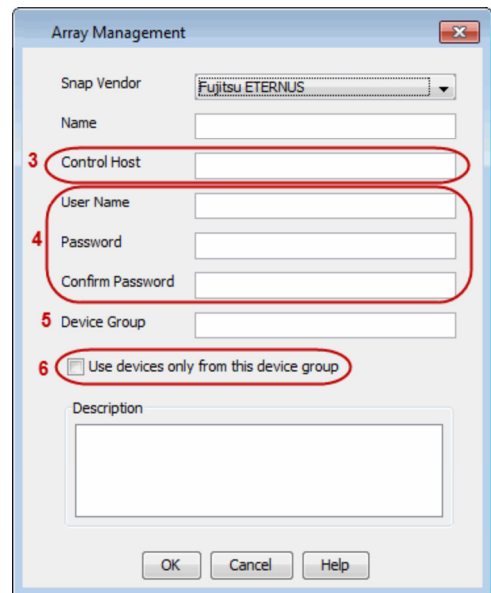


3.
  - Select **Fujitsu ETERNUS** from the **Snap Vendor** list.
  - Specify the CM IP Address of the array in the **Name** field.

For reference purposes, the screenshot on the right shows the CM IP Address for the Fujitsu storage device.



4.
  - Enter the CM IP Address of the array in the **Control Host** field.
  - Enter the access information of a user with administrative privileges in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the RAID group or Thin Provisioning group created on the array to be used for clone operations. Device groups are not applicable for Snap snapshots.
  - Select the **Use devices only from this device group** option to use only the snapshot devices available in the device group specified above.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.



# SnapProtect™ Backup - Hitachi Data Systems

◀ Previous   Next ▶

## PRE-REQUISITES

- Device Manager Server (7.1.1 or higher) installed on any computer.
- RAID Manager (01-25-03/05 or higher) installed on the client and proxy computers.
- Device Manager Agent installed on the client and proxy computers and configured to the Device Manager Server.

The hostname of the proxy computer and the client computer should be visible on the Device Manager Server.

- Appropriate licenses for Shadow Image and COW snapshot.
- For VSP, USP, USP-V and AMS 2000 series, create the following to allow COW operations:
  - COW pools
  - V-VOLs (COW snapshots) that matches the exact block size of P-VOLs devices.
- For HUS, ensure that the source and target devices have the same **Provisioning Attribute** selected. For e.g., if the source is **Full Capacity Mode** then the target device should also be labeled as **Full Capacity Mode**.

## ADDITIONAL REQUIREMENTS FOR VMWARE

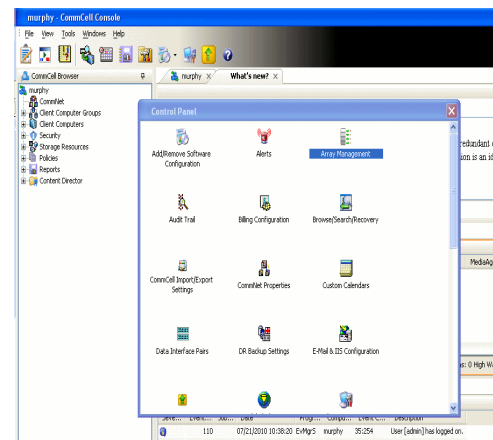
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- HDS LUNs are exposed to the Virtual Server *iDataAgent* client and ESX server.
- All HDS pre-requisites are installed and configured on the Virtual Server *iDataAgent* client computer.
- The Virtual Server client computer is the physical server.
- The Virtual Machine HotAdd feature is not supported.

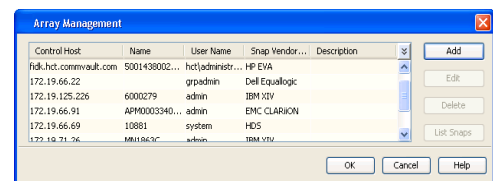
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

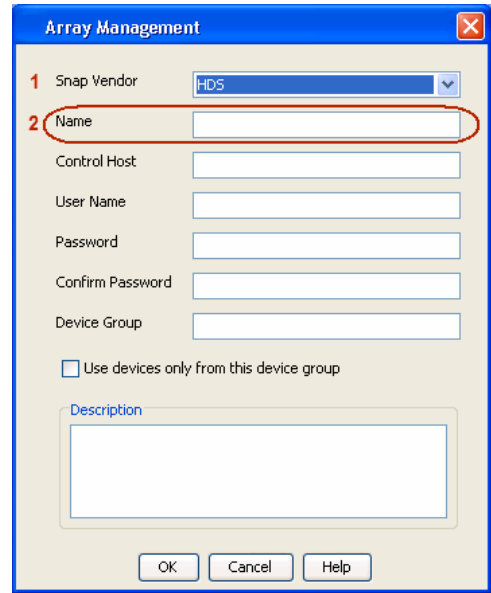
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



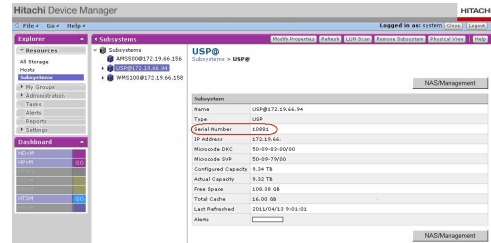
2. Click **Add**.



3.
  - Select **HDS** from the **Snap Vendor** list.
  - Specify the serial number of the array in the **Name** field.



For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



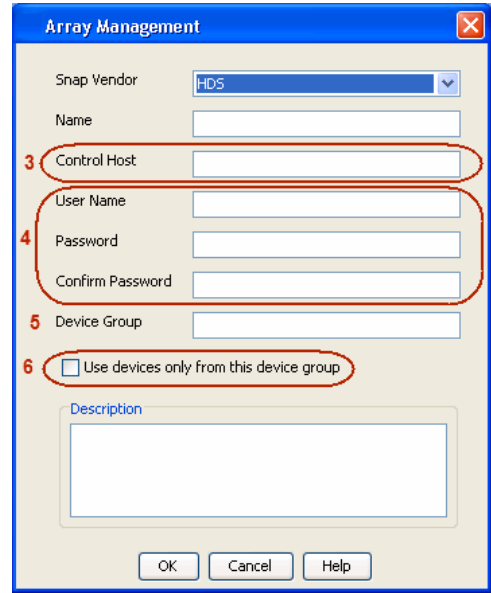
4.
  - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
  - Enter the user access information in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. The device group should have the following naming convention:

<COW\_POOL\_ID>-<LABEL> or <LABEL>-<COW\_POOL\_ID>

where <COW\_POOL\_ID> (for COW job) should be a number. This parameter is required.

<LABEL> (for SI job) should not contain special characters, such as hyphens, and should not start with a number. This parameter is optional.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - HP StorageWorks EVA

◀ Previous   Next ▶

## SETUP THE HP SMI-S EVA

HP-EVA requires Snapshot and Clone licenses for the HP Business Copy EVA feature.

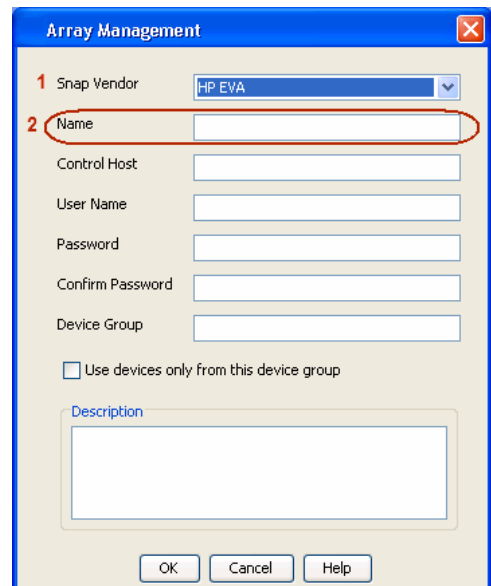
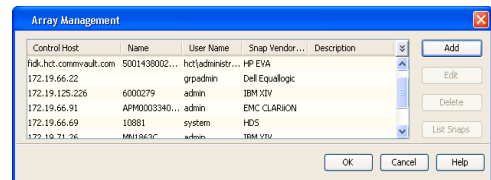
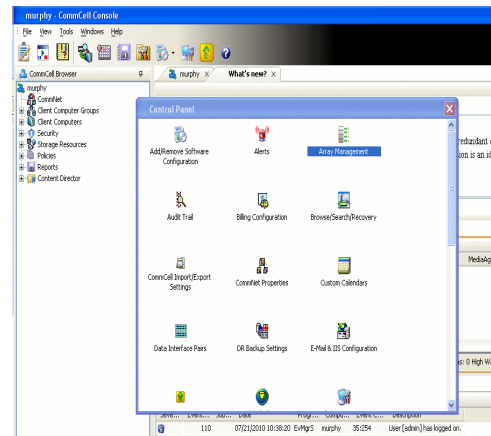
The following steps provide the necessary instructions to setup the HP EVA:

1. Download the HP SMI-S EVA and the HP Command View EVA software on a supported server from the HP web site.
2. Run the Discoverer tool located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\EVAProvider\bin folder to discover the HP-EVA arrays.
3. Use the CLIRefreshTool.bat tool to sync with the SMIS server after using the Command View GUI to perform any active management operations (like adding new host group or LUN). This tool is located in the C:\Program Files\Hewlett-Packard\mpxManager\SMI-S\CXWSCimom\bin folder.

## SETUP THE ARRAY INFORMATION

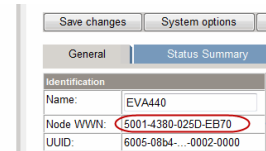
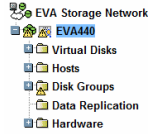
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
2. Click **Add**.
3.
  - Select **HP EVA** from the **Snap Vendor** list.
  - Specify the **World Wide Name** of the array node in the **Name** field.



The World Wide Name (WWN) is the serial number for the HP EVA storage device. See the screenshot on the right for a WWN example.

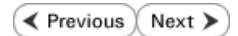
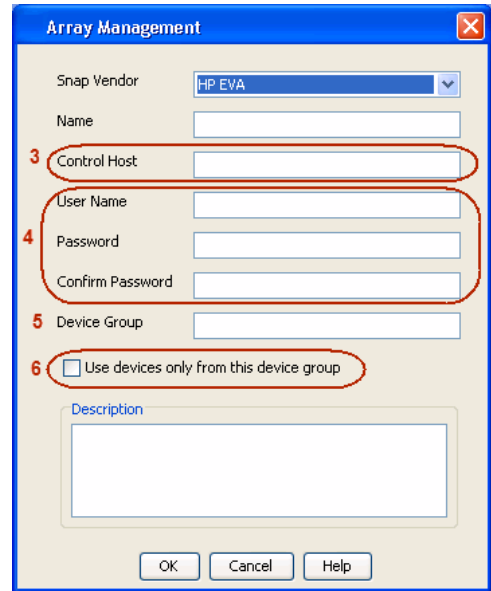
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



4.
  - Enter the name of the management server of the array in the **Control Host** field.

Ensure that you provide the host name and not the fully qualified domain name or TCP/IP address of the host.

- Enter the user access information in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the hardware disk group created on the array to be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - IBM SAN Volume Controller (SVC)

◀ Previous    Next ▶

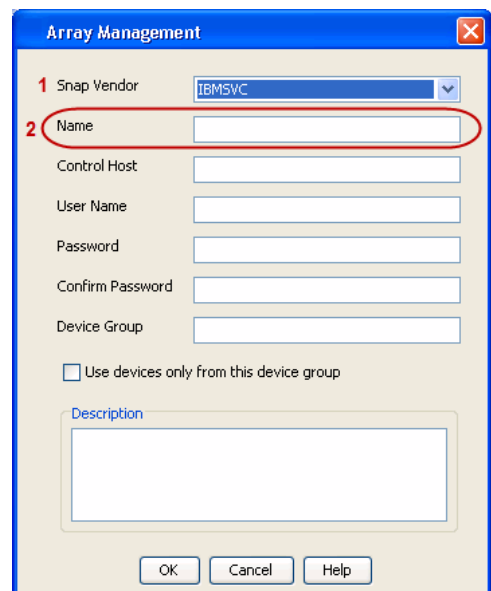
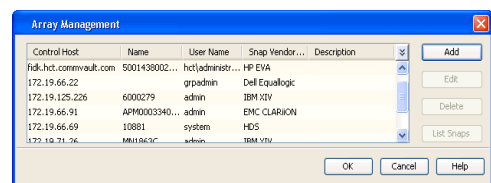
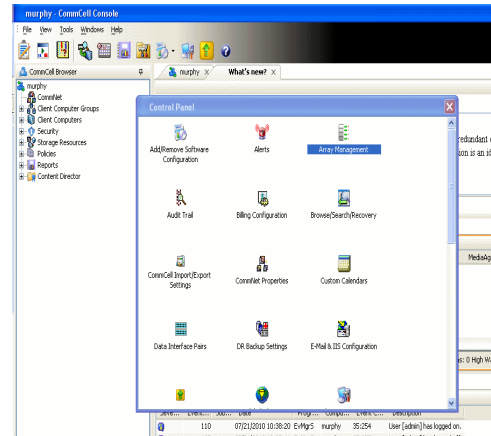
## PRE-REQUISITES

- IBM SVC requires the FlashCopy license.
- Ensure that all members in the IBM SVC array are running firmware version 6.1.0.7 or higher.
- Ensure that proxy computers are configured and have access to the storage device by adding a host group with ports and a temporary LUN.

## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

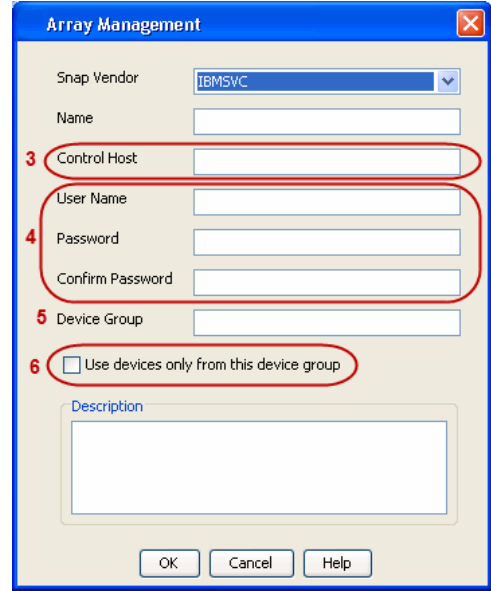
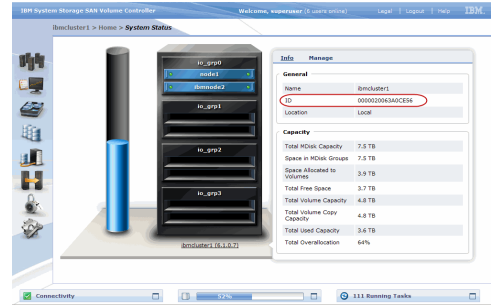
- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
  - Specify the 16-digit ID of the storage device in the **Name** field.



The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

4.

- Enter the Management IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the local application administrator in the **Username** and **Password** fields.
- In the **Device Group** field, specify the name of the physical storage pools created on the array to be used for snapshot (flash copy) operations.  
If you do not specify a device group, the default storage pool will be used for snapshot operations.
- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.





# SnapProtect™ Backup - IBM XIV

◀ Previous   Next ▶

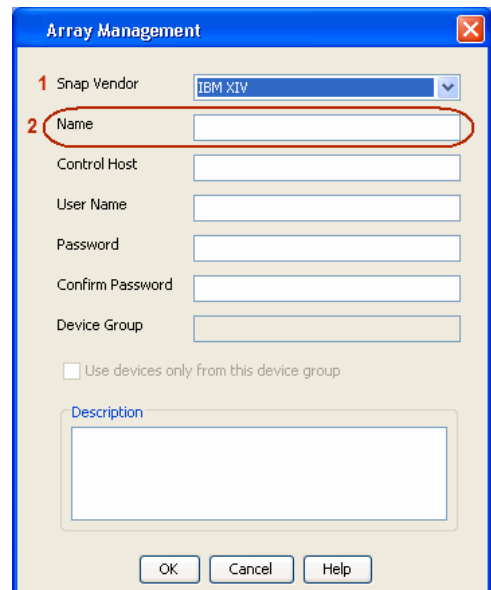
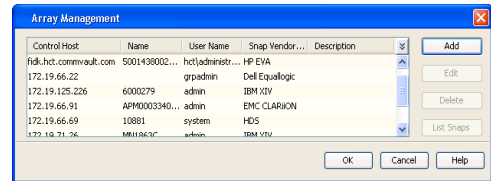
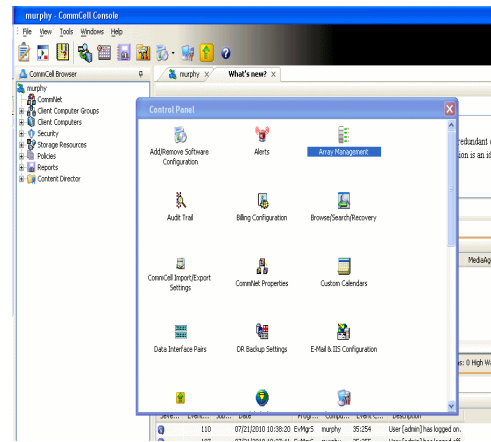
## PRE-REQUISITES

1. IBM XCLI (2.3 or higher) installed on the client and proxy computers. On Unix computers, XCLI version 2.4.4 should be installed.
2. Set the location of XCLI in the environment and system variable path.
3. If XCLI is installed on a client or proxy, the client or proxy should be rebooted after appending XCLI location to the system variable path. You can use the `XCLI_BINARY_LOCATION` registry key to skip rebooting the computer.

## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

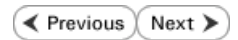
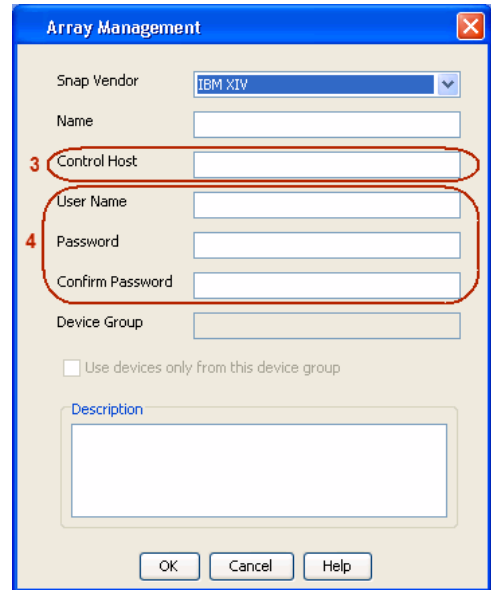
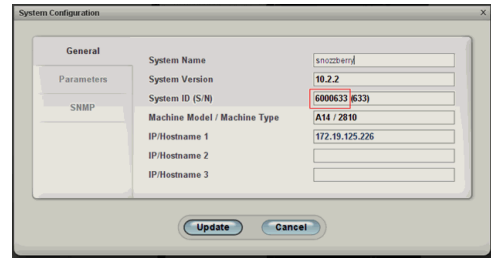
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
2. Click **Add**.
3.
  - Select **IBM XIV** from the **Snap Vendor** list.
  - Specify the 7-digit serial number for the array in the **Name** field.



The **System ID (S/N)** is the serial number for the IBM XIV storage device. See the screenshot on the right for reference.

4.

- Enter the IP address or host name of the array in the **Control Host** field.
- Enter the user access information of the application administrator in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - LSI

◀ Previous Next ▶

## PREREQUISITES

- Ensure that the LSI Storage Management Initiative Specification (SMIS) server has access to the LSI array through TCP/IP network to perform SnapProtect operations.
- Ensure that the client has access to:
  - SMIS server through TCP/IP network.
  - LSI array through iSCSI or Fiber Channel network.
- Ensure that proxy computers are configured and have access to the storage device by adding a temporary LUN to the "host" using the Storage Management Console.

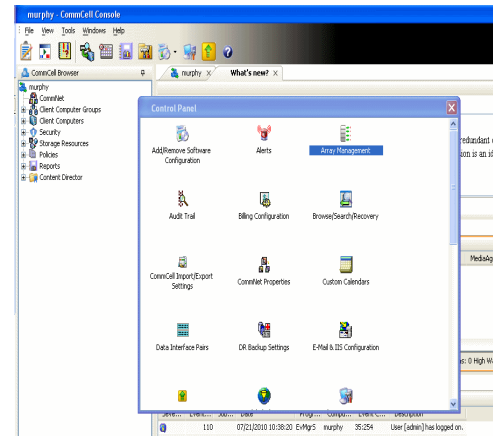
## ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using SAN transport mode, ensure that the Client and the ESX Server reside in the same host group configured in the LSI array, as one volume cannot be mapped to multiple host groups.

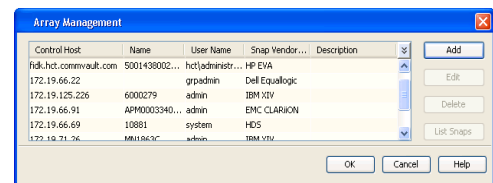
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

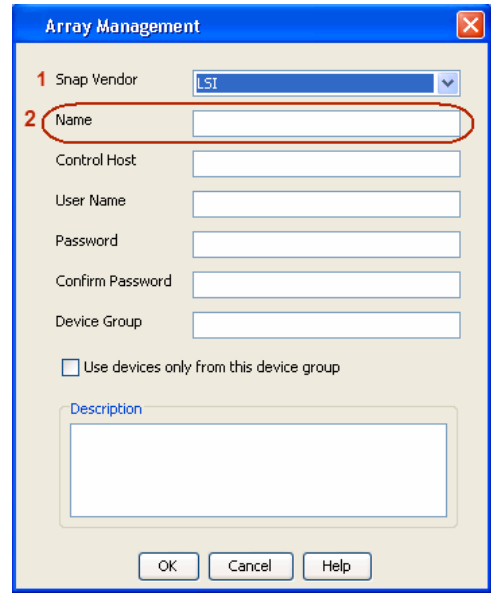
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

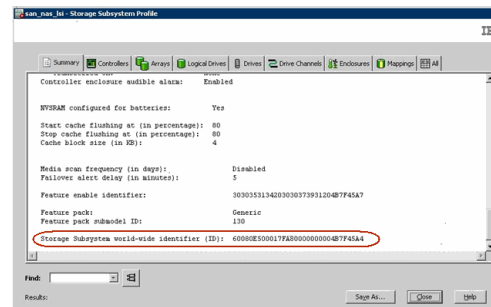


3.
  - Select **LSI** from the **Snap Vendor** list.
  - Specify the serial number for the array in the **Name** field.



The **Storage Subsystem world-wide identifier (ID)** is the serial number for the LSI storage device.

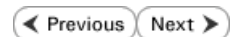
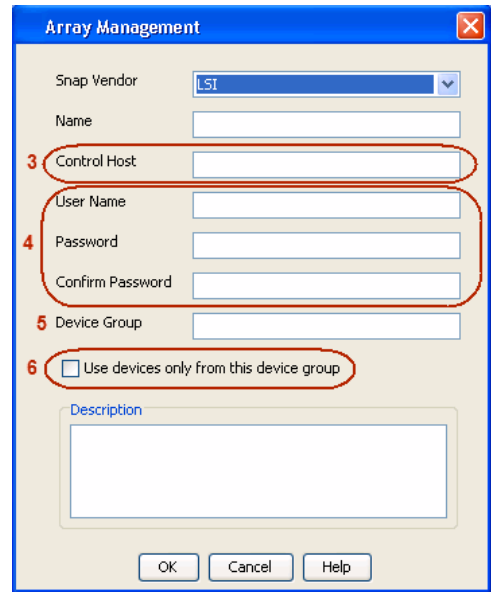
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



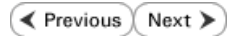
4.
  - Specify the name of the device manager server where the array was configured in the **Control Host** field.
  - Enter the user access information using the LSI SMIS server credentials of a local user in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot operations. If you do not have a device group created on the array, specify None.

If you specify None in the **Device Group** field but do have a device group created on the array, the default device group will be used for snapshot operations.

- Select the **Use devices only from this device group** option to use only the snapshots devices available in the device group specified above.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK** to save the information.



# SnapProtect™ Backup - NetApp



## PREREQUISITES

### LICENSES

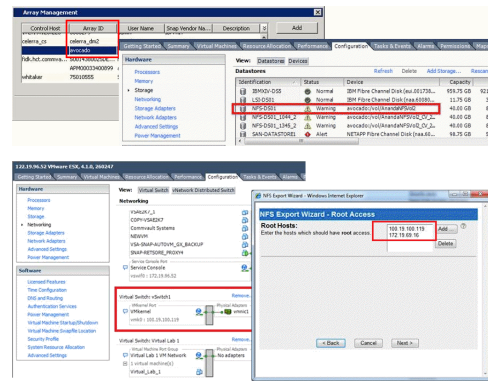
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

## ADDITIONAL REQUIREMENTS FOR VMWARE

When performing SnapProtect operations on VMware using NFS file-based protocol, ensure the following:

The NetApp storage device name specified in Array Management matches that on the ESX Server.

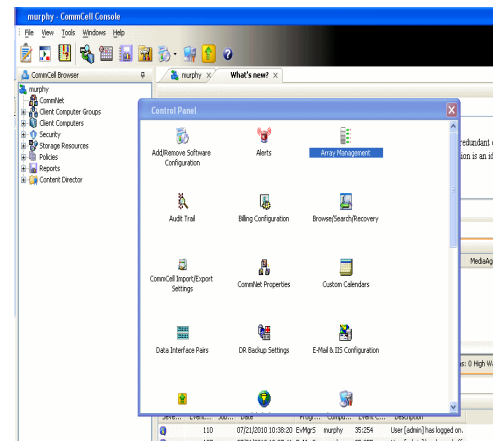
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



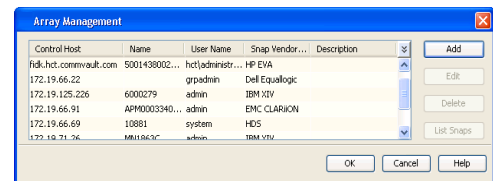
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



- Click **Add**.



- Select **NetApp** from the **Snap Vendor** list.
  - Specify the name of the file server in the **Name** field.
  - You can provide the host name, fully qualified domain

name or TCP/IP address of the file server.

- If the file server has more than one host name due to multiple domains, provide one of the host names based on the network you want to use for administrative purposes.
- Enter the user access information with administrative privileges in the **Username** and **Password** fields.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.

Array Management

Snap Vendor: NetApp

Name: [Text Box]

Control Host: [Text Box]

User Name: [Text Box]

Password: [Text Box]

Confirm Password: [Text Box]

Device Group: [Text Box]

Use devices only from this device group

Description: [Text Area]

OK Cancel Help

◀ Previous Next ▶

# SnapProtect™ Backup - NetApp SnapVault/SnapMirror

◀ Previous   Next ▶

## OVERVIEW

SnapVault allows a secondary NetApp filer to store SnapProtect snapshots. Multiple primary NetApp file servers can backup data to this secondary filer. Typically, only the changed blocks are transferred, except for the first time where the complete contents of the source need to be transferred to establish a baseline. After the initial transfer, snapshots of data on the destination volume are taken and can be independently maintained for recovery purposes.

SnapMirror is a replication solution that can be used for disaster recovery purposes, where the complete contents of a volume or qtree is mirrored to a destination volume or qtree.

## PREREQUISITES

### LICENSES

- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- iSCSI Initiator must be configured on the client and proxy computers to access the storage device.

For the Virtual Server Agent, the iSCSI Initiator is required when the agent is configured on a separate physical server and uses iSCSI datastores. The iSCSI Initiator is not required if the agent is using NFS datastores.

- FFCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for the specific data types.
- Protection Manager, Operations Manager, and Provisioning Manager licenses for DataFabric Manager 4.0.2 or later.
- SnapMirror Primary and Secondary Licenses for disaster recovery operations.
- SnapVault Primary and Secondary License for backup and recovery operations.
- HTTP/HTTPS licenses on the NetApp file server to allow communication.

### ARRAY SOFTWARE

- DataFabric Manager (DFM) - A server running NetApp DataFabric® Manager server software. DataFabric Manager 4.0.2 or later is required.
- SnapMirror - NetApp replication technology used for disaster recovery.
- SnapVault - NetApp replication technology used for backup and recovery.

## SETTING UP SNAPVAULT

Before using SnapVault and SnapMirror, ensure the following conditions are met:

1. On your source file server, use the `license` command to check that the `sv_ontap_pri` and `sv_ontap_sec` licenses are available for the primary and secondary file servers respectively.
2. Enable SnapVault on the primary and secondary file servers as shown below:

```
options snapvault.enable on
```

3. On the primary file server, set the access permissions for the secondary file servers to transfer data from the primary as shown in the example below:

```
options snapvault.access host=secondary_filer1, secondary_filer2
```

4. On the secondary file server, set the access permissions for the primary file servers to restore data from the secondary as shown in the example below:

```
options snapvault.access host=primary_filer1, primary_filer2
```

## INSTALLING DATAFABRIC MANAGER

- The Data Fabric Manager (DFM) server must be installed. For more information, see Setup the DataFabric Manager Server.
- The following must be configured:
  - Discover storage devices
  - Add Resource Pools to be used for the Vault/Mirror storage provisioning

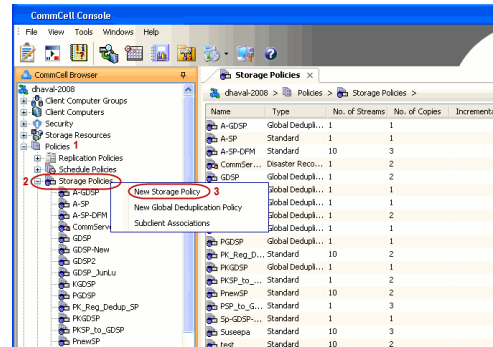
## CONFIGURATION

Once you have the environment setup for using SnapVault and SnapMirror, you need to configure the following before performing a SnapVault or SnapMirror operation.

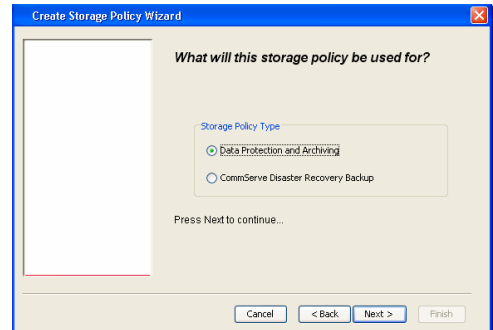
## CREATE STORAGE POLICY

Use the following steps to create a storage policy.

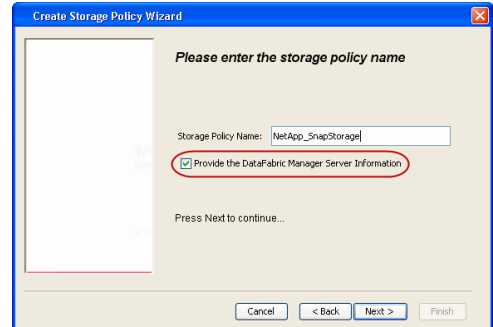
1.
  - From the CommCell Browser, navigate to **Policies**.
  - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



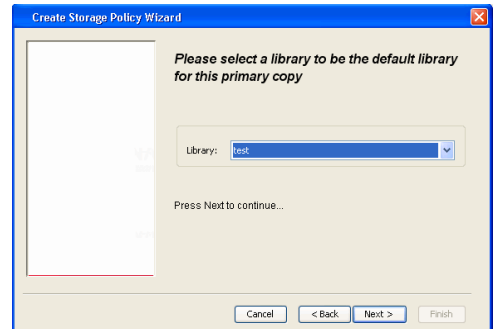
3.
  - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
  - Select **Provide the DataFabric Manager Server Information**.
  - Click **Next**.



4.
  - In the **Library** list, select the default library to which the Primary Copy should be associated.

It is recommended that the selected disk library uses a LUN from the File server.

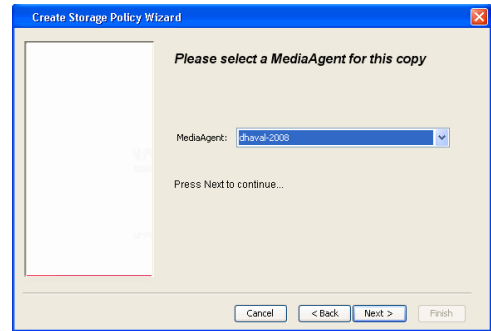
- Click **Next**.



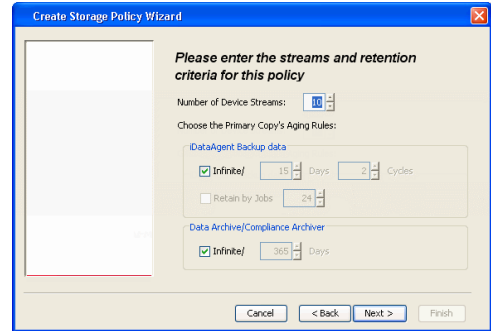
5.
  - Select a MediaAgent from the **MediaAgent** list.
  - Click **Next**.



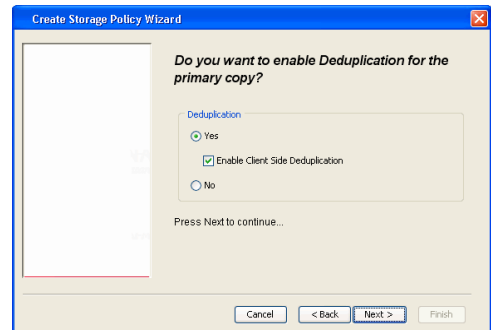
6. Click **Next**.



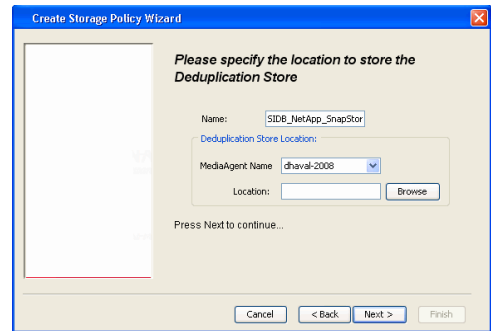
7. Click **Next**.



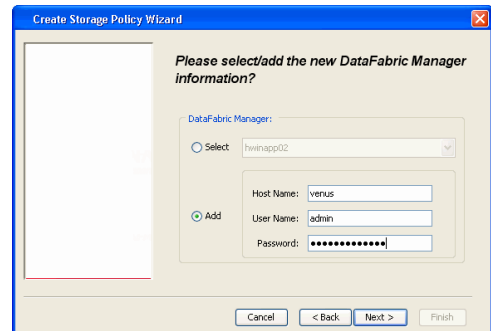
- 8.
- Verify **Name** and **MediaAgent Name**.
  - Click **Browse** to specify location for **Deduplication Store**.
  - Click **Next**.

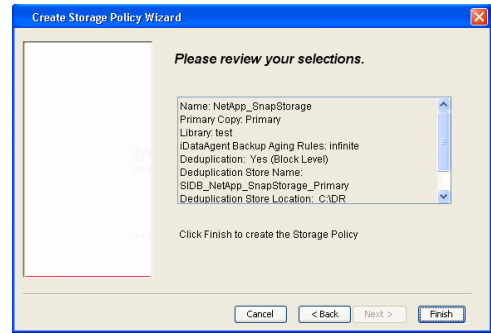


- 9.
- Provide the DataFabric Manager server information.
    - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
    - If you want to add a new DataFabric Manager Server, click **Add**.
  - Click **Next**.



10. Click **Finish**.



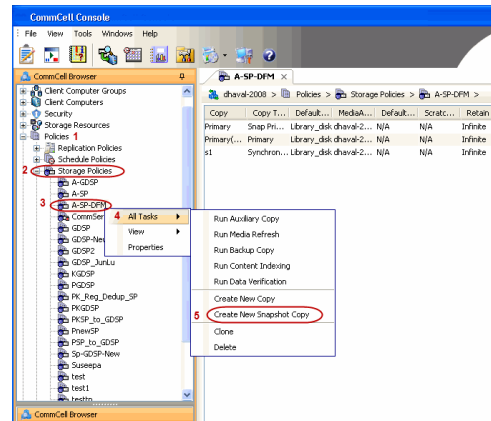


11. The new Storage Policy creates the following:
  - **Primary Snap Copy**, used for local snapshot storage
  - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

### CREATE A SECONDARY SNAPSHOT COPY

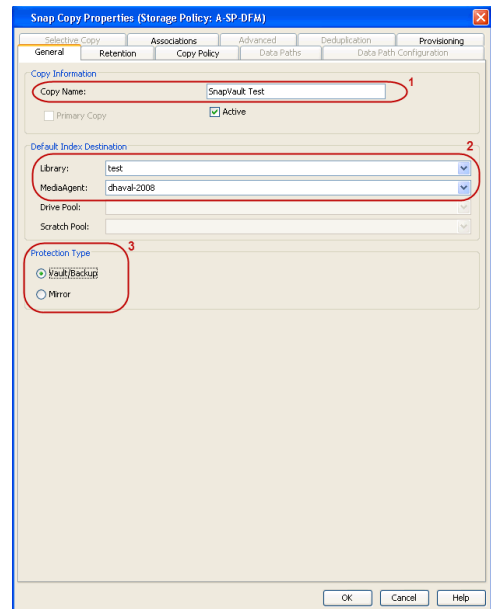
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

1.
  - From the CommCell Browser, navigate to **Policies | Storage Policies**.
  - Right-click the storage policy and click **All Tasks | Create New Snapshot Copy**.



2.
  - Enter the **Copy Name**.
  - Select the **Library** and **MediaAgent** from the drop-down list.
  - Click **Vault/Backup** or **Mirror** protection type based on your needs.

It is recommended that the selected disk library uses a CIFS or NFS share or a LUN on the File server.

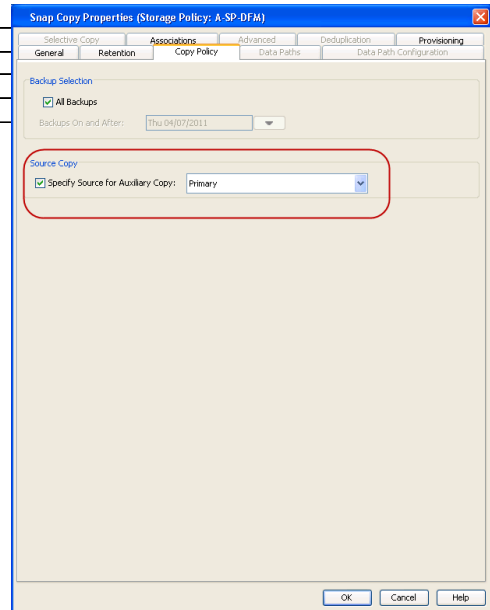


3.
  - Click the **Copy Policy** tab.
  - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

Copies can be created for the topologies listed in the following table:

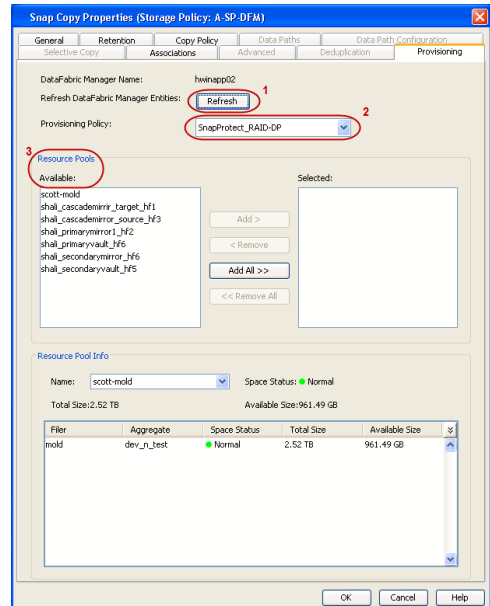
| TOPOLOGY | SOURCE COPY |
|----------|-------------|
|----------|-------------|

|                       |         |
|-----------------------|---------|
| Primary-Mirror        | Primary |
| Primary-Mirror-Vault  | Mirror  |
| Primary-Vault         | Primary |
| Primary-Vault-Mirror  | Vault   |
| Primary-Mirror-Mirror | Mirror  |



- Click the **Provisioning** tab.
  - Click **Refresh** to display the DFM entities.
  - Select the **Provisioning Policy** from the drop-down list.
  - Select the **Resource Pools** available from the list.
  - Click **OK**.

The secondary snapshot copy is created.



- If you are using a Primary-Mirror-Vault (P-M-V) or Primary-Vault (P-V) topology on ONTAP version higher than 7.3.5 (except ONTAP 8.0 and 8.0.1), perform the following steps:

- Connect to the storage device associated with the source copy of your topology. You can use SSH or Telnet network protocols to access the storage device.
- From the command prompt, type the following:
 

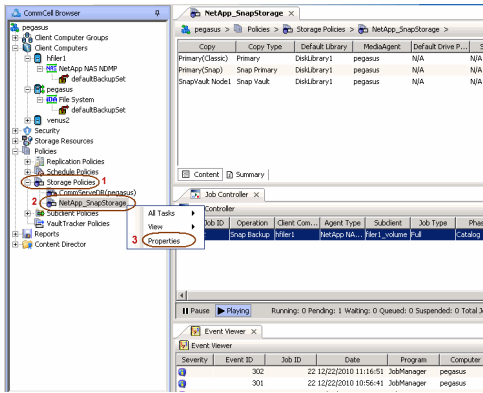
```
options snapvault.snapshot_for_dr_backup named_snapshot_only
```
- Close the command prompt window.

It is recommended that you perform this operation on all nodes in the P-M-V topology.

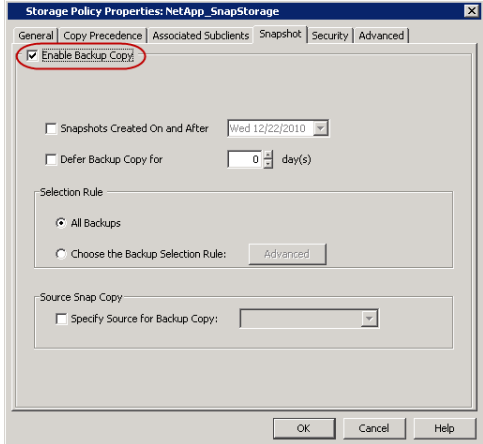
## CONFIGURE BACKUP COPY

Follow the steps given below to configure Backup Copy for moving snapshots to media.

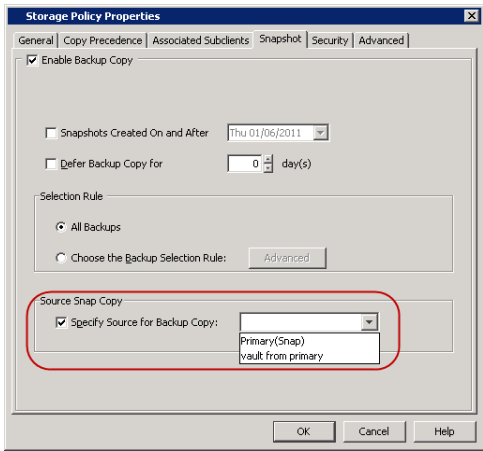
- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.



2.
  - Click the **Snapshot** tab.
  - Select **Enable Backup Copy** option to enable movement of snapshots to media.
  - Click **OK**.



3.
  - Select **Specify Source for Backup Copy**.
  - From the drop-down list, select the source copy to be used for performing the backup copy operation.

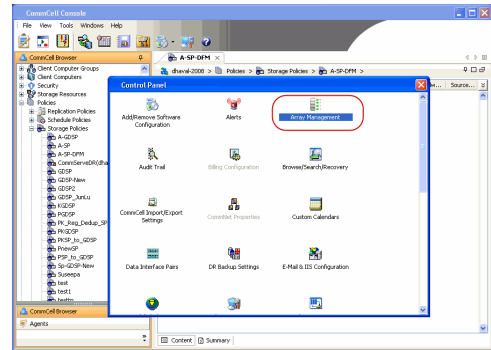


## SETUP THE ARRAY INFORMATION

The following steps describe the instructions to set up the primary and secondary arrays.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

2. Click **Add**.

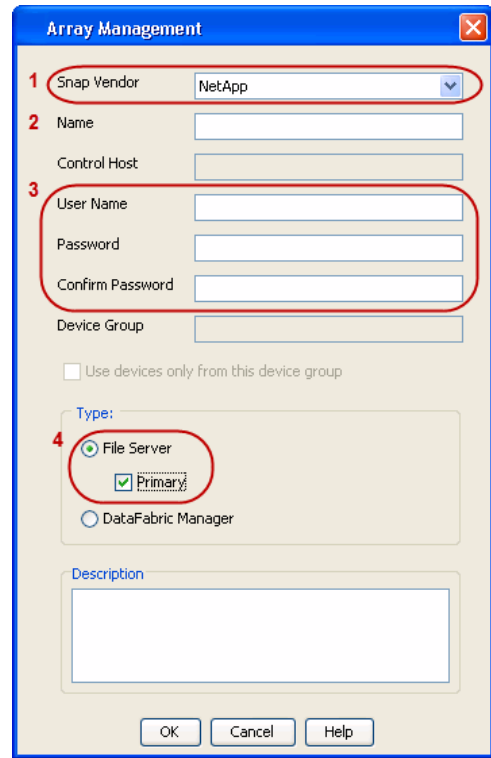
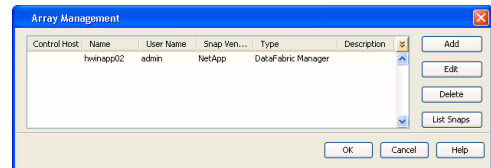


3.
  - Select **NetApp** from the **Snap Vendor** list.
  - Specify the name of the primary file server in the **Name** field.

The name of primary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address. However, if you plan to create a Vaut/Mirror copy, ensure the IP address of the primary file server resolves to the primary IP of the network interface and not to an alias.

You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

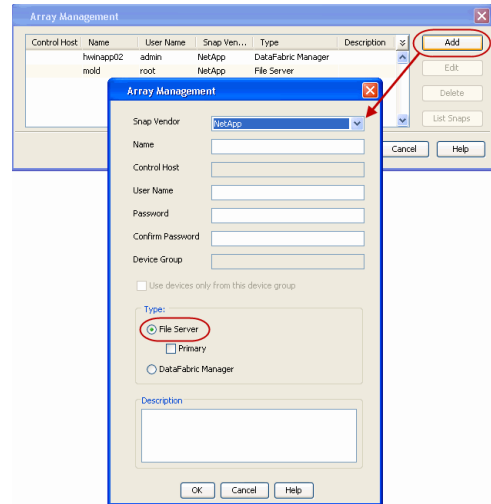
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



4.
  - Click **Add** again to enter the information for the secondary array.
  - Specify the name of the secondary file server in the **Name** field.

The name of secondary file server may be different in the DataFabric Manager, CommServe, MediaAgent and other entities, but it should resolve to the same IP address.

- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
- Click **OK**.



## SEE ALSO

### Import Wizard Tool

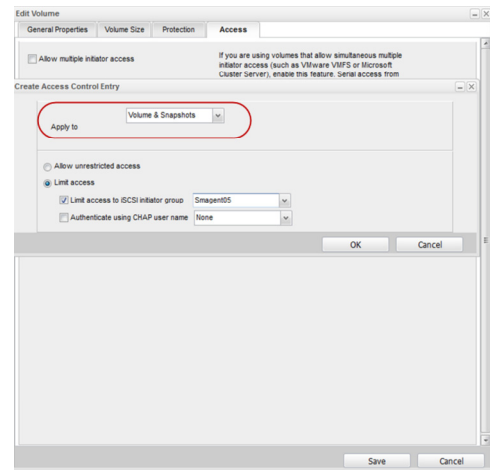
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

# SnapProtect™ Backup - Nimble

◀ Previous Next ▶

## PREREQUISITES

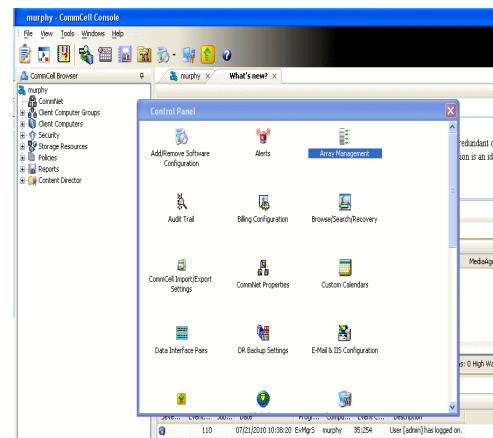
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry** to **Snapshots Only**.
- Ensure that a temporary LUN is allocated to all ESX Servers that are used for snapshot operations.



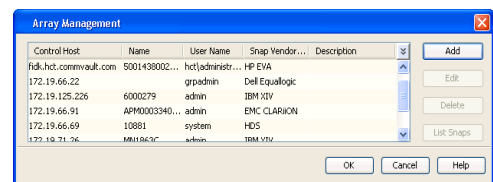
## SETUP THE ARRAY INFORMATION

Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.



3.
  - Select **Nimble** from the **Snap Vendor** list.
  - Specify the Data IP Address of the array in the **Name** field.

If you have more than one Data IP Address configured, you will need to add the array information for each of the configured Data IP addresses.

- Enter the Management IP Address of the array in the **Control Host** field.

For reference purposes, the screenshot on the right shows the Data IP Address and Management IP for the Nimble storage device.

| Name | Status | Type           | Data IP Address | Subnet Mask   | MTU      | Bytes |
|------|--------|----------------|-----------------|---------------|----------|-------|
| eth1 |        | Data only      | 172.19.108.100  | 255.255.252.0 | Standard | 1500  |
| eth2 |        | Data only      | 172.19.108.101  | 255.255.252.0 | Standard | 1500  |
| eth3 |        | Not configured |                 |               | Standard | 1500  |
| eth4 |        | Not configured |                 |               | Standard | 1500  |

4.
  - Enter the access information of a user with administrative privileges in the **Username** and **Password** fields.
  - Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.
  - Click **OK** to save the information.



## SnapProtect™ Backup - Data Replicator

< Previous    Next >

### PRE-REQUISITES

#### INSTALLATION

- The use of Data Replicator with the SnapProtect backup requires MediaAgent, File System iDataAgent, and ContinuousDataReplicator on the source, destination, and proxy computers.

The use of a proxy server to perform SnapProtect operations is supported when a hardware storage array is used for performing the SnapProtect backup.

- The operating system of the MediaAgent to be used for SnapProtect backup must be either the same or higher version than the source computer.

#### STORAGE POLICY REQUIREMENTS

The Primary Snap Copy to be used for creating the snapshot copy must be a disk library.

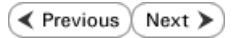
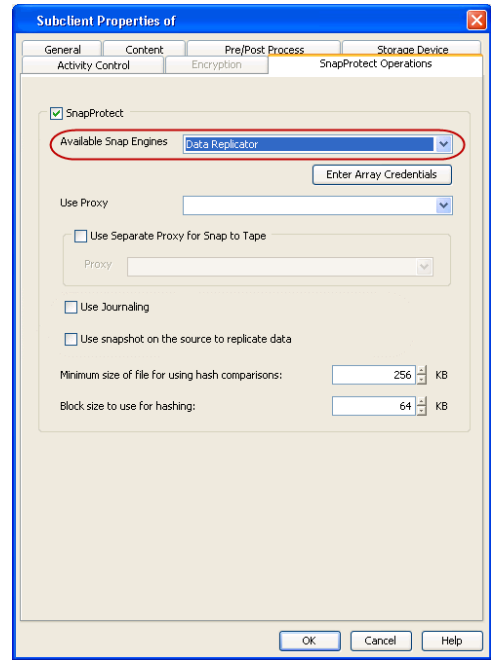
If the Storage Policy or the disk library being used by the subclient is updated, the subclient should be recreated.

### SETUP THE ARRAY

1.
  - From the CommCell Console, navigate to <Client> | <Agent>.
  - Right-click the subclient and click **Properties**.
2.
  - Click the **SnapProtect Operations** tab.
  - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down

list.

- Click **OK**.



# Getting Started - Windows File System Backup

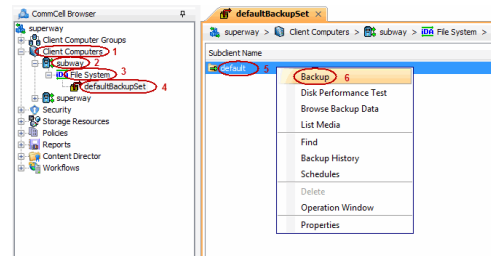
◀ Previous Next ▶

## PERFORM A BACKUP

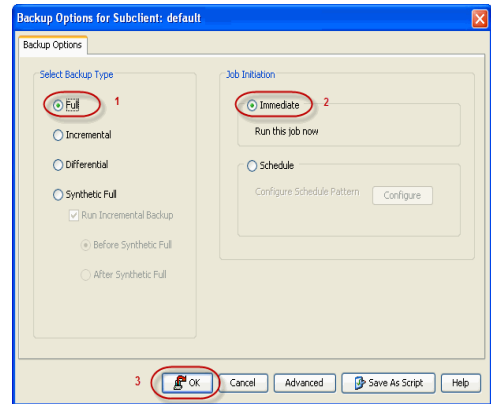
Once the storage policy is configured, you are ready to perform your first backup.

The following section provides step-by-step instructions for performing your first backup:

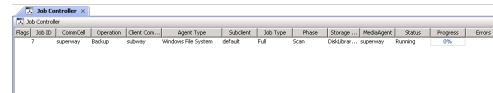
- From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.
  - Right-click the default subclient and click **Backup**.



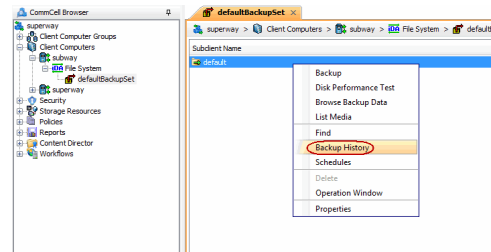
- Click **Full** as backup type and then click **Immediate**.
  - Click **OK**.



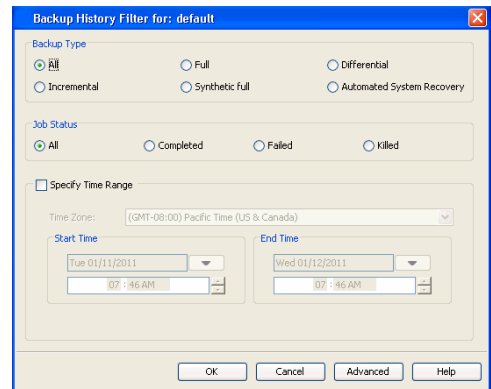
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



- Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.

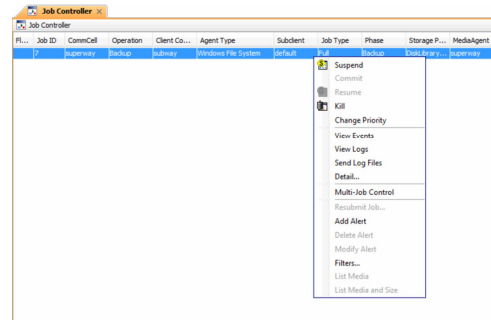


- Click **OK**.



- You can view the following details about the job by right-clicking the job:

- Items that failed during the job
- Items that succeeded during the job
- Details of the job
- Events of the job
- Log files of the job
- Media associated with the job



# Getting Started - Vault/Mirror Copy

◀ Previous   Next ▶

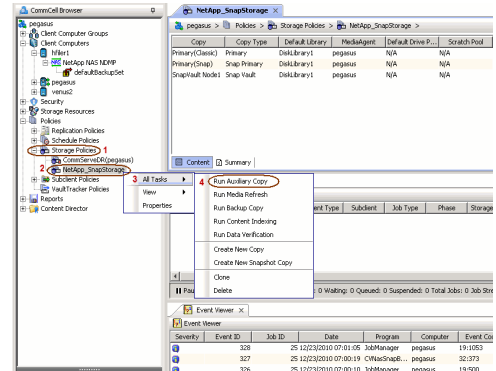
## SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

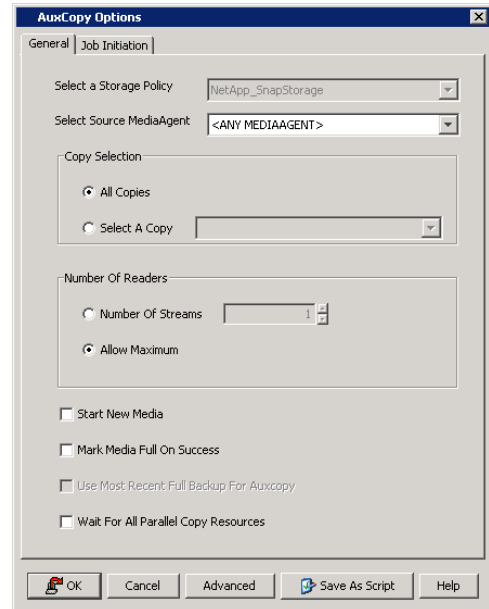
### INITIATE VAULT/MIRROR COPY

Follow the steps to initiate a Vault/Mirror copy.

- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks | Run Auxiliary Copy**.

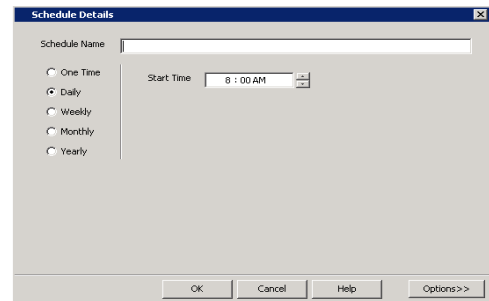


- Select the desired options and click the **Job Initiation** tab.
  - Select **Schedule** to configure the schedule pattern and click **Configure**.



- Enter the schedule name and select the appropriate scheduling options.
  - Click **OK**.

The SnapProtect software will call any available DataFabric Manager APIs at the start of the Auxiliary Copy job to detect if the topology still maps the configuration.



Once the Vault/Mirror copy of the snapshot is created, you cannot re-copy the same snapshot to the Vault/Mirror destination.

◀ Previous   Next ▶

# Getting Started - Snap Movement to Media

◀ Previous Next ▶

## SKIP THIS PAGE IF YOU ARE NOT USING A TAPE DEVICE.

Click **Next** ▶ to Continue.

### BACKUP COPY OPERATIONS

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the SnapProtect backup or at a later time.

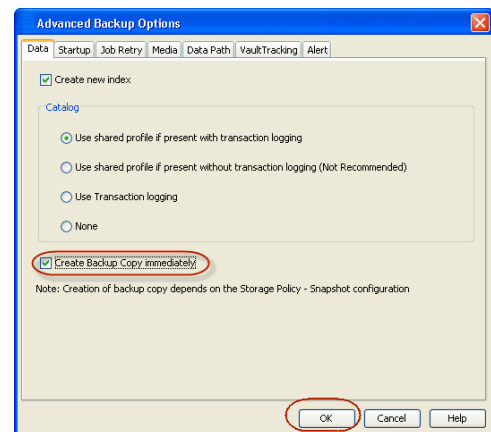
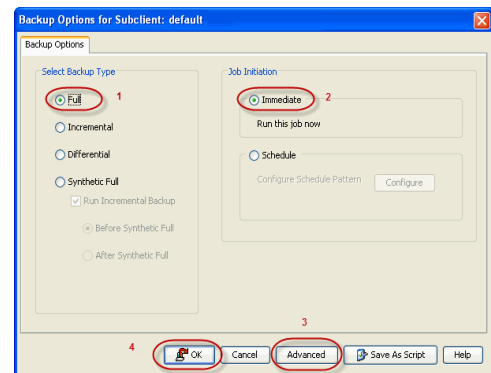
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

#### INLINE BACKUP COPY

Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

Depending on the Agent you are using, your screens may look different than the examples shown in the steps below.

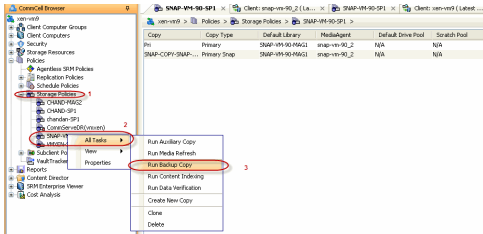
1.
  - From the CommCell Console, navigate to **Client Computers** | **<Client>** | **<Agent>** | **defaultBackupSet**.
  - Right click the default subclient and click **Backup**.
  - Select **Full** as backup type.
  - Click **Advanced**.
  
2.
  - Select **Create Backup Copy immediately** to create a backup copy.
  - Click **OK**.



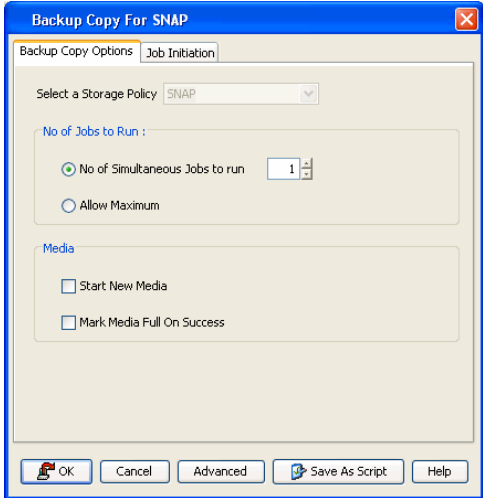
#### OFFLINE BACKUP COPY

Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

1.
  - From the CommCell Console, navigate to **Policies** | **Storage Policies**.
  - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



# Getting Started - Windows File System Restore



## PERFORM A RESTORE

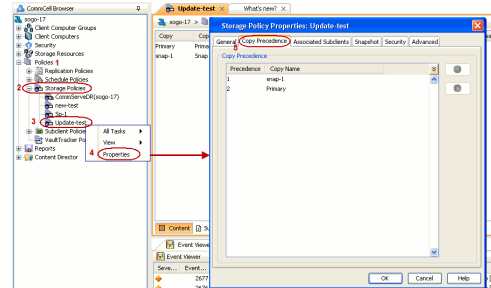
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring the backup data from copies.

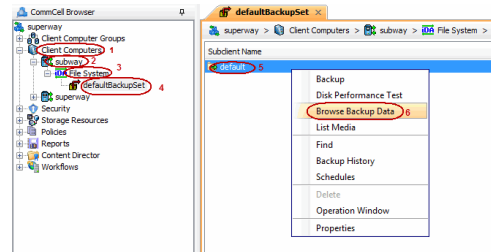
- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.
  - Click the **Copy Precedence** tab.
  - By default, the snapshot copy is set to 1 and is used for the operation.

You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.

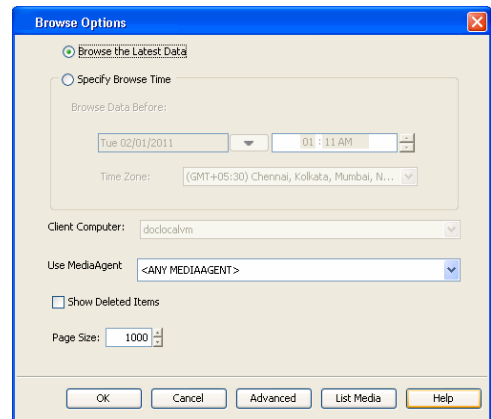
- Click **OK**.



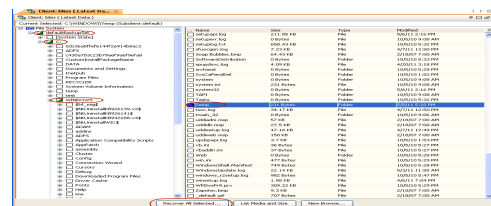
- From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.
  - Right-click the default subclient and then click **Browse Backup Data**.



- Click **OK**.



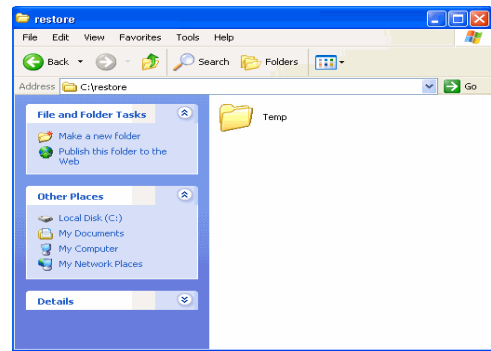
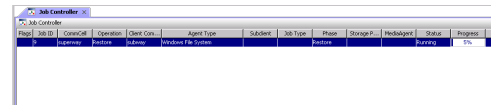
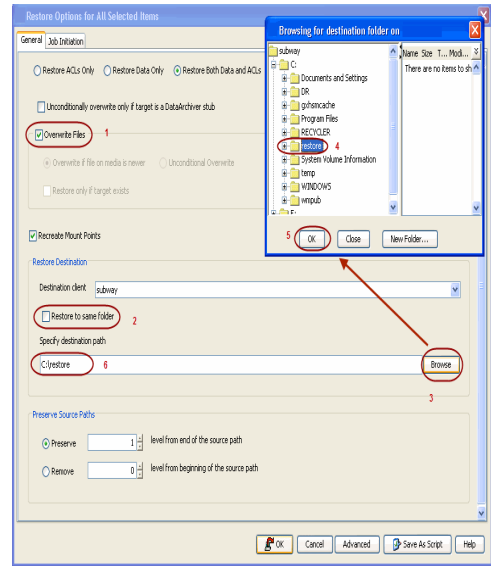
- Expand the **defaultBackupSet** and navigate to **Documents and Settings** folder.
  - Select the **Documents and Settings** folder.
  - Click **Recover All Selected**.



- Clear the **Overwrite Files** and **Restore to same folder** options.
  - Specify the destination path by clicking **Browse** button.  
This will ensure that the existing files are not overwritten.
  - Click **OK**.



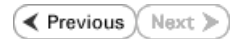
- 6. You can monitor the progress of the restore job in the **Job Controller** window of the CommCell Console.
- 7. Once the File System is restored, verify that the restored files/folders are available in the restore destination.



**CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.**

If you want to further explore this Agent's features read the Advanced sections of this documentation.

If you want to configure another client, go back to Setup Clients.



# SnapProtect™ Backup - Support

## TABLE OF CONTENTS

**Initial SnapProtect Setup**

**License Requirements**

**Supported Storage Arrays**

**Backup Types**

**Platforms**

**Supported Volume Managers**

**Multipath I/O Support**

## INITIAL SNAPPROTECT SETUP

Initial deployment and successful run of SnapProtect backup may take around 4 weeks due to the various environment dependencies. The following parameters are known to affect the deployment and initial run and hence need a thorough evaluation:

- Firmware versions on the array
- Device types
- Mode of access
- Security configuration
- Operating Systems interacting with the storage array
- Application layout on the storage array LUNs

## LICENSE REQUIREMENTS

- The SnapProtect feature requires the **Snap Protect Enabler** license.
- The NetApp SnapVault/SnapMirror feature requires the **NetApp Snap Management** license.

## SUPPORTED STORAGE ARRAYS

The SnapProtect backup is designed to work in conjunction with the following storage arrays, which provide snapshot functionality for data protection operations:

| SUPPORTED HARDWARE ARRAYS |                                 |                                                                     |                                                        |                                                                                                                              |                                                               |                                                                                                                                                                            |
|---------------------------|---------------------------------|---------------------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VENDOR                    | SNAPSHOT                        | VERSION/FIRMWARE                                                    | REQUIRED LICENSING                                     | REQUIRED SOFTWARE                                                                                                            | PROTOCOL                                                      | NOTES/CAVEATS                                                                                                                                                              |
| <b>DELL COMPELLENT</b>    | Snapshot                        | Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x | Snapshot Replay licensing                              | None                                                                                                                         | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*<br>iSCSI | Supported on Windows, Linux and VMware.<br>No HyperV<br>Compellent Live Volume feature is not supported.                                                                   |
| <b>DELL EQUALLOGIC</b>    | Snapshot<br>Clone               | 4.2.0                                                               | Included                                               | None                                                                                                                         | iSCSI                                                         | On Red Hat Linux computers using version 5.0, only 32-bit is supported.<br>No HyperV, or UNIX.<br>Boot from SAN volumes is not supported.                                  |
| <b>EMC CLARIION</b>       | SnapView Snap<br>SnapView Clone | CX500 / CX700<br>CX3-10 thru CX3-80<br>CX4-120 thru CX4-960         | SnapView Snapshot/Clone<br>Solutions Enabler Licensing | Solutions Enabler 6.5.1 or higher on Client and Proxy<br>Navisphere CLI on Client and Proxy<br>NaviAgent on Client and Proxy | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*          | No HyperV<br>Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap |

|                                 |                                          |                                                                                                     |                                                                            |                                                                                                                                                                                                                   |                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                          |                                                                                                     |                                                                            |                                                                                                                                                                                                                   |                                                                       | operations.<br>Not supported on HP-UX                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>EMC VNX</b>                  | SnapView Snap<br><br>SnapView Clone      | VNX 5100, 5300, 5500, 5700, 7500                                                                    | SnapView Snapshot/Clone<br><br>Solutions Enabler Licensing                 | Solutions Enabler 7.1 or higher on Client and Proxy<br><br>Unisphere CLI on Client and Proxy<br><br>Unisphere Host Agent on Client and Proxy                                                                      | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*<br><br>iSCSI | No HyperV<br><br>VMware with NFS datastores are not supported.<br><br>iSCSI PowerPath LUNs are not supported.<br><br>Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.<br><br>For configuring a VNX array, refer to the step-by-step instructions provided for EMC Clariion.<br><br>Not supported on HP-UX |
| <b>EMC CELERRA</b>              | SnapSure Snap                            | DART 5.5 or Newer                                                                                   | SnapSure Snap License<br><br>Solutions Enabler Licensing                   | Solutions Enabler 6.5.1 or higher on Client and Proxy<br><br>Navisphere CLI on Client and Proxy                                                                                                                   | NFS                                                                   | Supported on VMware 4.x.<br><br>No HyperV<br><br>Not supported on HP-UX                                                                                                                                                                                                                                                                                                                                                            |
| <b>EMC SYMMETRIX</b>            | TimeFinder Snap<br><br>TimeFinder Mirror | DMX3 or Newer                                                                                       | TimeFinder Snap, Mirror, Clone Licenses<br><br>Solutions Enabler Licensing | Solutions Enabler 6.4 or higher on Client and Proxy                                                                                                                                                               | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*              | No HyperV<br><br>Remote SymApi Server is not supported.<br><br>Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.                                                                                                                                                                                           |
| <b>EMC VMAX</b>                 | TimeFinder Snap, Mirror and Clone        | VMAX                                                                                                | TimeFinder Snap, Mirror, Clone Licenses<br><br>Solutions Enabler Licensing | Solutions Enabler 7.2 or higher on Client and Proxy                                                                                                                                                               | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*              | No HyperV<br><br>Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.                                                                                                                                                                                                                                         |
| <b>FUJITSU ETERNUS DX</b>       | SnapOPC Snap<br><br>EC Clone             | Fujitsu ETERNUS DX V10L22-1000 or higher<br><br>ETERNUS DX S2 series - 80, 90, 410, 440, 8100, 8700 | Local Copy<br><br>Thin Provisioning                                        | None                                                                                                                                                                                                              | iSCSI<br><br>Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)* | No HyperV<br><br>Revert is not supported.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>HITACHI DATA SYSTEMS AMS</b> | Copy-on-Write<br><br>Shadow Image        | AMS 100, 200, & 500<br><br>AMS 1000, 2100, 2300, & 2500                                             | Licenses for Copy-on-Write (COW) snapshot and Shadow Image                 | Device Manager 7.1.1 (or higher) Agent installed on Client and Proxy<br><br>Device Manager Server 7.1.1 (or higher) installed on any computer<br><br>RAID Manager (01-25-03/05 or higher) installed on Client and | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*              | No HyperV<br><br>The Virtual Server iDataAgent must be installed on a physical server and not on a virtual machine.<br><br>The Virtual Machine HotAdd feature is not supported.<br><br>The Virtual Server                                                                                                                                                                                                                          |

|                                      |                                      |                           |                                                            |                                                                                                                                                                                                                                                                             |                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------|--------------------------------------|---------------------------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                      |                                      |                           |                                                            | Proxy                                                                                                                                                                                                                                                                       |                                                                       | iDataAgent supports SnapProtect Backups when Hitachi Dynamic Link Manager (HDLM) plugin for VMWare is used for multipathing on the VMWare ESX Server.                                                                                                                                                                                                                                                                                                                                                   |
| <b>HITACHI DATA SYSTEMS USP/VSP</b>  | Copy-on-Write Shadow Image           | HDS USP, USPv, VSP        | Licenses for Copy-on-Write (COW) snapshot and Shadow Image | Device Manager 7.1.1 (or higher) Agent installed on Client and Proxy<br><br>Device Manager Server 7.1.1 (or higher) installed on any computer<br><br>RAID Manager (01-25-03/05 or higher) installed on Client and Proxy                                                     | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*              | No HyperV<br><br>COW support for USP volumes.<br><br>COW and SI support for VSP volumes. Dynamic Provisioned volumes (DP-VOL) are also supported.<br><br>The Virtual Server iDataAgent must be installed on a physical server and not on a virtual machine.<br><br>The Virtual Machine HotAdd feature is not supported.<br><br>The Virtual Server iDataAgent supports SnapProtect Backups when Hitachi Dynamic Link Manager (HDLM) plugin for VMWare is used for multipathing on the VMWare ESX Server. |
| <b>HITACHI DATA SYSTEMS HUS</b>      | Copy-on-Write Shadow Image           | HUS 100 series            | Licenses for Copy-on-Write (COW) snapshot and Shadow Image | Device Manager 7.2.1 (or higher) Agent installed on Client and Proxy<br><br>Device Manager Server 7.2.1 (or higher) installed on any computer<br><br>RAID Manager (01-26-03/02 or higher) installed on Client                                                               | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*              | No HyperV<br><br>The Virtual Server iDataAgent must be installed on a physical server and not on a virtual machine.<br><br>The Virtual Machine HotAdd feature is not supported.<br><br>The Virtual Server iDataAgent supports SnapProtect Backups when Hitachi Dynamic Link Manager (HDLM) plugin for VMWare is used for multipathing on the VMWare ESX Server.                                                                                                                                         |
| <b>HP EVA</b>                        | EVA Business Copy Snapshot and Clone | EVA                       | HP Business Copy EVA feature                               | HP SMI-S EVA on Server<br><br>Command View Version 9.1, 9.3, 10.0                                                                                                                                                                                                           | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*<br><br>iSCSI | No HyperV                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>HP (HDS OEM) XP, P9500 ARRAYS</b> | Copy-on-Write Shadow Image           | XP 12000 – 24000<br>P9500 | Licenses for Copy-on-Write (COW) snapshot and Shadow Image | HP StorageWorks Command View Advanced Edition Agent (Device Manager 7.1.1 or higher) installed on client and proxy computers<br><br>HP StorageWorks Command View Advanced Edition Server (Device Manager 7.1.1 or higher) installed on any computer.<br><br>HP StorageWorks | Fibre Channel<br><br>FCoE (Fibre Channel over Ethernet)*              | No HyperV The Virtual Machine HotAdd feature is not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                     |                                          |                                                                                                                                                                                                                                                                                                                   |                                                              |                                                                                                             |                                                                      |                                                                                                                                                 |
|-------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     |                                          |                                                                                                                                                                                                                                                                                                                   |                                                              | RAID Manager installed on client and proxy computers.                                                       |                                                                      |                                                                                                                                                 |
| <b>HP 3PAR</b>                      | Snapshot and Clone                       | InServ F200 3.1.2 or higher                                                                                                                                                                                                                                                                                       | Thin Provisioning (4096G) Virtual Copy                       | 3PAR SMI-S on Server                                                                                        | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*<br>iSCSI        | No HyperV<br><br>Also supports 2.3.1 (MU4) or higher except 3.1.1.342, 3.1.1 MU1 + Patch 10 and 3.1.1 (MU2)                                     |
| <b>IBM SVC</b>                      | Flash Copy<br>Space-efficient Flash Copy | SVC / V7000 6.1.0.7 or higher                                                                                                                                                                                                                                                                                     | FlashCopy                                                    | IBM SMI-S on Server                                                                                         | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*<br>iSCSI        | No HyperV                                                                                                                                       |
| <b>IBM XIV</b>                      | Snap                                     | ANY XIV Array                                                                                                                                                                                                                                                                                                     | Included                                                     | IBM XCLI 2.3 or higher on Client and proxy                                                                  | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*<br>iSCSI        | No HyperV                                                                                                                                       |
| <b>NETAPP E-SERIES (LSI ARRAYS)</b> | Snapshot<br>VolumeCopy                   | Dell MD Series - 3000(i), 3200(i), 3220(i)<br><br>IBM DS - 3200, 3300, 3400 - 3512, 3524, 3950, 4100, 4200, 4300, 4400, 4500 - 4700, 4800, 5020, 5100, 5300<br><br>SGI IS - 220, 350, 400, 4xxx, 5xxx<br><br>SGI TP - 9300(s), 9400(s), 9500(s)<br><br>Sun - 25xx, 61xx, 65xx, 6780, 9176, FLX210, FLX240, FLX280 | Snapshot<br>VolumeCopy                                       | LSI SMI-S on Server and server 10.10.6054 or higher                                                         | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*<br>iSCSI        | No HyperV<br><br>SAN Transport mode with Virtual Server iDataAgent is not supported as snapshots cannot be mapped to two different host groups. |
| <b>NETAPP</b>                       | Snapshot                                 | ONTAP 7.3.5 or ONTAP 8.1.x (7-mode only)                                                                                                                                                                                                                                                                          | FlexClone<br>SnapRestore<br>SnapVault/Mirror for replication | A server running NetApp DataFabric Manager server software 4.0.2 or later, or OnCommand UM 5.x is required. | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*<br>iSCSI<br>NFS | Supported on HP-UX running on Intel Itanium processors using Fibre Channel.                                                                     |
| <b>NIMBLE</b>                       | Snapshot                                 | 1.2.2.0-17686<br><br>1.3.0.0-22989                                                                                                                                                                                                                                                                                | Included                                                     | None                                                                                                        | iSCSI                                                                | Supported on x64-bit Windows platforms                                                                                                          |

**SUPPORTED HARDWARE ARRAYS FOR REPLICATED ENVIRONMENTS**

| VENDOR                                  | SNAPSHOT                | VERSION/FIRMWARE                                                         | REQUIRED LICENSING                                                         | REQUIRED SOFTWARE                                                                                                                                                   | PROTOCOL                                                             | NOTES/CAVEATS                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|-------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NETAPP WITH SNAPVAULT SNAPMIRROR</b> | SnapVault<br>SnapMirror | ONTAP 7.3.5 or higher<br>ONTAP 8.0.1, 8.0.2 and 8.1.0 (7-mode supported) | SnapVault/SnapMirror Primary and Secondary<br><br>FlexClone<br>SnapRestore | DataFabric Manager version 4.0.2 (Apr 2011) or OnCommand 5.0 and 5.1 with ONTAP 8.1.0<br><br>Provisioning Manager, Protection Manager, & Operation Manager Licenses | Fibre Channel<br>FCoE (Fibre Channel over Ethernet)*<br>iSCSI<br>NFS | Supported on HP-UX running on Intel Itanium processors using Fibre Channel.<br><br>vFilers not supported as a destination.<br><br>For vFiler NAS iDataAgent clients, indexing snapshot data is only supported with ONTAP 8.1.1 or later or if the physical file server containing the vfiler is entered into Array Management. |

\*Supported through Field Certification. Contact your Software Provider or Professional Services to see if the specific FCoE can be supported.

**SUPPORTED SOFTWARE SNAPSHOT ENGINES**

|  |
|--|
|  |
|--|

| VENDOR                 | SNAPSHOT       | VERSION/FIRMWARE | REQUIRED LICENSING                                                                                                                       | REQUIRED SOFTWARE        | NOTES/CAVEATS |
|------------------------|----------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|---------------|
| <b>DATA REPLICATOR</b> | Not applicable | Not applicable   | Local native snapshot license (Volume manager snapshot license or QSnap license)<br>Hardware Snap Engine or native snap or QSnap license | ContinuousDataReplicator |               |

LUNs should be from same storage array. LUNs from different storage arrays of same model/vendor or different models/vendors are not supported.

Dynamic Disks on Window Operating Systems are not supported.

When performing SnapProtect backup for a Windows MSCS Cluster, a separate proxy server (external to the cluster nodes) must be used for mount, backup and restore operations as disk signature conflicts may occur if these operations are performed from one of the servers in the cluster.

The use of iSCSI is not supported when performing SnapProtect operations on computers running Solaris.

Boot from SAN volumes is not supported.

When the client is running on a virtual machine, you can perform the SnapProtect backup of the Fibre channel RDM devices if they are located on the NetApp storage array. However, you cannot use Virtual Server *iDataAgent* to perform the SnapProtect backup in such scenario. You can use any other *iDataAgent*, such as File System *iDataAgent* or Exchange Database *iDataAgent* etc.

For information on the supported snapshot engines, see Hardware Snapshot Engine Compatibility Matrix.

## BACKUP TYPES

The following table lists the Agents supporting the SnapProtect backup and provides information about the various options supported by each of these Agents.

| AGENTS                          | FULL BACKUP | INCREMENTAL BACKUP | DIFFERENTIAL BACKUP | NOTES                                                                                                                                                                                                                                          |
|---------------------------------|-------------|--------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VIRTUAL SERVER (VMWARE)</b>  | √           | √                  |                     | Backup of VM Templates is not supported.<br>Virtual Server instances configured with ESX server are not supported. Instances should be configured using Virtual Center.<br>SRM is not supported.                                               |
| <b>EXCHANGE DATABASE</b>        | √           | √                  | √                   | SnapProtect backups are not supported on Exchange 2007 CCR Passive nodes.<br>DDR snapshots are not supported on Exchange 2010 DAG clients.<br>SRM is not supported.                                                                            |
| <b>ORACLE</b>                   | √           | √                  |                     | Incremental backups are applicable for Backup copies.<br>See Backup Copy Operations for more information.                                                                                                                                      |
| <b>MICROSOFT SQL SERVER</b>     | √           |                    | √                   | Transactional Log backups always use the traditional backup method. Log backups are stored in the Primary (classic) copy.                                                                                                                      |
| <b>NAS</b>                      | √           | √                  | √                   |                                                                                                                                                                                                                                                |
| <b>VIRTUAL SERVER (HYPER-V)</b> | √           |                    |                     | SnapProtect backups support online virtual machines with NetApp file servers.<br>Other storage array vendors use the traditional backup method. To perform a SnapProtect backup, the virtual machine must be offline.<br>SRM is not supported. |
| <b>SAP FOR ORACLE</b>           | √           |                    |                     |                                                                                                                                                                                                                                                |
| <b>DB2</b>                      | √           |                    |                     | Backup of partial databases is not supported.<br>Log files always use the                                                                                                                                                                      |

|                            |   |   |   |                                                                                                                                                                           |
|----------------------------|---|---|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            |   |   |   | traditional backup method.                                                                                                                                                |
| <b>UNIX FILE SYSTEM</b>    | ✓ | ✓ | ✓ | On Demand Backup Set is not supported for SnapProtect Backup.<br>Raw partitions in Unix are supported.<br>Mirrored Volume Manager/ZFS/ASM configuration is not supported. |
| <b>WINDOWS FILE SYSTEM</b> | ✓ | ✓ | ✓ | On Demand Backup Set is not supported for SnapProtect Backup.                                                                                                             |

## PLATFORMS

The following table lists the platforms supported for SnapProtect backup. The latest updates should be installed on all the platforms.

For AIX and Solaris, SnapProtect backups are supported for clients using the 32-bit packages of Calypso.

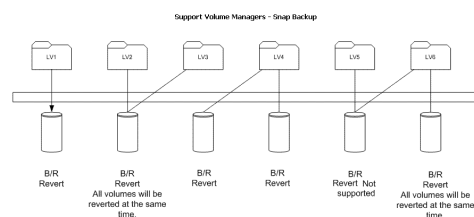
IntelliSnap with Veritas Volume Manager requires ALUA compliant LUNs (primary and secondary). For non-compliant ALUA LUNs, a workaround is explained in this Symantec KB article.

| OPERATING SYSTEM                                                               | CLUSTER SUPPORT                | FILE SYSTEMS                     | DATABASES                                                                 | APPLICATIONS                                                    |
|--------------------------------------------------------------------------------|--------------------------------|----------------------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------|
| <b>WINDOWS 2003 AND HIGHER</b>                                                 | MSCS                           | NTFS                             | SQL version 2005, 2008, 2012<br>Exchange 2003, 2007, 2010 – including DAG |                                                                 |
| <b>VMWARE ESX</b>                                                              |                                | iSCSI/FC/NFS datastores          | ESX vSphere 4.x & vSphere 5.0                                             |                                                                 |
| <b>AIX 5.3, 6.1, 7.1 (LPARS SUPPORTED, VIRTUAL SCSI DEVICES NOT SUPPORTED)</b> | Veritas Cluster, HACMP         | JFS, JFS2, VxFS                  | Oracle 10g R2, Oracle 11g R1 & R2, DB2 version 9 or higher                | SAP Brtools 7.0 & 7.1 on Oracle 10g R2, Oracle 11g R1 & R2      |
| <b>HP-UX 11 V2/V3 (PA-RISC AND ITANIUM)</b>                                    | Veritas Cluster, Service Guard | HFS, VxFS, VxCFS                 | Oracle 10g R2, Oracle 11g R1 & R2 DB2 version 9 or higher                 | SAP Brtools 7.0 & 7.1 on Oracle 10g R2, Oracle 11g R1 & R2      |
| <b>ORACLE ENTERPRISE LINUX 5.X AND 6.X</b>                                     |                                | ext2, ext3, reiserfs, VxFS       | Oracle 10g R2, Oracle 11g R1 & R2, DB2 version 9 or higher                | SAP Brtools 7.0, 7.1 & 7.2 on Oracle 10g R2, Oracle 11g R1 & R2 |
| <b>RED HAT/CENTOS LINUX 4.X AND 5.X</b>                                        | Linux Cluster Veritas Cluster  | ext2, ext3, reiserfs, VxFS       | Oracle 10g R2, Oracle 11g R1 & R2, DB2 version 9 or higher                | SAP Brtools 7.0 & 7.1 on Oracle 10g R2, Oracle 11g R1 & R2      |
| <b>RED HAT/CENTOS LINUX 6.X</b>                                                | Linux Cluster Veritas Cluster  | ext2, ext3, ext4, reiserfs, VxFS | Oracle 10g R2, Oracle 11g R1 & R2, DB2 version 9 or higher                | SAP Brtools 7.0, 7.1 & 7.2 on Oracle 10g R2, Oracle 11g R1 & R2 |
| <b>SOLARIS 10 SPARC (SOLARIS ZONES SUPPORTED)</b>                              | Sun Cluster Veritas Cluster    | UFS, VxFS, ZFS                   | Oracle 10g R2, Oracle 11g R1 & R2, DB2 version 9 or higher                | SAP Brtools 7.0, 7.1 & 7.2 on Oracle 10g R2, Oracle 11g R1 & R2 |
| <b>SOLARIS 11 EXPRESS</b>                                                      |                                | UFS, VxFS, ZFS                   |                                                                           |                                                                 |
| <b>SUSE LINUX ENTERPRISE SERVER 10.2 AND 11</b>                                | Veritas Cluster                | ext2, ext3, ext4, reiserfs, VxFS | Oracle 10g R2, Oracle 11g R1 & R2, DB2 version 9 or higher                | SAP Brtools 7.0 & 7.1 on Oracle 10g R2, Oracle 11g R1 & R2      |

The above list *does not* provide a comprehensive list of supported platforms for each agent. See System Requirements for information on the platforms supported by the individual Agents.

## SUPPORTED VOLUME MANAGERS

- Logical Volume Manager
  - All versions supported on AIX and Linux
  - Versions 1.0 and 2.x supported on HP-UX
- VERITAS Volume Manager (VxVM) 5.0 for AIX, Linux and Solaris
- Solaris ZFS Mirror
- Solaris Volume Manager



When using the Solaris Volume Manager, ensure that a

complete disk is used for a metaset. Also, ensure that the metaset is owned by single host and the ownership of the metaset is attained before performing the SnapProtect backup operations.

**Supported Configurations:**

- One Physical Volume containing one Logical Volume
- One Physical Volume containing one or more Logical Volumes
- Multiple Physical Volumes containing one Logical Volume
- Multiple Physical Volumes containing one or more Logical Volume

The adjacent diagram summarizes the Volume Manager support for SnapProtect backup.

**MULTIPATH I/O SUPPORT**

- For EMC CLARiiON, the SnapProtect backup is supported on the following Multipath I/O software. This support is provided using the SNAP\_WITH\_MULTIPATH\_SOFTWARE registry key.
  - EMC Powerpath on AIX, Linux and Solaris.
- For Dell EqualLogic, install Dell EqualLogic Host Integration Tools package to support Multipath I/O.
- HP PVlinks, Solaris MPxIO, Linux Device Mapper and AIX MPIO are supported in HPUX, Solaris, Linux and AIX respectively.
- VXVM DMP is supported in AIX, Solaris and HPUX.
- HDLM is not a supported MPIO solution with SnapProtect.