

User Guide - SnapProtect

GENERAL

OVERVIEW

PRE-DEPLOYMENT

SNAPPROTECT SUPPORT

GETTING STARTED

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

ADVANCED

CLIENTS

VIRTUAL SERVER (VMWARE)

EXCHANGE DATABASE

ORACLE (UNIX)

MICROSOFT SQL SERVER

NAS

VIRTUAL SERVER (MICROSOFT HYPER-V)

SAP FOR ORACLE (UNIX)

DB2 (UNIX)

UNIX FILE SYSTEM

WINDOWS FILE SYSTEM

STORAGE ARRAYS

3PAR

DELL COMPELLENT

DELL EQUALLOGIC

EMC CLARIION

EMC SYMMETRIX

HITACHI DATA SYSTEMS

HP EVA

IBM SVC

IBM XIV

LSI

NETAPP

DATA REPLICATOR

NIMBLE

TOOLS

SNAPTEST

BEST PRACTICES

FAQS

TROUBLESHOOTING

SNAP MINING

VIRTUAL SERVER (VMWARE)

ACCESSING EXCHANGE DATA FROM VMWARE SNAPSHOTS

EXCHANGE MAILBOX

ACCESSING EXCHANGE DATA FROM DATABASE SNAPSHOTS

EXCHANGE MAILBOX ARCHIVER

ACCESSING ARCHIVED EXCHANGE DATA FROM DATABASE SNAPSHOTS

SHAREPOINT SERVER

ACCESSING SHAREPOINT DATA FROM SQL DATABASE SNAPSHOTS

SNAP MINING SUPPORT

SnapProtect™ Backup - Overview

TABLE OF CONTENTS

Introduction

Advantages of using SnapProtect Backup

How Does SnapProtect Work

Terminology

INTRODUCTION

The SnapProtect™ backup enables you to create a point-in-time snapshot of the data to be used for various data protection operations. SnapProtect backup works in conjunction with software and hardware storage arrays to provide snapshot functionality for data protection operations. An effective way to backup live data is to temporarily quiesce it, take a snapshot, and then resume live operations.

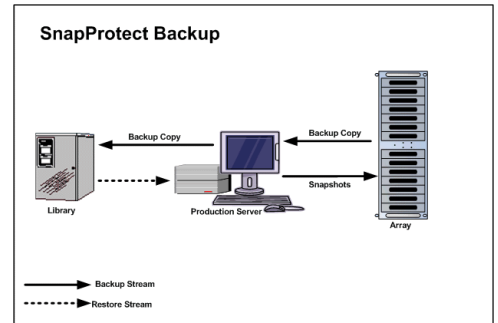
You can use the SnapProtect backup to perform any level of backups (e.g. Full, Incremental, or Differential). The backup types supported for SnapProtect backup varies for different agents. During an incremental or a differential SnapProtect backup even though the snapshot of a complete volume is created, only new or data changed since the last backup is available for recovery operations. When you switch from a snap to a traditional backup or vice versa, the next job is converted to a full backup.

See SnapProtect Backup - Support for the support related information for the SnapProtect backup.

WHERE TO GO NEXT

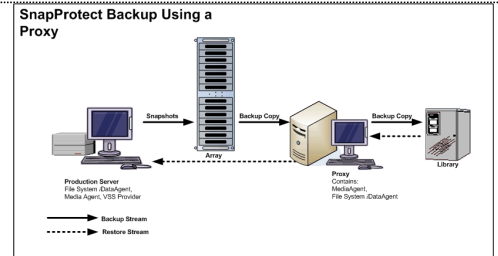
Getting Started - SnapProtect

Walks you through the process of installing and configuring SnapProtect.



PROXY SERVER

While performing a SnapProtect backup or any subsequent operations, you can use a proxy server to reduce the load on the production server. Also, the backup copy operation will use the proxy to move the snap to backup media. The use of a proxy server to perform SnapProtect operations is supported when a hardware storage array is used for performing the SnapProtect backup.



ADVANTAGES OF USING SNAPPROTect BACKUP

The following table lists some of the advantages of using SnapProtect backup over other available backup solutions.

FEATURE SUPPORT	GENERIC SOFTWARE SOLUTION	CALYPSO SNAPPROTect BACKUP
Backup to Tape		✓
During incremental or log backup only relevant incremental or log data is moved to media enabling significant reduction in media usage.		✓
Hardware Agnostic - No dependency on the hardware array vendor changes		✓
Snapshot copy, backup copy, and tape copy creation and management are seamless. Application aware snapshots creation can be scheduled. The snapshots can be cataloged/indexed for restore and movement to media based on policies.		✓
To reduce load on the production server, a proxy server can be used for operations like movement to media, integrity check.		✓
Restores can be performed directly from media to the application server.		✓
Ability to mix and match SnapProtect backup with traditional backups. You can perform full SnapProtect backups combined with incremental log backups being moved to media and still perform a seamless restore.		✓
All data management operations can be performed from the CommCell Console.		✓

HOW DOES SNAPPROTect BACKUP WORK

The SnapProtect backup includes the following operations:

Backup job is scheduled using the CommCell Console. When the backup job is started:

- The array is accessed to create a snapshot.
- The snapshot is mounted on the proxy or source computer for post backup operations.
- The snapshot is unmounted.

This snapshot is used for backup copy operations. This can also be used for restore/mount operations.

During the Backup Copy operations:

- The snapshot is mounted to the source or proxy computer.
- The mounted snapshot is treated like file system and the required contents are read.
- The file system backup is performed to Primary Copy of the storage policy.
- When the backup copy job is finished, the snapshot is unmounted.

Data Aging:

- The jobs for the snapshot are pruned based on the retention policy of the snapshot copy.
- The snapshots related to the pruned jobs are deleted from the array periodically.

TERMINOLOGY

The SnapProtect Backup documentation uses the following terminology:

STORAGE DEVICE	A device used for backup or archival purposes.
STORAGE ARRAY	A high-end, intelligent disk storage system. The SnapProtect software is designed to work in conjunction with the snapshot ability built into the storage array.
PROXY	A computer other than the production server on which you can perform SnapProtect operations. Using a proxy often results in less load on the production server.
SNAPSHOT COPY	An additional copy of the protected data which is used in SnapProtect operations.

Pre-Deployment Test - Unix

Unix | Windows

TABLE OF CONTENTS

Installation


Perform test

INSTALLATION

1. Mount the **Software Install Package** to the client computer.
2. The product banner and other information is displayed.
Press **Enter** to continue.
3. Read the license agreement. Type **y** and press **Enter** to continue.
4. Enter **2** to select the **Advance options**.
5. Enter **2** to **Pre-install software Components [De-couple mode]**.
6. 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 name and IP addresses depend on the computer in which the software is installed and may be different from the example shown.
7. Press **Enter**.
8. Type the appropriate number to install **MediaAgent** and **Unix File System iDataAgent**.
Press **Enter**.

VIEW VIDEO

Click  to view a video for performing diagnostic test of your environment for SnapProtect operations.

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]

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

- [Custom Package Creator]
- 1) Create a custom install package
- [De-coupled Installer]
- 2) Pre-install software Components (De-coupled Mode)
- [Integrated File Archiver]
- 3) File System iDataAgent with Archiving Enabler
- [Customized Cluster Agents]
- 4) Veritas Cluster Agents
- [Third Party Connector]
- 5) Symantec NetBackup Agent
 - 6) IBM Tivoli Storage Manager

[Done]

9) Exit this menu

Your choice: [1] 2

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.

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 client.company.com
Select the Calypso module that you would like to install

- [] 1) Media Agent [1301] [CVGxMA]
[] 2) File System IDA [1101] [CVGxIDA]

> >>>>>> NEXT PAGE >>>>>>>

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

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

10. Press **Enter**.

11. 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.

12. Press **Enter**.

It is recommended to download the latest Service pack(s). Type **Yes** and press **Enter** to automatically install the available updates during installation.

13. 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:

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

14. 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.

15. Press **Enter**.

16. Type the **Group name** and press **Enter**.

```
=help]
Enter number(s)/one of "a,n,r,q,d,>,<,>?" here:
Install Calypso on physical machine client.company.com
Select the Calypso module that you would like to install
[ ] 1) Media Agent          [1301] [CVGxMA]
[ ] 2) File System IDA      [1101] [CVGxIDA]
>) >>>>>>> NEXT PAGE >>>>>>>
[a=all n=none r=reverse q=quit d=done >=next <=previous ?
=help]
Enter number(s)/one of "a,n,r,q,d,>,<,>?" here: 2
Do you want to use the agents for restore only without
consuming licenses? [no]
Installation Scripts Pack provides extra functions and
latest support and fix performed during setup time. Please
specify how you want to get this pack.
If you choose to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.
1) Download from the software provider website.
2) Use the one in the installation media
3) Use the copy I already have by entering its unix path
Your choice: [1] 2
Keep Your Install Up to Date - Latest Service Pack
Latest Service Pack provides extra functions and latest
support and fix for the packages you are going to install.
You can download the latest service pack from software
provider website.
If you decide to download it from the website now, please
make sure you have internet connectivity at this time.
This process may take some time depending on the internet
connectivity.
Do you want to download the latest service pack now? [no]
Press <ENTER> to continue ...
Please specify where you want us to install Calypso
binaries.
It must be a local directory and there should be at least
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 Calypso 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 Calypso processes, all
temporary and configuration files will be created with -
rw-rw-rw permissions.
If you're planning to backup Oracle DB you should use
"dba" group.
Would you like to assign a specific group to Calypso?
[yes]
Please enter the name of the group which will be assigned
to all Software files and on behalf of which all Software
```

Press **Enter** again.

17. 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**.

18. The installation is now complete.

processes will run.

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

Group name: dba

REMINDER

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

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

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

Please enter the port numbers.

Port Number for CVD : [8600]

Port Number for EvMgrC: [8602]

Done.

REMINDER - You must register the client before decoupled installation is considered complete.

Thank you for choosing Bull.

PERFORM TEST

The following procedure provides step-by-step instructions to configure and test your snap environment.

1. Create a Lun on the array and map it to the client computer.
Ensure that the Lun is visible on the client computer as a device node.
2. Use the mapped device node to create a Volume Group.

For example, use the following command:

On AIX

```
mkvg -y vg_name hdisk12
```

On Linux:

```
pvccreate /dev/sdd
```

```
vgcreate vg_name /dev/sdd
```

```
vgchange -a y vg_name
```

3. Create a Logical Volume in the Volume Group.

For example, use the following command:

On AIX:

```
mklv -y lv_name vg_name 2G
```

On Linux:

```
lvcreate -n lv_name -L 2G vg_name
```

4. Create a File System on the Logical Volume.

For example, use the following command:

On AIX:

```
crfs -v jfs2 -d lv_name -a logname=INLINE -m /snaptest
```

On Linux:

```
mke2fs lv_name
```

5. Create a directory to mount snapshots.
6. Use the following commands to run the Snaptest tool:
 - Locate /opt/Calypso folder by running the below command.

```
[root@ntr Calypso]# cd /opt/Calypso/Base
```

- [root@ntr Calypso]# ./SnapTest

If you have multiple instance installed, run the following command for SnapTest tool:

```
[root@ntr Calypso]# ./Base/SnapTest -vm Instance<XXX>
```

7. Press **Enter**.

This tool helps to perform operations such as...

```
-> Automatic Snap Tests
```


8. Press **Enter**.

```
-> Individual Snap Tests
-> Hardware Snapshot Engine Detection
-> SCSI Inquiry
-> Scan HBA/IQN Adapters
```

NOTE: Please make sure that the mount points used for this test are not being used by any other application. If they are in use, it may cause data corruption or data loss. Please refer to our online documentation for list of supported Operating systems, Hardware Snapshot engines and File systems.

Press <ENTER> to continue...

```
SnapTest Version      Main Menu
```

```
-----
Perform automatic snap tests or launch Advanced
Operations such as Array Configuration, Snapshot
Engine Detection etc. Automatic snap tests take one
or more source mounts to snap and performs series of
Snap related operations on them. In order to perform
these snap operations, array configuration such as
array id, control host and user credentials is
required. If no array configuration is found,
Automatic Snaptests takes you to Array Configuration
screen.
```

1. Automatic Snap Tests
2. Advanced Operations
0. Exit

Choose your option [1]:

9. Type **Y** and press **Enter**.

```
SnapTest              Automatic Snap Operations
```

```
-----
-
```

We will perform the following operations on the given mount point[s].

- Create snapshots
- Mount snapshots
- Unmount snapshots
- Revert original volumes to snapshots
- Delete snapshots

WARNING:

Revert is inherently risky and can cause data loss.

Do you want to perform revert operation as part of this test? [Y/N] [N] : Y

10. Specify the path of mount directory and press **Enter**.
Enter all the mount points that you want to test.

Enter source mount paths to snap (separate by commas, if more than one) : /snap1

11. Press **Enter** to add the detected array.

```
SnapTest              Automatic Snap Operations
```

```
-----
-----
```

Source Mount Point : /snap1

Detecting underlying devices... /dev/sdh

Detecting snapshot engine... <Array Name> SNAP

No [<Array Name> SNAP] arrays found in database. Array configuration is required to do snap operations.

Do you want to add <Array Name> Array? [Y/N] [Y] :

12. Specify the following information for the detected array:

- Array ID
- Control host name/ip
- User name
- Password
- Reenter password
- Device group

```
SnapTest              Add Array
```

```
-----
```

Vendor : <Array Name>

Enter array ID :

Enter control host name/ip :

Enter user name :

- Use only devices belonging to the above device group [y/n]

13. The setup is tested for snapshot operations (create, mount, unmount, revert, and delete).

The snap test is now complete. You can now use this environment for performing SnapProtect operations.

14. Type **0** and press **Enter**.

```

Enter password :
Enter password again :
Enter device group :

SnapTest          Automatic Snap Operations
-----
Mount points to be snapped : /snap1
Engine for /snap1 : <Array Name> SNAP
Creating snapshot... SUCCESS
Snapshot name : SP_805326_805326_-1
Mounting snapshot...SUCCESS
Unmounting snapshot... SUCCESS
Reverting to snapshot... SUCCESS
Deleting snapshot... SUCCESS

Congratulations!!! Automatic Snap test completed
successfully.

Press <ENTER> to continue...

SnapTest Version      Main Menu
-----

Perform automatic snap tests or launch Advanced
Operations such as Array Configuration, Snapshot
Engine Detection etc. Automatic snap tests take one
or more source mounts to snap and performs series of
Snap related operations on them. In order to perform
these snap operations, array configuration such as
array id, control host and user credentials is
required. If no array configuration is found,
Automatic Snaptests takes you to Array Configuration
screen.

1. Automatic Snap Tests
2. Advanced Operations
0. Exit

Choose your option [1]:

```

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

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
DELL COMPELLENT	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 FCoE (Fibre Channel over Ethernet)* iSCSI	Supported on Windows, Linux and VMware. No HyperV Compellent Live Volume feature is not supported.
DELL EQUALLOGIC	Snapshot Clone	4.2.0	Included	None	iSCSI	On Red Hat Linux computers using version 5.0, only 32-bit is supported. No HyperV, or UNIX. Boot from SAN volumes is not supported.
EMC CLARIION	SnapView Snap SnapView Clone	CX500 / CX700 CX3-10 thru CX3-80 CX4-120 thru CX4-960	SnapView Snapshot/Clone Solutions Enabler Licensing	Solutions Enabler 6.5.1 or higher on Client and Proxy Navisphere CLI on Client and Proxy NaviAgent on Client and Proxy	Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap

						operations. Not supported on HP-UX
EMC VNX	SnapView Snap SnapView Clone	VNX 5100, 5300, 5500, 5700, 7500	SnapView Snapshot/Clone Solutions Enabler Licensing	Solutions Enabler 7.1 or higher on Client and Proxy Unisphere CLI on Client and Proxy Unisphere Host Agent on Client and Proxy	Fibre Channel FCoE (Fibre Channel over Ethernet)* iSCSI	No HyperV VMware with NFS datastores are not supported. iSCSI PowerPath LUNs are not supported. Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations. For configuring a VNX array, refer to the step-by-step instructions provided for EMC Clariion. Not supported on HP-UX
EMC CELERRA	SnapSure Snap	DART 5.5 or Newer	SnapSure Snap License Solutions Enabler Licensing	Solutions Enabler 6.5.1 or higher on Client and Proxy Navisphere CLI on Client and Proxy	NFS	Supported on VMware 4.x. No HyperV Not supported on HP-UX
EMC SYMMETRIX	TimeFinder Snap TimeFinder Mirror	DMX3 or Newer	TimeFinder Snap, Mirror, Clone Licenses Solutions Enabler Licensing	Solutions Enabler 6.4 or higher on Client and Proxy	Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV Remote SymApi Server is not supported. Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
EMC VMAX	TimeFinder Snap, Mirror and Clone	VMAX	TimeFinder Snap, Mirror, Clone Licenses Solutions Enabler Licensing	Solutions Enabler 7.2 or higher on Client and Proxy	Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV Client Components (SYMCLI) are required only during the initial one-time configuration. Base Components (with SYMAPI) are necessary and required for all snap operations.
FUJITSU ETERNUS DX	SnapOPC Snap EC Clone	Fujitsu ETERNUS DX V10L22-1000 or higher ETERNUS DX S2 series - 80, 90, 410, 440, 8100, 8700	Local Copy Thin Provisioning	None	iSCSI Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV Revert is not supported.
HITACHI DATA SYSTEMS AMS	Copy-on-Write Shadow Image	AMS 100, 200, & 500 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 Device Manager Server 7.1.1 (or higher) installed on any computer RAID Manager (01-25-03/05 or higher) installed on Client and	Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV The Virtual Server iDataAgent must be installed on a physical server and not on a virtual machine. The Virtual Machine HotAdd feature is not supported. 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.
HITACHI DATA SYSTEMS USP/VSP	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 Device Manager Server 7.1.1 (or higher) installed on any computer RAID Manager (01-25-03/05 or higher) installed on Client and Proxy	Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV COW support for USP volumes. COW and SI support for VSP volumes. Dynamic Provisioned volumes (DP-VOL) are also supported. The Virtual Server iDataAgent must be installed on a physical server and not on a virtual machine. The Virtual Machine HotAdd feature is not supported. 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.
HITACHI DATA SYSTEMS HUS	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 Device Manager Server 7.2.1 (or higher) installed on any computer RAID Manager (01-26-03/02 or higher) installed on Client	Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV The Virtual Server iDataAgent must be installed on a physical server and not on a virtual machine. The Virtual Machine HotAdd feature is not supported. 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.
HP EVA	EVA Business Copy Snapshot and Clone	EVA	HP Business Copy EVA feature	HP SMI-S EVA on Server Command View Version 9.1, 9.3, 10.0	Fibre Channel FCoE (Fibre Channel over Ethernet)* iSCSI	No HyperV
HP (HDS OEM) XP, P9500 ARRAYS	Copy-on-Write Shadow Image	XP 12000 – 24000 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 HP StorageWorks Command View Advanced Edition Server (Device Manager 7.1.1 or higher) installed on any computer. HP StorageWorks	Fibre Channel FCoE (Fibre Channel over Ethernet)*	No HyperV The Virtual Machine HotAdd feature is not supported.

				RAID Manager installed on client and proxy computers.		
HP 3PAR	Snapshot and Clone	InServ F200 3.1.2 or higher	Thin Provisioning (4096G) Virtual Copy	3PAR SMI-S on Server	Fibre Channel FCoE (Fibre Channel over Ethernet)* iSCSI	No HyperV Also supports 2.3.1 (MU4) or higher except 3.1.1.342, 3.1.1 MU1 + Patch 10 and 3.1.1 (MU2)
IBM SVC	Flash Copy Space-efficient Flash Copy	SVC / V7000 6.1.0.7 or higher	FlashCopy	IBM SMI-S on Server	Fibre Channel FCoE (Fibre Channel over Ethernet)* iSCSI	No HyperV
IBM XIV	Snap	ANY XIV Array	Included	IBM XCLI 2.3 or higher on Client and proxy	Fibre Channel FCoE (Fibre Channel over Ethernet)* iSCSI	No HyperV
NETAPP E-SERIES (LSI ARRAYS)	Snapshot VolumeCopy	Dell MD Series - 3000(i), 3200(i), 3220(i) IBM DS - 3200, 3300, 3400 - 3512, 3524, 3950, 4100, 4200, 4300, 4400, 4500 - 4700, 4800, 5020, 5100, 5300 SGI IS - 220, 350, 400, 4xxx, 5xxx SGI TP - 9300(s), 9400 (s), 9500(s) Sun - 25xx, 61xx, 65xx, 6780, 9176, FLX210, FLX240, FLX280	Snapshot VolumeCopy	LSI SMI-S on Server and server 10.10.6054 or higher	Fibre Channel FCoE (Fibre Channel over Ethernet)* iSCSI	No HyperV SAN Transport mode with Virtual Server iDataAgent is not supported as snapshots cannot be mapped to two different host groups.
NETAPP	Snapshot	ONTAP 7.3.5 or ONTAP 8.1.x (7-mode only)	FlexClone SnapRestore 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 FCoE (Fibre Channel over Ethernet)* iSCSI NFS	Supported on HP-UX running on Intel Itanium processors using Fibre Channel.
NIMBLE	Snapshot	1.2.2.0-17686 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
NETAPP WITH SNAPVAULT SNAPMIRROR	SnapVault SnapMirror	ONTAP 7.3.5 or higher ONTAP 8.0.1, 8.0.2 and 8.1.0 (7-mode supported)	SnapVault/SnapMirror Primary and Secondary FlexClone SnapRestore	DataFabric Manager version 4.0.2 (Apr 2011) or OnCommand 5.0 and 5.1 with ONTAP 8.1.0 Provisioning Manager, Protection Manager, & Operation Manager Licenses	Fibre Channel FCoE (Fibre Channel over Ethernet)* iSCSI NFS	Supported on HP-UX running on Intel Itanium processors using Fibre Channel. vFilers not supported as a destination. 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
DATA REPLICATOR	Not applicable	Not applicable	Local native snapshot license (Volume manager snapshot license or QSnap license) 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
VIRTUAL SERVER (VMWARE)	√	√		Backup of VM Templates is not supported. Virtual Server instances configured with ESX server are not supported. Instances should be configured using Virtual Center. SRM is not supported.
EXCHANGE DATABASE	√	√	√	SnapProtect backups are not supported on Exchange 2007 CCR Passive nodes. DDR snapshots are not supported on Exchange 2010 DAG clients. SRM is not supported.
ORACLE	√	√		Incremental backups are applicable for Backup copies. See Backup Copy Operations for more information.
MICROSOFT SQL SERVER	√		√	Transactional Log backups always use the traditional backup method. Log backups are stored in the Primary (classic) copy.
NAS	√	√	√	
VIRTUAL SERVER (HYPER-V)	√			SnapProtect backups support online virtual machines with NetApp file servers. Other storage array vendors use the traditional backup method. To perform a SnapProtect backup, the virtual machine must be offline. SRM is not supported.
SAP FOR ORACLE	√			
DB2	√			Backup of partial databases is not supported. Log files always use the

				traditional backup method.
UNIX FILE SYSTEM	✓	✓	✓	On Demand Backup Set is not supported for SnapProtect Backup. Raw partitions in Unix are supported. Mirrored Volume Manager/ZFS/ASM configuration is not supported.
WINDOWS FILE SYSTEM	✓	✓	✓	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.

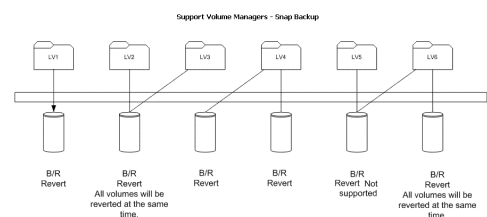
IntelliSnap with Veritas Volume Manager requires ALUA compliant LUNs (primary and secondary). For non-compliant ALUA LUNs, a workaround is explained in this Symantec KB article.

OPERATING SYSTEM	CLUSTER SUPPORT	FILE SYSTEMS	DATABASES	APPLICATIONS
WINDOWS 2003 AND HIGHER	MSCS	NTFS	SQL version 2005, 2008, 2012 Exchange 2003, 2007, 2010 - including DAG	
VMWARE ESX		iSCSI/FC/NFS datastores	ESX vSphere 4.x & vSphere 5.0	
AIX 5.3, 6.1, 7.1 (LPARS SUPPORTED, VIRTUAL SCSI DEVICES NOT SUPPORTED)	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
HP-UX 11 V2/V3 (PA-RISC AND ITANIUM)	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
ORACLE ENTERPRISE LINUX 5.X AND 6.X		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
RED HAT/CENTOS LINUX 4.X AND 5.X	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
RED HAT/CENTOS LINUX 6.X	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
SOLARIS 10 SPARC (SOLARIS ZONES SUPPORTED)	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
SOLARIS 11 EXPRESS		UFS, VxFS, ZFS		
SUSE LINUX ENTERPRISE SERVER 10.2 AND 11	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.

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

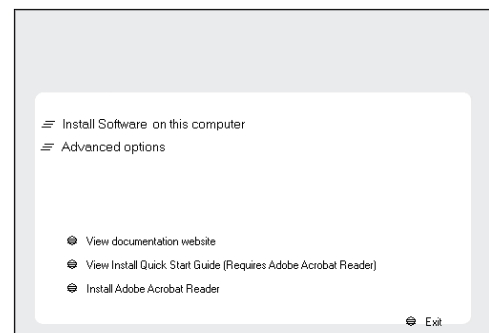
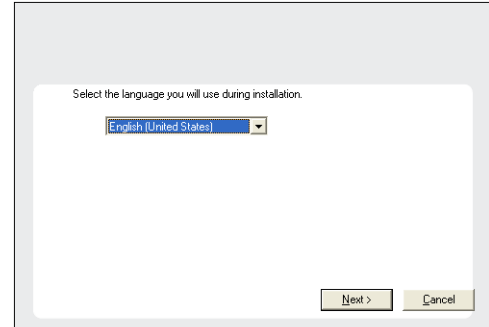
Review the licenses required for the SnapProtect feature.

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.

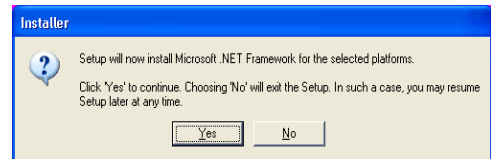
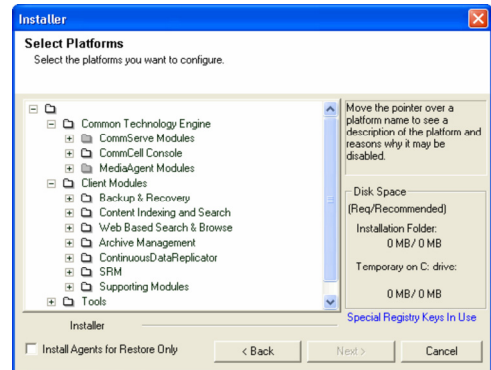
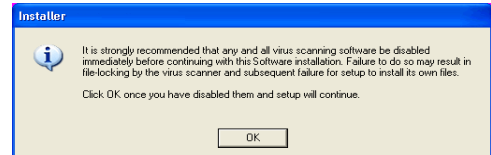
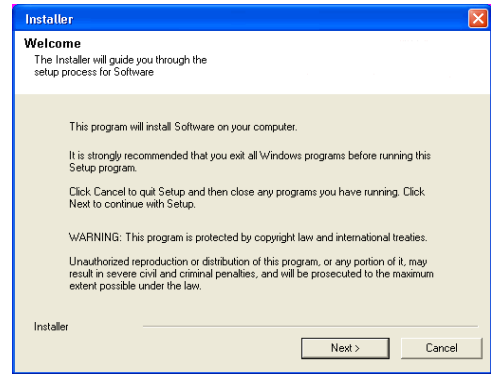
NOTES

- 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**.

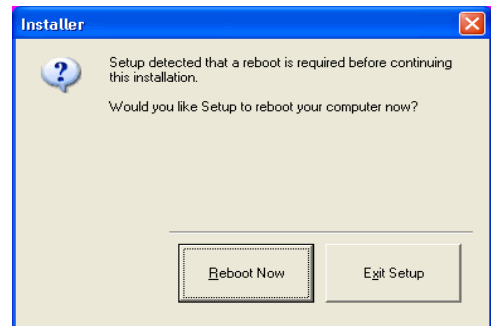
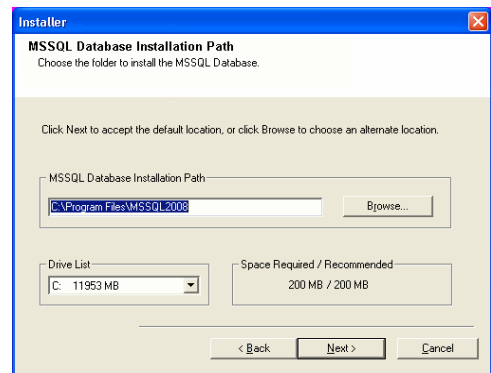
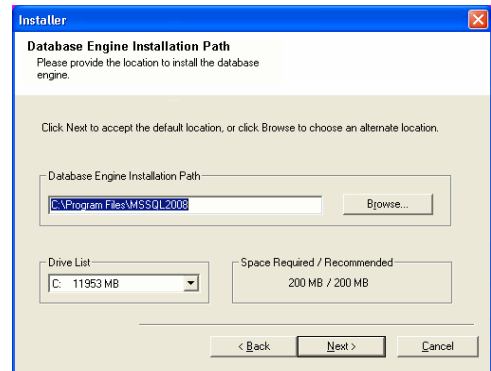
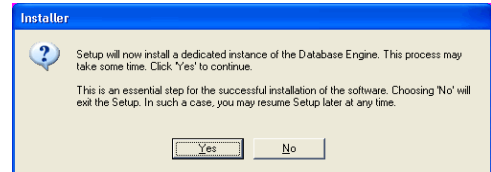
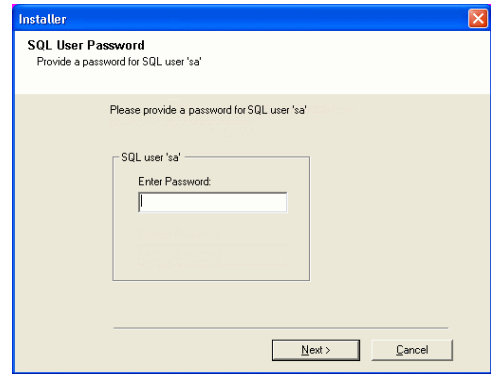
NOTES

- 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.

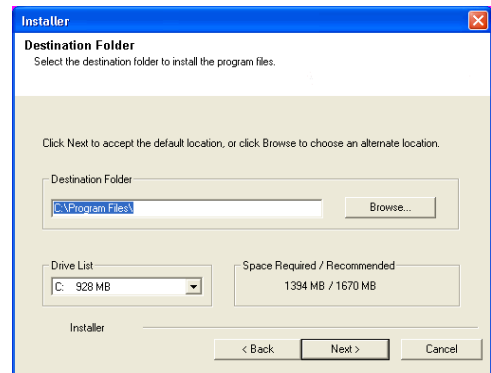
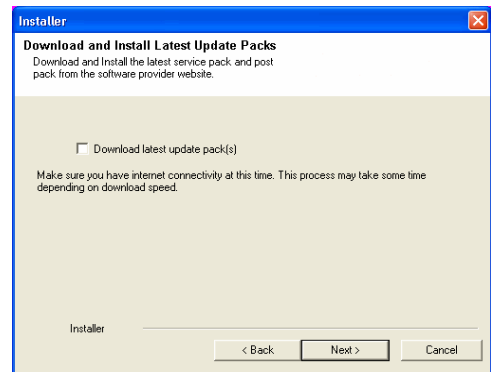
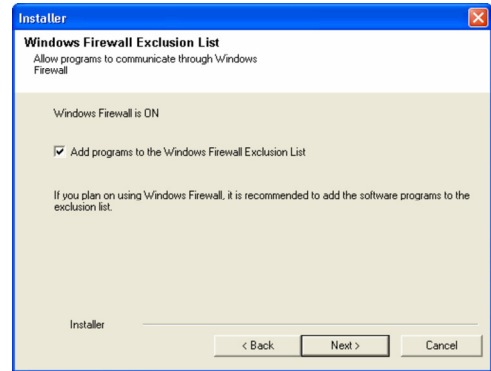
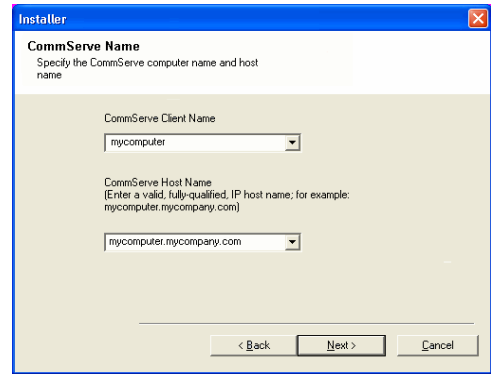
19. Verify the location of the database.

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.

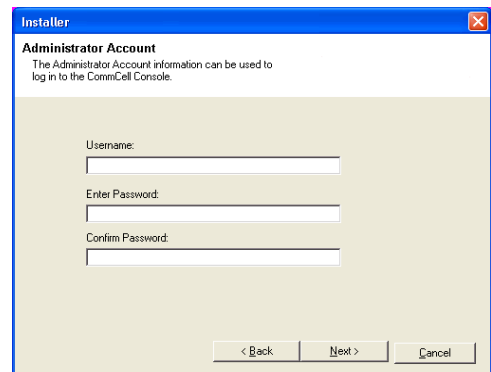
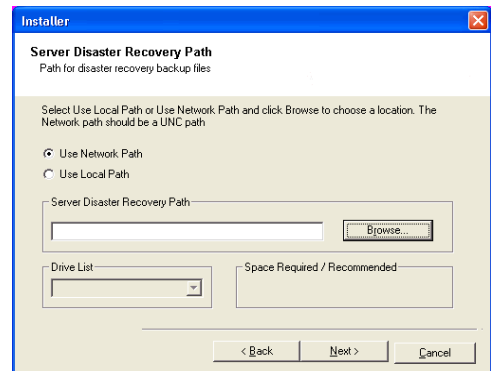
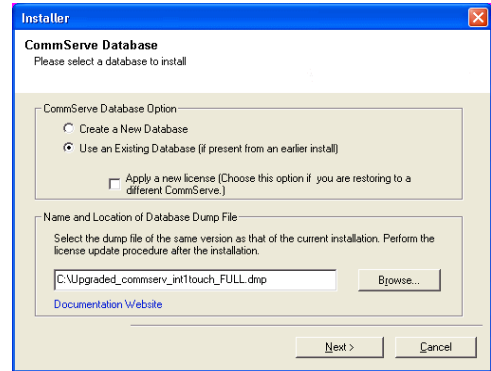
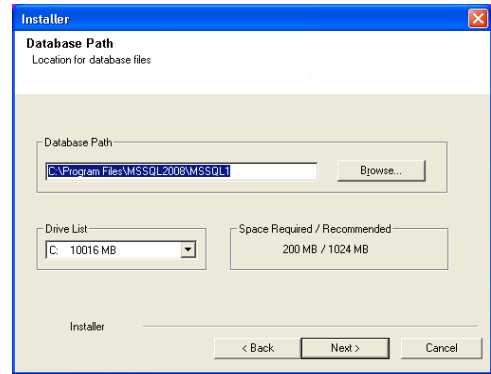
22. Enter the **CommCell Username** and **CommCell Password**.

Click **Next**.

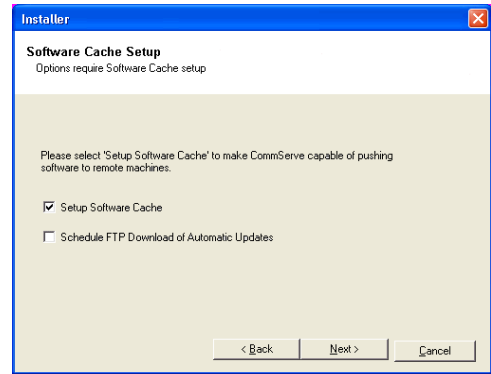
Make note of the **CommServe Username** and **CommCell Password**.

This is needed later to launch the CommCell Console.

23. Click **Next**.



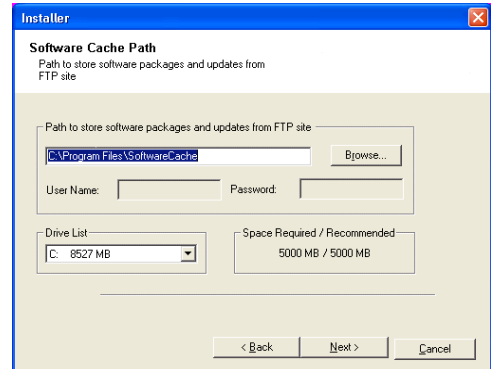
24. Verify the location where the update files from the FTP site should be stored.
 Click **Browse** to change the default location.
 Click **Next**.



25. Click **Next**.

NOTES

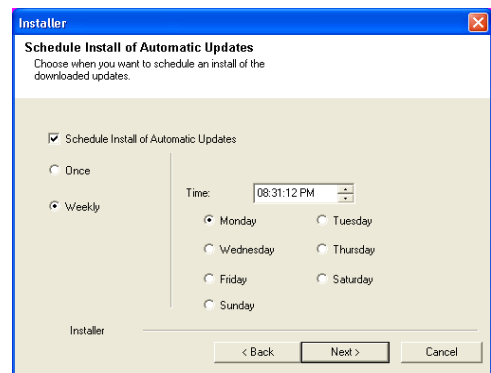
- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.



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.

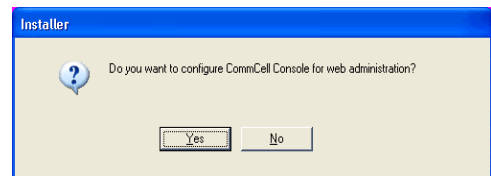


27. Select **Yes** to stop Removable Storage Services on the MediaAgent.

NOTES

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

Click **Next**.



28. Click **OK**.

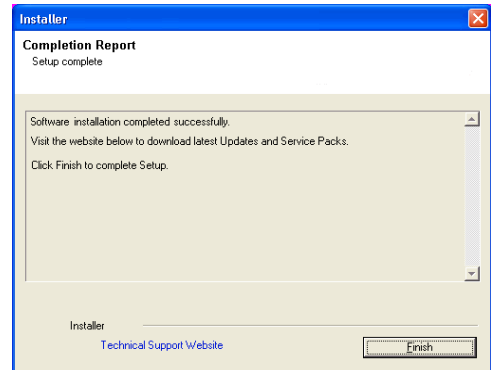
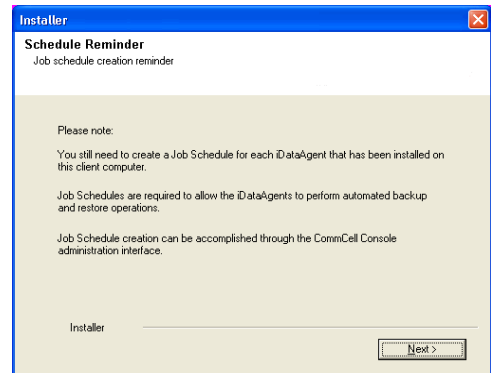
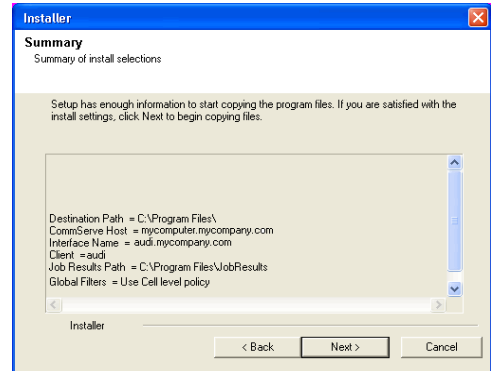
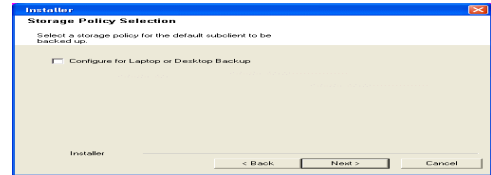
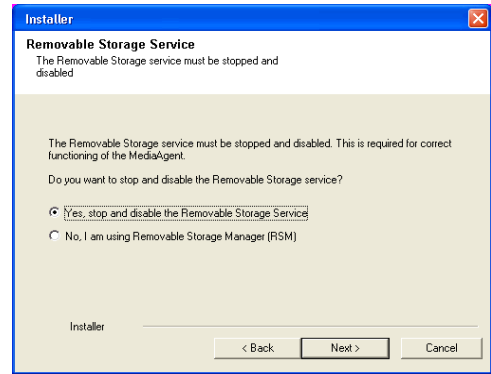
29. Click **Next**.

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**.



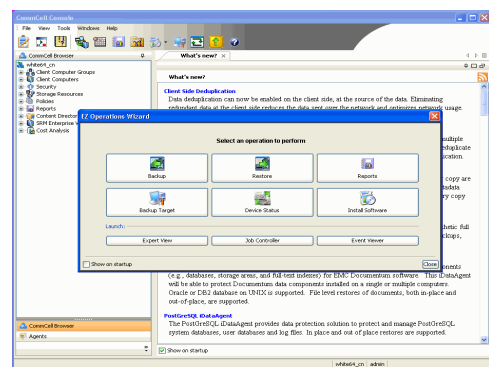
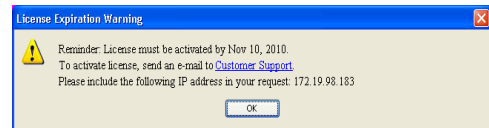
Getting Started

◀ 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:

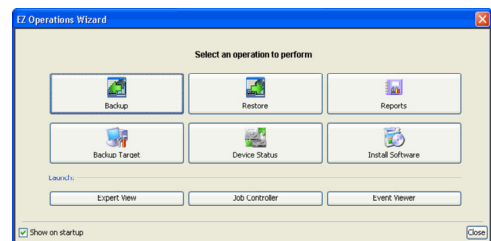
- **Option 1:** Configuring a Disc Device
- **Option 2:** Configuring a Tape Device

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

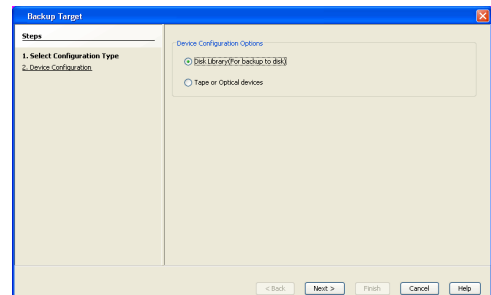
1. Click the **Backup Target** button on **EZ Operations Wizard**.



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

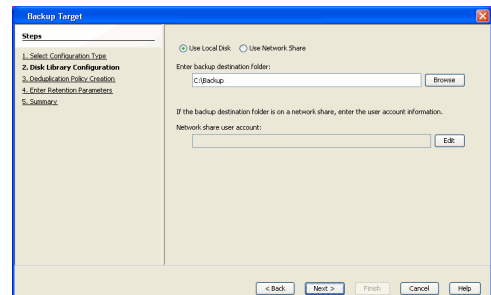


2. Click **Disc Library (For backup to disc)** and click **Next**.

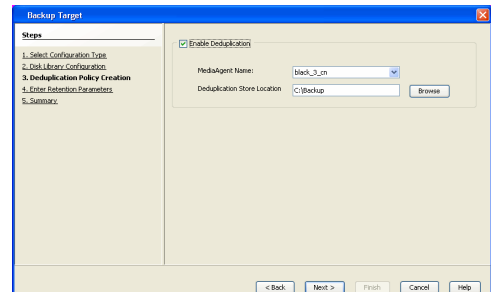


3.
 - Click **Use Local Disk**.
 - Type the name of the folder in which the disc library must be located in the **Enter backup destination folder** box or click the **Browse** button to select the folder.
 - Click **Next**.

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

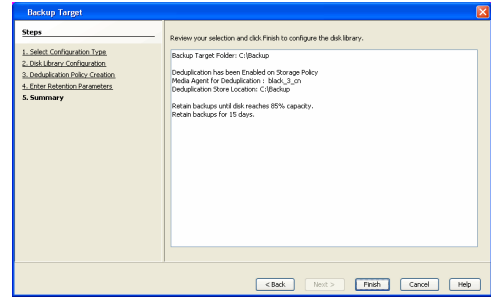
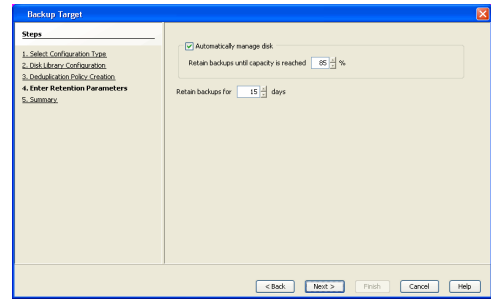


4.
 - Click and select the **Enable Deduplication** option - this will save disc space for storage.
 - Type the name of the folder in which the deduplication database must be located in the **Deduplication Store location** box or click the **Browse** button to select the folder.
 - Click **Next**.



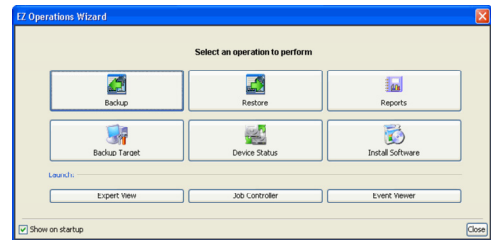
5. Click **Next**.

- Click **Finish**.



OPTION 2: CONFIGURING A TAPE DEVICE

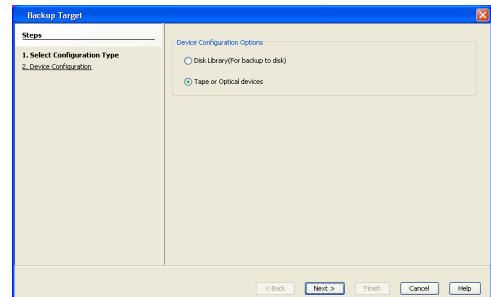
- Click the **Backup Target** button on **EZ Operations Wizard**.



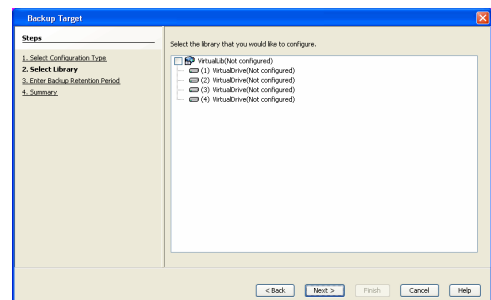
If the **EZ Operations Wizard** is not displayed double-click the icon in the toolbar.



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

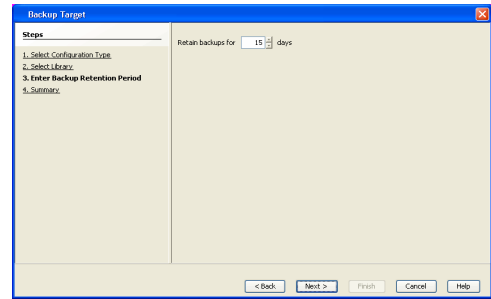


- Click and select the library you wish to configure.
Click **Next**.

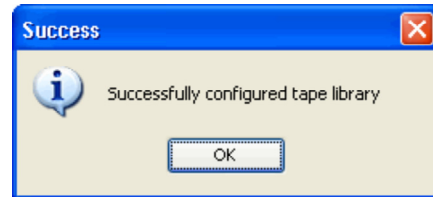
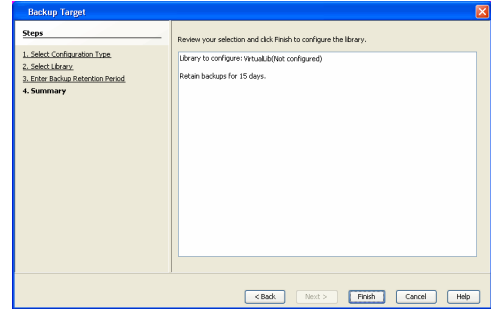


- Click **Next**.

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.

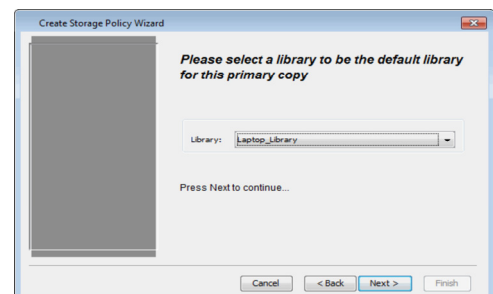
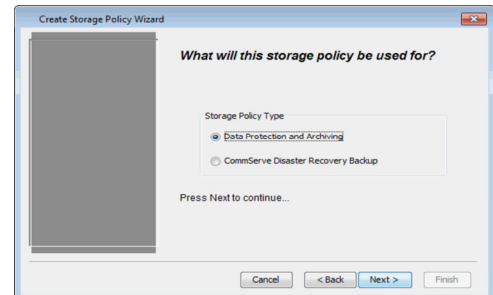
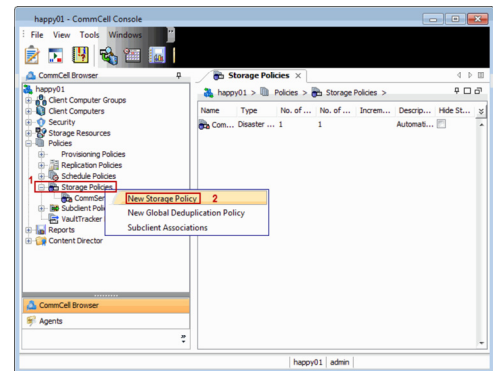
A storage policy acts as a channel through which data is transferred to the storage device. As the name indicates, a storage policy allows you to establish a comprehensive set of storage parameters - such as data retention, streams, deduplication, etc., for the data channeled through the storage policy.

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.

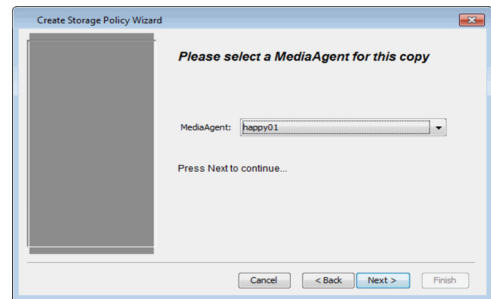
USING DISK LIBRARY

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

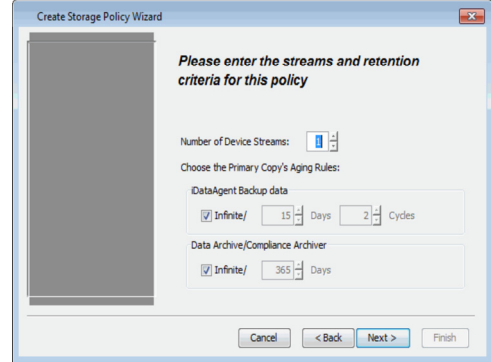
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.
2. Click **Next**.
3. Specify the name of the **Storage Policy** in the **Storage Policy Name** box and then click **Next**.
4. In the **Library** list, select the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



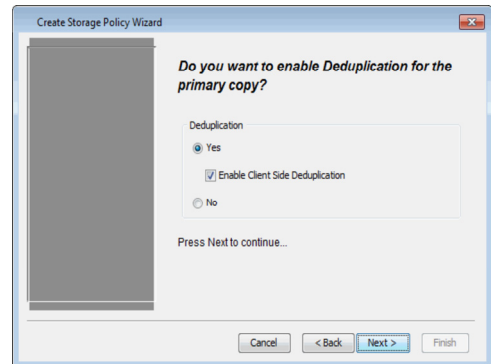
5. In the **MediaAgent** list, select a MediaAgent and then click **Next**.



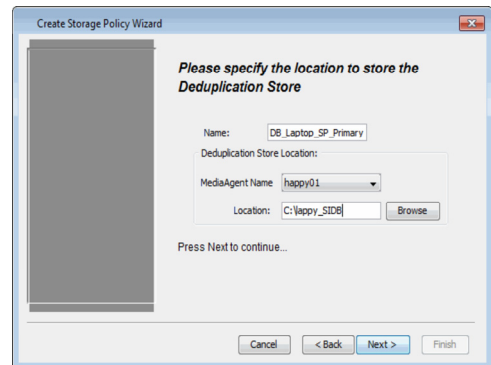
6. Click **Next**.



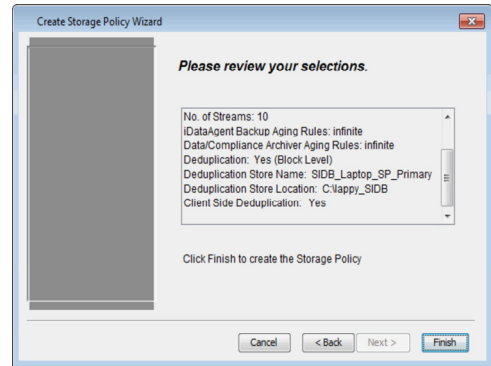
7. Click **Next**.



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



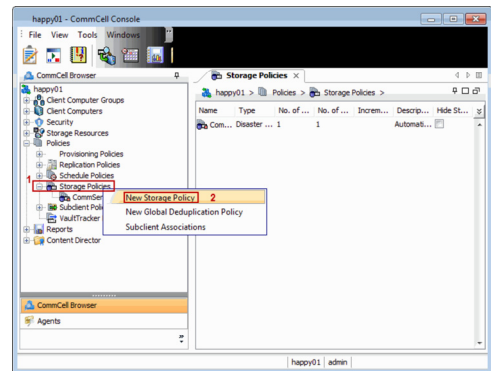
9. Review the details and click **Finish** to create the Storage Policy.
 The new Storage Policy creates the **Primary Classic Copy**, which will be used for data movement to tape, disk or cloud.



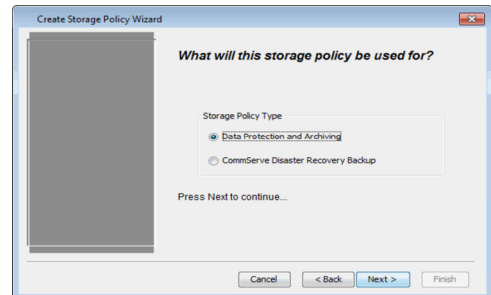
USING TAPE LIBRARY

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

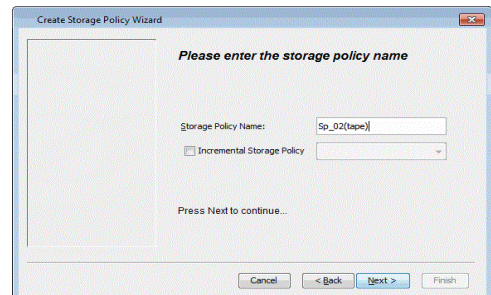
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



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**.

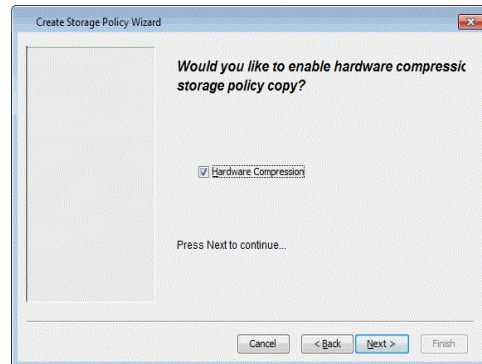
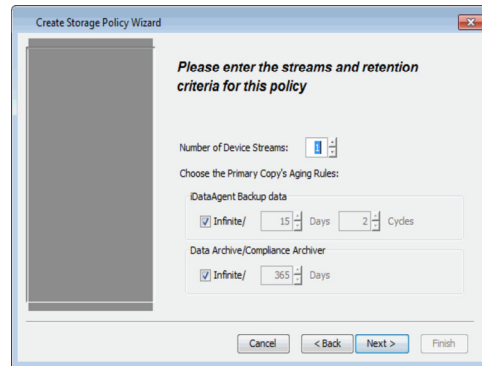
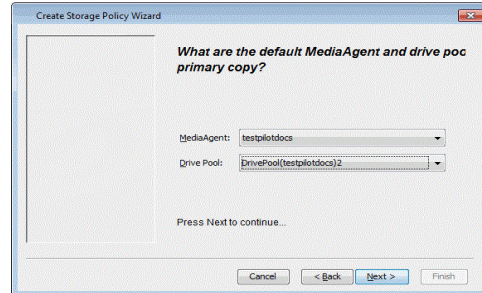
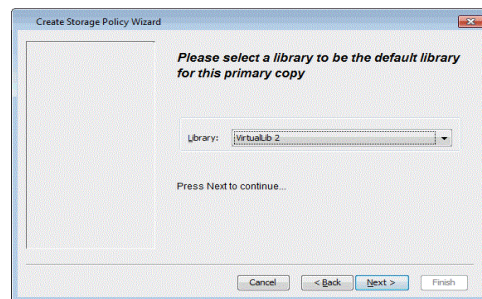
5.
 - In the **MediaAgent** list, select a MediaAgent.
 - From the **Drive Pool** list, select a default drive pool and then click **Next**.

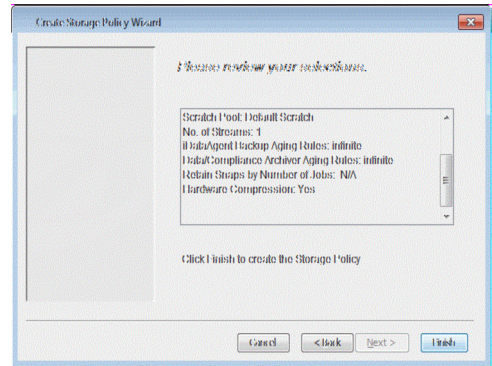
6. From the **Scratch Pool** list, select the default scratch pool and then click **Next**.

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**.

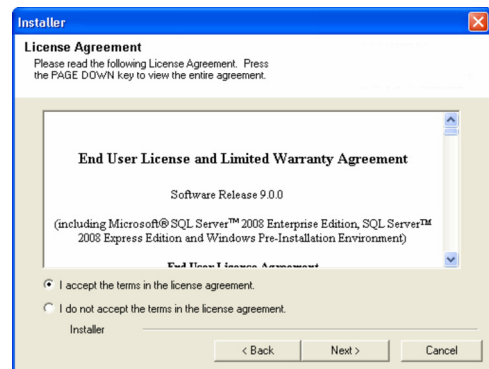
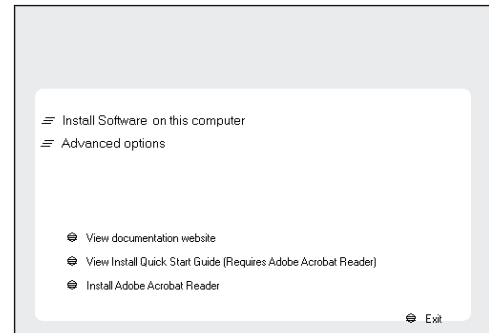
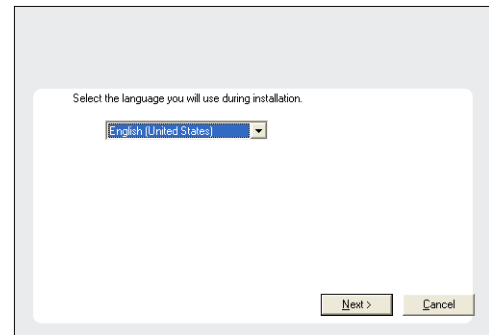
BEFORE YOU BEGIN

Download Software Packages

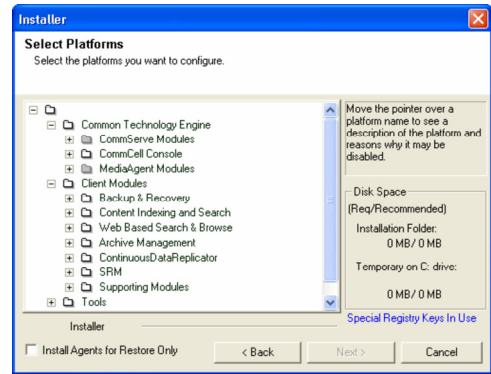
Download the latest software package to perform the install.

SnapProtect Support - Platforms

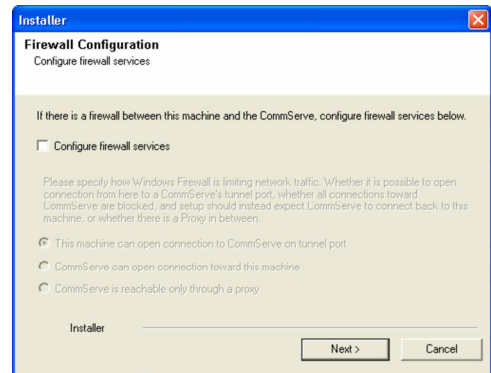
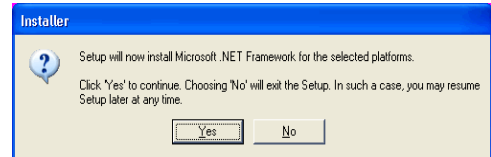
Make sure that the computer in which you wish to install the software satisfies the minimum requirements.



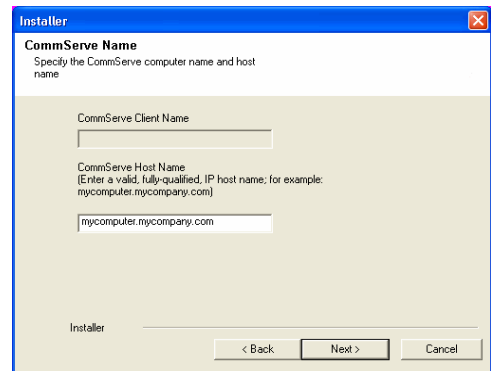
6. Click **YES** to install Microsoft .NET Framework package.
 - This prompt is displayed only when Microsoft .NET Framework is not installed.
 - Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.
7. 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**.



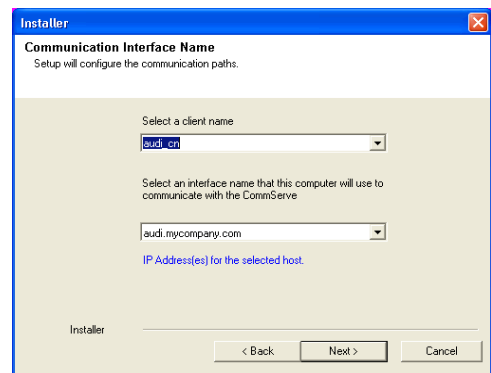
8. Enter the fully qualified domain name of the **CommServe Host Name**.
 Click **Next**.
 Do not use space and the following characters when specifying a new name for the CommServe Host Name:
`\ | ` ~ ! @ # $ % ^ & * () + = < > / ? , [] { } ; : ; " ' " "`



9. Click **Next**.



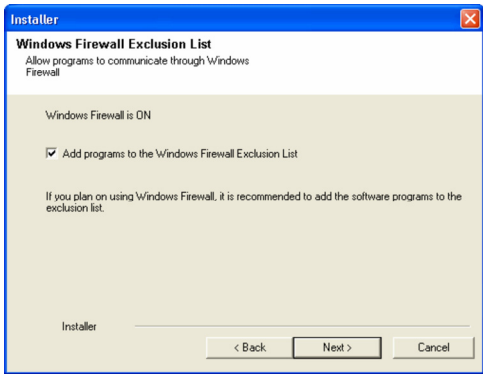
10. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.



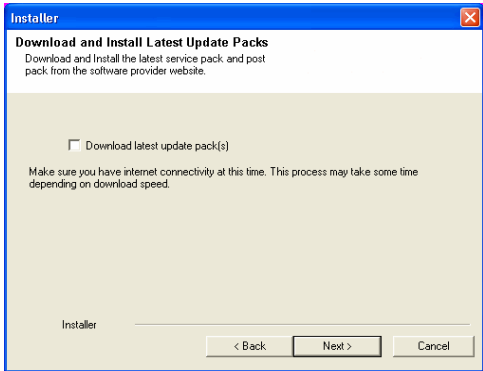
Click **Next**.

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.

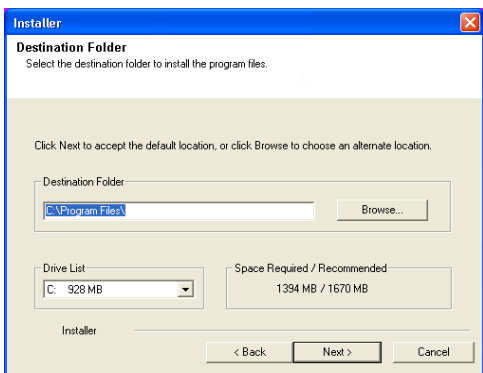
Click **Browse** to change the default location.

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:

/ : * ? " < > | #

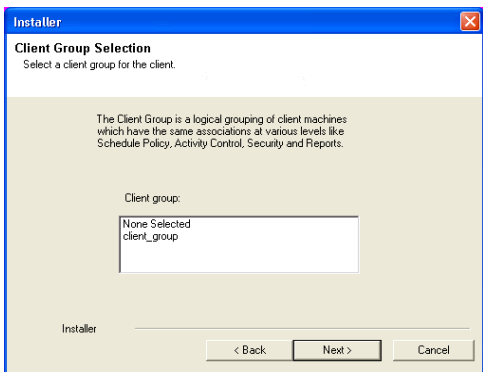
It is recommended that you use alphanumeric characters only.



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**.

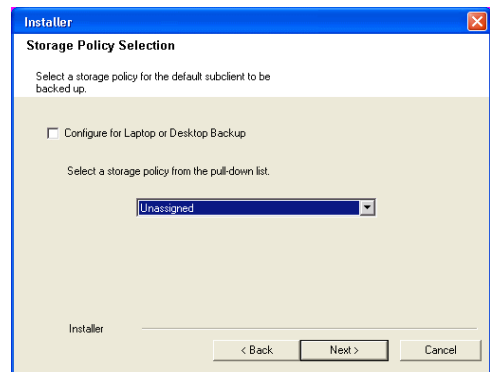
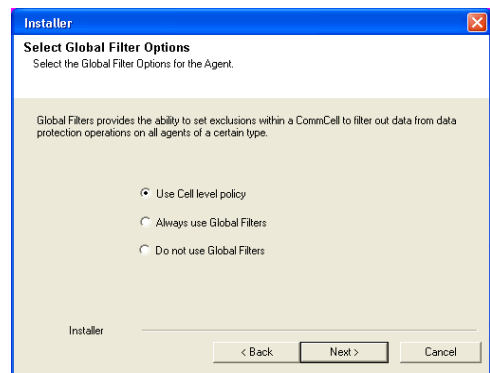
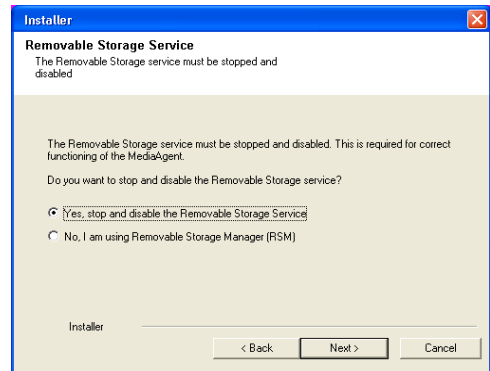
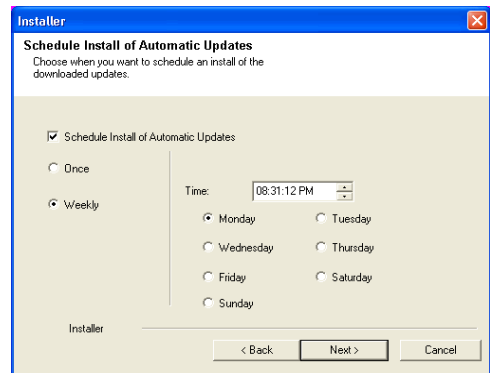
15. Select **Yes** to stop Removable Storage Services on the MediaAgent.
Click **Next**.

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

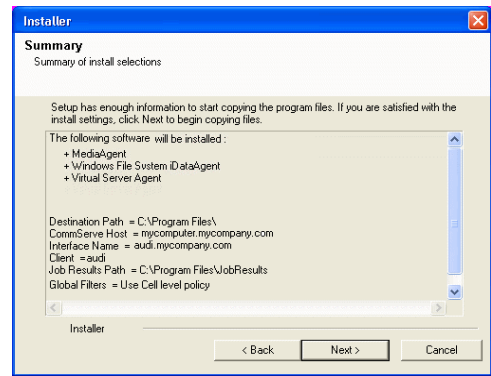
16. Click **Next**.

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

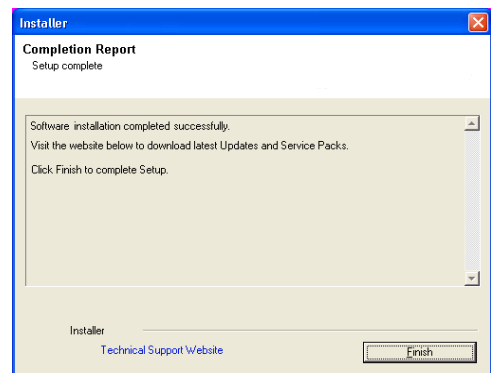
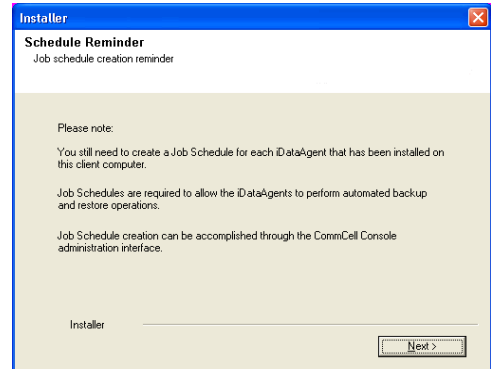
18. Click **Next**.



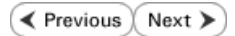
19. Click **Next**.



20. Click **Finish**.



Getting Started - VMware Configuration



CONFIGURATION

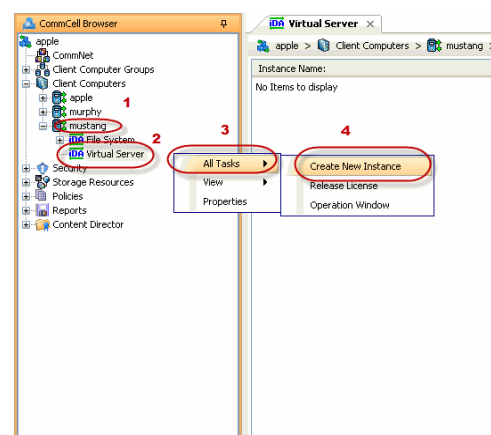
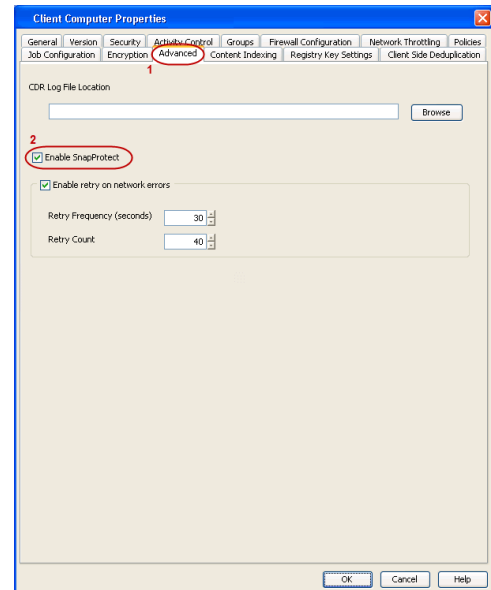
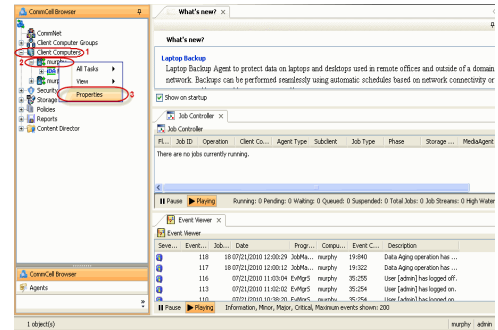
Once the Virtual Server *iDataAgent* has been installed, configure an Instance, a Backup Set and a Subclient to facilitate backups. The following sections provide the necessary steps required to create and configure these components for a first SnapProtect backup of a Virtual Center.

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

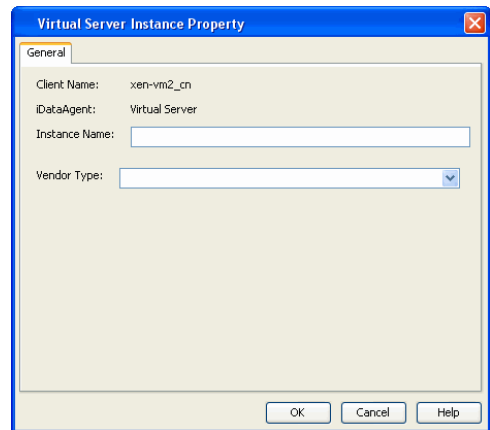
2.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.

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

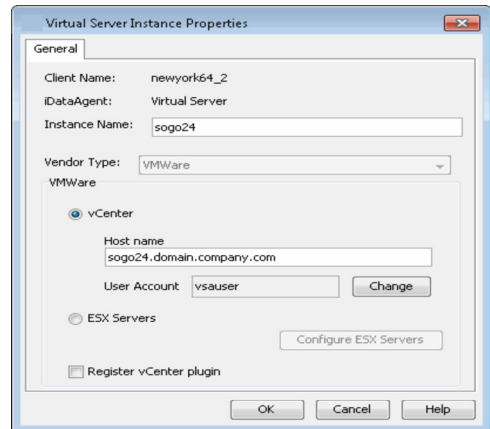
4.
 - Enter the **Instance Name**.
 - Select **VMware** from **Vendor Type** menu.



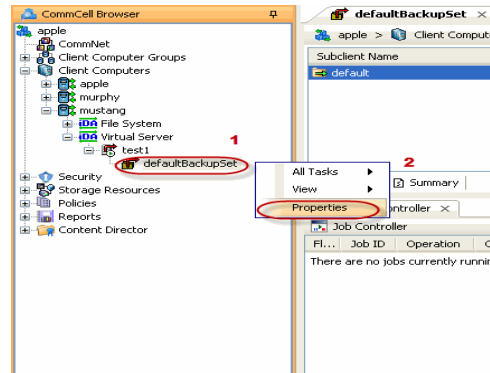
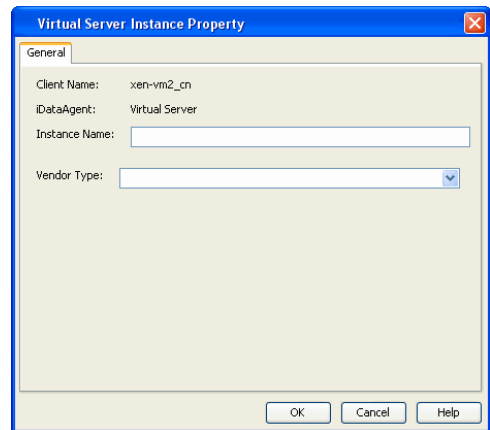
5.
 - Click **Virtual Center**.
ESX Server instances are not supported for SnapProtect operations.
 - Click **Configure Password**.
 - Enter the username and password associated with the Virtual Center.



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



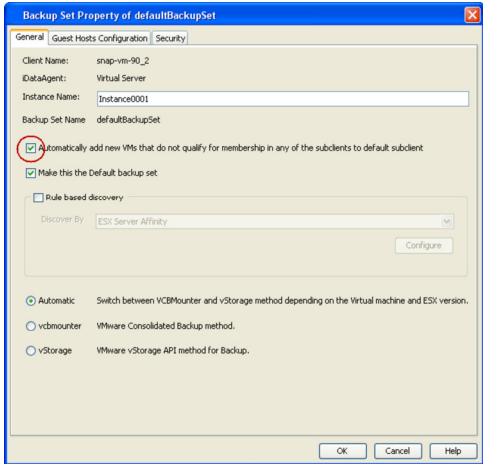
7.
 - From the CommCell Browser, right-click the **Default Backup Set**.
 - Click **Properties**.



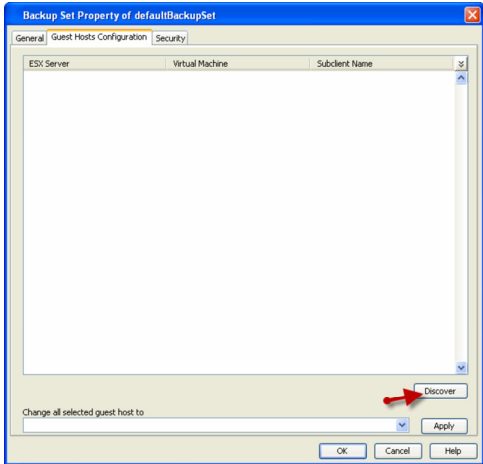
8.
 - Select **Automatically add new VMs that do not qualify for membership in any of the subclients**.

- Click **OK**.

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

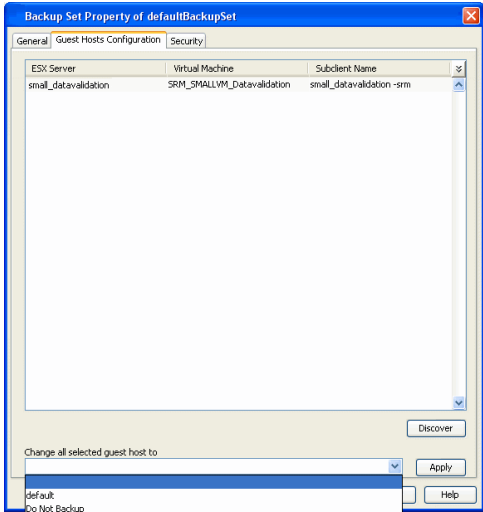


9. Click **Discover** on the **Guest Hosts Configuration** tab.
The discovery process might take several minutes to complete.



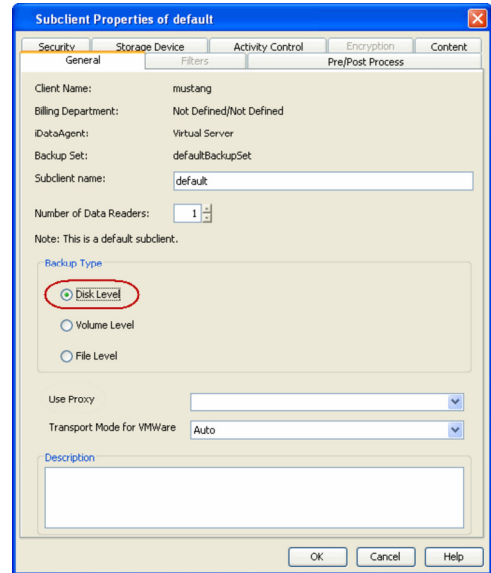
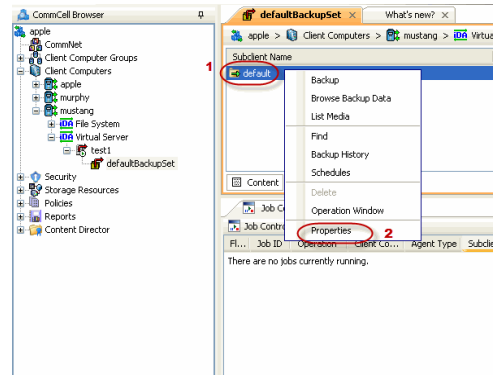
10.
 - Select a virtual machine to back up from the **Virtual Machine** column.
Ensure the virtual machine selected is not a VM template. Virtual machine templates are not supported for backup.

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

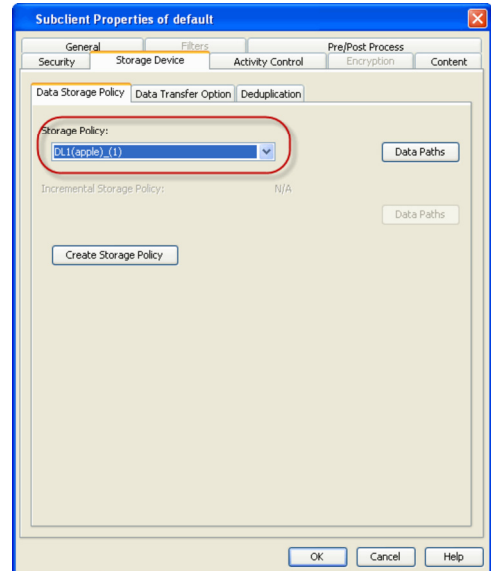


11.
 - From the CommCell Browser, navigate to the default subclient.
 - Click **Properties**.

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



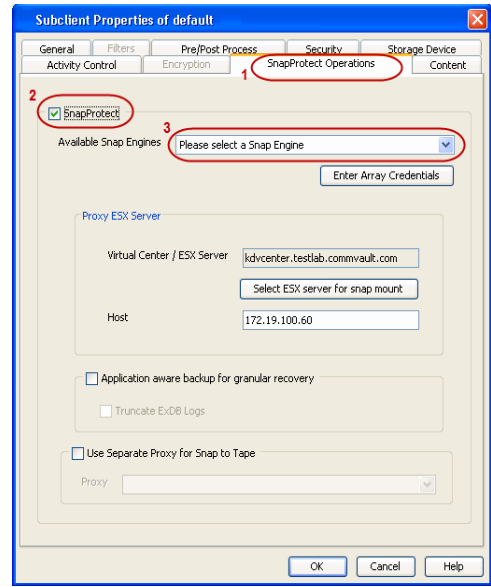
13.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.



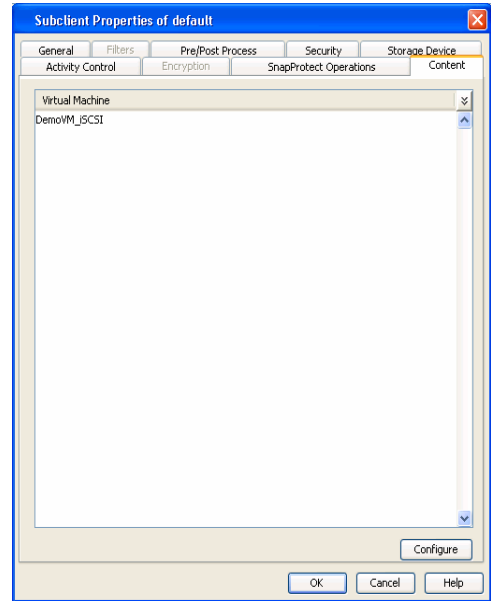
14.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - Click **Use Separate Proxy for Snap to Tape** if you want to perform SnapProtect 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.

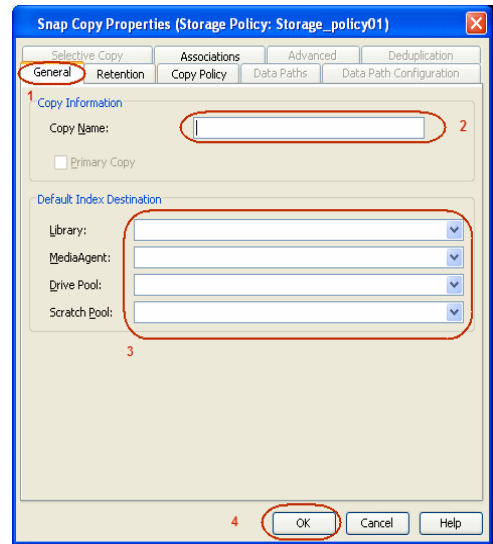
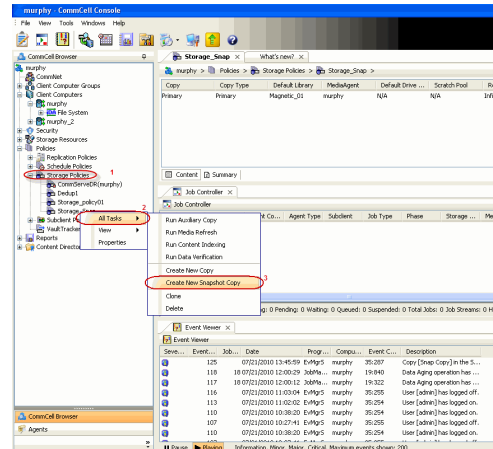
CREATE A SNAPSHOT COPY



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**.

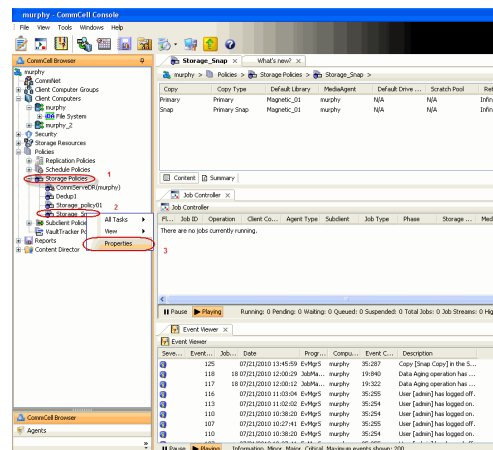
2.
 - Enter the copy name in the **Copy Name** field.
 - Select the **Library, MediaAgent, master Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



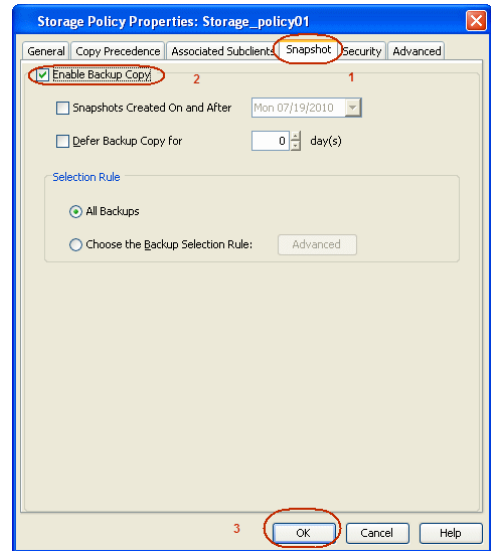
CONFIGURE BACKUP COPY

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

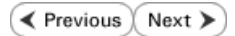
[◀ Previous](#) [Next ▶](#)

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



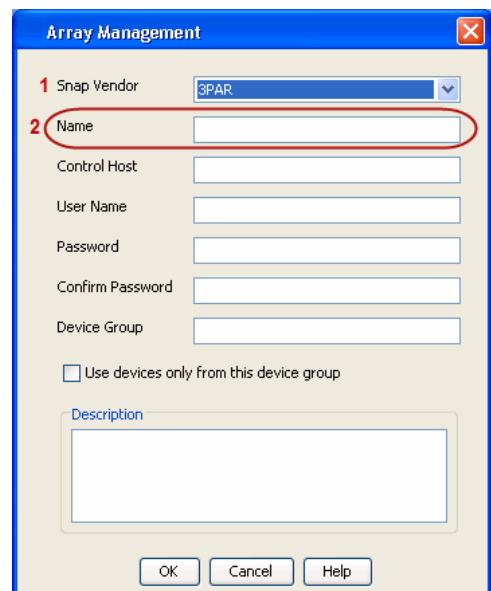
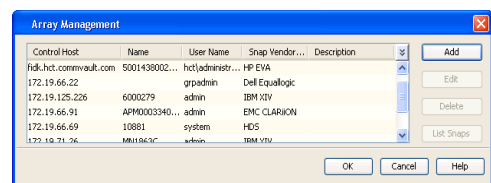
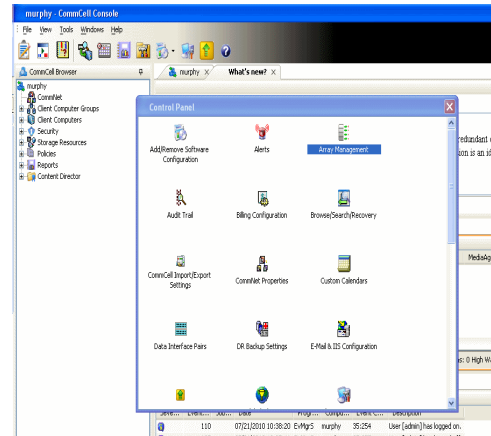
PRE-REQUISITES

- 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

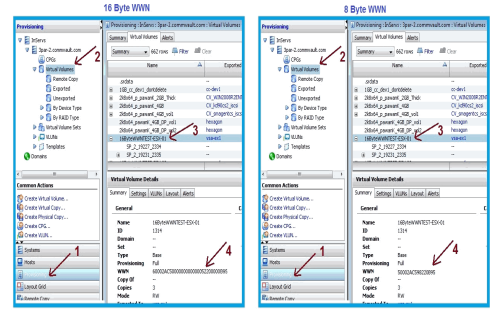
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

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

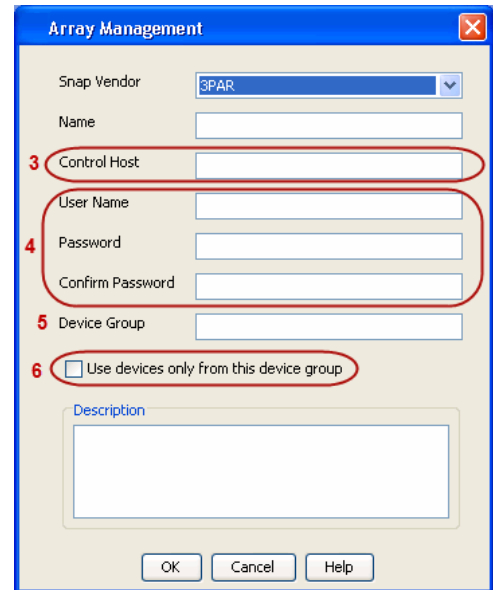
After adding all the values, the resulting array name is 2FF70002AC000B95.



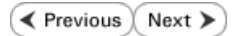
- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be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

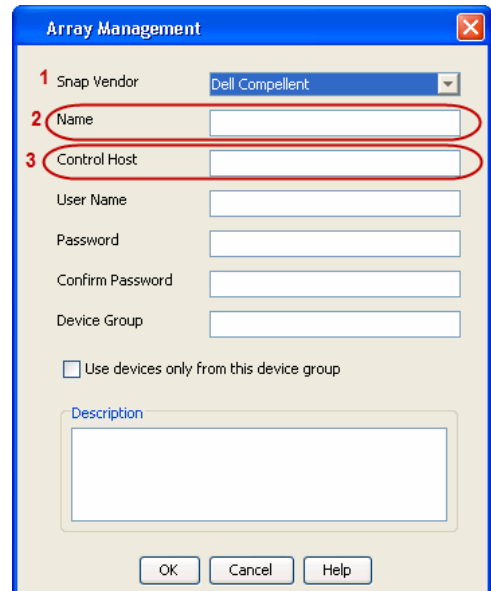
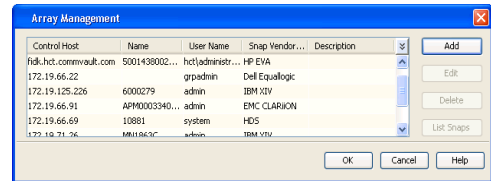
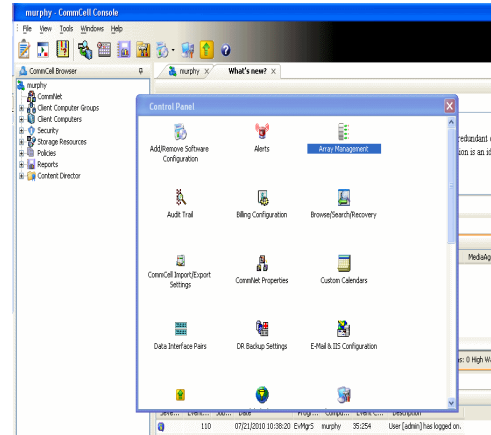
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

SETUP THE ARRAY INFORMATION

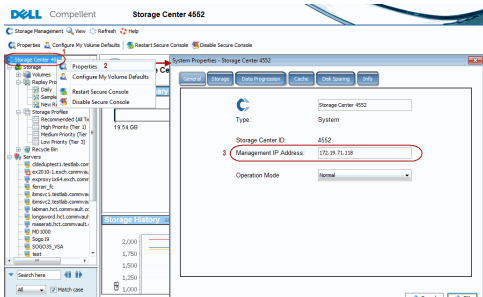
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- 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.

Array Management ✖

Snap Vendor: Dell Compellent

Name:

Control Host:

User Name:

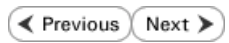
Password:

Confirm Password:

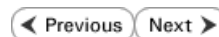
Device Group:

Use devices only from this device group

Description:



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

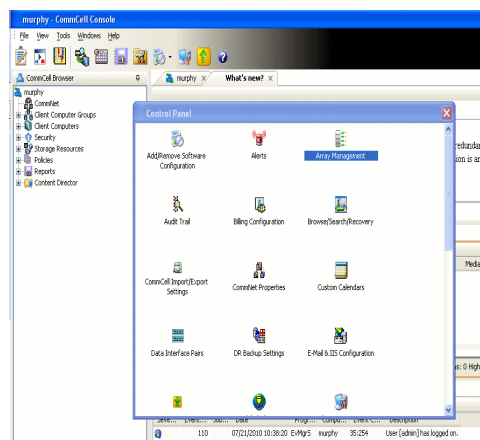
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing 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.

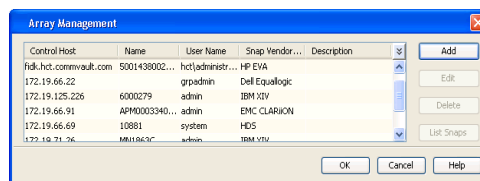
SETUP THE ARRAY INFORMATION

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**.

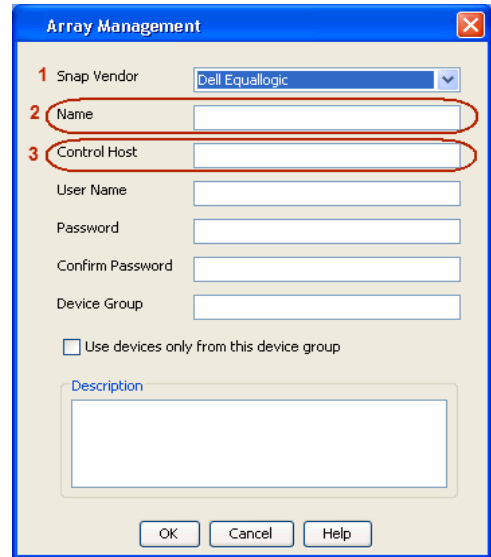


2. Click **Add**.

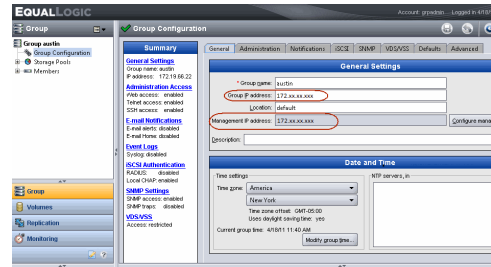


3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

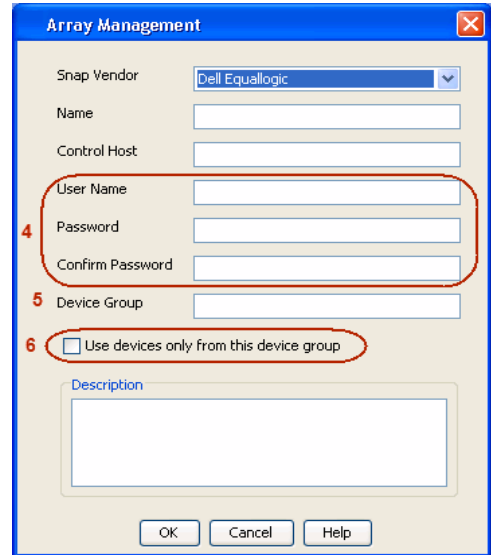
No entry is required in the **Name** field if there is no Management IP address configured.
 - Specify the Group IP address in the **Control Host** field.



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.

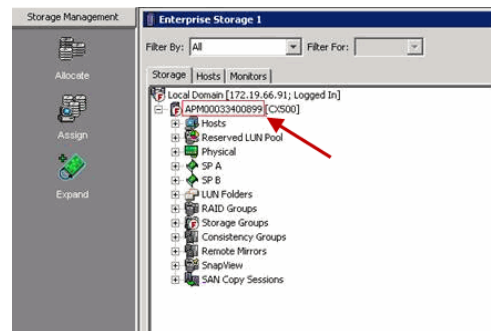
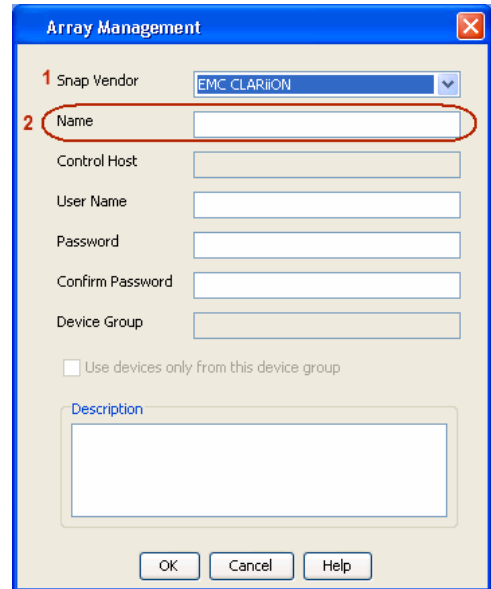
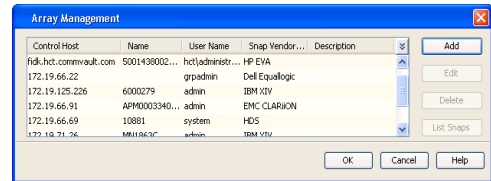
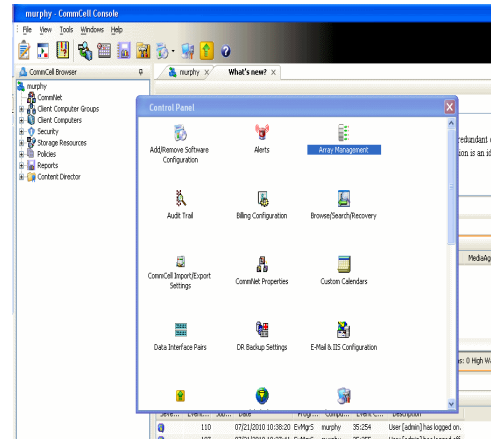
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

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

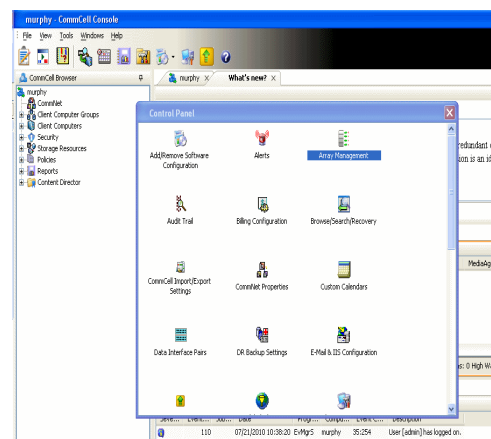
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

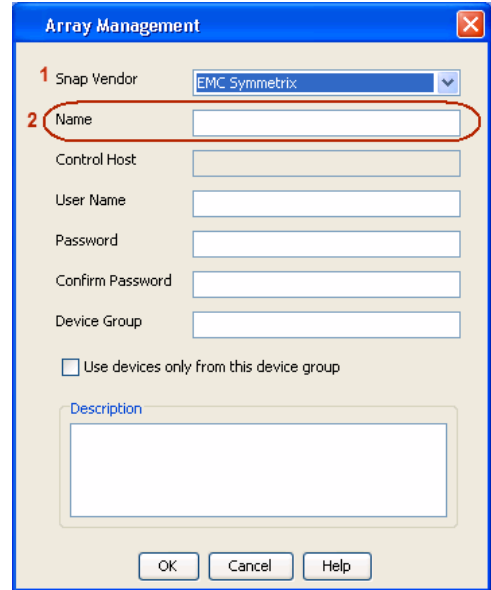
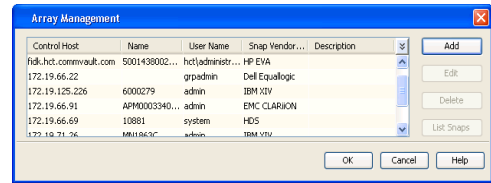
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

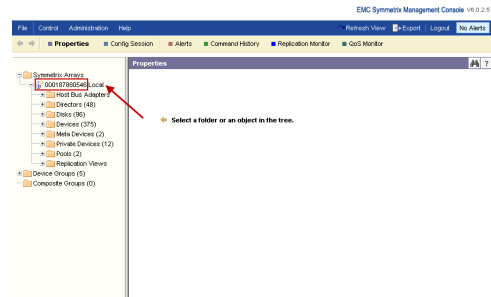


2. Click **Add**.

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

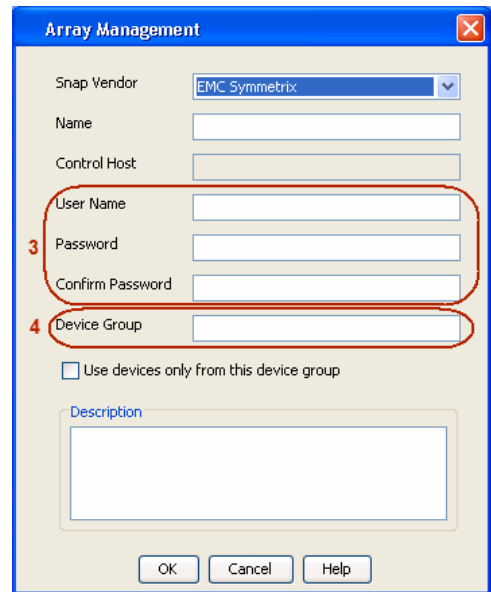


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



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

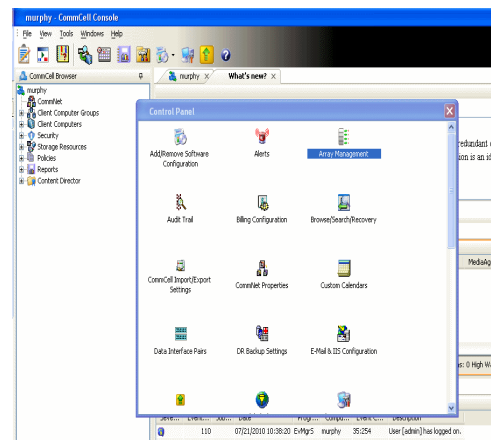
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

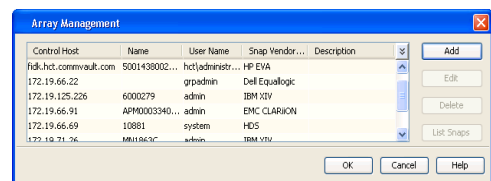
SETUP THE ARRAY INFORMATION

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

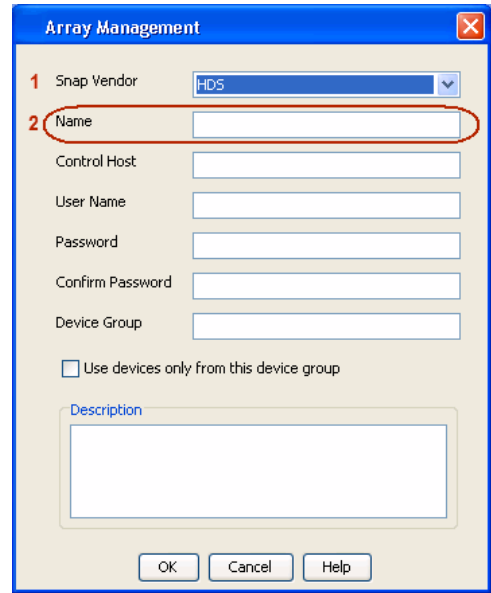
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



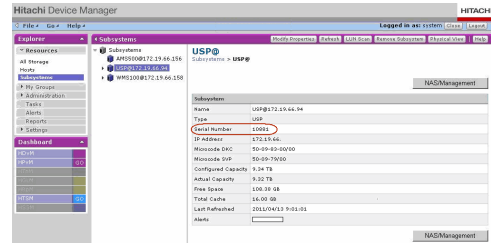
2. Click **Add**.



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.



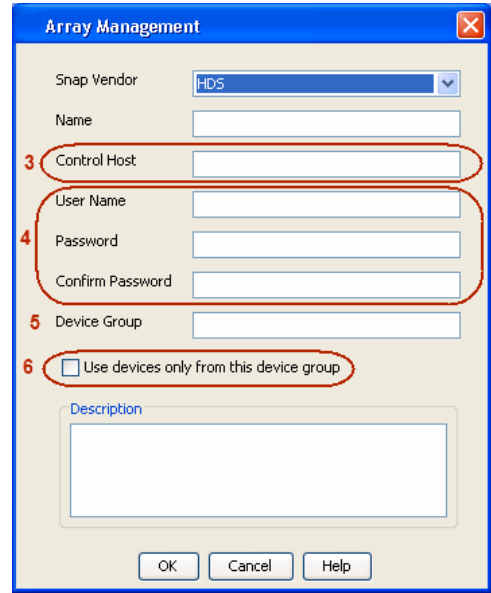
4.
 - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot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

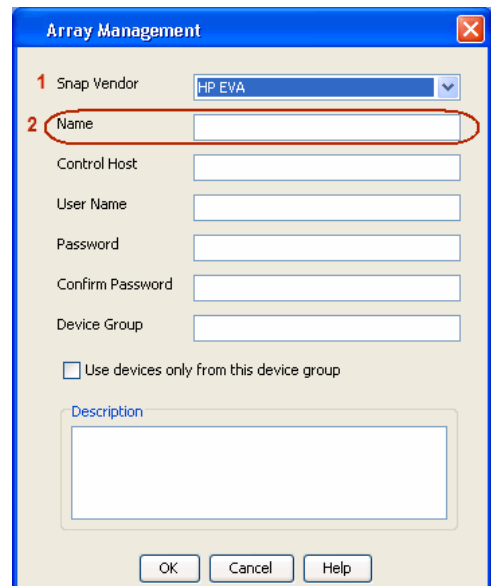
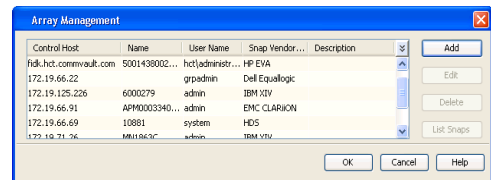
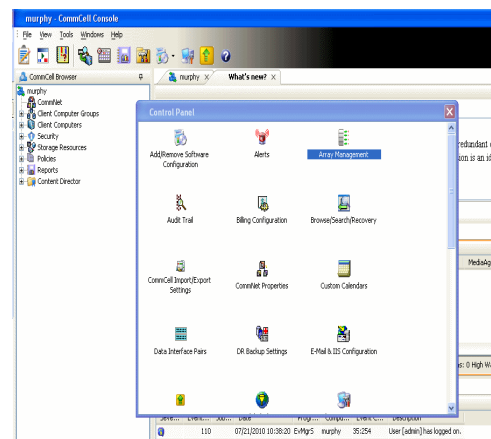
The following steps provide the necessary instructions to setup the HP EVA:

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

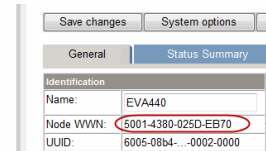
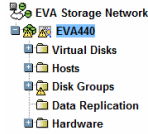
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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 ▶

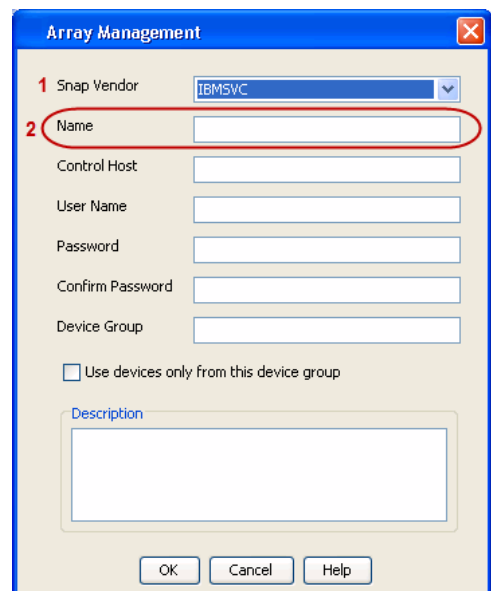
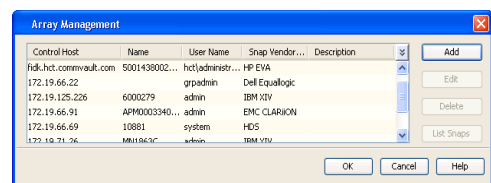
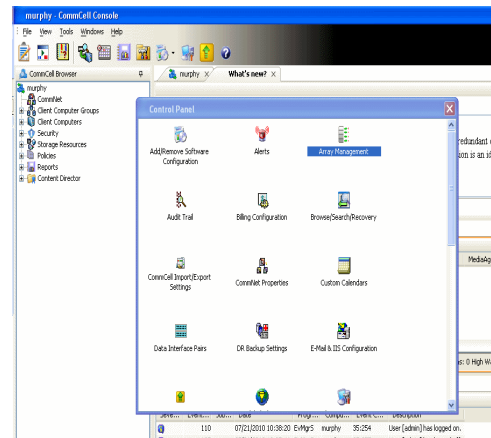
PRE-REQUISITES

- 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.

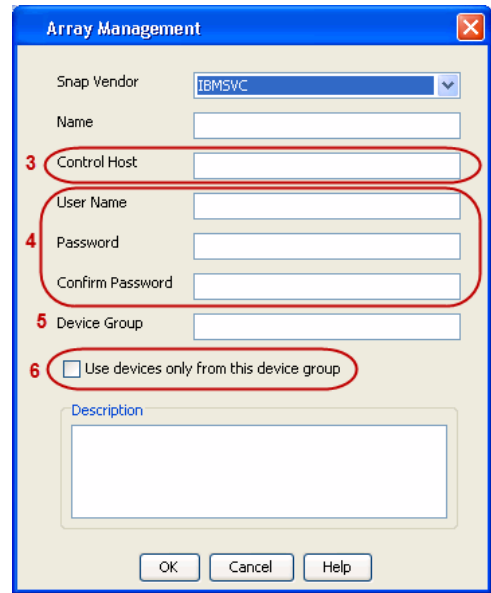
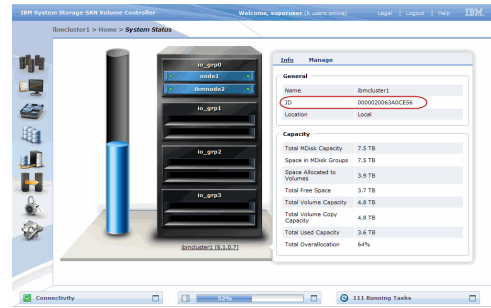
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



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



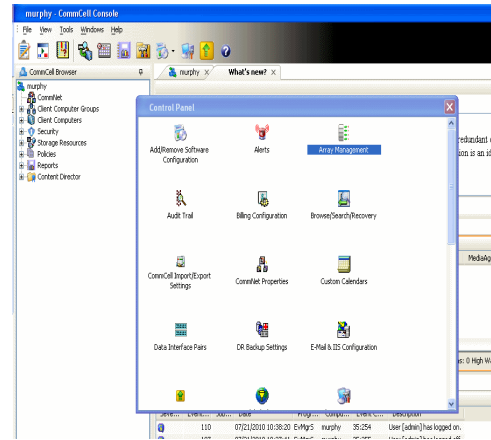
PRE-REQUISITES

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.

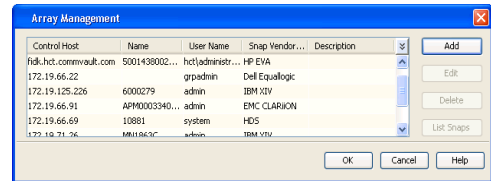
SETUP THE ARRAY INFORMATION

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

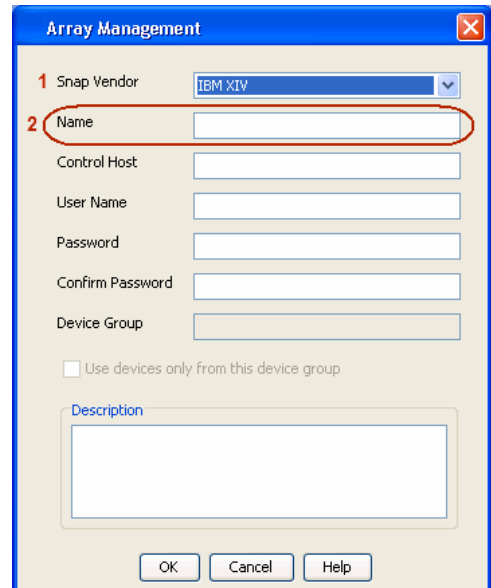
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



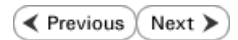
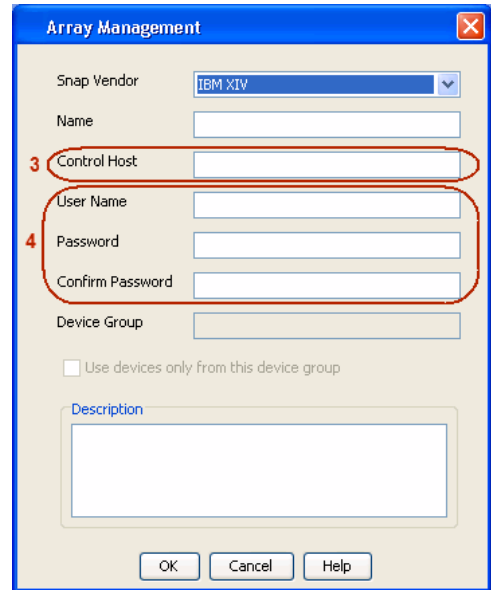
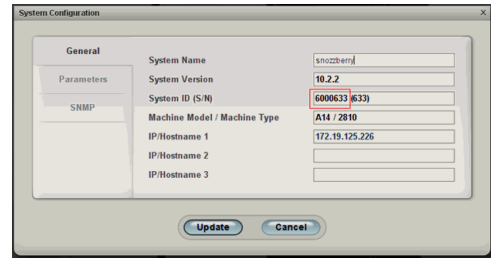
3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



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



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.

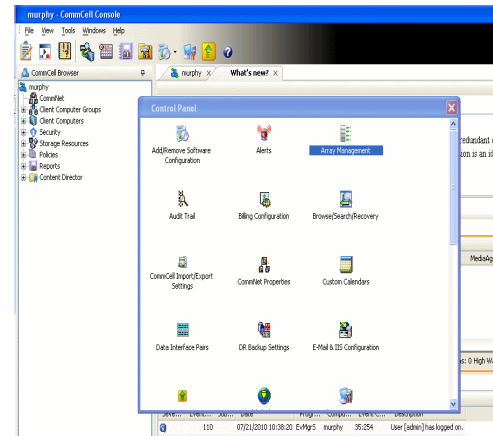
ADDITIONAL REQUIREMENTS FOR VMWARE

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.

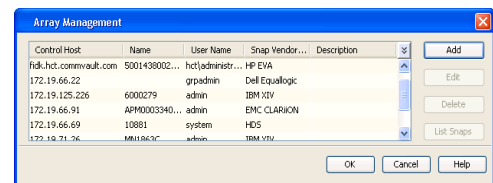
SETUP THE ARRAY INFORMATION

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

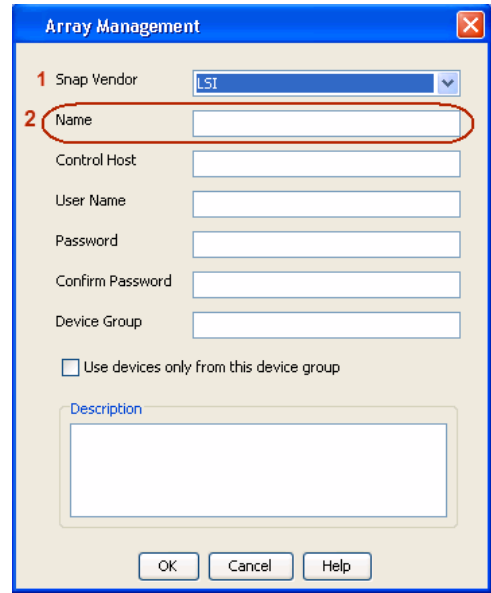
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

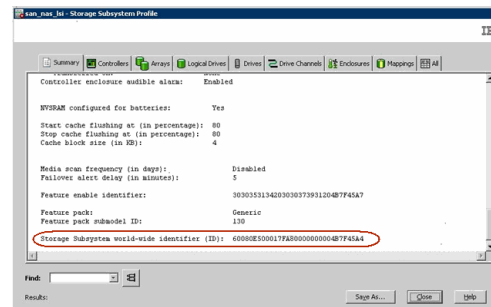


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



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

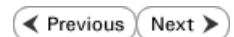
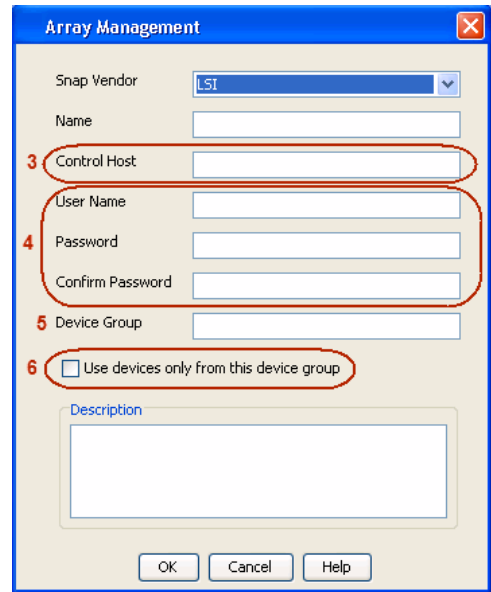
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



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

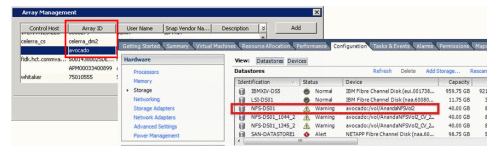
LICENSES

- 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.

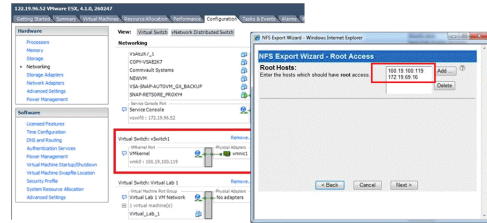
ADDITIONAL REQUIREMENTS FOR VMWARE

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.



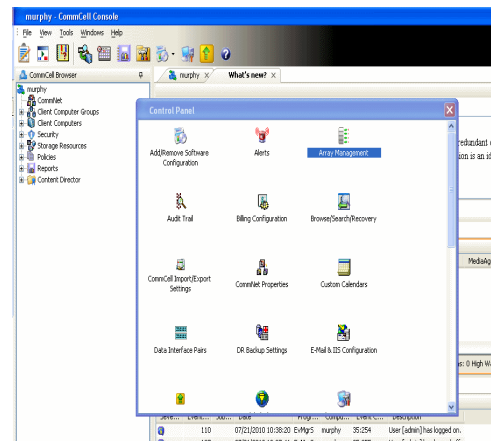
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



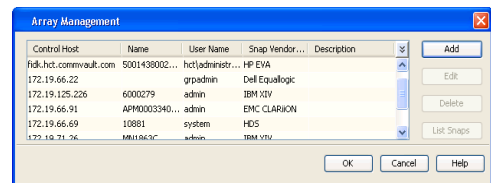
SETUP THE ARRAY INFORMATION

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: [Text Field]

Control Host: [Text Field]

User Name: [Text Field]

Password: [Text Field]

Confirm Password: [Text Field]

Device Group: [Text Field]

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

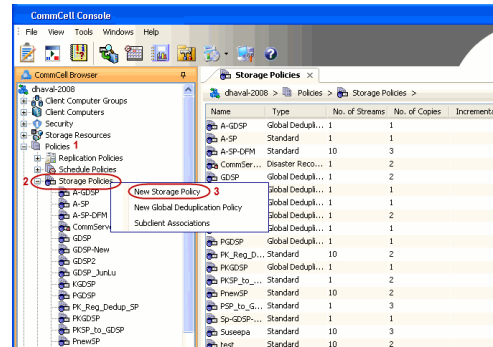
CONFIGURATION

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

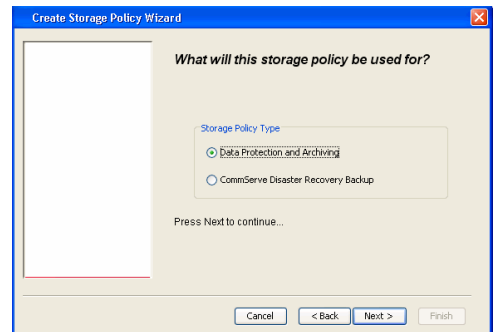
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

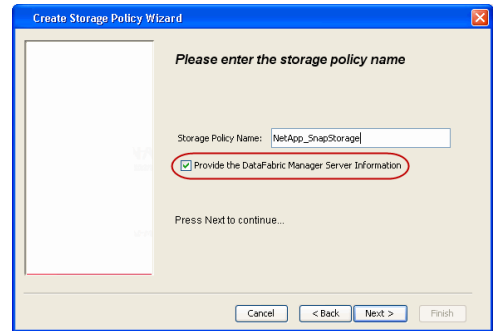
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



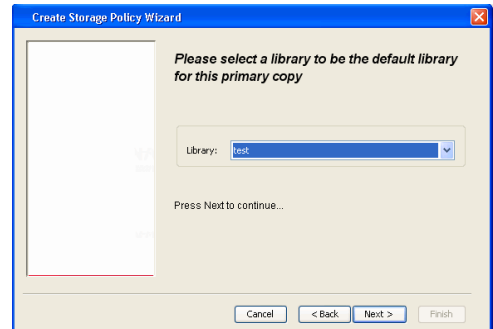
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



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

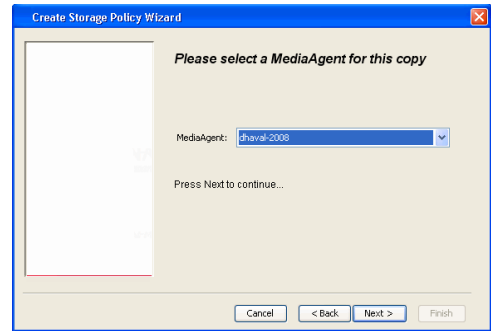
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

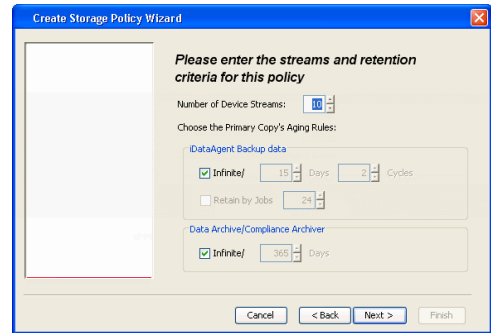


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

6. Click **Next**.

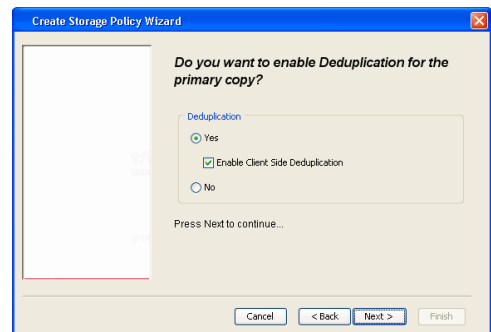


7. Click **Next**.



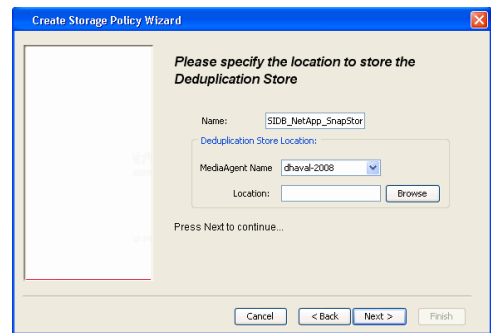
8.

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

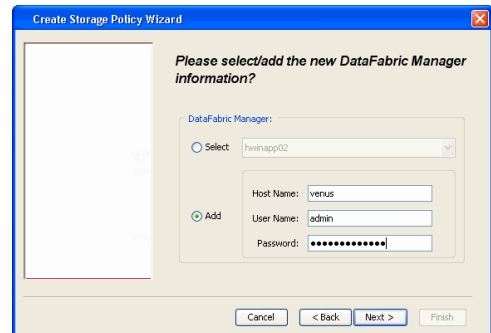


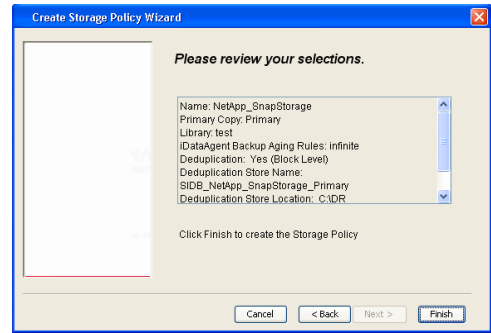
9.

- 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**.



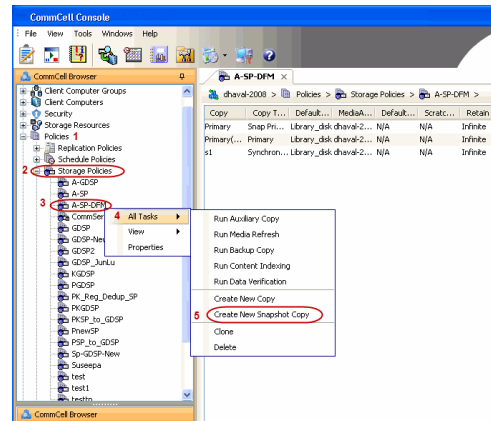


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

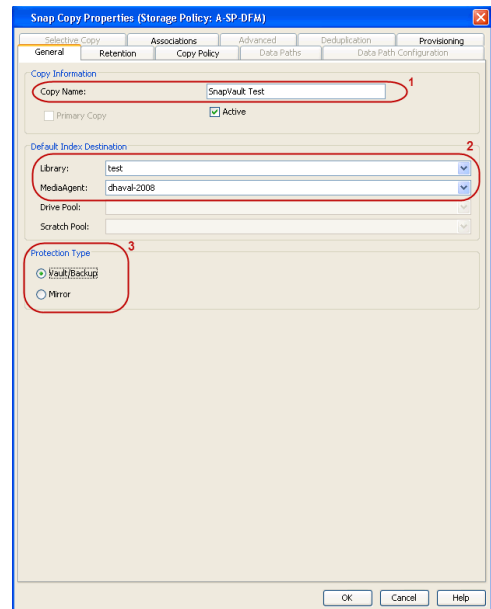
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

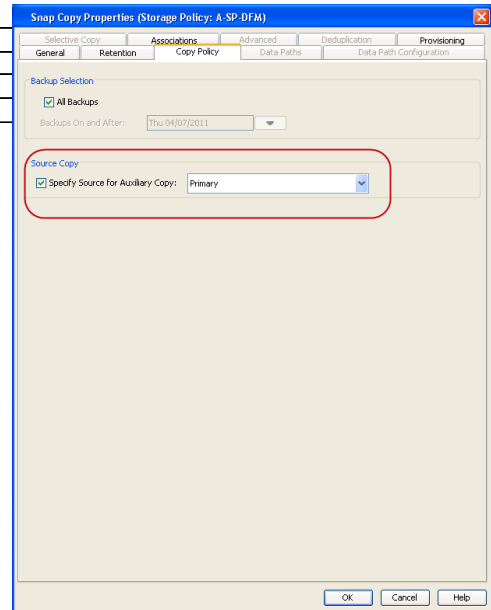


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

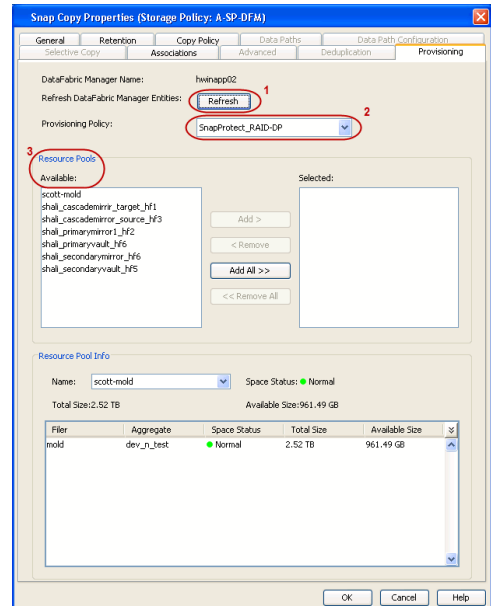
TOPOLOGY	SOURCE COPY
----------	-------------

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.

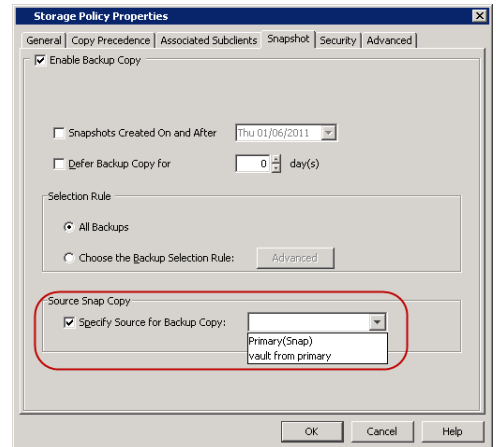
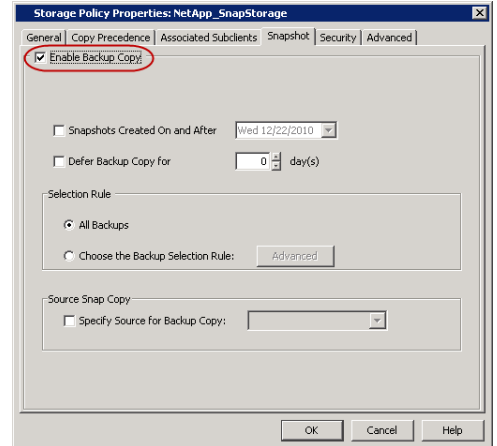
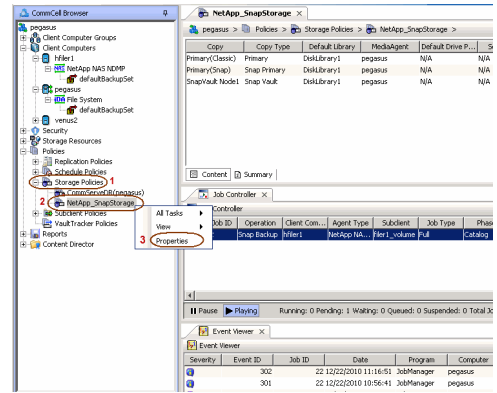
CONFIGURE BACKUP COPY

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.

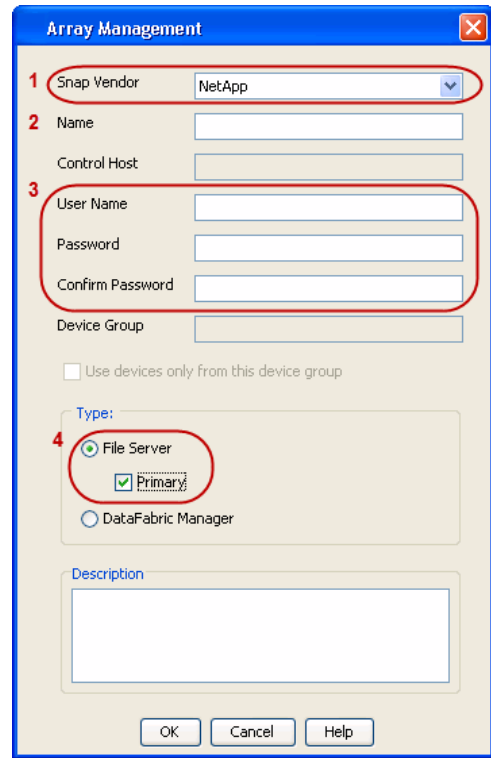
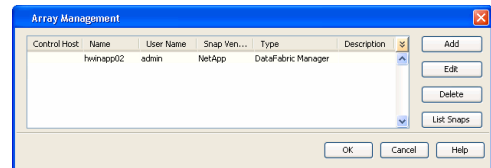
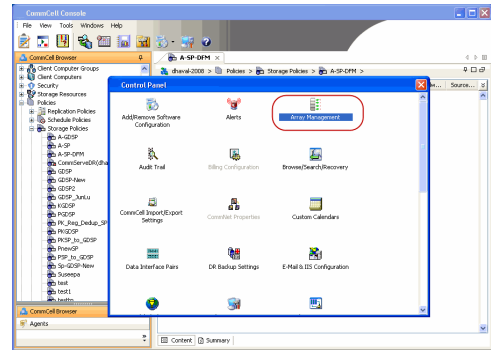
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

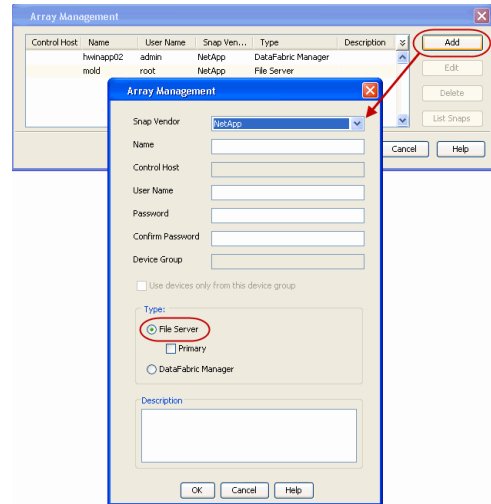
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

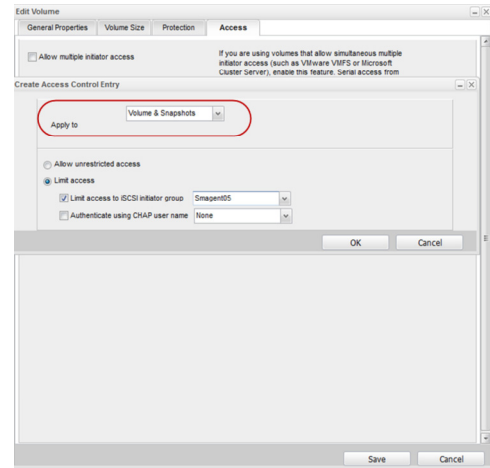
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

SnapProtect™ Backup - Nimble



PREREQUISITES

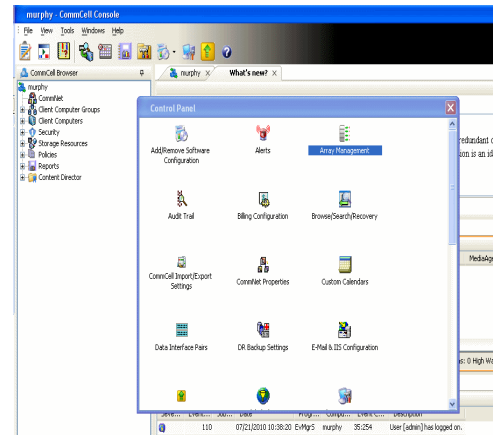
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry**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



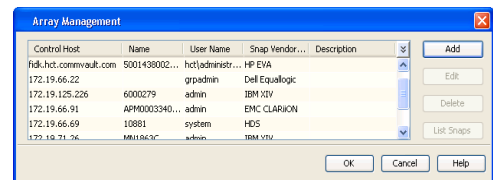
SETUP THE ARRAY INFORMATION

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.

Array Management

Snap Vendor: Nimble

Name: [Text Field]

Control Host: [Text Field]

User Name: [Text Field]

Password: [Text Field]

Confirm Password: [Text Field]

Device Group: [Text Field]

Use devices only from this device group

Type:

- File Server
- Primary
- DataFabric Manager

Description: [Text Area]

OK Cancel Help

< Previous Next >

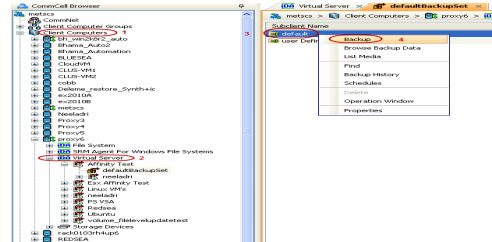
Getting Started - VMware Backup

PERFORM A BACKUP

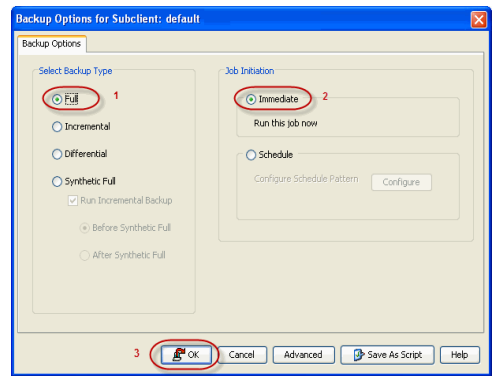
After configuring your Instance, Backup Set and Subclient, you are ready to perform your first backup.

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

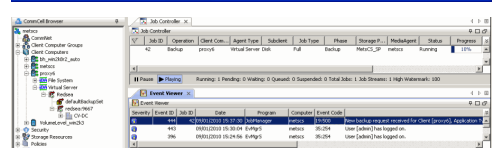
- From the CommCell Console, navigate to **Client Computers | Virtual Server**.
 - Right-click the **Subclient** and click **Backup**.



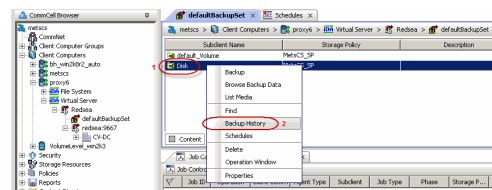
- Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.



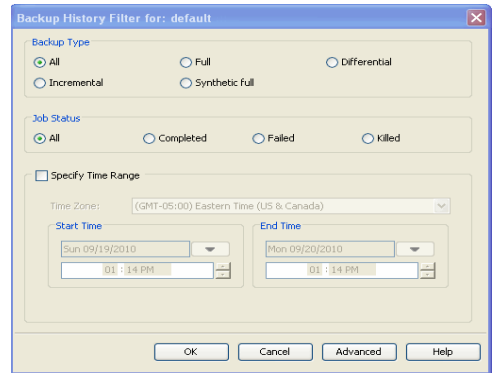
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



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

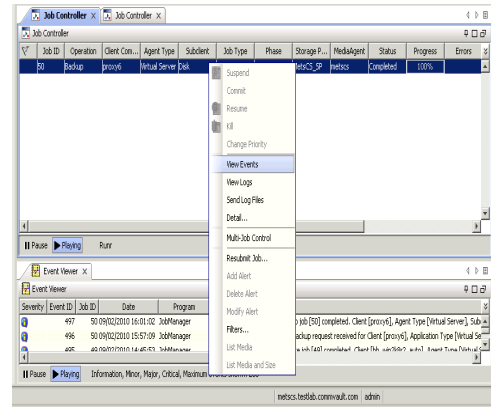


- Click **OK**.



- 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



Getting Started - Vault/Mirror Copy

◀ Previous Next ▶

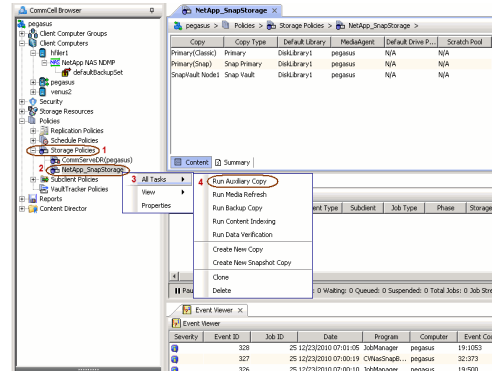
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

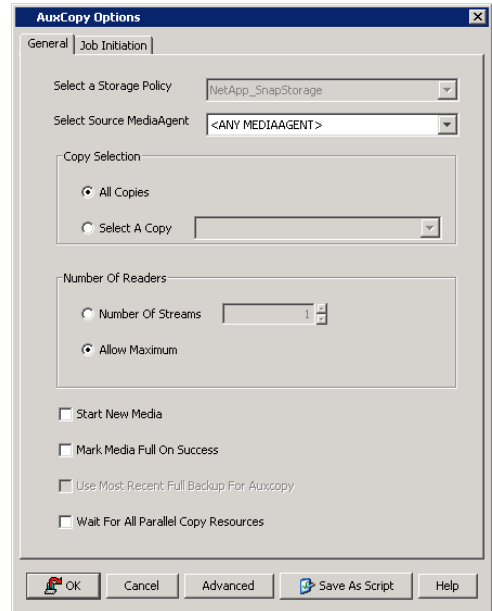
INITIATE VAULT/MIRROR COPY

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**.

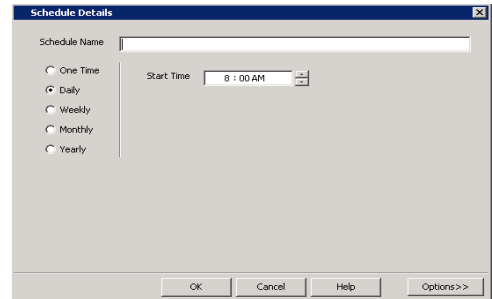


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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

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

Click **Next** ▶ to Continue.

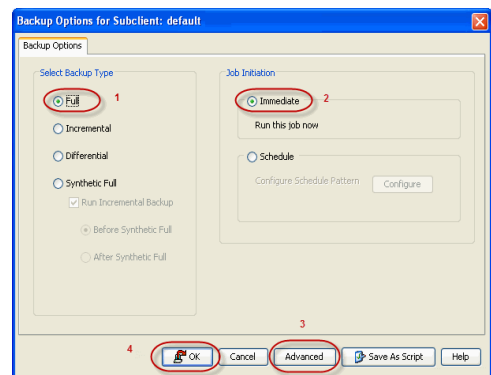
BACKUP COPY OPERATIONS

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

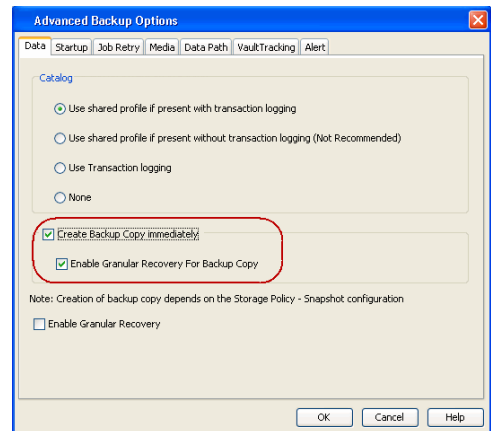
Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect 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.

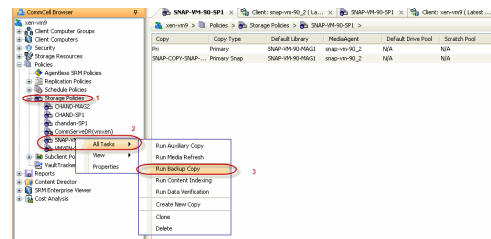
Enable Granular Recovery for Backup Copy is automatically selected. This option allows you to view the file/folder level details of the backup copy.
 - If you want to view the file/folder level details of the snapshot copy, select **Enable Granular Recovery**.
 - Click **OK**.



OFFLINE BACKUP COPY

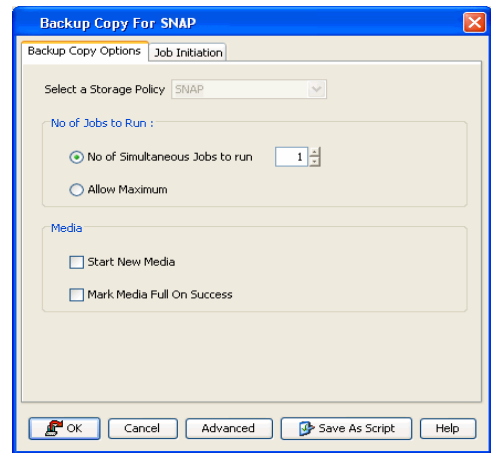
Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

- 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

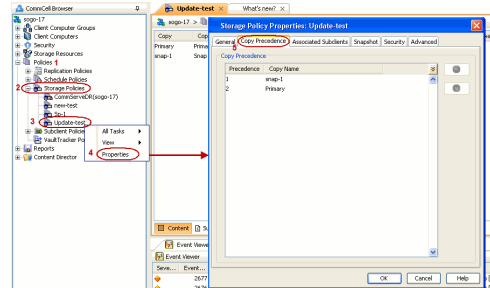
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

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

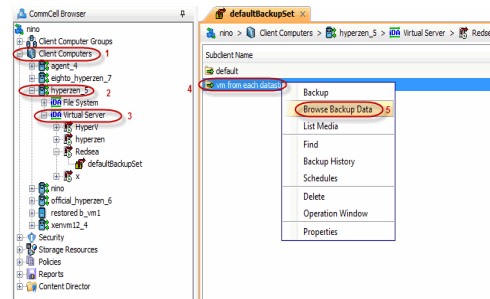
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.

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.

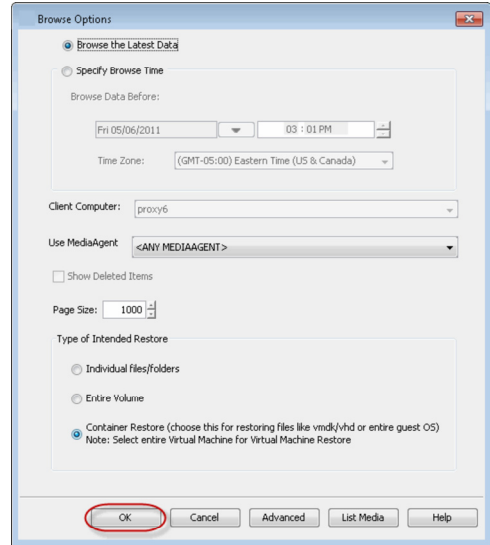
 - Click **OK**.



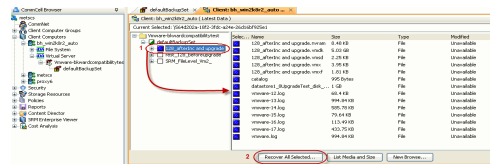
- From the CommCell Console, navigate to **<Client> | Virtual Server**.
 - Right-click the subclient that contains the data you want to restore and click **All Tasks | Browse Backup Data**.



- 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**.



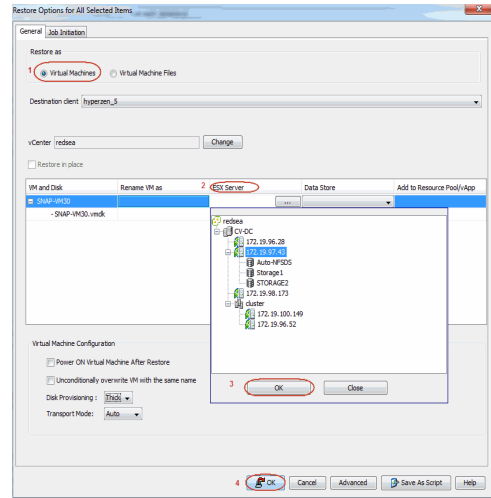
- Select the virtual machine under the backup set. Its entire contents will be automatically selected in the right pane.
 - Click **Recover All Selected**.



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

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

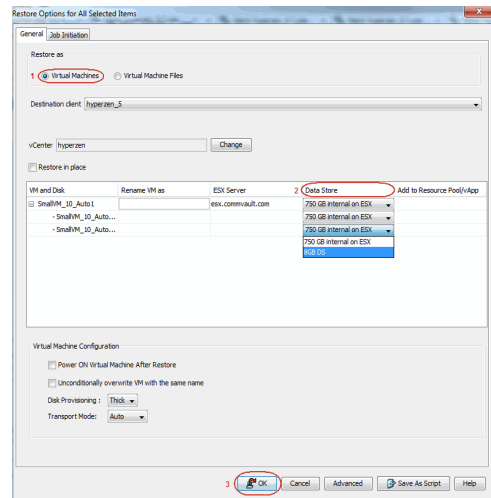
If the selected datastore does not meet the minimum requirements needed to restore the virtual machine, you can repeat this step until an acceptable datastore is found.



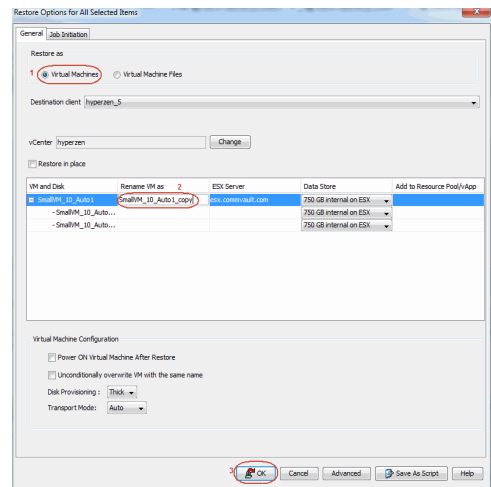
7. Enter the **VM Name** for the virtual machine.

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

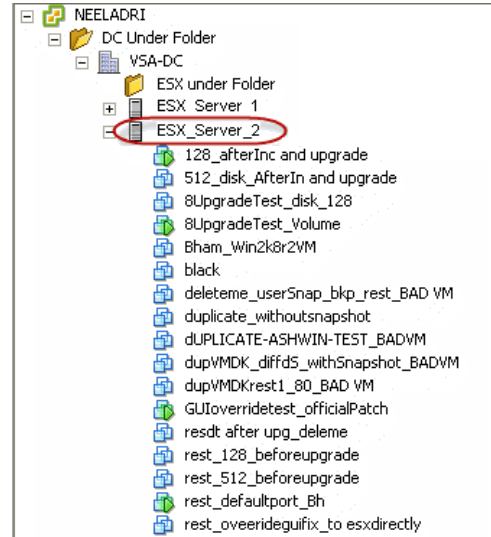
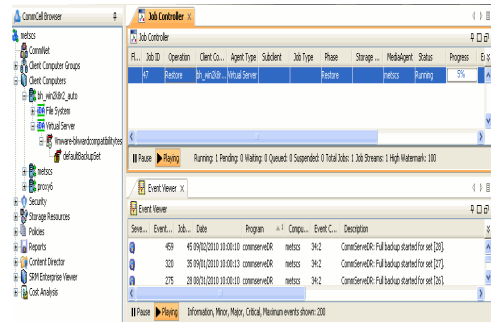
- Click **OK**.



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.

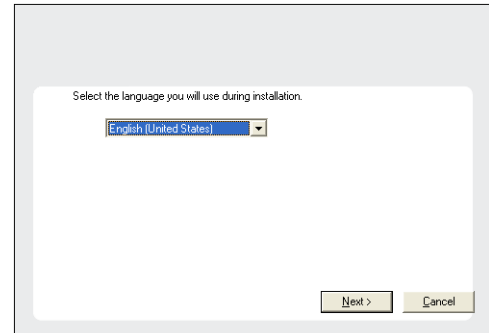
SnapProtect Support - Platforms

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

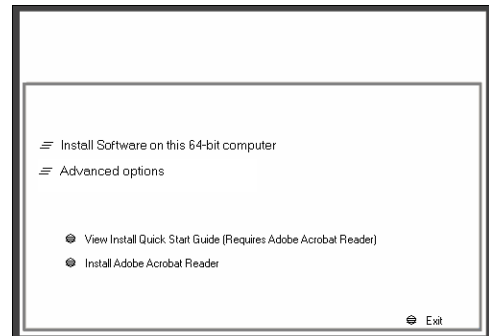
INSTALL THE EXCHANGE DATABASE iDATAAGENT

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**.

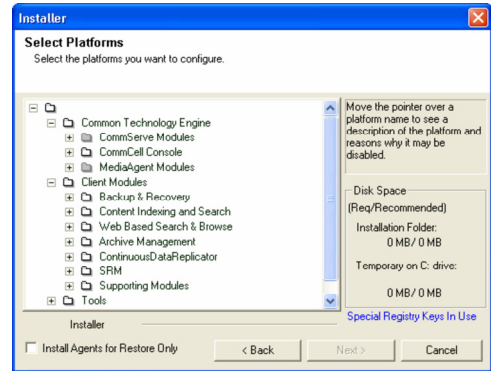
6.
 - Expand **Client Modules | Backup & Recovery | Exchange**, and select **Exchange Database /DataAgent**.
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
 - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
 - Click **Next**.



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.

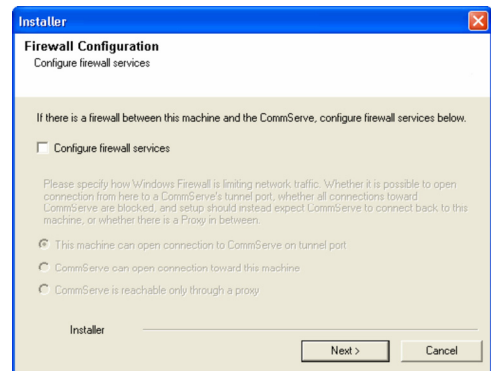
If firewall configuration is not required, click **Next**.



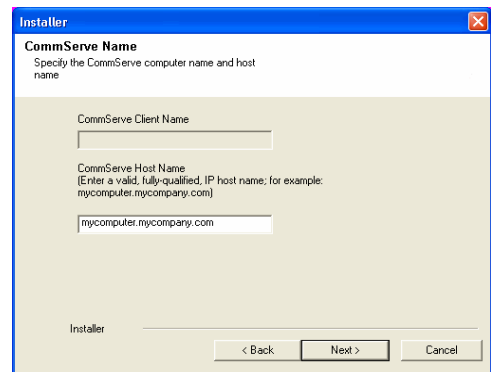
8. Enter the fully qualified domain name of the **CommServe Host Name**.
Click **Next**.

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:

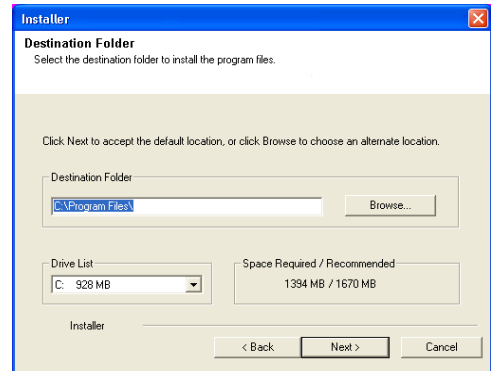
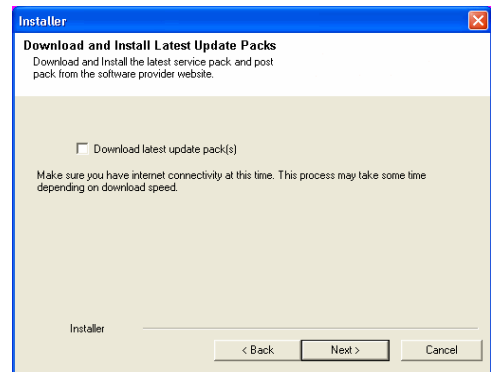
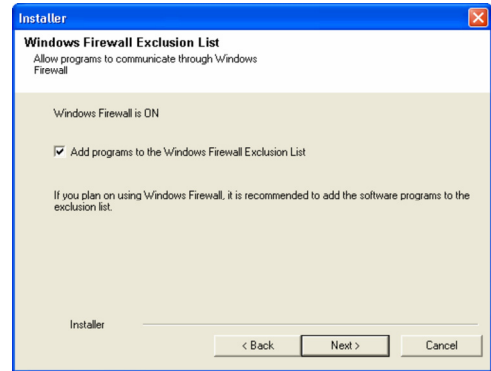
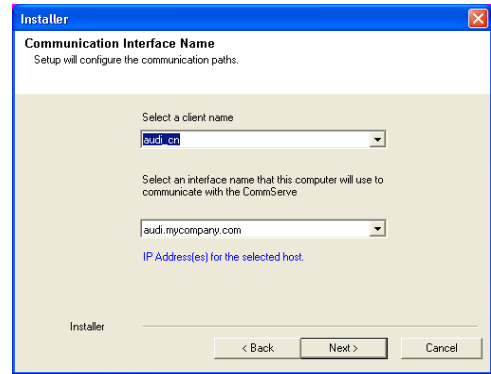
/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

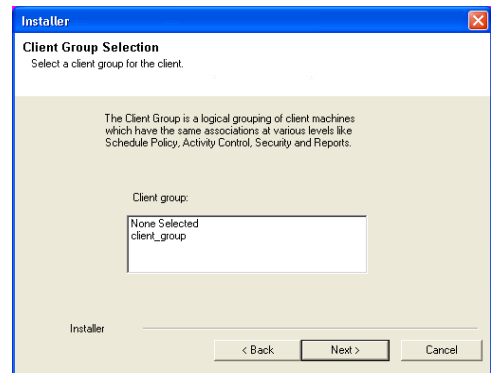
13. Select a Client Group from the list.

Click **Next**.

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

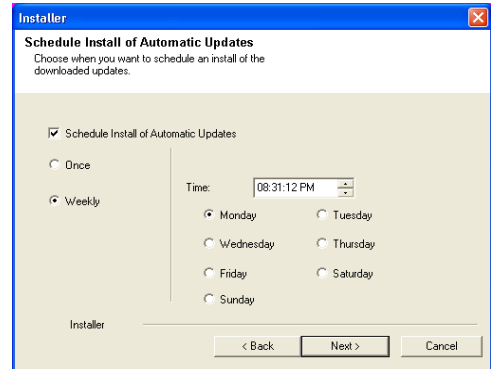


14. Click **Next**.

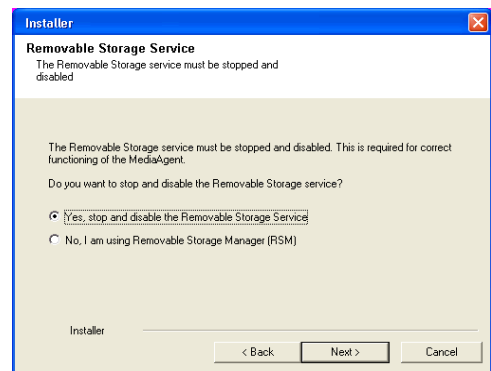


15. Select **Yes** to stop Removable Storage Services on the MediaAgent.
Click **Next**.

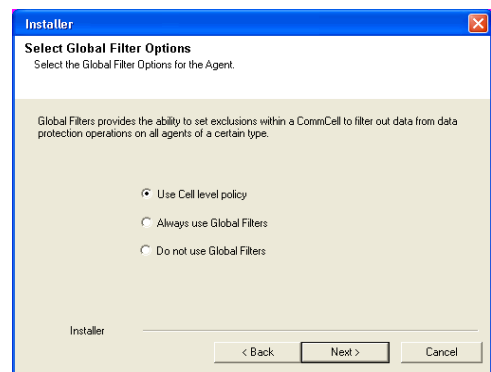
This prompt will not appear if Removable Storage Services are already disabled on the computer.



16. Click **Next**.



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



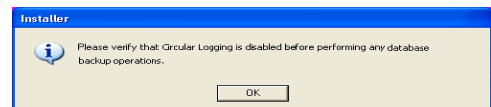
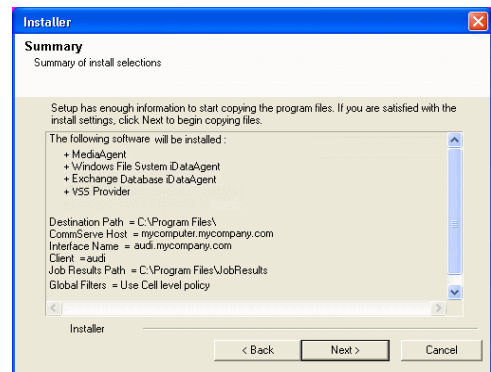
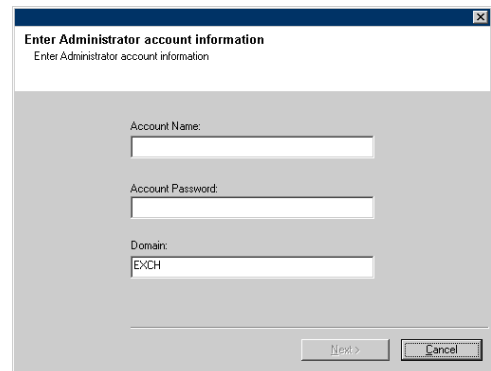
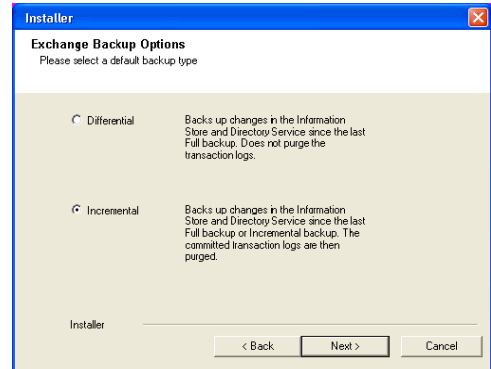
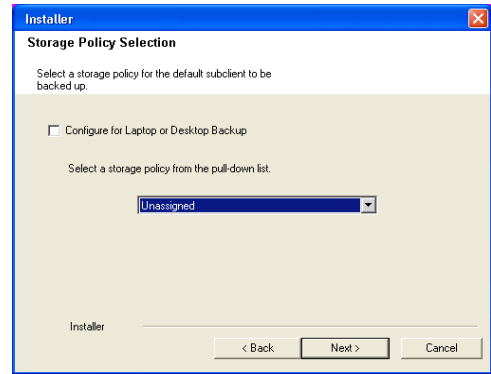
19. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.
 - **Differential** - Specifies that each non-full Exchange Database backup secures all data that has changed since the last full backup. Transaction logs are not purged.
 - **Incremental**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

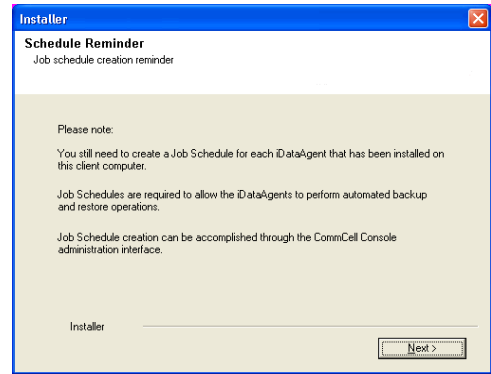
20. Click **Next**.

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.

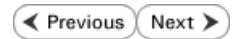
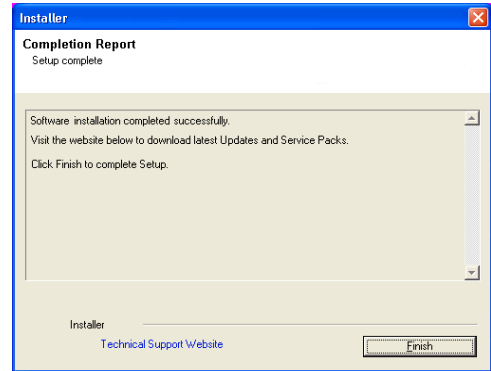
Click **OK**.



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**.

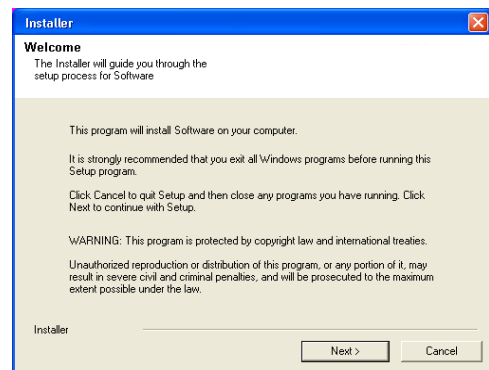
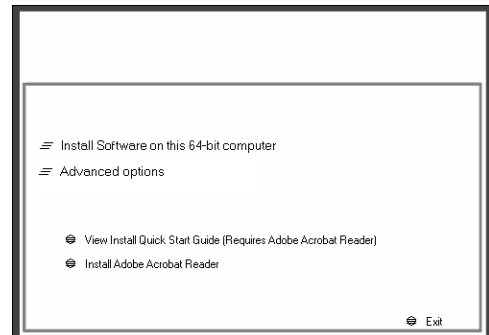
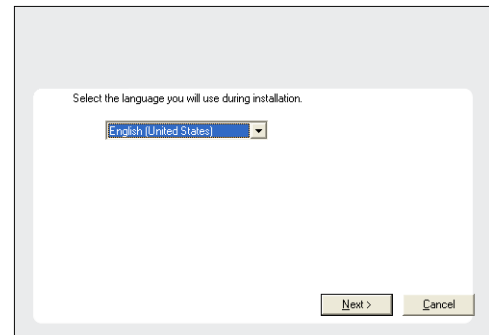
BEFORE YOU BEGIN

Download Software Packages

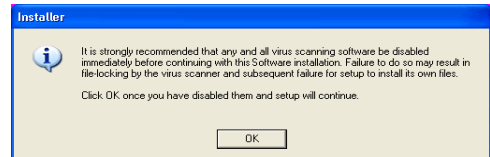
Download the latest software package to perform the install.

SnapProtect Support - Platforms

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



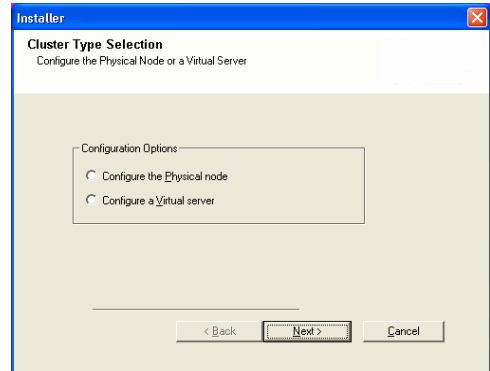
7. Select **I accept the terms in the license agreement**.
Click **Next**.



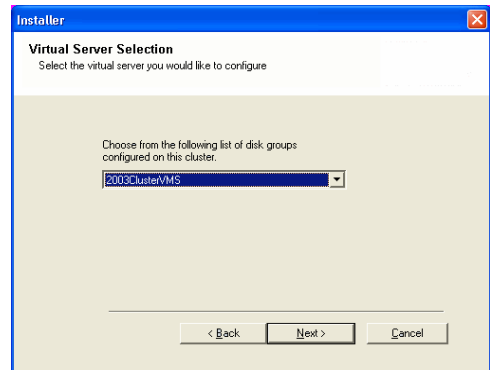
8. Select **Configure a Virtual Server**.
Click **Next**.



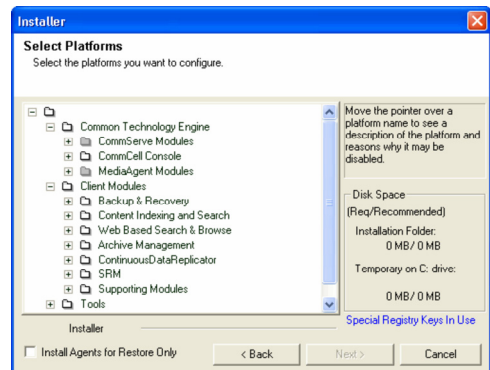
9. Select the disk group in which the virtual server resides.
Click **Next**.



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**.

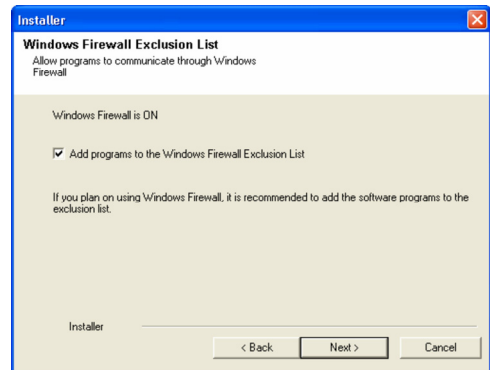
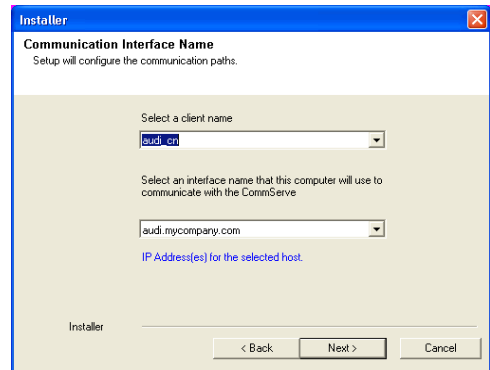
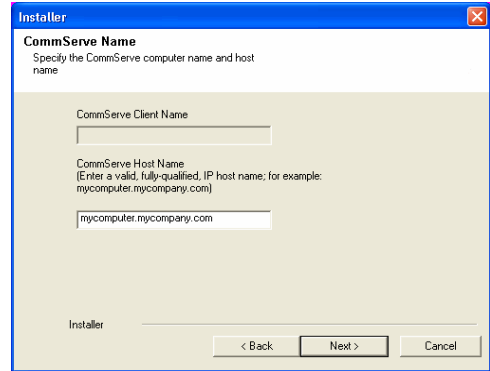
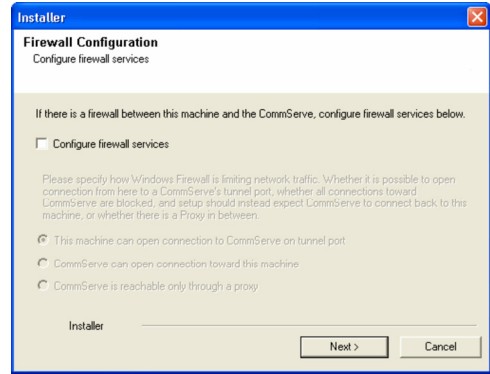
14. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

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.

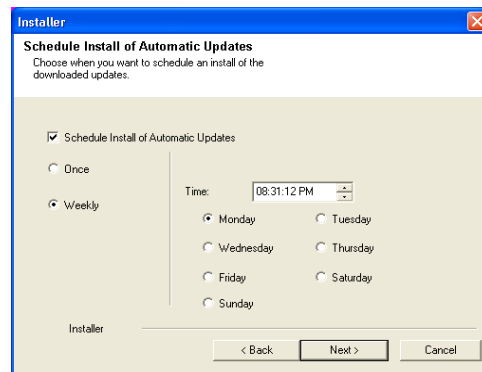
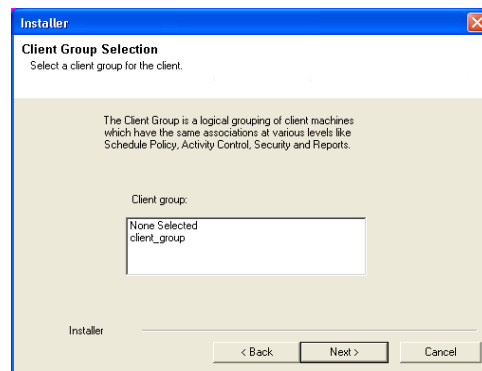
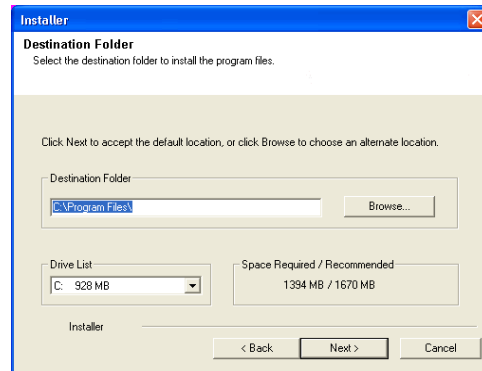
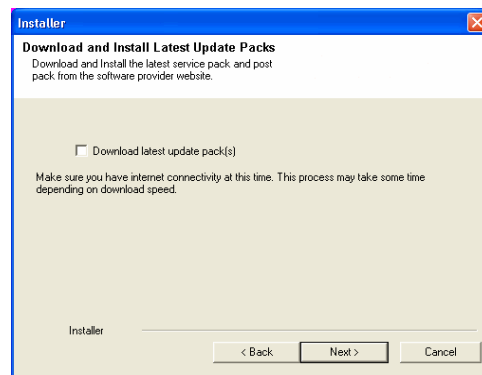
Click **Next**.

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

18. Click **Next**.

19. Select a **Storage Policy**.

Click **Next**.



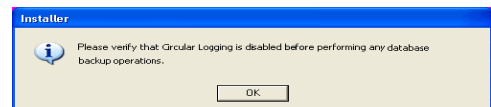
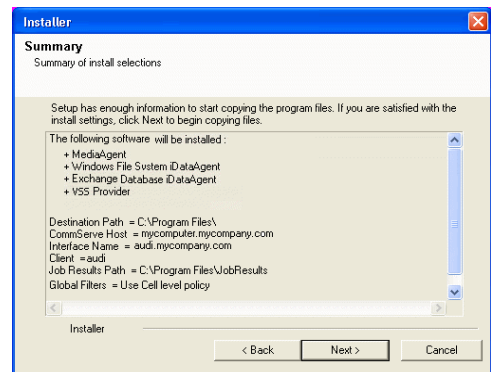
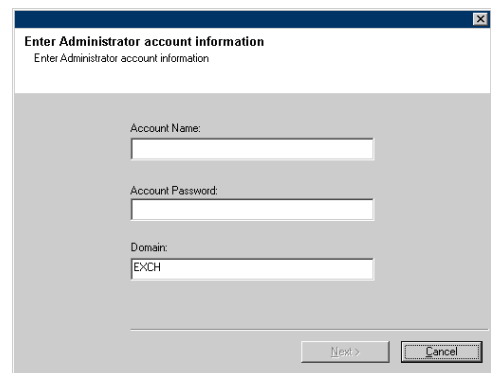
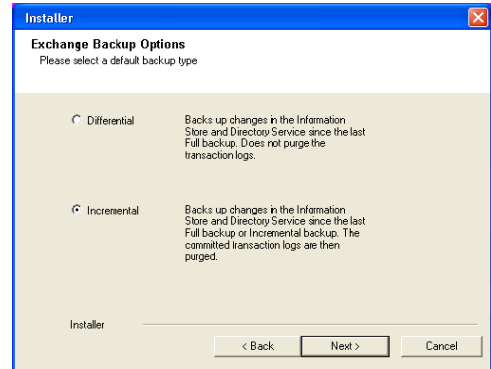
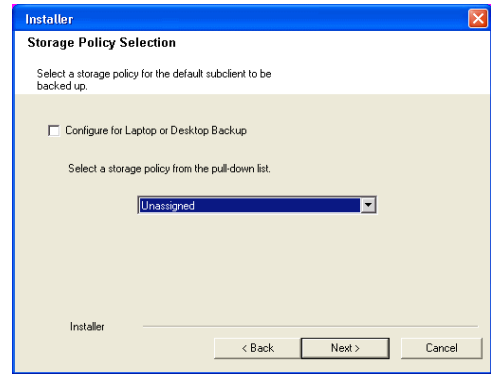
20. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.
- **Differential** - Specifies that each non-full Exchange Database backup secures all data that has changed since the last full backup. Transaction logs are not purged.
 - **Incremental**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

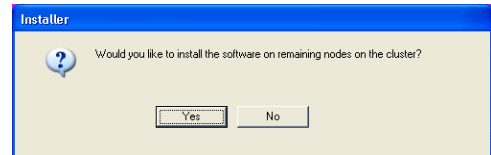
22. Click **Next**.

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**.

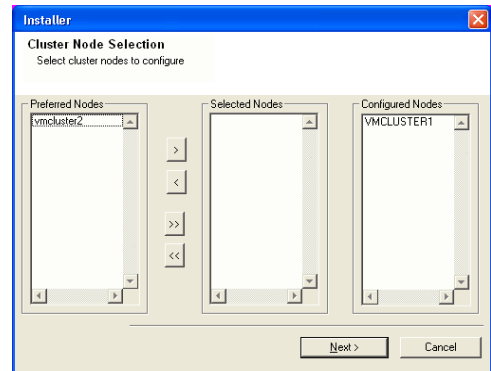


24. To install the software on the remaining nodes of the cluster, click **Yes**.
To complete the install for this node only, click **No**.



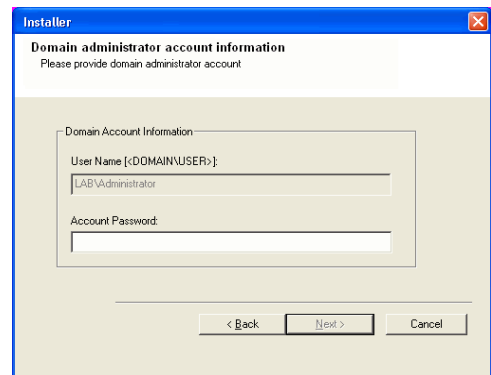
25. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.
Once you complete your selections, click **Next**.

- 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**.



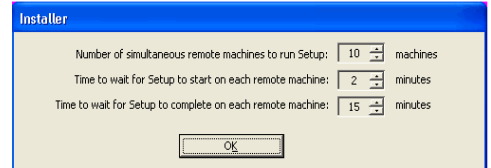
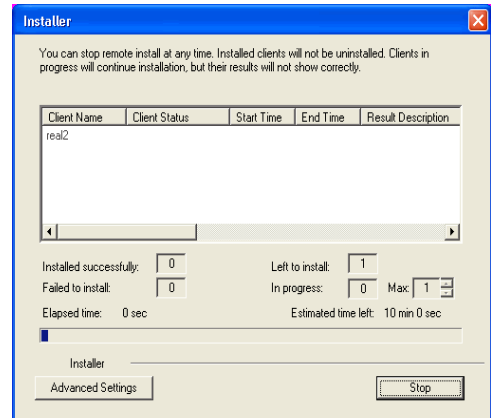
27. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

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*.

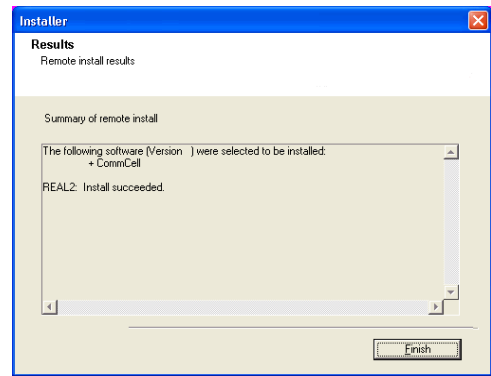


28. Read the summary for remote installation to verify that all selected nodes were installed successfully.

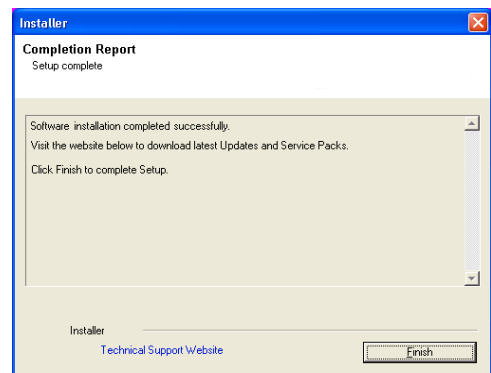
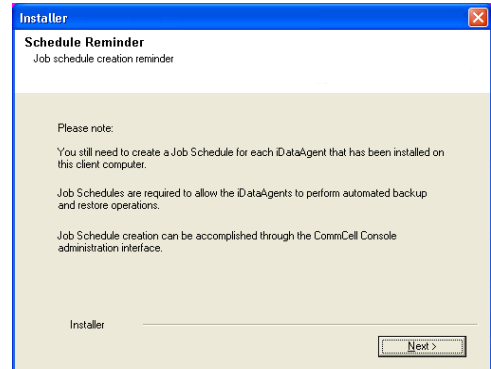
Click **Next**.

- 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



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

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**.

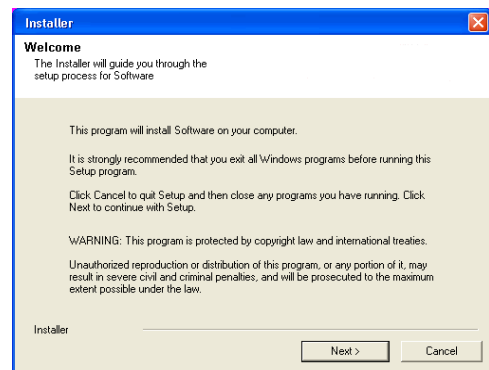
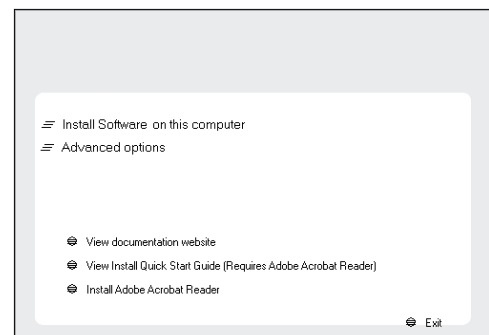
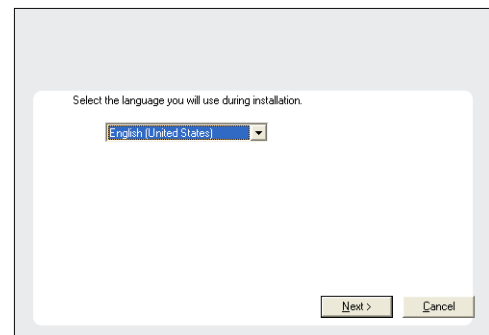
BEFORE YOU BEGIN

Download Software Packages

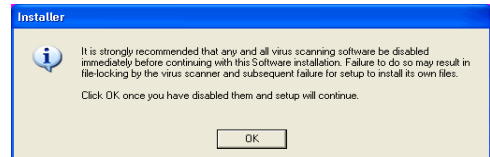
Download the latest software package to perform the install.

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.**



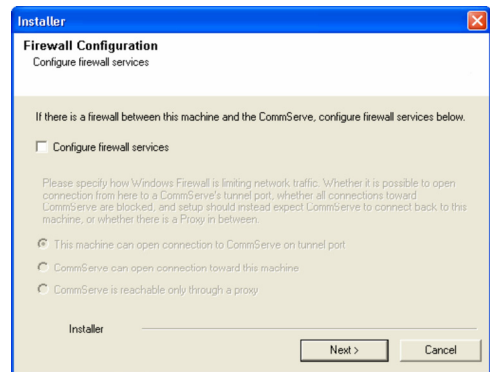
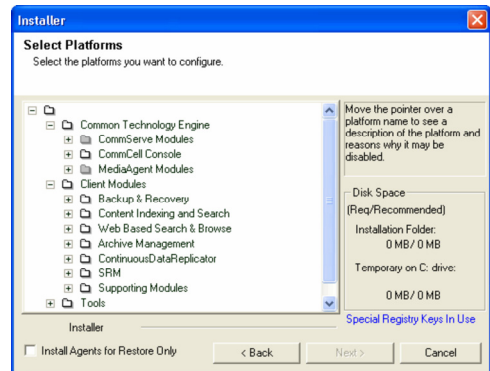
10.
 - Expand **Client Modules | Backup & Recovery | Exchange**, and select **Exchange Database /DataAgent.**
 - Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent.**
 - Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider.**
 - Click **Next.**



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.

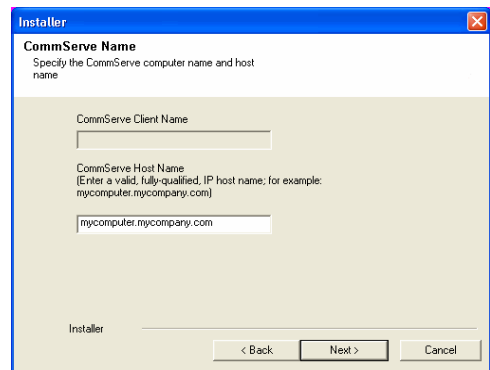
If firewall configuration is not required, click **Next.**



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:

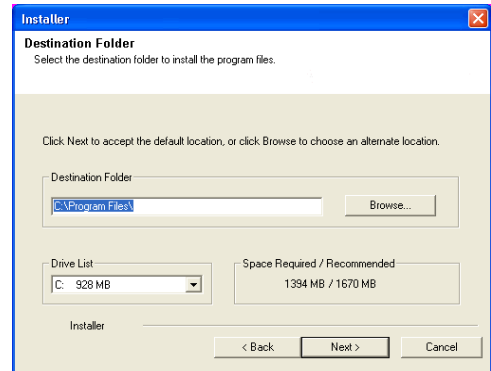
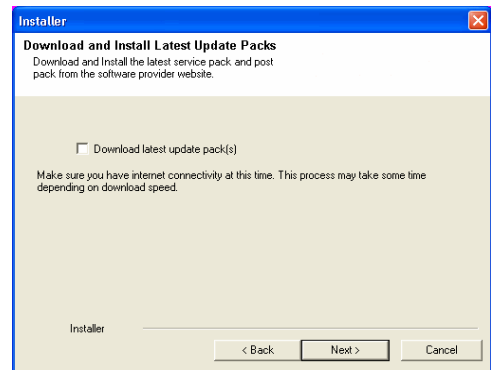
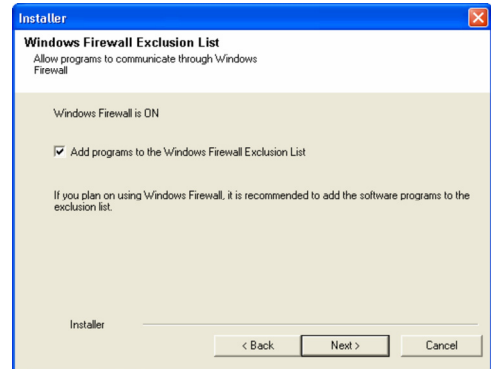
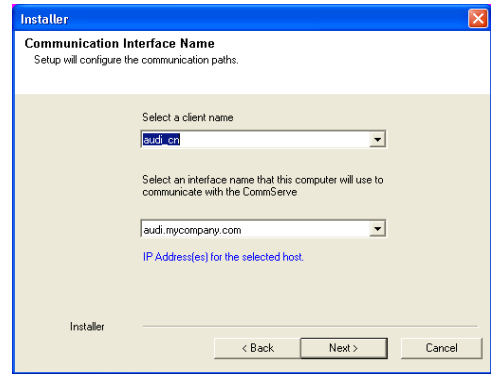
/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

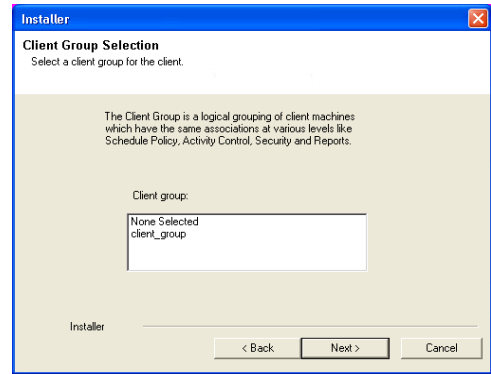
17. Select a Client Group from the list.

Click **Next**.

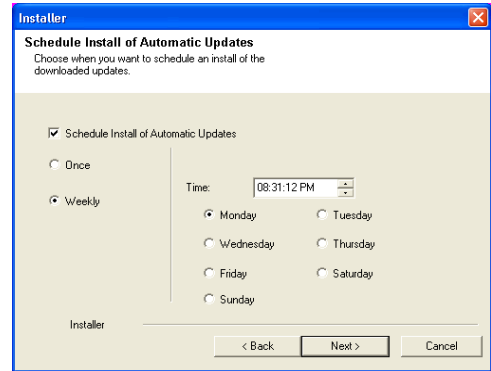
This screen will be displayed if Client Groups are configured in the CommCell Console.



18. Click **Next**.

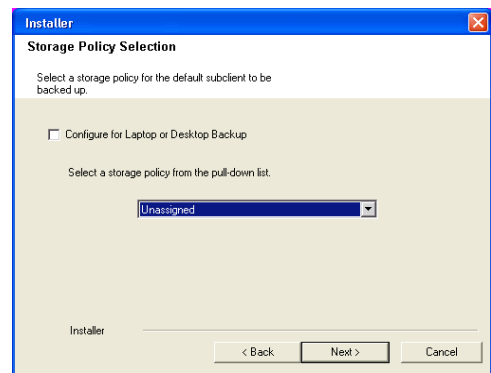


19. Select a **Storage Policy**.
Click **Next**.



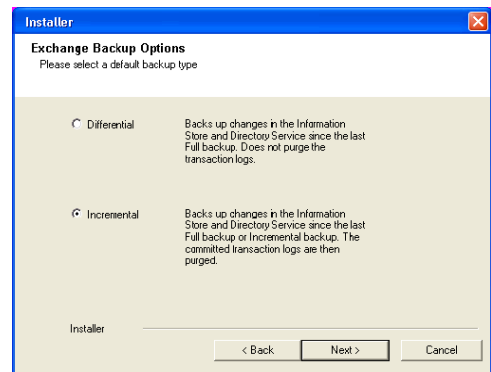
20. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.

- **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.

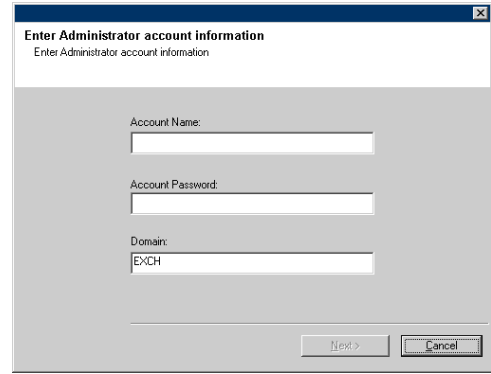


21. Enter the user credentials to access the Exchange Server to perform the backup operation.

- 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**.

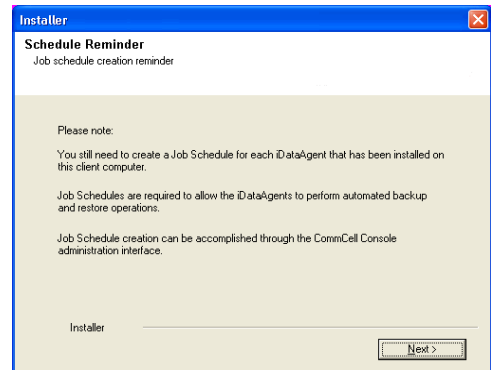
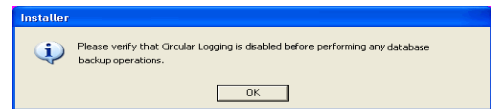
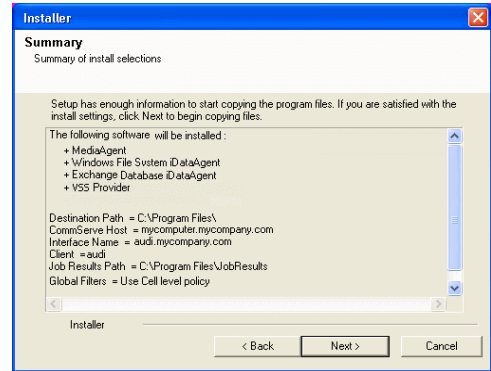


23. The install program displays a reminder to verify that Circular Logging is disabled before performing any database backup operations. To verify that Circular Logging is disabled:

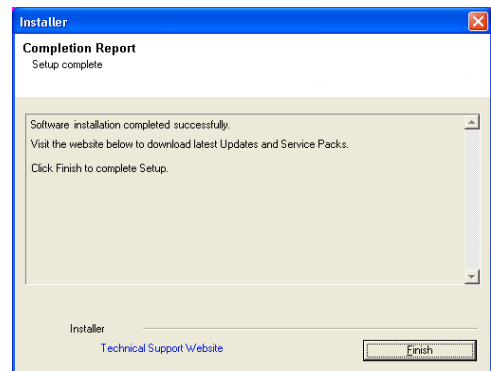
- From Exchange System Manager, navigate to and expand the server that the Database iDataAgent is being installed on.
- Verify that the Circular Logging check box has not been selected for each Storage Group. If Circular Logging has been enabled for a Storage Group, disable it at this time.

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

- 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**.

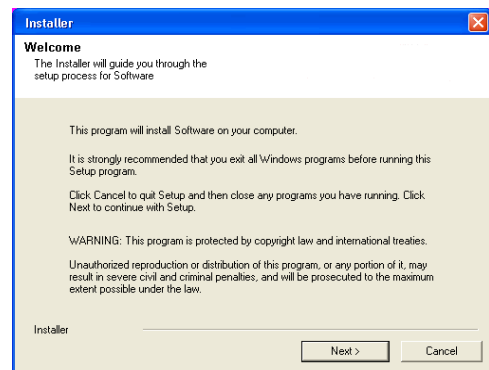
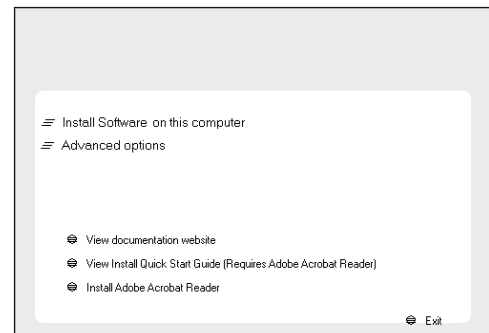
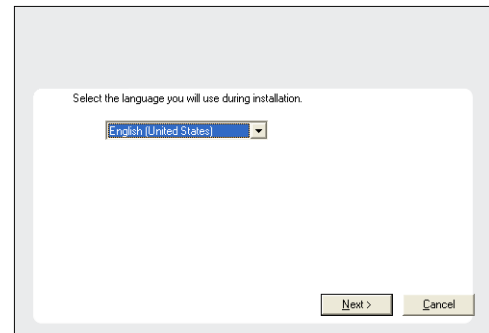
BEFORE YOU BEGIN

Download Software Packages

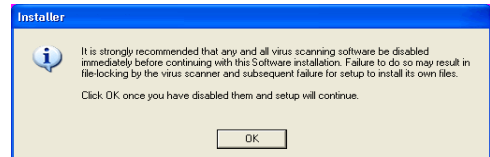
Download the latest software package to perform the install.

SnapProtect Support - Platforms

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



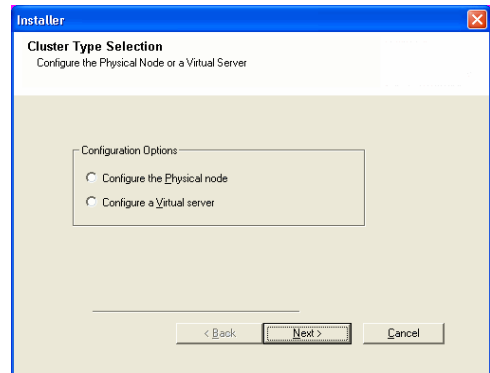
7. Select **I accept the terms in the license agreement**.
Click **Next**.



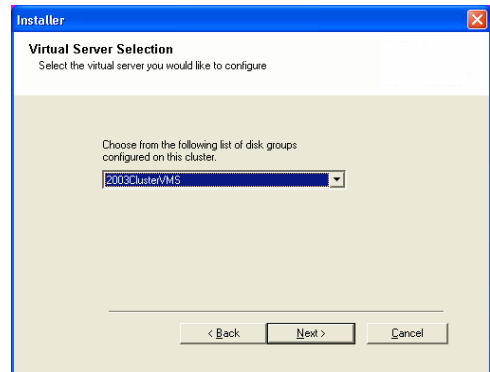
8. Select **Configure a Virtual Server**.
Click **Next**.



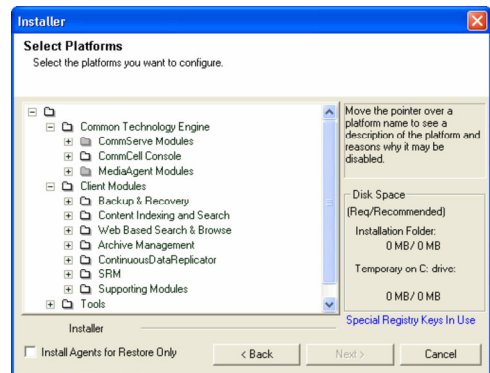
9. Select the disk group in which the virtual server resides.
Click **Next**.



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**.

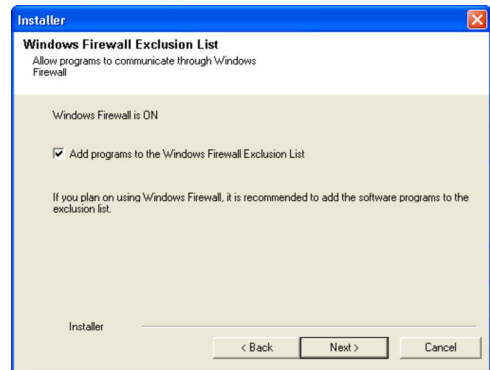
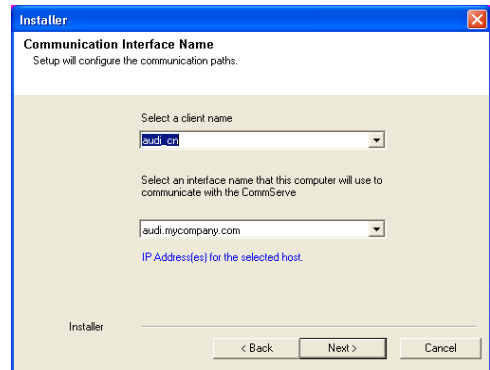
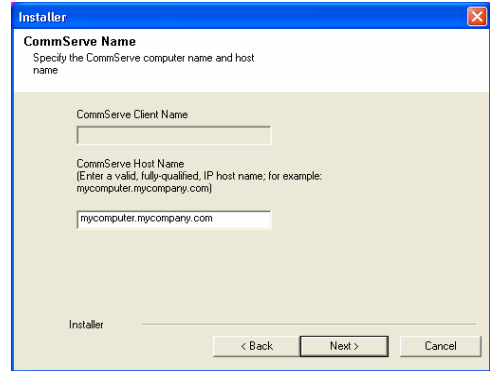
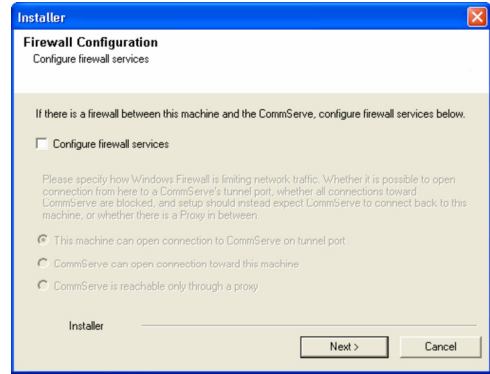
14. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

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.

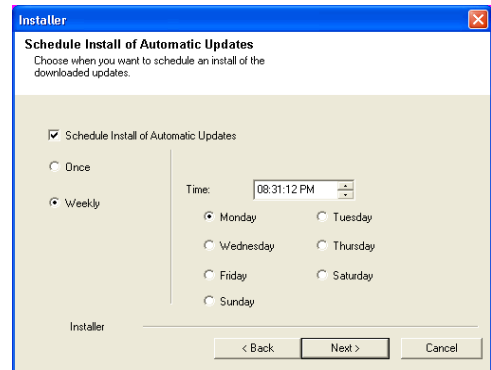
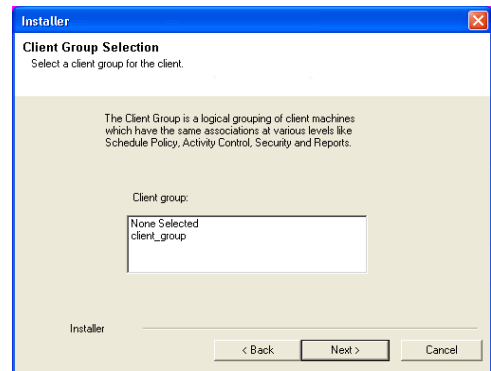
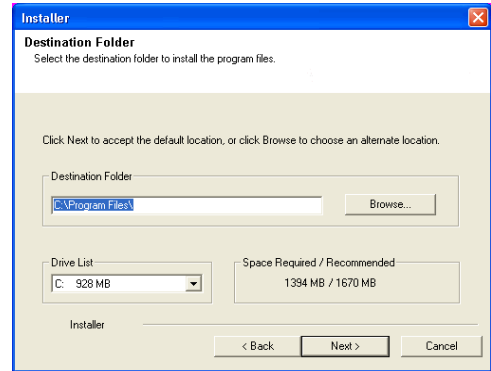
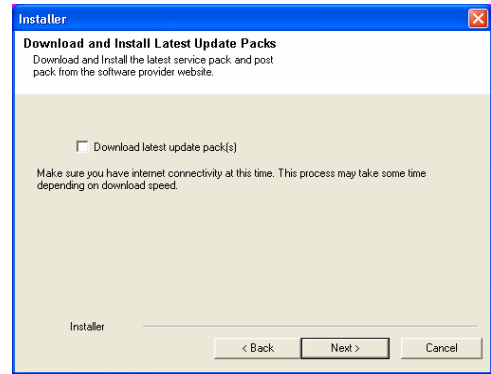
Click **Next**.

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

18. Click **Next**.

19. Select a **Storage Policy**.

Click **Next**.



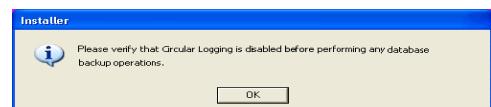
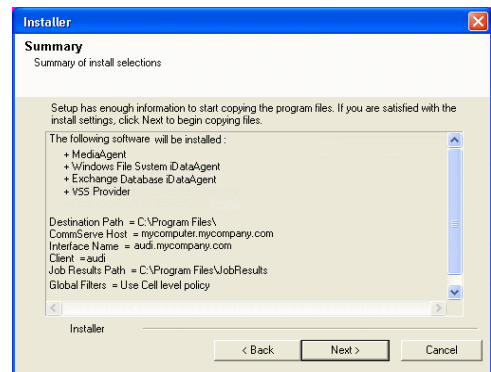
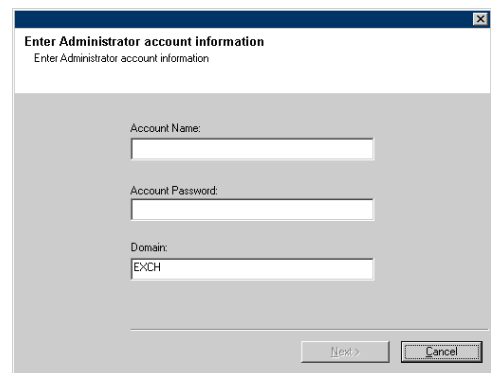
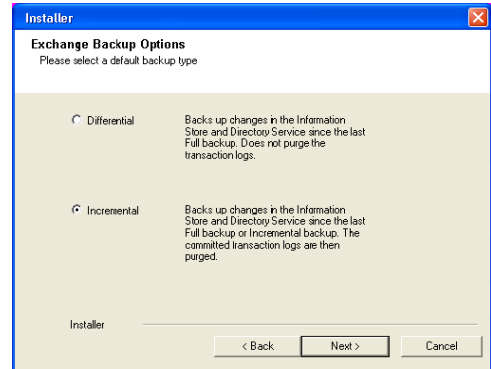
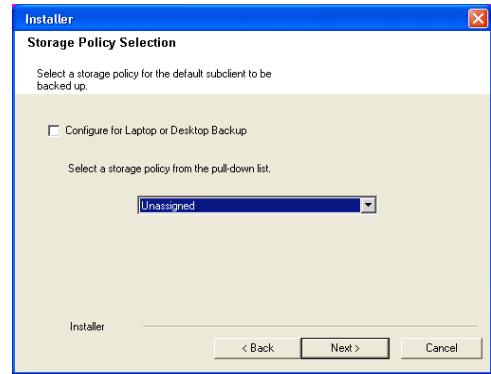
20. Select the backup type for Exchange Database backups. Choose either of the following options, then click **Next**.
- **Differential** - Specifies that each non-full Exchange Database backup secures all data that has changed since the last full backup. Transaction logs are not purged.
 - **Incremental**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

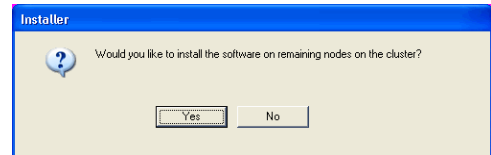
22. Click **Next**.

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.

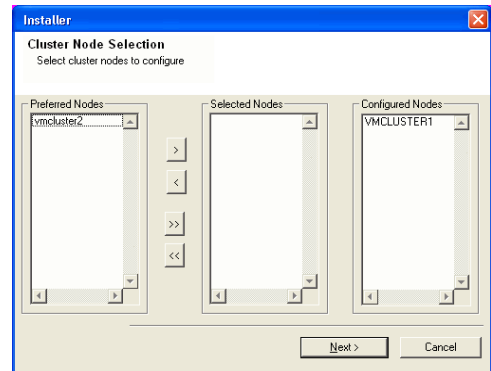
Click **OK**.



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

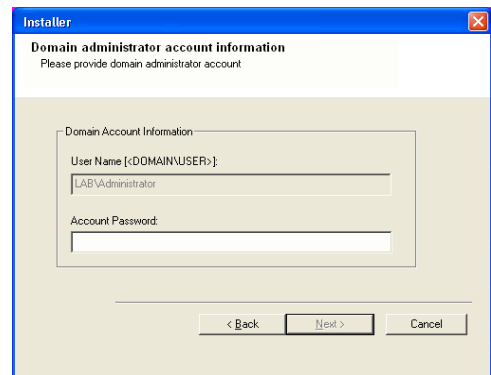


25. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.
Once you complete your selections, click **Next**.



- 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**.

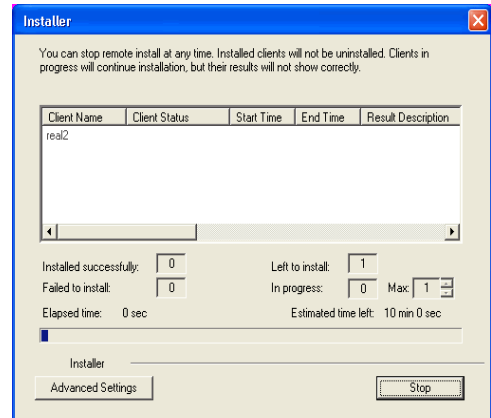
27. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

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

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

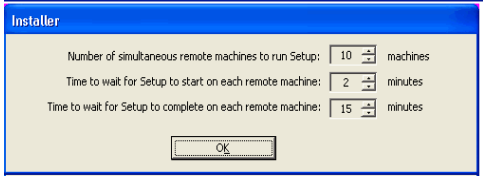
- Maximum number of nodes on which Setup can run simultaneously.
- Time allocated for Setup to begin executing on each node, after which the install attempt will fail.
- Time allocated for Setup to complete on each node, after which the install attempt will fail.

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*.



Advanced Settings

Stop

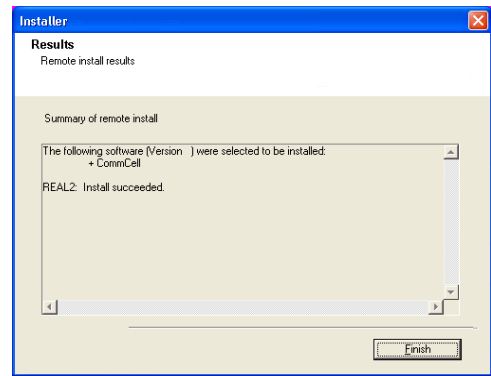


28. Read the summary for remote installation to verify that all selected nodes were installed successfully.

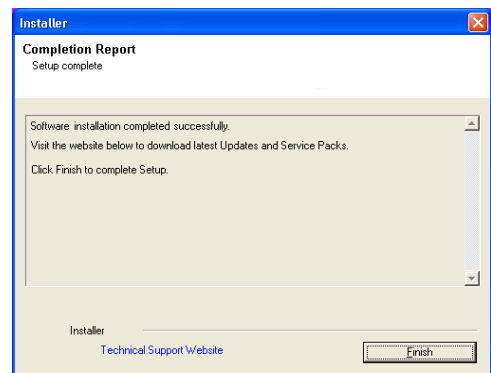
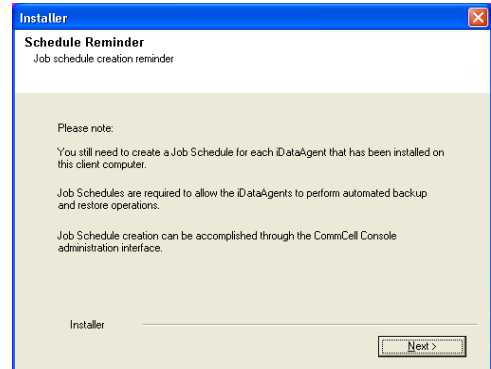
Click **Next**.

- 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 ▶

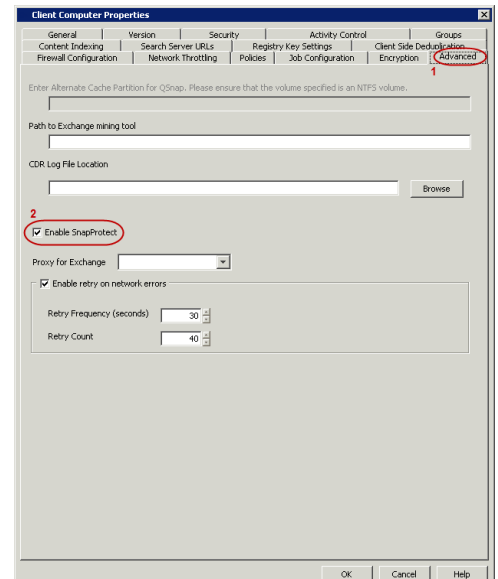
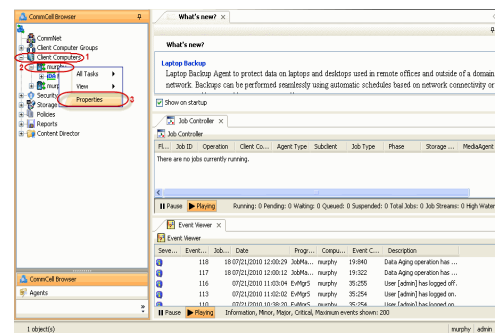
PRE-REQUISITES

- 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.

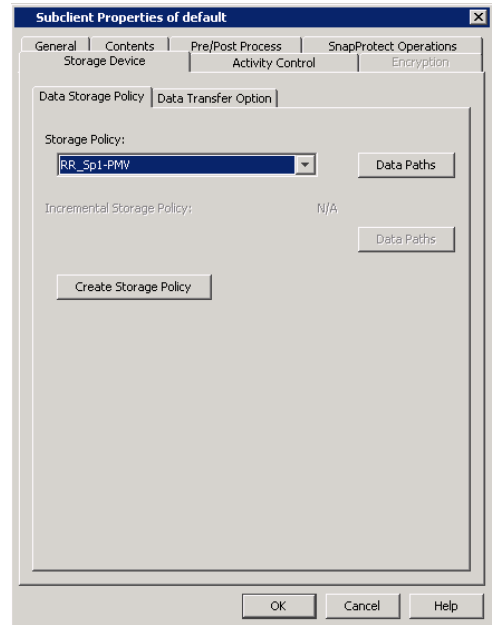
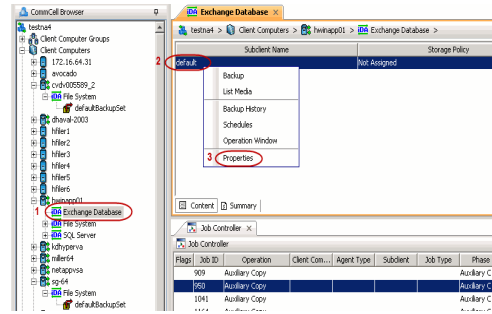
CONFIGURATION

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**.



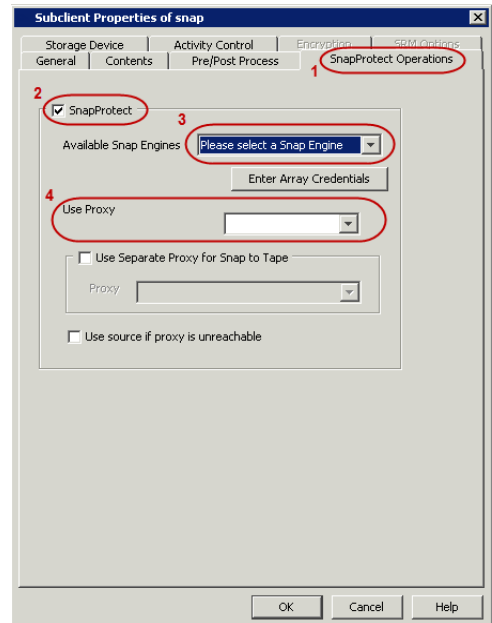
4.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.



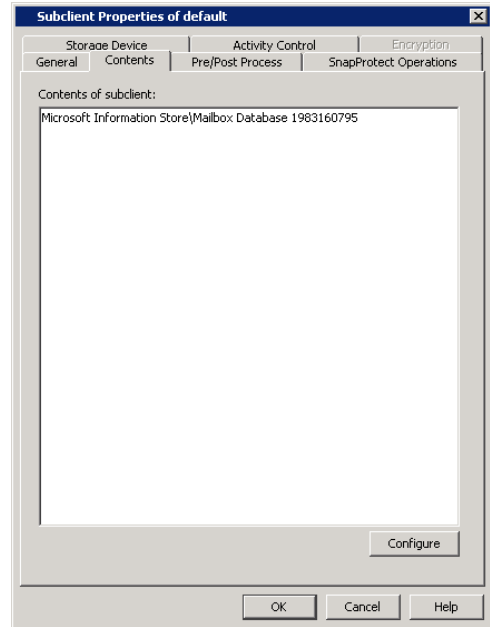
5.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy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

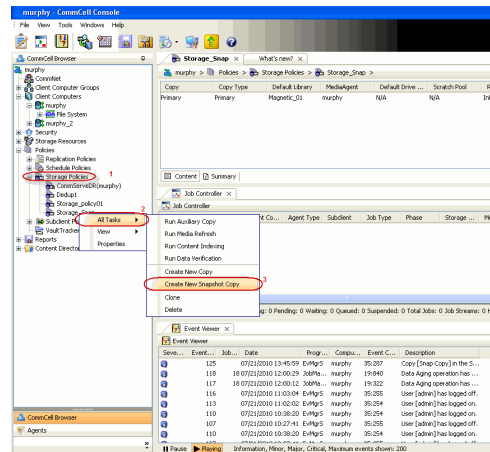
Click **Next** to Continue.

CREATE A SNAPSHOT COPY

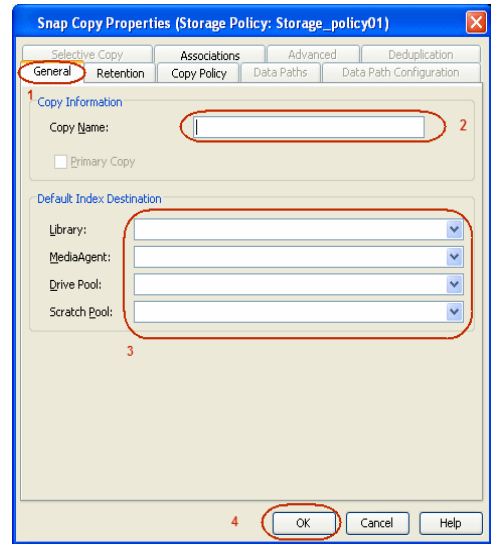


Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

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



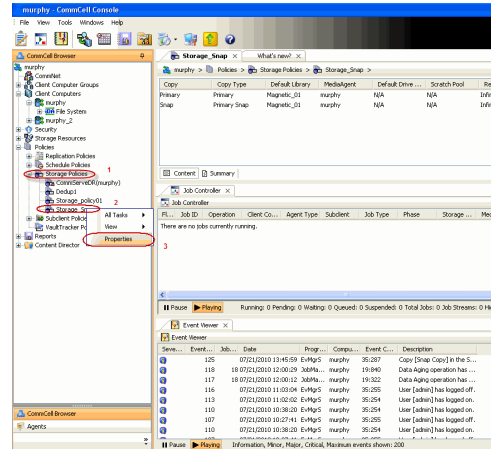
2.
 - Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



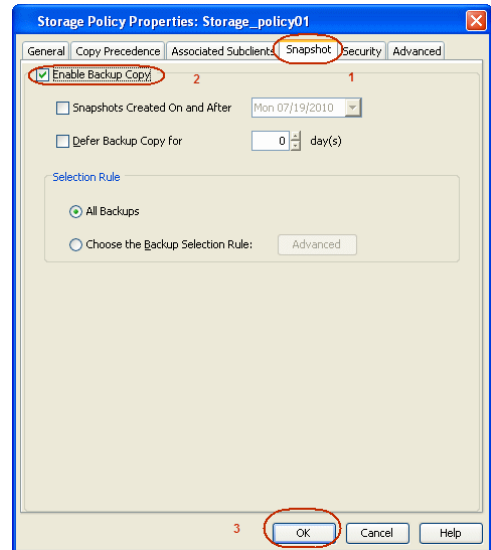
CONFIGURE BACKUP COPY

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 ▶

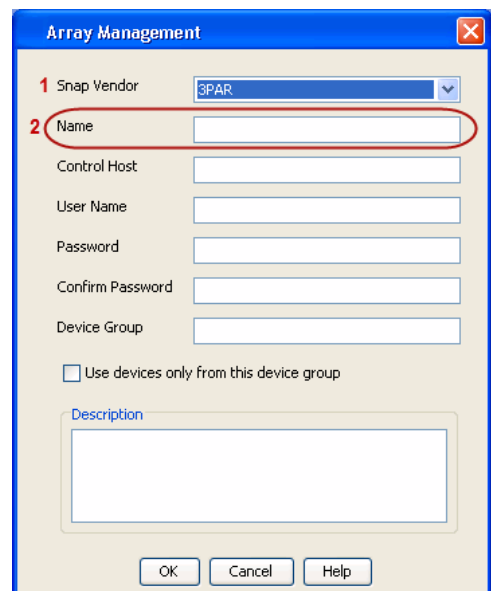
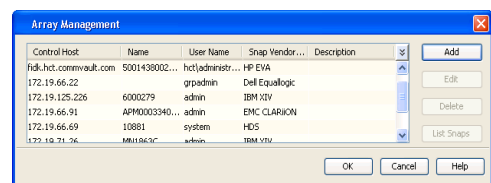
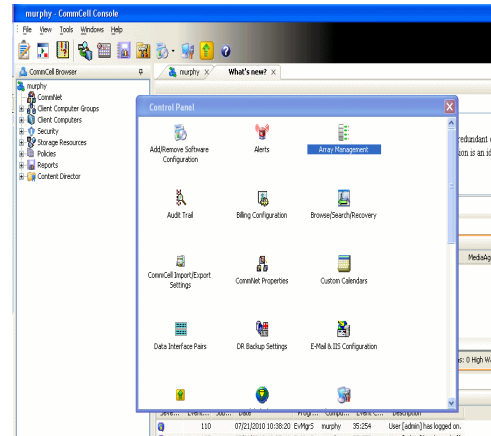
PRE-REQUISITES

- 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 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

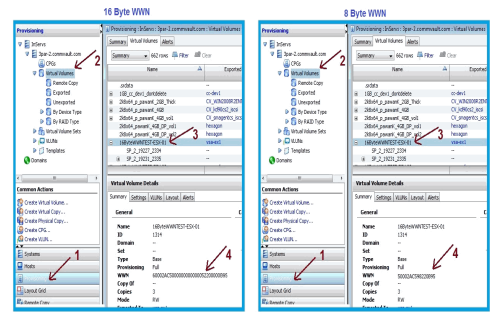
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

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

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

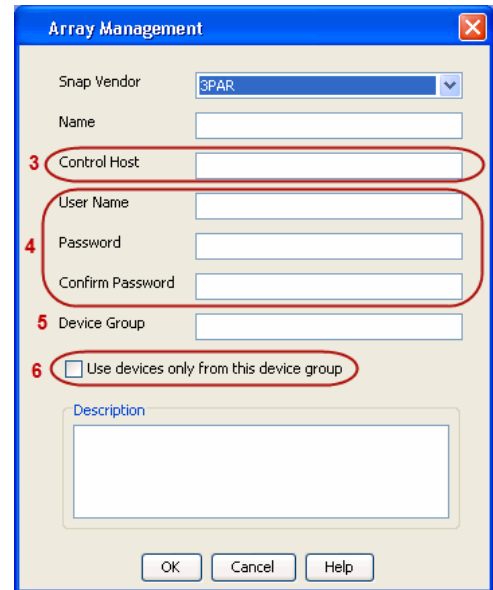
$\text{DevID.substr}(4,3)$ is 2AC and $\text{DevID.substr}(26,6)$ is 000B95

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



4.

- 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

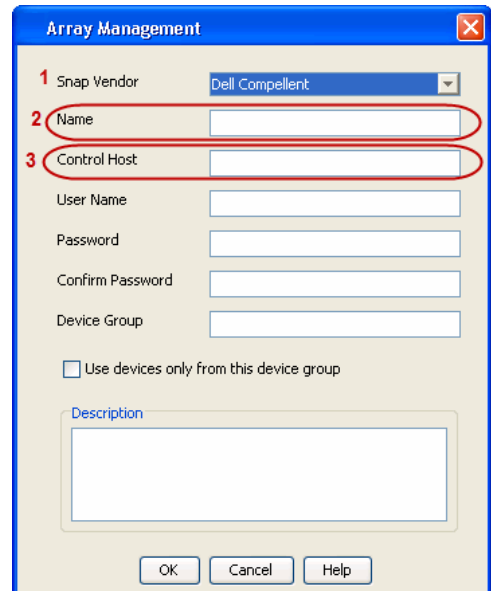
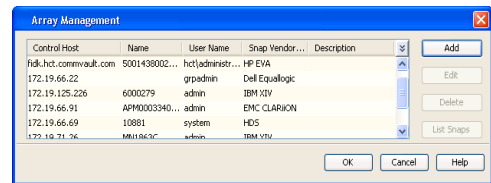
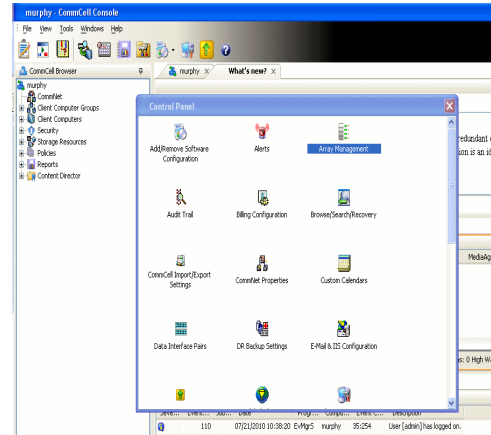
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

SETUP THE ARRAY INFORMATION

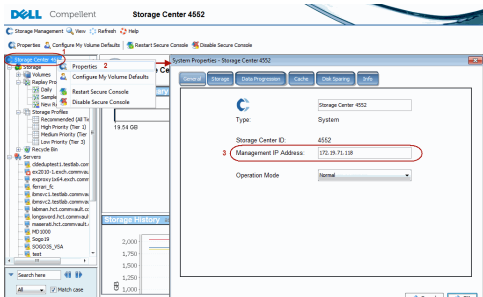
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- 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.

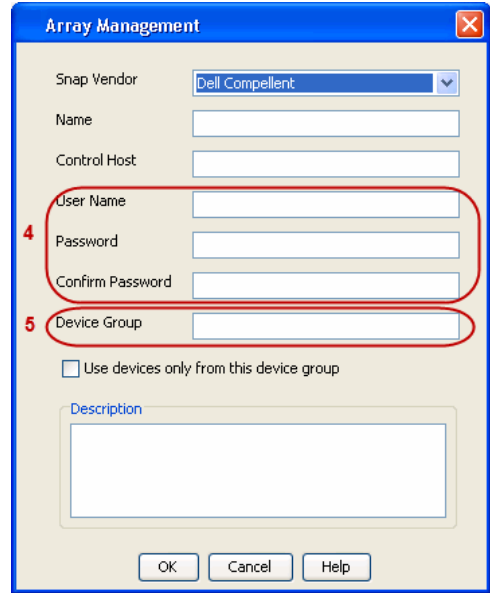
The Management IP address is also referred as the Storage Center IP address.



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

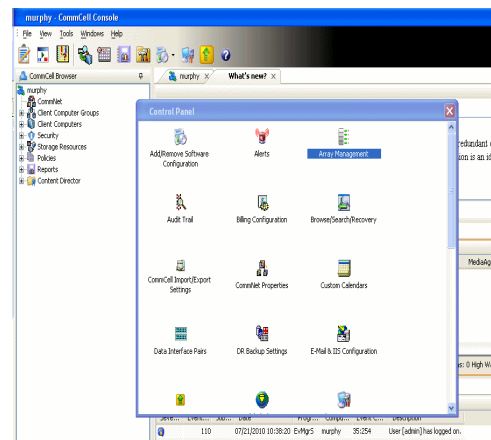
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing 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.

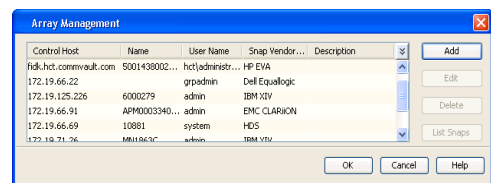
SETUP THE ARRAY INFORMATION

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**.

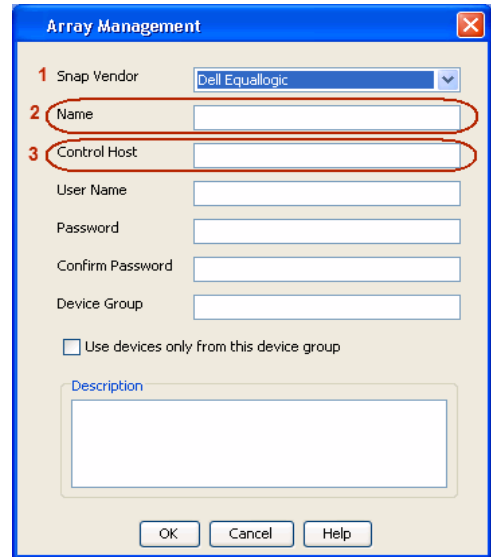


2. Click **Add**.

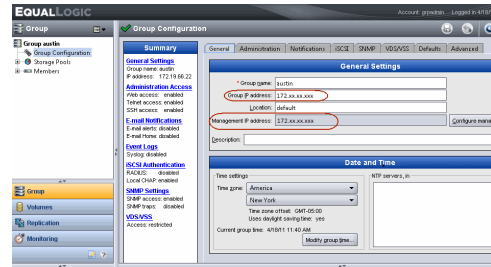


3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

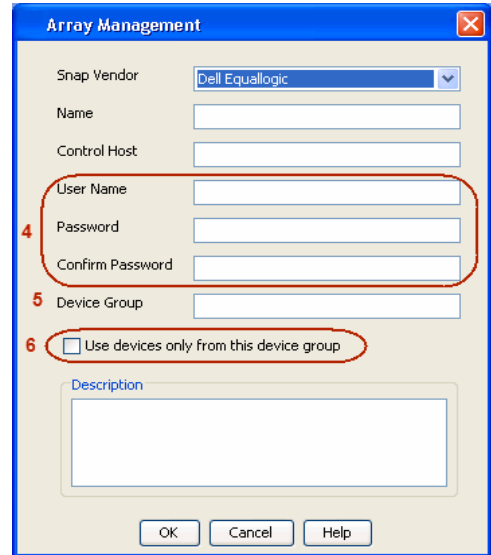
No entry is required in the **Name** field if there is no Management IP address configured.
 - Specify the Group IP address in the **Control Host** field.



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:

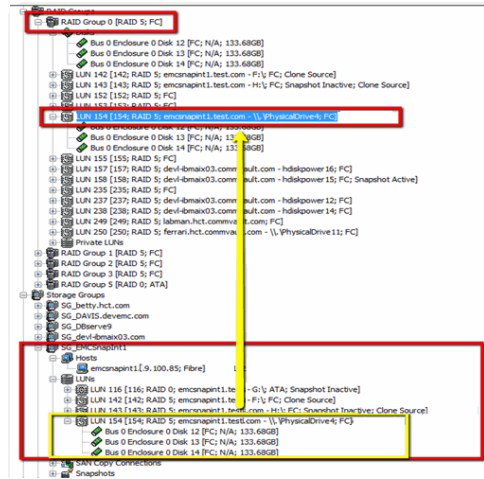
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

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.

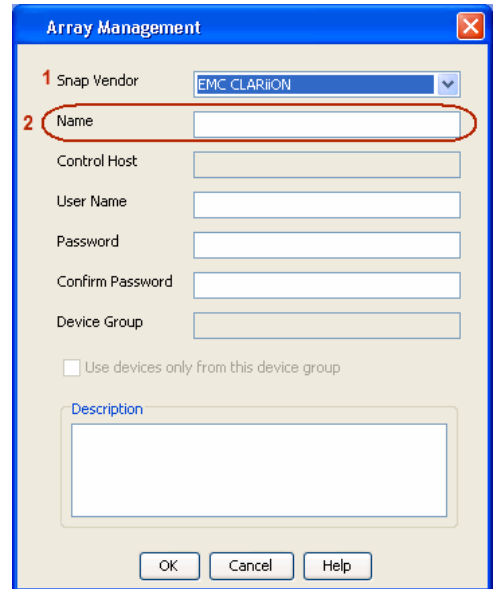
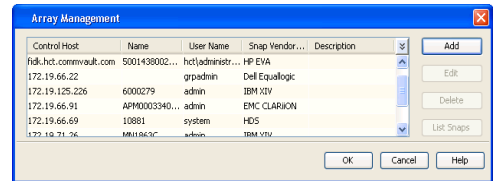
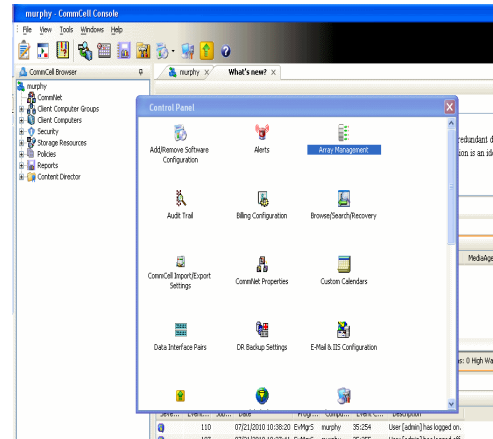
SETUP THE ARRAY INFORMATION

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

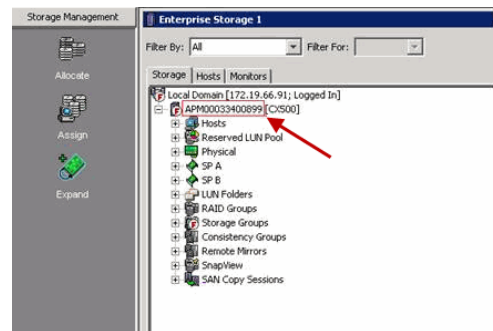
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

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

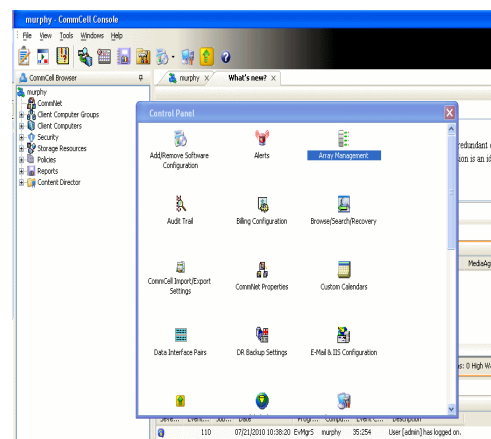
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

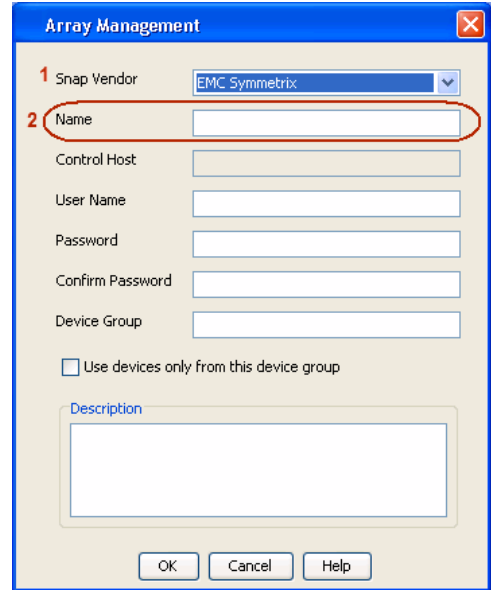
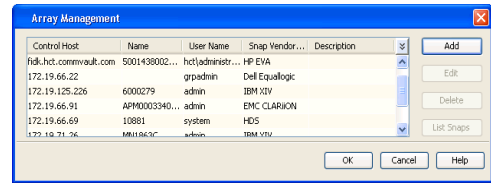
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

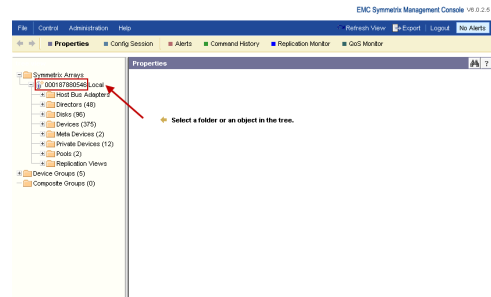


- Click **Add**.

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

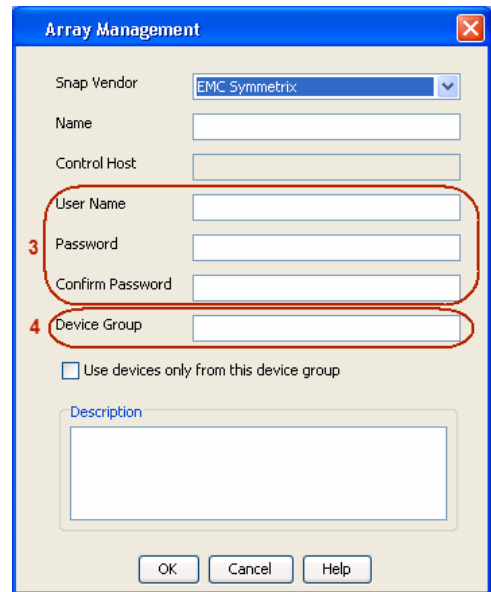


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.

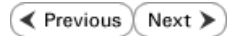


4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. 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



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

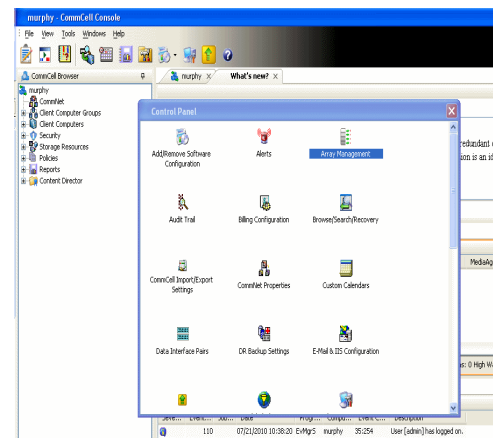
If pre-paired sessions are not available, destination volumes are automatically created for clone snapshots. If a non-existing device group is specified during array configuration in the CommCell Console, a destination volume is created based on the source volume type. However, if a valid device group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

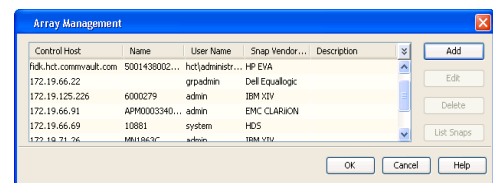
SETUP THE ARRAY INFORMATION

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**.

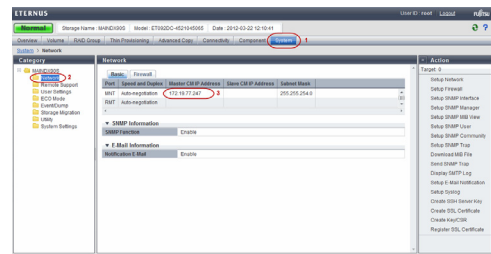
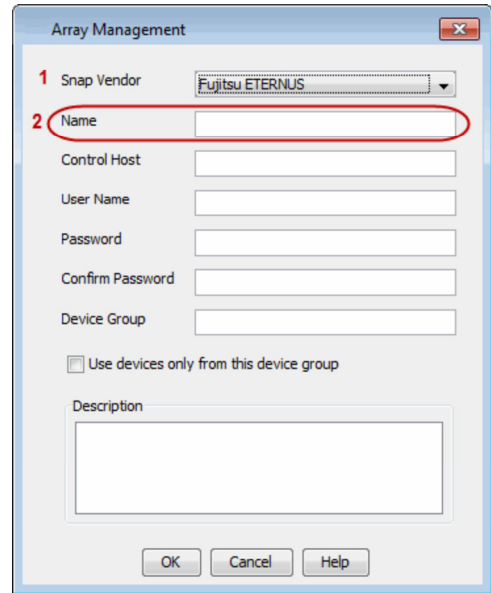


2. Click **Add**.

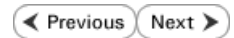
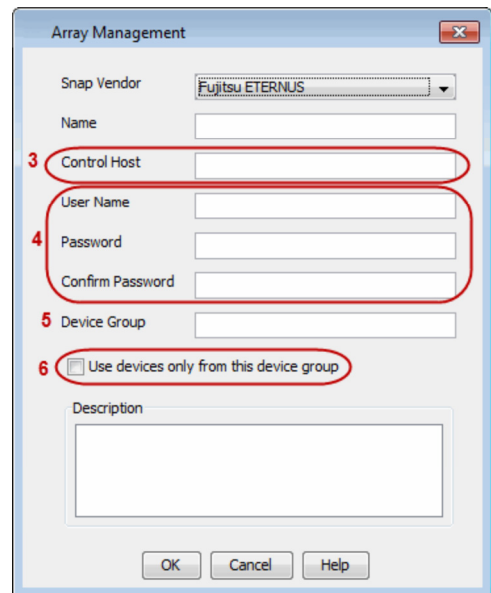


3.
 - Select **Fujitsu ETERNUS** from the **Snap Vendor** list.
 - Specify the CM IP Address of the array in the **Name** field.

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

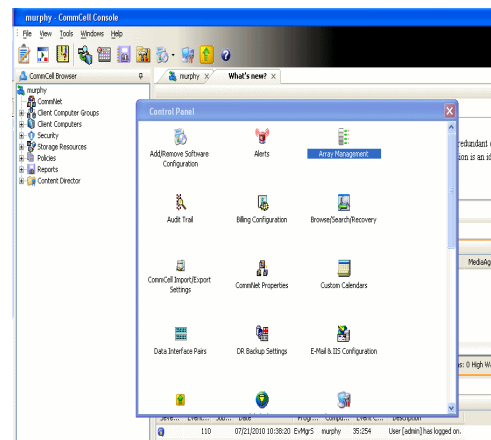
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

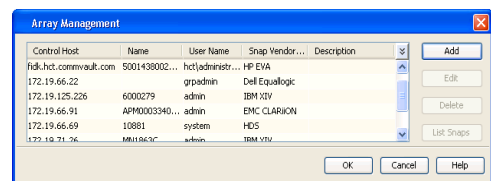
SETUP THE ARRAY INFORMATION

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

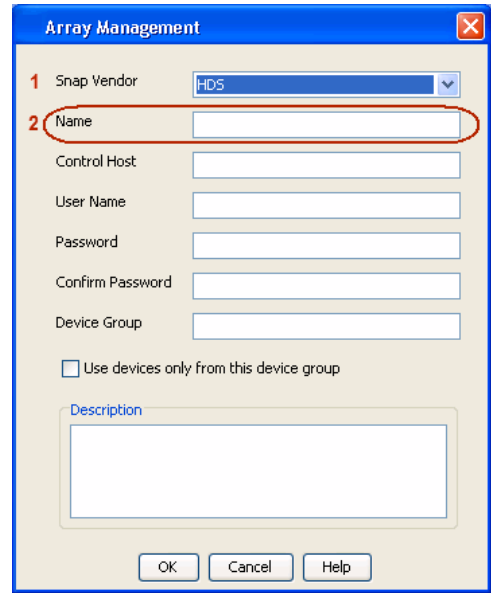
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



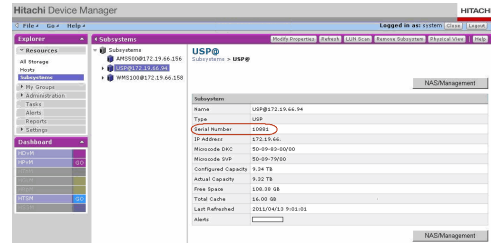
2. Click **Add**.



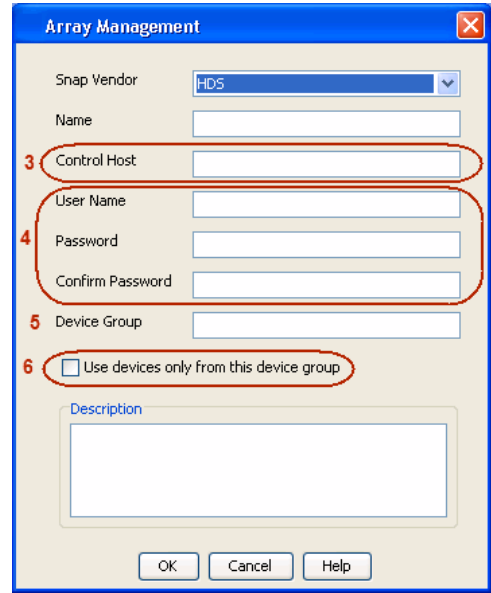
3.
 - Select **HDS** from the **Snap Vendor** list.
 - Specify the serial number of the array in the **Name** field.



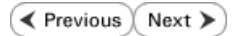
For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



- 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



SETUP THE HP SMI-S EVA

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

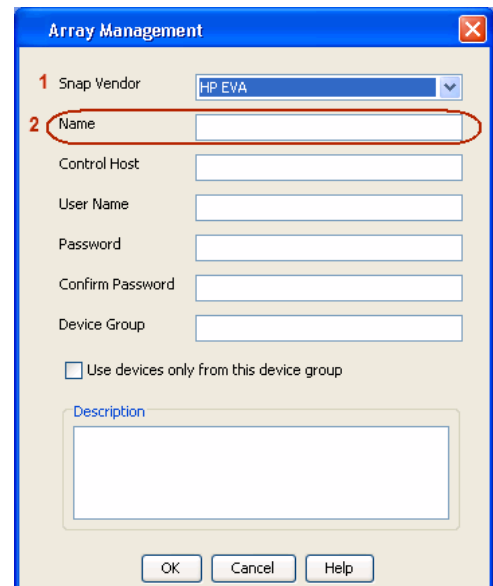
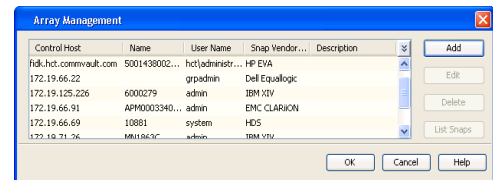
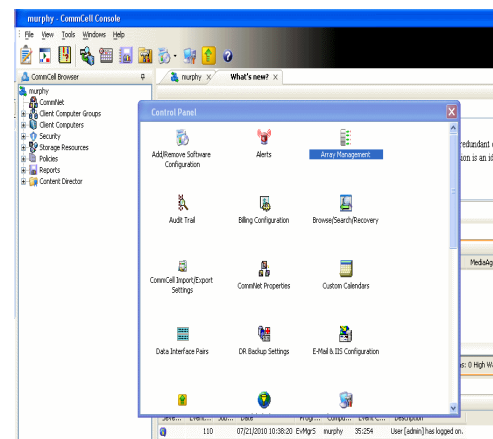
The following steps provide the necessary instructions to setup the HP EVA:

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

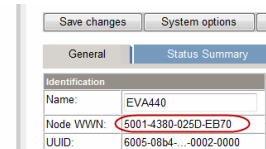
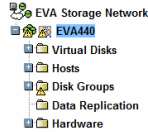
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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.

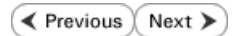
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



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 ▶

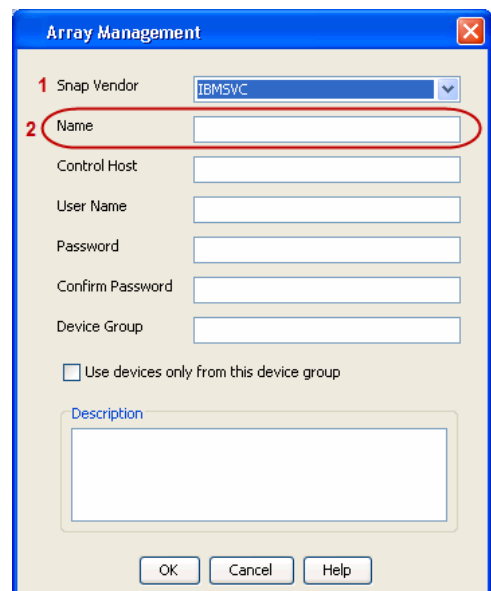
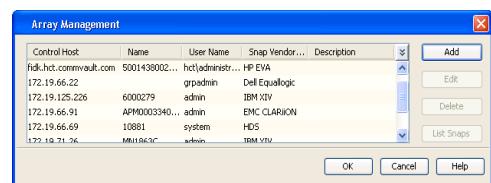
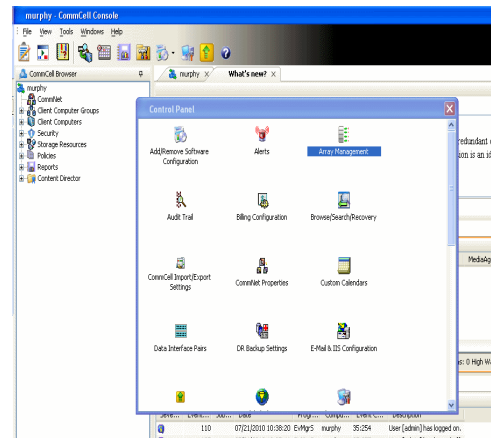
PRE-REQUISITES

- 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.

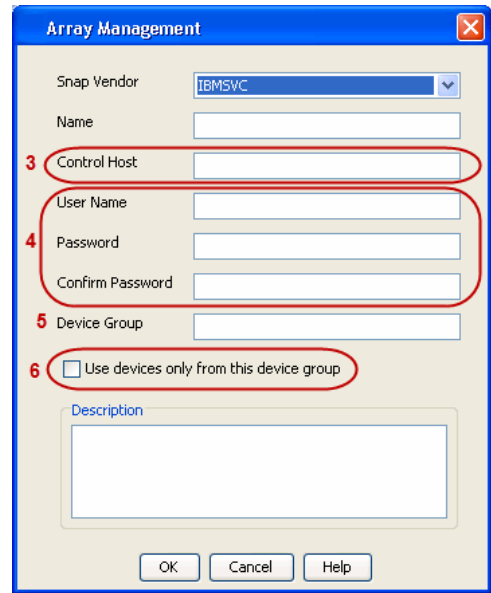
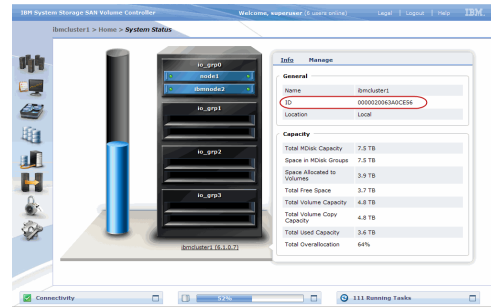
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



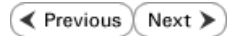
The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

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



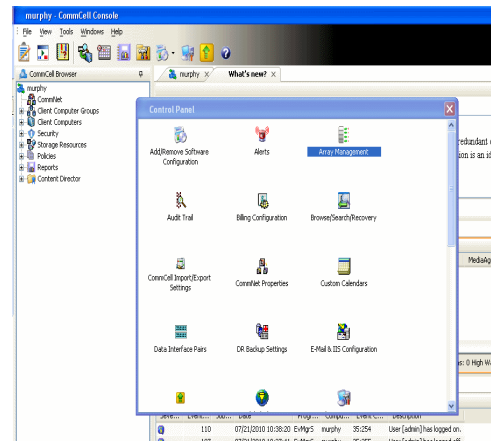
PRE-REQUISITES

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.

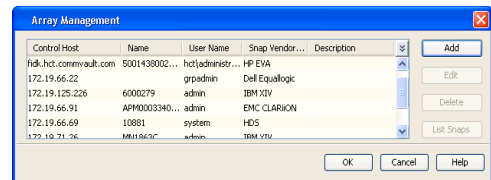
SETUP THE ARRAY INFORMATION

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

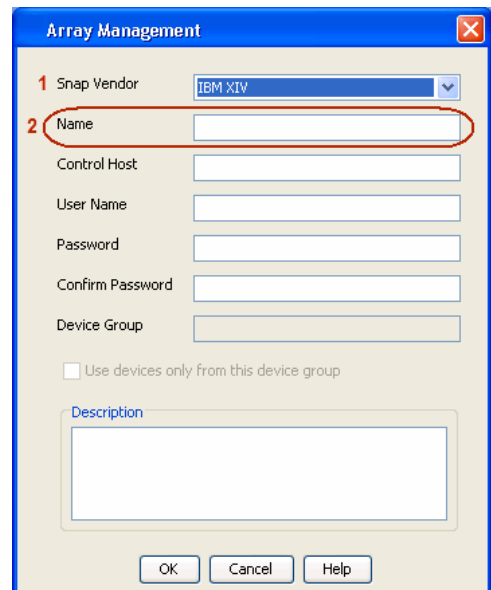
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



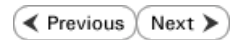
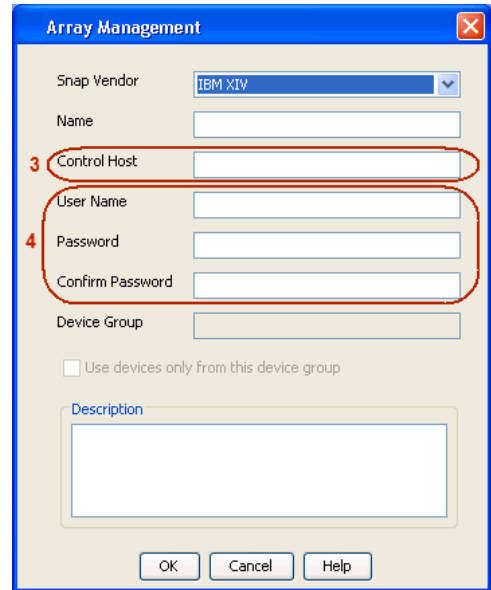
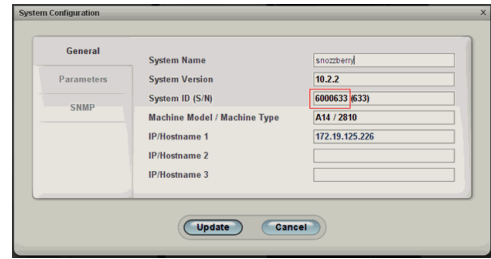
3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



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.

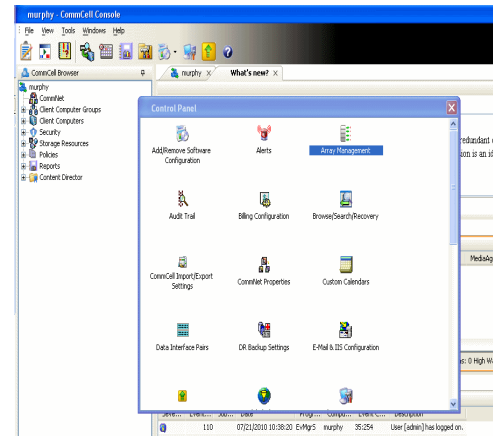
ADDITIONAL REQUIREMENTS FOR VMWARE

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.

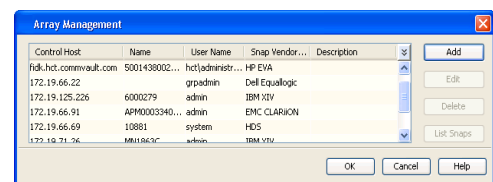
SETUP THE ARRAY INFORMATION

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

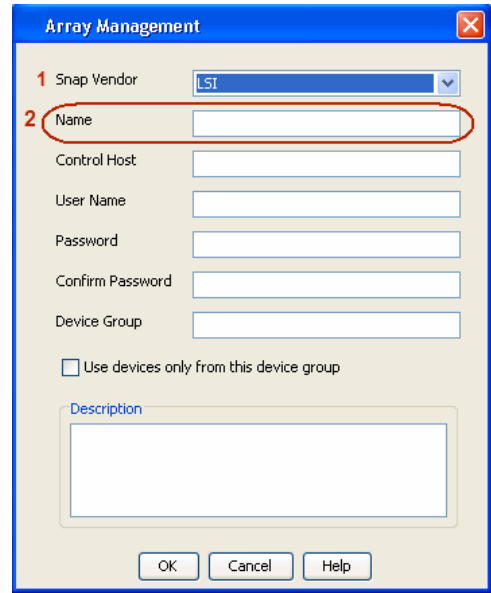
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

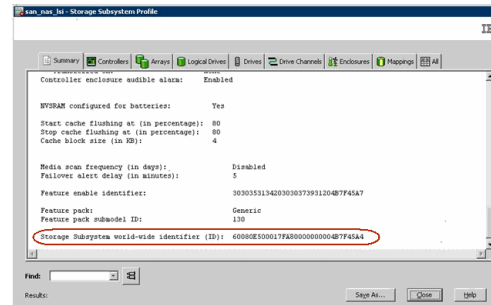


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



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

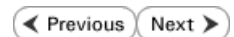
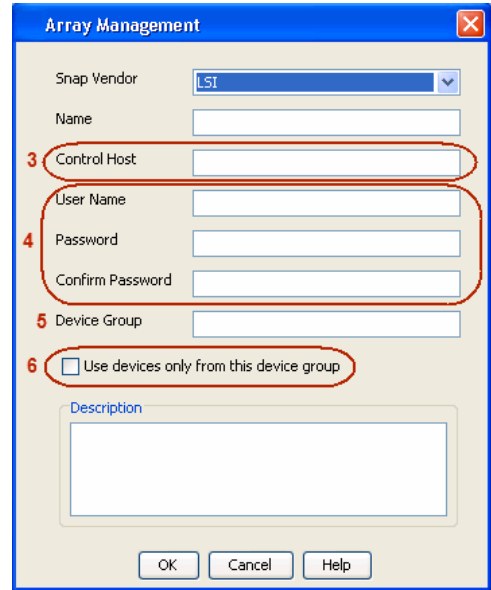
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



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: [Text Field]

Control Host: [Text Field]

User Name: [Text Field]

Password: [Text Field]

Confirm Password: [Text Field]

Device Group: [Text Field]

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

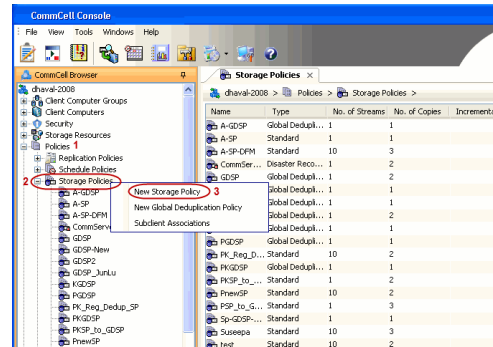
CONFIGURATION

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

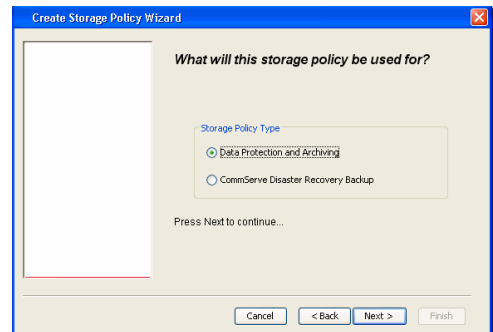
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

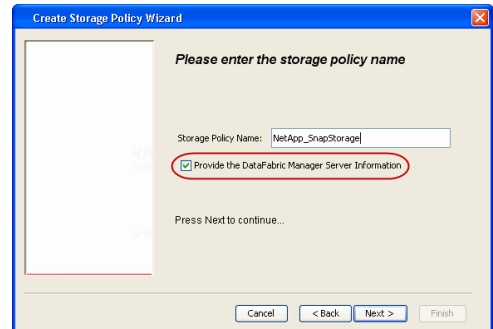
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



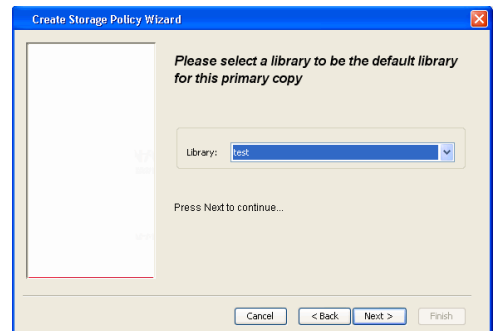
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



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

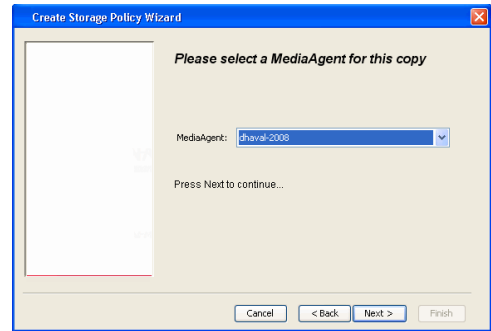
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

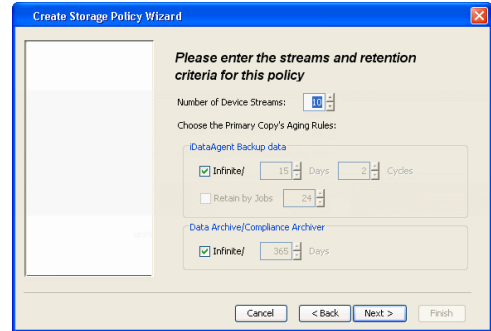


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

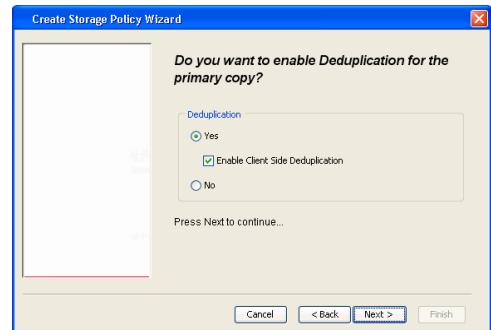
6. Click **Next**.



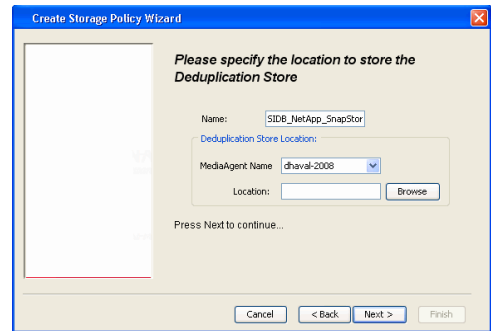
7. Click **Next**.



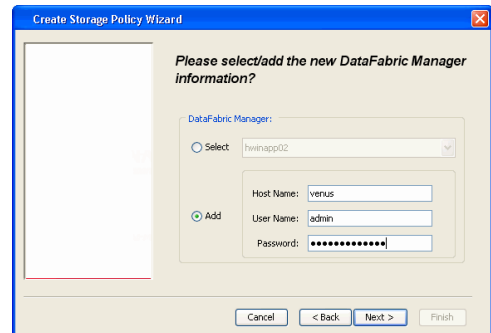
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

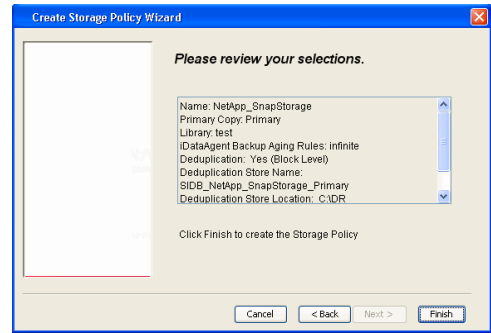


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



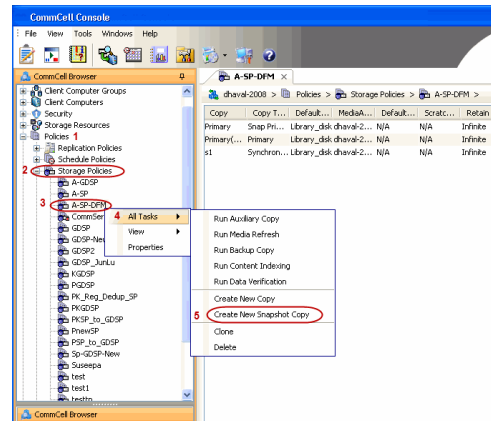


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

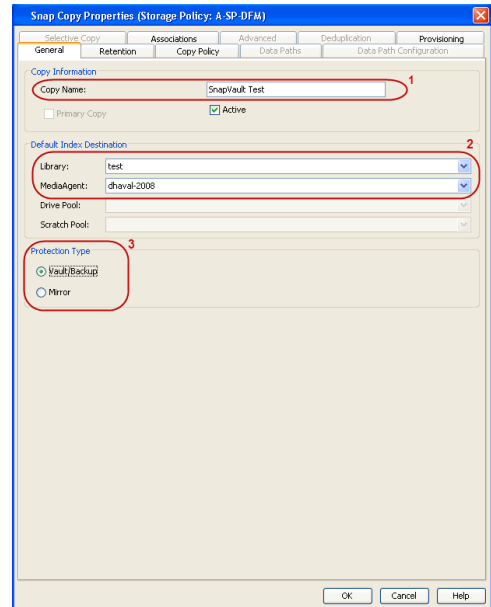
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

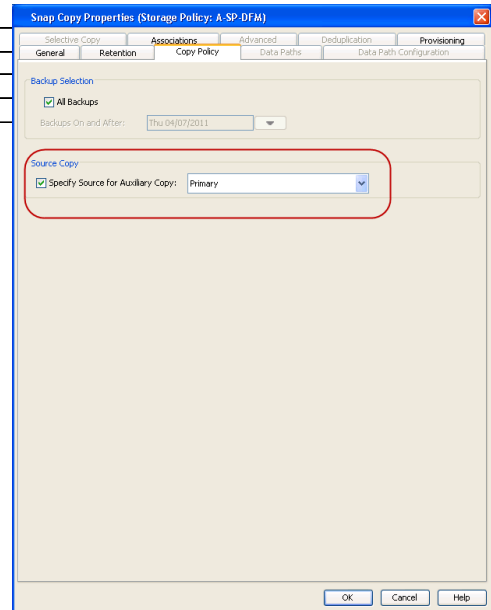


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

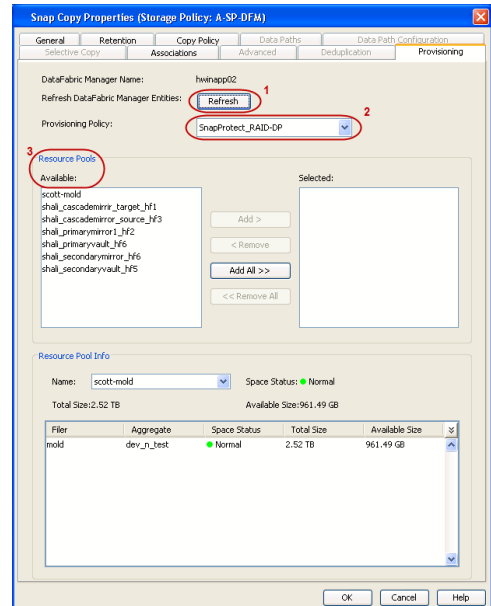
TOPOLOGY	SOURCE COPY
----------	-------------

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.

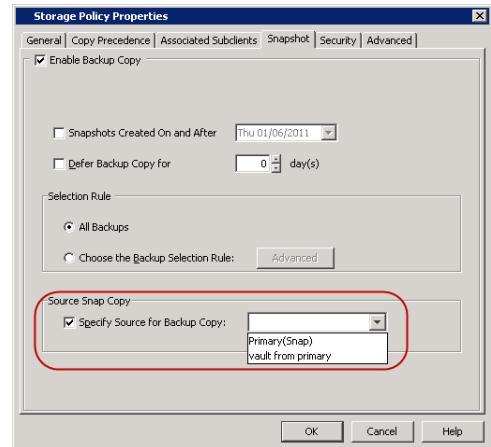
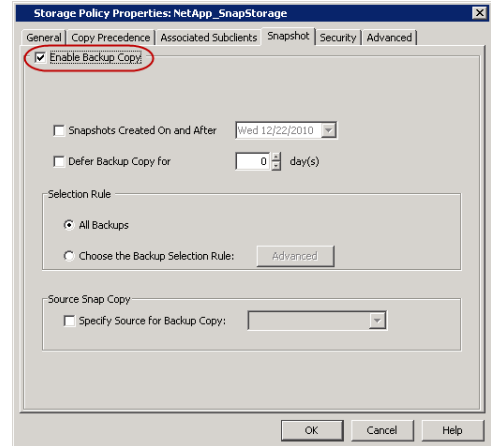
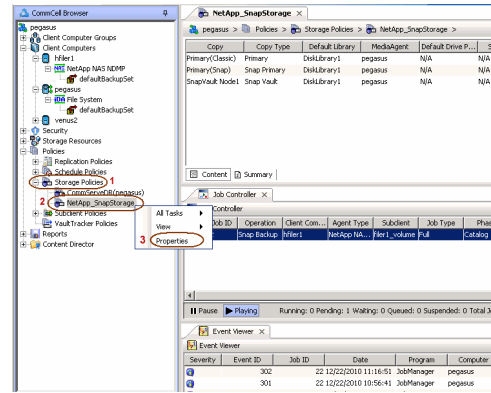
CONFIGURE BACKUP COPY

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.

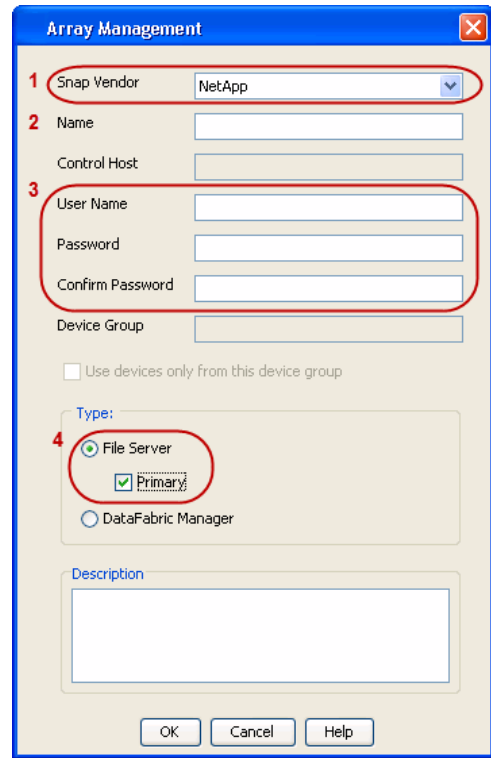
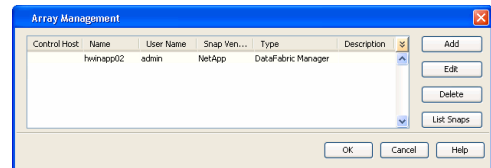
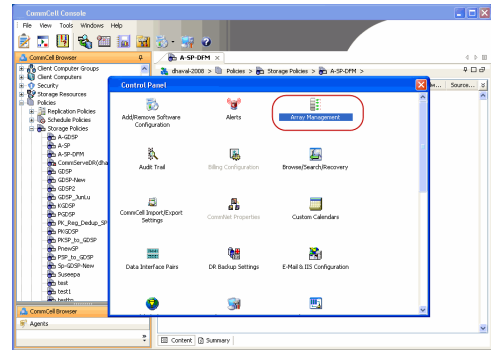
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

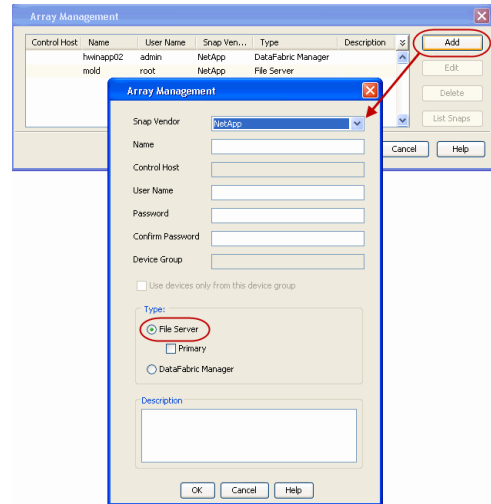
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

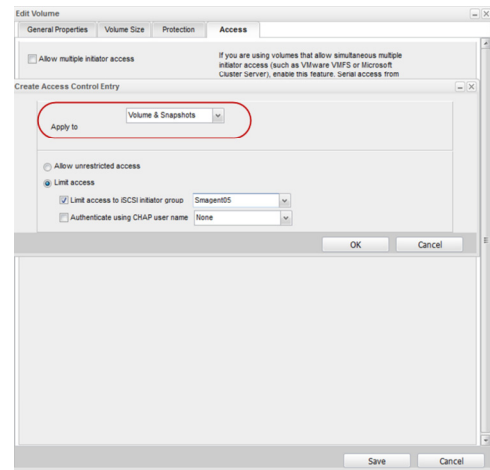
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

SnapProtect™ Backup - Nimble

◀ Previous Next ▶

PREREQUISITES

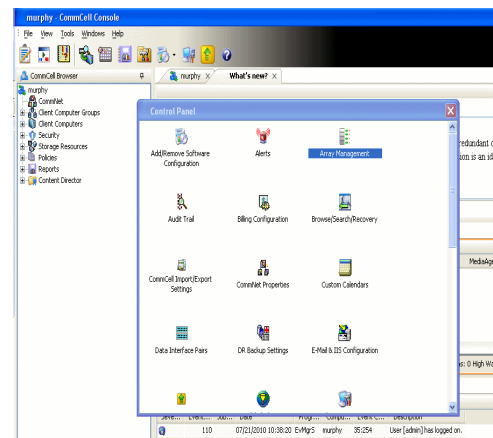
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry**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



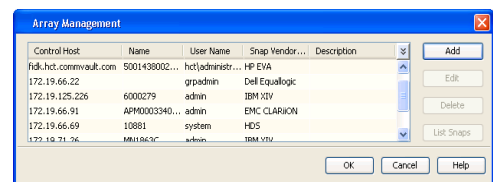
SETUP THE ARRAY INFORMATION

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.

Array Management

Snap Vendor: Nimble

Name: []

Control Host: []

User Name: []

Password: []

Confirm Password: []

Device Group: []

Use devices only from this device group

Type:

- File Server
- Primary
- DataFabric Manager

Description: []

OK Cancel Help

< 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.

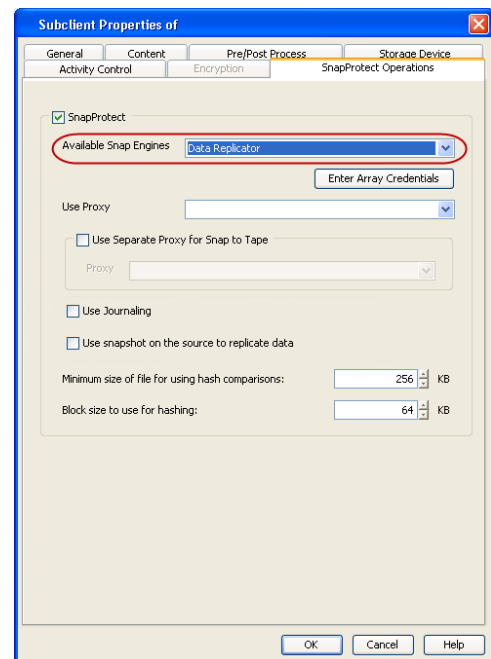
STORAGE POLICY REQUIREMENTS

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

- 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**.

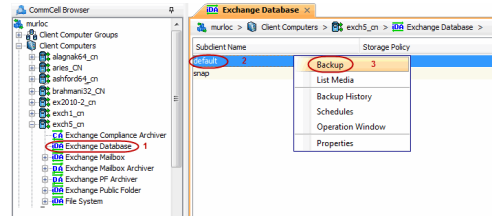


◀ Previous Next ▶

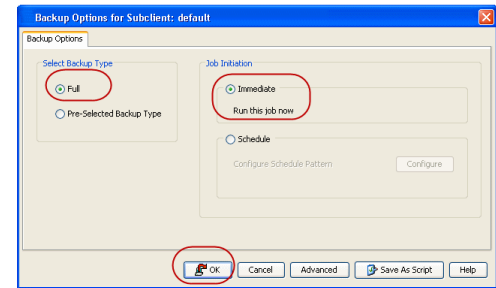
Getting Started - Exchange Database iDataAgent Backup

PERFORM A BACKUP

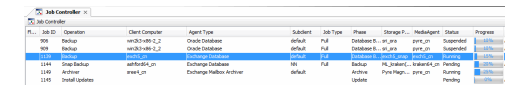
1. Ensure that Circular Logging has been disabled on the Exchange Server.
2.
 - From the CommCell Console, navigate to **Client Computers | <Client> | Exchange Database**.
 - Right-click the **default subclient** and click **Backup**.



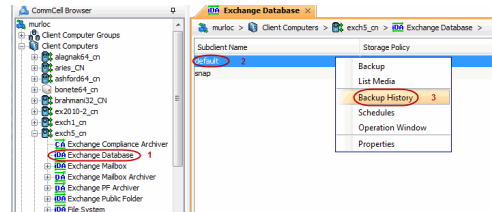
3.
 - Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.



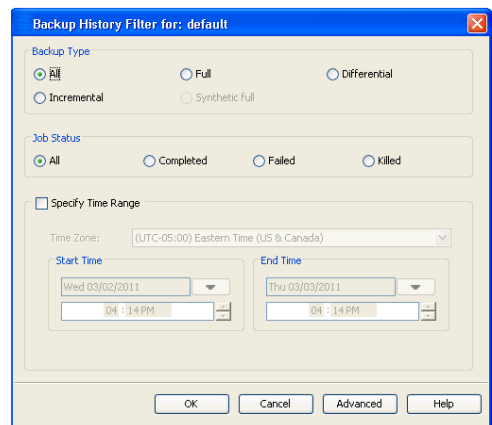
4. You can track the progress of the job from the **Job Controller** window of the CommCell console.



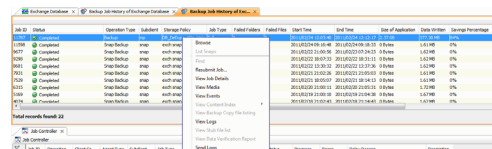
5. Once job is complete, view the details of job from the **Backup History**. Right-click the **Subclient** and select **Backup History**.



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

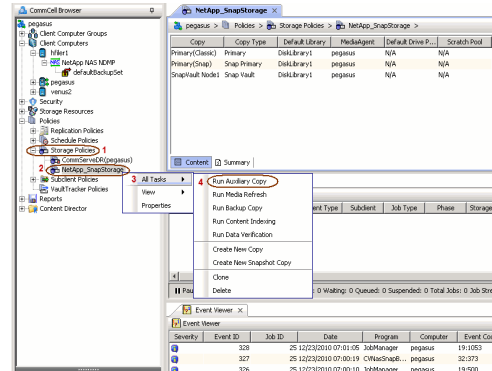
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

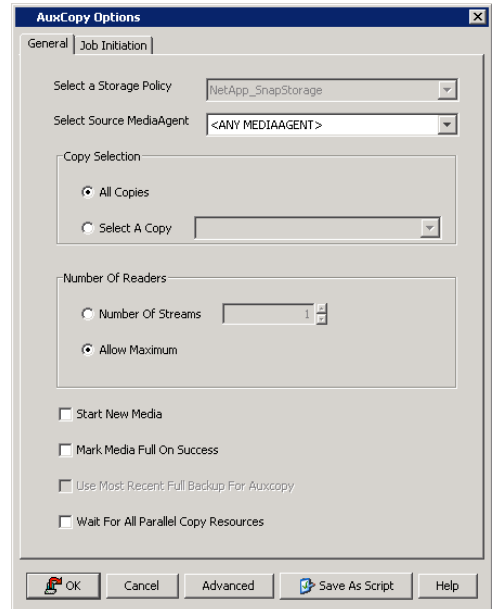
INITIATE VAULT/MIRROR COPY

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**.

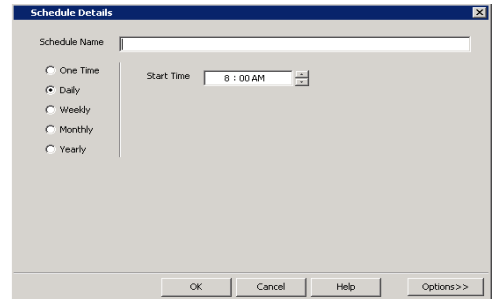


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

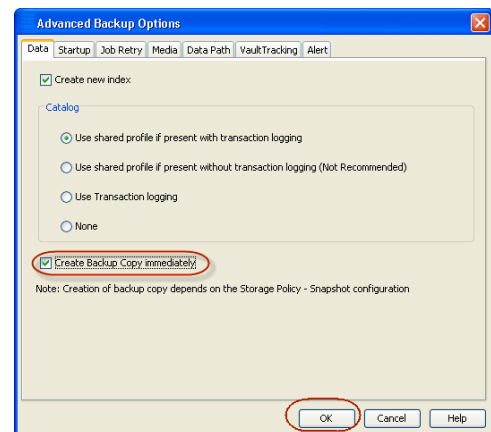
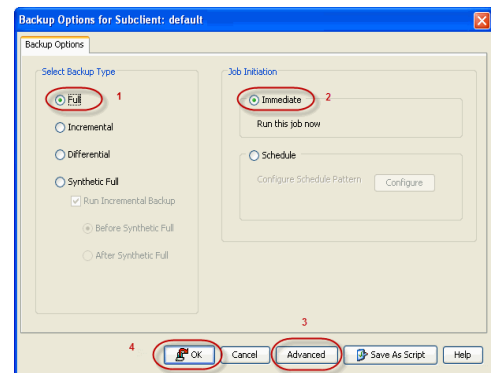
INLINE BACKUP COPY

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.

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**.

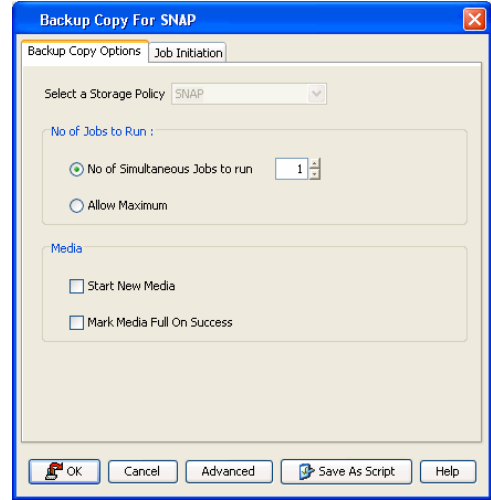
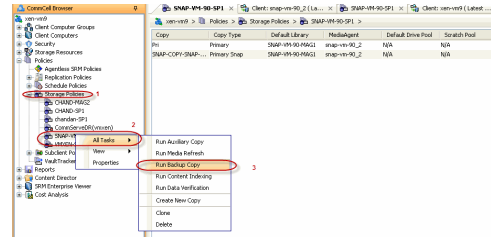


OFFLINE BACKUP COPY

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 Exchange Database Restore

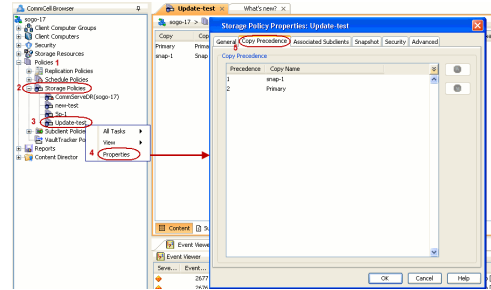


PERFORM A RESTORE

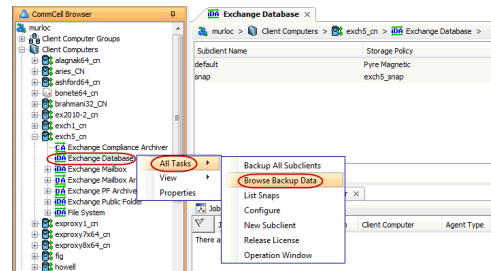
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

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

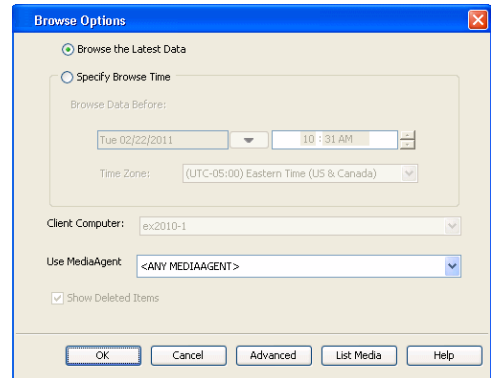
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
 - Click **OK**.



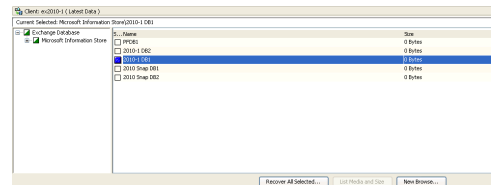
- From the CommCell Console, navigate to **Client Computers | <Client> | Exchange Database**.
 - Right-click the Agent and then click **All Tasks | Browse Backup Data**.



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

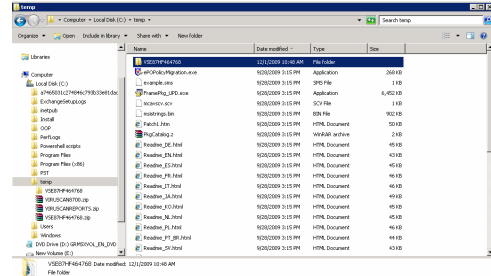
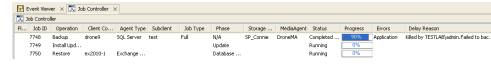
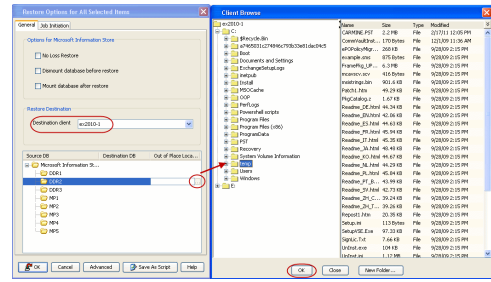


- Select the Microsoft Information Store in the left pane. Select a database in the right pane.
 - Click **Recover All Selected**.



- 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.

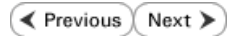
Now you have a choice of either adding another package to the existing installation or configure Calypso on a virtual machine for use in a cluster.

- 1) Add another package to stone.company.com
- 2) Install Calypso on a virtual machine
- 3) Exit

Your choice: [1] 3



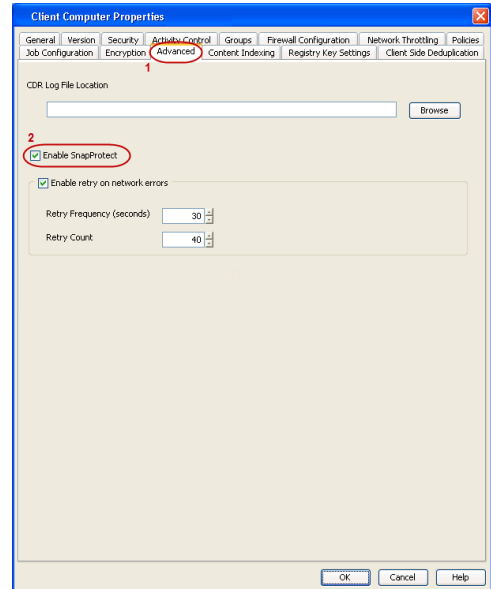
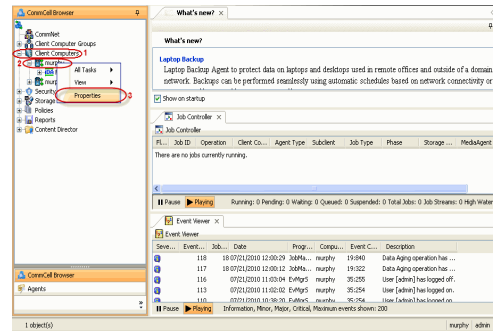
Getting Started - Oracle Configuration



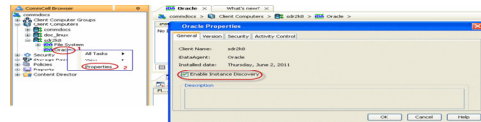
CONFIGURATION

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**.



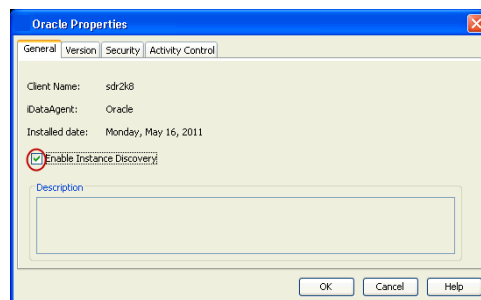
- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click **Oracle** and then click **Properties**.



- Select the **Enable Instance Discovery** checkbox.
 - Click **OK**.

If the instances are discovered automatically, go to step 7.

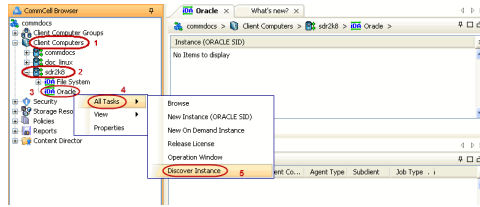
If the instances are not discovered automatically, follow the step given below to manually discover the instances.



- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click **Oracle**, point to **All Tasks** and then click **Discover Instance**.

6. Click **Yes**.

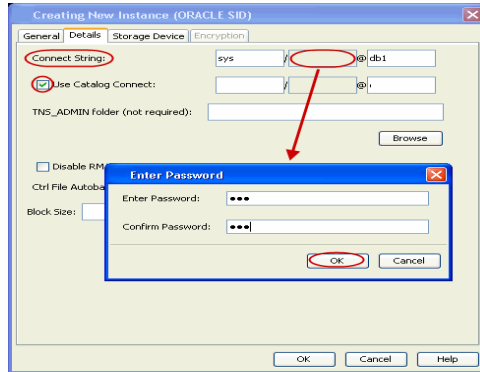
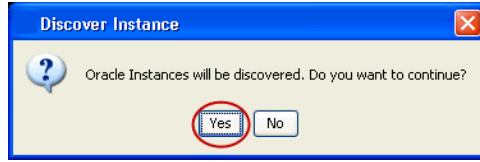
If your Oracle database uses an ASM instance and the instance is in a different Oracle Home, you may have to manually add the instance as the discovery operation may not find it. When configuring the instance, verify the database status shows as STARTED.



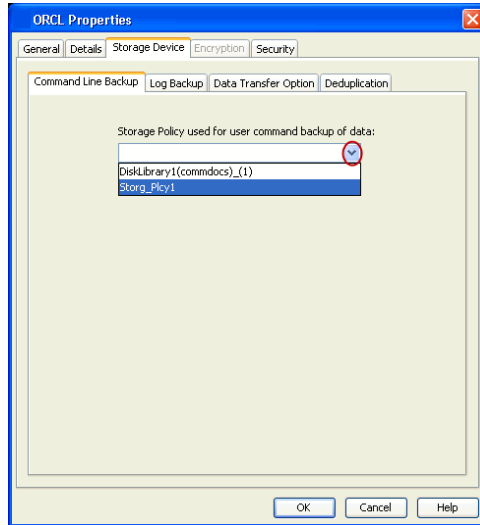
- 7.
- From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
 - Right-click the **<Instance>** and then click **Properties**.

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**.

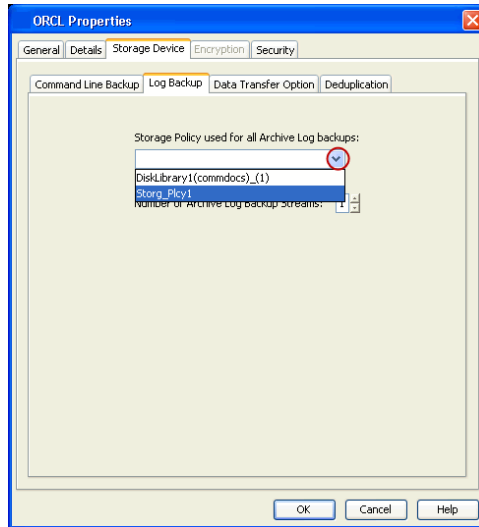


- 9.
- Click the **Storage Device** tab.
 - In the **Storage Policy used for user command backup of data** box, select a storage policy name.

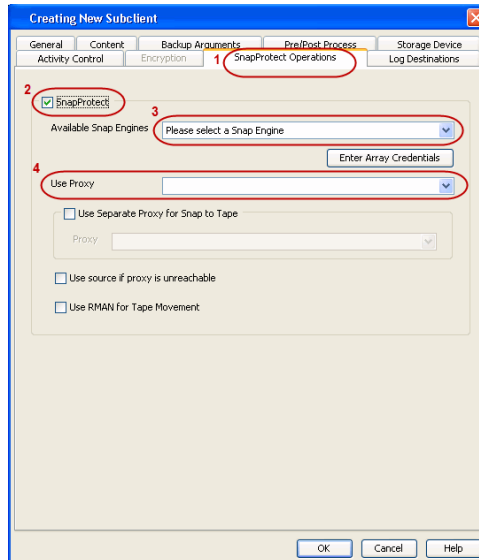
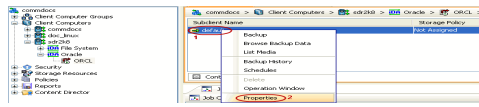


- 10.
- Click the **Logs Backup** tab.
 - In the **Storage Policy used for all Archive Log backups** box, select a storage policy name.
 - Click **OK**.

11.
 - From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle | <Instance>**.
 - Right-click the default subclient and then click **Properties**.

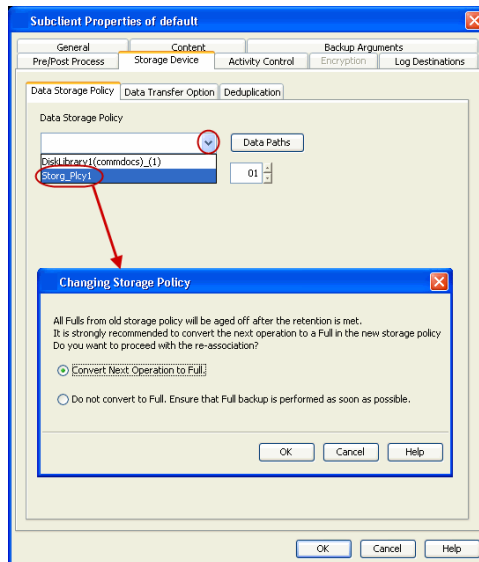


12.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where backup copy operations will 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.



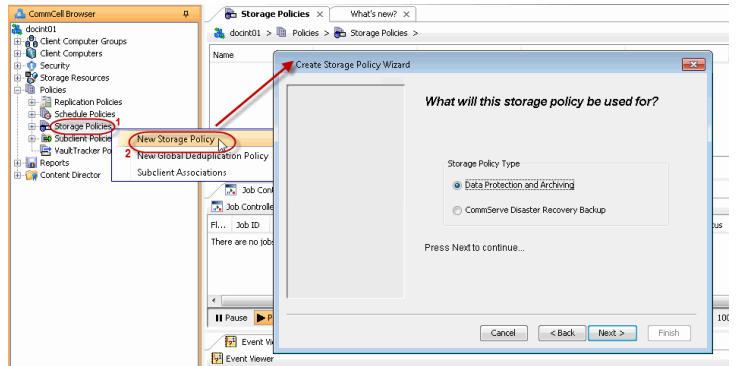
13.
 - Click the **Storage Device** tab.
 - In the **Data Storage Policy** list, select a Storage Policy name.
 - Click **OK** to convert the next backup as a full backup.
 - Click **OK**.

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.

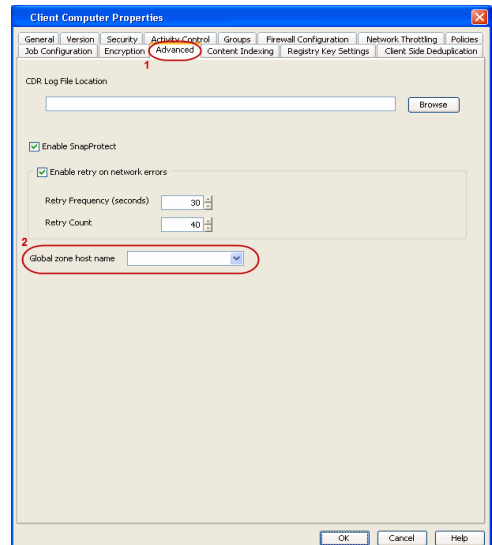
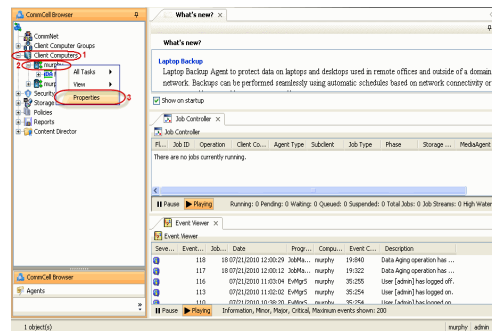
Click **Next** to Continue.

ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE

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**.
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.

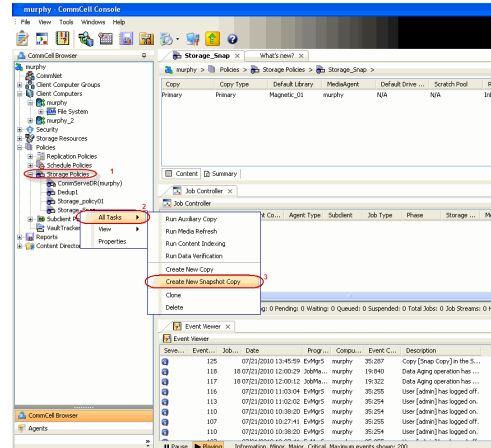
Click **Next** ➤ to Continue.

Next ➤

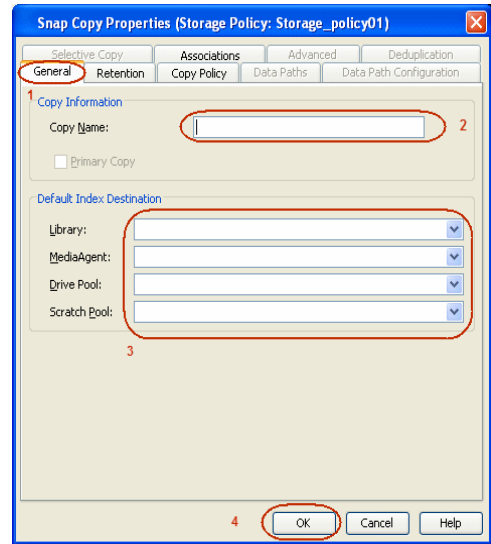
CREATE A SNAPSHOT COPY

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**.

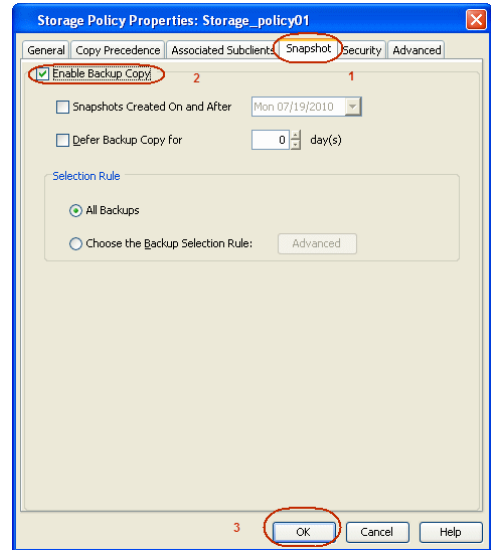
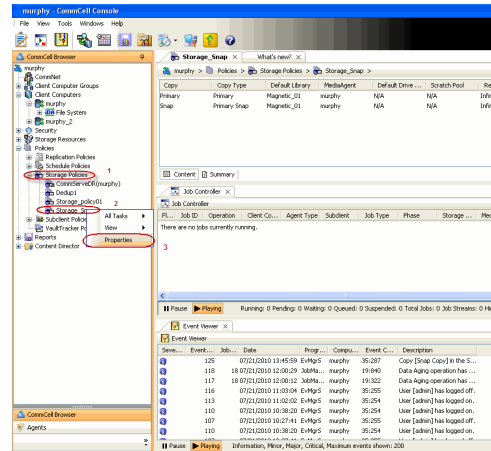


CONFIGURE BACKUP COPY

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

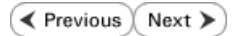
◀ Previous Next ▶

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



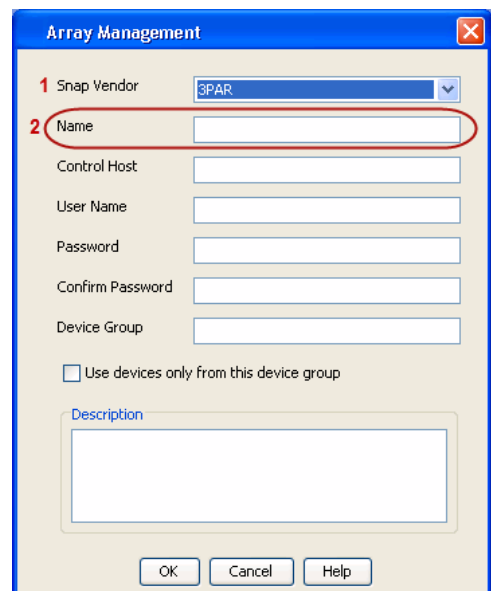
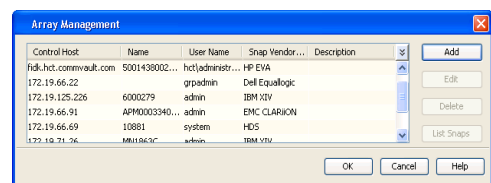
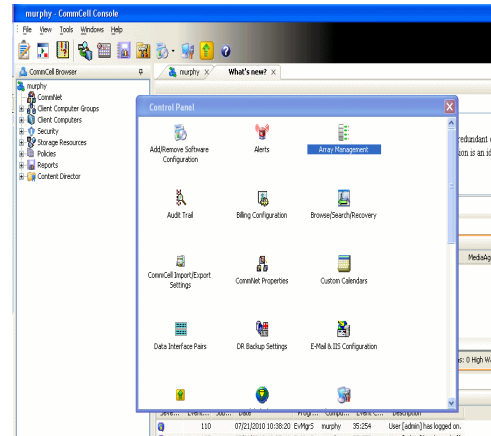
PRE-REQUISITES

- 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

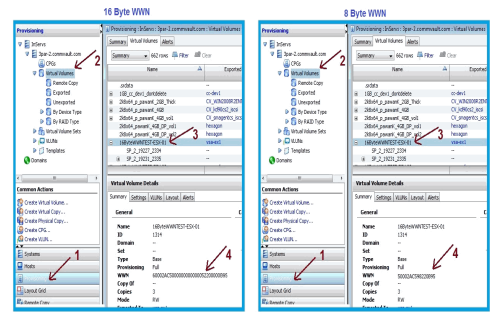
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

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

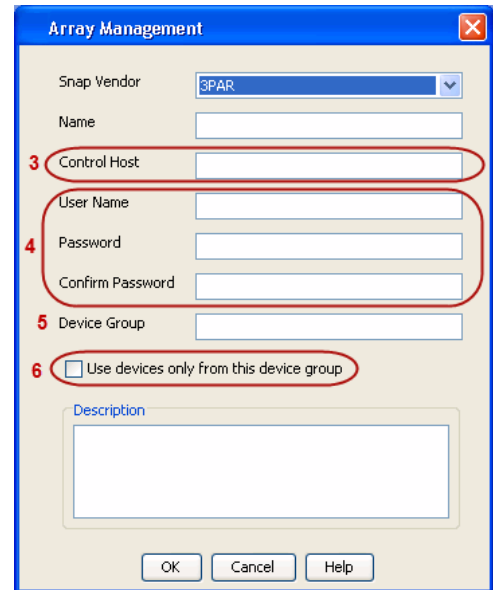
After adding all the values, the resulting array name is 2FF70002AC000B95.



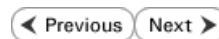
- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be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

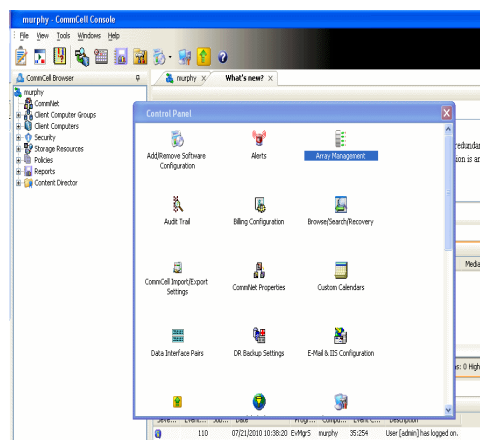
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing 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.

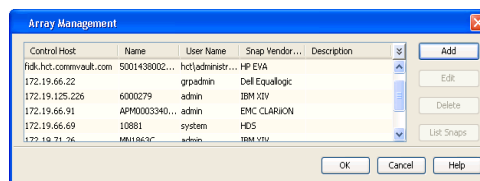
SETUP THE ARRAY INFORMATION

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**.



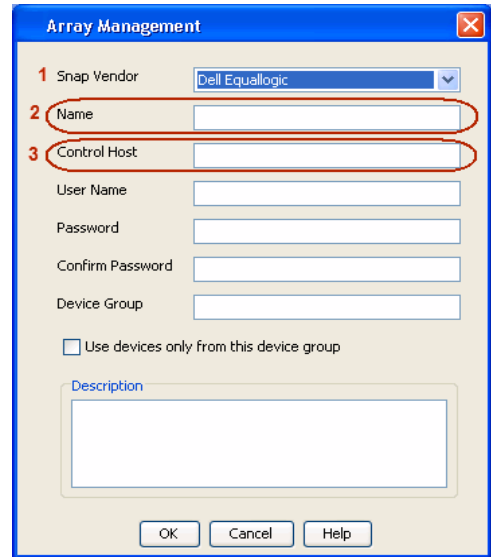
2. Click **Add**.



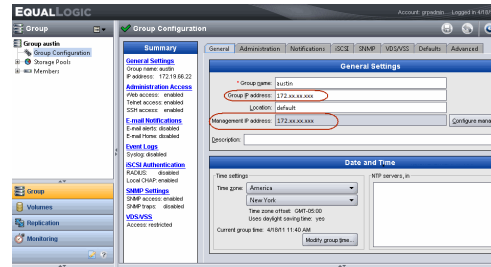
3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

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

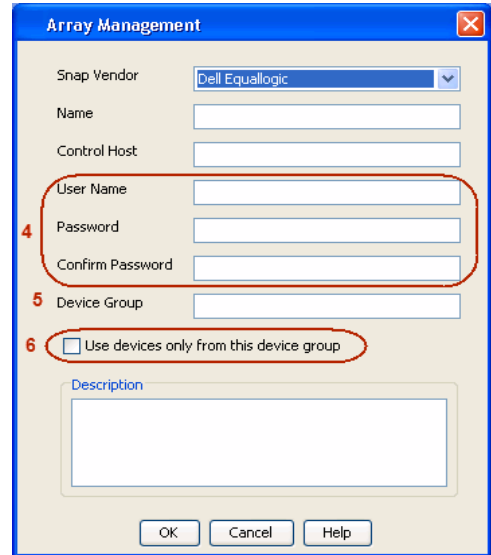
- Specify the Group IP address in the **Control Host** field.



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.

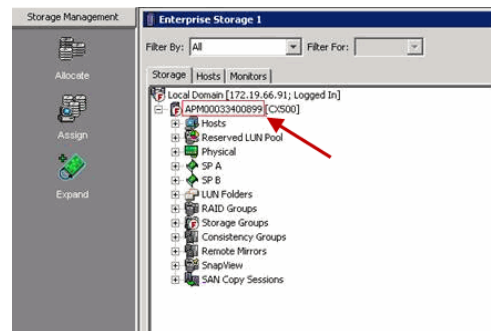
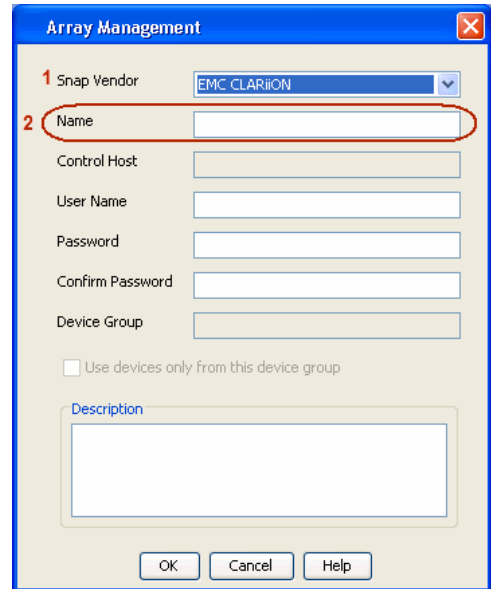
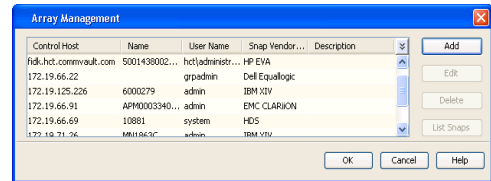
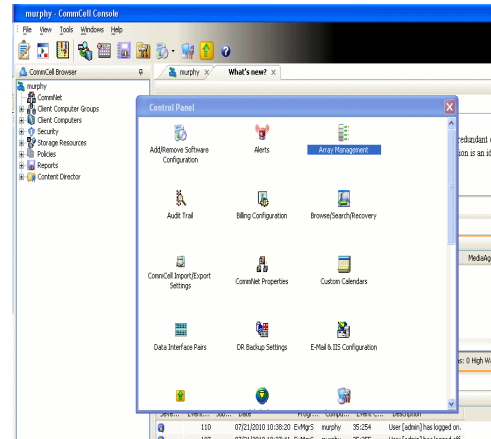
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

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

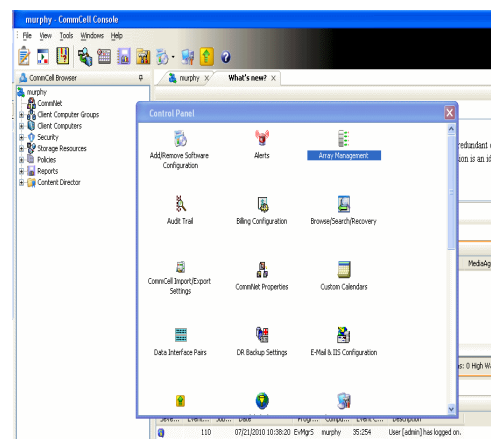
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

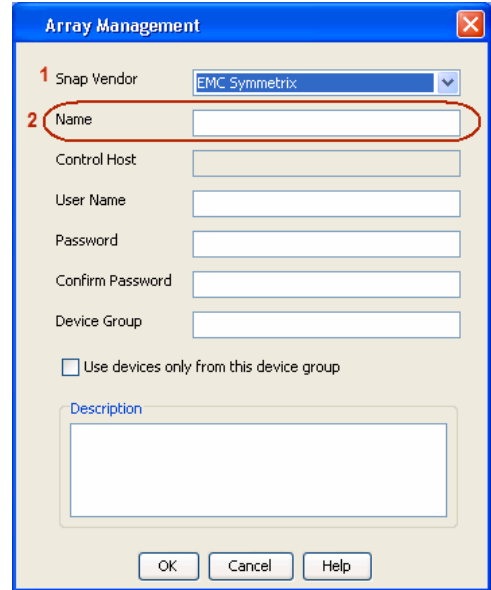
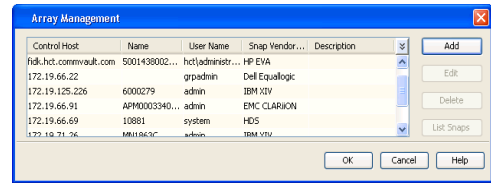
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

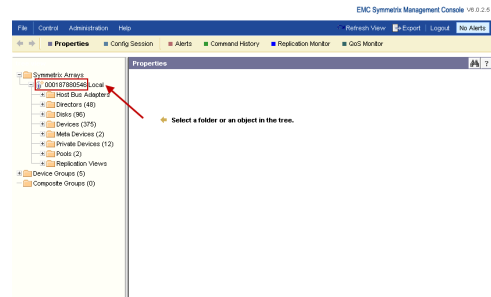


2. Click **Add**.

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

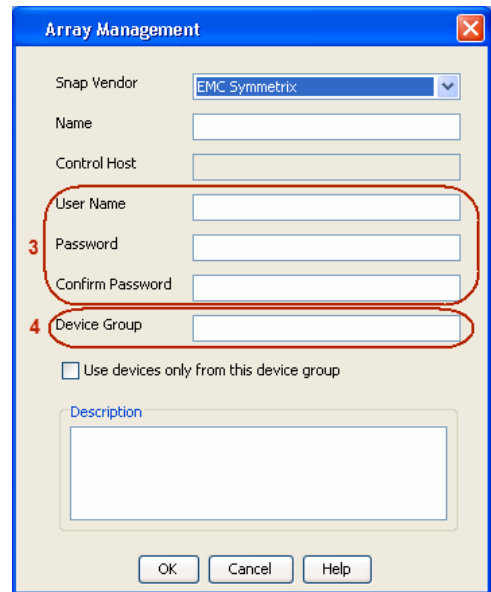


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.

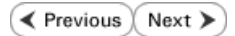


4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. 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

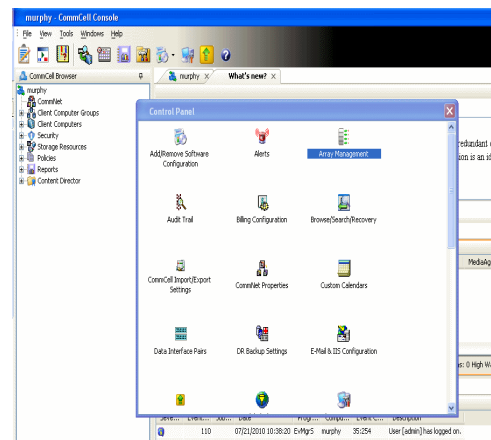
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

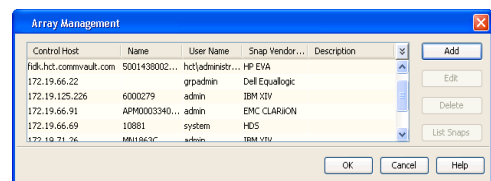
SETUP THE ARRAY INFORMATION

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

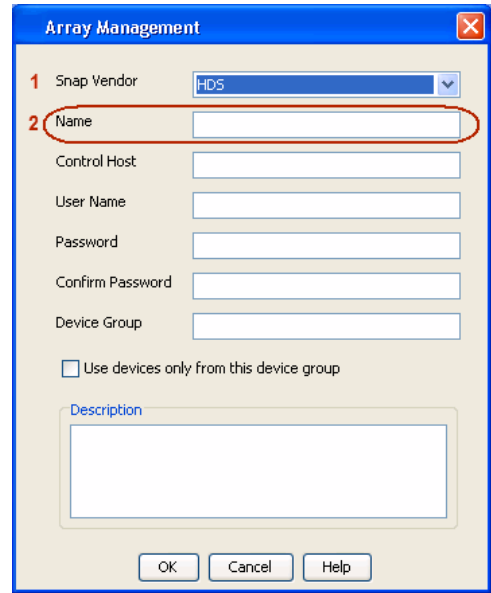
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



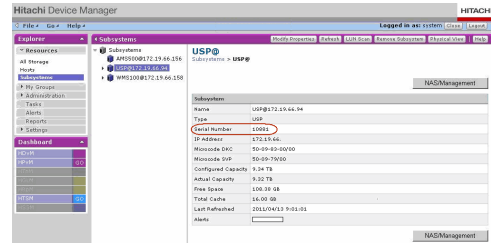
2. Click **Add**.



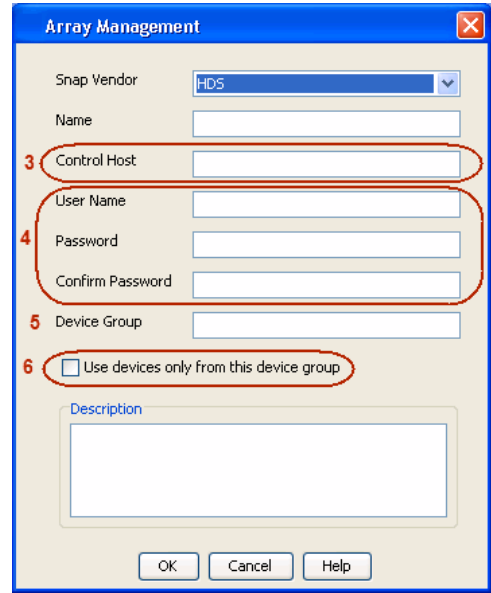
3.
 - Select **HDS** from the **Snap Vendor** list.
 - Specify the serial number of the array in the **Name** field.



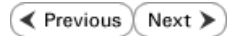
For reference purposes, the screenshot on the right shows the serial number for the HDS storage device.



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.

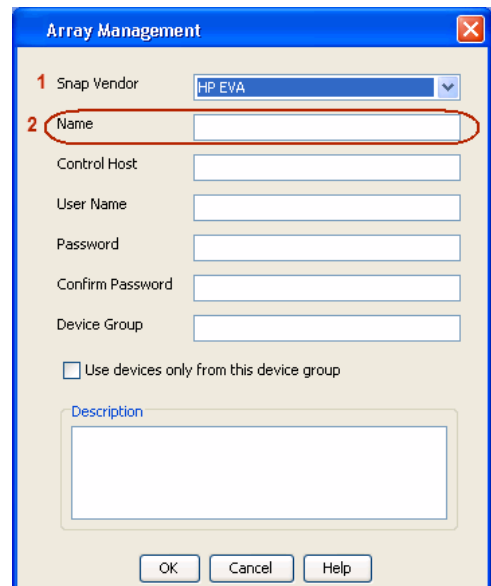
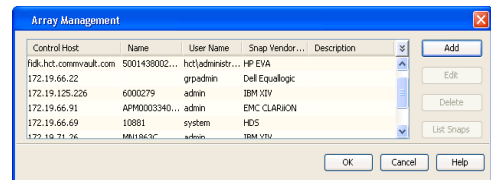
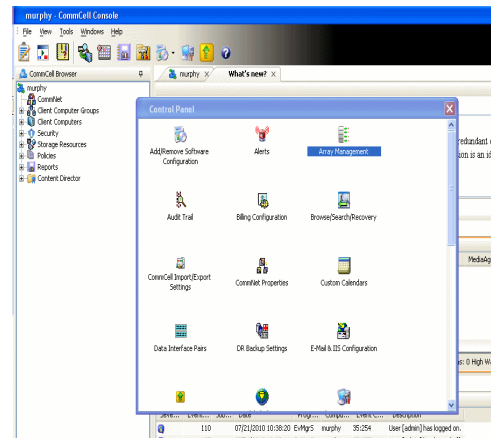
The following steps provide the necessary instructions to setup the HP EVA:

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

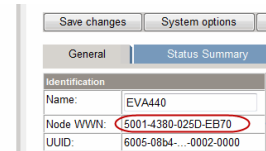
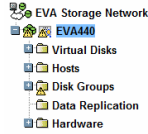
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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 ▶

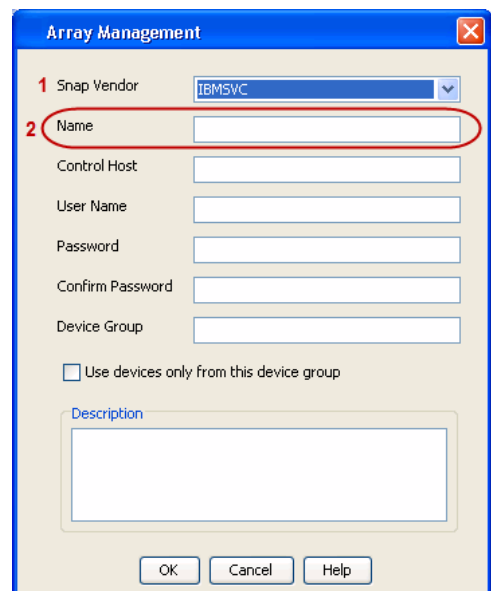
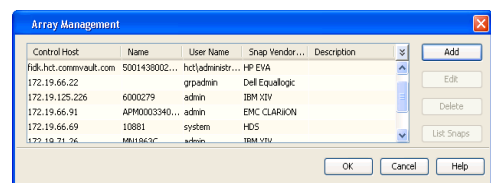
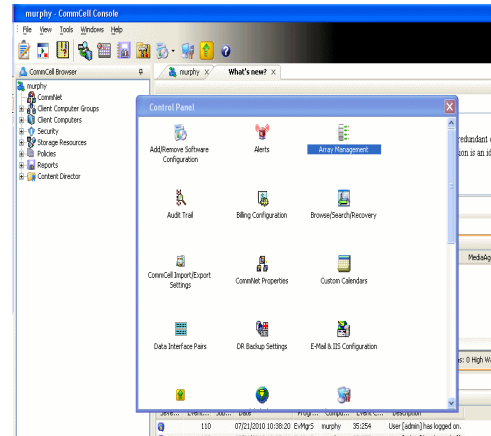
PRE-REQUISITES

- 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.

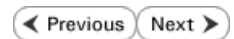
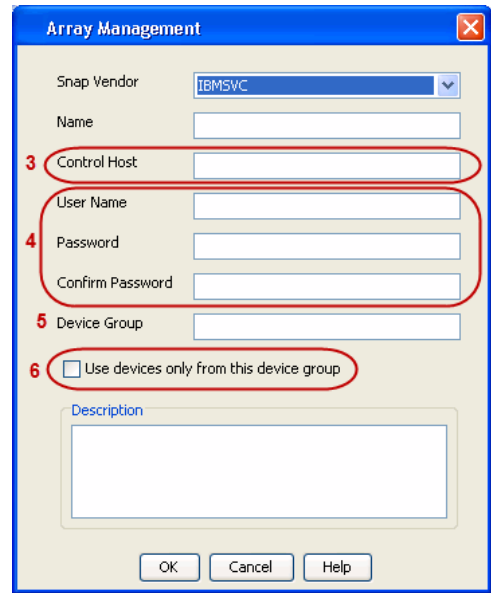
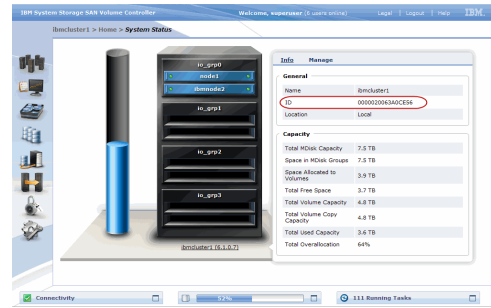
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



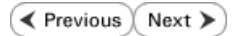
The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

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



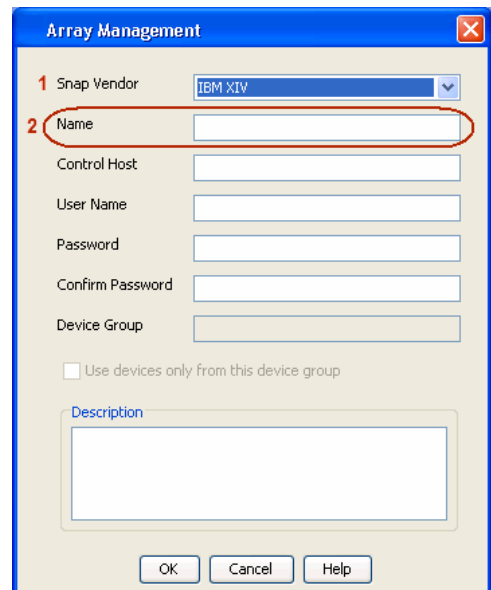
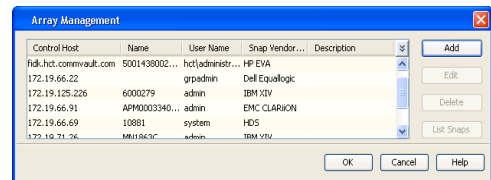
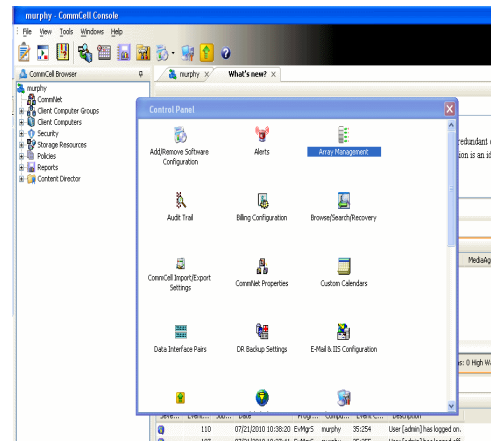
PRE-REQUISITES

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.

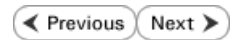
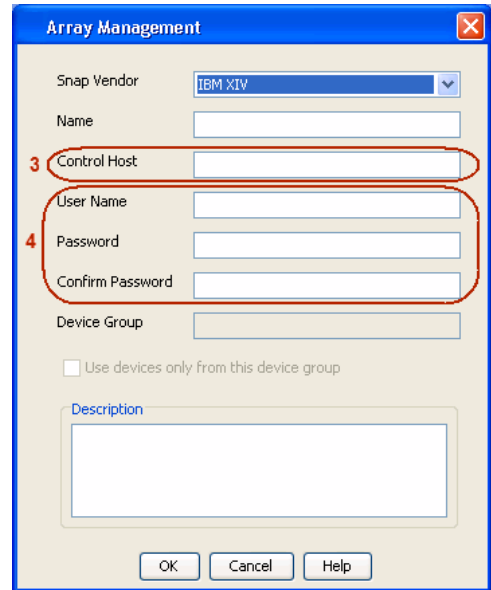
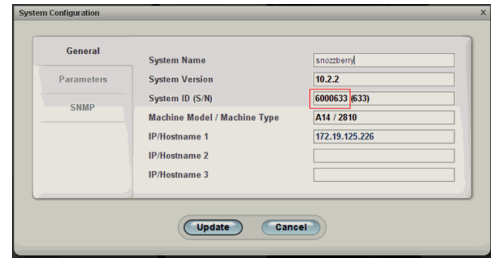
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
2. Click **Add**.
3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



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.

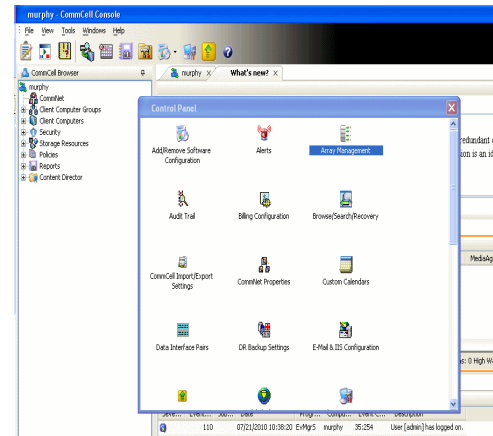
ADDITIONAL REQUIREMENTS FOR VMWARE

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.

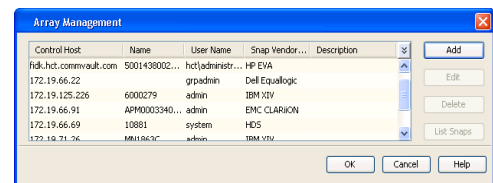
SETUP THE ARRAY INFORMATION

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

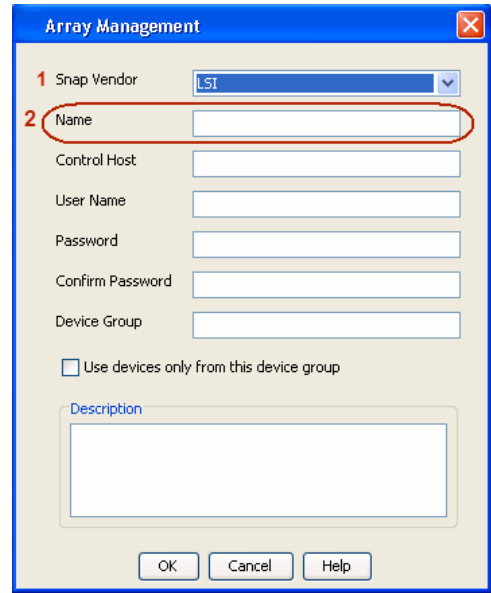
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

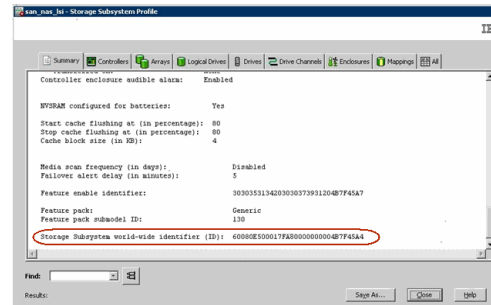


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



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

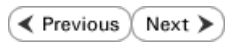
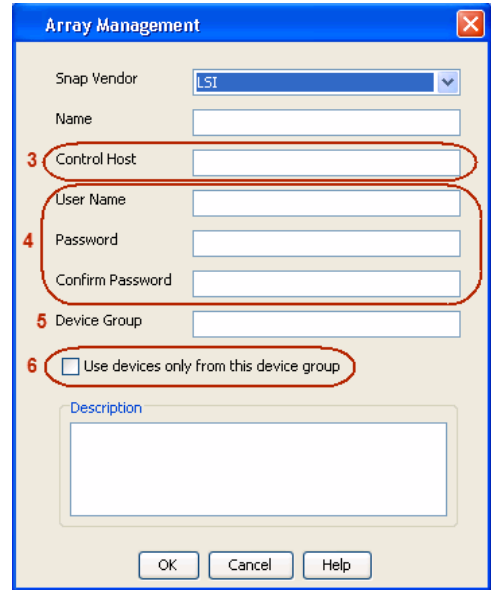
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



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.



SnapProtect™ Backup - NetApp

PREREQUISITES

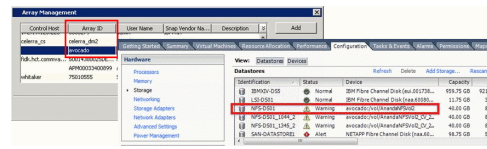
LICENSES

- 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.

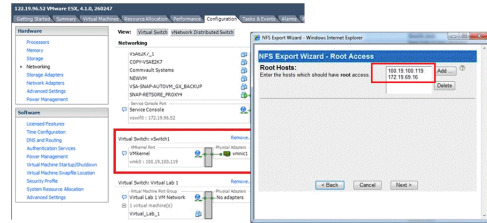
ADDITIONAL REQUIREMENTS FOR VMWARE

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.



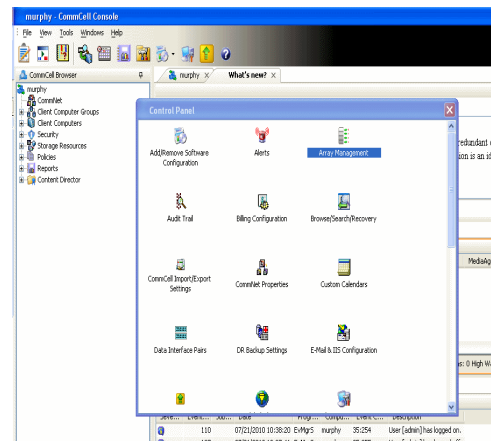
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



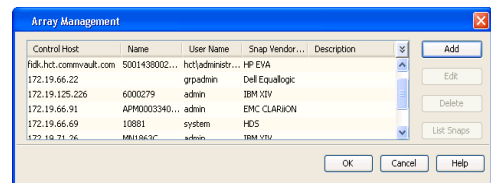
SETUP THE ARRAY INFORMATION

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

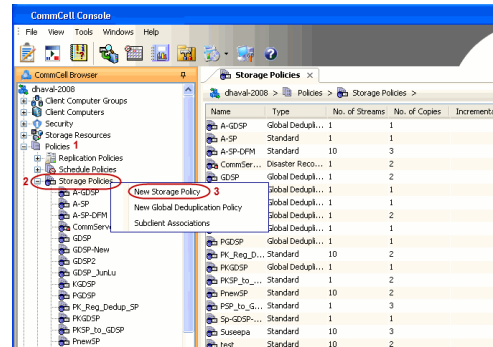
CONFIGURATION

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

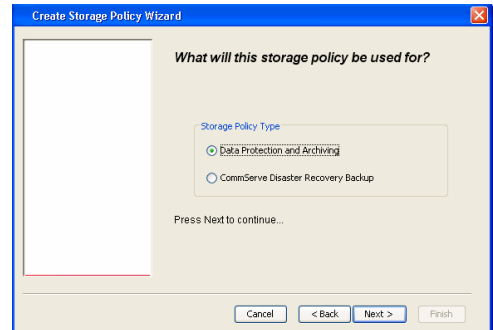
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

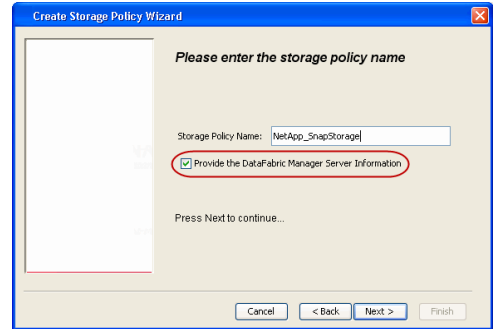
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



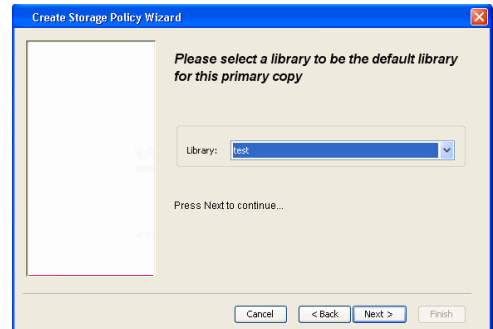
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



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

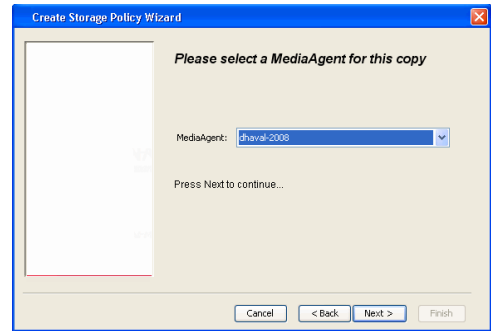
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

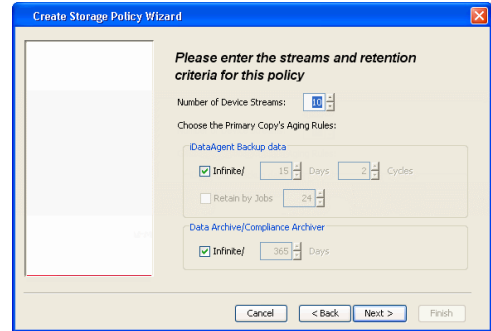


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

6. Click **Next**.

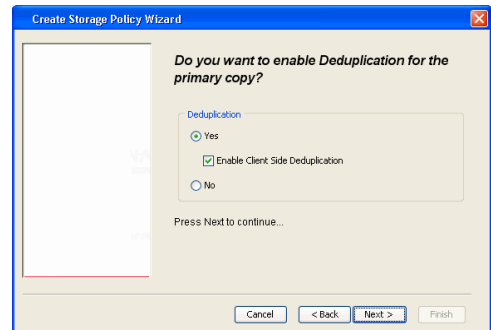


7. Click **Next**.



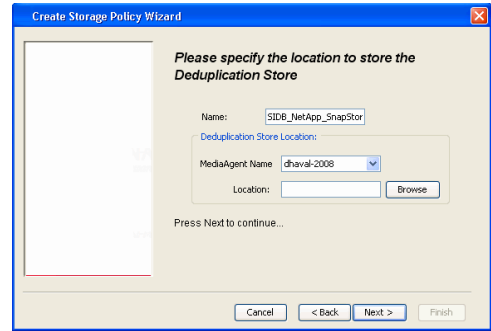
8.

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

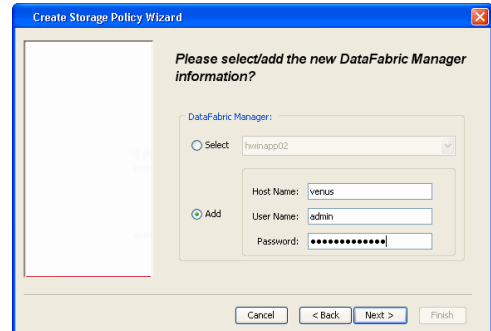


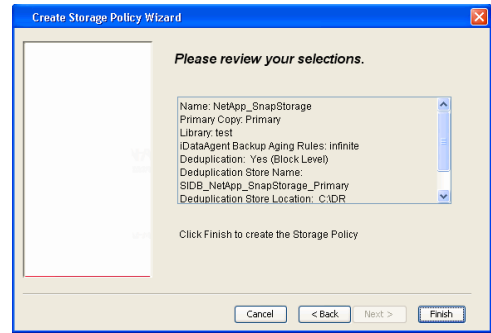
9.

- 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**.



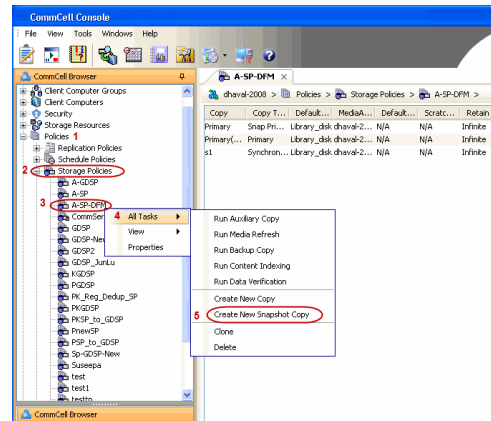


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

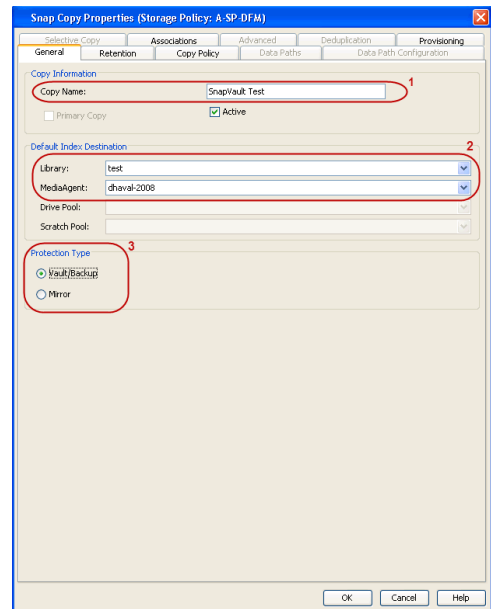
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

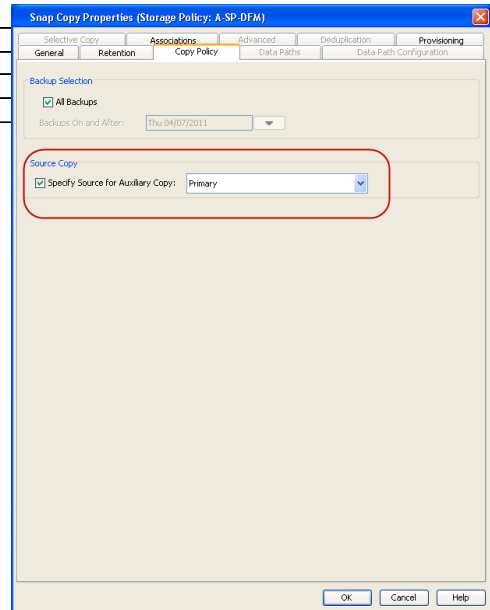


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

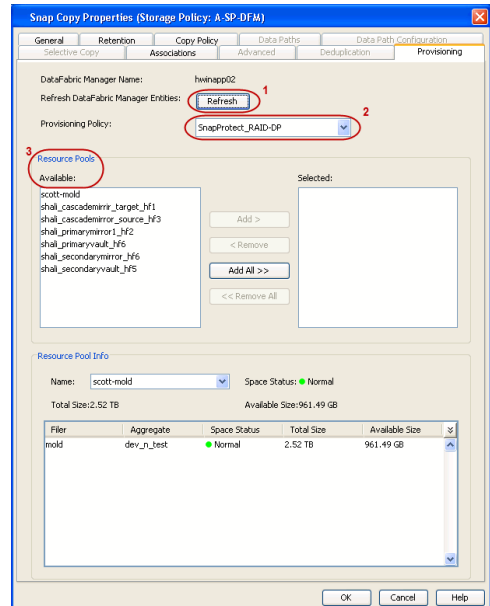
TOPOLOGY	SOURCE COPY
----------	-------------

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.

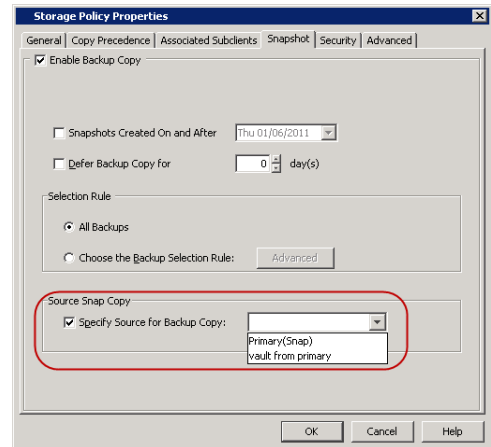
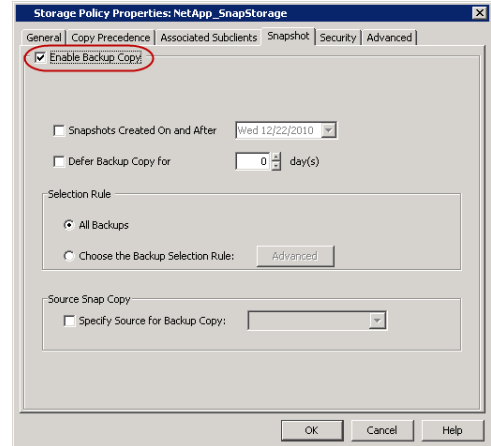
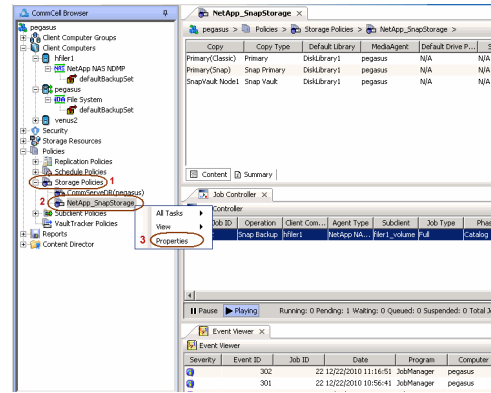
CONFIGURE BACKUP COPY

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.

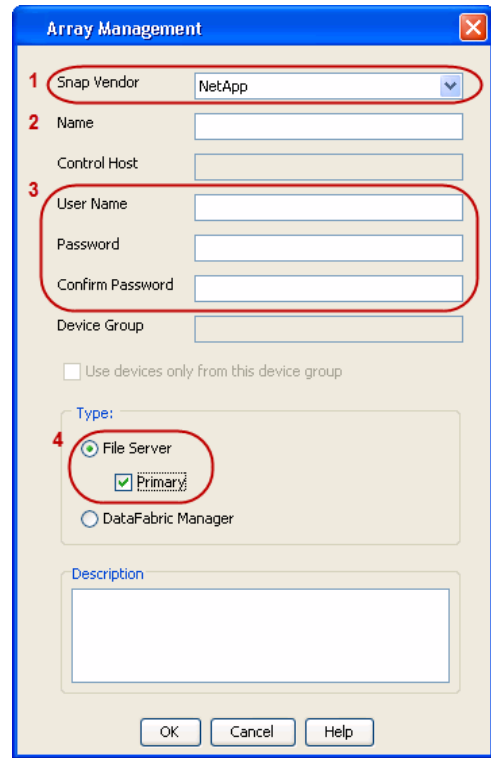
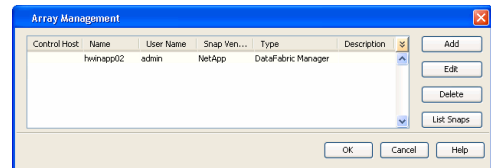
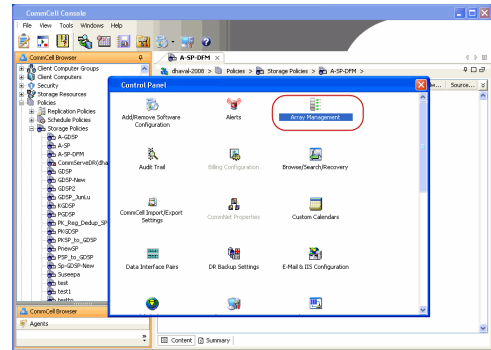
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

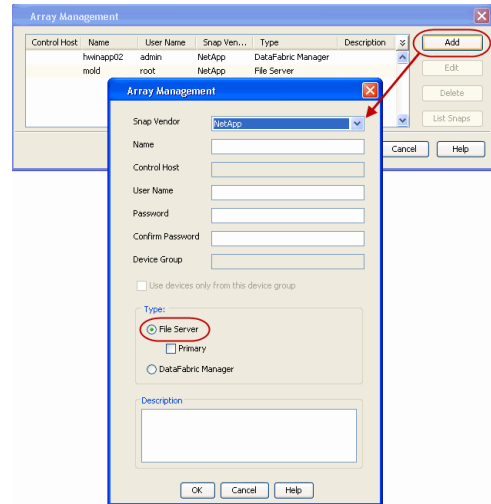
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

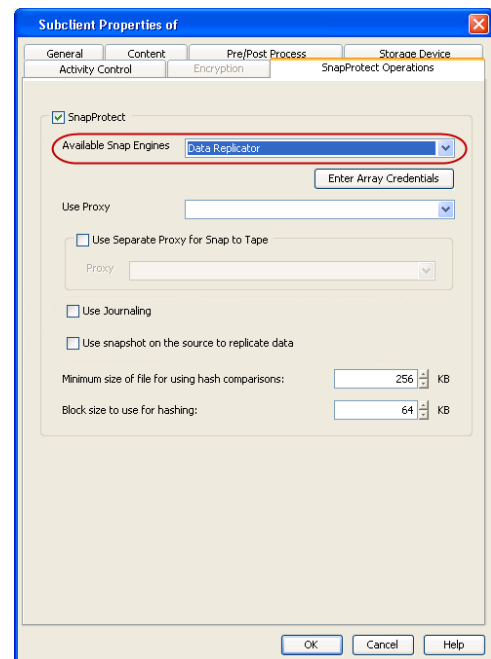
STORAGE POLICY REQUIREMENTS

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

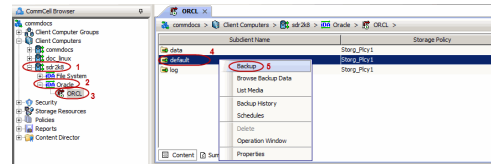
- From the CommCell Console, navigate to <Client> | <Agent>.
 - Right-click the subclient and click **Properties**.
- Click the **SnapProtect Operations** tab.
 - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down list.
 - Click **OK**.



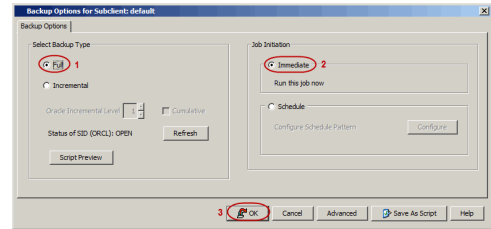
◀ Previous Next ▶

Getting Started Backup - Oracle iDataAgent

- From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **Oracle** | **<Instance>**.
 - Right-click the default subclient and click **Backup**.



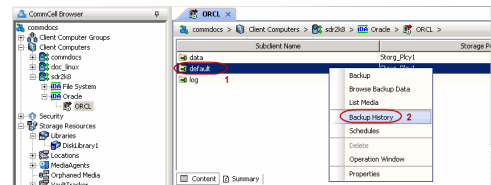
- Click **Full** as backup type and then click **Immediate**.
 - Click **OK**.



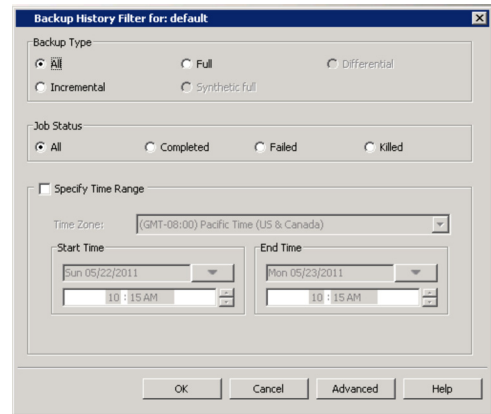
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



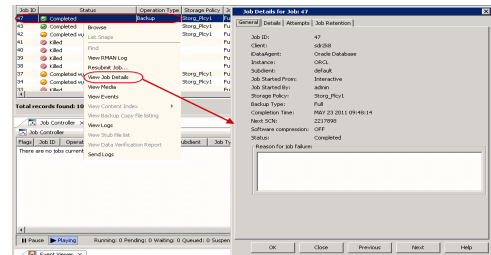
- Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.



- 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

◀ Previous Next ▶

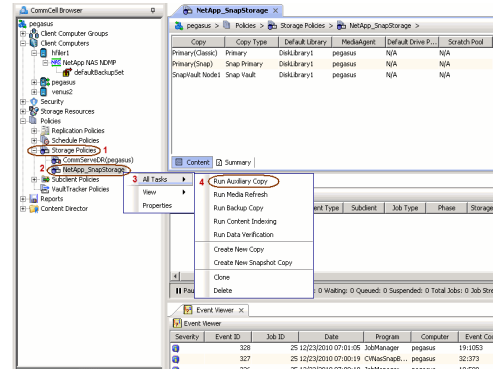
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

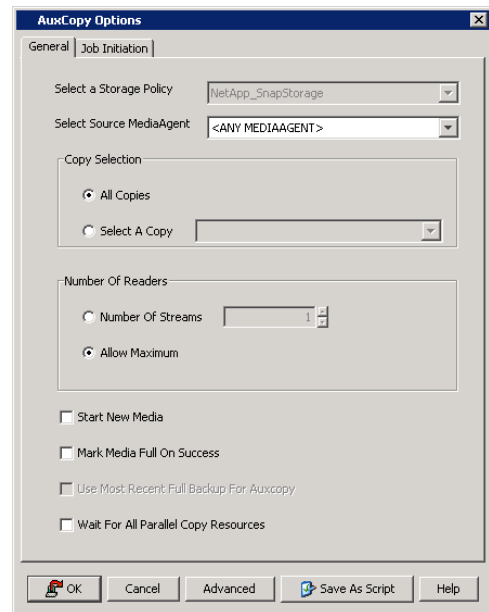
INITIATE VAULT/MIRROR COPY

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**.

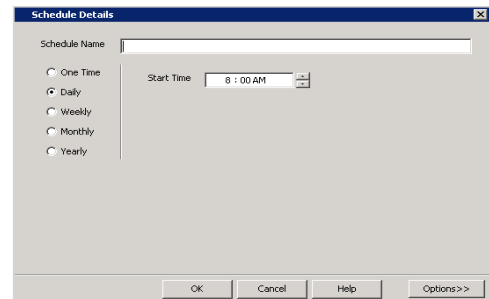


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

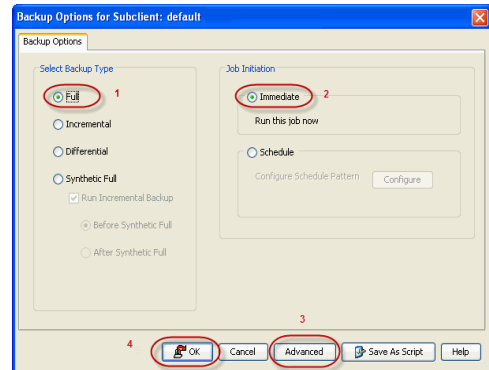
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

INLINE BACKUP COPY

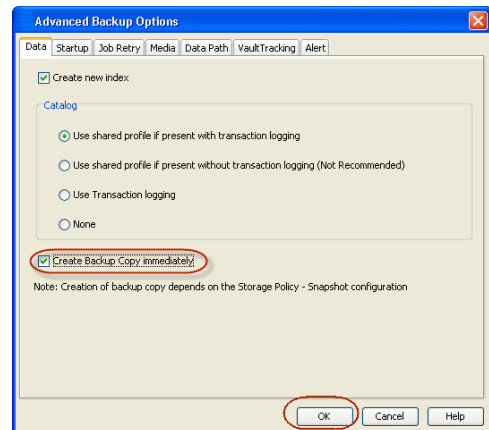
Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect 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**.

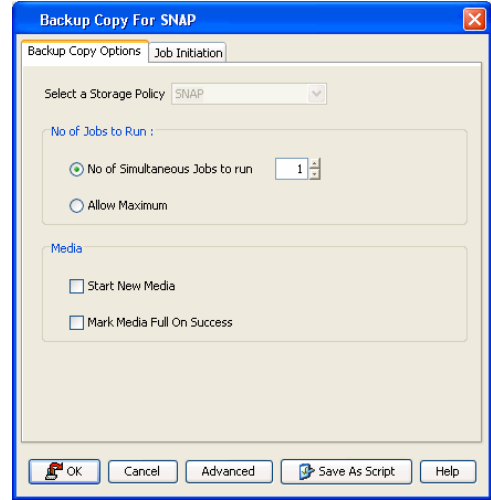
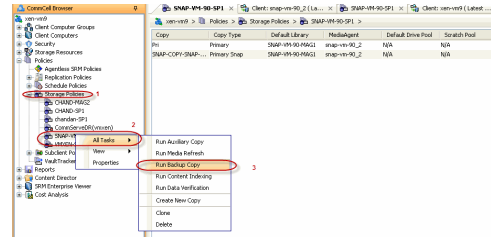


OFFLINE BACKUP COPY

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 - Oracle Restore

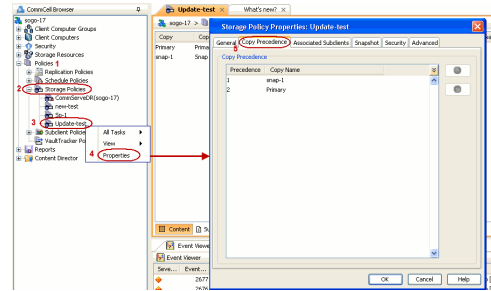


PERFORM A RESTORE

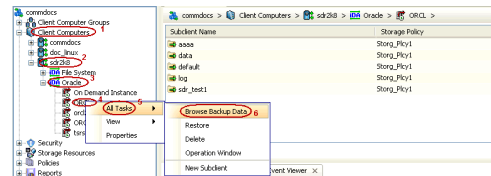
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring a database.

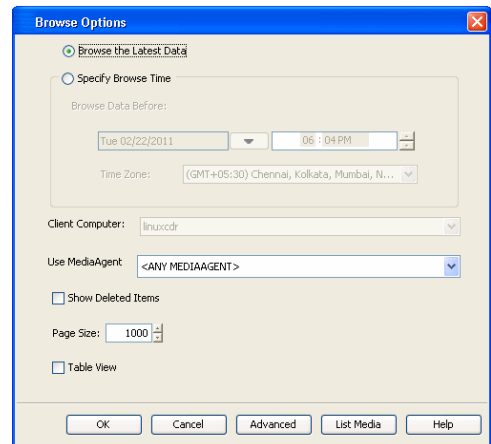
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
 - Click **OK**.



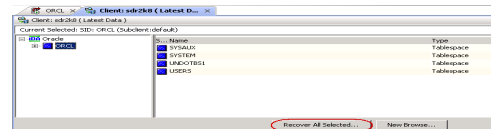
- From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
 - Right-click the **<Instance>**, point to **All Tasks**, and then click **Browse Backup Data**.



- Click **OK**.



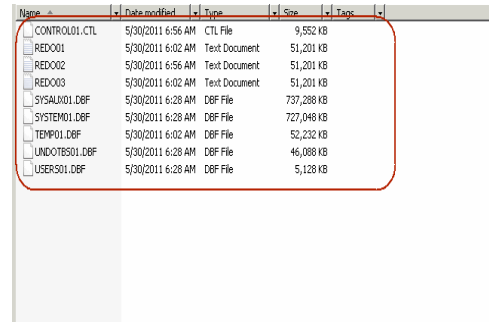
- In the right pane of the Browse window, click the **<Instance>** and select all the entities.
 - Click **Recover All Selected**.



- 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.

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.

INSTALL THE MICROSOFT SQL SERVER *i*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 *i*DataAgent**.

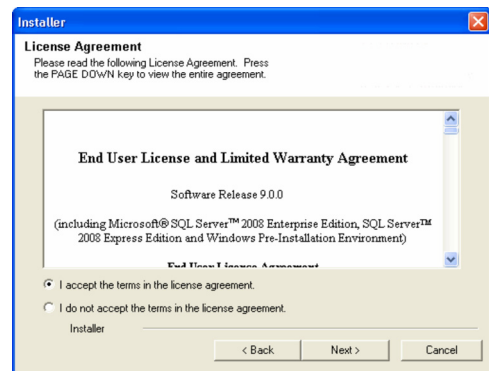
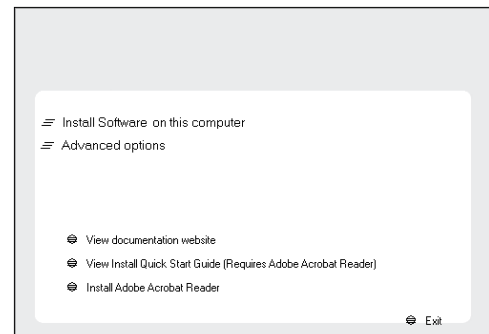
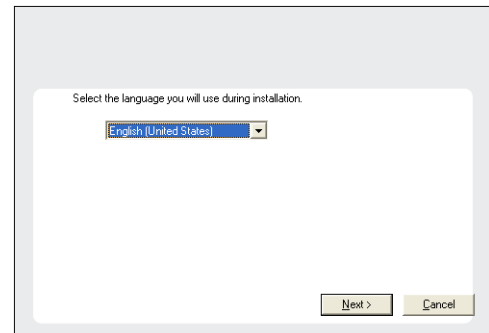
BEFORE YOU BEGIN

Download Software Packages

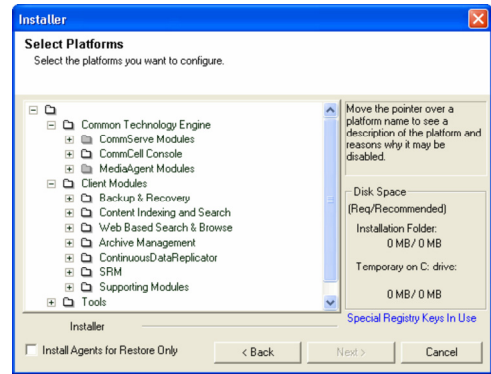
Download the latest software package to perform the install.

SnapProtect Support - Platforms

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



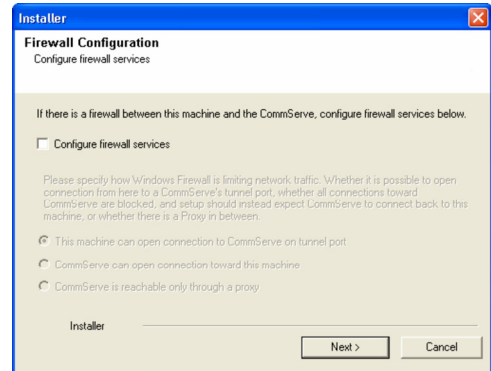
- Expand **Common Technology Engine | MediaAgent Modules**, and select **MediaAgent**.
- Expand **Client Modules | ContinuousDataReplicator**, and select **VSS Provider**.
- Click **Next**.



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**.

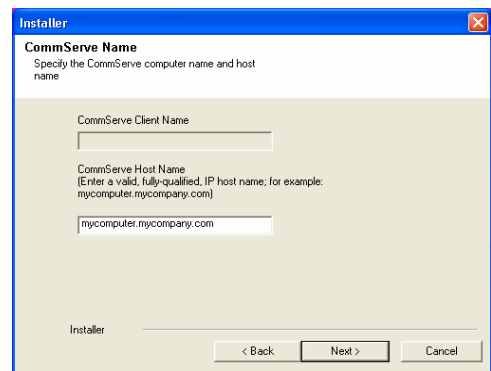


8. Enter the fully qualified domain name of the **CommServe Host Name**.

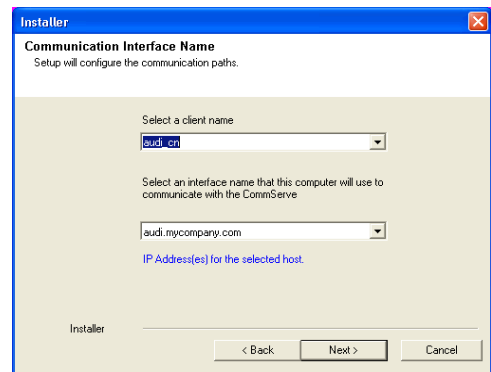
Click **Next**.

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.

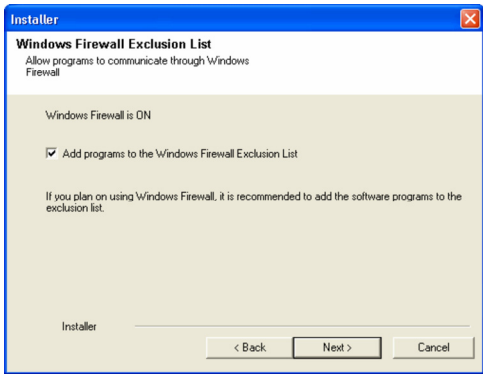
Click **Next**.

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.

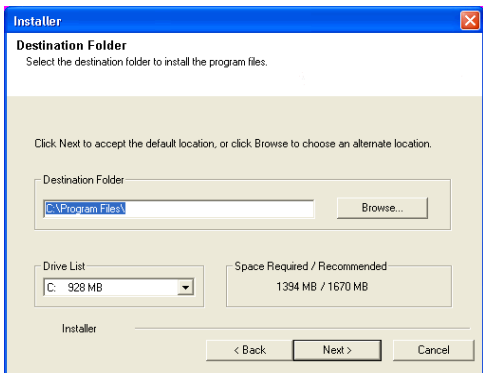
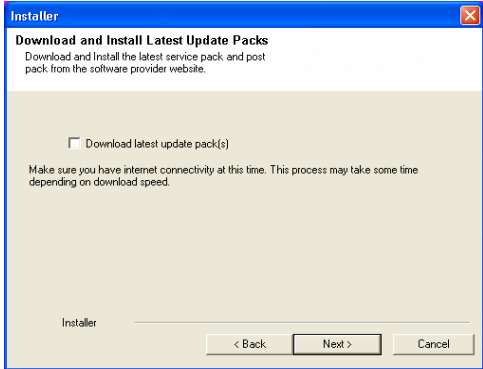
Click **Browse** to change the default location.

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:

/ : * ? " < > | #

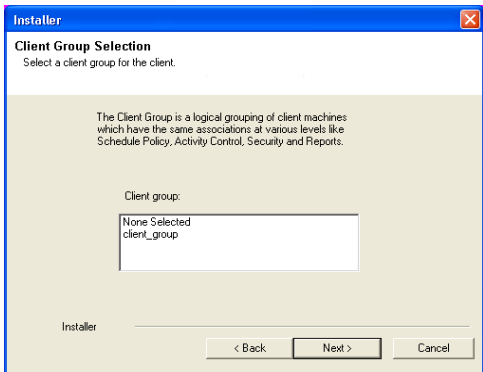
It is recommended that you use alphanumeric characters only.



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**.

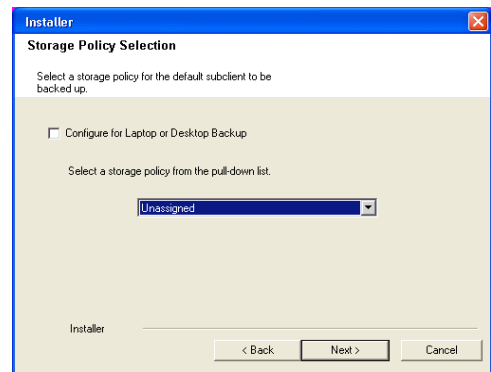
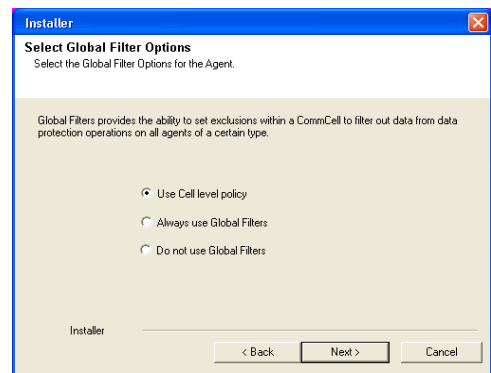
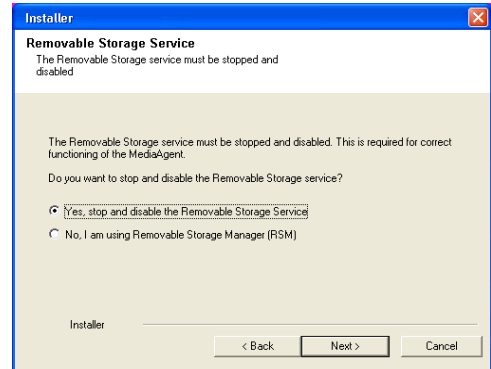
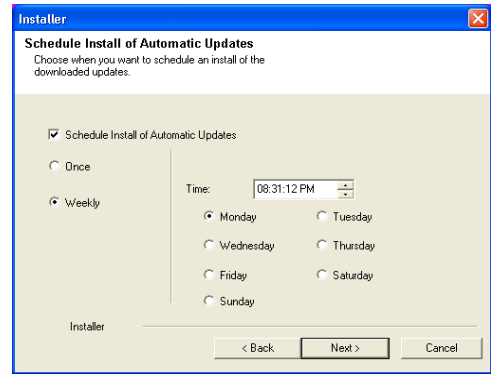
This prompt will not appear if Removable Storage Services are already disabled on the computer.

16. Click **Next**.

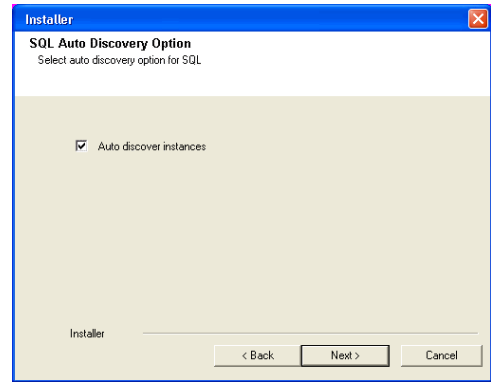
17. Select a **Storage Policy**.
Click **Next**.

18. Click **Next**.

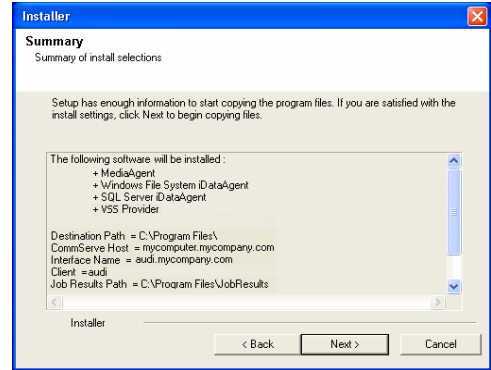
When **Auto Discover Instances** is enabled, new instances are automatically discovered every 24 hours.



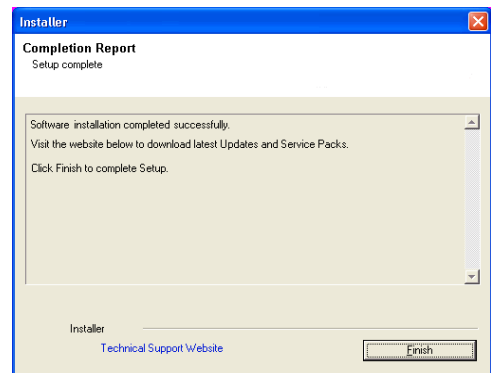
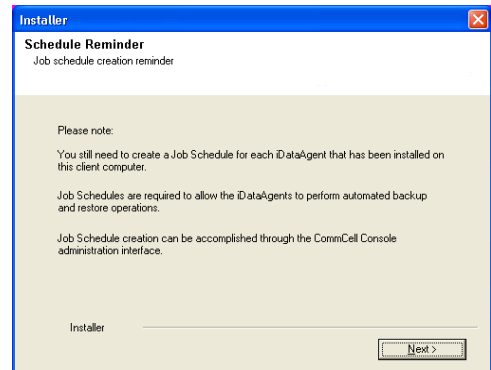
19. Click **Next**.



20. Click **Next**.



21. Click **Finish**.



Getting Started - Microsoft SQL Server Configuration

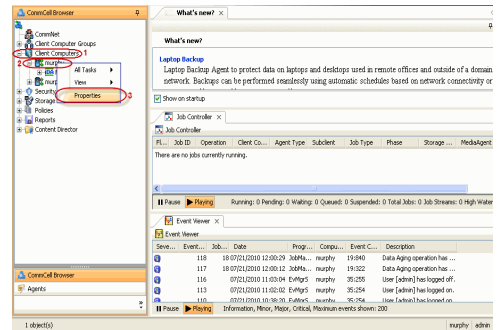
PRE-REQUISITES

- 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.

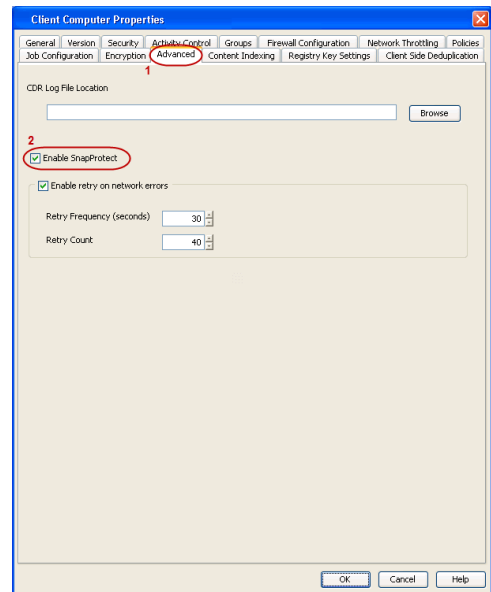
CONFIGURATION

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.

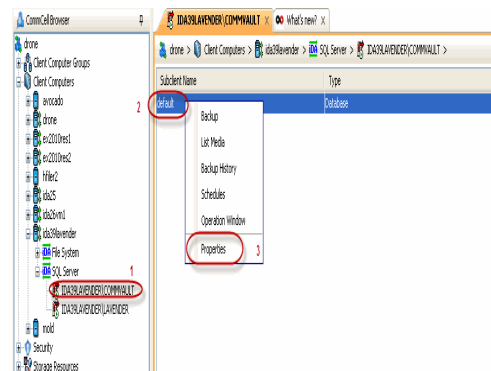
1.
 - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.



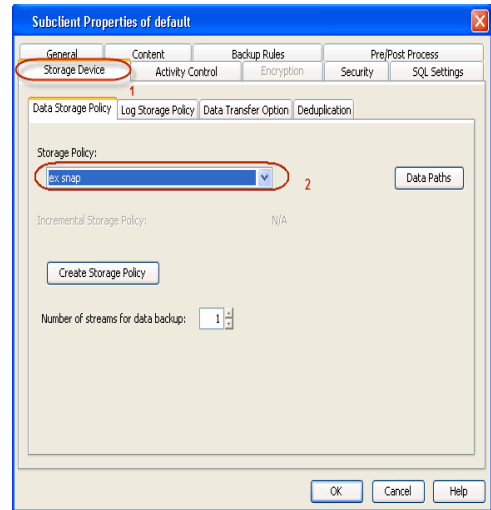
2.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.



3.
 - From the CommCell Browser, navigate to **<Client>** | **SQL Server**.
 - Right-click the default subclient and click **Properties**.



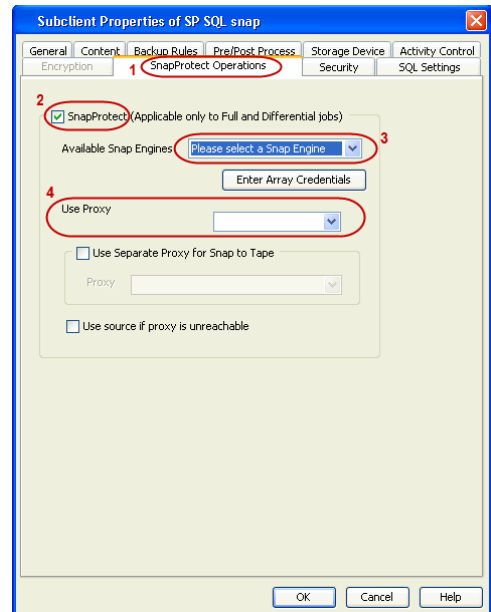
4.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.



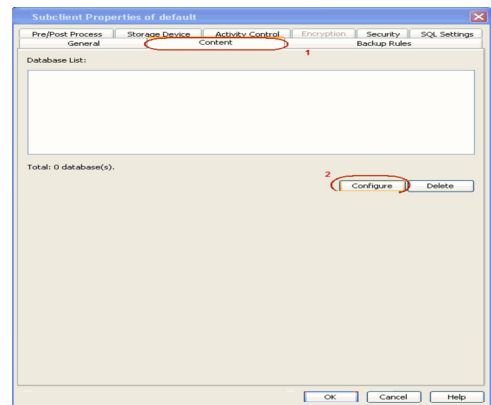
5.
 - Click the **SnapProtect Operations** tab.
 - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
 - Select the storage array from the **Available Snap Engine** drop-down list.
 - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup copy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



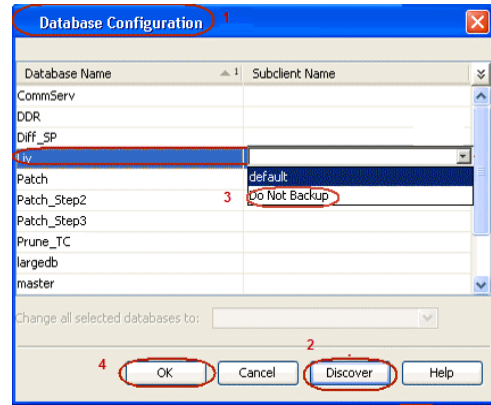
6.
 - Select the **Content** tab.
 - Click **Configure** to discover and associate databases to the subclient.



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.

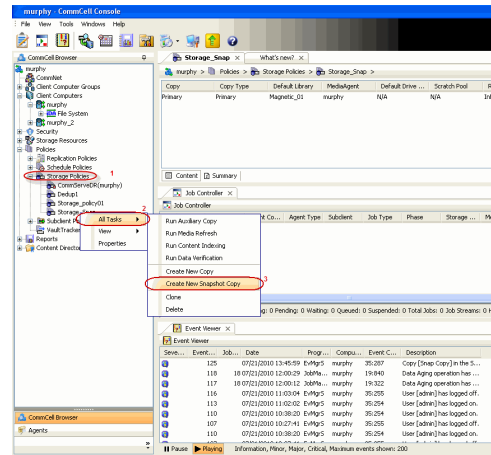
Click **Next** ➤ to Continue.

CREATE A SNAPSHOT COPY

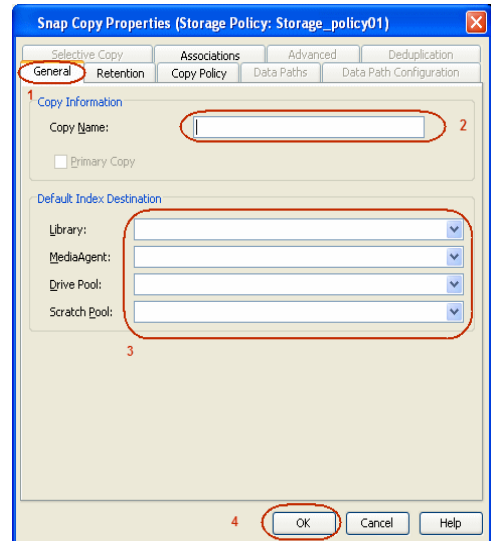
Next ➤

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**.



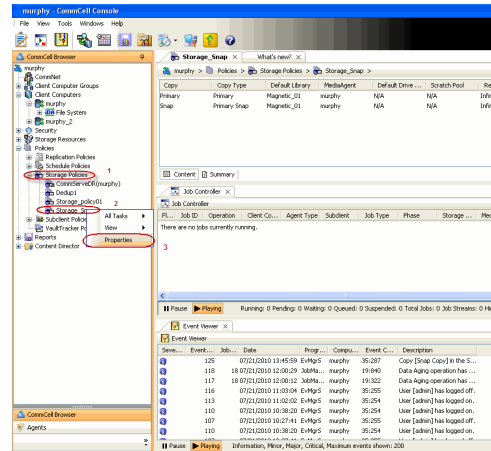
- Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



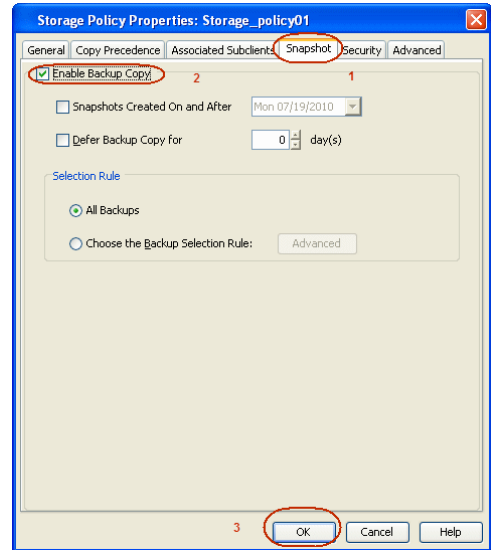
CONFIGURE BACKUP COPY

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

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

◀ Previous Next ▶

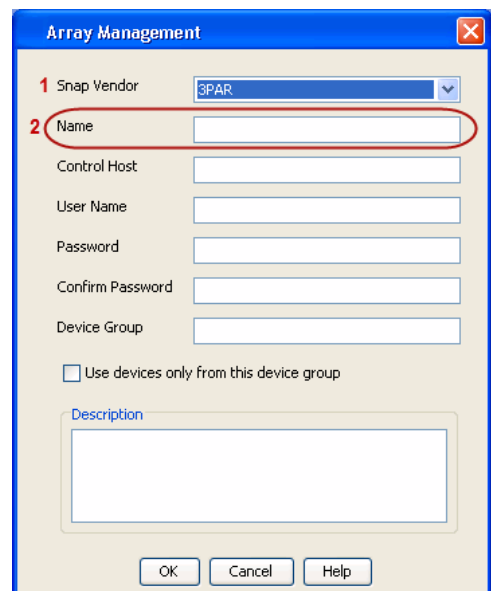
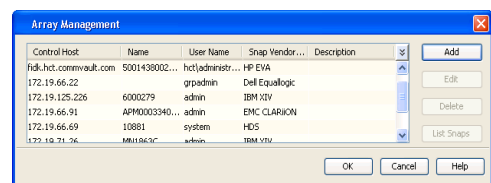
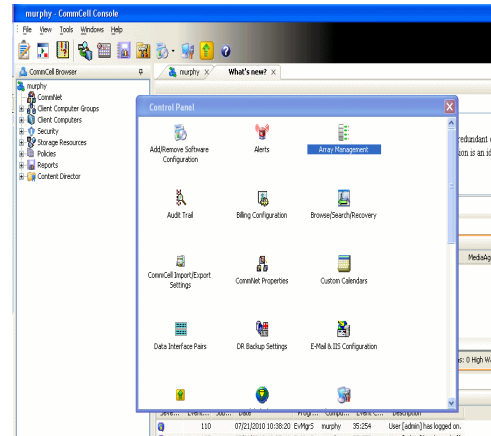
PRE-REQUISITES

- 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

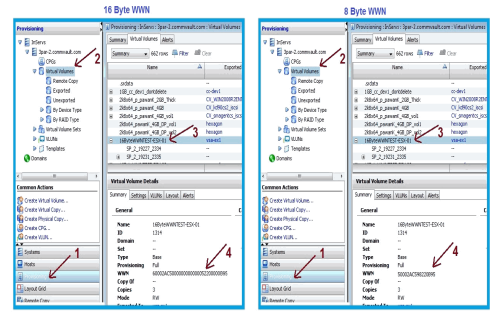
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

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

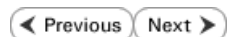
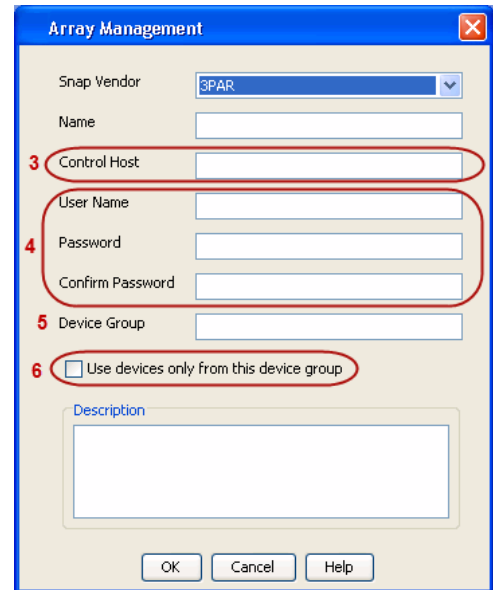
After adding all the values, the resulting array name is 2FF70002AC000B95.



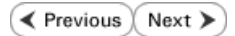
- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be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



PRE-REQUISITIES

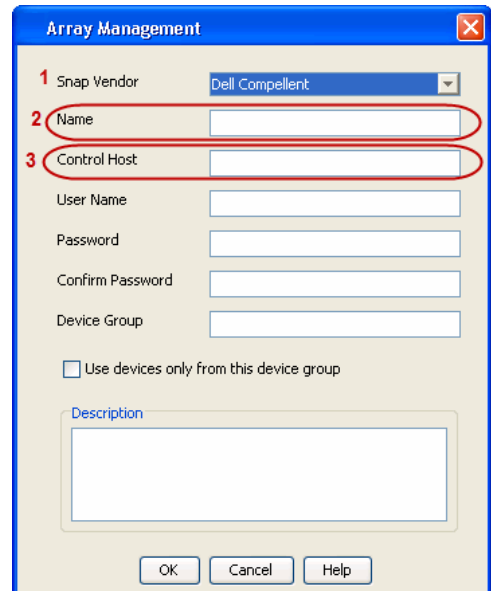
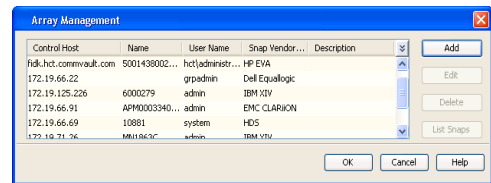
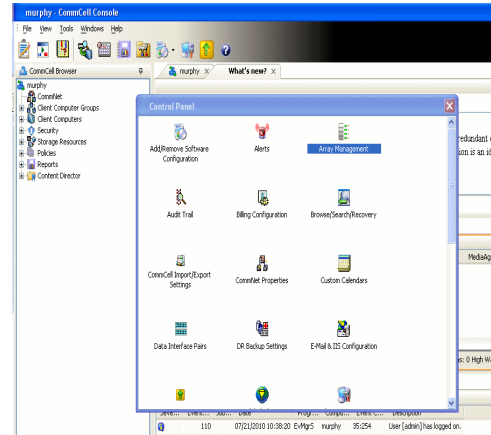
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

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.

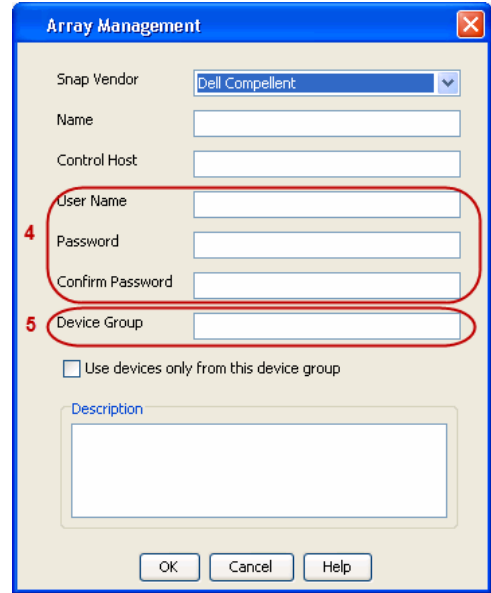
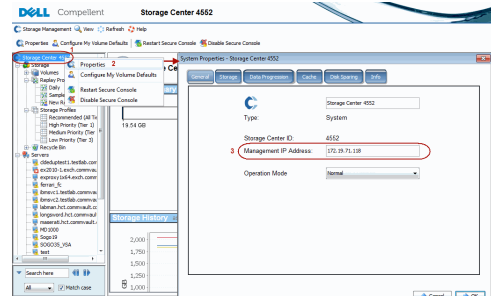
The Management IP address is also referred as the Storage Center IP address.



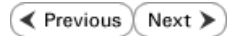
For reference purposes, the screenshot on the right shows the Storage Center Management Console of the Dell Compellent storage device displaying the Management IP address.

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

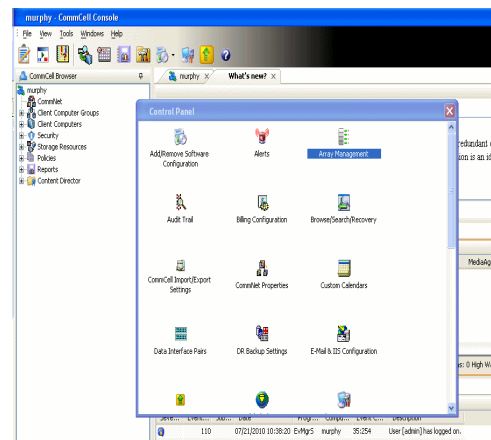
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing 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.

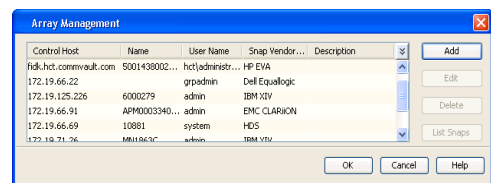
SETUP THE ARRAY INFORMATION

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**.



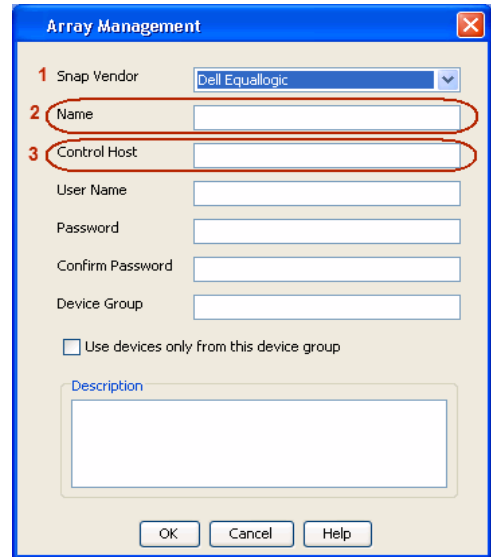
2. Click **Add**.



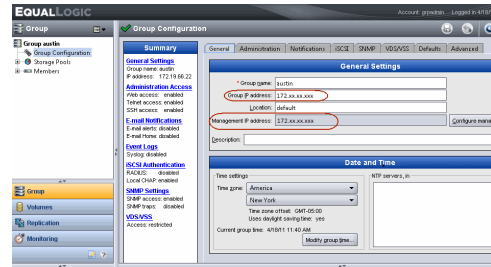
3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

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

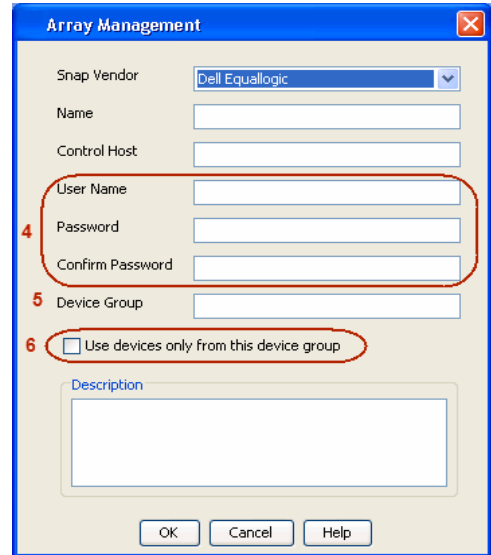
- Specify the Group IP address in the **Control Host** field.



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.

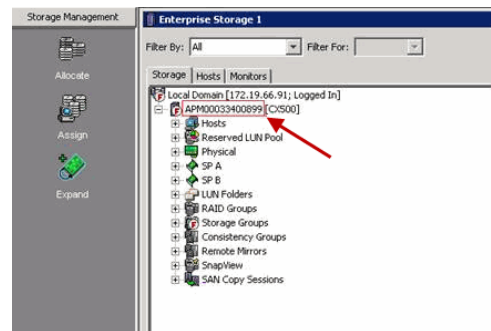
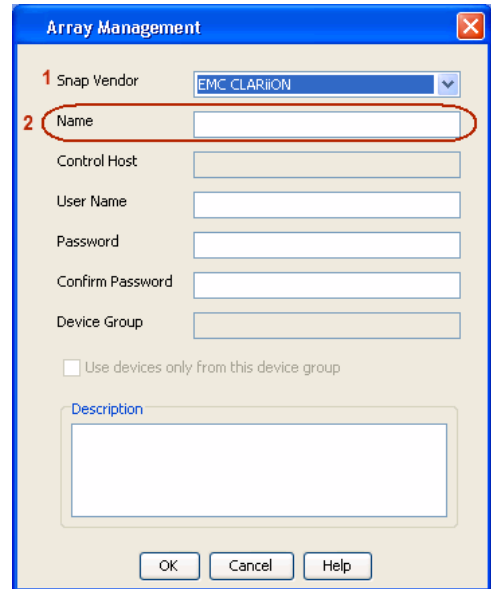
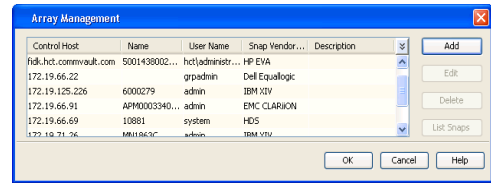
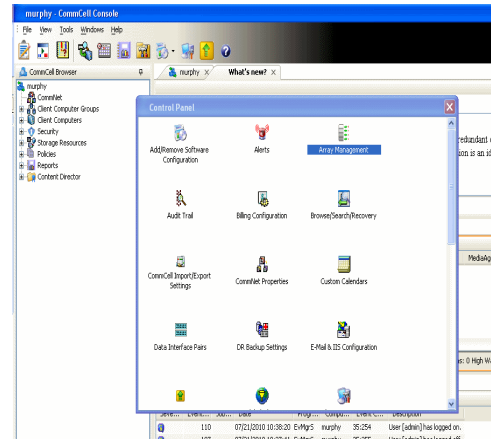
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

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

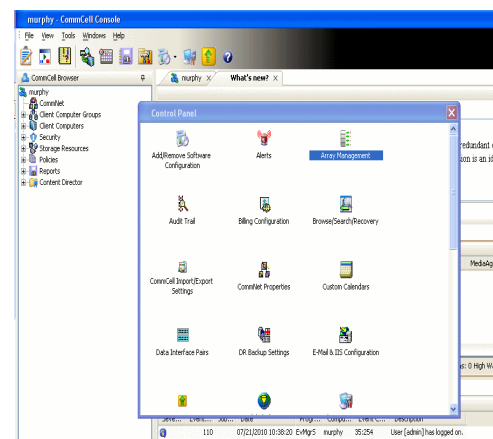
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

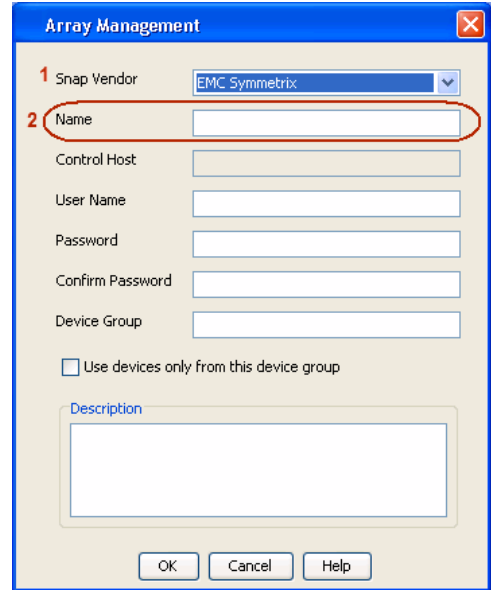
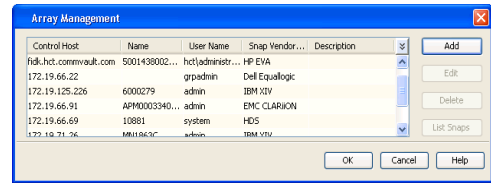
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

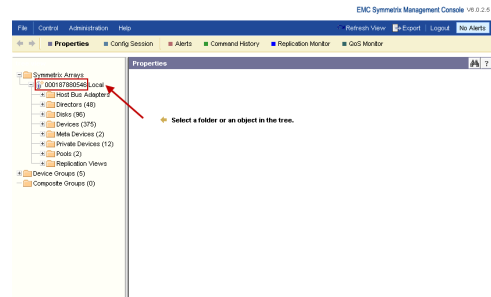


2. Click **Add**.

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

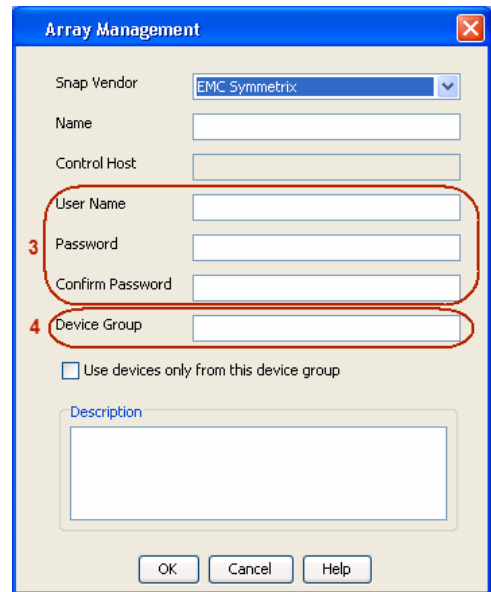


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.

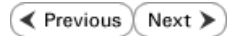


4.
 - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. 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



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

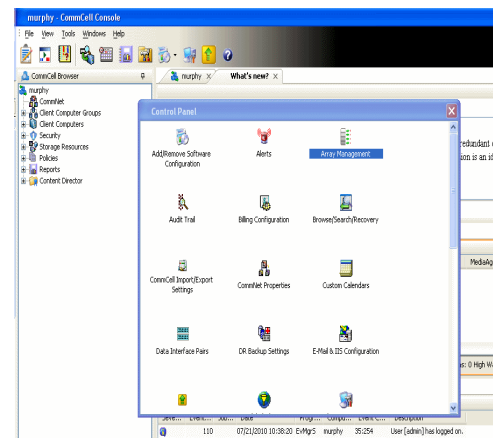
If pre-paired sessions are not available, destination volumes are automatically created for clone snapshots. If a non-existing device group is specified during array configuration in the CommCell Console, a destination volume is created based on the source volume type. However, if a valid device group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

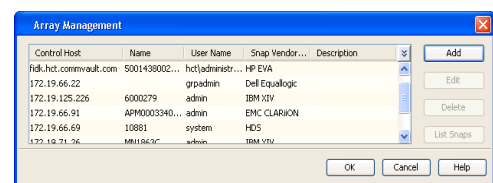
SETUP THE ARRAY INFORMATION

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**.

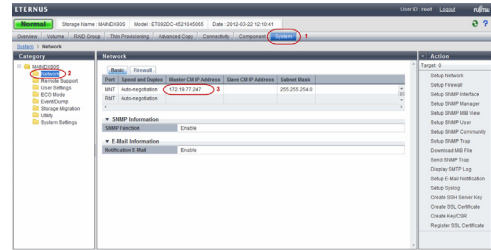
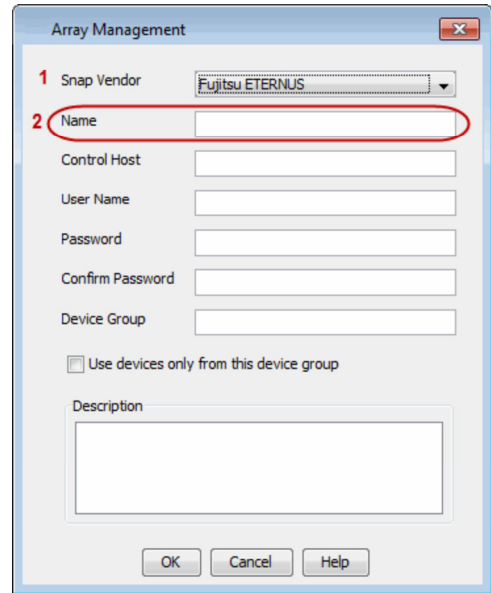


2. Click **Add**.

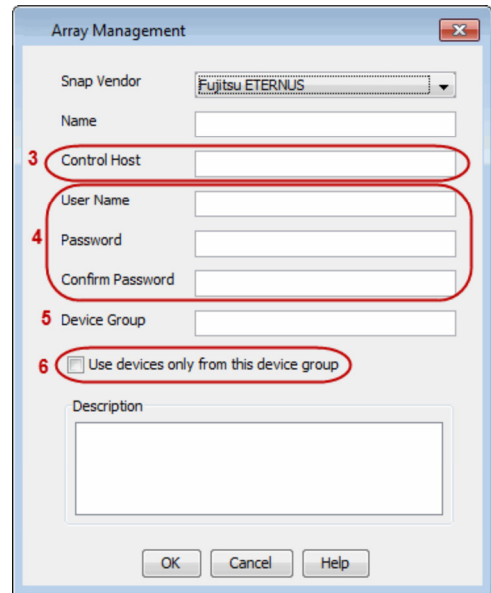


3.
 - Select **Fujitsu ETERNUS** from the **Snap Vendor** list.
 - Specify the CM IP Address of the array in the **Name** field.

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



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

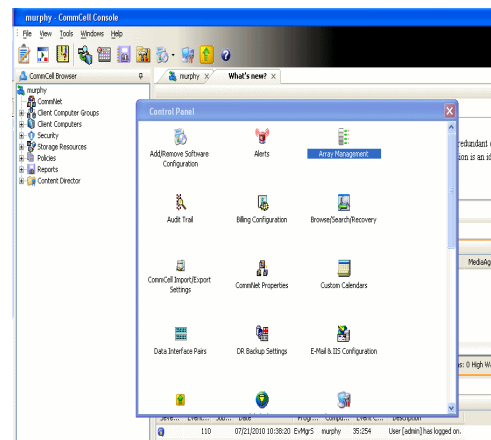
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

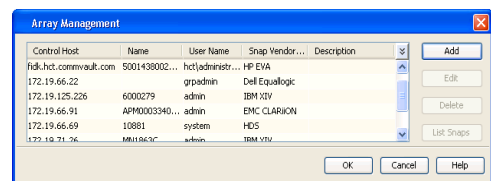
SETUP THE ARRAY INFORMATION

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

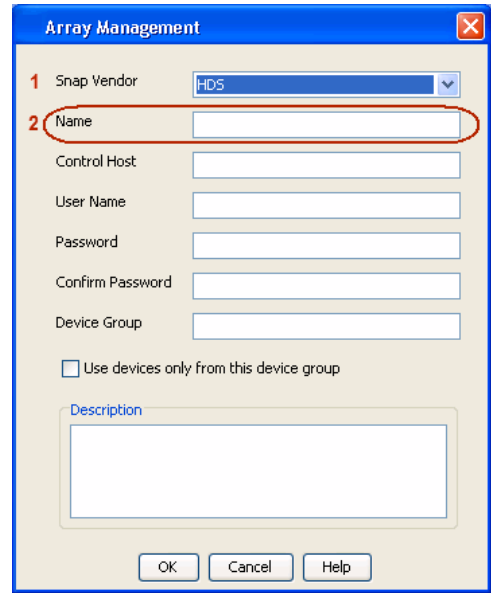
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



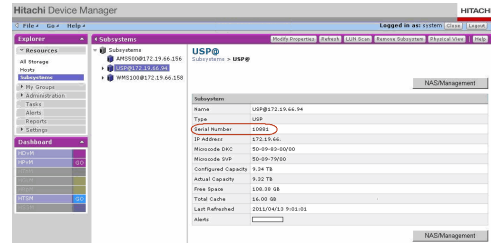
2. Click **Add**.



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.



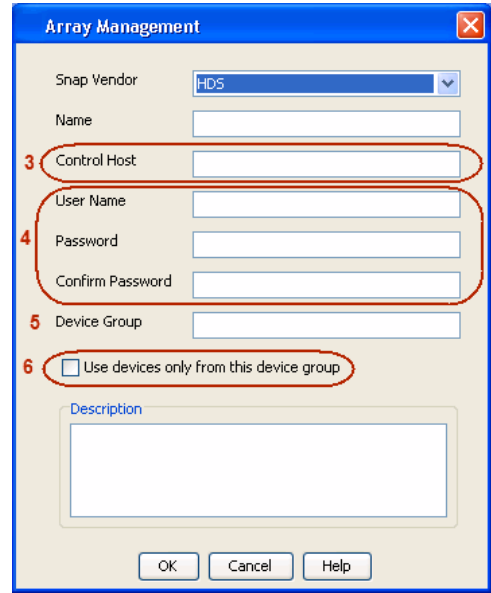
4.
 - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot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

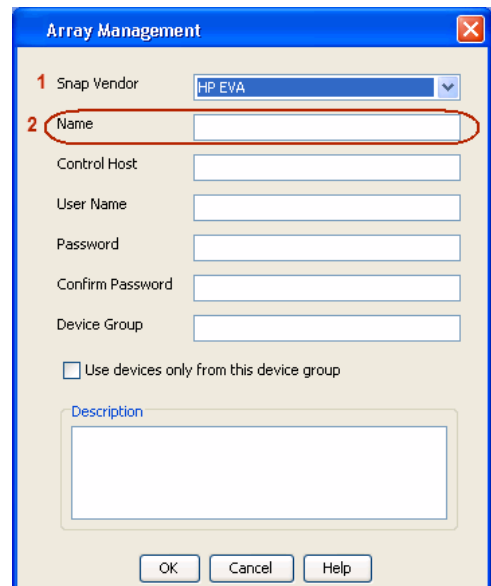
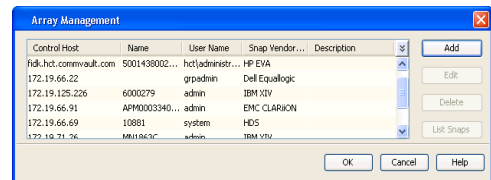
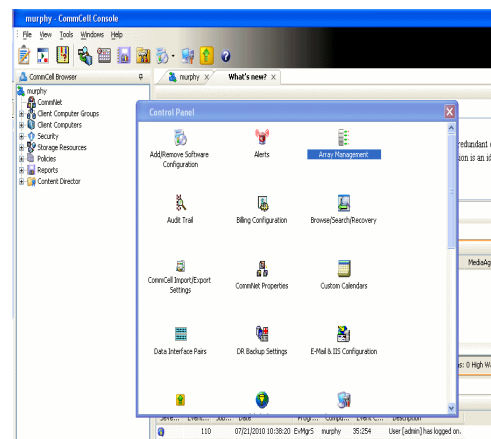
The following steps provide the necessary instructions to setup the HP EVA:

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

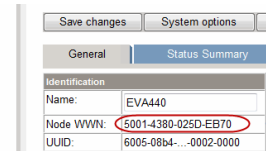
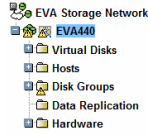
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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.

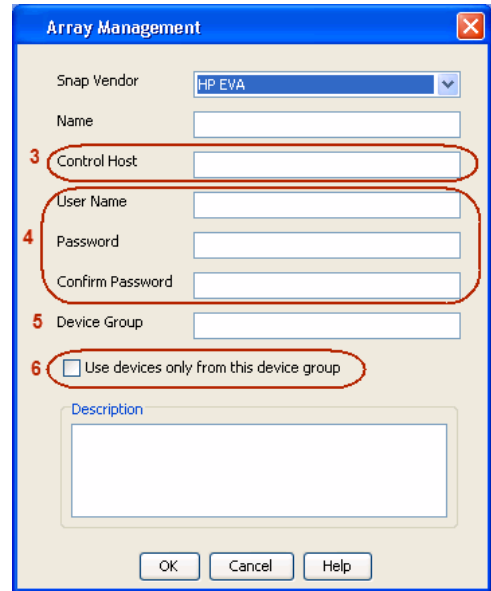
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



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 ▶

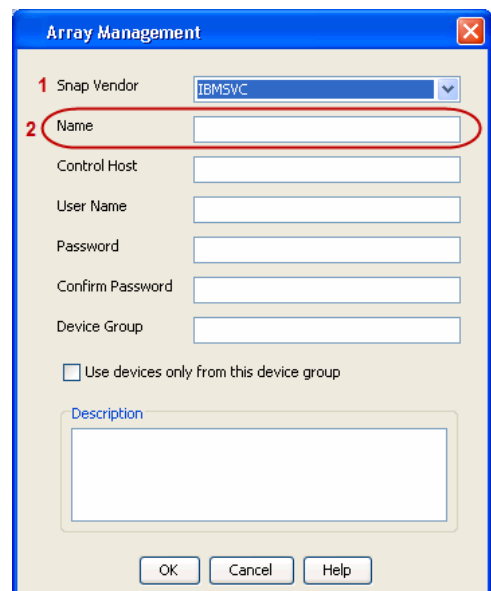
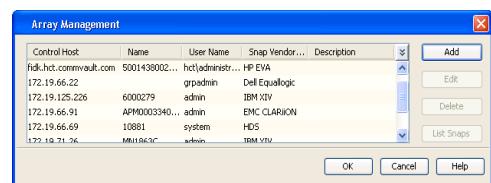
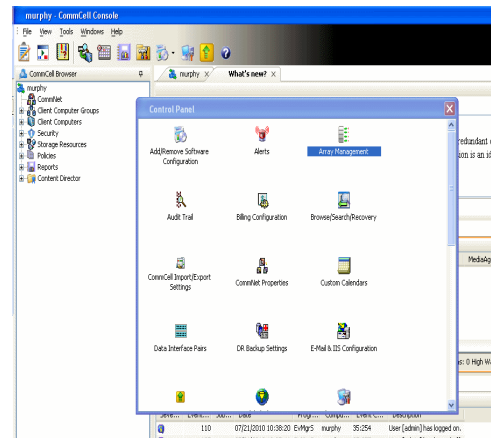
PRE-REQUISITES

- 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.

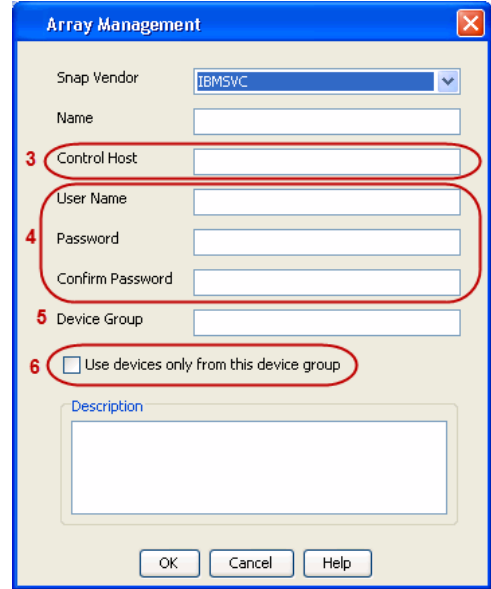
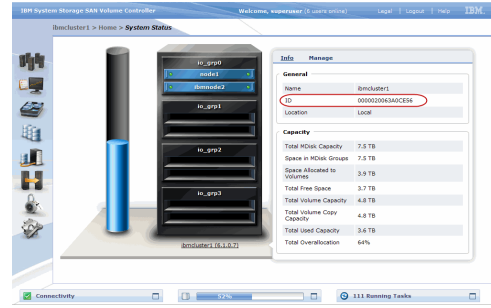
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



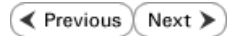
The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

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



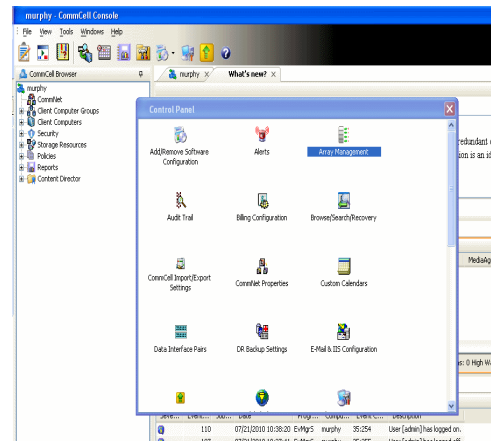
PRE-REQUISITES

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.

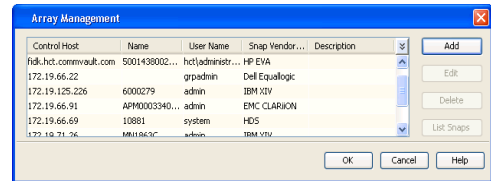
SETUP THE ARRAY INFORMATION

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

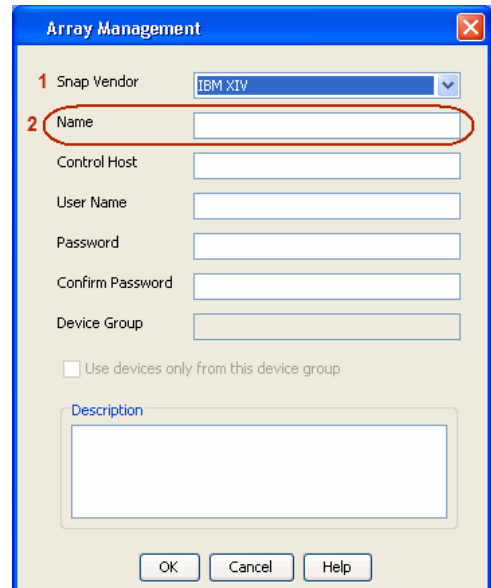
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



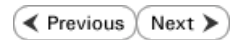
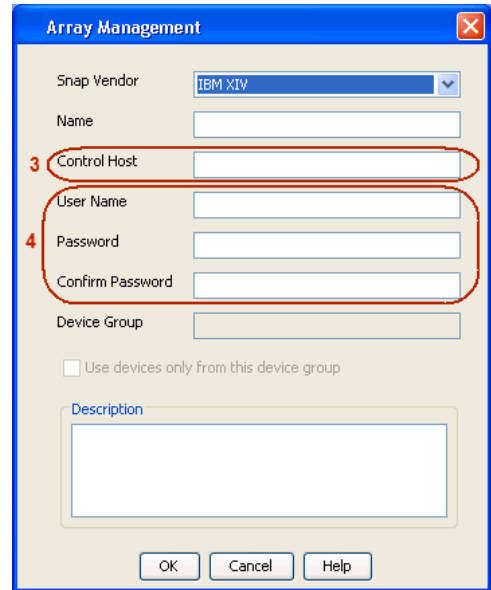
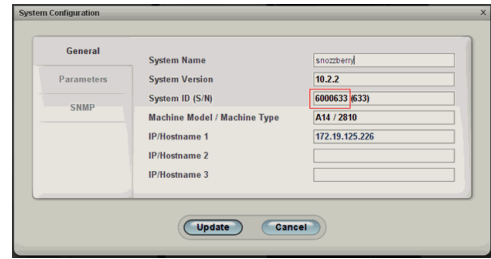
3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



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.

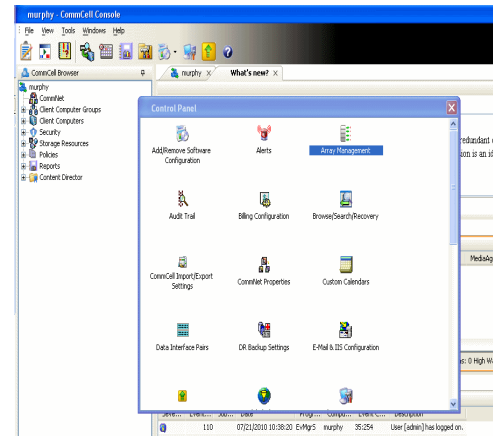
ADDITIONAL REQUIREMENTS FOR VMWARE

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.

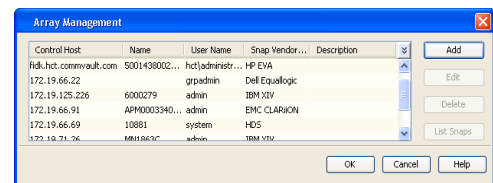
SETUP THE ARRAY INFORMATION

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

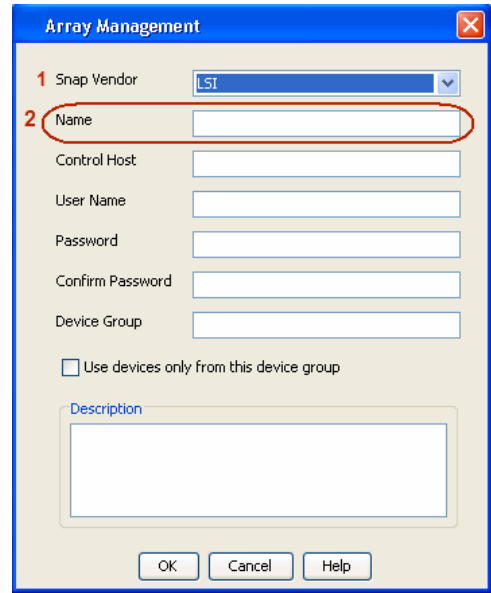
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

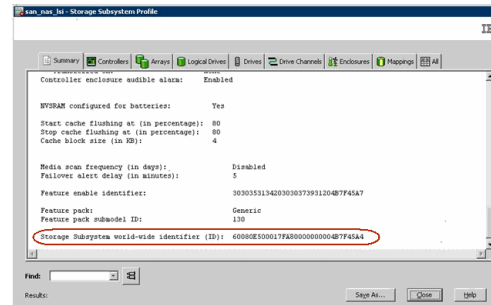


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



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

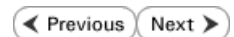
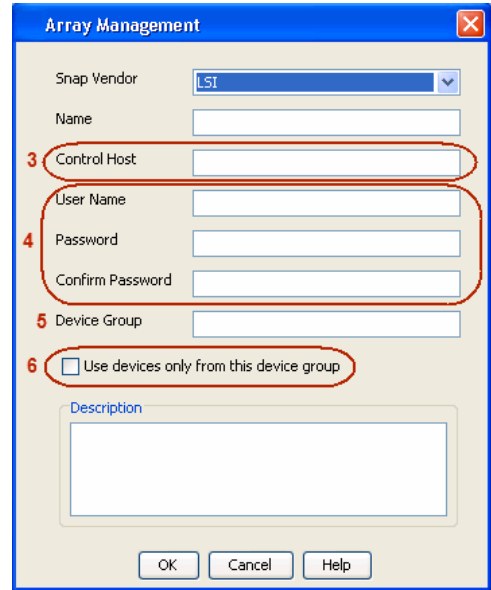
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



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 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

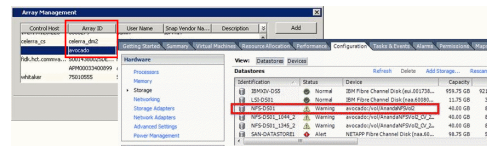
LICENSES

- 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.

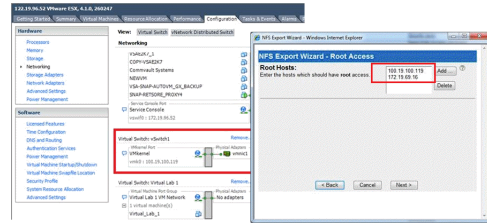
ADDITIONAL REQUIREMENTS FOR VMWARE

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.



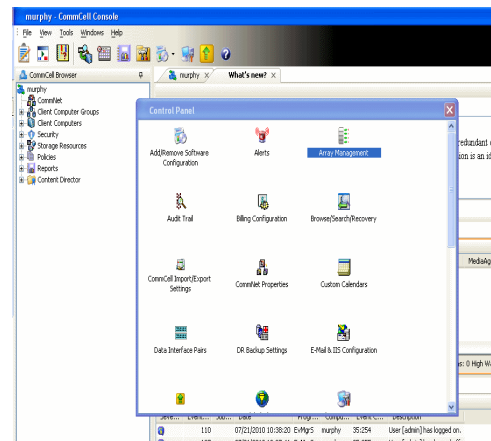
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



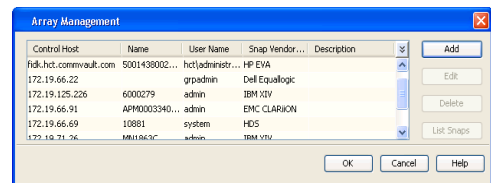
SETUP THE ARRAY INFORMATION

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

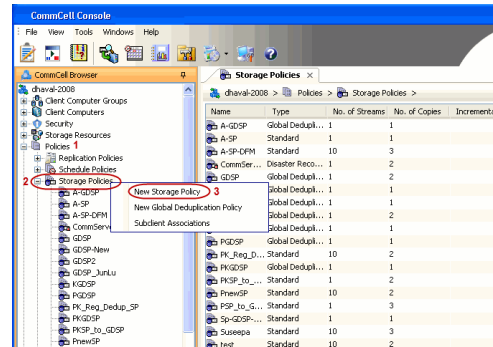
CONFIGURATION

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

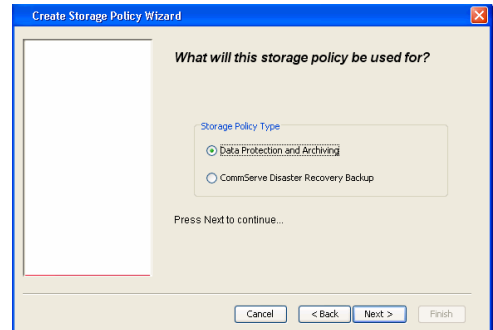
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

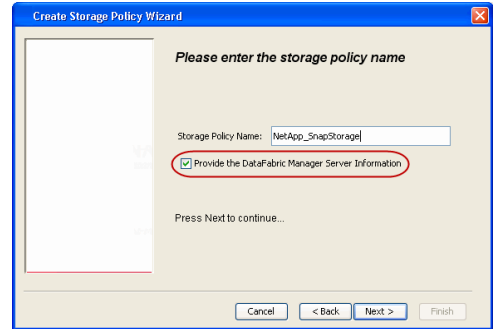
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



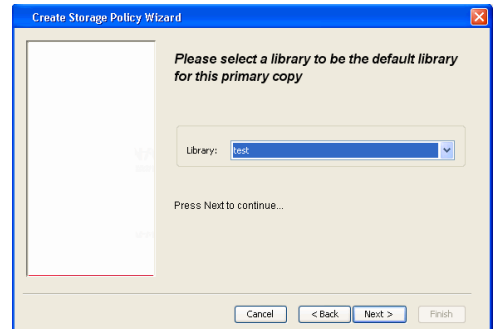
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



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

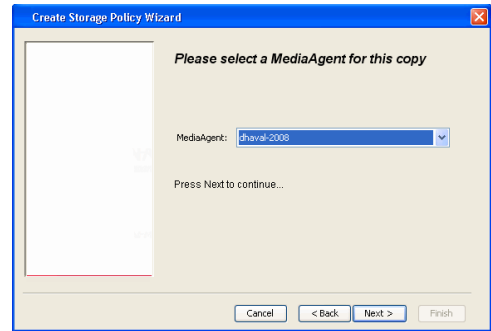
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

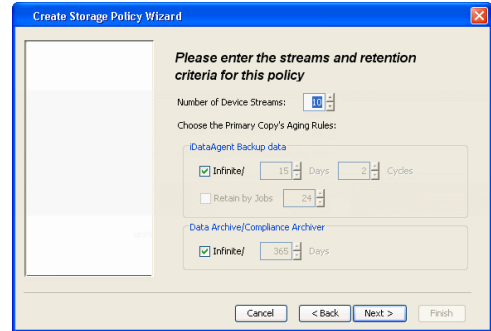


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

6. Click **Next**.

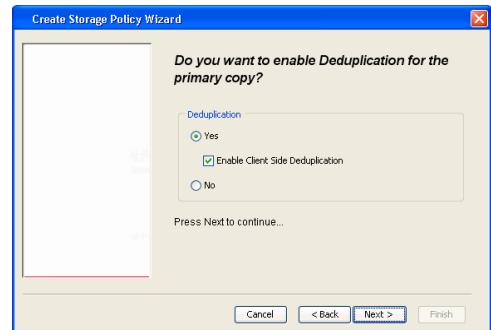


7. Click **Next**.



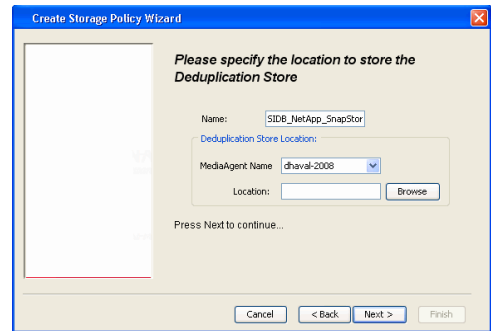
8.

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

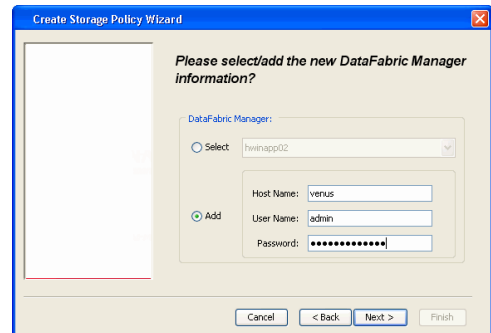


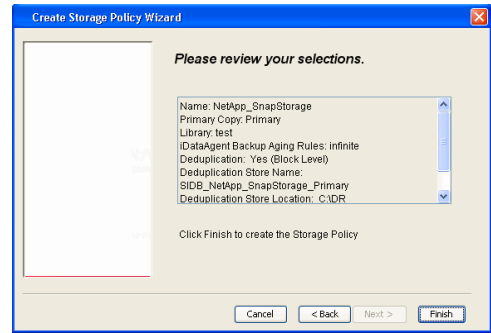
9.

- 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**.



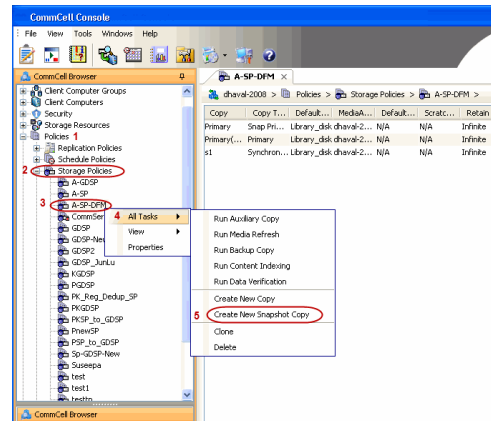


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

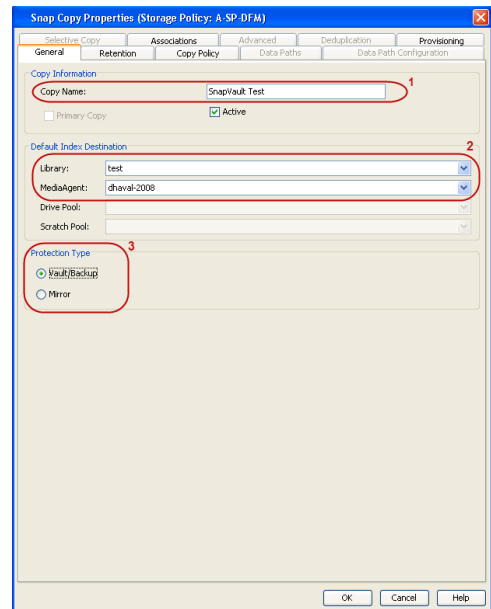
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

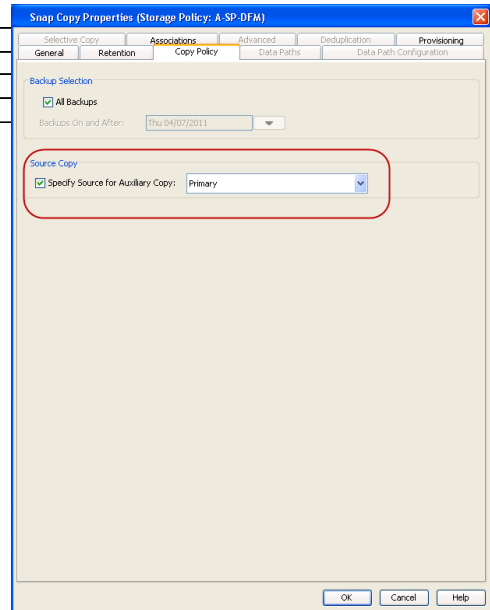


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

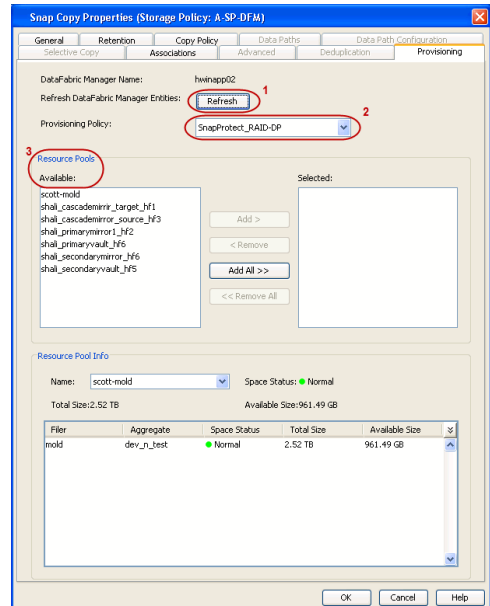
TOPOLOGY	SOURCE COPY
----------	-------------

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.

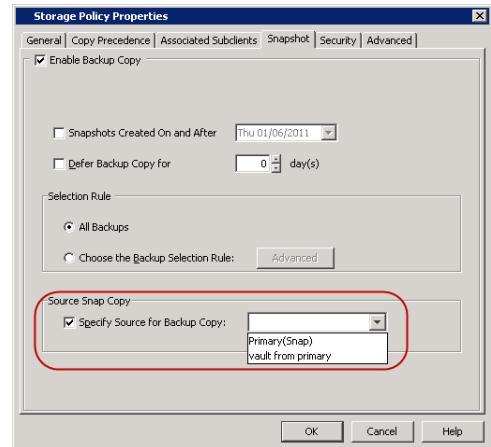
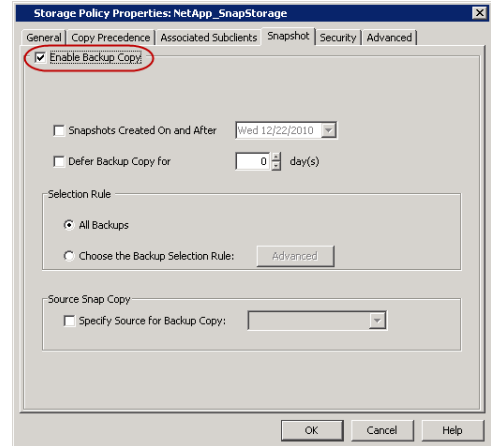
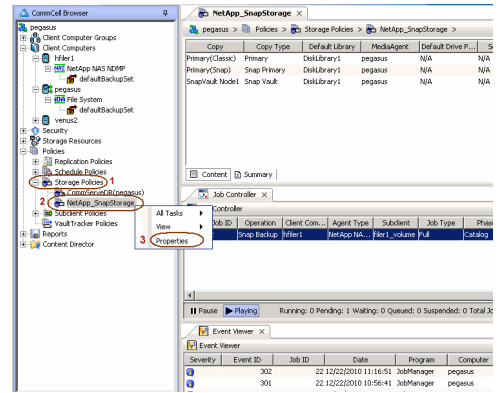
CONFIGURE BACKUP COPY

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.

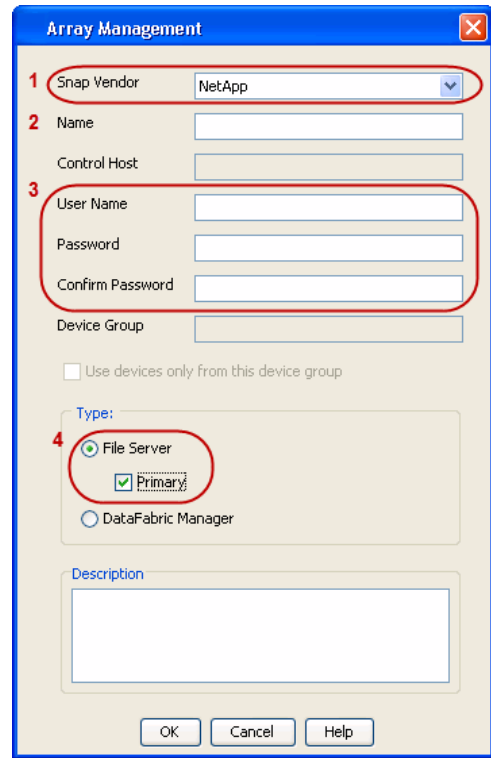
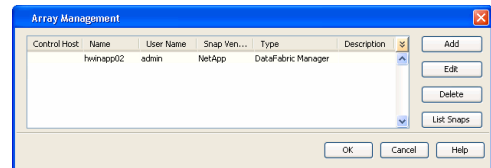
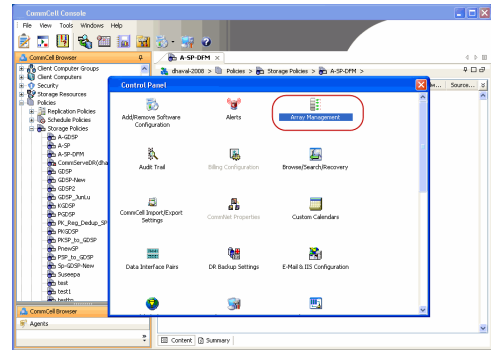
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

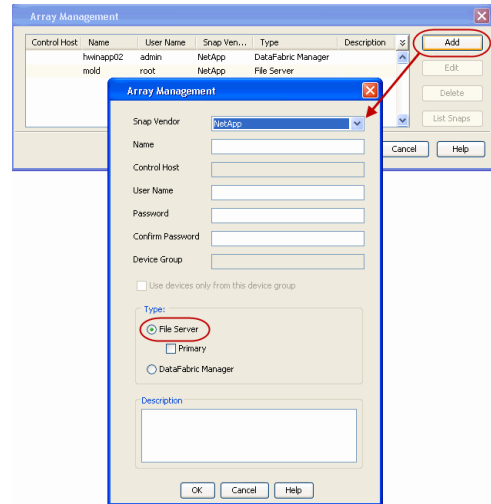
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

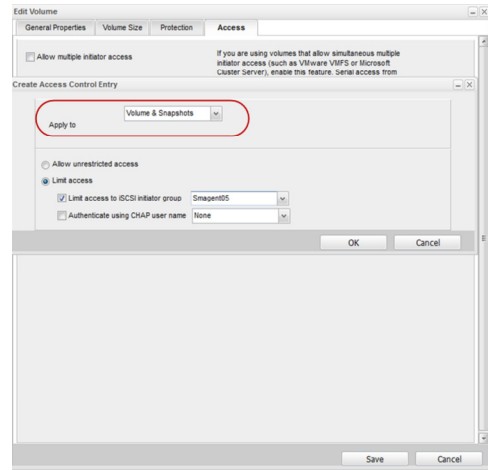
Import Wizard Tool

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

SnapProtect™ Backup - Nimble

PREREQUISITES

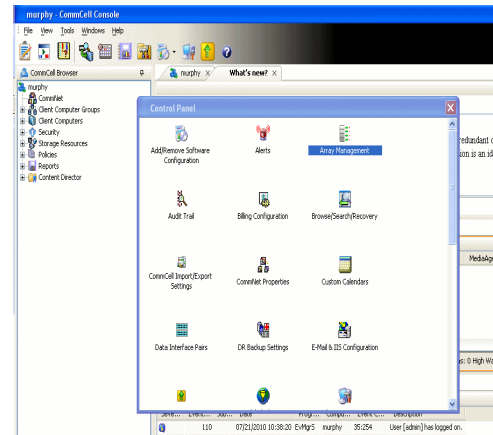
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry**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



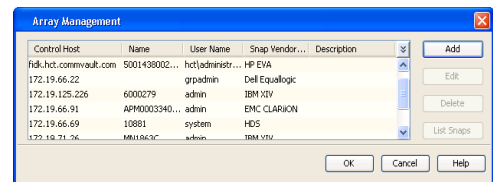
SETUP THE ARRAY INFORMATION

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.

Array Management

Snap Vendor: Nimble

Name: [Text Field]

Control Host: [Text Field]

User Name: [Text Field]

Password: [Text Field]

Confirm Password: [Text Field]

Device Group: [Text Field]

Use devices only from this device group

Type:

- File Server
- Primary
- DataFabric Manager

Description: [Text Area]

OK Cancel Help

◀ 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.

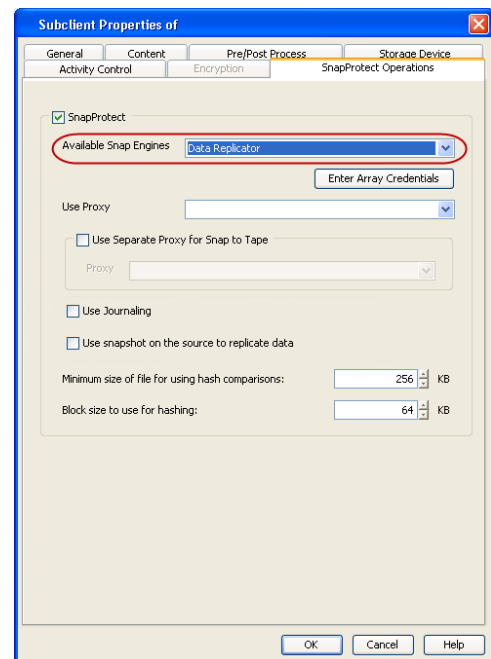
STORAGE POLICY REQUIREMENTS

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

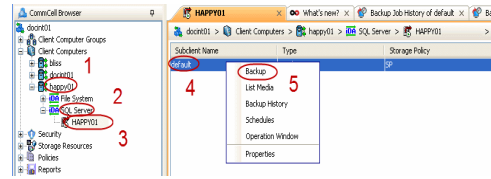
- From the CommCell Console, navigate to <Client> | <Agent>.
 - Right-click the subclient and click **Properties**.
- Click the **SnapProtect Operations** tab.
 - Ensure **Data Replicator** is selected from the **Available Snap Engine** drop-down list.
 - Click **OK**.



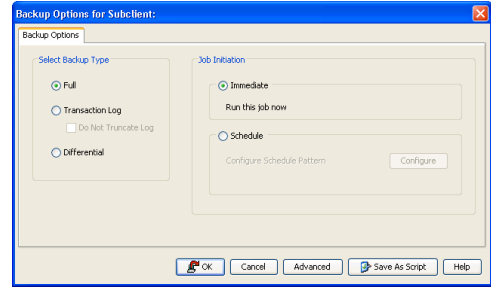
◀ Previous Next ▶

Getting Started Backup - SQL Server *iDataAgent*

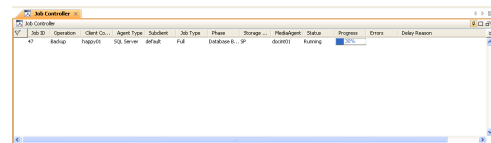
- From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **SQL Server** | **<Instance>**.
 - Right-click the default subclient and click **Backup**.



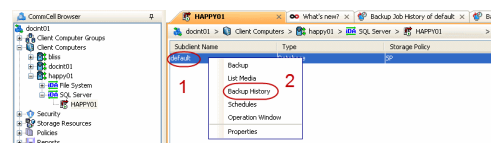
- Click **Full** as backup type and then click **Immediate**.
 - Click **OK**.



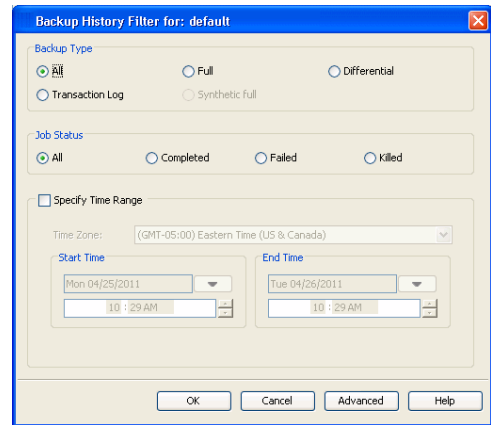
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



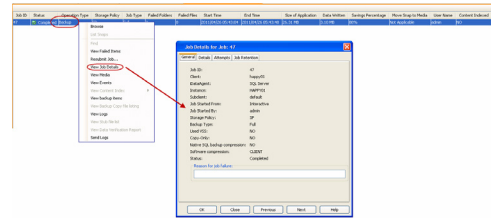
- Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.



- Click **OK**.



- Right-click the job to:
 - Browse the 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

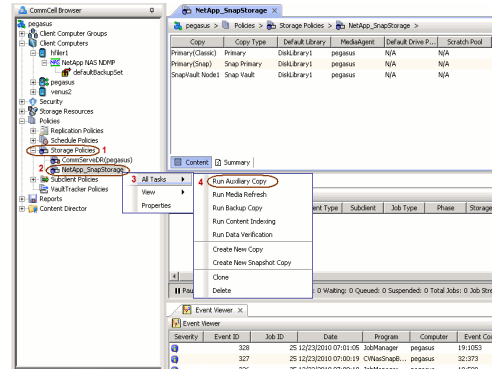
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

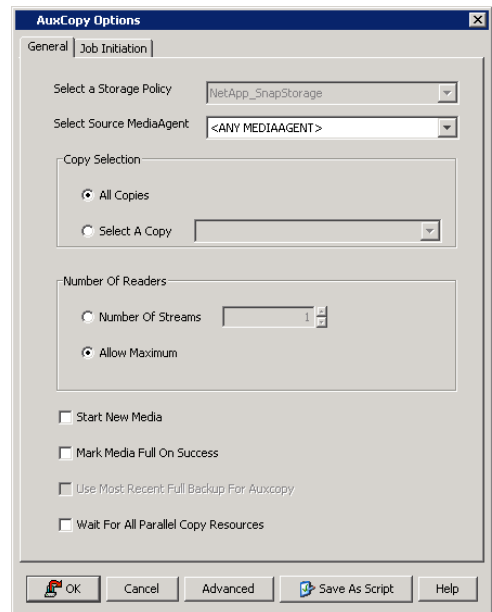
INITIATE VAULT/MIRROR COPY

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**.

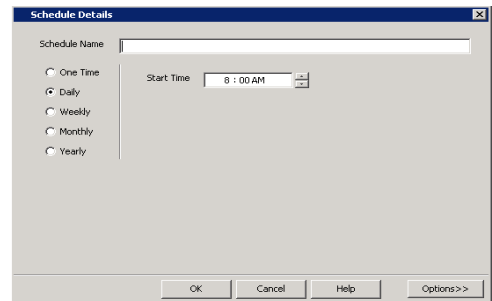


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

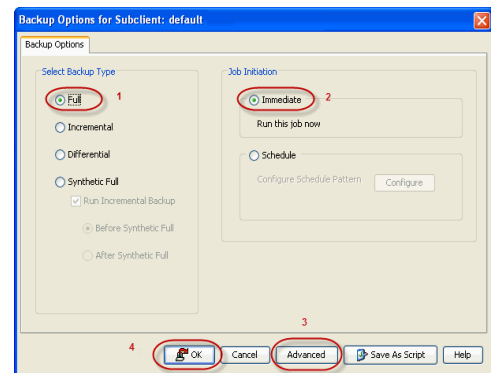
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

INLINE BACKUP COPY

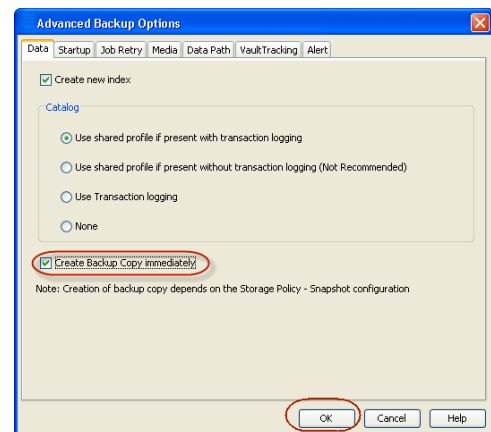
Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect 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**.

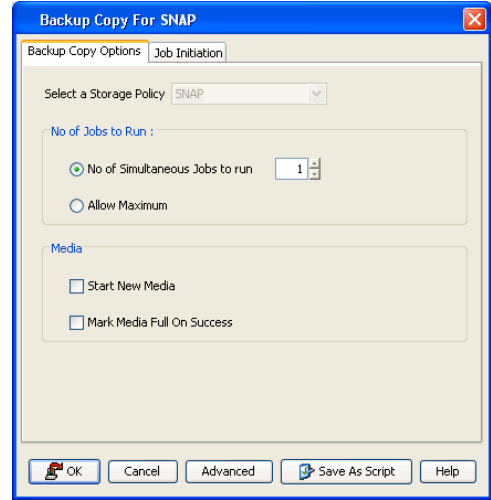
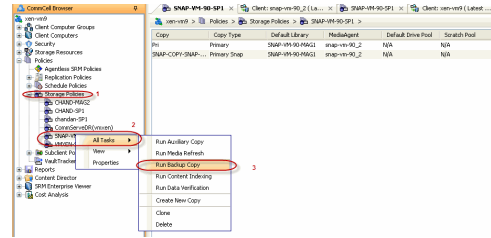


OFFLINE BACKUP COPY

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**.



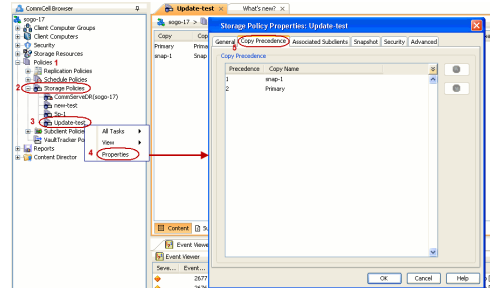
Getting Started - Microsoft SQL Server Restore

PERFORM A RESTORE

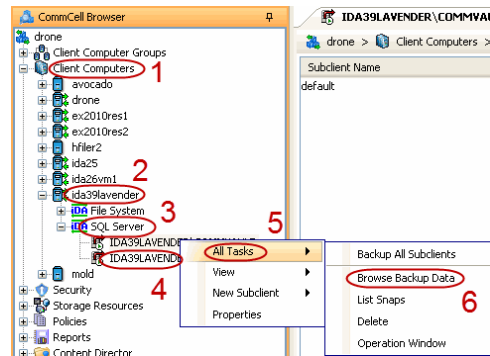
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring a database to a different location on the same destination server.

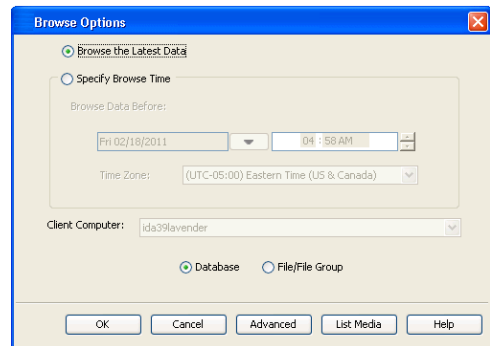
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
 - Click **OK**.



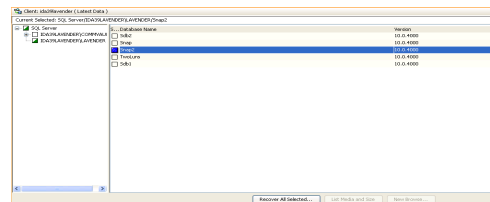
- From the CommCell Browser, navigate to **Client Computers | <Client> | SQL Server**.
 - Right-click the instance and then click **All Tasks | Browse Backup Data**.



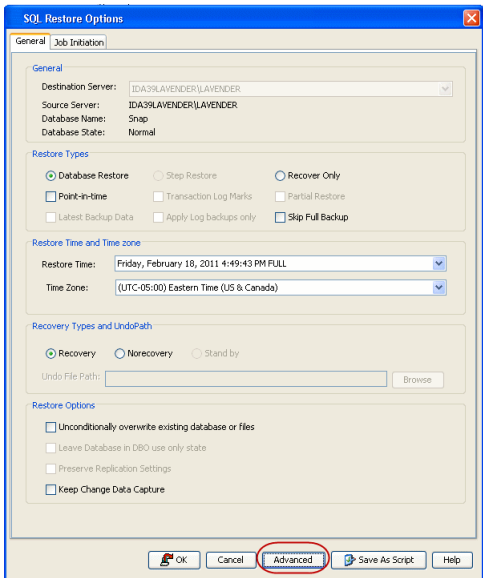
- Click **OK**.



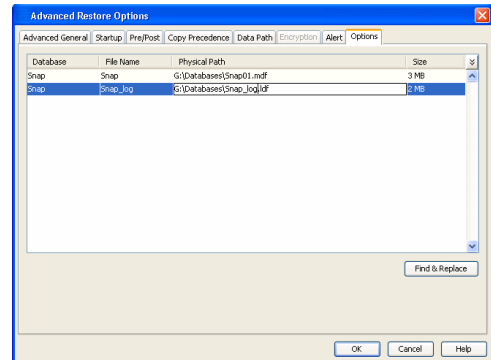
- Click the instance node in the left pane. Select the database you want to restore in the right pane.
 - Click **Recover All Selected**.



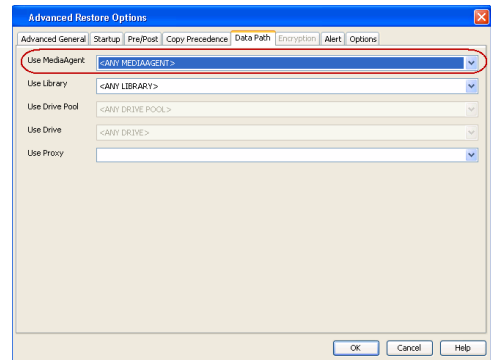
- Click **Advanced**.



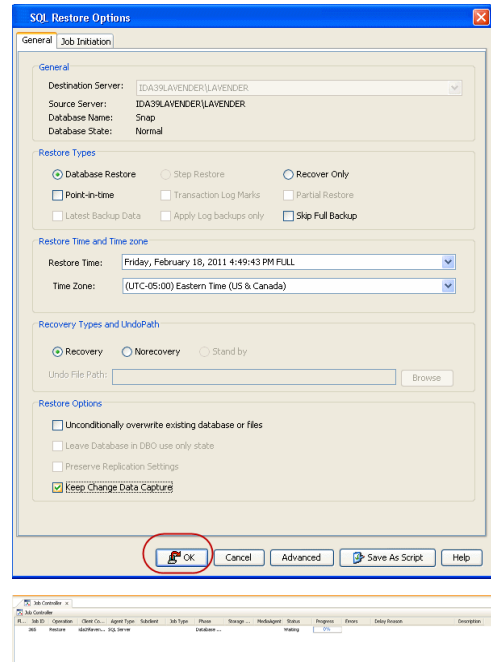
6.
 - Click the **Options** tab.
 - Rename the database name under the **Database** column.
 - Change the path of the database and log files under the **Physical Path** column.
 - Click **OK**.



7.
 - Click the **Data Path** tab.
 - Select a Windows MediaAgent from the **Use MediaAgent** drop-down list.
 - Click **OK**.



8. Click **OK**.



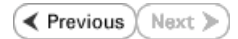
9. You can monitor the progress of the restore job in the **Job Controller**.

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

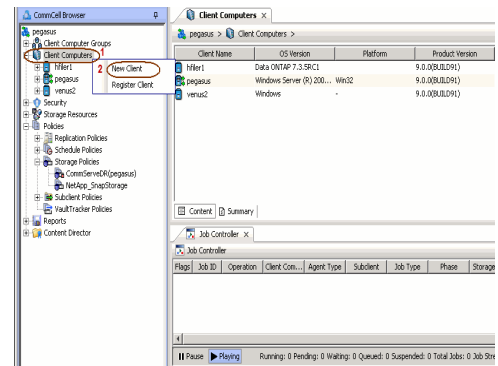
- Prior to performing a SnapProtect backup, ensure that all the available hotfixes for Virtual Disk Service (VDS) and VSS are applied.
- When performing SnapProtect backup for a Windows Cluster, a proxy server must be used for performing backup and restore operations.
- SnapProtect backup on Windows supports basic disks.

CONFIGURATION

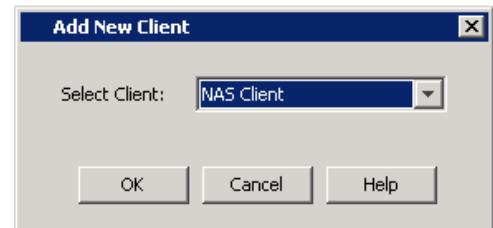
The software for the NAS *iDataAgent* is installed automatically as part of the MediaAgent installation. However, the client is not automatically created in the CommCell Console.

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**.

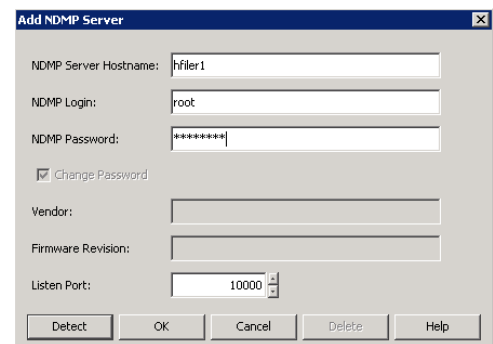
For any ONTAP version, do not provide the host name or IP address of the management port (e.g., e0M). Use the host name or IP address of a data port (e.g., e0A, e0B).

- Click **Detect**.
- Click **OK**.

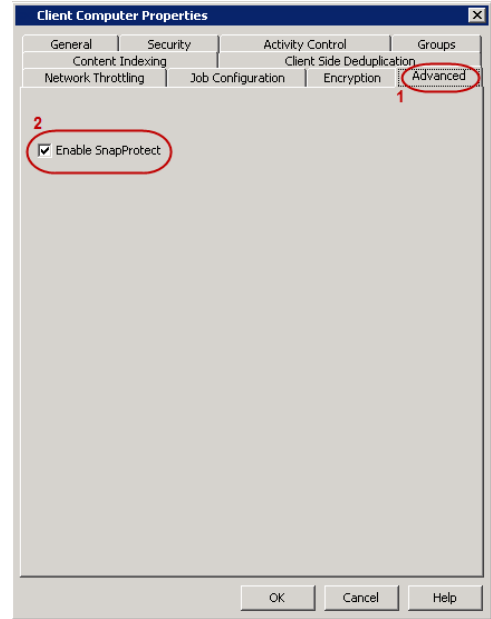
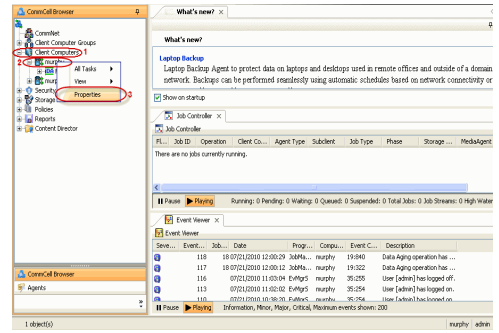
A new client is created and listed under the Client Computers node. The default subclient is created automatically.

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.

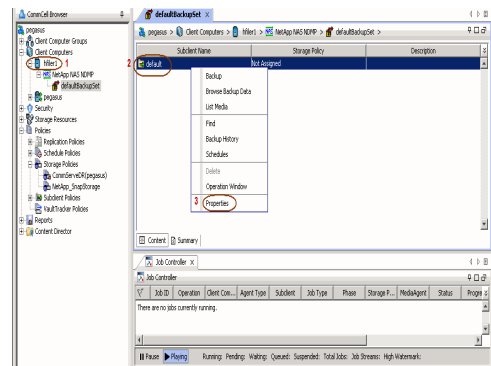
4. From the CommCell Browser, right-click the NAS client just created and select **Properties**.



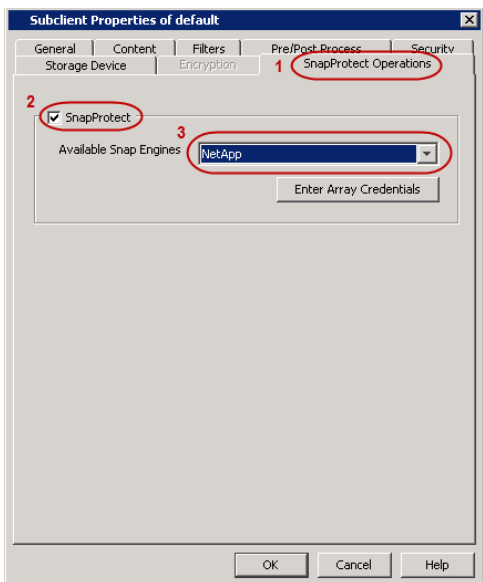
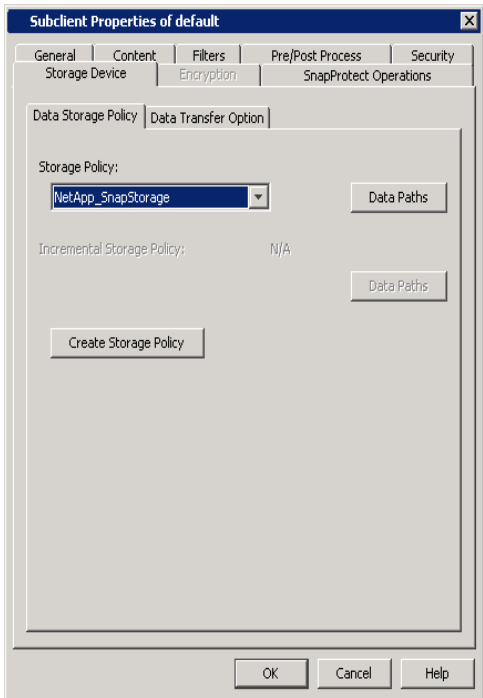
5.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.



6.
 - From the CommCell Browser, right-click the subclient.
 - Click **Properties**.



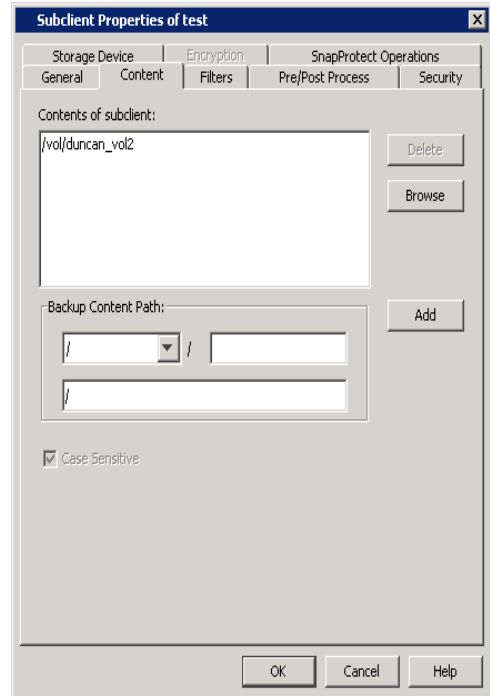
7.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.



- 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.

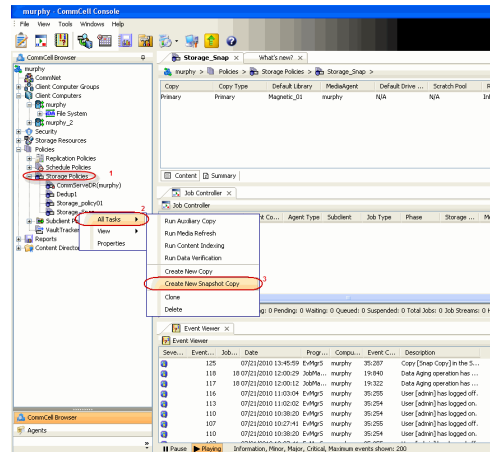
Click **Next** ➤ to Continue.

CREATE A SNAPSHOT COPY

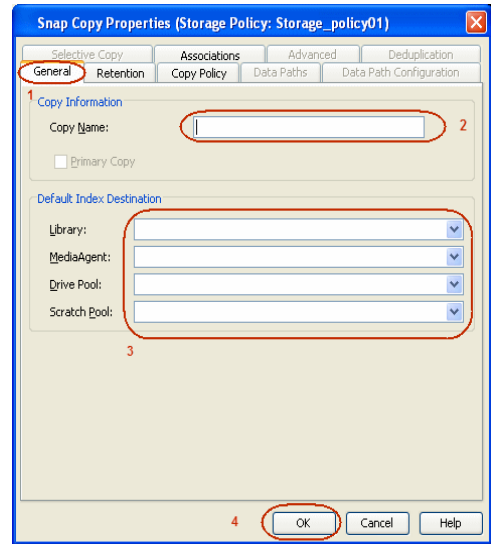


Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

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



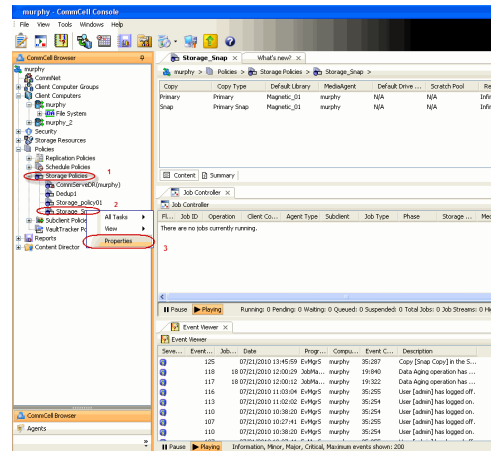
2.
 - Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



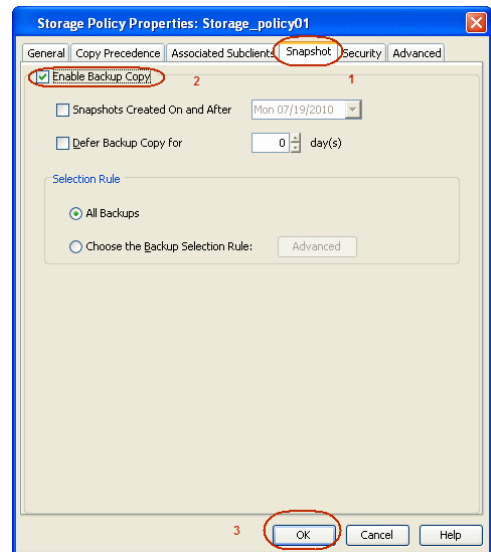
CONFIGURE BACKUP COPY

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

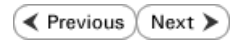
- From the CommCell Browser, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.



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



SnapProtect™ Backup - NetApp



PREREQUISITES

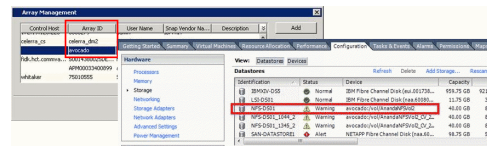
LICENSES

- 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.

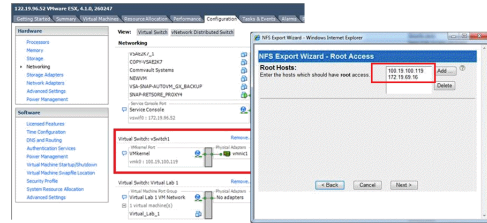
ADDITIONAL REQUIREMENTS FOR VMWARE

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.



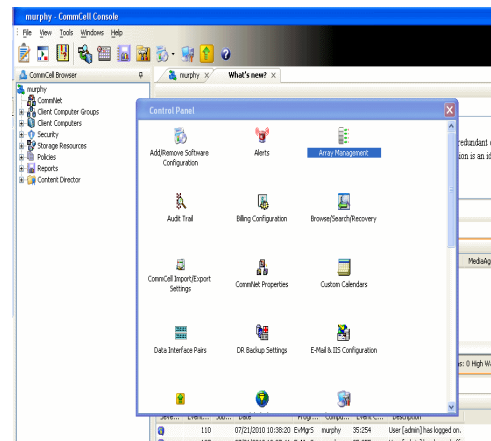
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



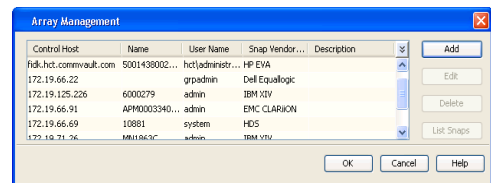
SETUP THE ARRAY INFORMATION

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

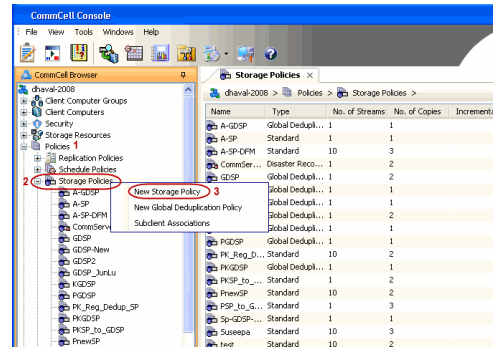
CONFIGURATION

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

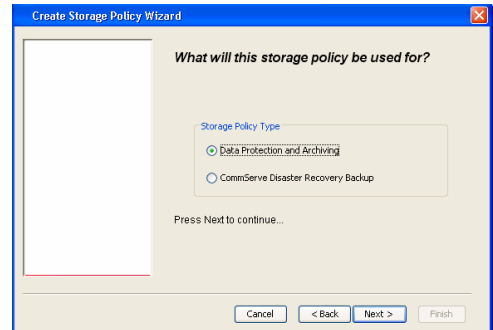
CREATE STORAGE POLICY

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**.



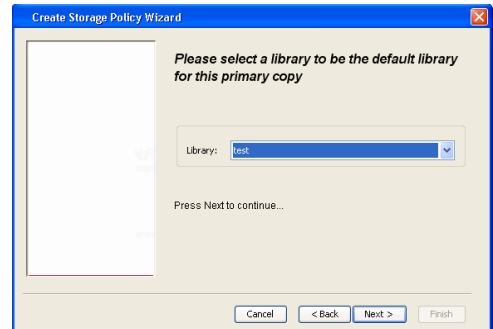
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



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

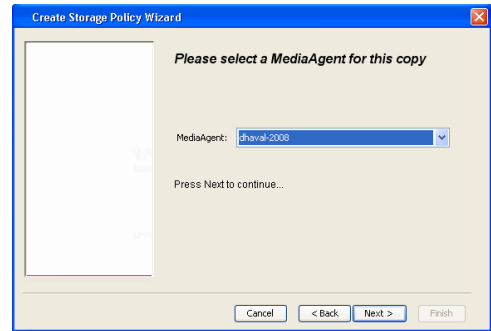
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

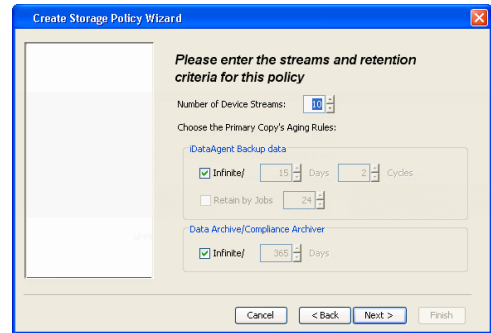


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

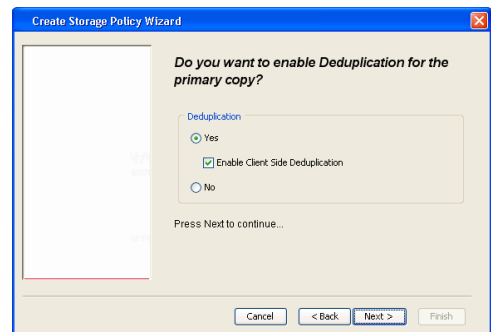
6. Click **Next**.



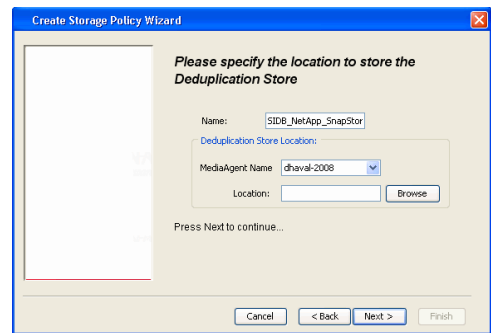
7. Click **Next**.



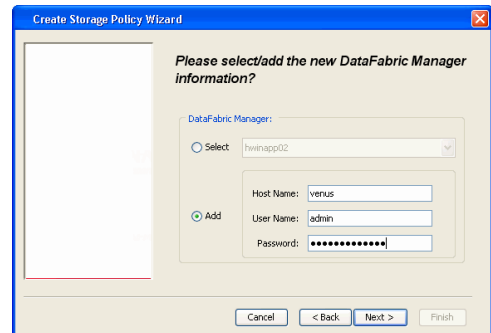
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

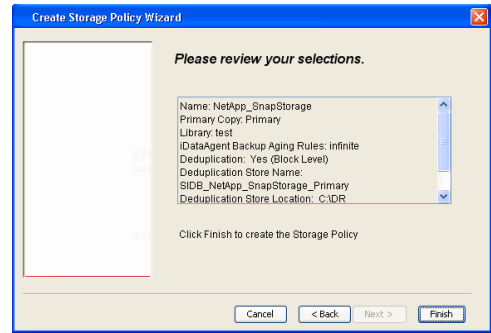


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



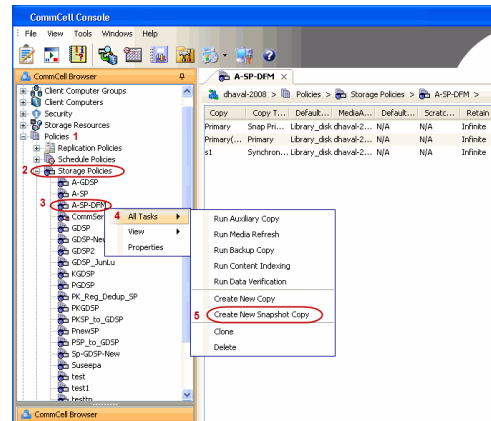


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

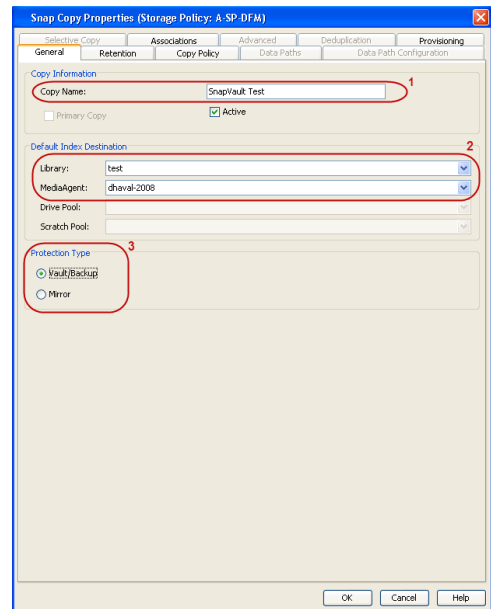
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

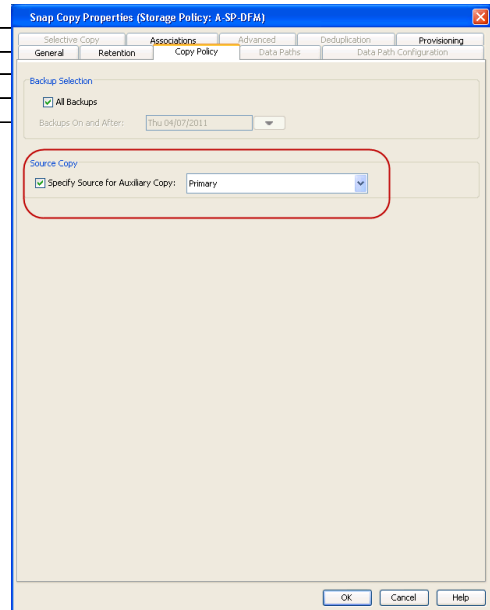


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

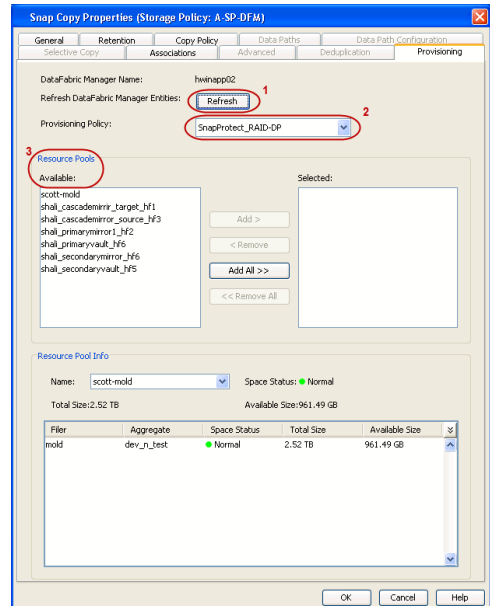
TOPOLOGY	SOURCE COPY
----------	-------------

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.

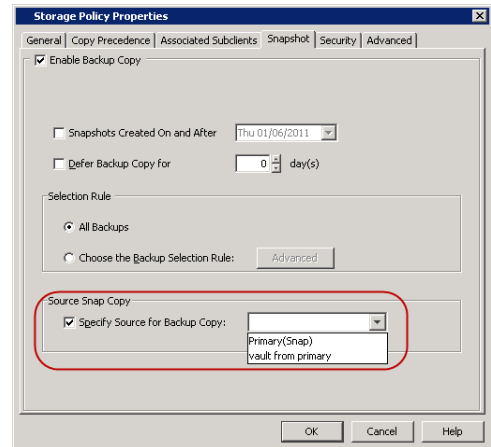
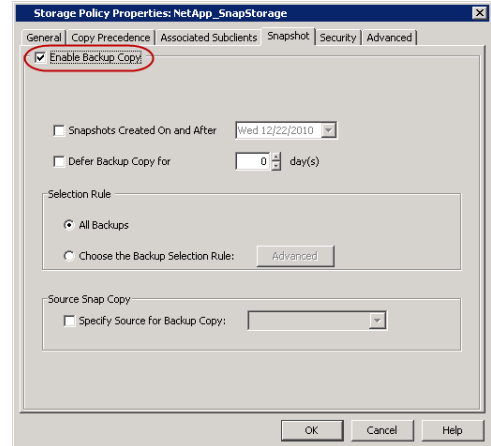
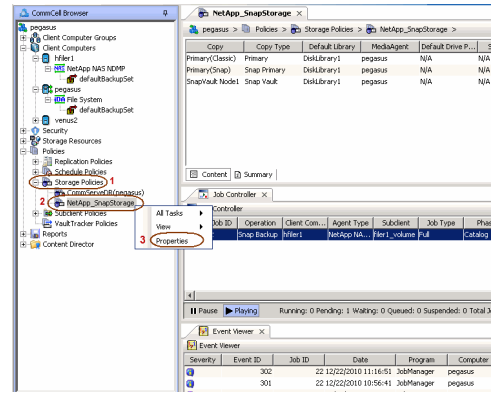
CONFIGURE BACKUP COPY

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.

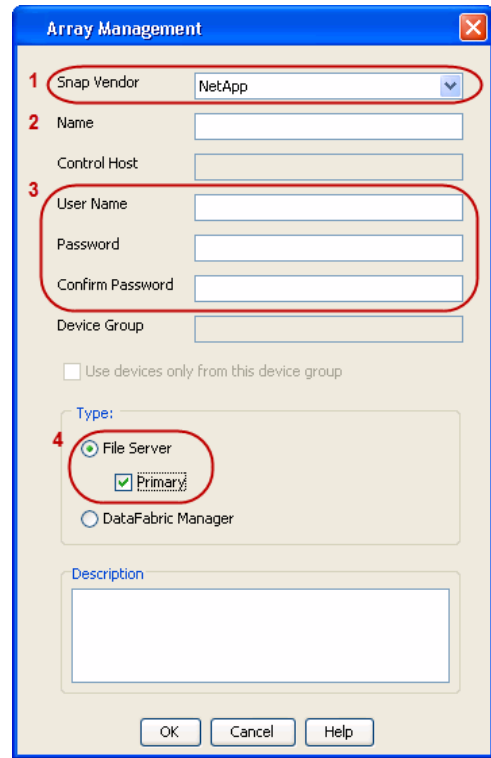
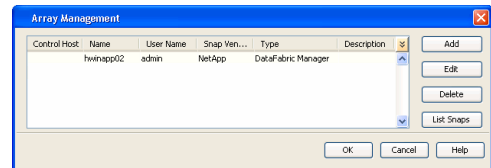
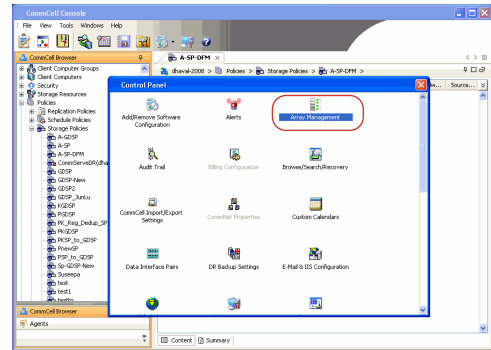
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

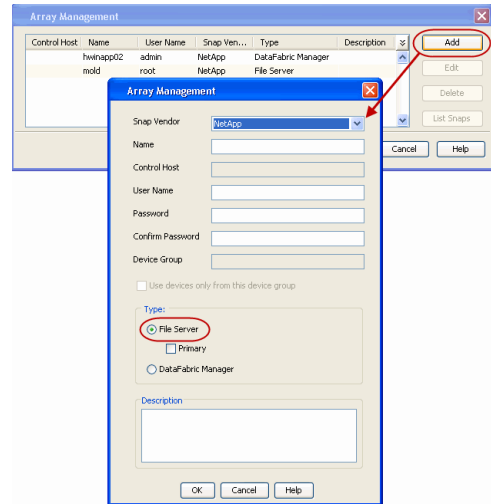
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

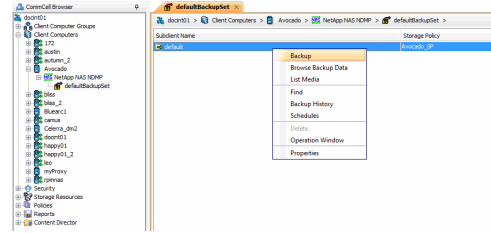
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.



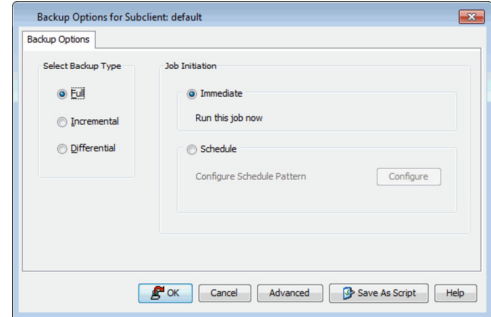
Getting Started - NAS iDataAgent Backup



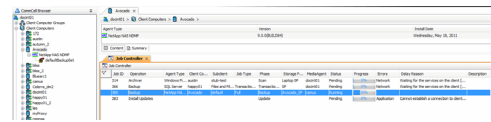
- From the CommCell Console, navigate to **<Client> | <File Server> NAS NDMP | defaultBackupSet**.
 - Right-click the **Subclient** and click **Backup**.



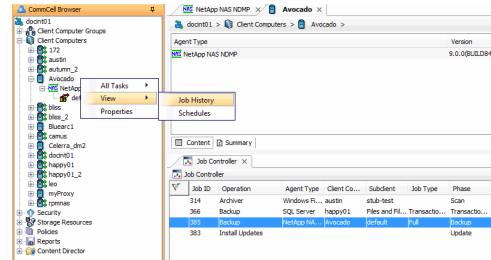
- Select **Full** as backup type.
If you are backing up vFiler data and the physical file server (where the vFiler resides) has not been specified in Array Management, click **Advanced**. From the **Advanced Backup Options** dialog box, click the **Skip Catalog phase for SnapProtect** option as indexing is not supported for vFiler backups.
 - Click **OK**.



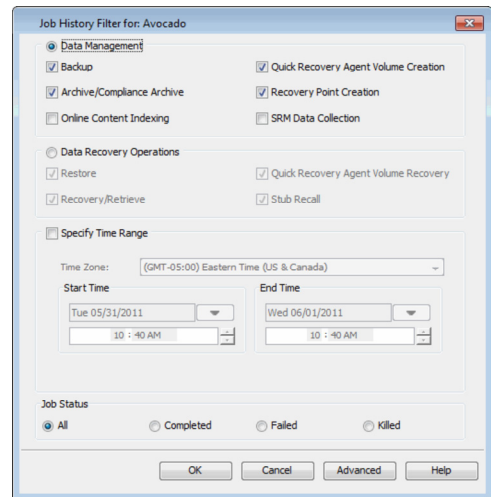
- You can track the progress of the job from the **Job Controller** window.



- Once job is complete, view the details of job from the **Job History**. Right-click the client computer, click **View | Job History**.

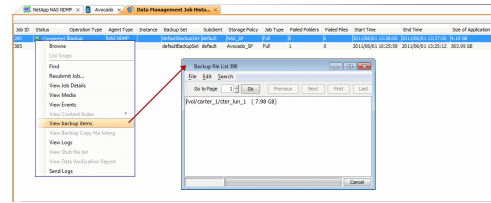


- Click **OK**.



- 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.



◀ Previous Next ▶

Getting Started - Vault/Mirror Copy

◀ Previous Next ▶

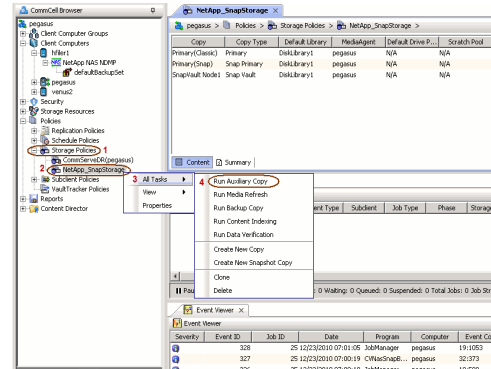
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

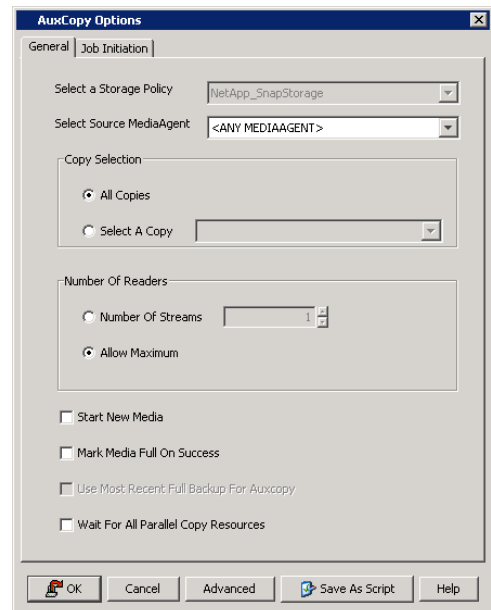
INITIATE VAULT/MIRROR COPY

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**.

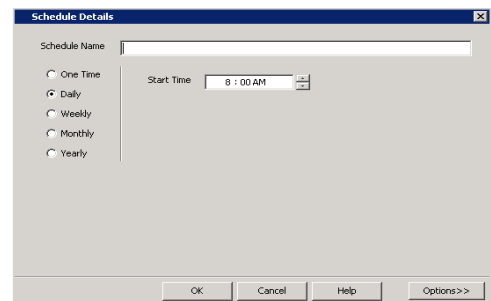


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

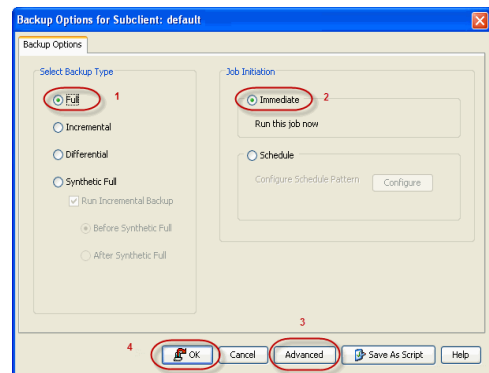
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

INLINE BACKUP COPY

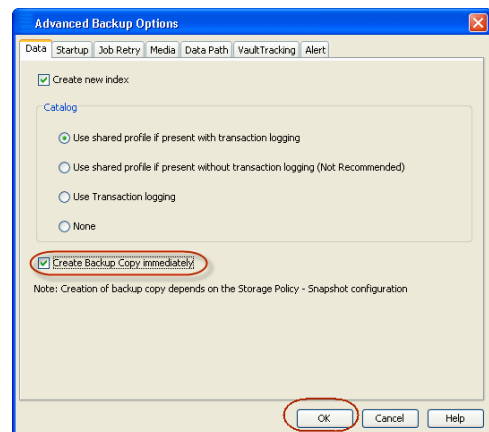
Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect 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**.

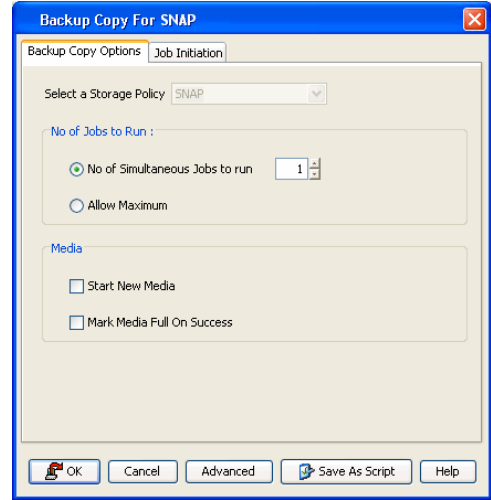
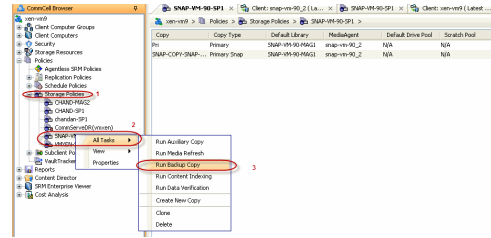


OFFLINE BACKUP COPY

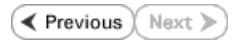
Backup copy operations performed independent of the SnapProtect backup job are known as offline backup copy.

- 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 - NAS Restore

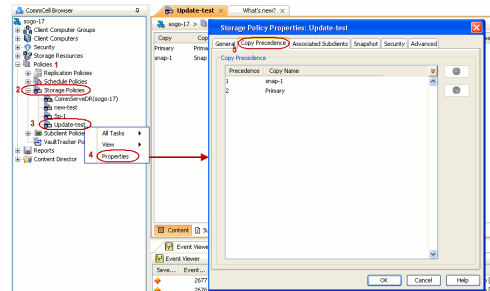


PERFORM A RESTORE

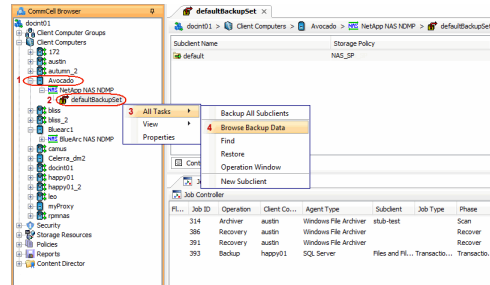
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

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.

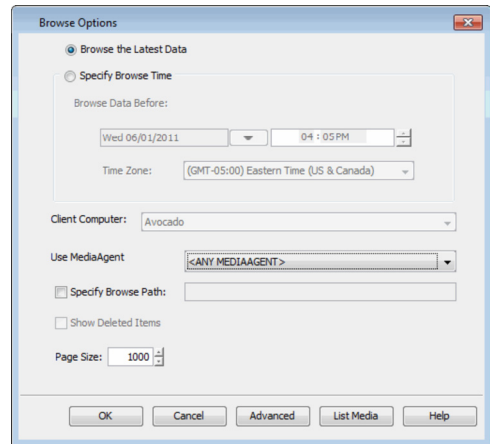
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - Select the backup copy and set the copy precedence as 1.
 - Click **OK**.



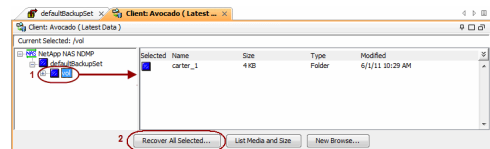
- From the CommCell Console, navigate to **<Client> | <File Server> NAS NDMP**.
 - Right-click the backup set and click **All Tasks | Browse Backup Data**.



- Click **OK**.

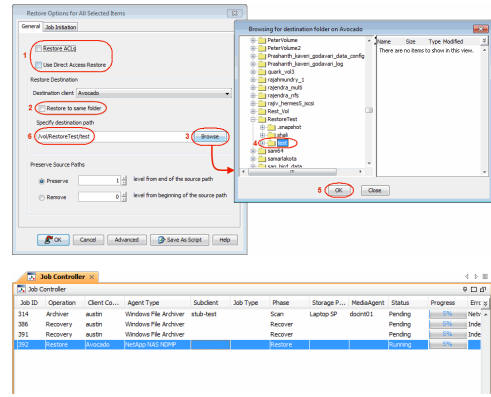


- Expand the backup set node in the left pane. Select the volume containing the data you want to restore.
 - Click **Recover All Selected**.



- 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.

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**.

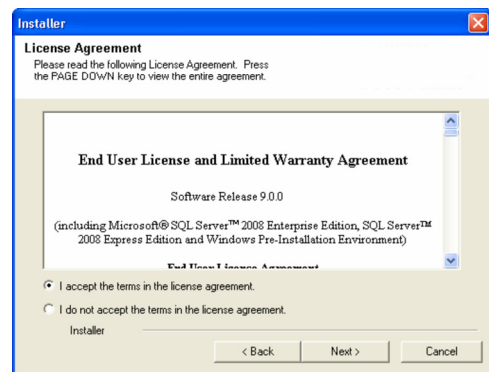
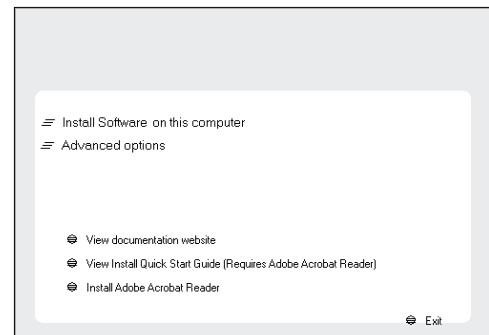
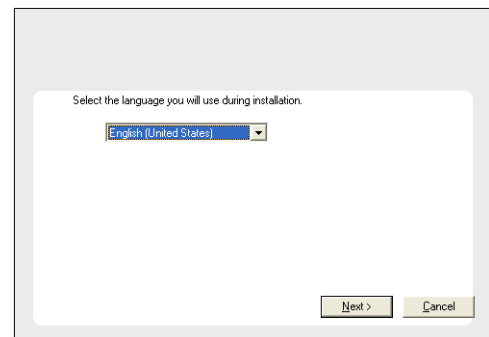
BEFORE YOU BEGIN

Download Software Packages

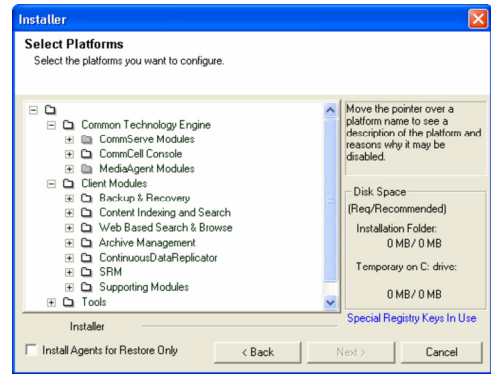
Download the latest software package to perform the install.

SnapProtect Support - Platforms

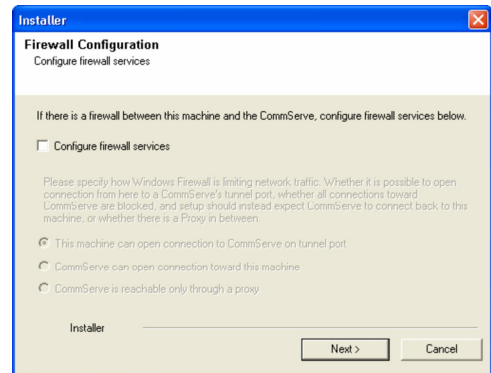
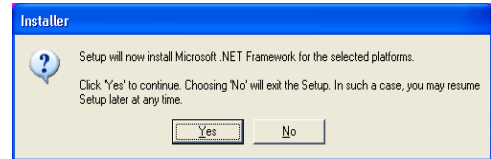
Make sure that the computer in which you wish to install the software satisfies the minimum requirements.



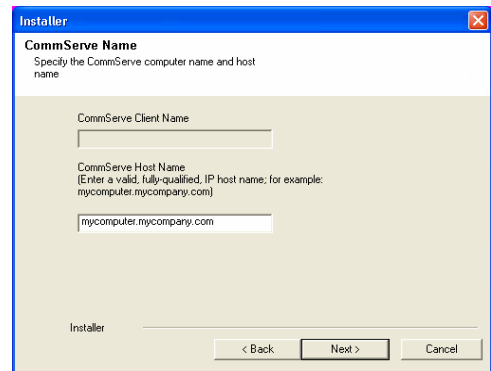
6. Click **YES** to install Microsoft .NET Framework package.
 - This prompt is displayed only when Microsoft .NET Framework is not installed.
 - Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.
7. 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**.



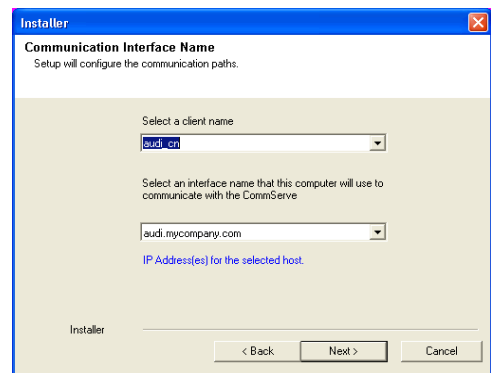
8. Enter the fully qualified domain name of the **CommServe Host Name**.
 Click **Next**.
 Do not use space and the following characters when specifying a new name for the CommServe Host Name:
`\ | ` ~ ! @ # $ % ^ & * () + = < > / ? , [] { } ; ' " ' "`



9. Click **Next**.



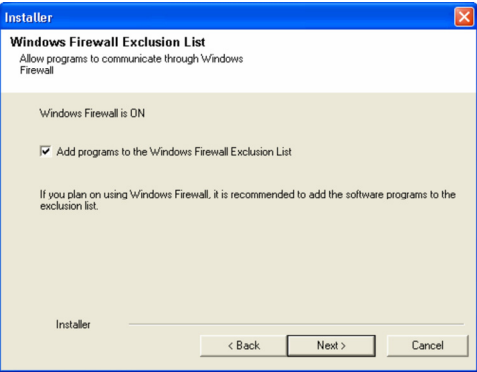
10. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.



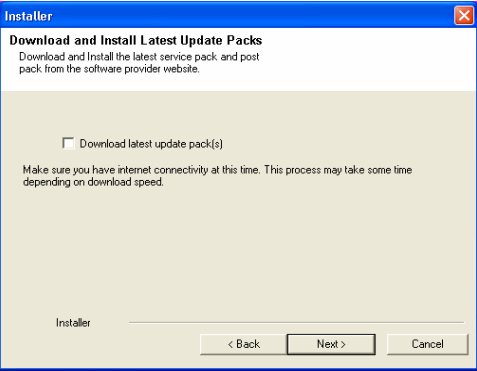
Click **Next**.

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.

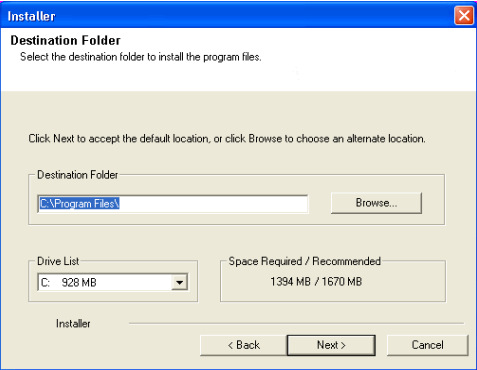
Click **Browse** to change the default location.

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:

/ : * ? " < > | #

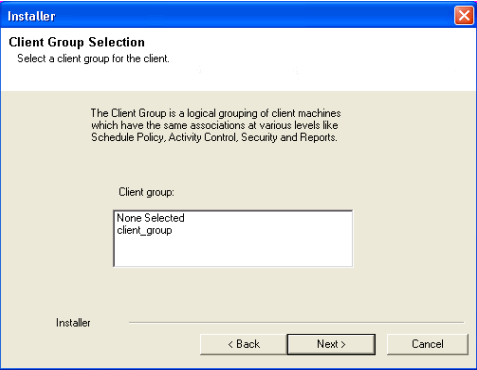
It is recommended that you use alphanumeric characters only.



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**.

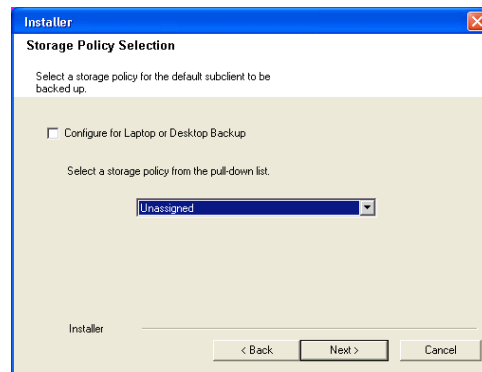
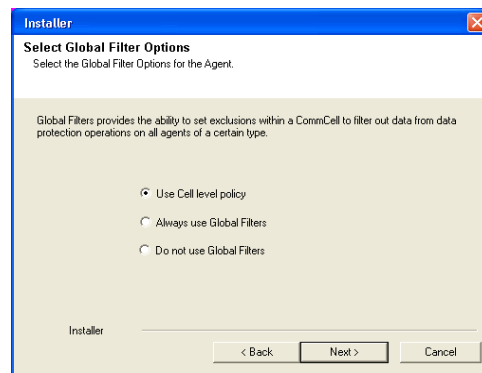
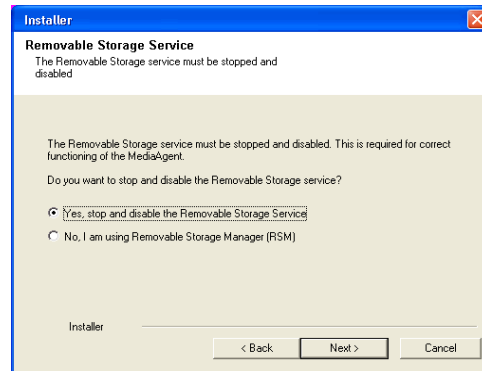
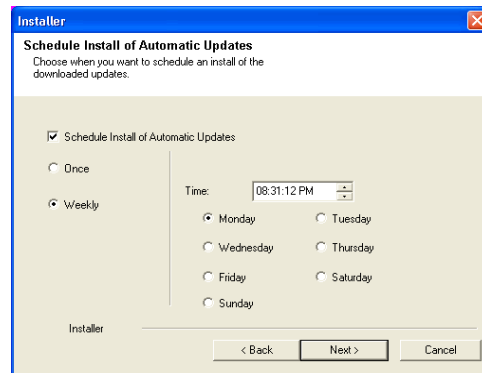
15. Select **Yes** to stop Removable Storage Services on the MediaAgent.
Click **Next**.

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

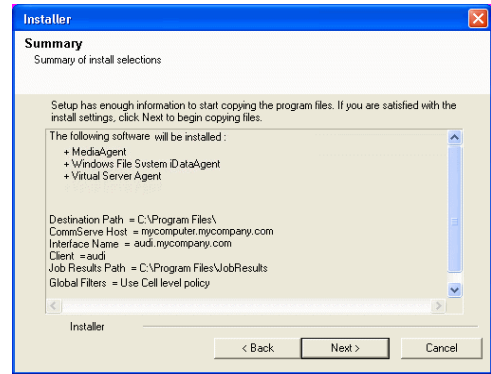
16. Click **Next**.

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

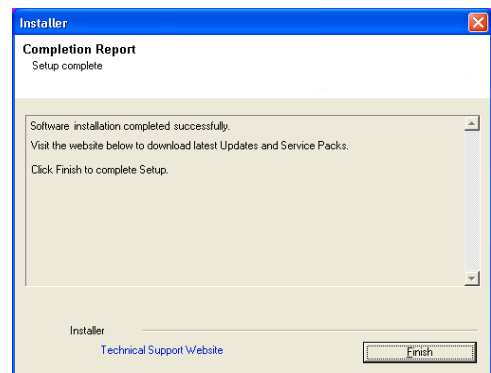
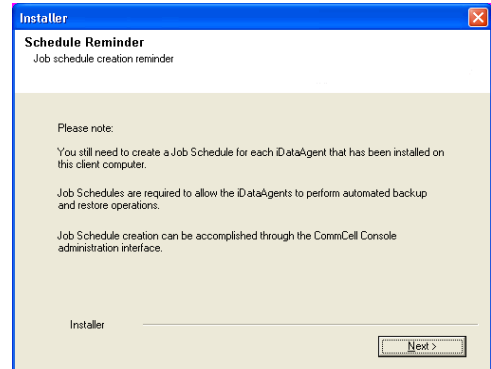
18. Click **Next**.



19. Click **Next**.



20. Click **Finish**.



Getting Started - Microsoft Hyper-V Configuration

CONFIGURATION

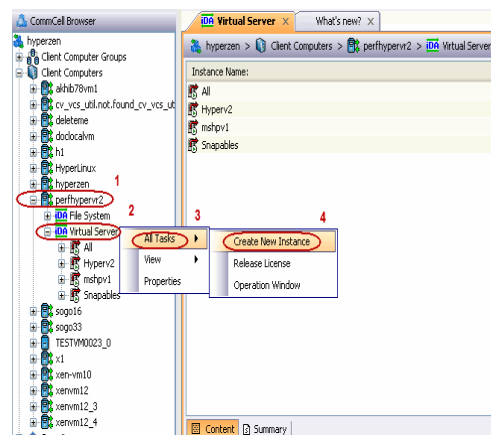
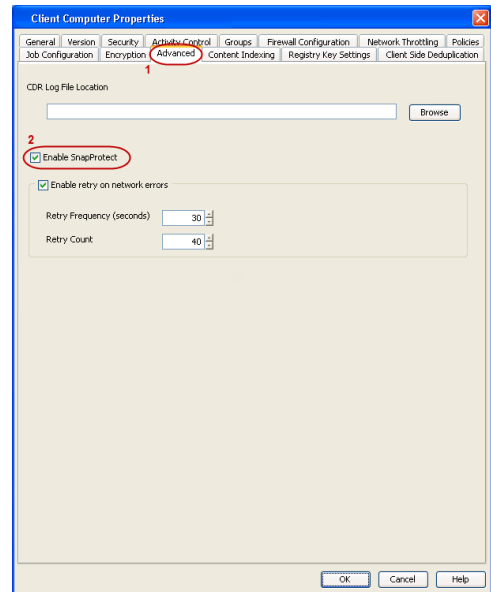
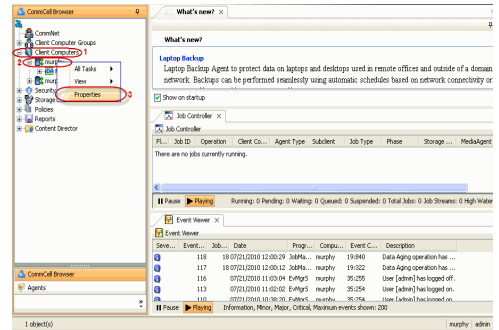
Once the Virtual Server *iDataAgent* has been installed, configure an Instance, a Backup Set and a Subclient to facilitate backups. The following sections provide the necessary steps required to create and configure these components for a first SnapProtect backup of a single virtual machine.

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

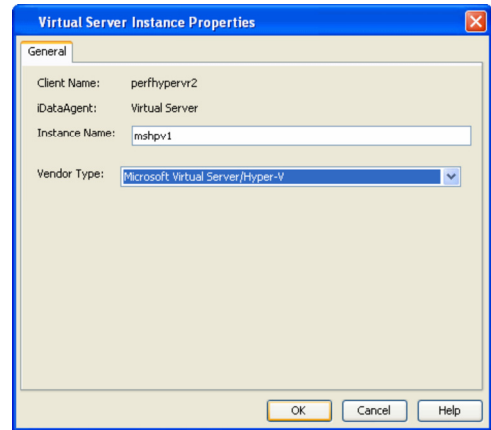
2.
 - Click on the **Advanced** tab.
 - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
 - Click **OK**.

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

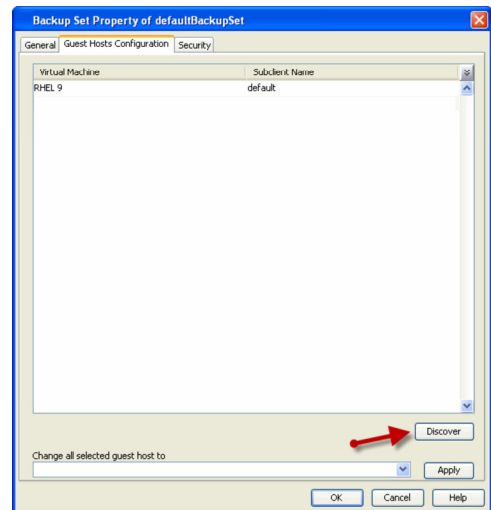
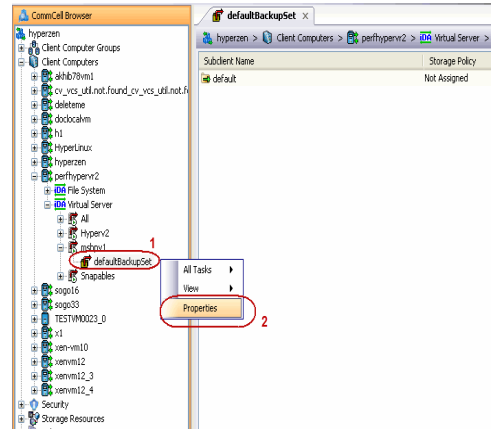
4.
 - Enter the **Instance Name**.
 - Select **Microsoft Virtual Server/Hyper-V** from **Vendor Type** menu.
 - Click **OK**.



5.
 - From the CommCell Browser, right-click the **Default Backup Set**.
 - Click **Properties**.

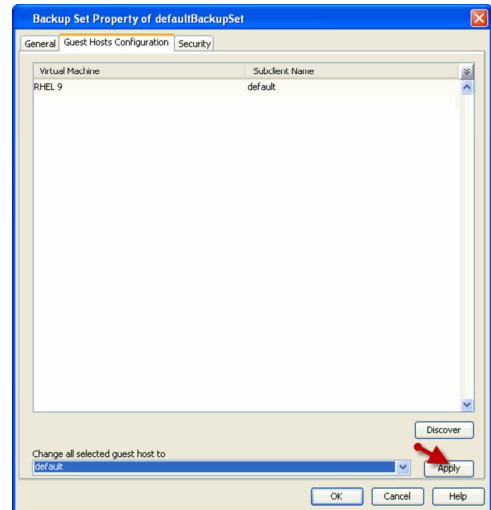


6. Click **Discover**, on the **Guest Hosts Configuration** tab. Discovery process might take several minutes to complete.

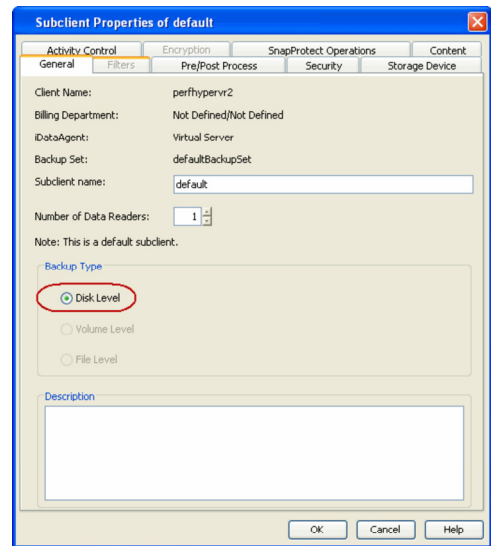
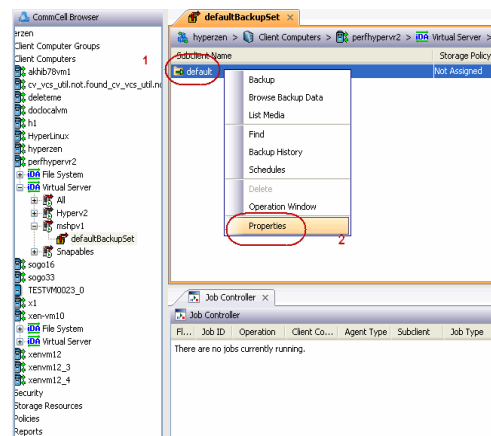


7.
 - Select the default subclient from **Change all selected guest hosts to**.
 - Click **Apply**.
 - Click **OK**.

8.
 - From the CommCell Browser, navigate to the default subclient.
 - Click **Properties**.



9. Ensure **Disk-Level** from **Backup Type** is selected.



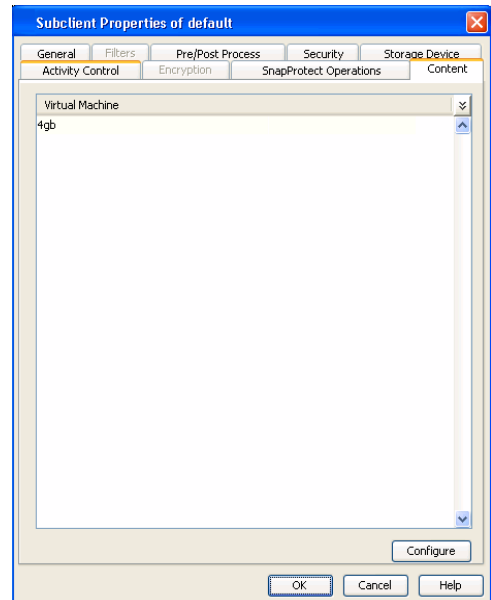
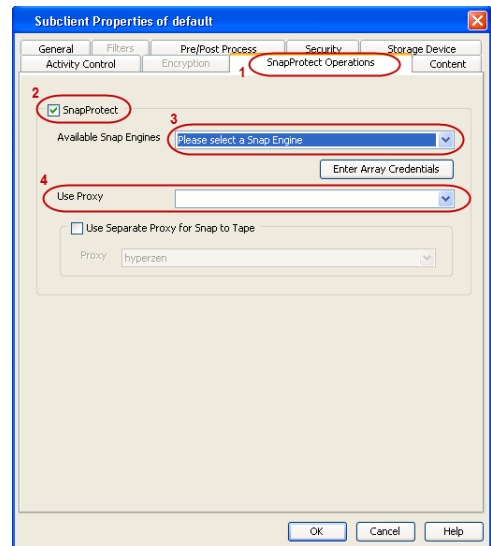
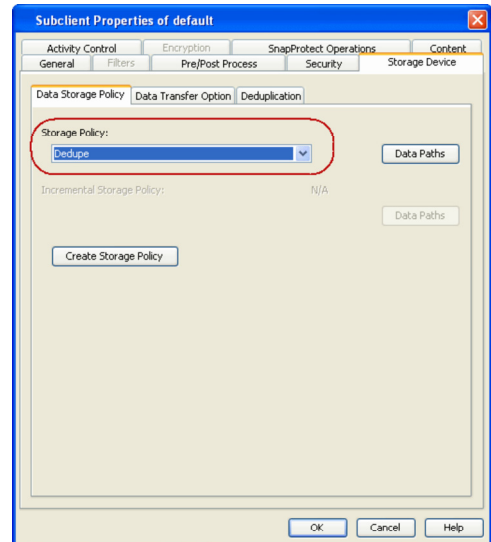
10.
 - Click the **Storage Device** tab.
 - In the **Storage Policy** box, select the storage policy name.

- 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.

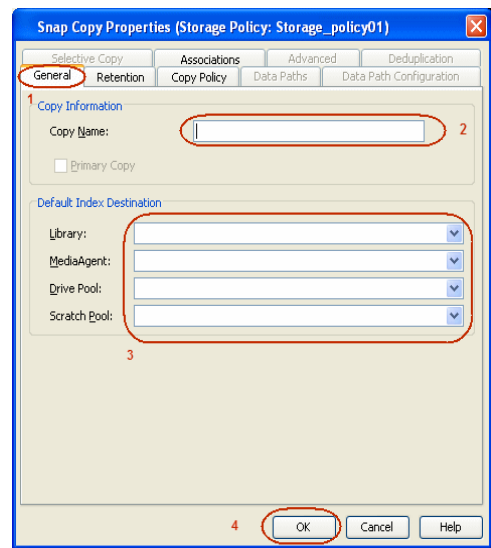
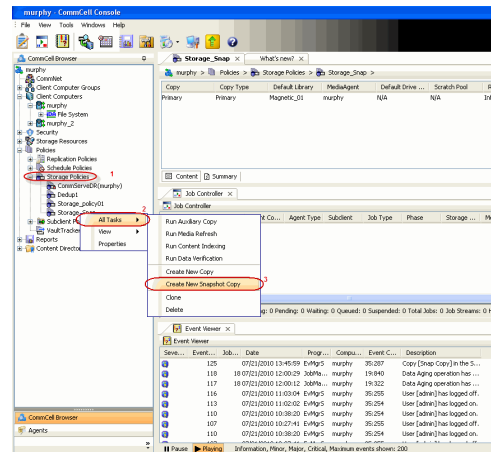
Click **Next** ➤ to Continue.

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.

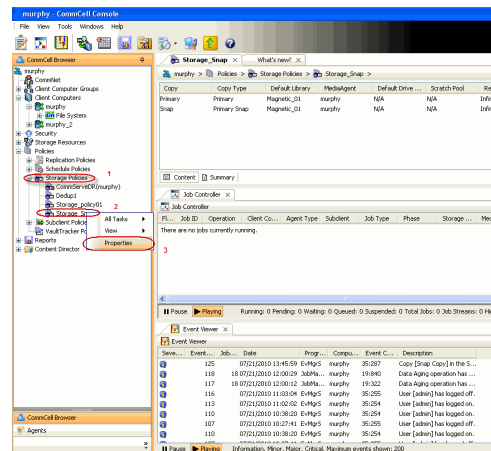
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks | Create New Snapshot Copy**.
- Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



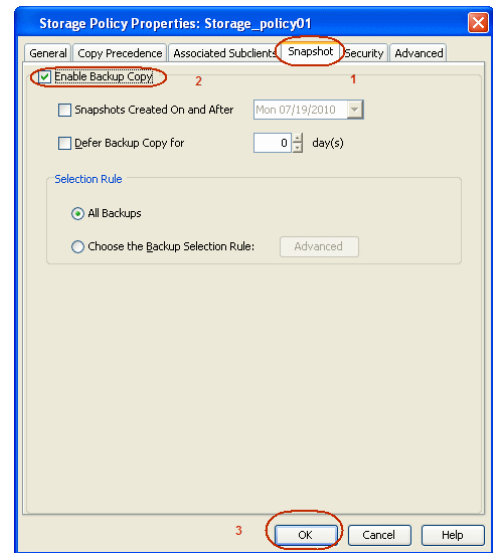
CONFIGURE BACKUP COPY

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**.
- 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

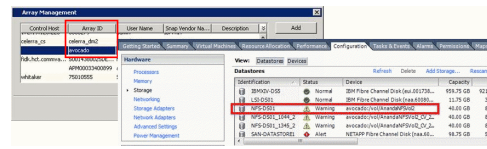
LICENSES

- 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.

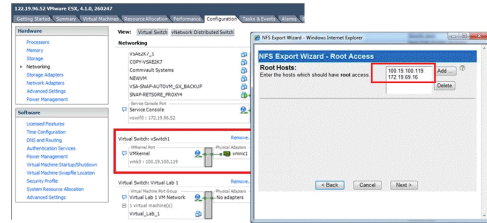
ADDITIONAL REQUIREMENTS FOR VMWARE

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.



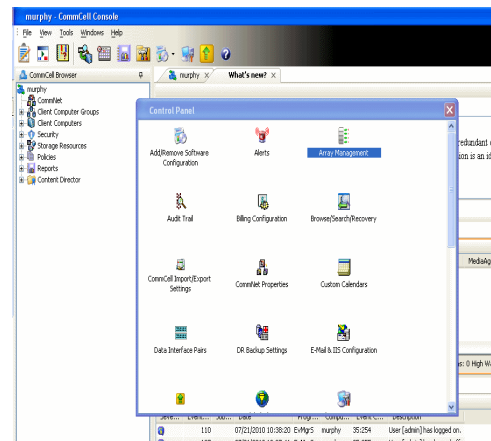
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



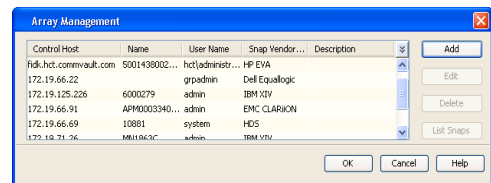
SETUP THE ARRAY INFORMATION

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: [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

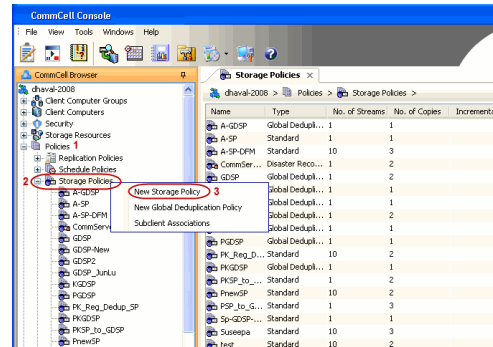
CONFIGURATION

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

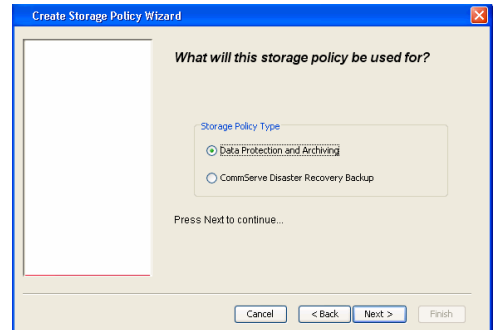
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

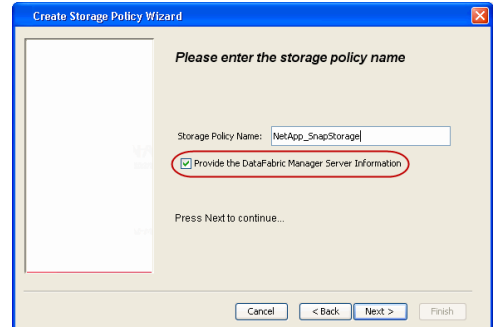
1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



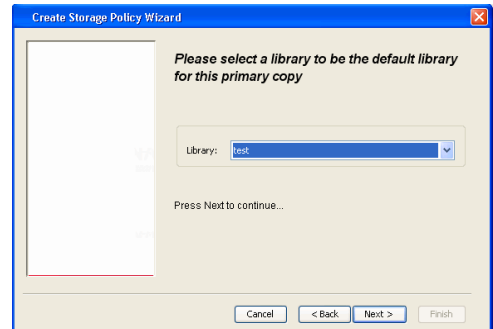
3.
 - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



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

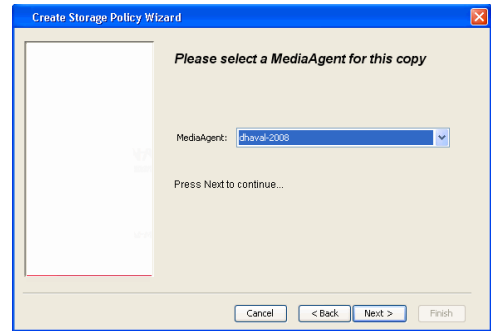
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

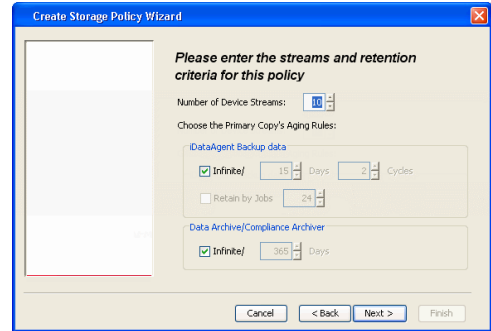


5.
 - Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

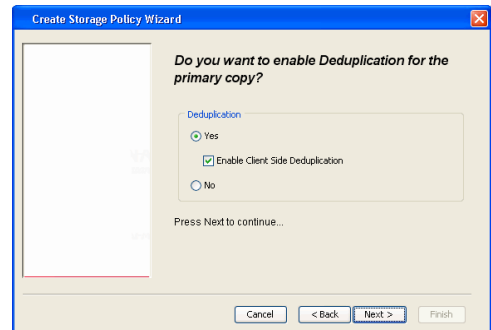
6. Click **Next**.



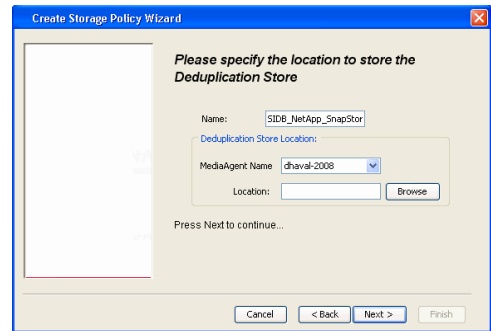
7. Click **Next**.



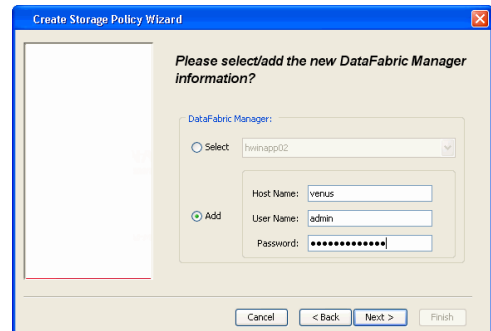
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

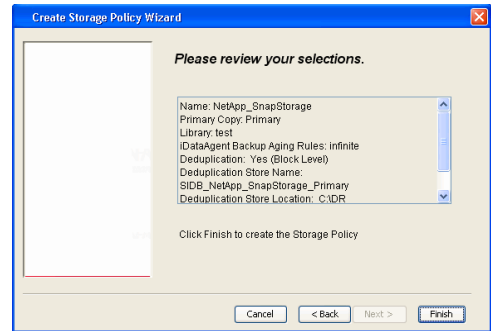


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



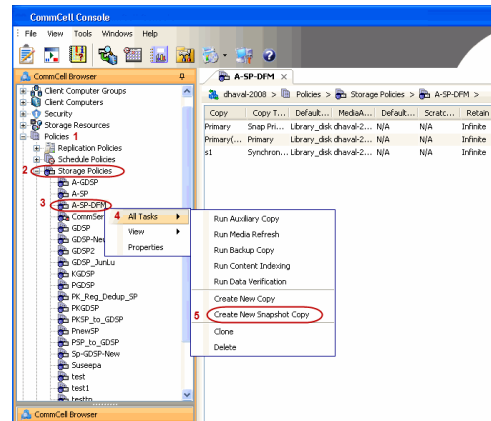


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

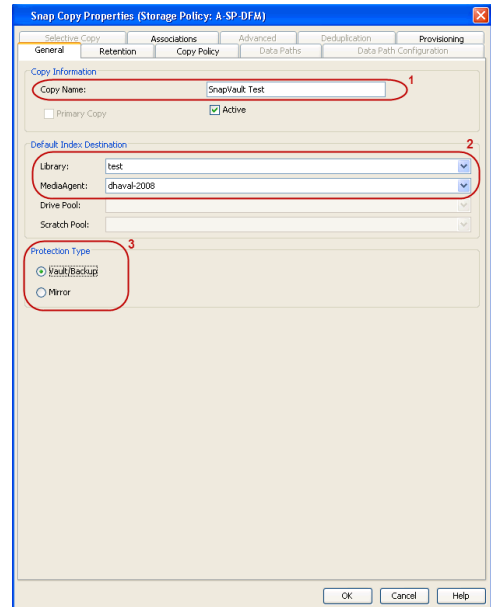
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

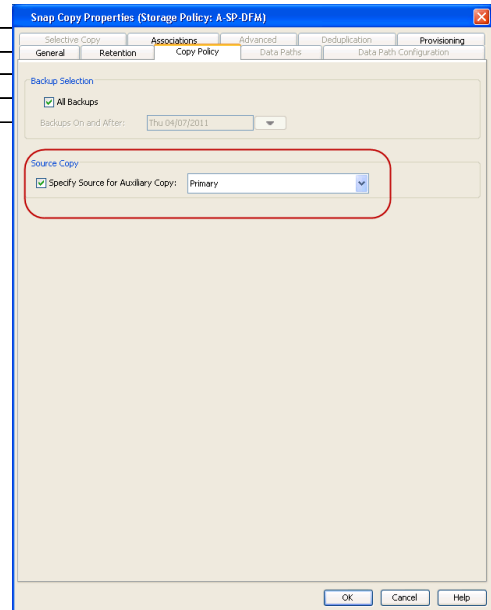


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

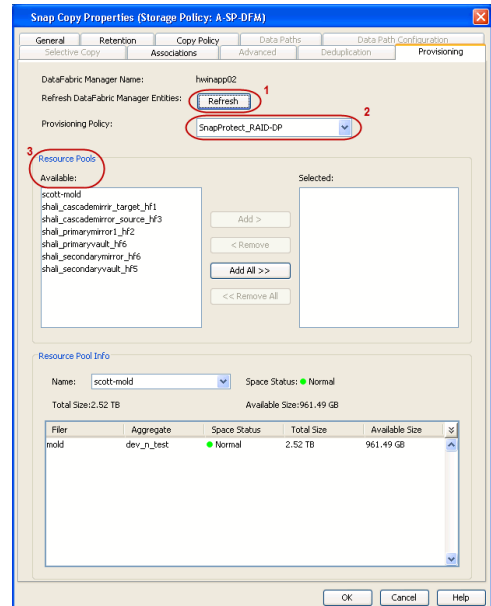
TOPOLOGY	SOURCE COPY
----------	-------------

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.

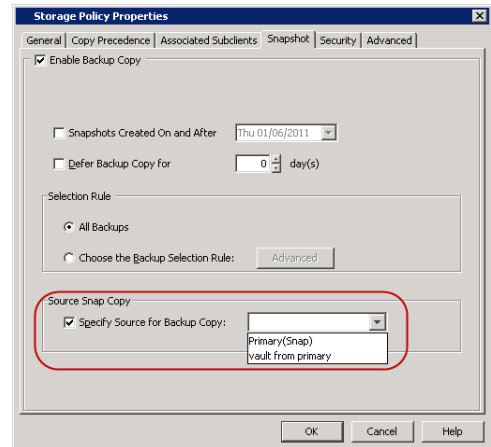
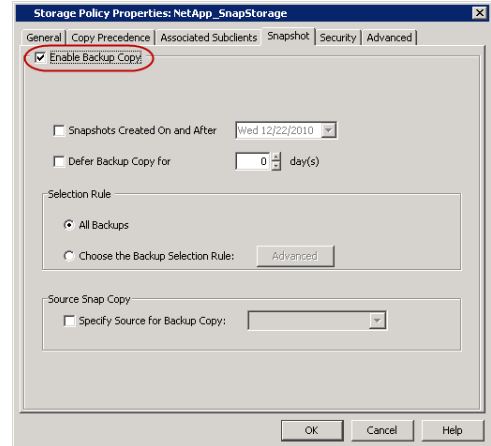
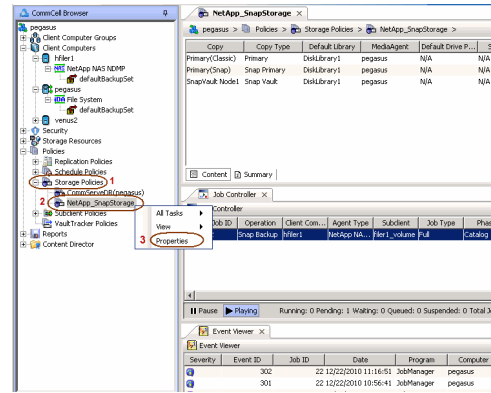
CONFIGURE BACKUP COPY

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.

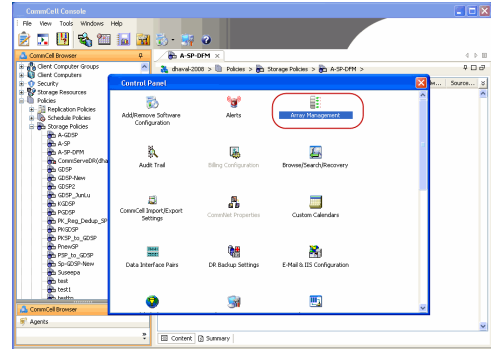


SETUP THE ARRAY INFORMATION

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**.

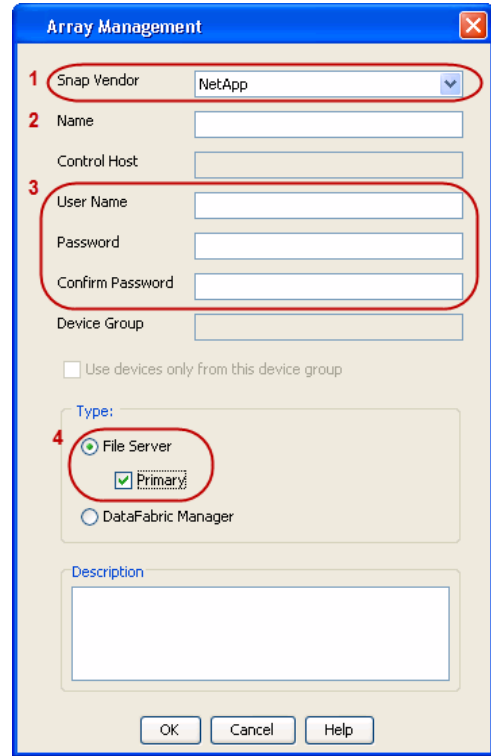
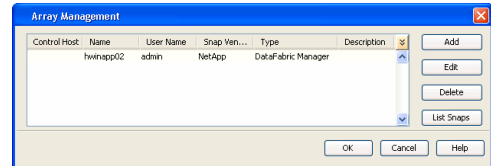


3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

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.

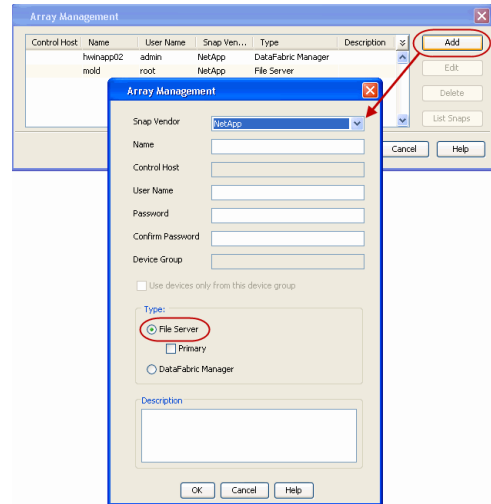
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

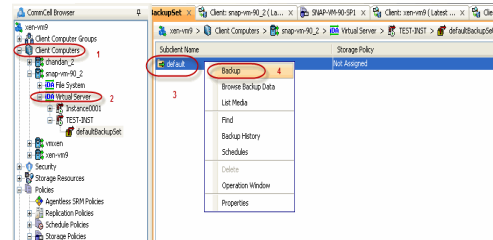
Getting Started - Microsoft Hyper-V Backup

PERFORM A BACKUP

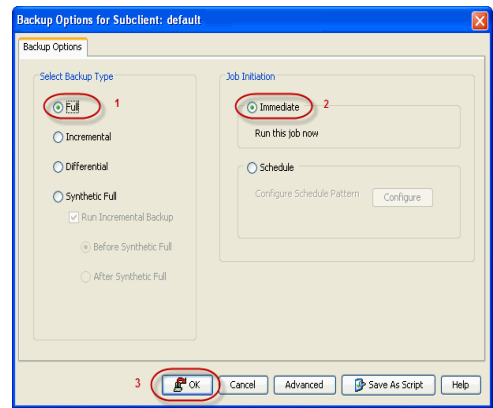
After configuring the Instance, BackupSet, and Subclient you are ready to perform your first backup.

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

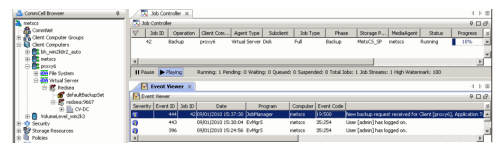
- From the CommCell Console, navigate to **Client Computers | Virtual Server**
 - Right-click the **Subclient** and click **Backup**.



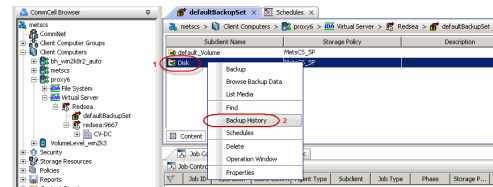
- Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.



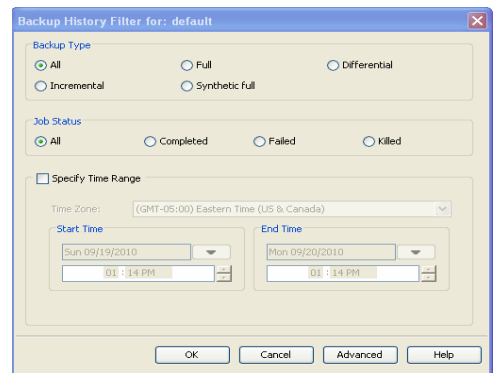
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



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

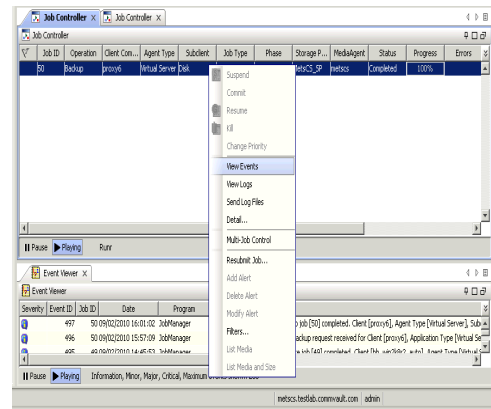


- Click **OK**.



- 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

◀ Previous Next ▶

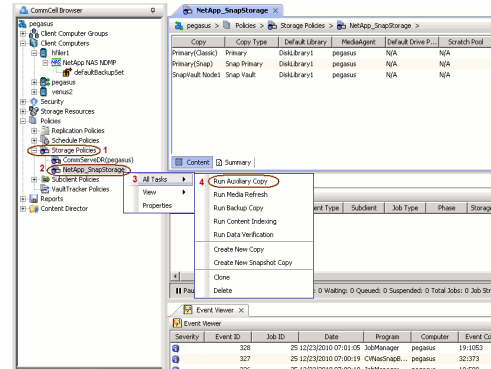
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

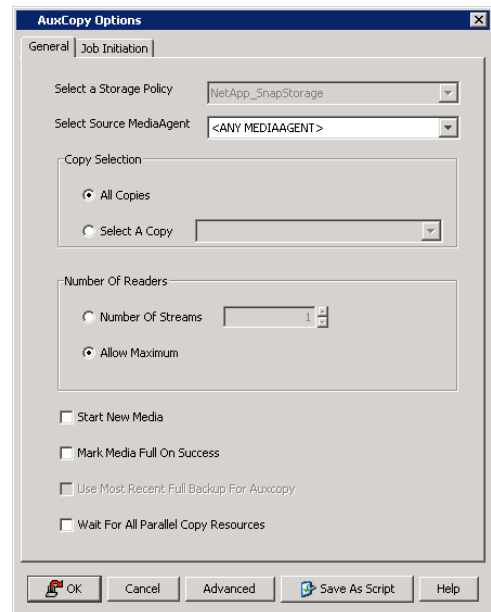
INITIATE VAULT/MIRROR COPY

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**.

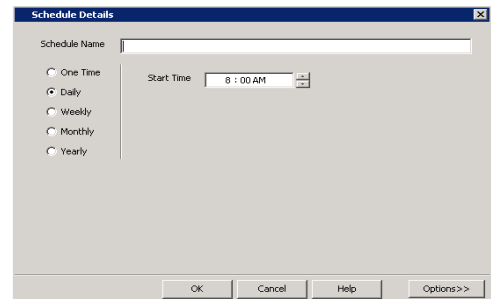


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

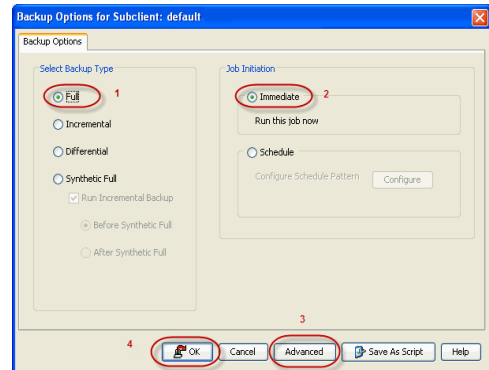
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

INLINE BACKUP COPY

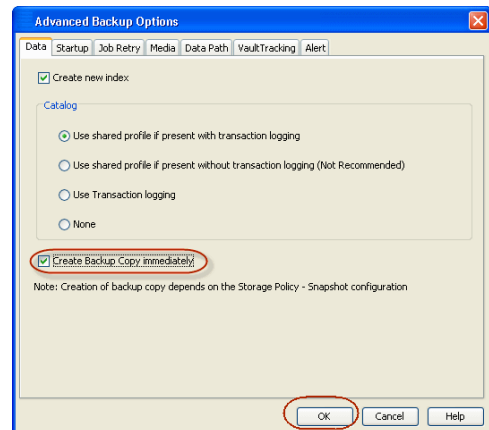
Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect 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**.



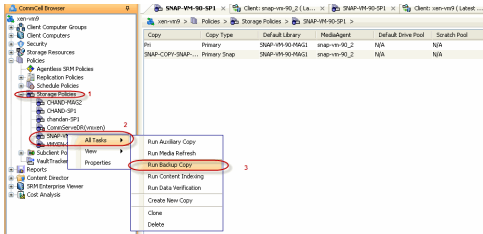
- Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



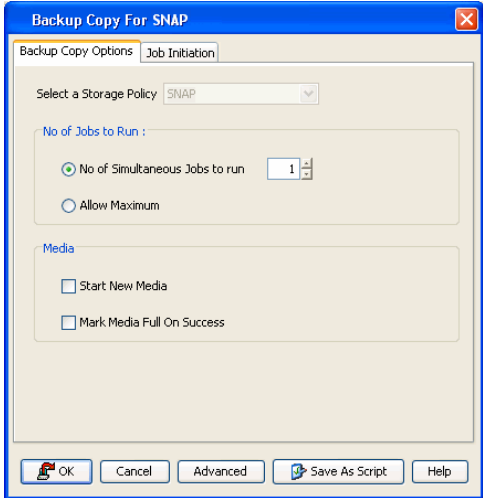
OFFLINE BACKUP COPY

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

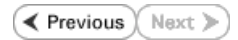
- From the CommCell Console, navigate to **Policies** | **Storage Policies**.
 - Right-click the **<storage policy>** and click **All Tasks** | **Run Backup Copy**.



2. Click **OK**.



Getting Started - Microsoft Hyper-V Restore



PERFORM A RESTORE

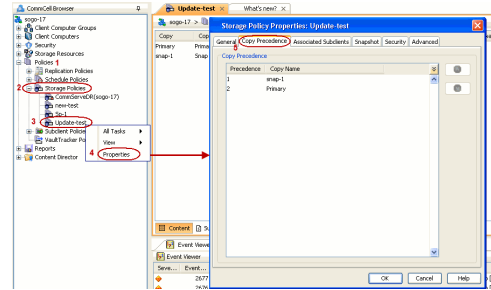
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections describe the steps involved in restoring a virtual machine.

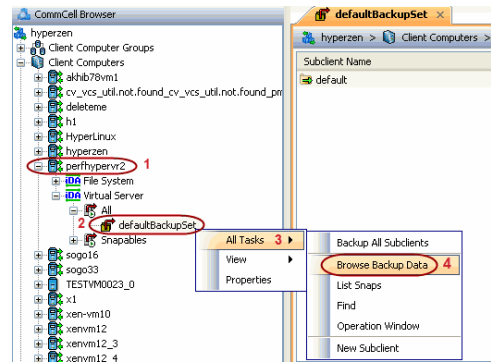
- From the CommCell Console, navigate to **Policies | Storage Policies**.
 - Right-click the **<storage policy>** and click **Properties**.
 - Click the **Copy Precedence** tab.
 - By default, the snapshot copy is set to 1 and is used for the operation.

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.

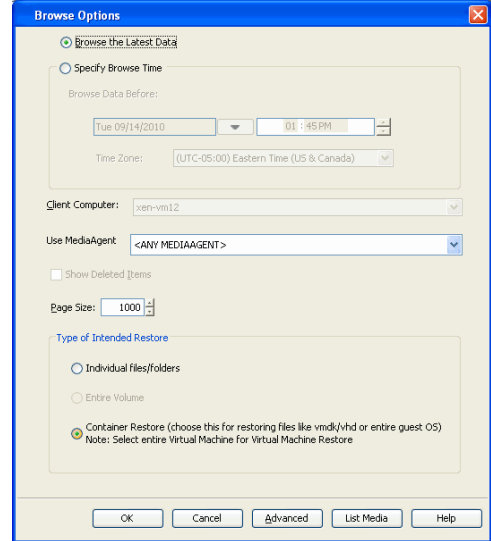
- Click **OK**.



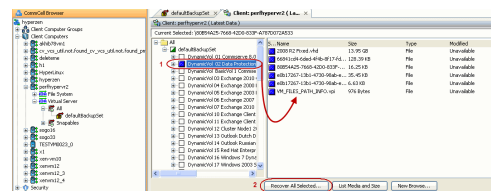
- From the CommCell Console, navigate to **<Client> | Virtual Server**.
 - Right-click the backup set that contains the data you want to restore and click **All Tasks | Browse Backup Data**.



- 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.

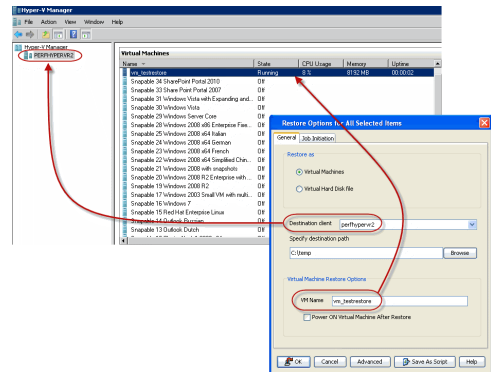
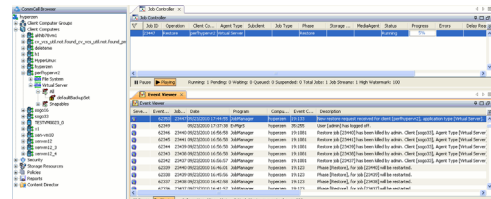
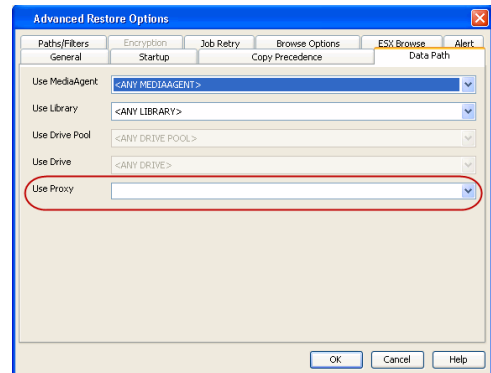
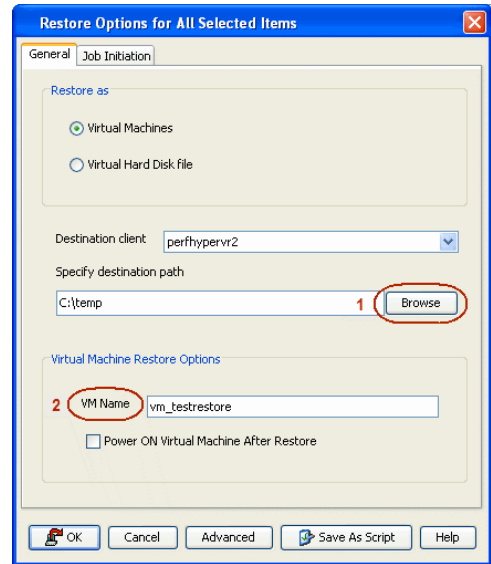
Ensure that you provide a fully qualified name for the virtual machine. Entering an IP address will cause the restore operation to fail.

- 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_semmns=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]

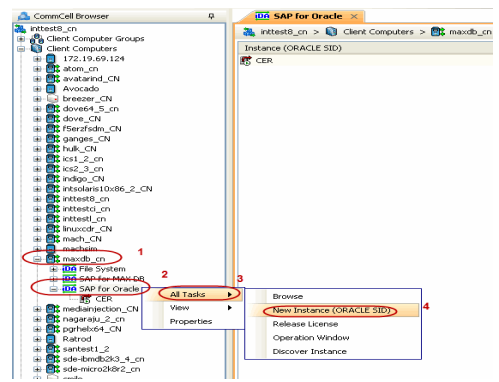
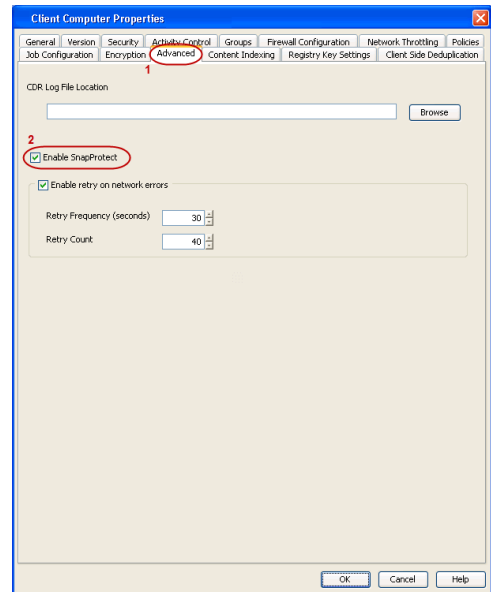
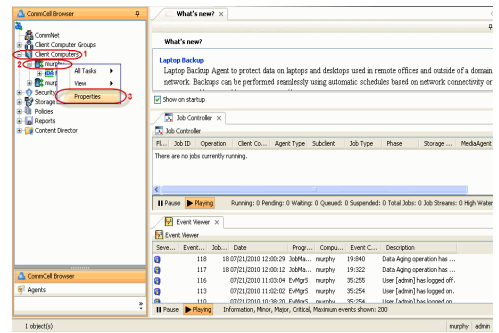


# Getting Started - SAP for Oracle Configuration

## 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.

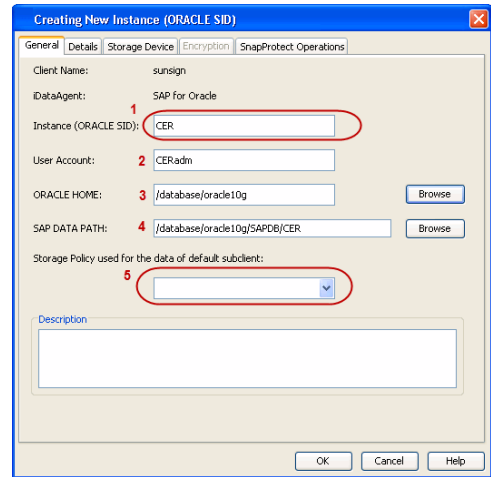
1.
  - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
  - Right-click the client and select **Properties**.
  
2.
  - Click on the **Advanced** tab.
  - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
  - Click **OK**.
  
3.
  - From 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.





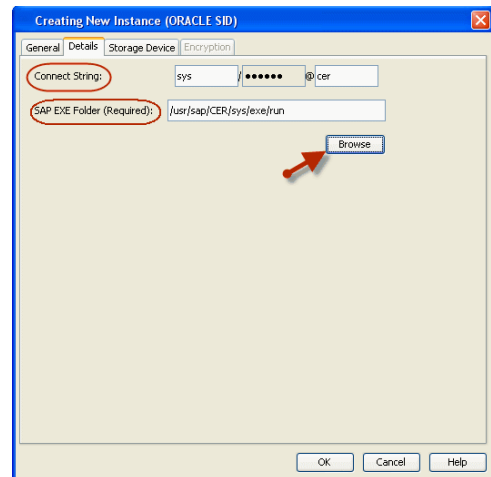
Make sure that the user has administrator privileges to access the Oracle application.

- **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.

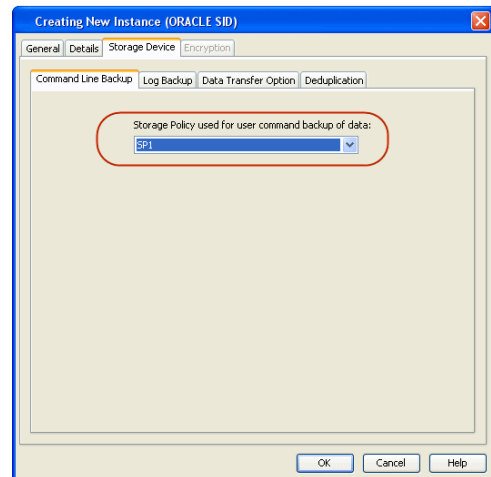


5. Click **Details** tab and add the following information:

- Enter the target database connect string in **Connect String**.
- **Browse** or enter the path to the SAP EXE folder in **SAP EXE Folder (Required)**.

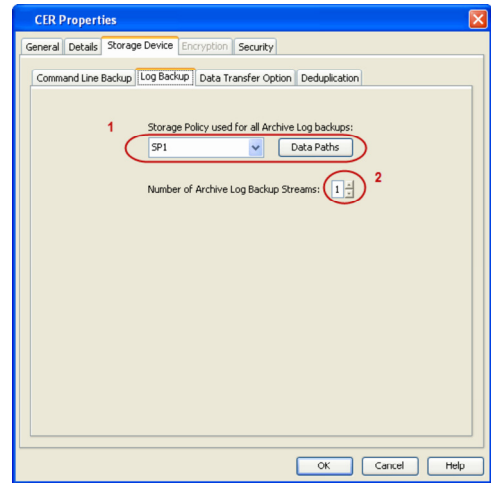


6. • Click **Storage Device** tab.  
 • Select a **Storage Policy used for user command backup of data** from the drop down list.

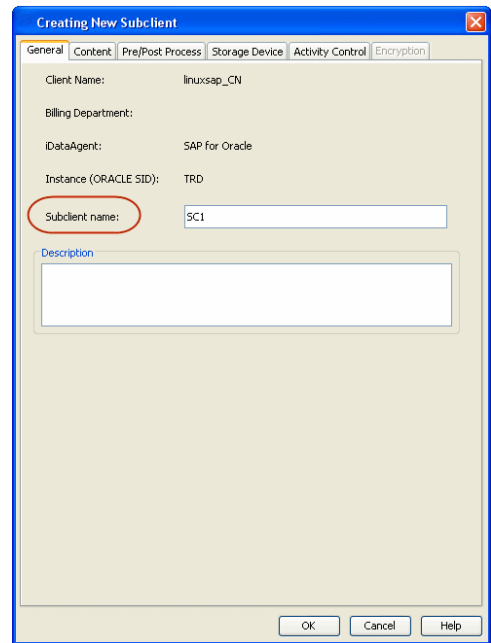
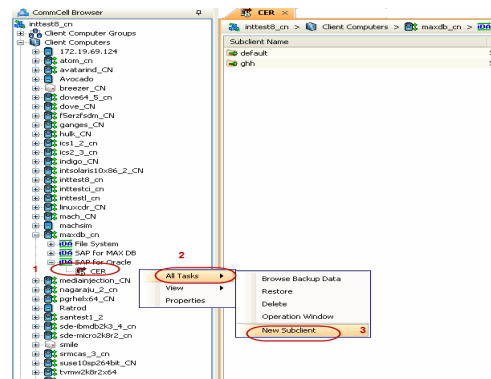


7. • Click **Log Backup** tab.  
 • Select a **Storage Policy used for all Archive Log backups** from the drop down list.  
 • Click **OK**.

8.
  - From the CommCell Browser, navigate to **<Client> | SAP for Oracle**.
  - Right-click the **<Instance>** and click **All Tasks | New Subclient**.



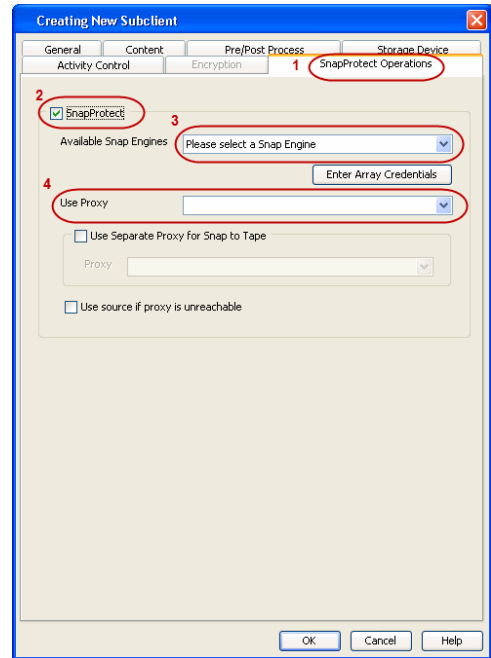
9. In the **Subclient Name** field, type a name.



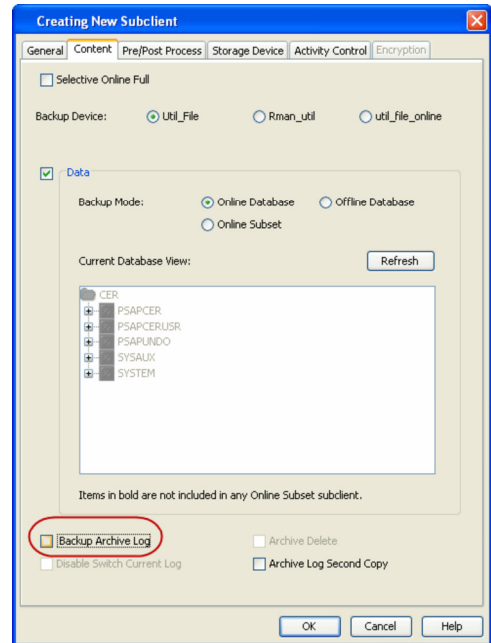
10.
  - Click the **SnapProtect Operations** tab.
  - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
  - Select the storage array from the **Available Snap Engine** drop-down list.
  - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup 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.

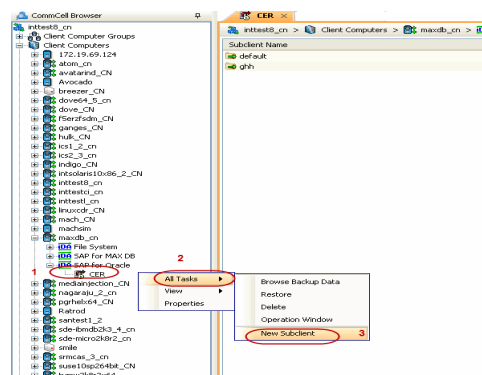
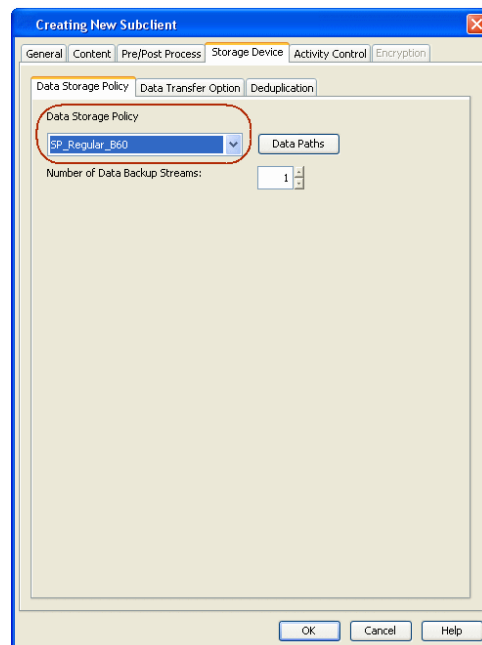


11. Click the **Content** tab and clear the check box for **Backup Archive Log**.

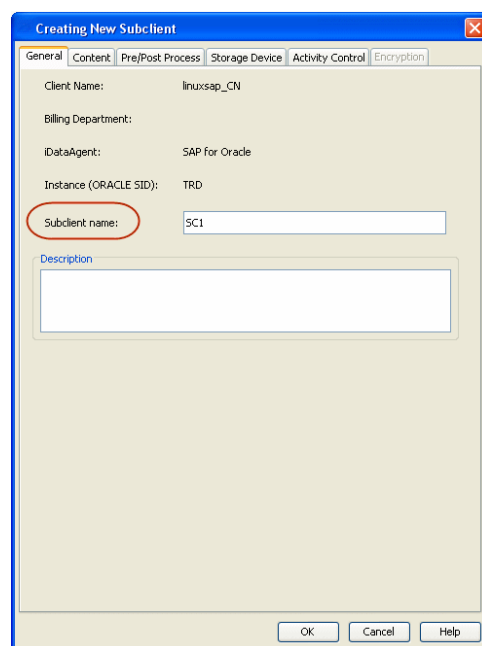


12.
  - Click the **Storage Device** tab.
  - Select a **Data Storage Policy** from the drop down list.
  - Click **OK**.

13.
  - From the CommCell Browser, navigate to **<Client> | SAP for Oracle**.
  - Right-click the **<Instance>** and click **All Tasks | New Subclient**.

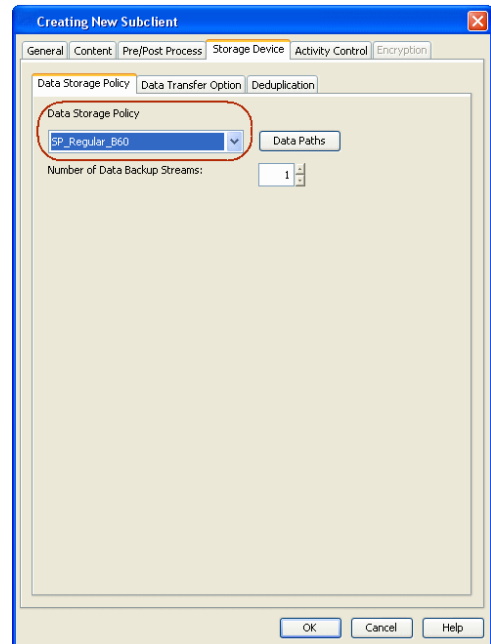
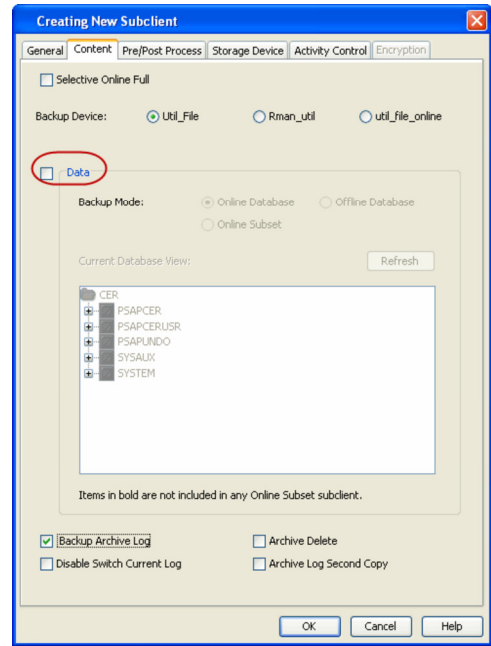


14. In the **Subclient Name** field, type a name.



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.

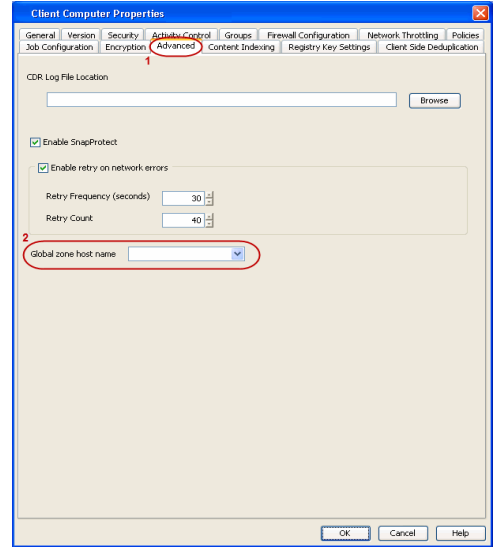
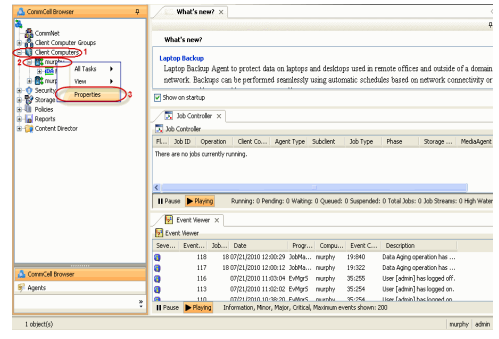
## ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE

**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.

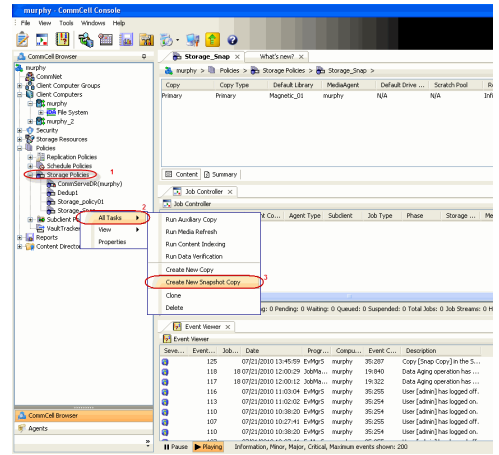
Click **Next** to Continue.

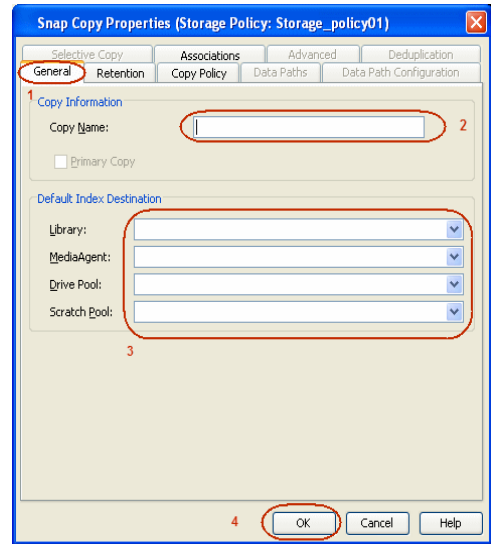
## CREATE A SNAPSHOT COPY



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**.

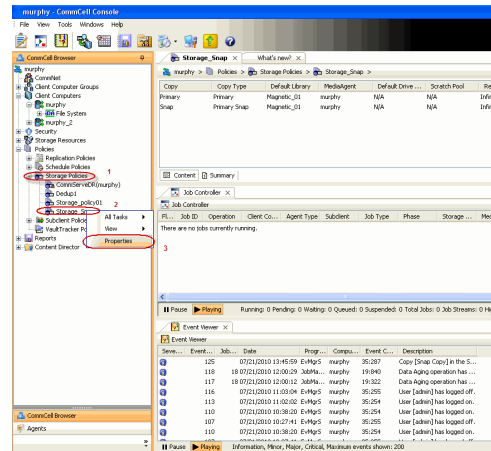




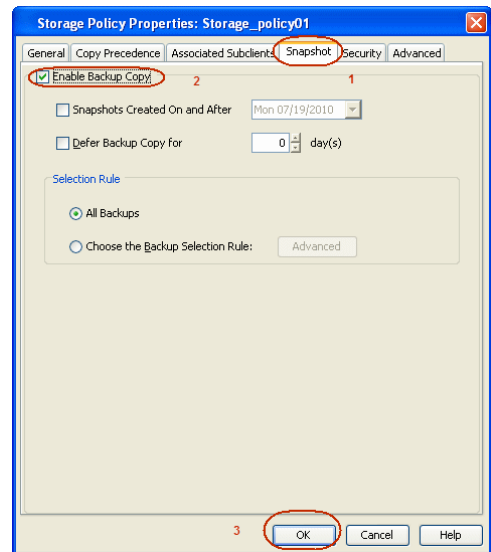
## CONFIGURE BACKUP COPY

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

◀ Previous Next ▶

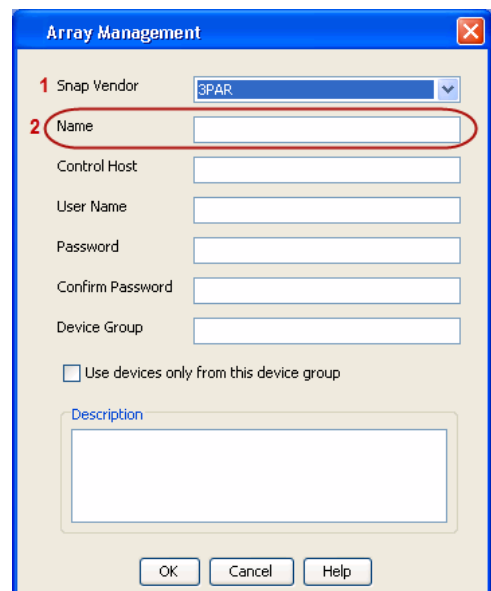
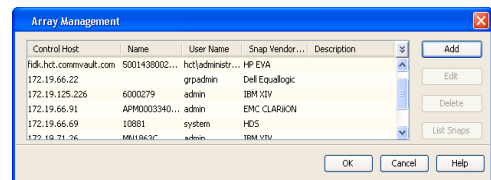
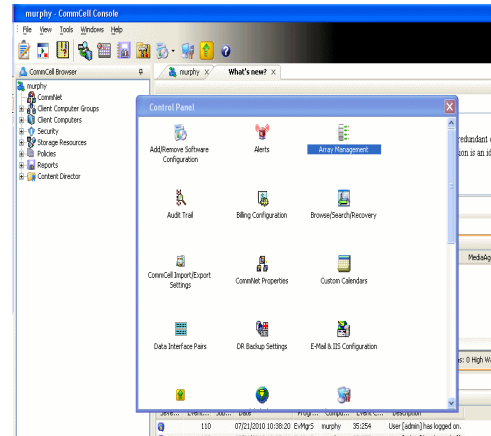
## PRE-REQUISITES

- 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

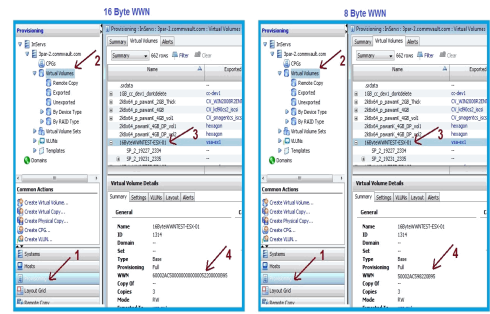
where  $\text{DevID.substr}(26,6)$  is the next 6 digits after the twenty sixth digit from the WWN number

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

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

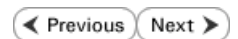
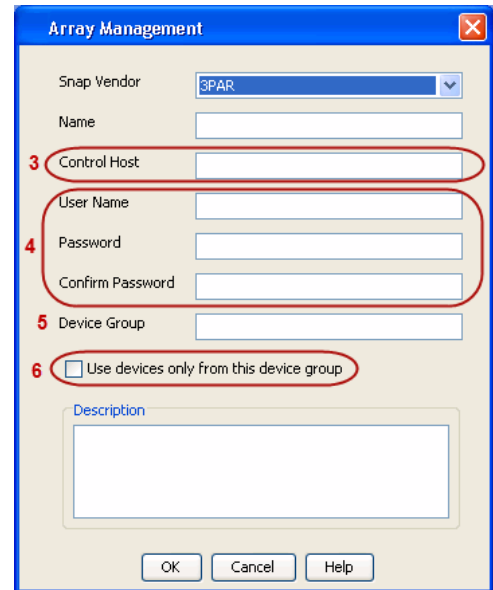
$\text{DevID.substr}(4,3)$  is 2AC and  $\text{DevID.substr}(26,6)$  is 000B95

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



4.

- 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

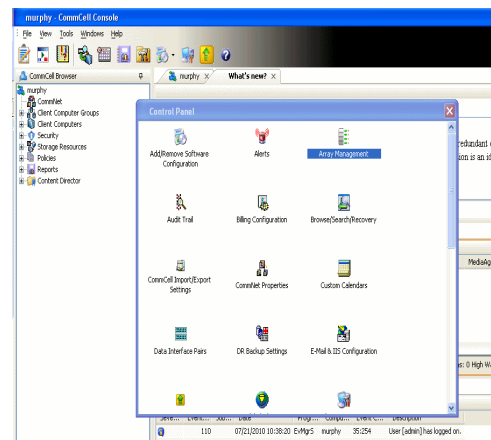
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
  - Create a new group administration account in the firmware, and set the desired permissions for this account.
  - If you plan to use the existing 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.

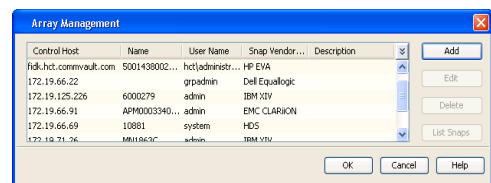
## SETUP THE ARRAY INFORMATION

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**.

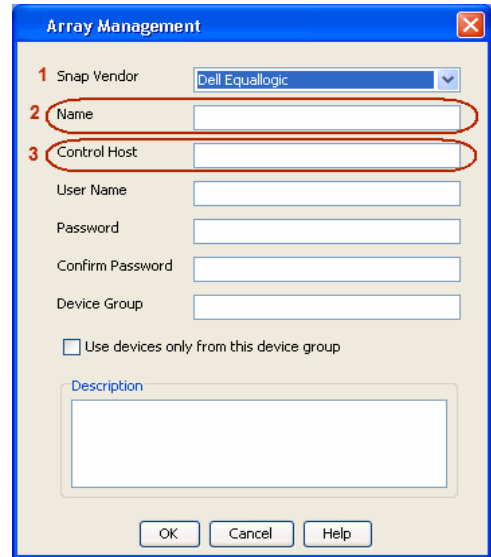


2. Click **Add**.

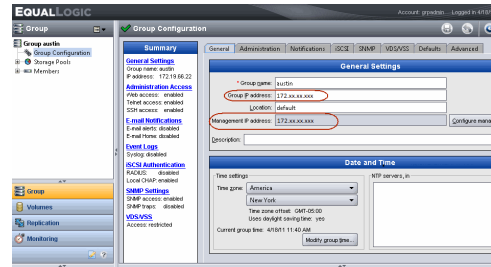


3.
  - Select **Dell Equallogic** from the **Snap Vendor** list.
  - Specify the Management IP address in the **Name** field.
 

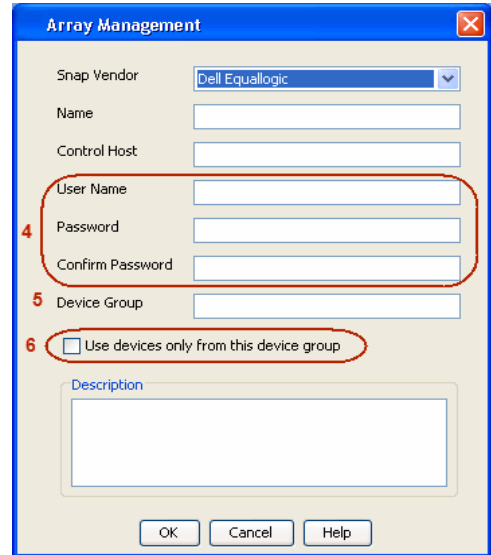
No entry is required in the **Name** field if there is no Management IP address configured.
  - Specify the Group IP address in the **Control Host** field.



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:

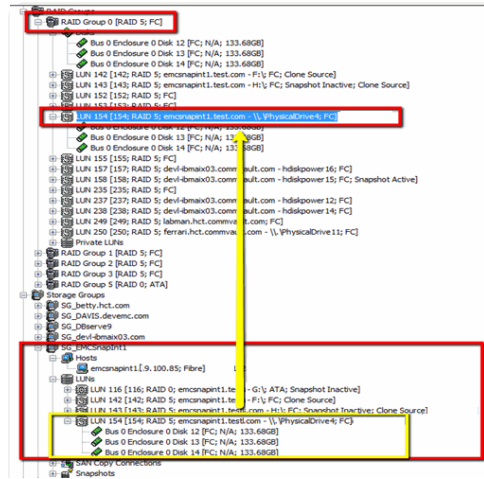
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

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.

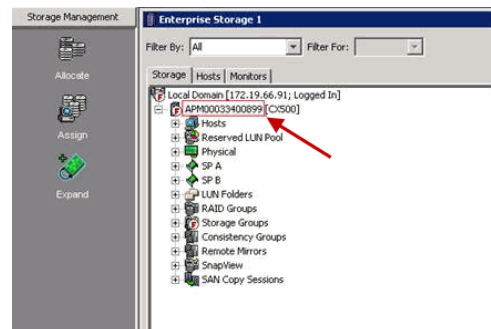
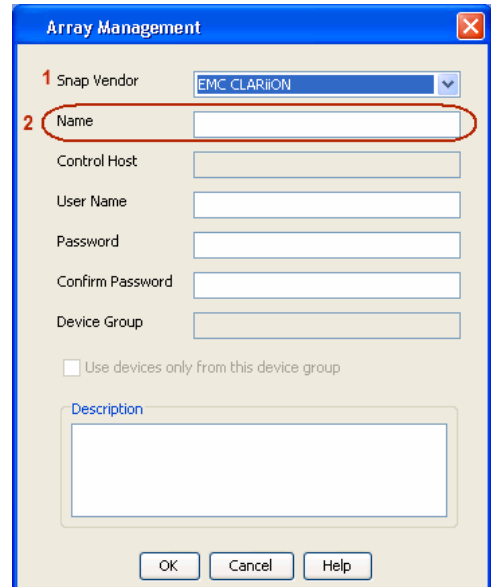
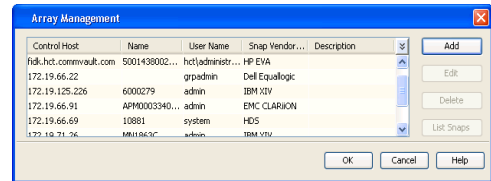
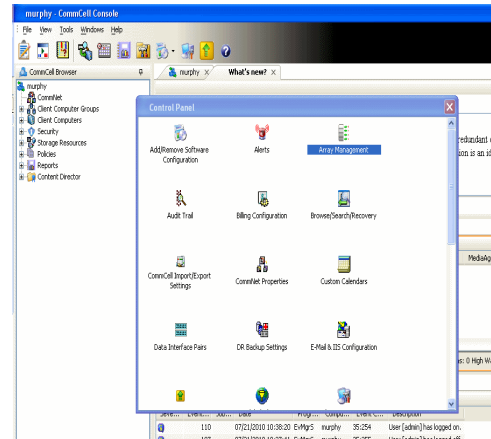
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

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

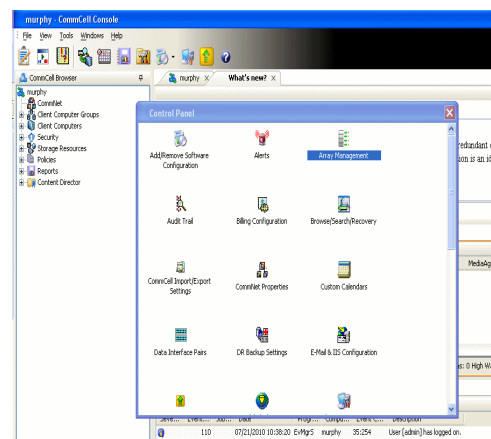
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

## SETUP THE ARRAY INFORMATION

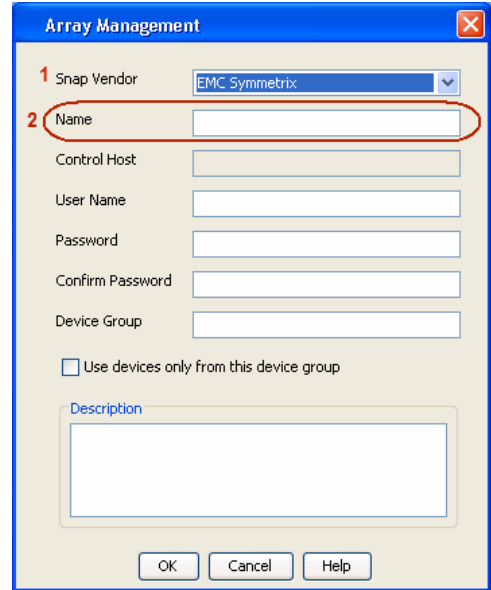
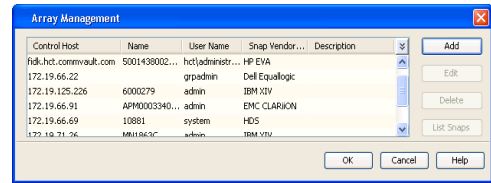
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

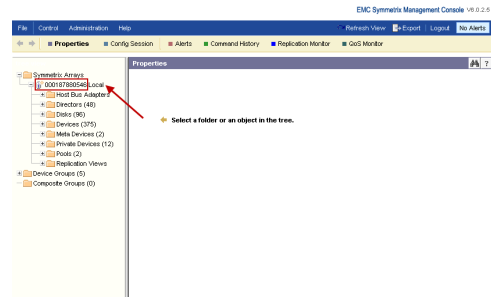


2. Click **Add**.

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

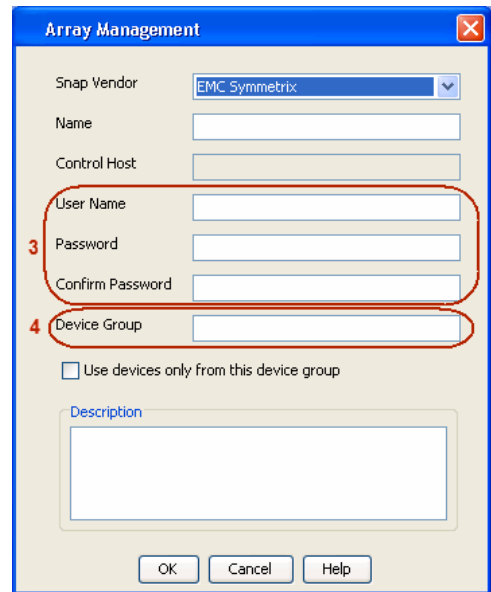


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.

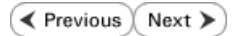


4.
  - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. 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

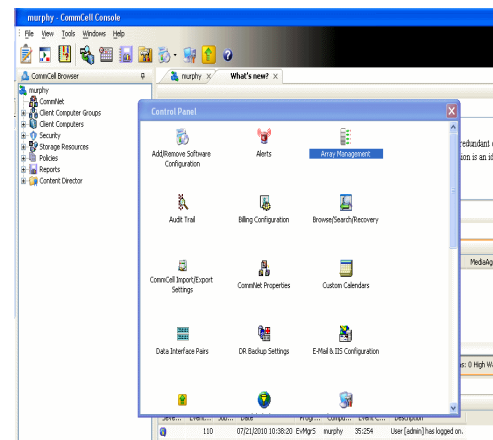
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

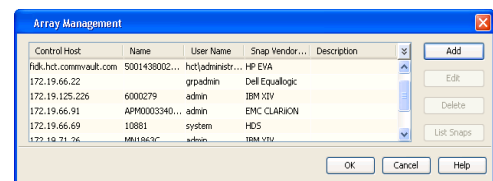
## SETUP THE ARRAY INFORMATION

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

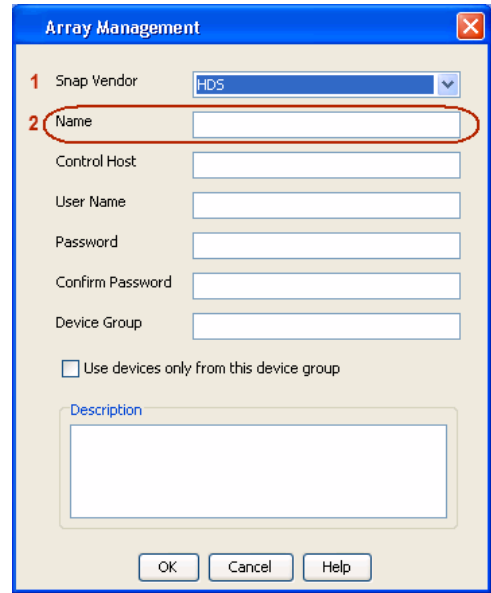
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



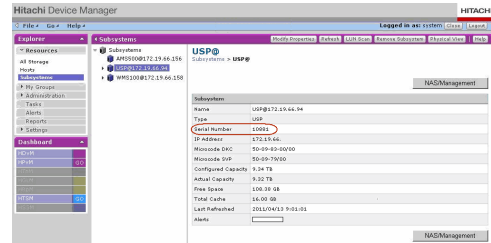
2. Click **Add**.



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.



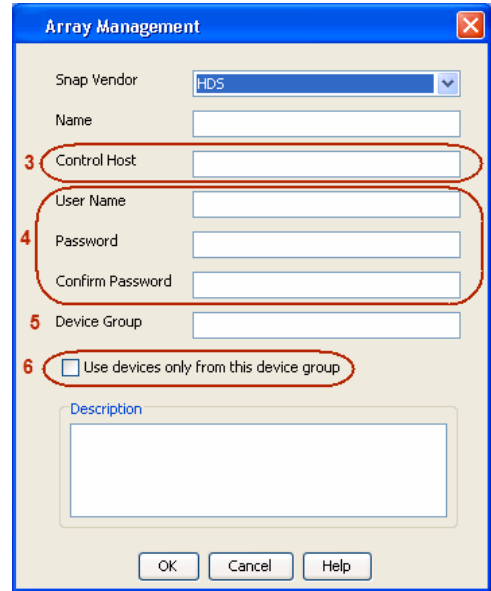
- 4.
- Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
  - Enter the user access information in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for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

◀ Previous   Next ▶

## SETUP THE HP SMI-S EVA

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

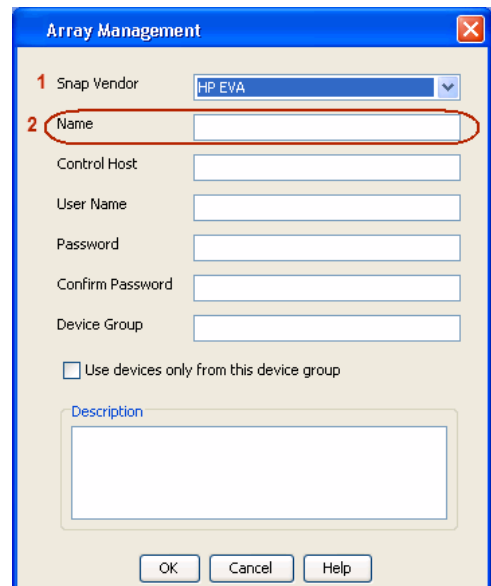
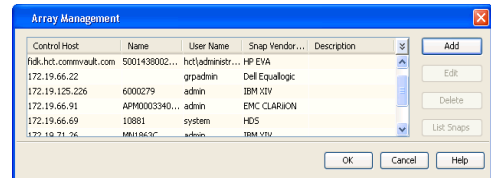
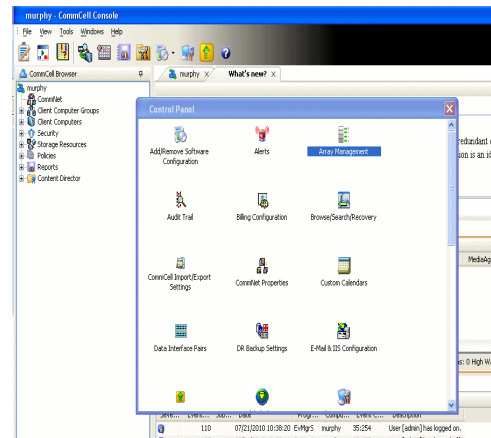
The following steps provide the necessary instructions to setup the HP EVA:

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

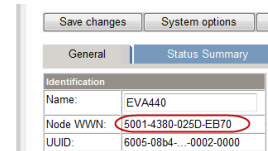
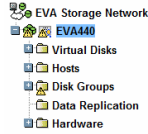
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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.

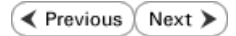
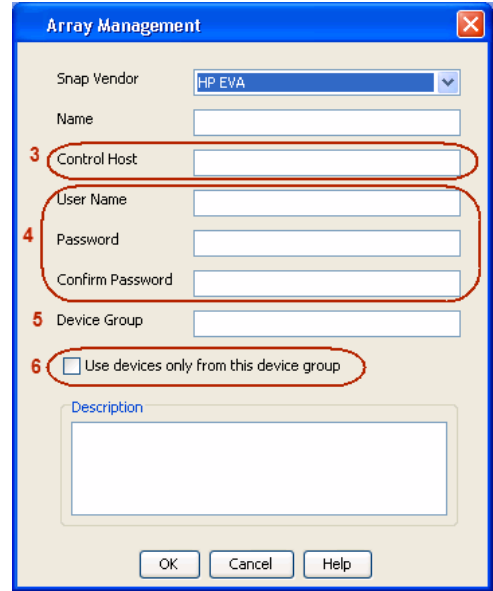
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



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 ▶

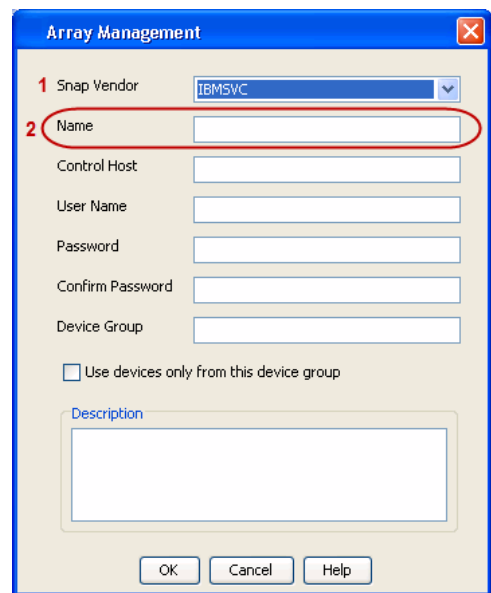
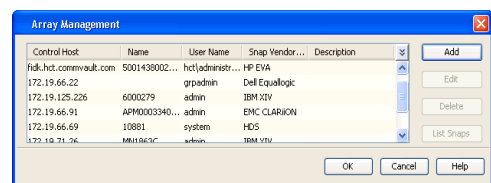
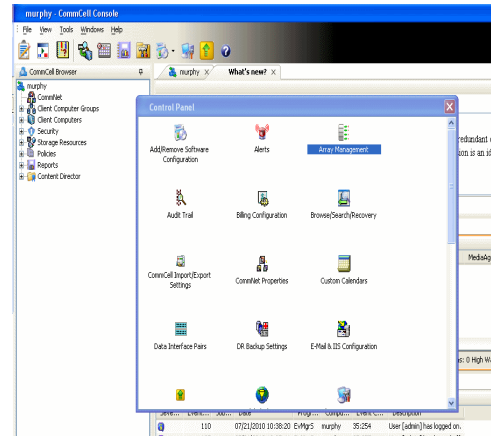
## PRE-REQUISITES

- 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.

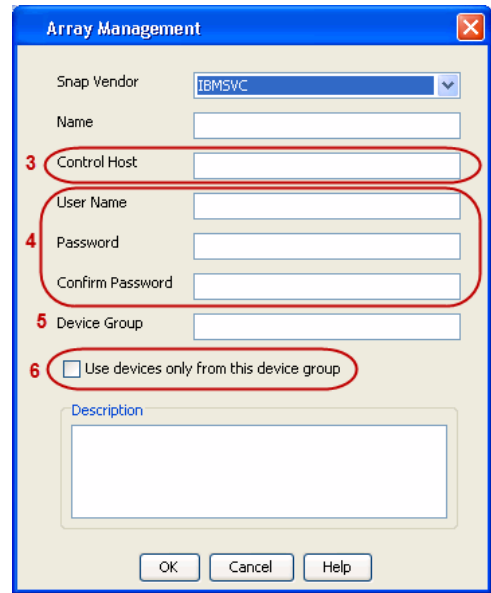
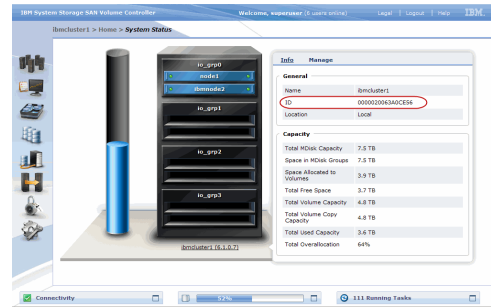
- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
  - Specify the 16-digit ID of the storage device in the **Name** field.



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

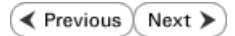
4.

- 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



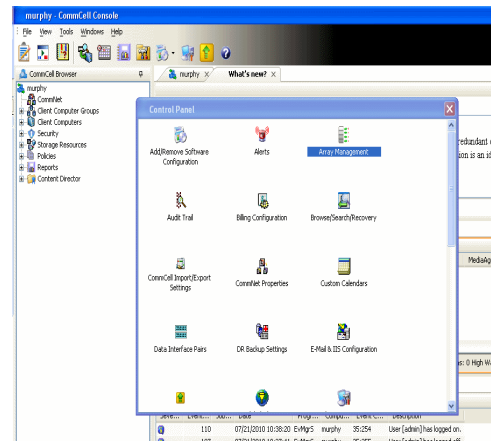
## PRE-REQUISITES

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.

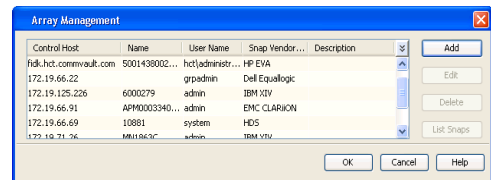
## SETUP THE ARRAY INFORMATION

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

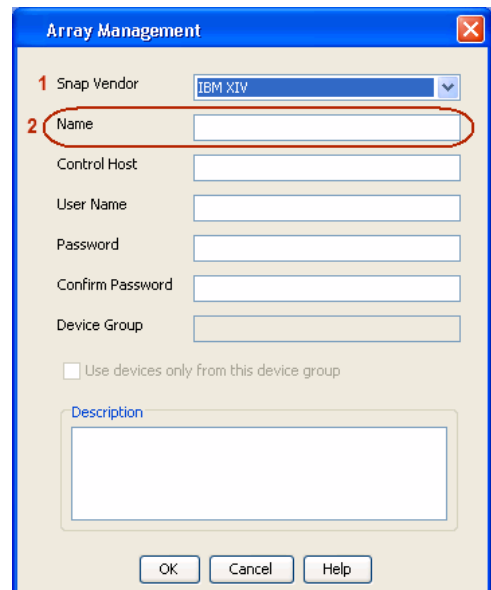
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

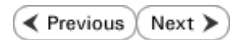
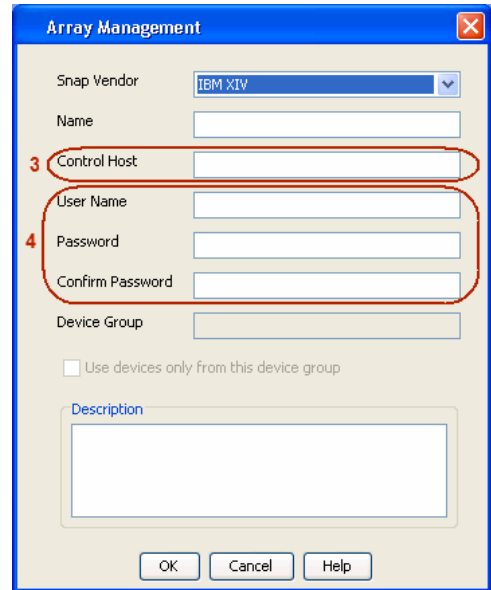
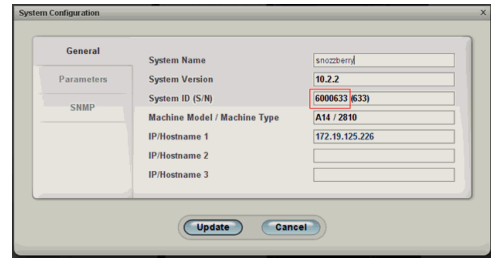


3.
  - Select **IBM XIV** from the **Snap Vendor** list.
  - Specify the 7-digit serial number for the array in the **Name** field.



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.

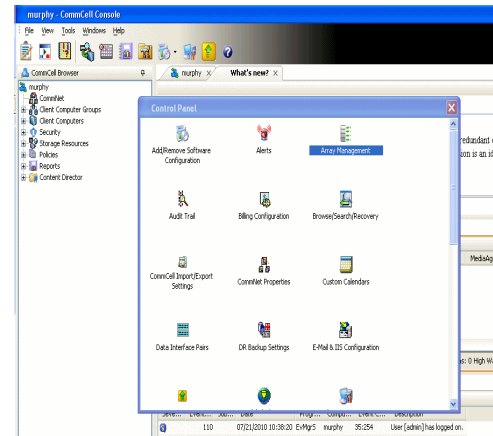
## ADDITIONAL REQUIREMENTS FOR VMWARE

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.

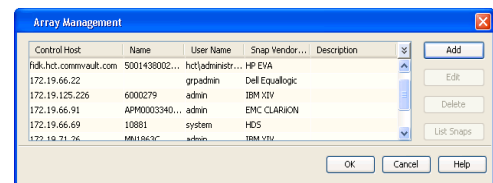
## SETUP THE ARRAY INFORMATION

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

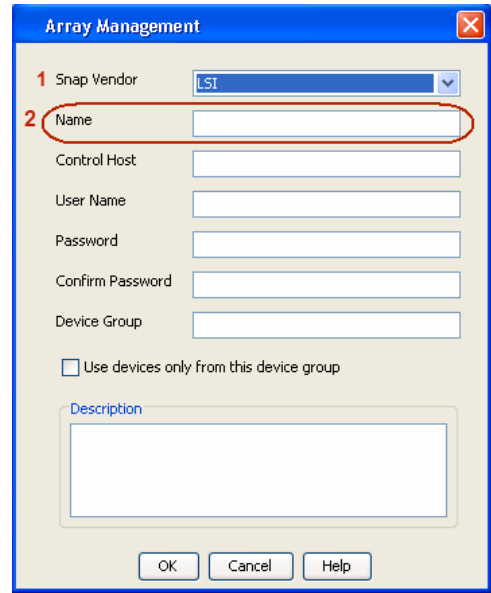
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

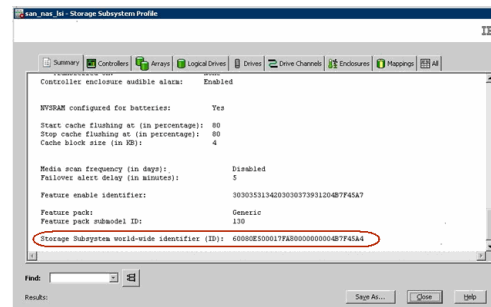


3.
  - Select **LSI** from the **Snap Vendor** list.
  - Specify the serial number for the array in the **Name** field.



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

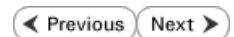
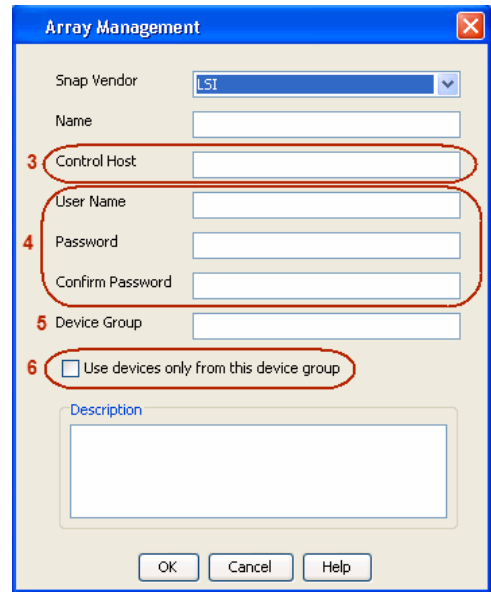
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



- 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 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

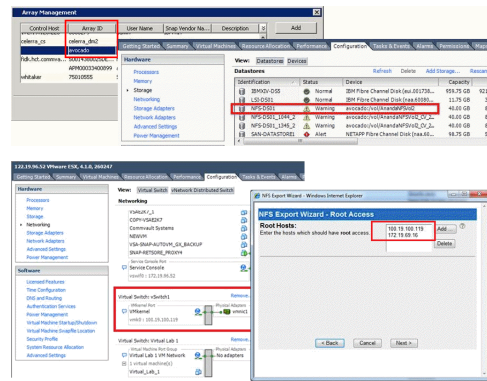
- SnapRestore license for Revert operations (LUNs and NFS shares).
- FlexClone license for backup and restore operations of NFS shares.
- FCP, iSCSI, CIFS, NFS licenses for features such as Fiber Channel Protocol, iSCSI protocol, CIFS file sharing, and NFS File Sharing. Use the appropriate license for 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.

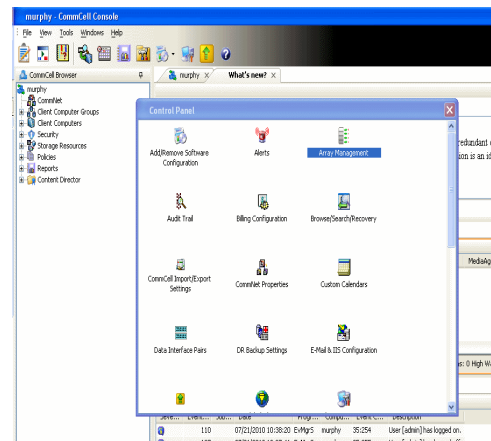
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



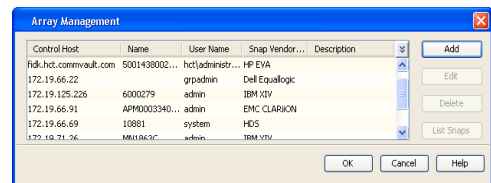
## SETUP THE ARRAY INFORMATION

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 Field]

Control Host: [Text Field]

User Name: [Text Field]

Password: [Text Field]

Confirm Password: [Text Field]

Device Group: [Text Field]

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

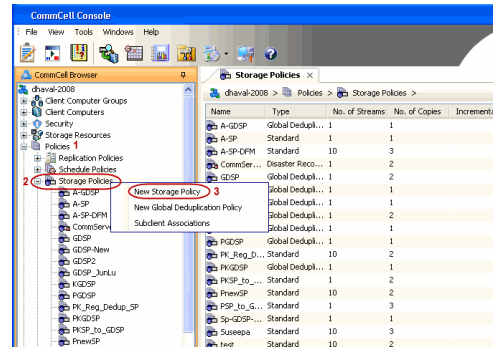
## CONFIGURATION

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

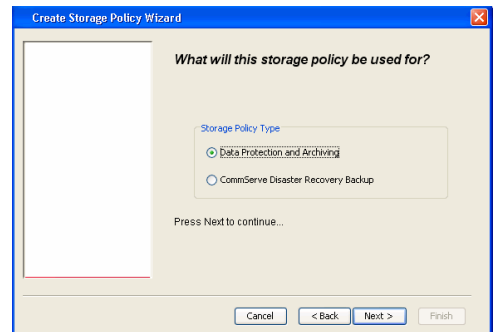
## CREATE STORAGE POLICY

Use the following steps to create a storage policy.

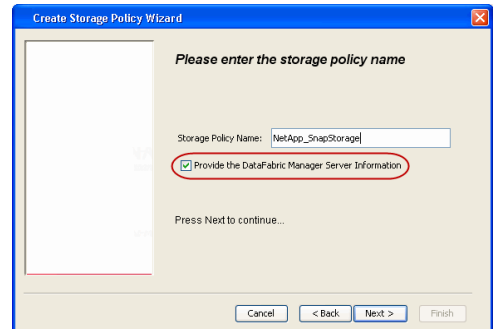
1.
  - From the CommCell Browser, navigate to **Policies**.
  - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



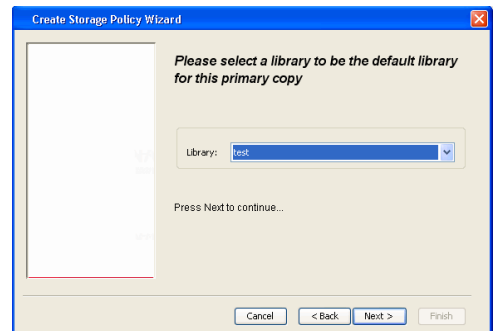
3.
  - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
  - Select **Provide the DataFabric Manager Server Information**.
  - Click **Next**.



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.

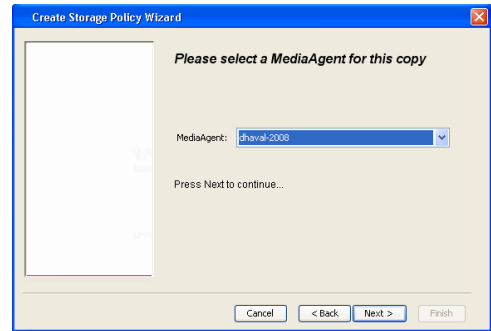
- Click **Next**.



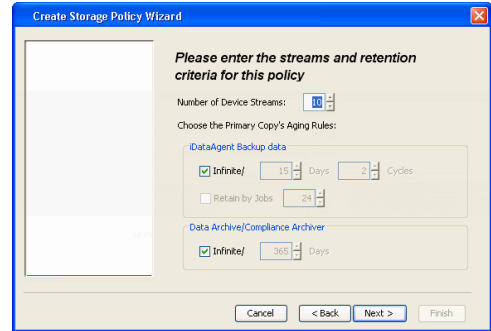
5.
  - Select a MediaAgent from the **MediaAgent** list.
  - Click **Next**.



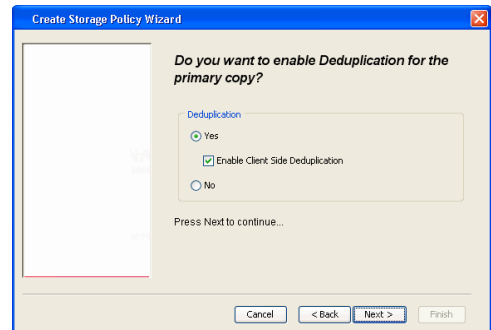
6. Click **Next**.



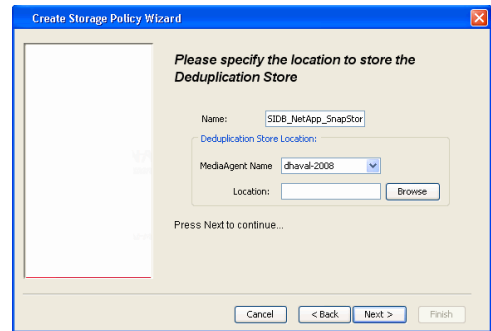
7. Click **Next**.



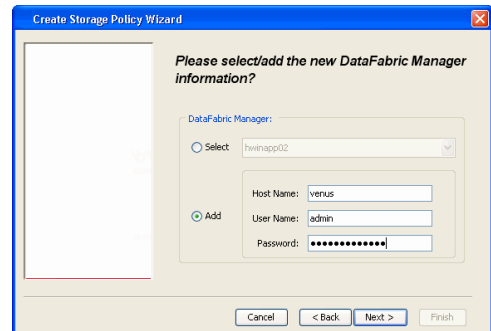
- 8.
- Verify **Name** and **MediaAgent Name**.
  - Click **Browse** to specify location for **Deduplication Store**.
  - Click **Next**.

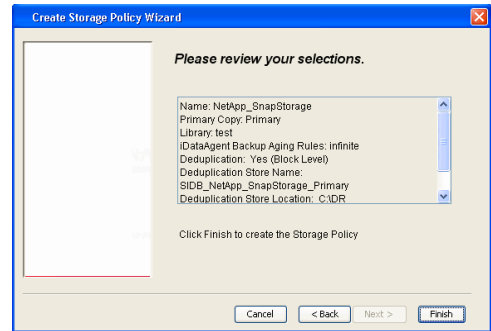


- 9.
- Provide the DataFabric Manager server information.
    - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
    - If you want to add a new DataFabric Manager Server, click **Add**.
  - Click **Next**.



10. Click **Finish**.



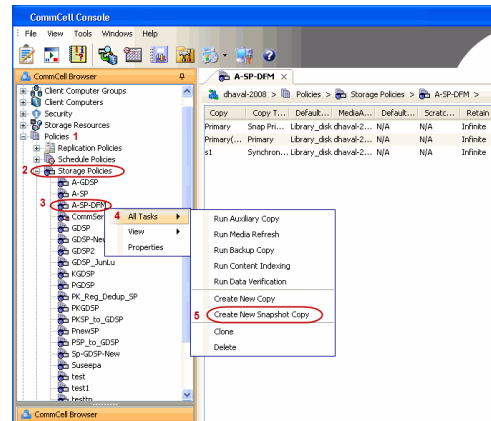


11. The new Storage Policy creates the following:
  - **Primary Snap Copy**, used for local snapshot storage
  - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

### CREATE A SECONDARY SNAPSHOT COPY

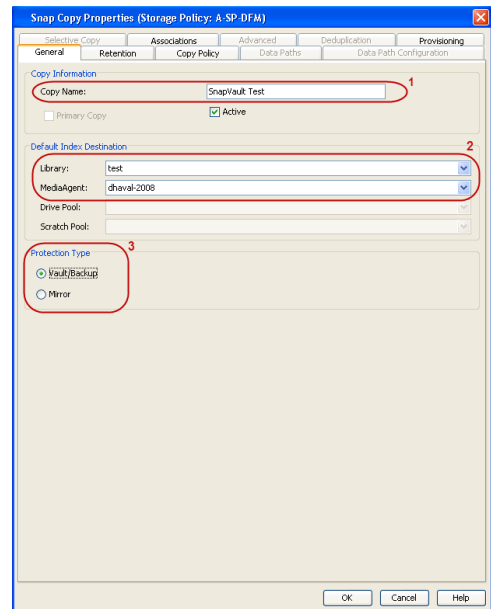
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

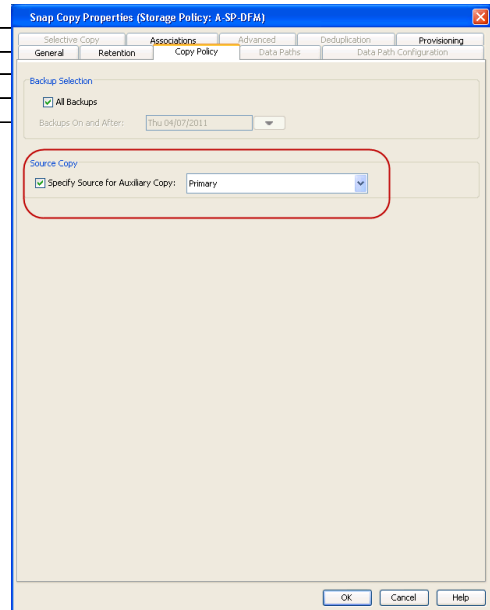


3.
  - Click the **Copy Policy** tab.
  - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

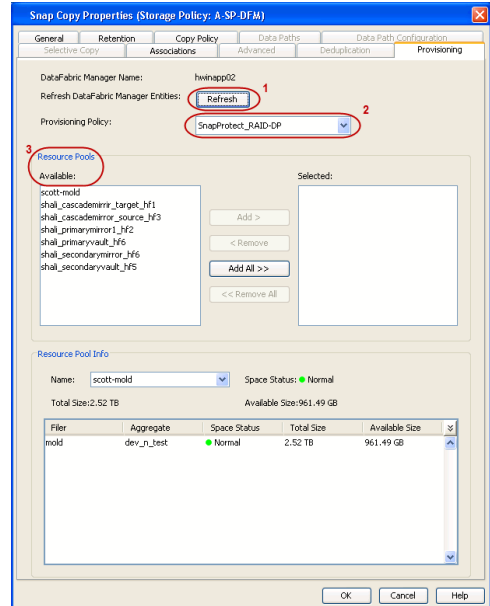
| TOPOLOGY | SOURCE COPY |
|----------|-------------|
|----------|-------------|

|                       |         |
|-----------------------|---------|
| 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.

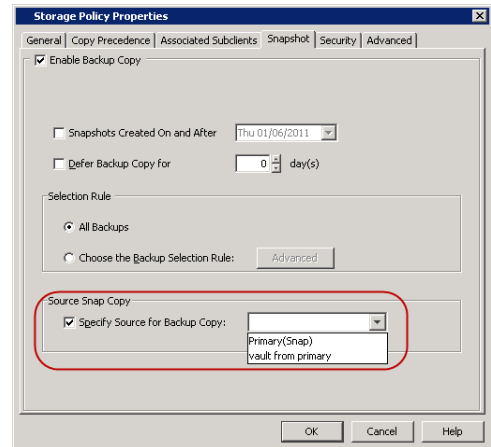
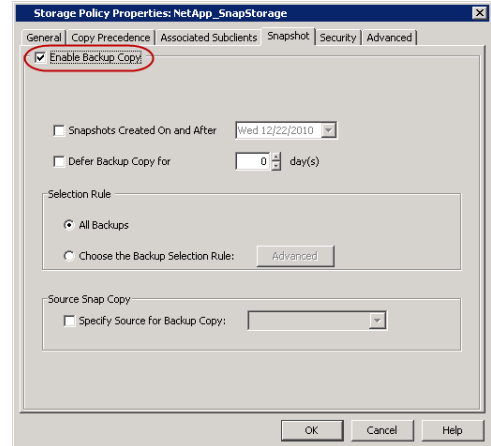
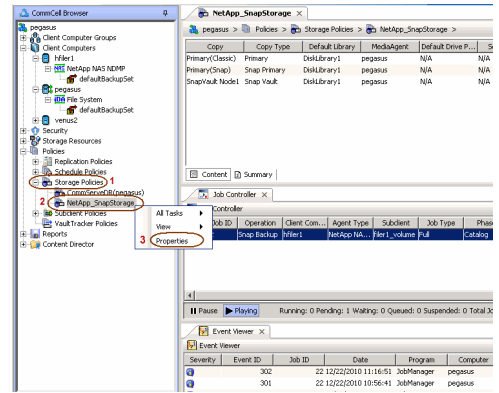
## CONFIGURE BACKUP COPY

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.

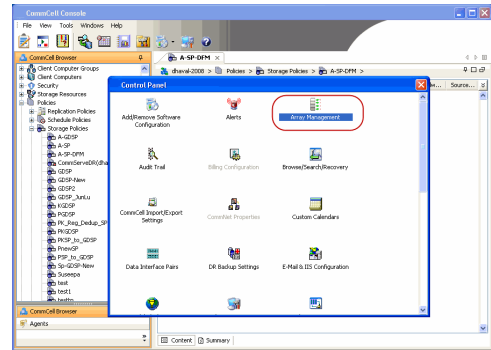


## SETUP THE ARRAY INFORMATION

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**.

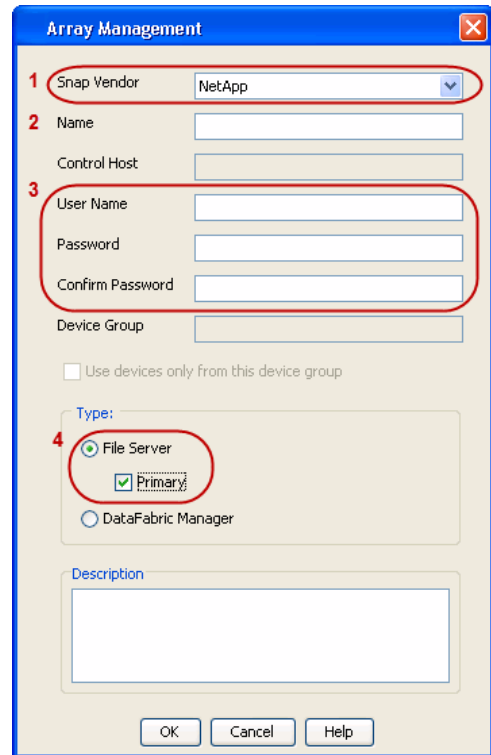
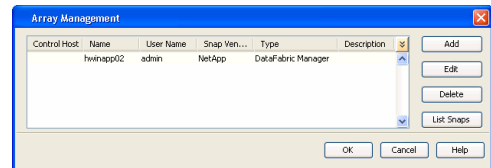


3.
  - Select **NetApp** from the **Snap Vendor** list.
  - Specify the name of the primary file server in the **Name** field.

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.

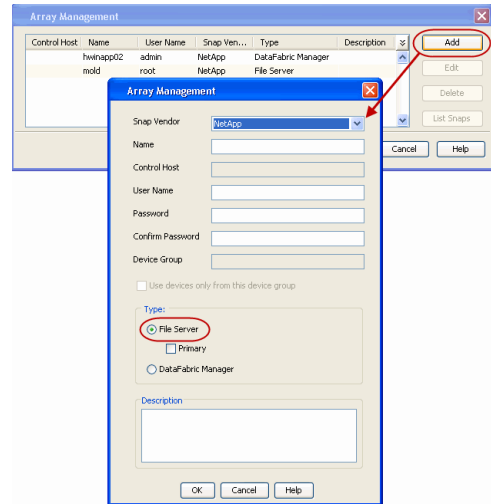
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

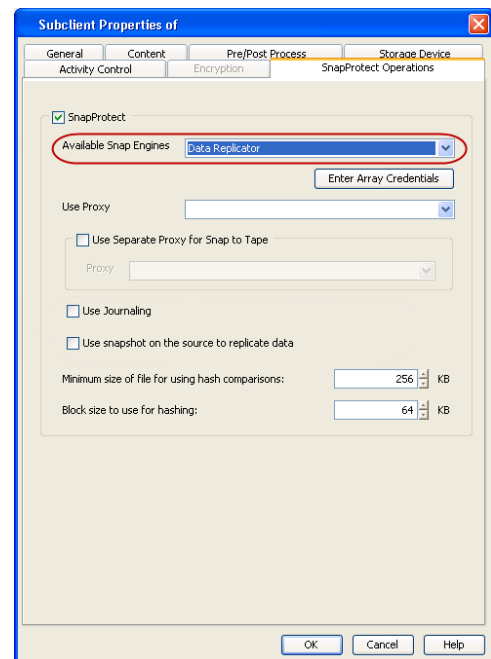
### STORAGE POLICY REQUIREMENTS

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.

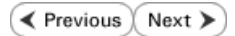
## SETUP THE ARRAY

- 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

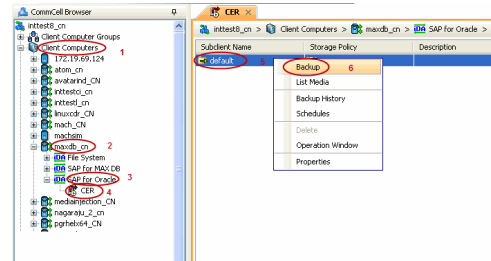


After configuring your instance, and subclient, you are ready to perform your first backup.

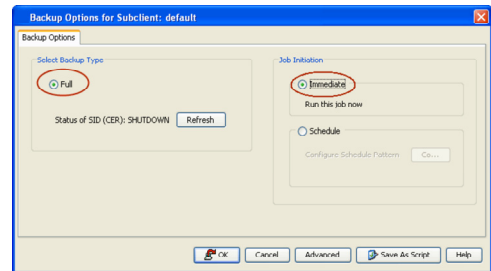
## PERFORM A BACKUP

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**.

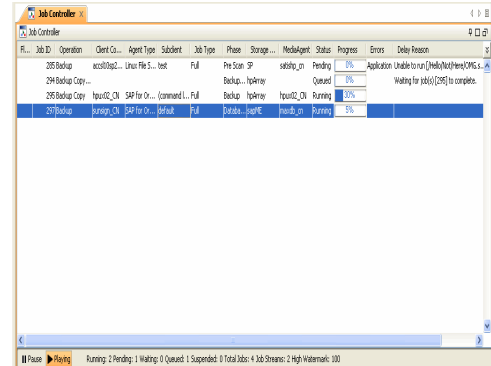


- Select **Full** as backup type and **Immediate** to run the job immediately.
  - Click **OK**.

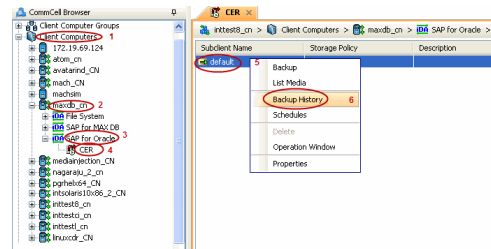


- You can track the progress of the job from the **Job Controller** window of the CommCell console.

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**.

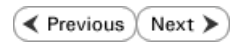
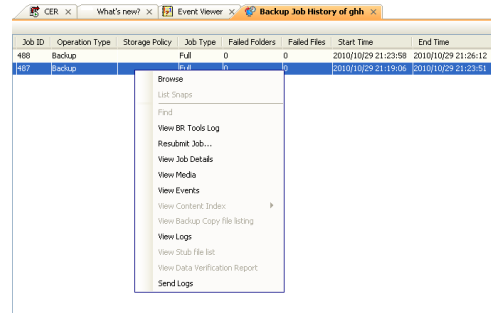
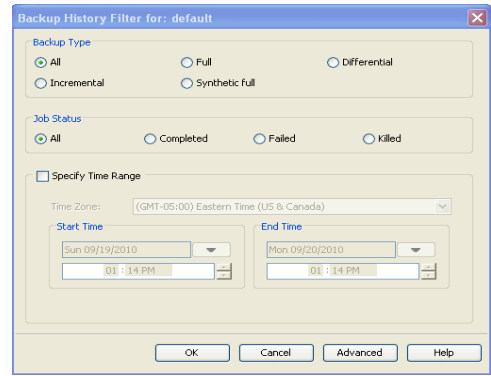


- Click **OK**.



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

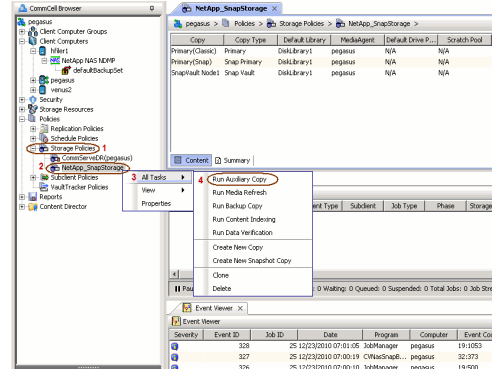
**SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.**

Click **Next** ▶ to Continue.

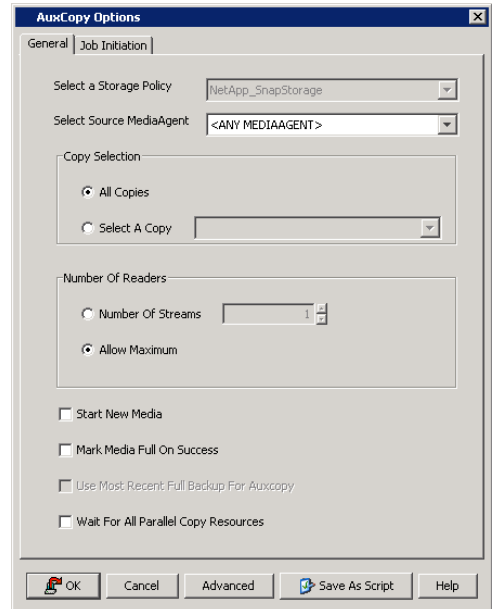
## INITIATE VAULT/MIRROR COPY

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**.

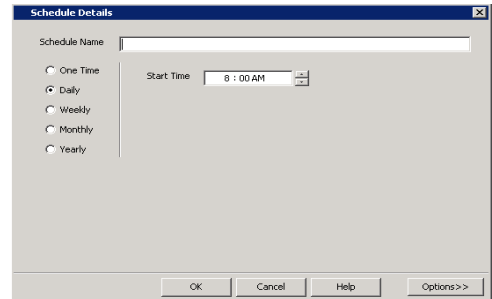


- Select the desired options and click the **Job Initiation** tab.
  - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

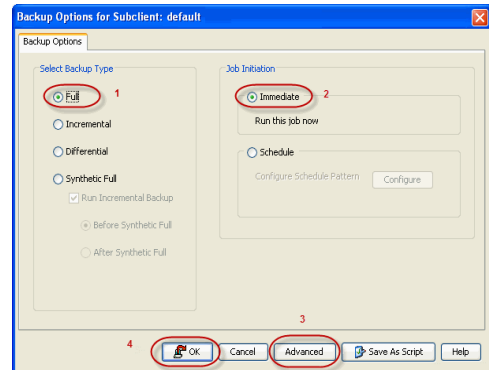
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

#### INLINE BACKUP COPY

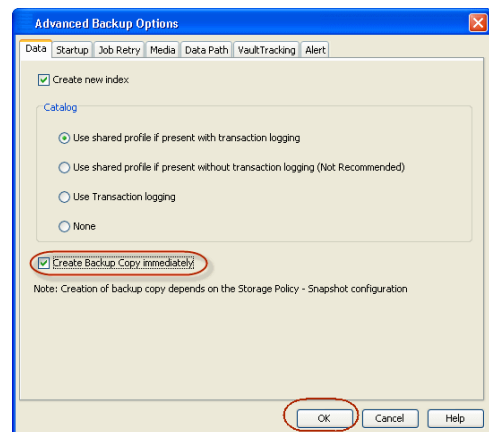
Backup copy operations performed during the SnapProtect backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current SnapProtect 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.

- 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**.

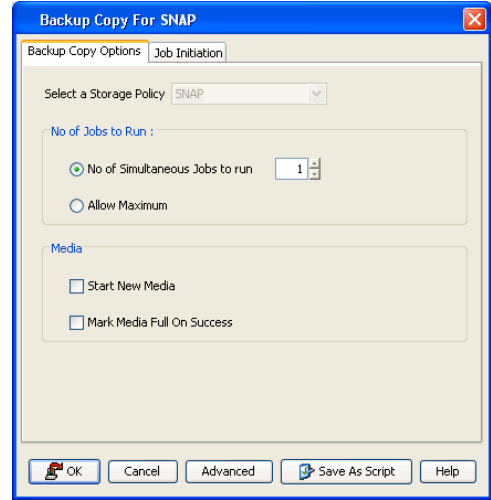
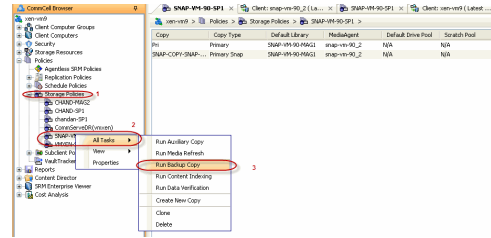


#### OFFLINE BACKUP COPY

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**.



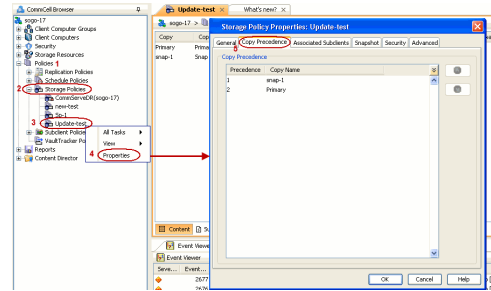
# Getting Started - SAP for Oracle Restore

## PERFORM A RESTORE

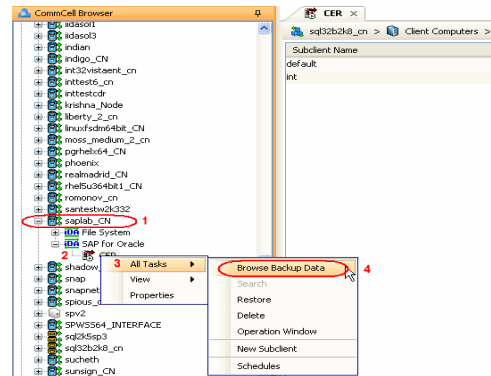
It is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following section comprehends the steps involved in restoring your entire database.

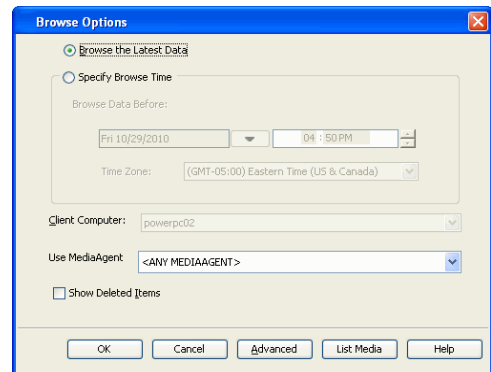
- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.
  - Click the **Copy Precedence** tab.
  - By default, the snapshot copy is set to 1 and is used for the operation.  
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
  - Click **OK**.



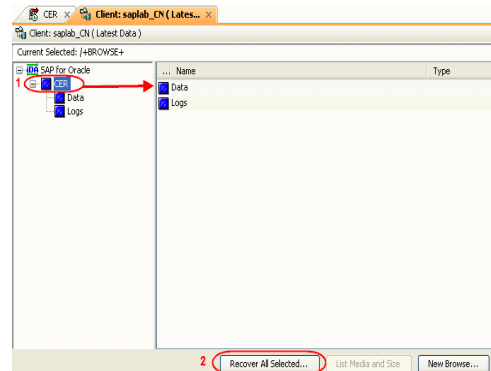
- From the CommCell Console, navigate to **<Client> | SAP for Oracle**.
  - Right-click the instance that contains the data you want to restore and click **All Tasks | Browse Backup Data**.



- Click **OK**.

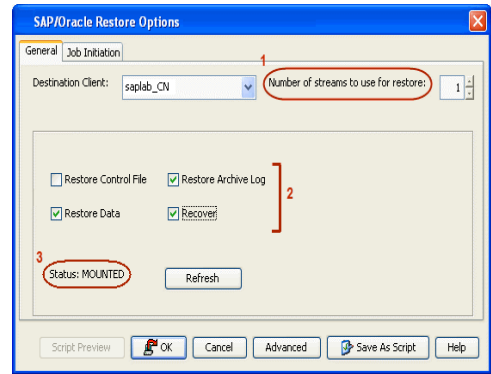


- Select the instance node in the left pane. The data and logs will be automatically selected in the right pane.
  - Click **Recover All Selected**.



- 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**.



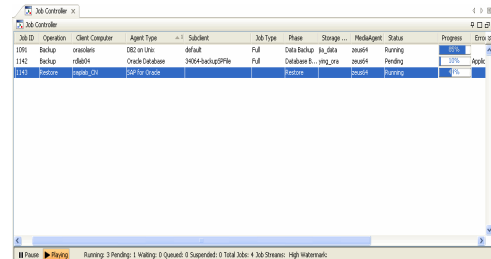
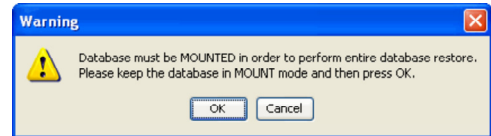
If the database is not mounted, a warning dialog appears to remind you to set the database in MOUNT mode.

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**.

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.

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

Number of streams [10]

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

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.

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.

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

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

20. Press **Enter**.

Changes saved into /etc/system.gal.1744

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_semmsl=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



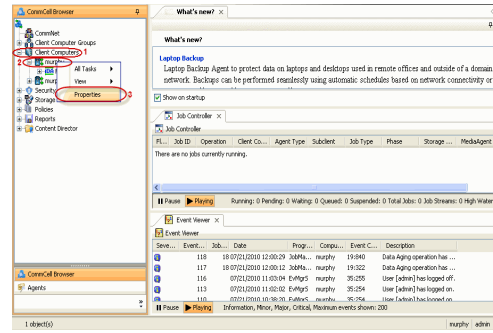
Getting Started - DB2 Configuration

CONFIGURATION

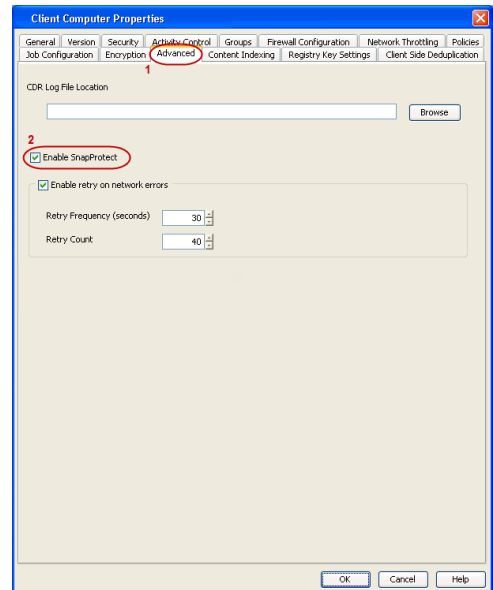
Once the DB2 *iDataAgent* is installed, configure an Instance and a Backup Set to facilitate backups. Each Backup Set references a DB2 database. Also it is recommended to create separate subclients for data backups and archive log backups.

The following sections provide the necessary steps required to create and configure these components for a first SnapProtect backup of the DB2 database.

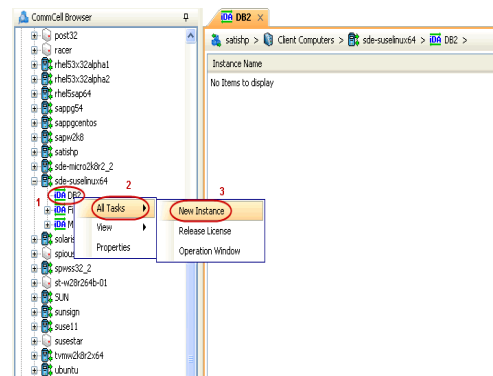
- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click the client and select **Properties**.



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

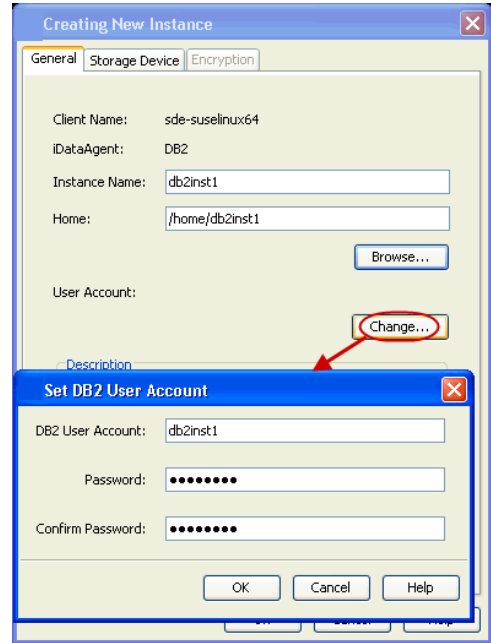
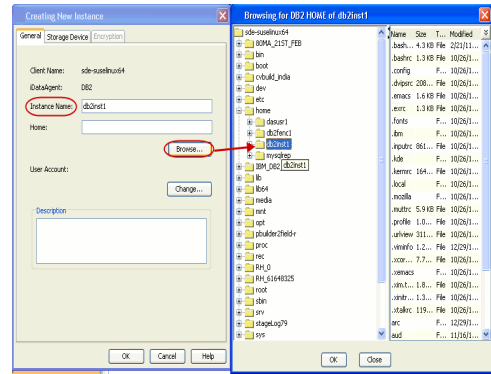


- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
 - Right-click **DB2** and click **All Tasks** | **New Instance**.

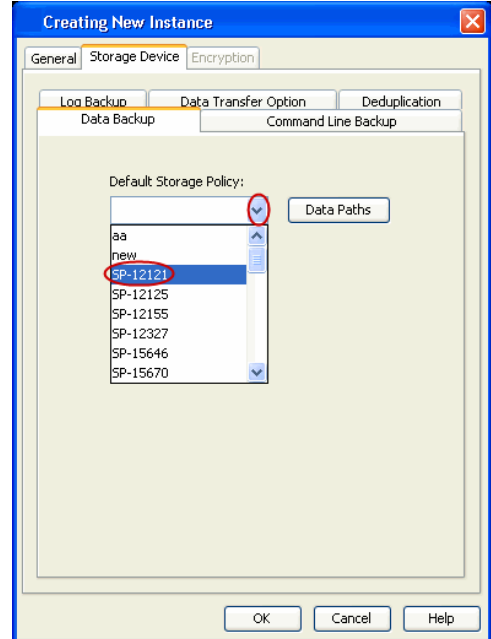


- In the **Instance Name** field, type a name.
 - In the **Home** field, click **Browse** and select the path to the DB2 application files.

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**.

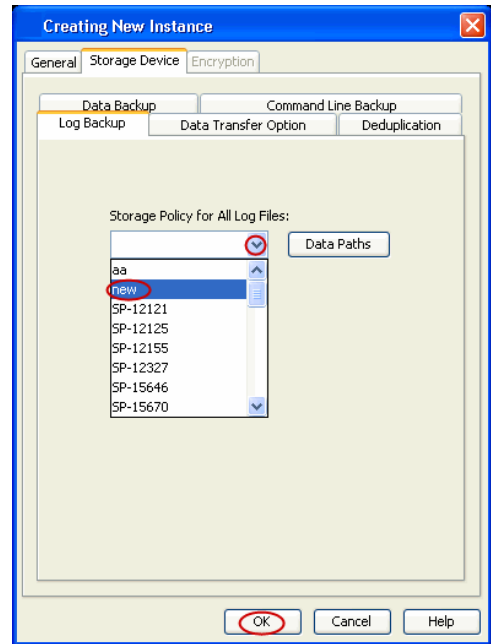
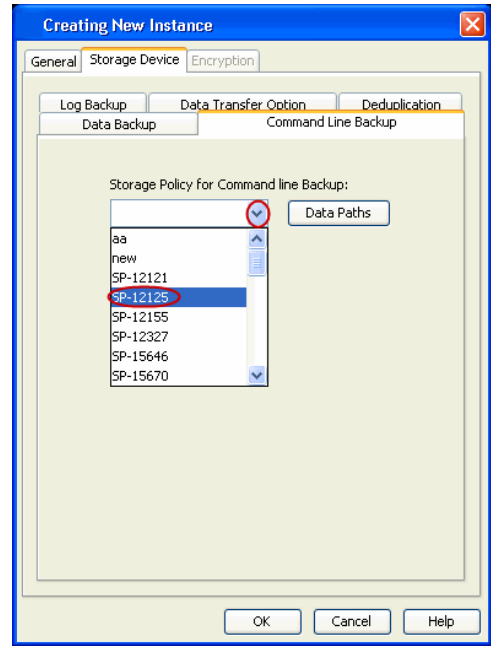


6.
 - Click the **Storage Device** tab.
 - In the **Default Storage Policy** box, select a storage policy name for data backups.

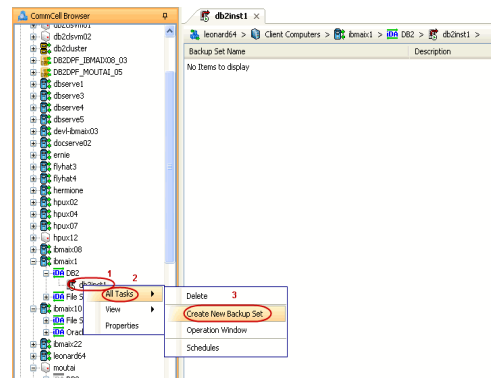


7.
 - Click the **Command Line Backup** tab.
 - In the **Storage Policy for Command Line Backup** box, select a storage policy name.

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**.

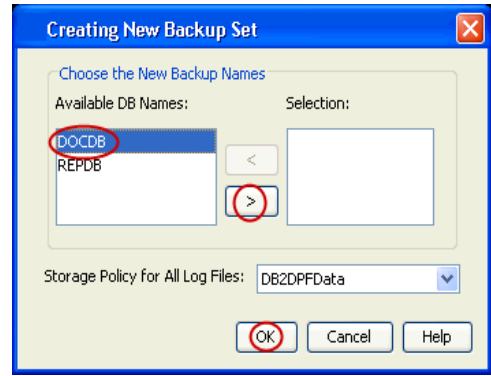


9.
 - From the CommCell Browser, navigate to **Client Computers | <Client> | DB2**.
 - Right-click the **<Instance>** and click **All Tasks | Create New Backup Set**.

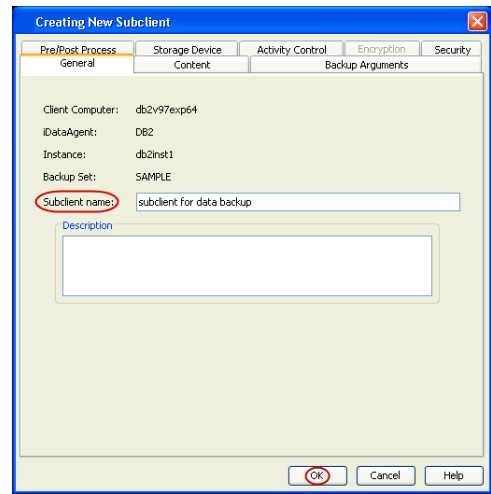
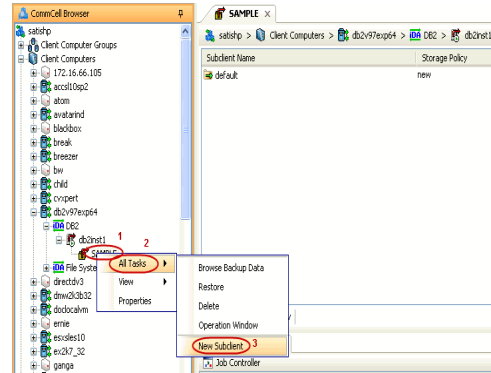


10.
 - Under **Available DB Names**, click the database name, and then click the arrow button to move the database name to the **Selection** box.
 - Click **OK**.

11.
 - From the CommCell Browser, navigate to the <Instance>.
 - Right-click the <Backup Set> and click **All Tasks | New Subclient**.

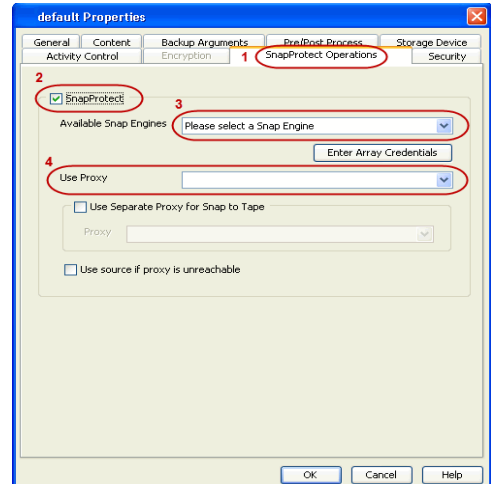


12. In the **Subclient Name** field, type a name.



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.

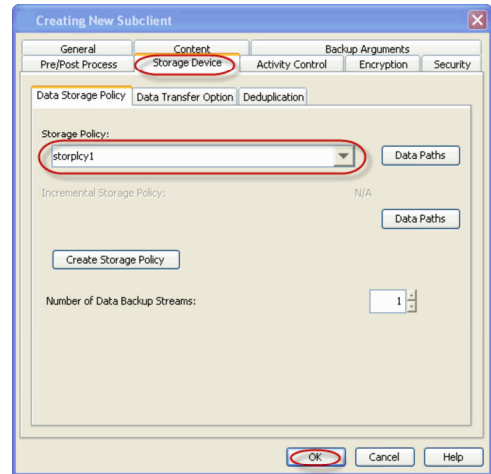
When performing IntelliSnap backup copy using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.



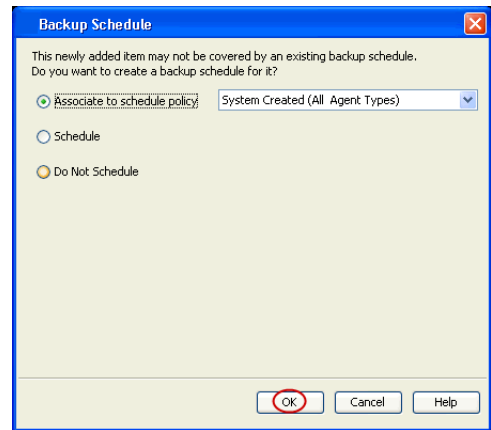
14.
 - Click the **Storage Device** tab.
 - In the **Data Storage Policy** list, select the same storage policy used for data backups in **Step 6**.

The subclient should use the same storage policy set for data backups at the instance level in order to prevent job failure.

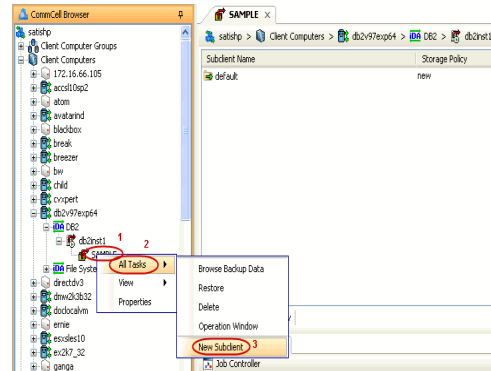
- Click **OK**.



15. Click **OK**.

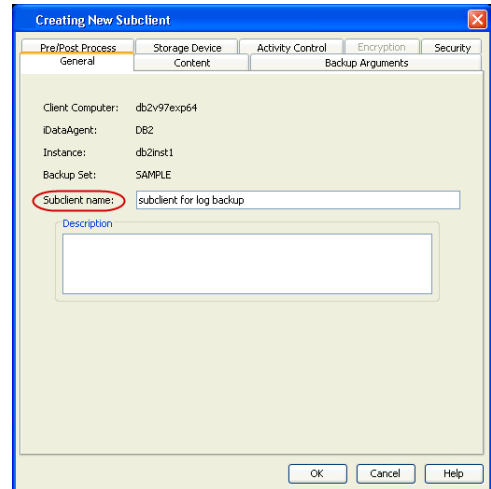


16.
 - From the CommCell Browser, navigate to the **<Instance>**.
 - Right-click the **<Backup Set>** and click **All Tasks | New Subclient**.

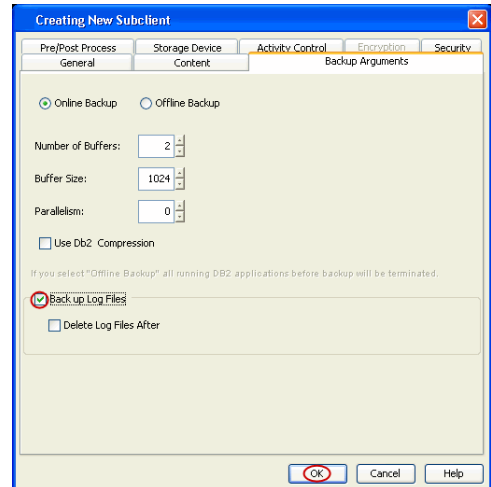
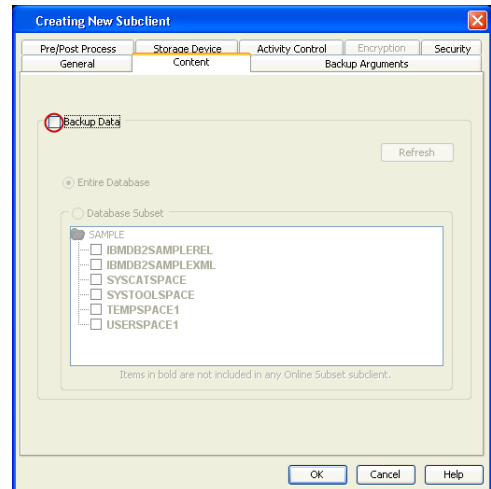


17. In the **Subclient Name** field, type a name.

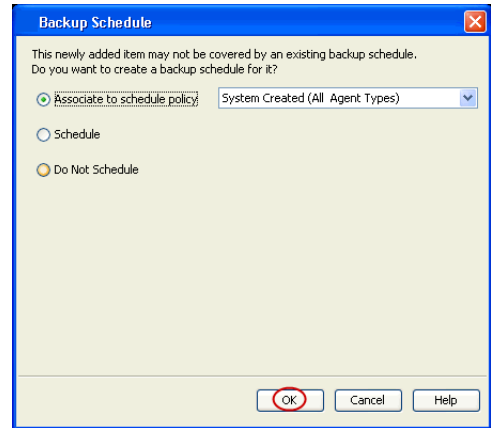
- 18.
- Click the **Content** tab.
 - Clear the **Backup Data** checkbox.



- 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.

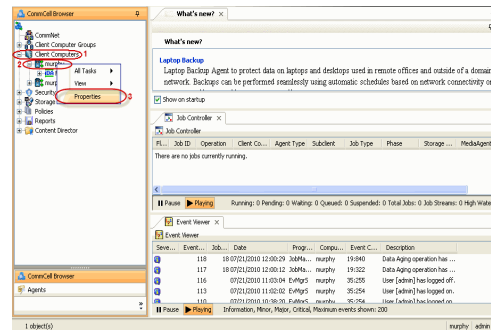
Click **Next** ► to Continue.

ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE

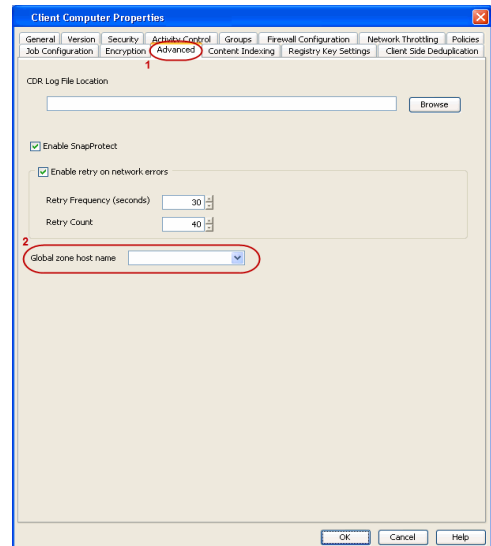


Follow the steps given below to enable SnapProtect backups on each of the non-global zone clients containing the application data.

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.



3. 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.

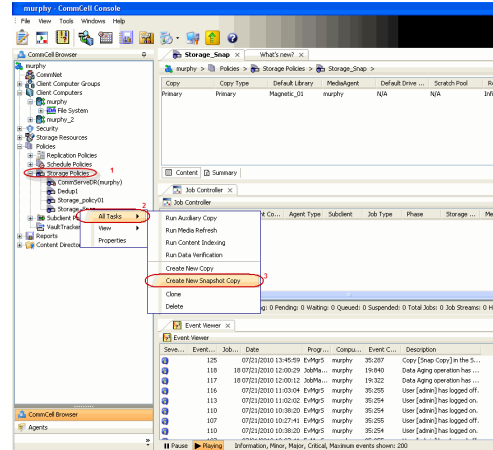
Click **Next** ► to Continue.

CREATE A SNAPSHOT COPY

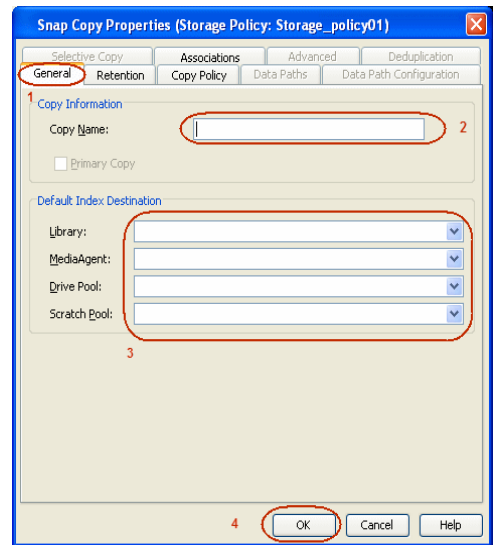


Create a snapshot copy for the Storage Policy. The following section provides step-by-step instructions for creating a Snapshot Copy.

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



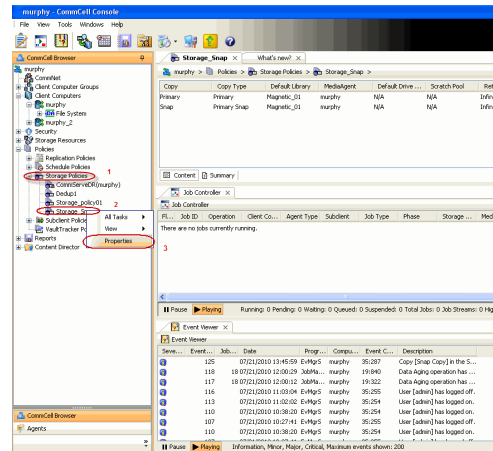
- Enter the copy name in the **Copy Name** field.
 - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
 - Click **OK**.



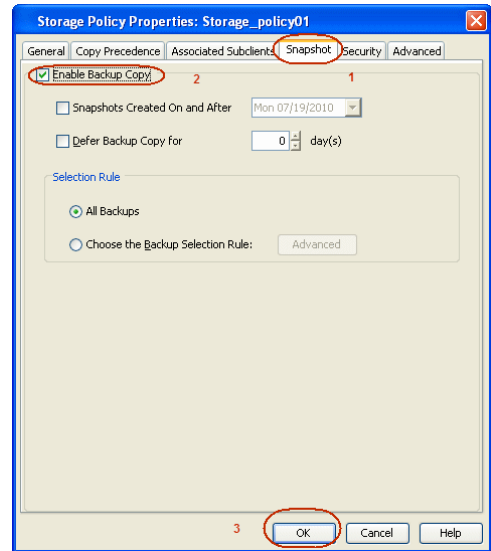
CONFIGURE BACKUP COPY

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

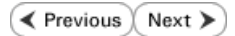
[◀ Previous](#) [Next ▶](#)

CHOOSE THE STORAGE ARRAY

HARDWARE STORAGE ARRAYS
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



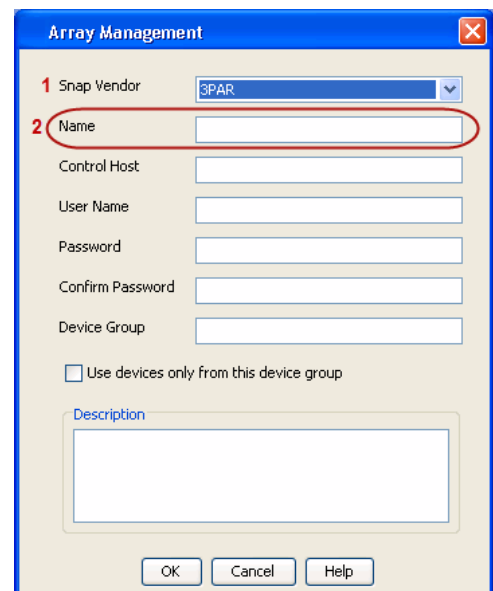
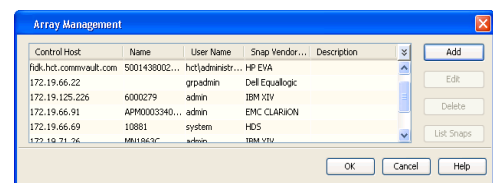
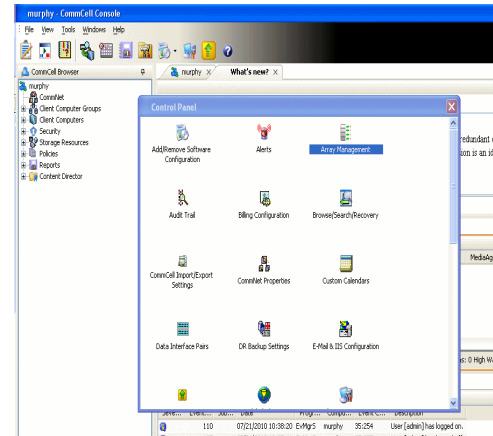
PRE-REQUISITES

- 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

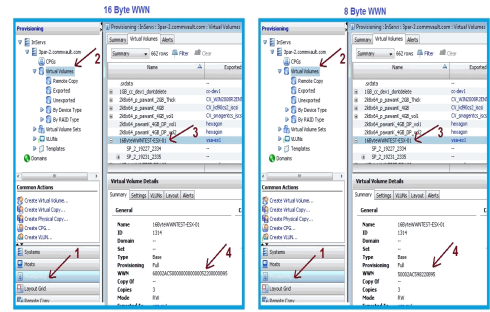
where $\text{DevID.substr}(26,6)$ is the next 6 digits after the twenty sixth digit from the WWN number

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

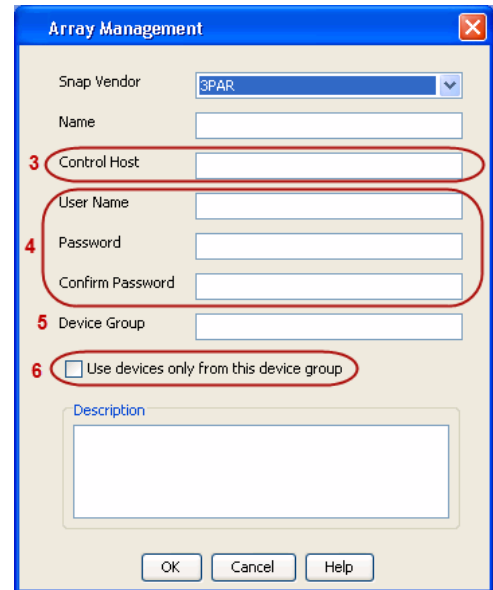
After adding all the values, the resulting array name is 2FF70002AC000B95.



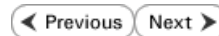
- Enter the IP address of the array in the **Control Host** field.
 - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the CPG group created on the array to be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

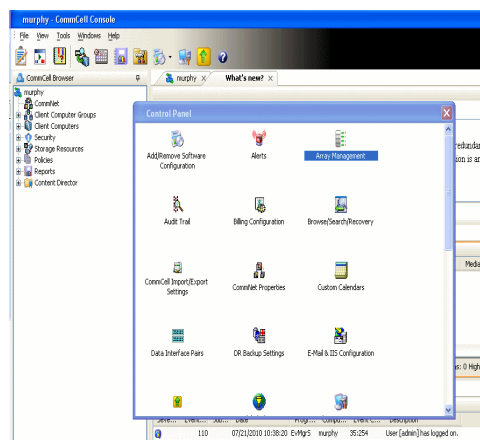
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
 - Create a new group administration account in the firmware, and set the desired permissions for this account.
 - If you plan to use the existing 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.

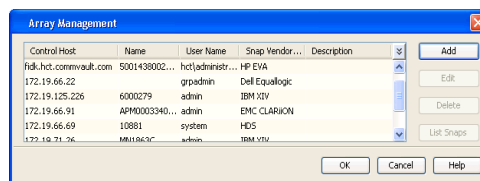
SETUP THE ARRAY INFORMATION

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**.

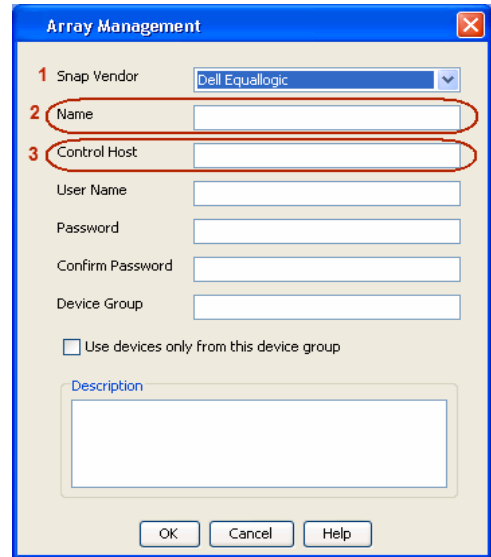


2. Click **Add**.

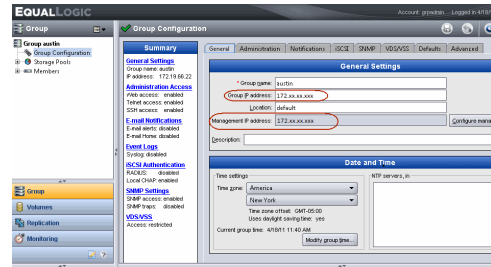


3.
 - Select **Dell Equallogic** from the **Snap Vendor** list.
 - Specify the Management IP address in the **Name** field.

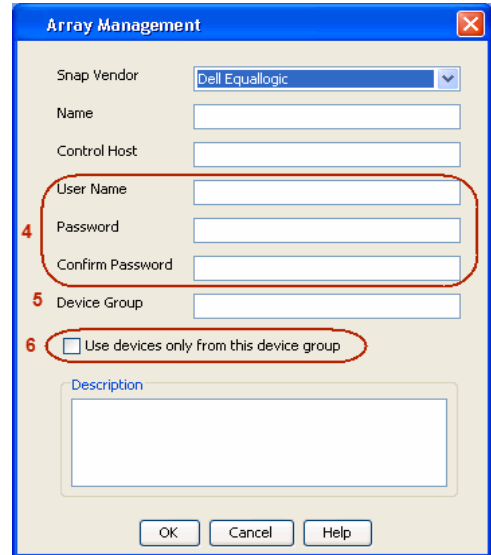
No entry is required in the **Name** field if there is no Management IP address configured.
 - Specify the Group IP address in the **Control Host** field.



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.

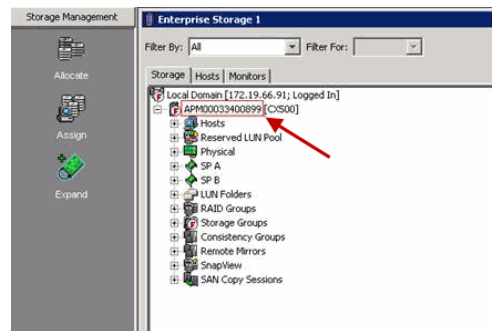
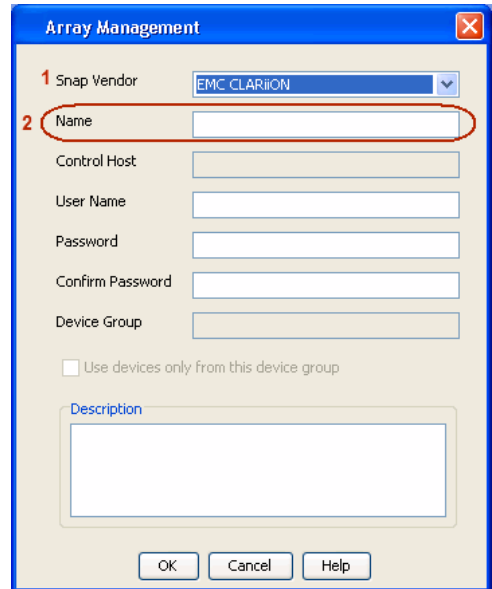
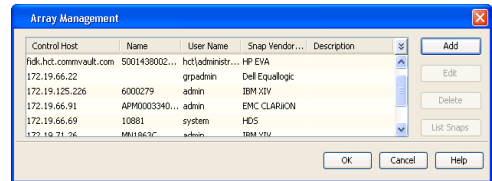
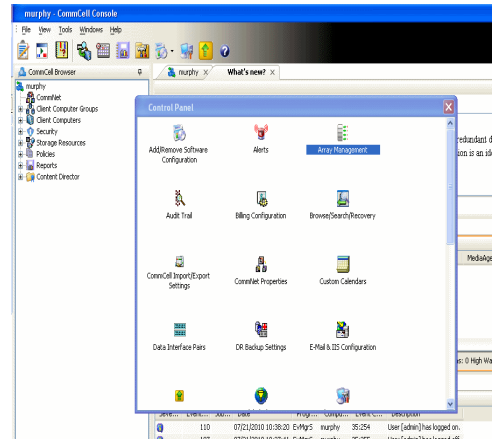
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.

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

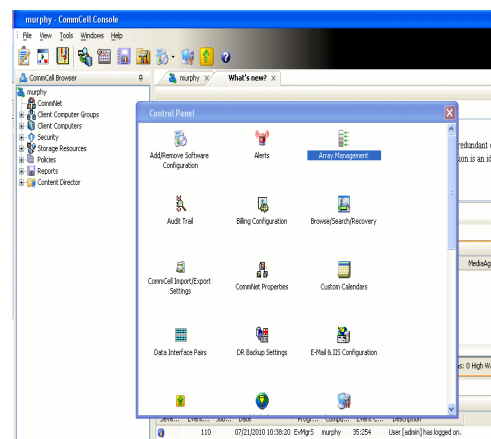
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

SETUP THE ARRAY INFORMATION

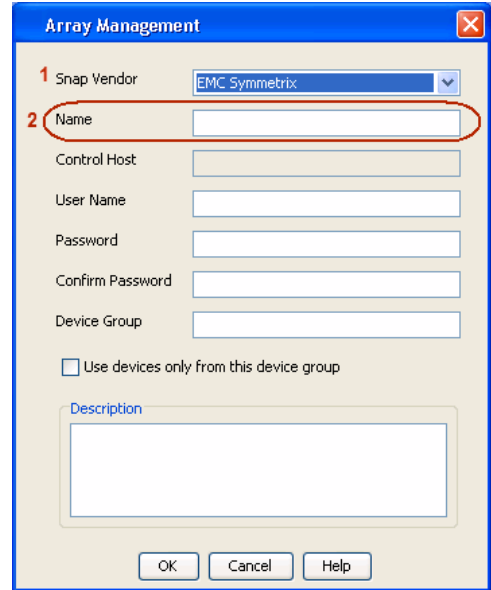
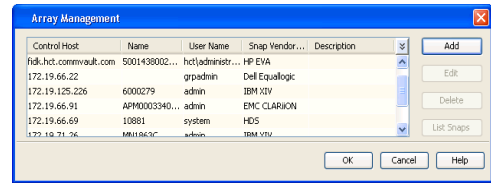
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

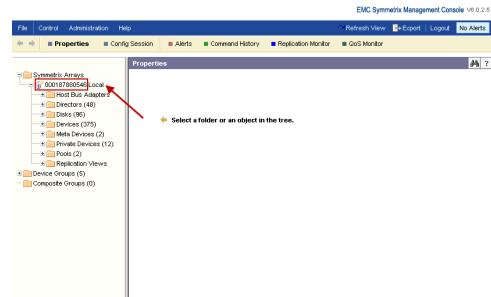


2. Click **Add**.

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

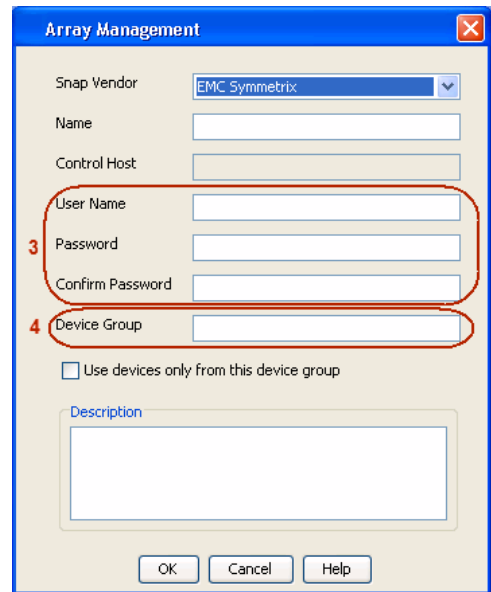


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



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

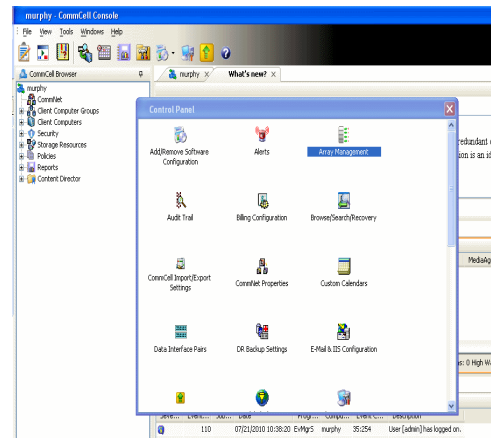
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

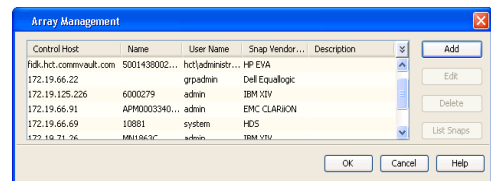
SETUP THE ARRAY INFORMATION

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

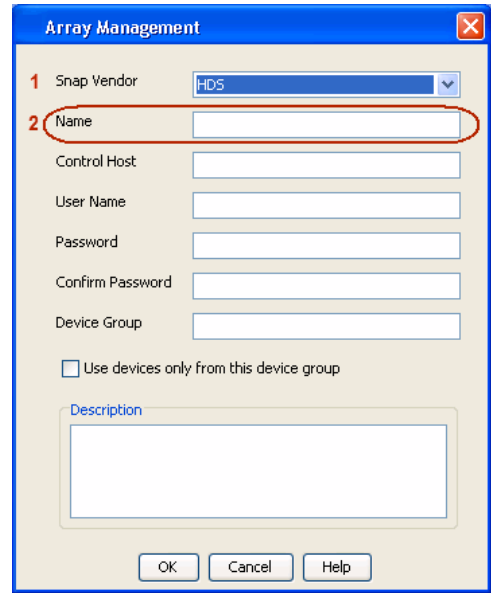
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



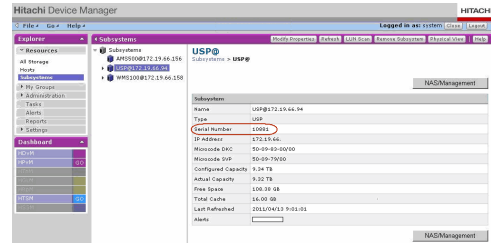
2. Click **Add**.



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.



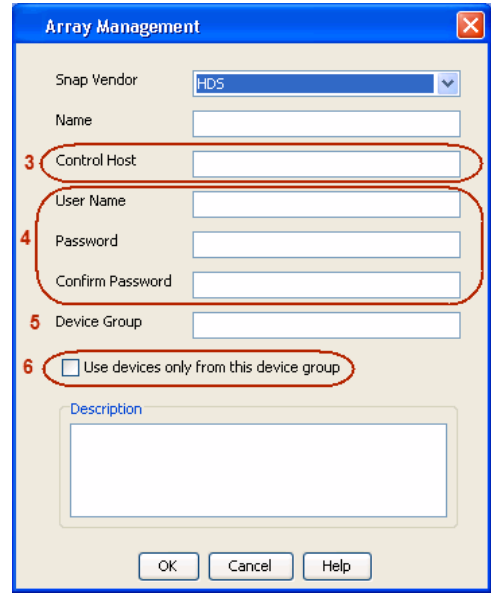
4.
 - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
 - Enter the user access information in the **Username** and **Password** fields.
 - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for snapshot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

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

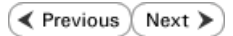
where <COW_POOL_ID> (for COW job) should be a number. This parameter is required.

<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.

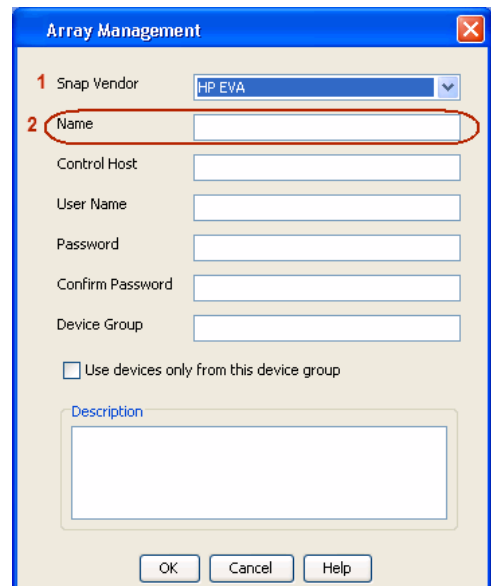
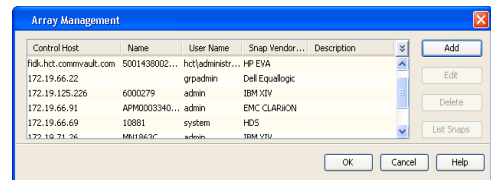
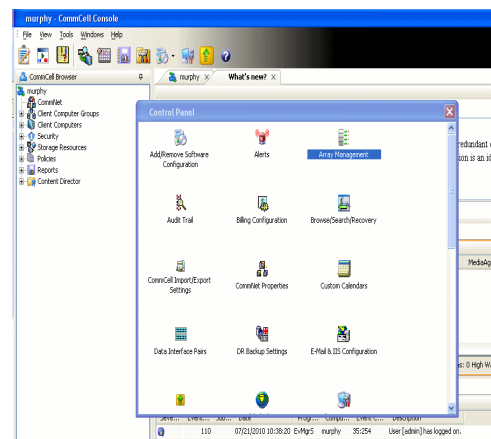
The following steps provide the necessary instructions to setup the HP EVA:

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

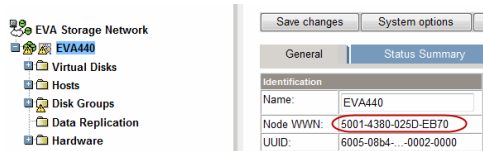
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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.

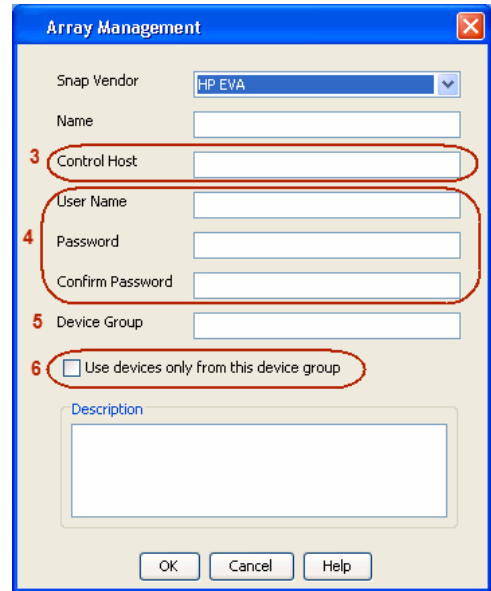
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



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 ▶

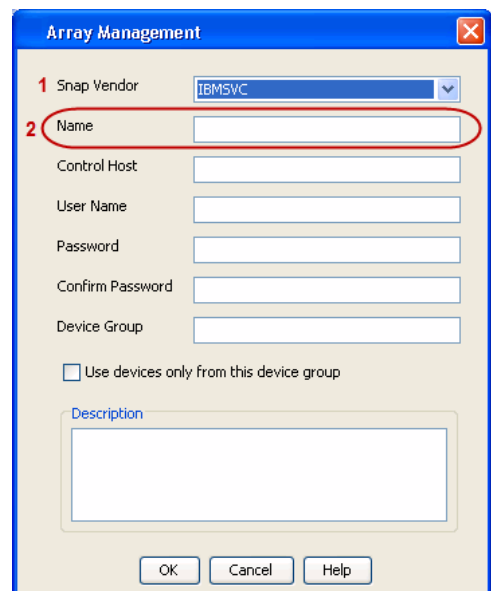
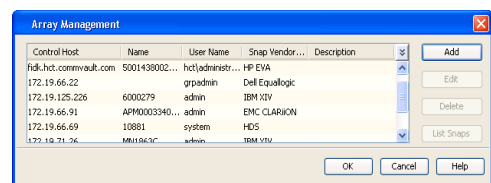
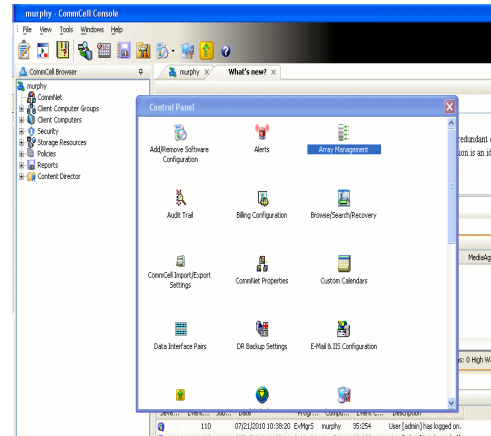
PRE-REQUISITES

- 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.

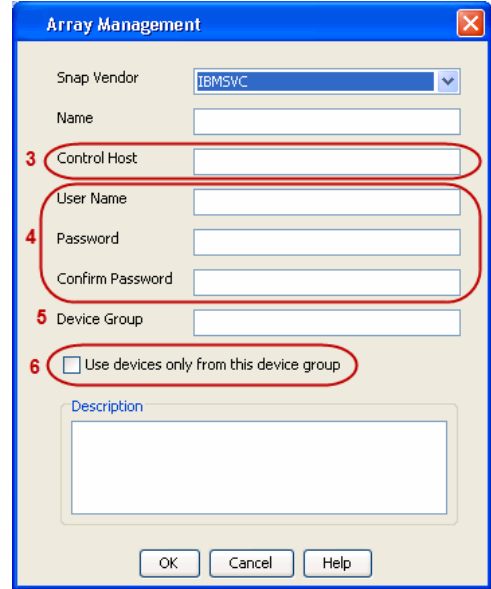
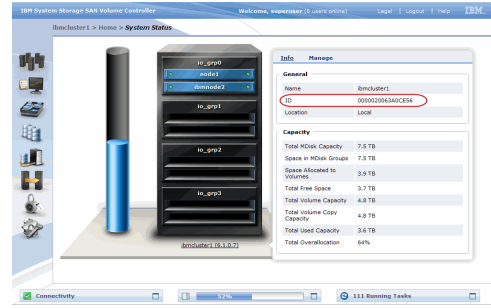
- From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
 - Specify the 16-digit ID of the storage device in the **Name** field.



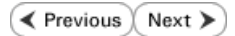
The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

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



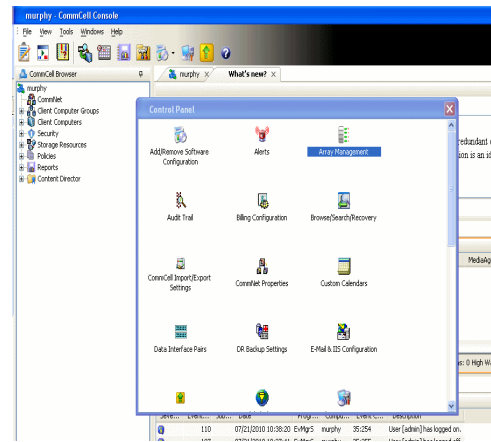
PRE-REQUISITES

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.

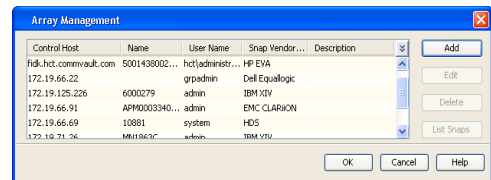
SETUP THE ARRAY INFORMATION

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

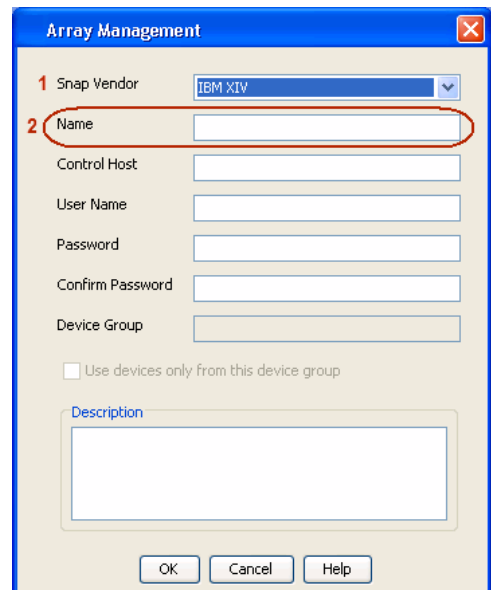
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.



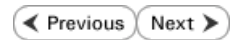
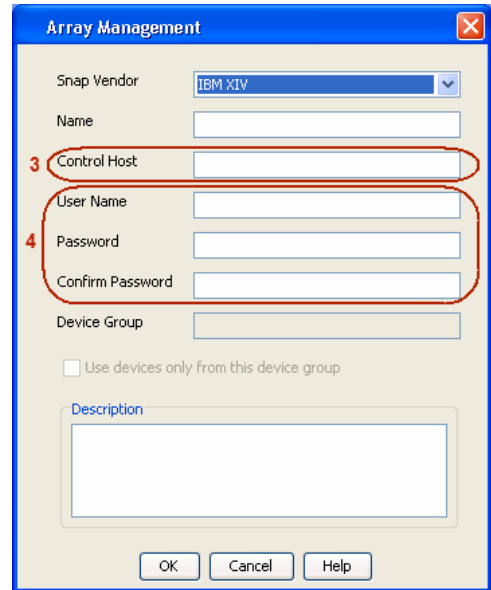
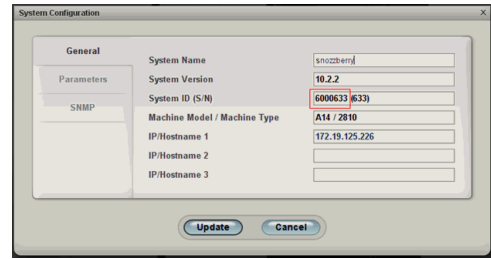
3.
 - Select **IBM XIV** from the **Snap Vendor** list.
 - Specify the 7-digit serial number for the array in the **Name** field.



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.

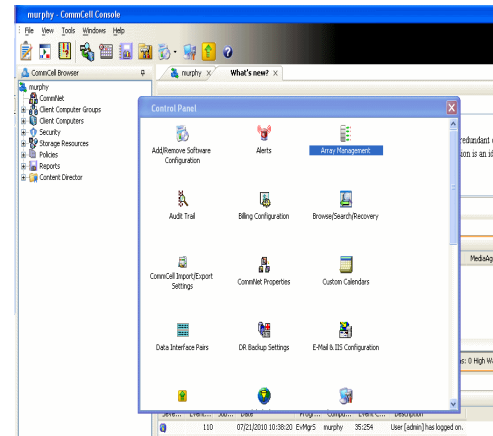
ADDITIONAL REQUIREMENTS FOR VMWARE

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.

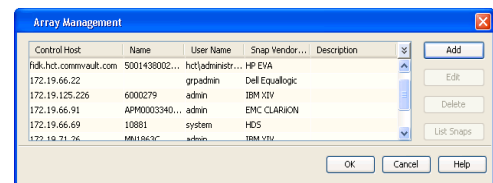
SETUP THE ARRAY INFORMATION

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

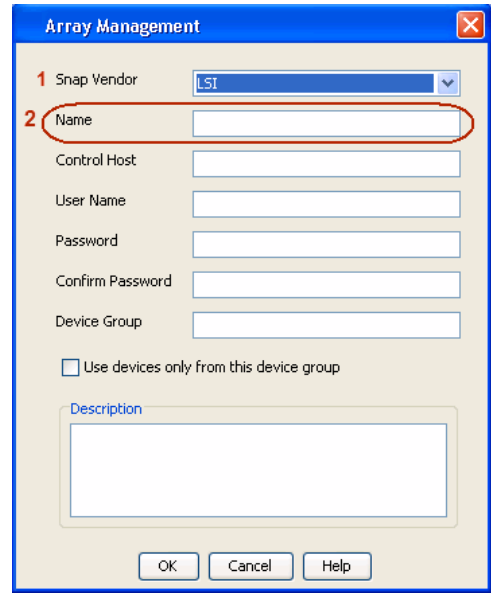
1.
 - From the CommCell Console, navigate to **Tools | Control Panel**.
 - Click **Array Management**.



2. Click **Add**.

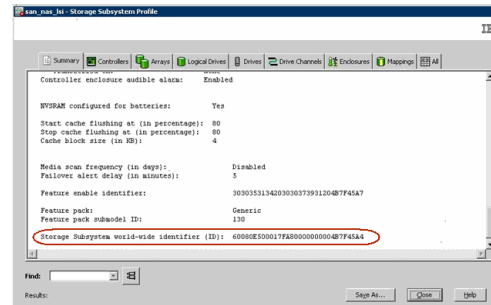


3.
 - Select **LSI** from the **Snap Vendor** list.
 - Specify the serial number for the array in the **Name** field.



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

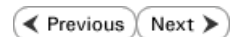
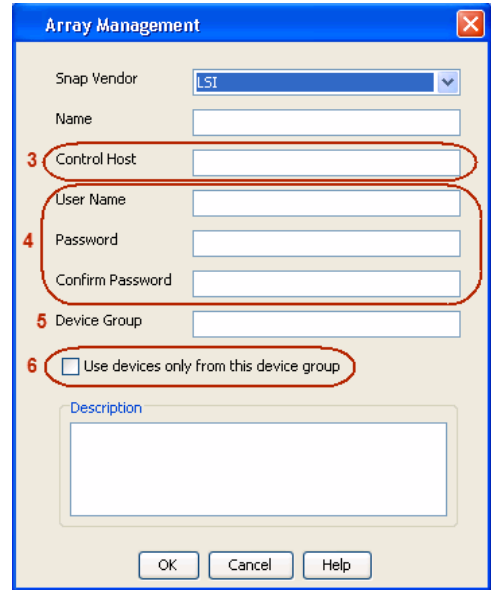
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



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 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

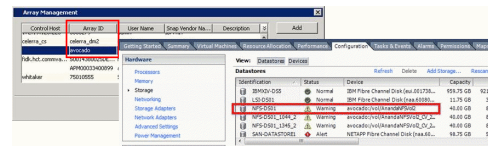
LICENSES

- 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.

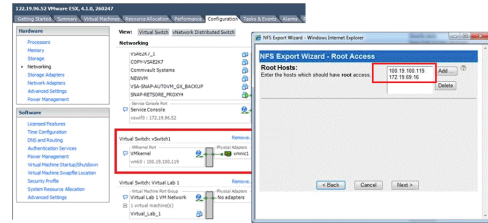
ADDITIONAL REQUIREMENTS FOR VMWARE

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.



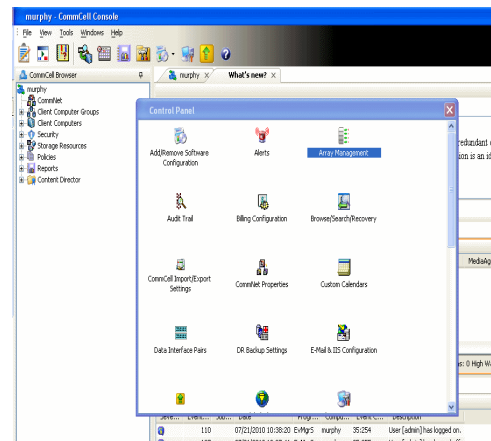
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



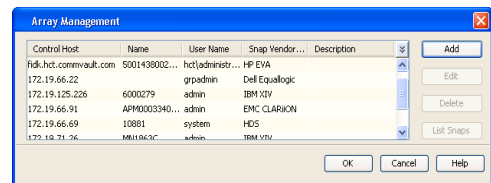
SETUP THE ARRAY INFORMATION

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

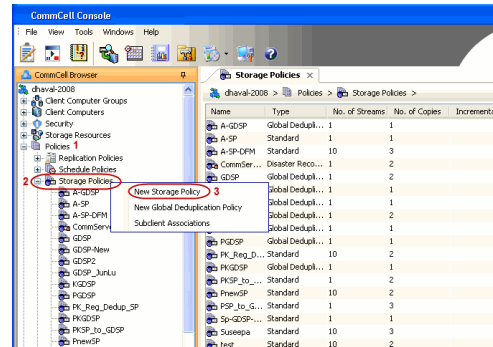
CONFIGURATION

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

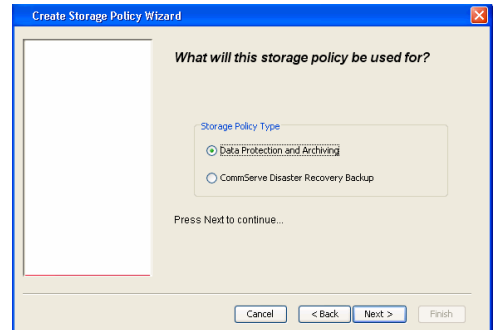
CREATE STORAGE POLICY

Use the following steps to create a storage policy.

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



- Click **Next**.



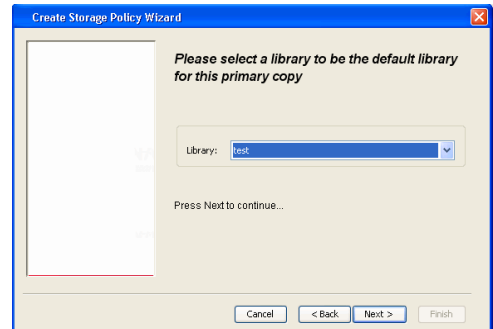
- Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
 - Select **Provide the DataFabric Manager Server Information**.
 - Click **Next**.



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

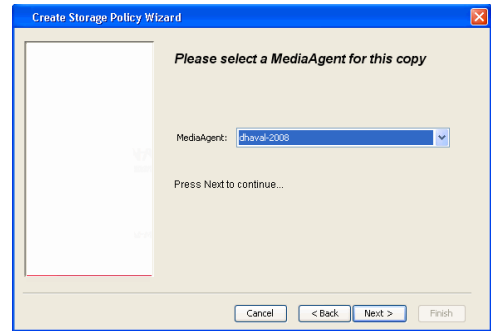
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

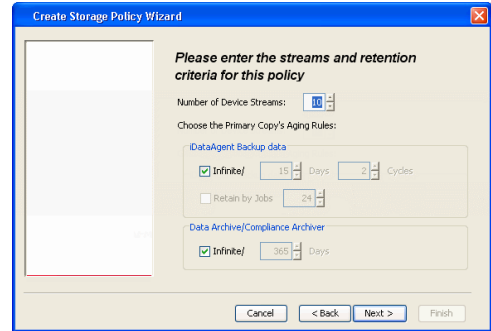


- Select a MediaAgent from the **MediaAgent** list.
 - Click **Next**.

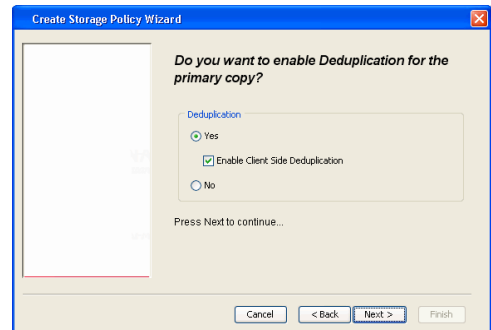
6. Click **Next**.



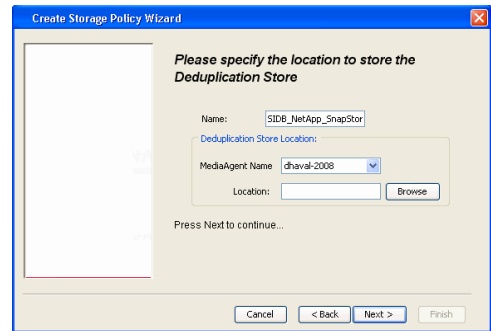
7. Click **Next**.



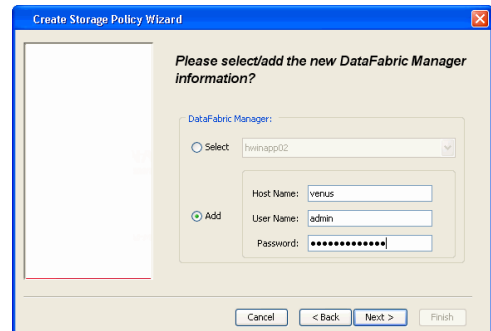
- 8.
- Verify **Name** and **MediaAgent Name**.
 - Click **Browse** to specify location for **Deduplication Store**.
 - Click **Next**.

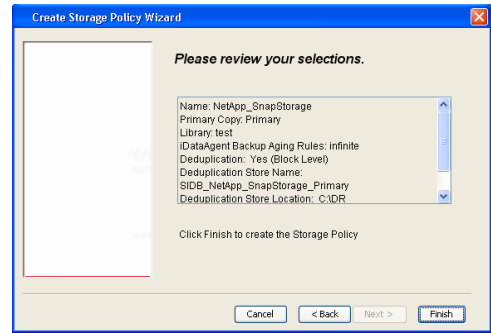


- 9.
- Provide the DataFabric Manager server information.
 - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
 - If you want to add a new DataFabric Manager Server, click **Add**.
 - Click **Next**.



10. Click **Finish**.



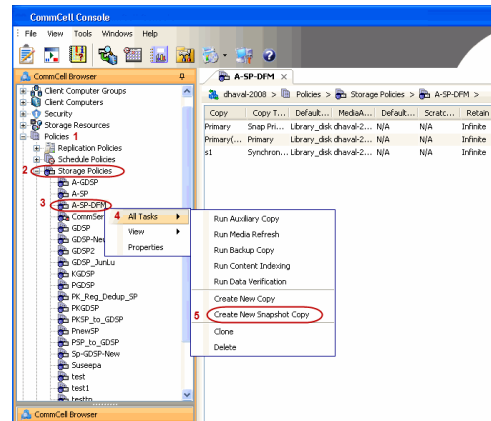


11. The new Storage Policy creates the following:
 - **Primary Snap Copy**, used for local snapshot storage
 - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

CREATE A SECONDARY SNAPSHOT COPY

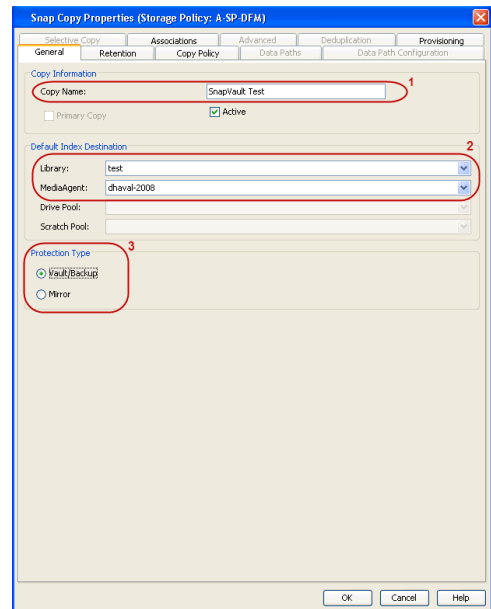
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

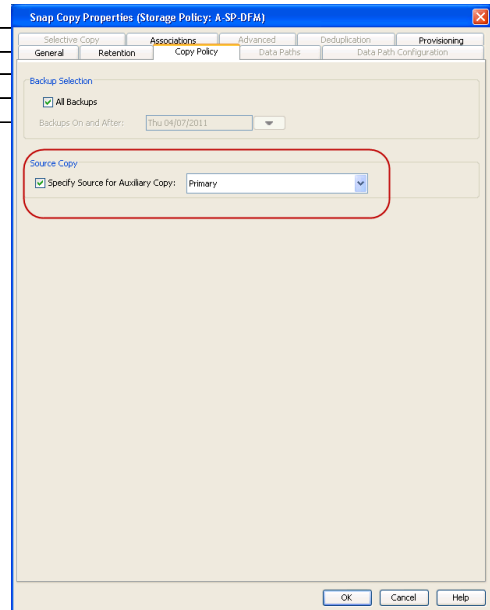


3.
 - Click the **Copy Policy** tab.
 - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

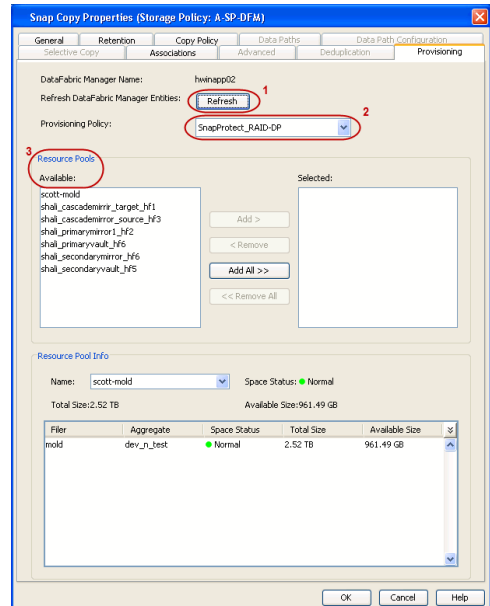
TOPOLOGY	SOURCE COPY
----------	-------------

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.

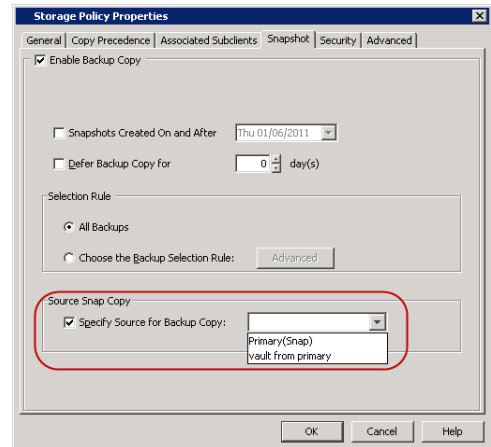
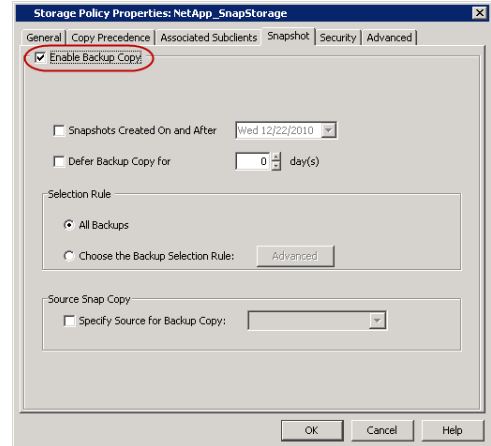
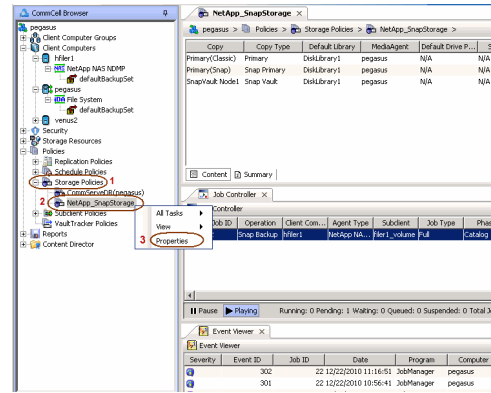
CONFIGURE BACKUP COPY

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.

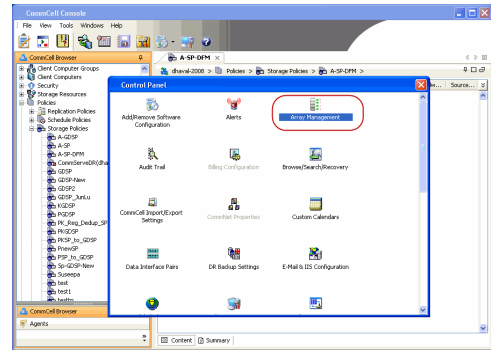


SETUP THE ARRAY INFORMATION

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**.

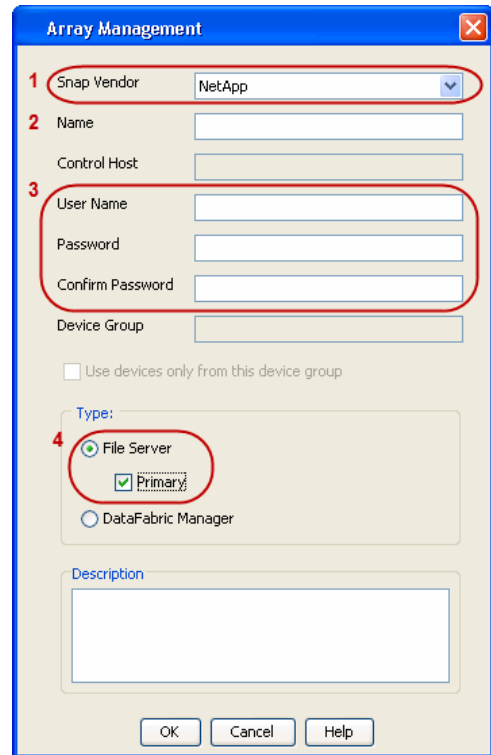
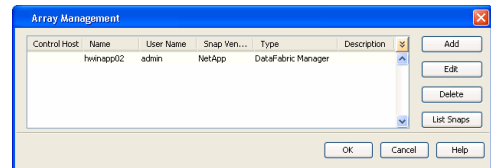


3.
 - Select **NetApp** from the **Snap Vendor** list.
 - Specify the name of the primary file server in the **Name** field.

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.

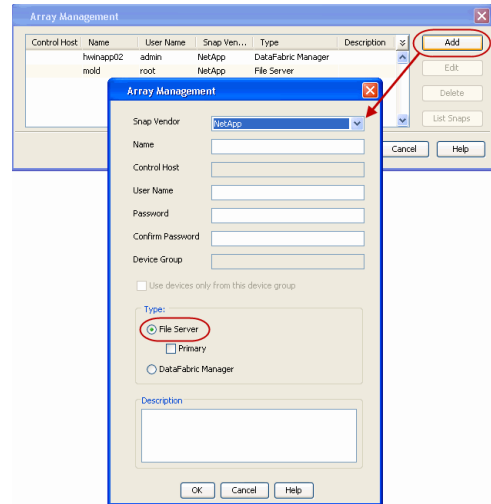
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

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:

1.
 - From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **DB2** | **<Instance>**
 - Right-click the subclient and click **Backup**.

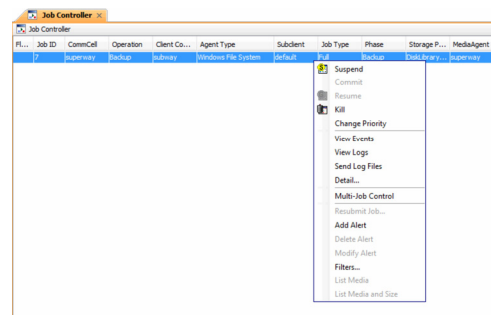
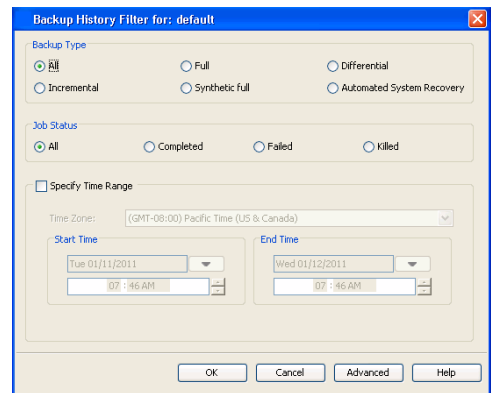
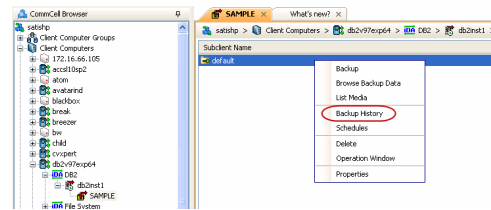
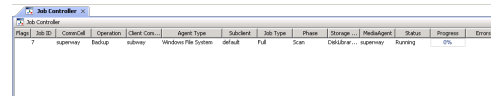
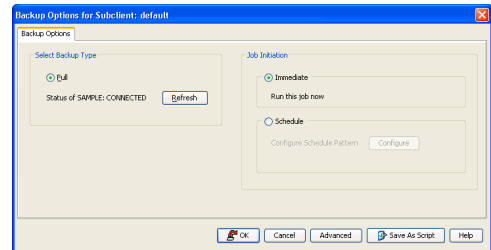
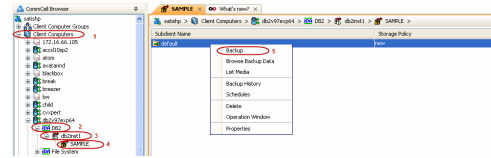
2.
 - Select **Full** as backup type and **Immediate** to run the job immediately.
 - Click **OK**.

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

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

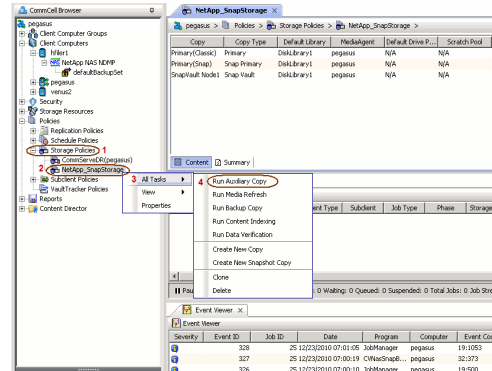
SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.

Click **Next** ▶ to Continue.

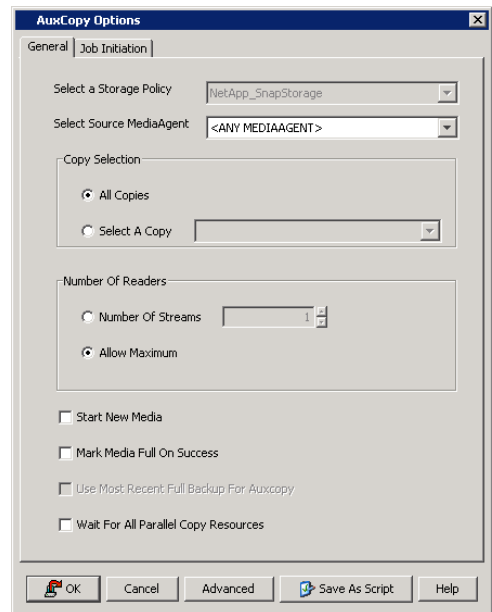
INITIATE VAULT/MIRROR COPY

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**.

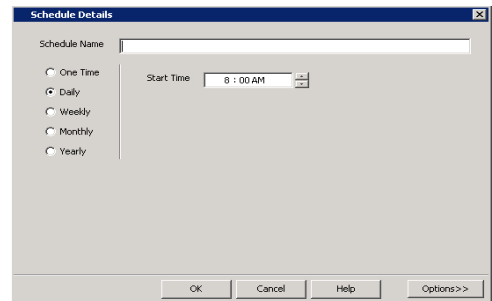


- Select the desired options and click the **Job Initiation** tab.
 - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

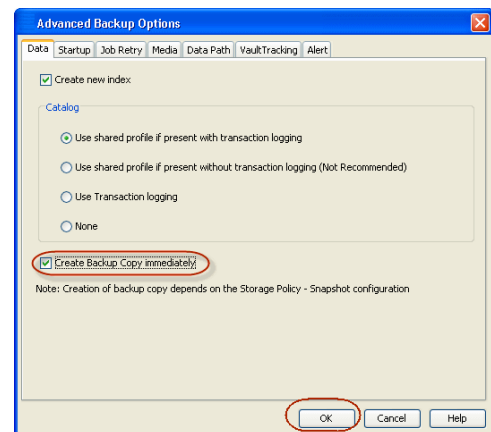
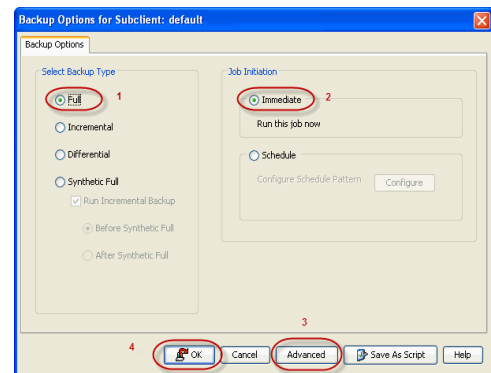
INLINE BACKUP COPY

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**.

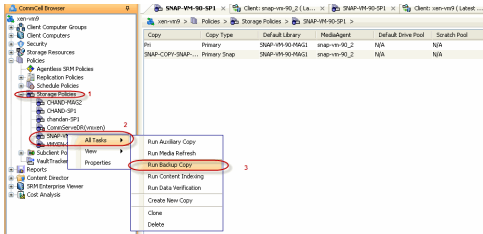
2.
 - Select **Create Backup Copy immediately** to create a backup copy.
 - Click **OK**.



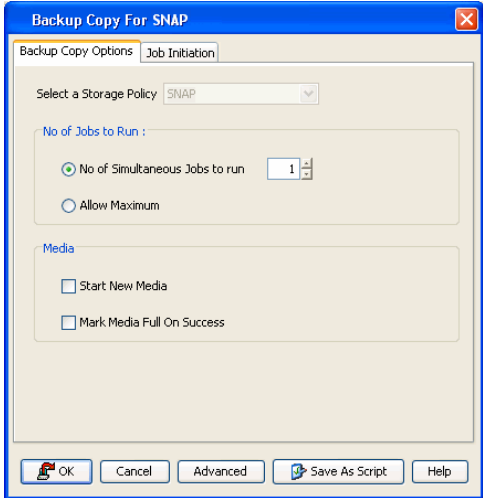
OFFLINE BACKUP COPY

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 - DB2 Restore

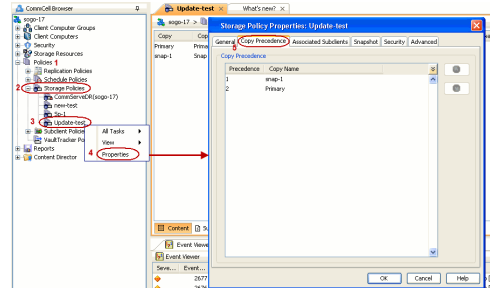
PERFORM A RESTORE

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.

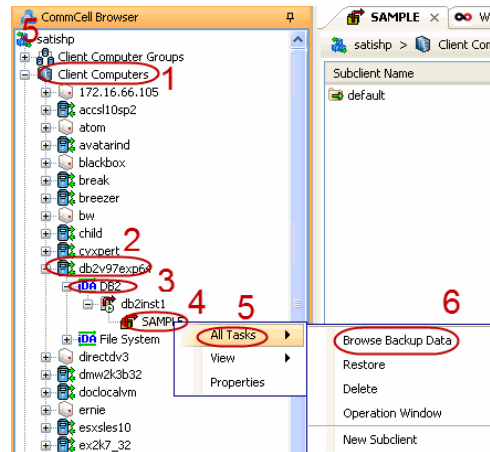
The following sections explain the steps for restoring the entire database to a different computer.

- 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.

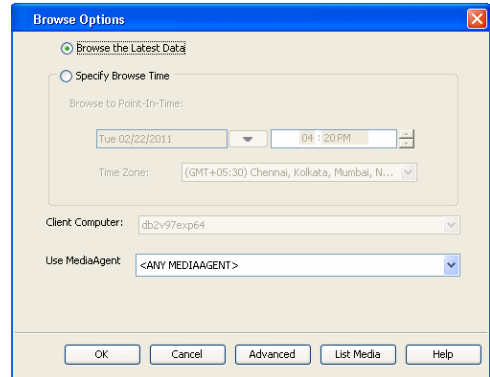
You can also use a different copy for performing the operation. For the copy that you want to use, set the copy precedence as 1.
 - Click **OK**.



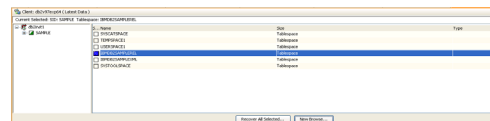
- From the CommCell Browser, navigate to **Client Computers | <Client> | DB2**.
 - Right-click the backup set and then click **All Tasks | Browse Backup Data**.



- Click **OK**.

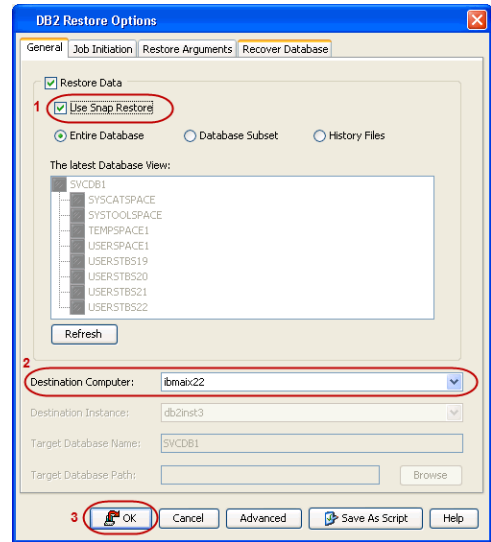


- Select the entire database in the left pane.
 - Click **Recover All Selected**.
- Select the **Use Snap Restore** checkbox to restore the database to a different computer.
 - Select the **Destination Computer** in which to restore the entire database.

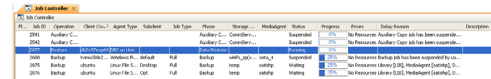


Ensure that the source and destination computers have the same directory structure and user/group IDs of the DB2 instance you are restoring.

- 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.

INSTALL THE UNIX FILE SYSTEM /DATAAGENT

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** 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.
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.

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.

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]
```

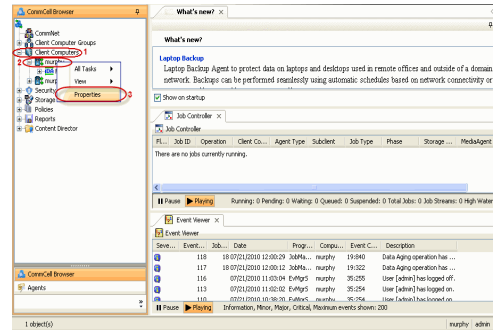


# Getting Started - Unix File System Configuration

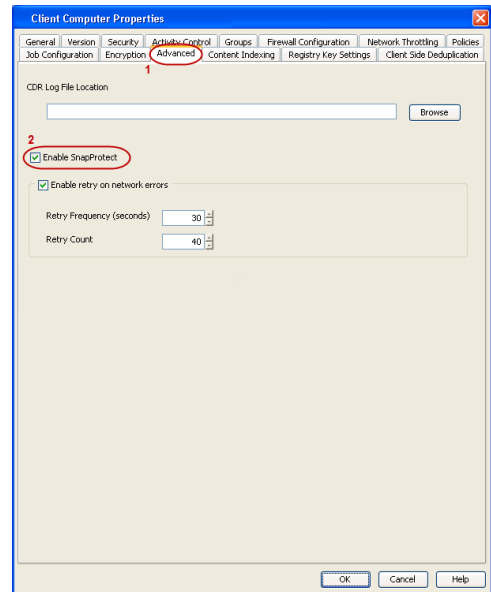
## CONFIGURATION

Once installed, the Linux File System *iDataAgent* requires some additional configuration before running your first SnapProtect backup. Follow the steps given below to complete the configuration for this Agent.

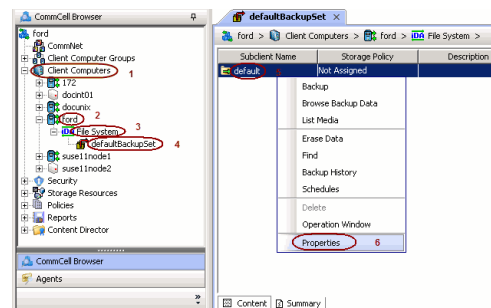
- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
  - Right-click the client and select **Properties**.



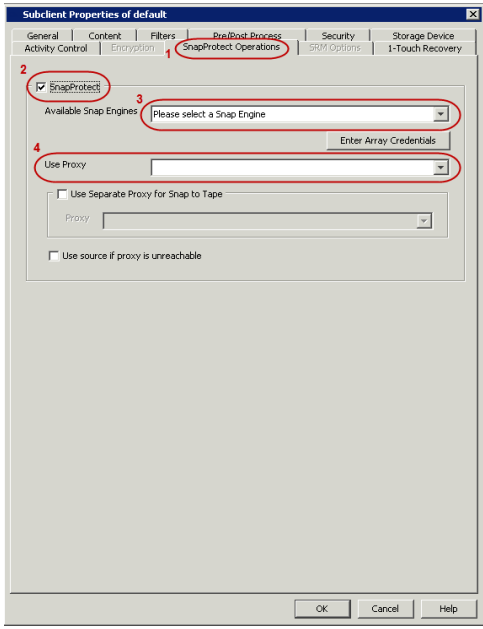
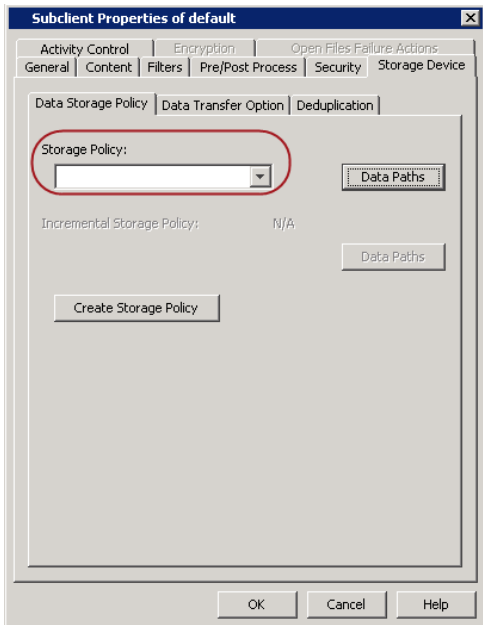
- Click on the **Advanced** tab.
  - Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
  - Click **OK**.



- From the CommCell Browser, navigate to **<Client>** | **File System**.
  - Right click the default 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.

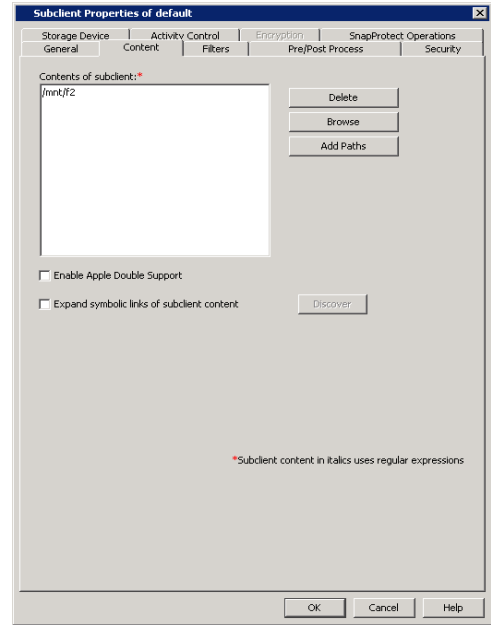
- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent. Select the MediaAgent from the **Proxy** list.

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 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.

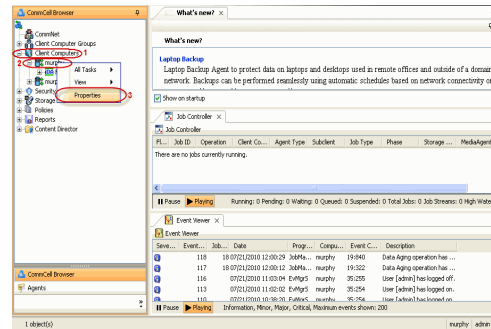
Click **Next** ➤ to Continue.

## ENABLE SNAPPROTECT BACKUPS ON SOLARIS ZONE

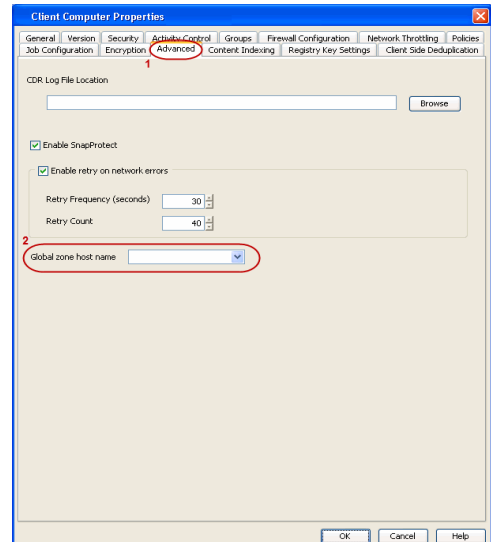
**Next** ➤

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.

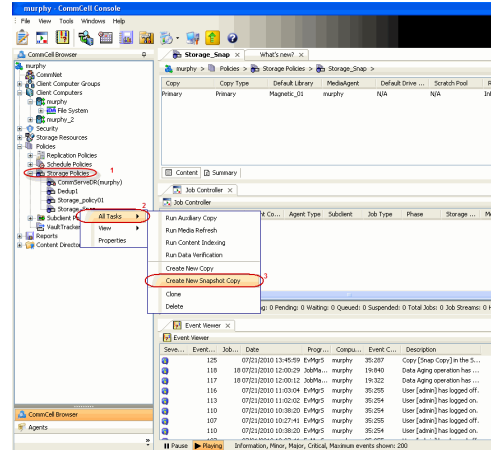
Click **Next** ➤ to Continue.

Next ➤

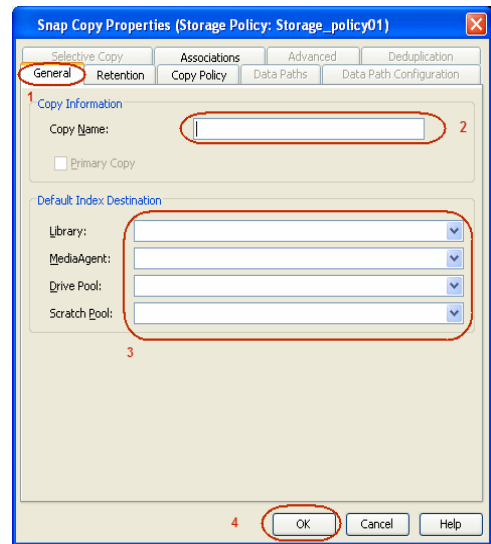
### CREATE A SNAPSHOT COPY

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**.



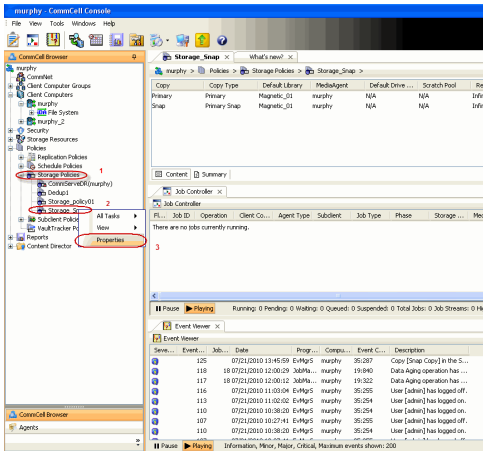
- Enter the copy name in the **Copy Name** field.
  - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
  - Click **OK**.



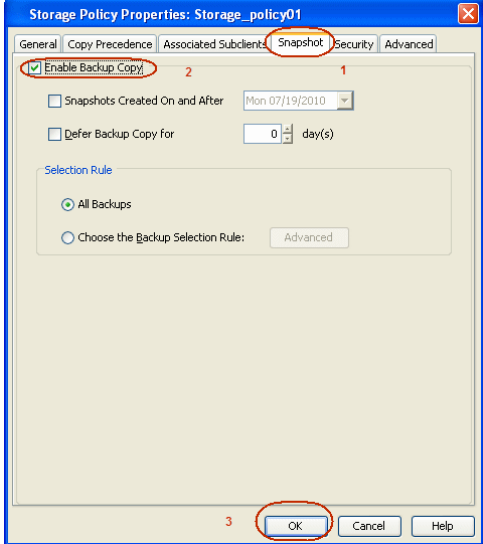
### CONFIGURE BACKUP COPY

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

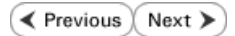
◀ Previous   Next ▶

## 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



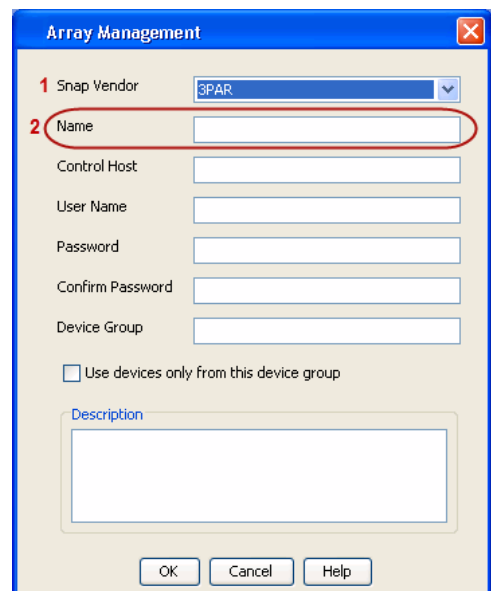
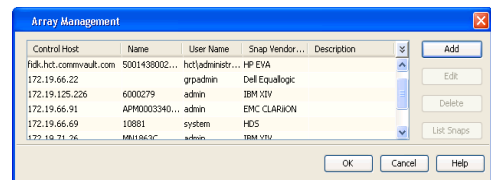
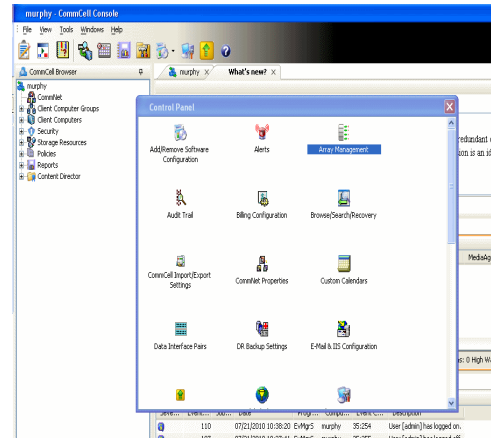
## PRE-REQUISITES

- 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

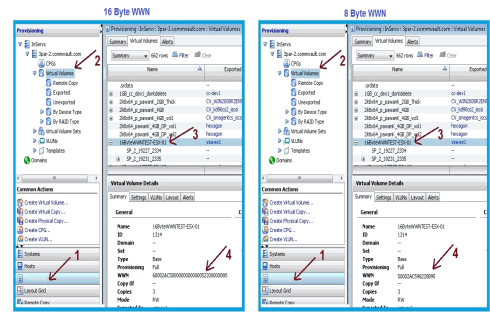
where  $\text{DevID.substr}(26,6)$  is the next 6 digits after the twenty sixth digit from the WWN number

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

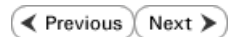
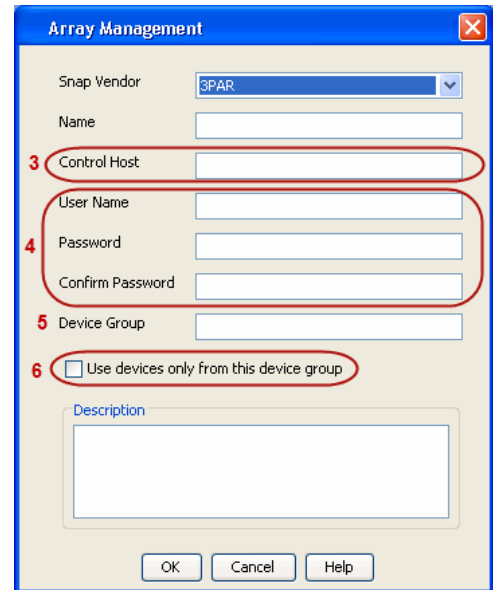
After adding all the values, the resulting array name is 2FF70002AC000B95.



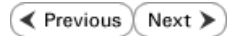
- Enter the IP address of the array in the **Control Host** field.
  - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the CPG group created on the array to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

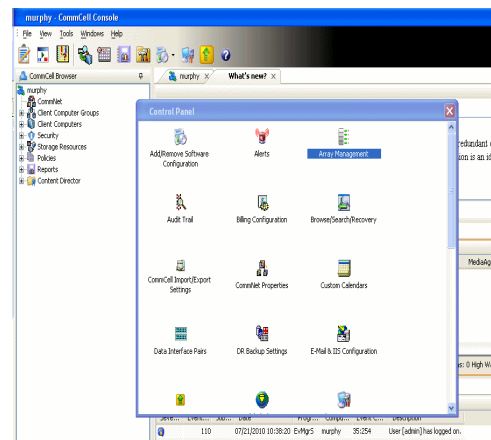
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
  - Create a new group administration account in the firmware, and set the desired permissions for this account.
  - If you plan to use the existing 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.

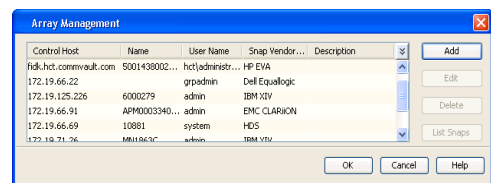
## SETUP THE ARRAY INFORMATION

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**.

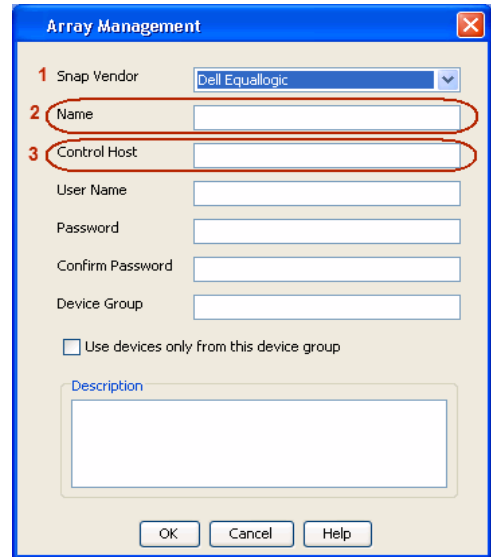


2. Click **Add**.

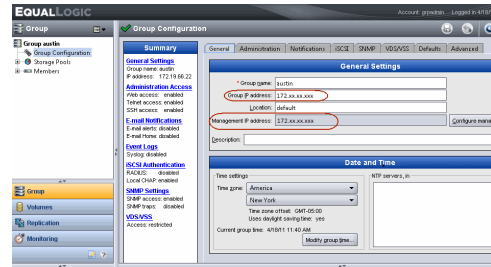


3.
  - Select **Dell Equallogic** from the **Snap Vendor** list.
  - Specify the Management IP address in the **Name** field.
 

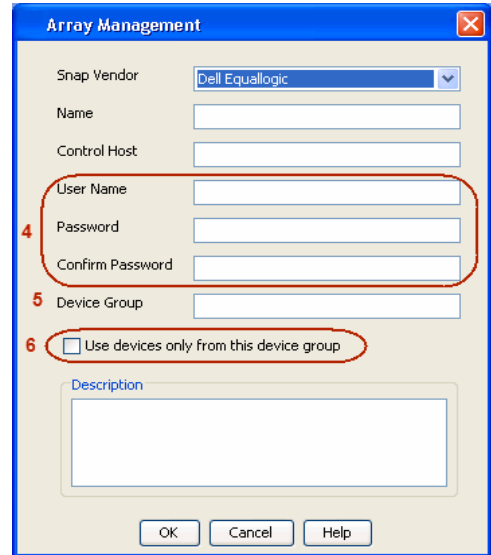
No entry is required in the **Name** field if there is no Management IP address configured.
  - Specify the Group IP address in the **Control Host** field.



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:

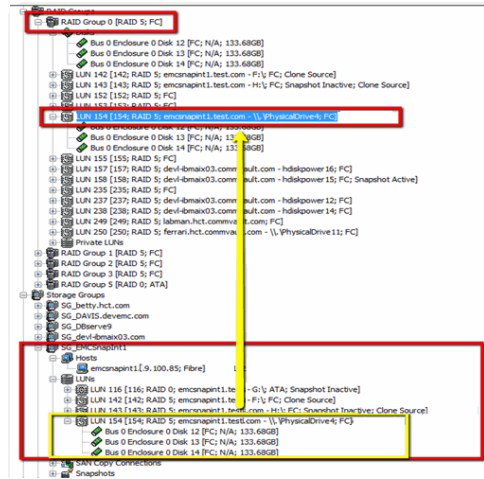
1. Create a RAID group
2. Bind the LUN
3. Create a Storage Group
4. Register the client computer (covered by installing NaviAgent)
5. Map the LUNs to the client computer where the NaviAgent resides
6. Reserved/Clone volumes target properly for SnapView

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.

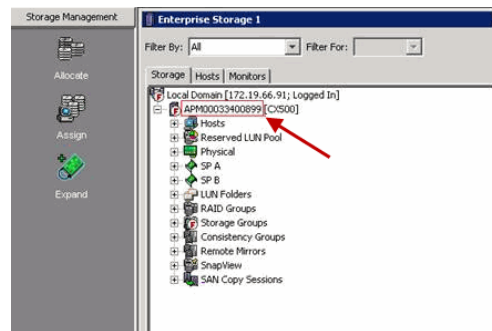
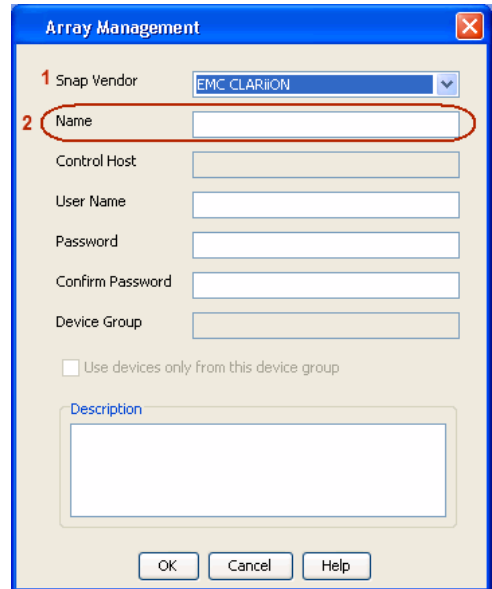
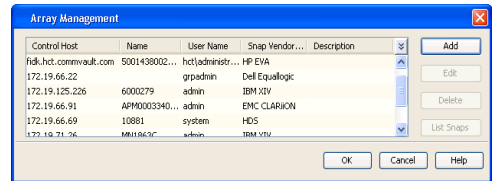
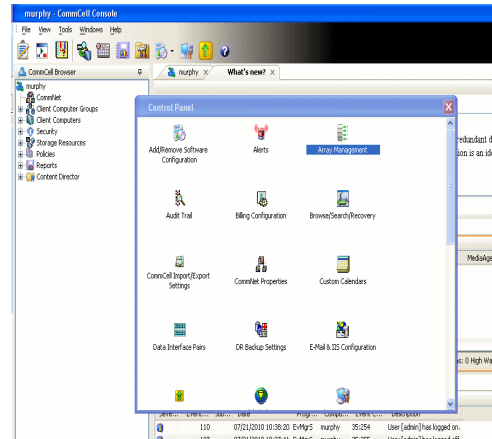
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

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

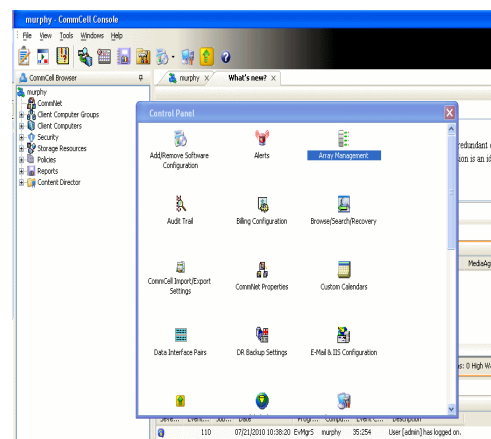
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

## SETUP THE ARRAY INFORMATION

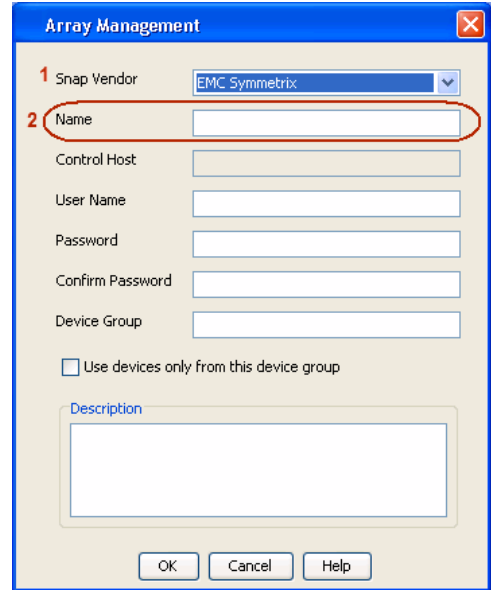
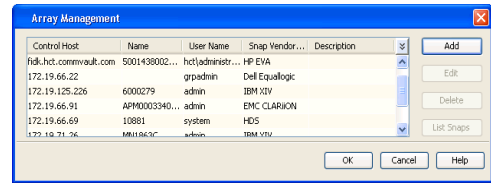
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

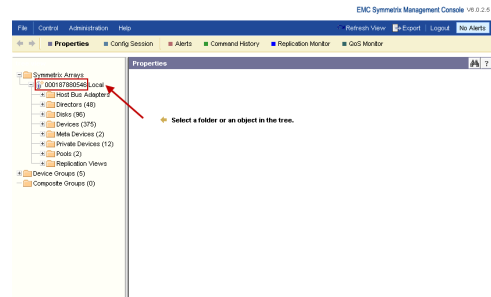


2. Click **Add**.

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

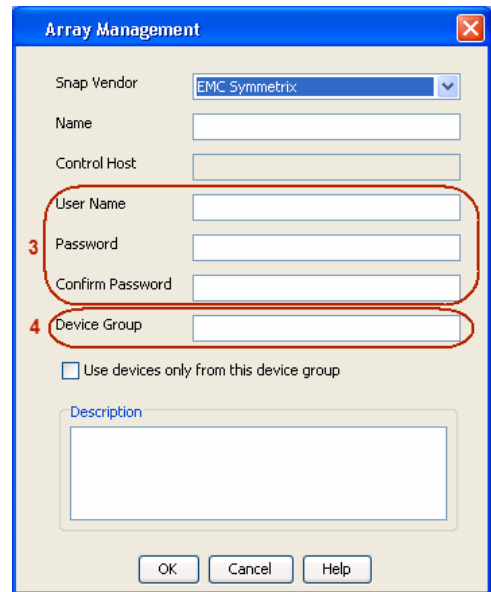


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



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



## 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

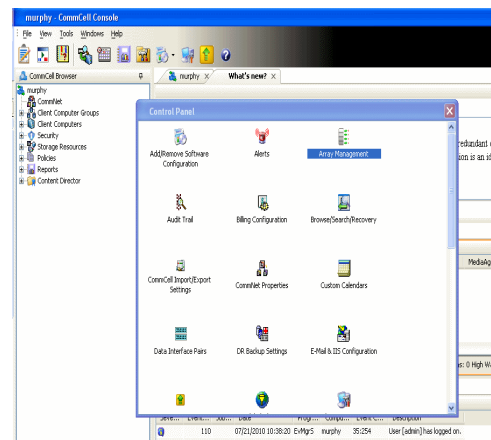
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

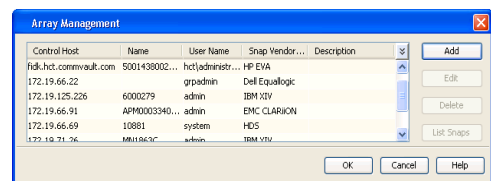
## SETUP THE ARRAY INFORMATION

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

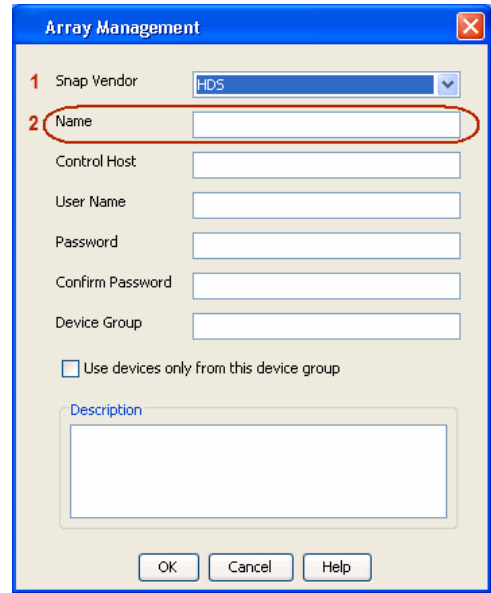
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



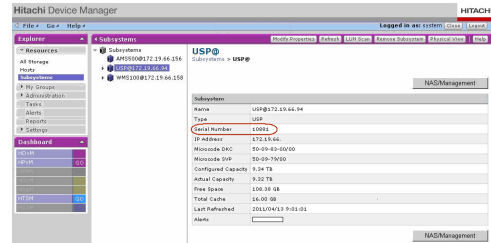
2. Click **Add**.



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.



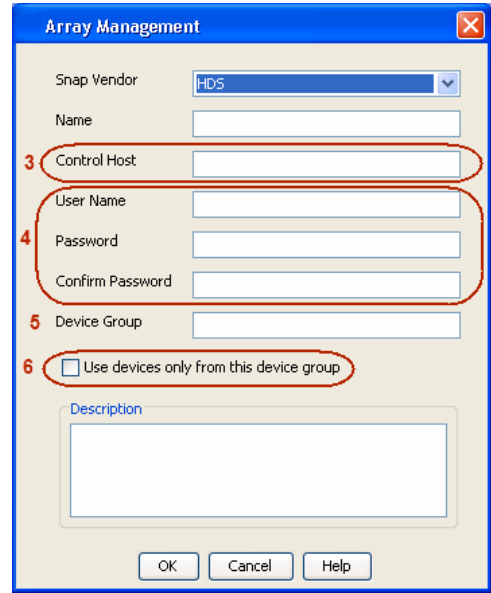
4.
  - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
  - Enter the user access information in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for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

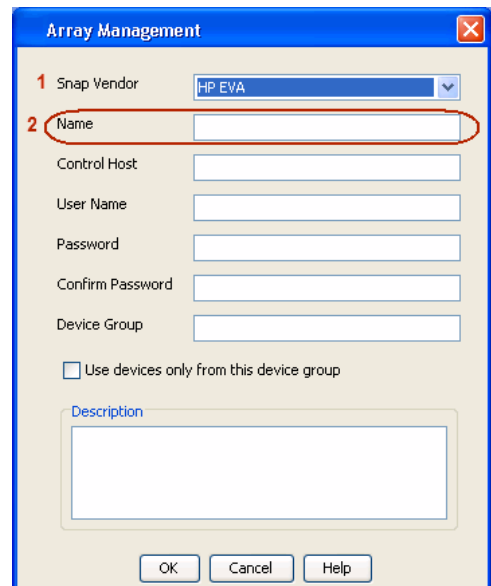
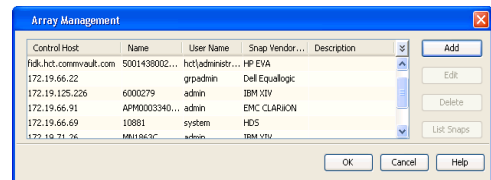
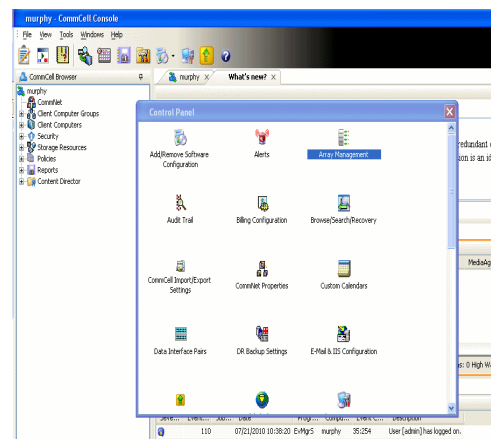
The following steps provide the necessary instructions to setup the HP EVA:

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

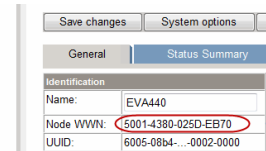
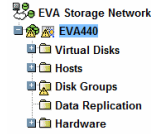
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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.

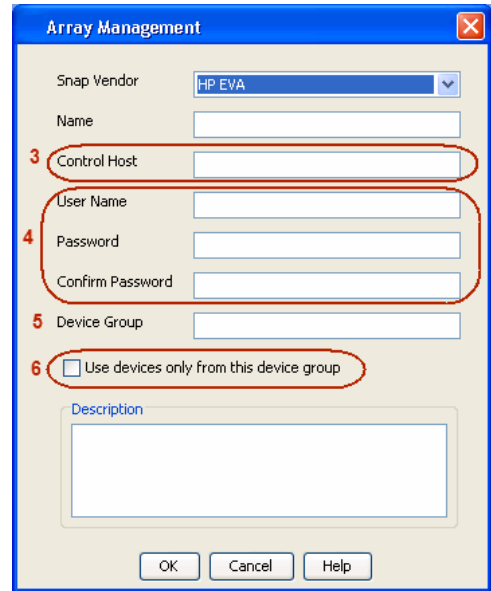
The array name must be specified without the dashes used in the WWN e.g., 50014380025DEB70.



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 ▶

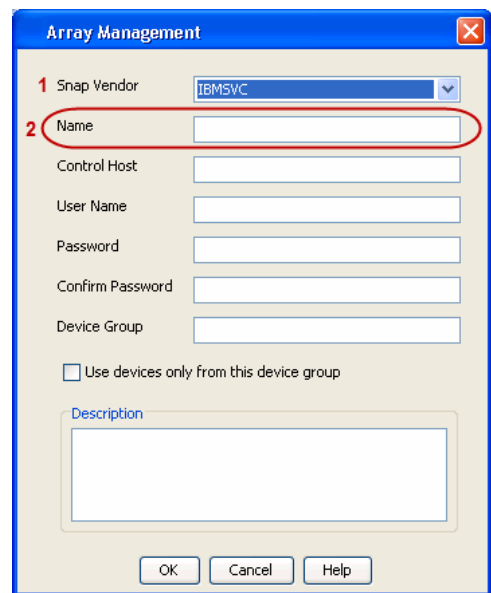
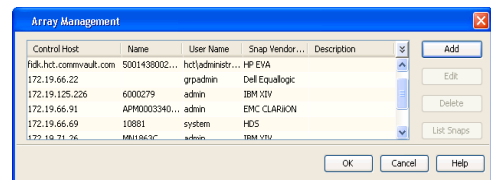
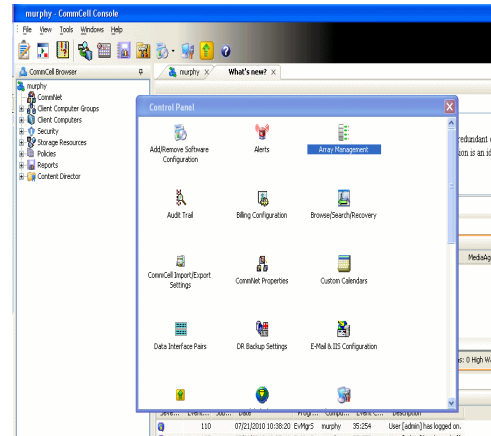
## PRE-REQUISITES

- 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.

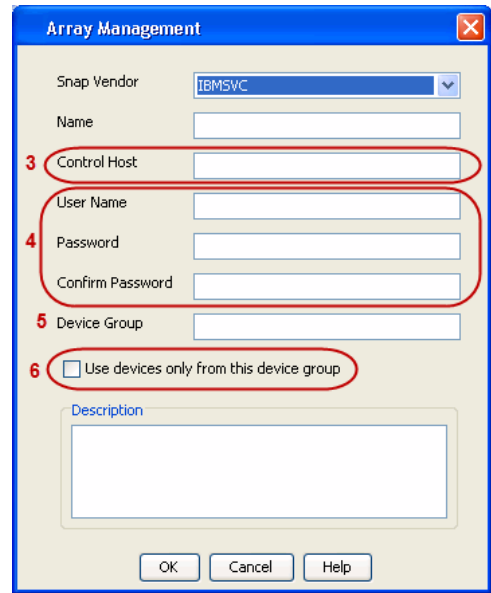
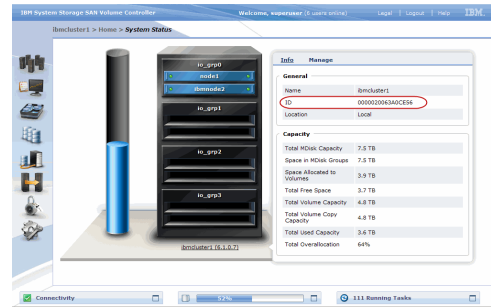
- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
  - Specify the 16-digit ID of the storage device in the **Name** field.



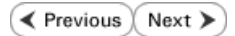
The **ID** is the device identification number for the IBM SVC storage device. See the screenshot on the right for reference.

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



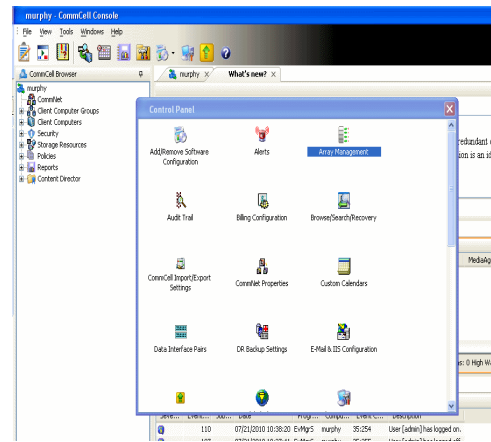
## PRE-REQUISITES

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.

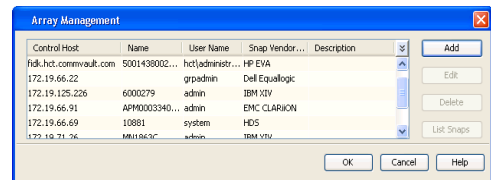
## SETUP THE ARRAY INFORMATION

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

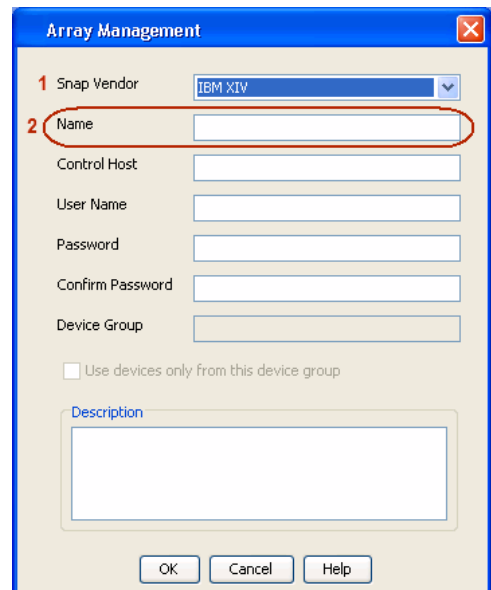
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.



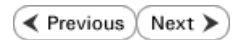
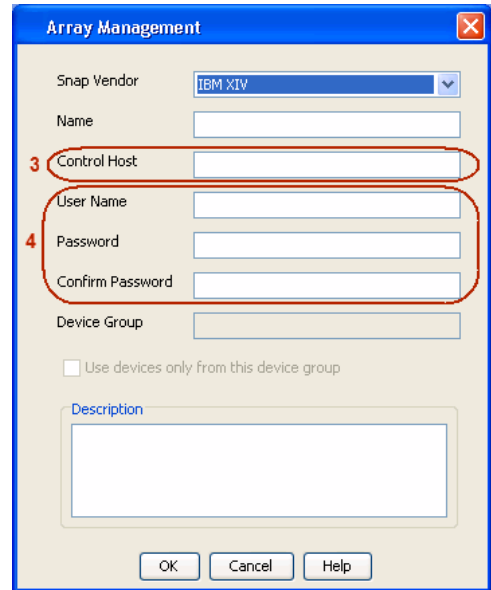
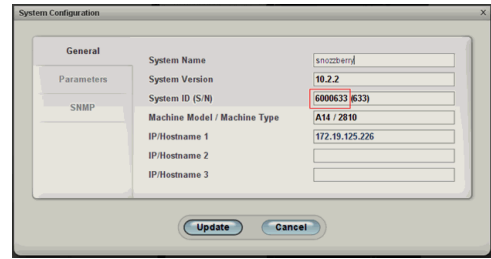
3.
  - Select **IBM XIV** from the **Snap Vendor** list.
  - Specify the 7-digit serial number for the array in the **Name** field.



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.

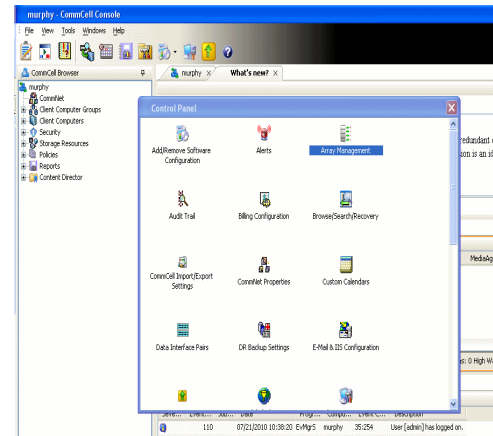
## ADDITIONAL REQUIREMENTS FOR VMWARE

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.

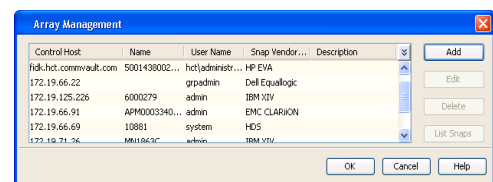
## SETUP THE ARRAY INFORMATION

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

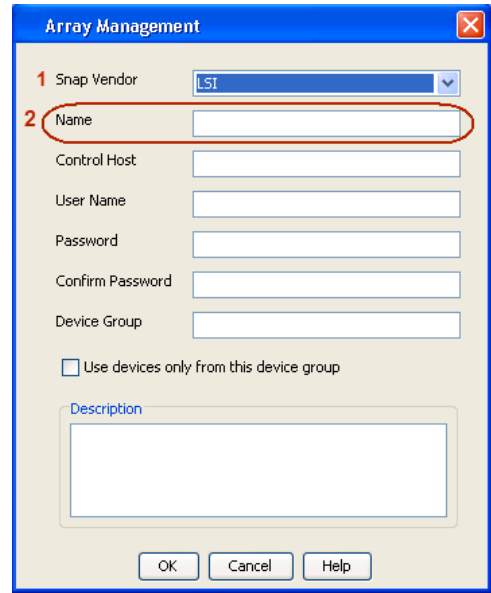
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

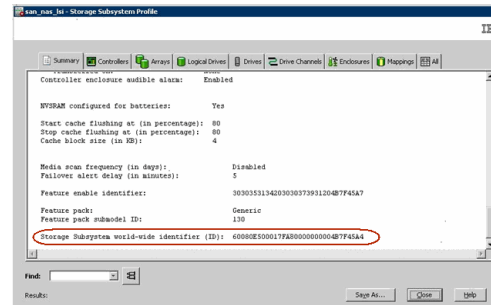


3.
  - Select **LSI** from the **Snap Vendor** list.
  - Specify the serial number for the array in the **Name** field.



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

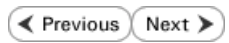
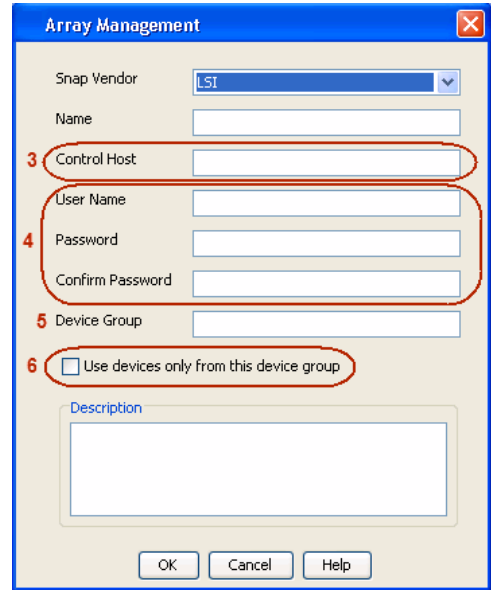
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



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 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

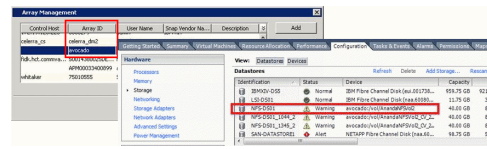
### LICENSES

- 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.

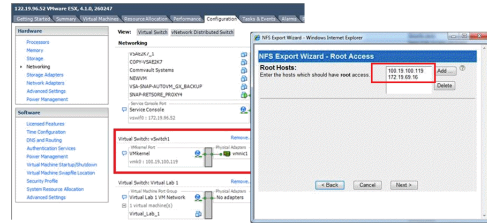
## ADDITIONAL REQUIREMENTS FOR VMWARE

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.



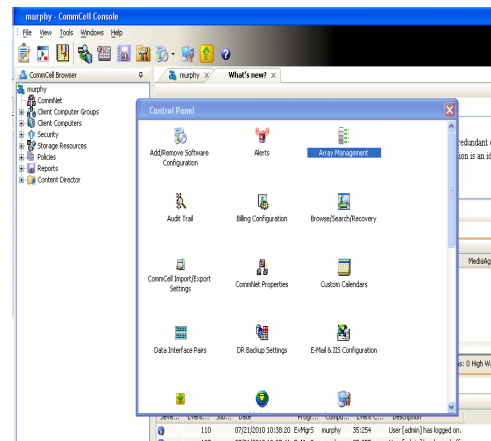
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



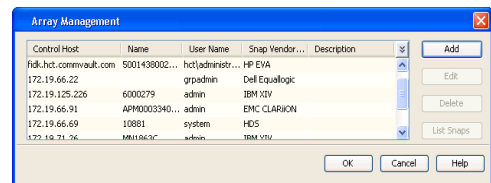
## SETUP THE ARRAY INFORMATION

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

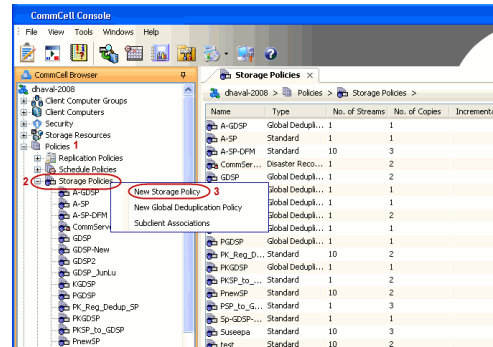
## CONFIGURATION

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

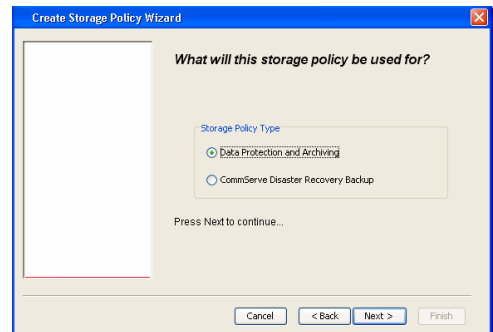
## CREATE STORAGE POLICY

Use the following steps to create a storage policy.

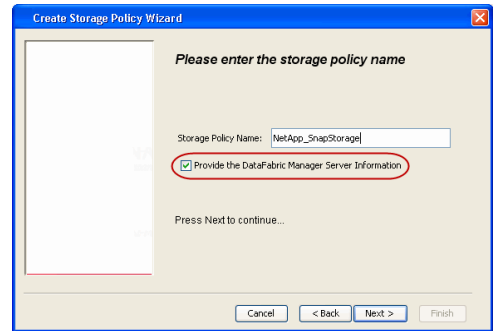
1.
  - From the CommCell Browser, navigate to **Policies**.
  - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



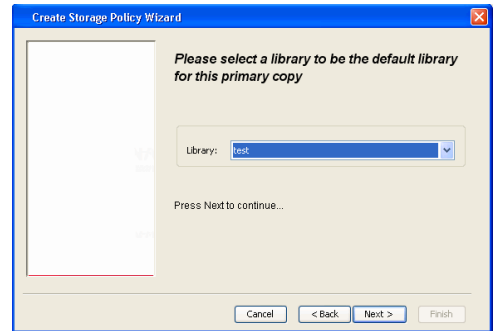
3.
  - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
  - Select **Provide the DataFabric Manager Server Information**.
  - Click **Next**.



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

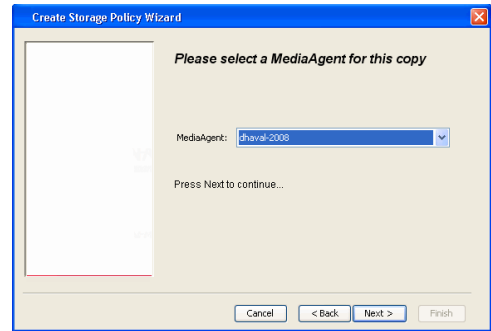
It is recommended that the selected disk library uses a LUN from the File server.

- Click **Next**.

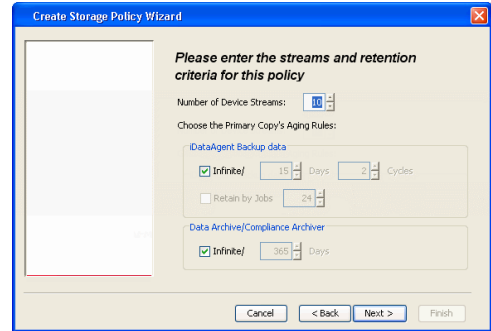


5.
  - Select a MediaAgent from the **MediaAgent** list.
  - Click **Next**.

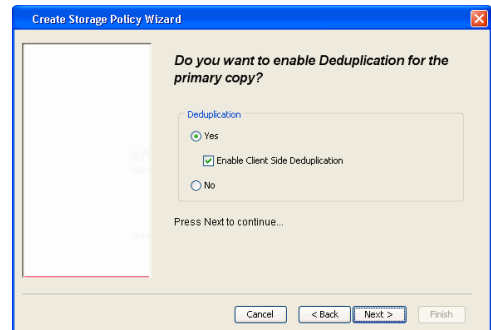
6. Click **Next**.



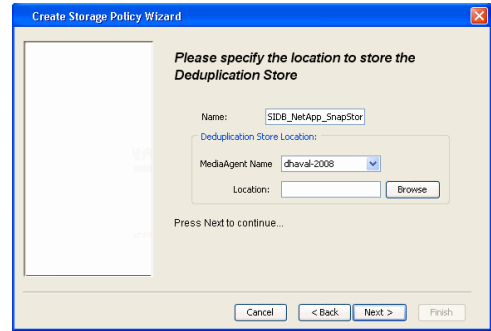
7. Click **Next**.



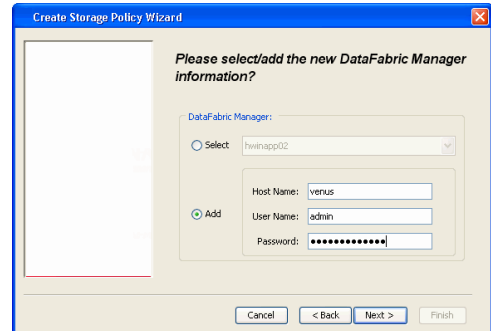
- 8.
- Verify **Name** and **MediaAgent Name**.
  - Click **Browse** to specify location for **Deduplication Store**.
  - Click **Next**.

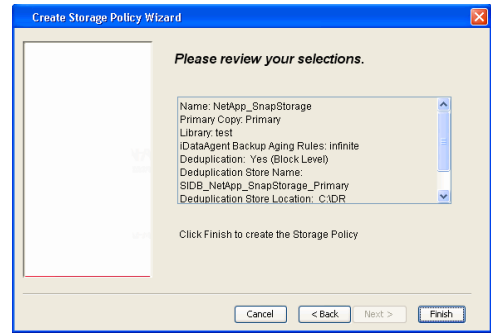


- 9.
- Provide the DataFabric Manager server information.
    - If a DataFabric Manager server exists, click **Select** to choose from the drop-down list.
    - If you want to add a new DataFabric Manager Server, click **Add**.
  - Click **Next**.



10. Click **Finish**.



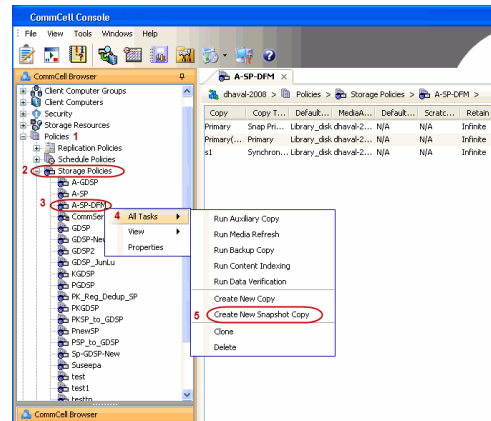


11. The new Storage Policy creates the following:
  - **Primary Snap Copy**, used for local snapshot storage
  - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

### CREATE A SECONDARY SNAPSHOT COPY

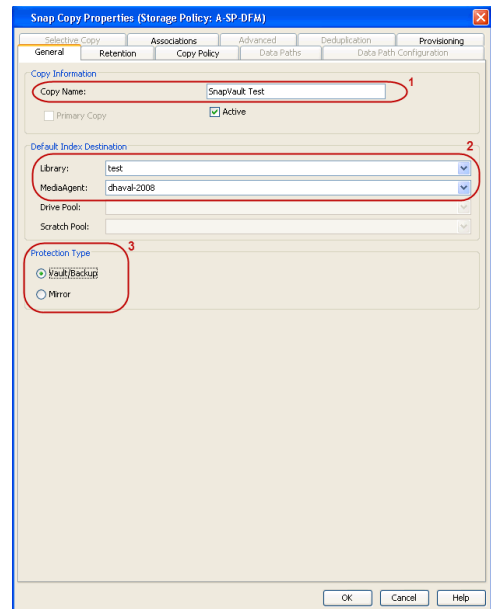
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

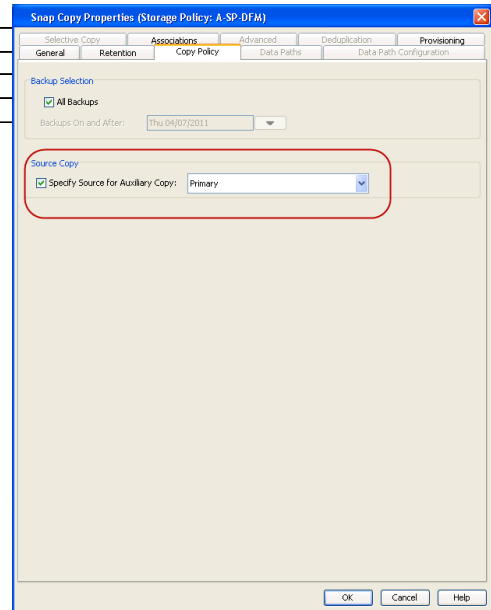


3.
  - Click the **Copy Policy** tab.
  - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

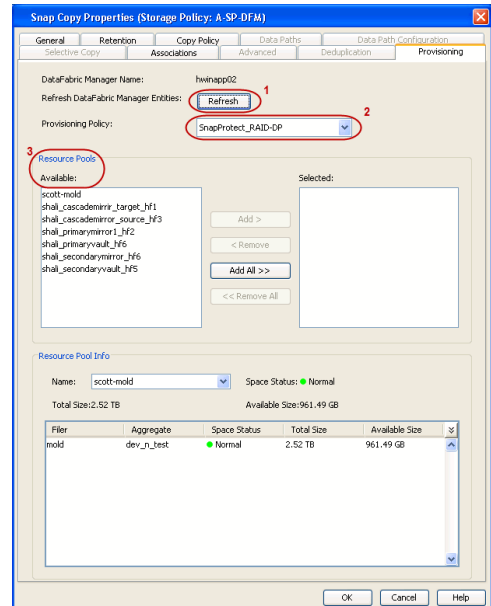
| TOPOLOGY | SOURCE COPY |
|----------|-------------|
|----------|-------------|

|                       |         |
|-----------------------|---------|
| 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.

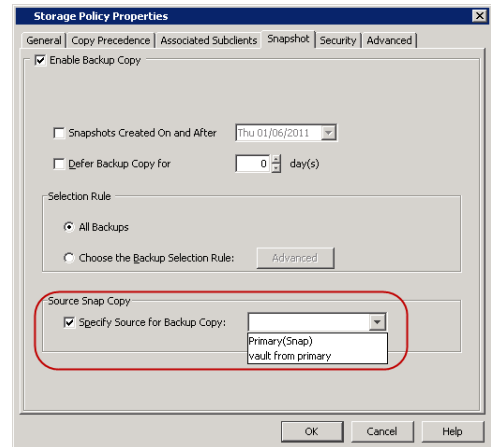
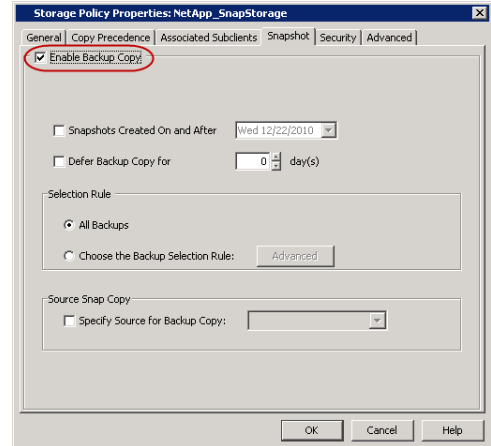
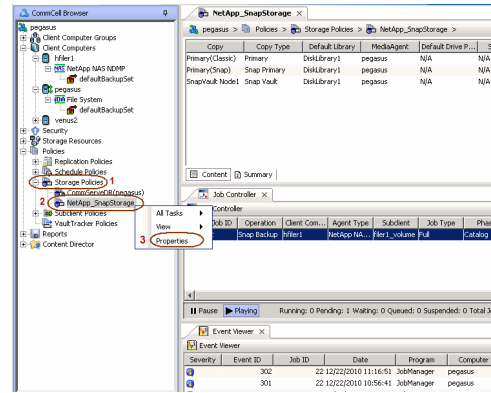
## CONFIGURE BACKUP COPY

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.

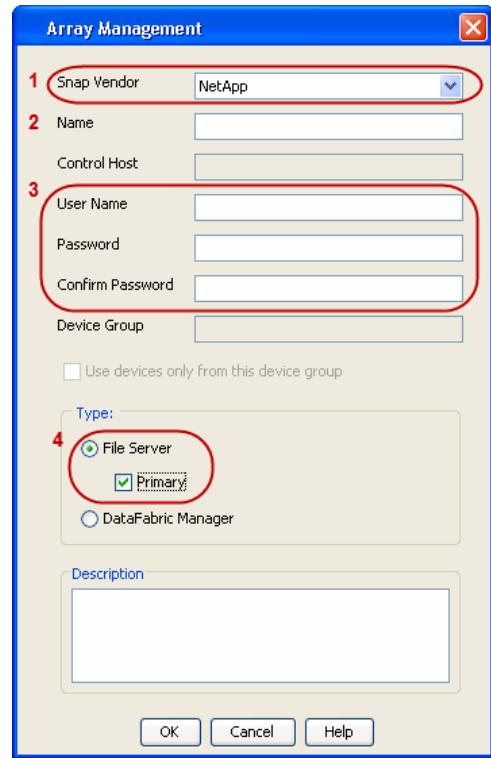
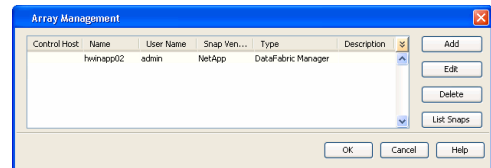
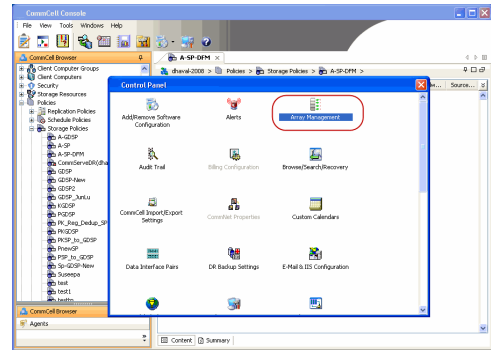
You can provide the host name, fully qualified domain name or TCP/IP address of the file server.

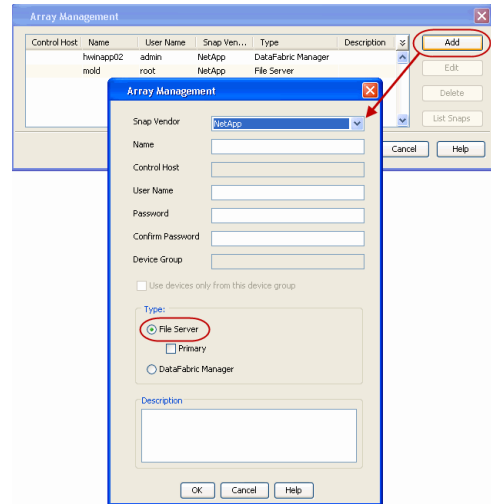
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

# 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.

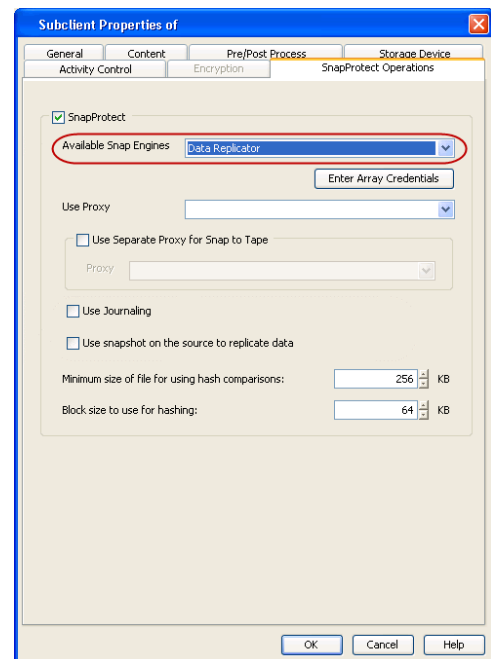
### STORAGE POLICY REQUIREMENTS

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

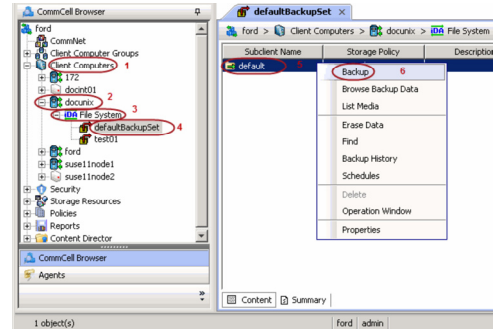
◀ Previous    Next ▶

## PERFORM A BACKUP

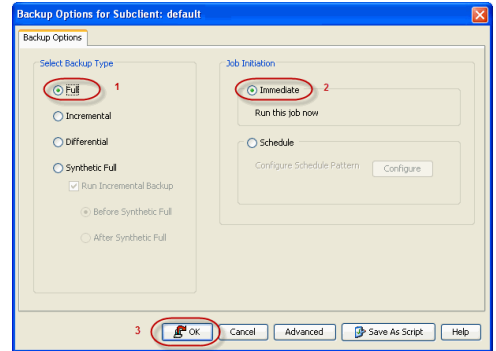
Once the storage policy is configured, you are ready to perform your first backup.

The following section provides step-by-step instructions for performing your first backup:

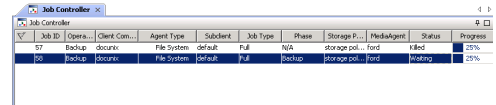
- From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.
  - Right-click the default subclient and click **Backup**.



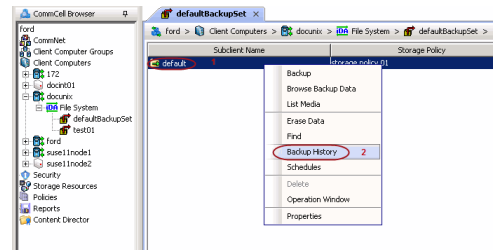
- Click **Full** as backup type and then click **Immediate**.
  - Click **OK**.



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



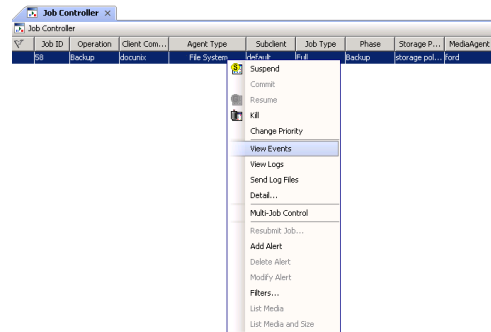
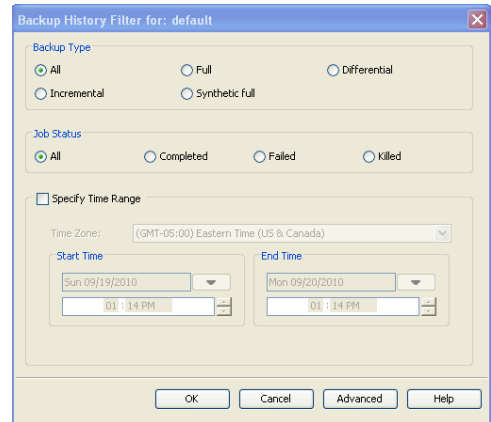
- Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.



- 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

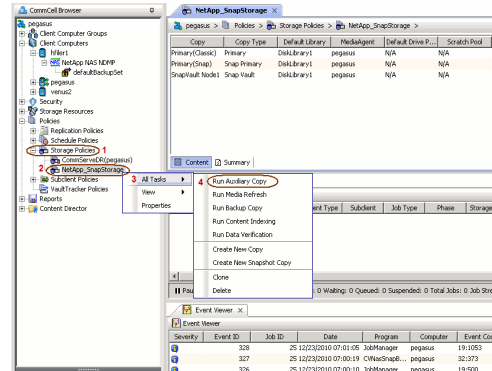
**SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.**

Click **Next** ▶ to Continue.

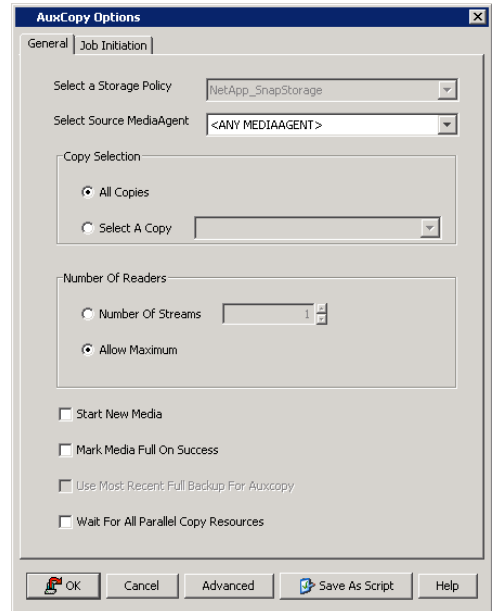
## INITIATE VAULT/MIRROR COPY

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**.

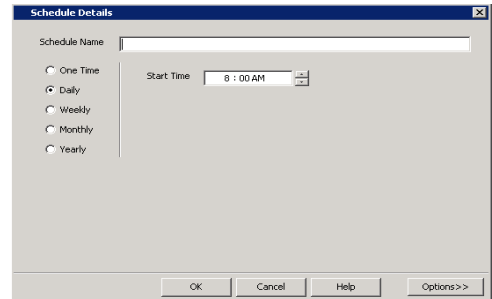


- Select the desired options and click the **Job Initiation** tab.
  - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

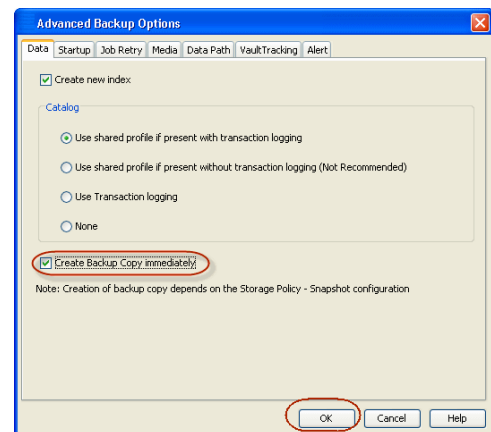
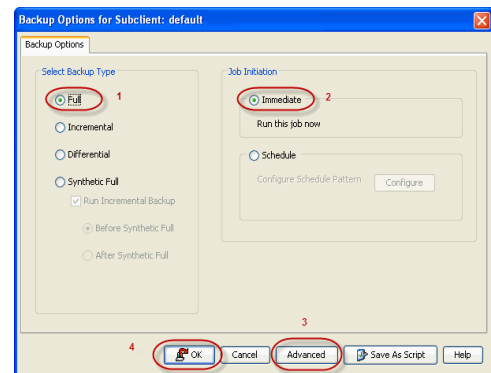
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

#### 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**.

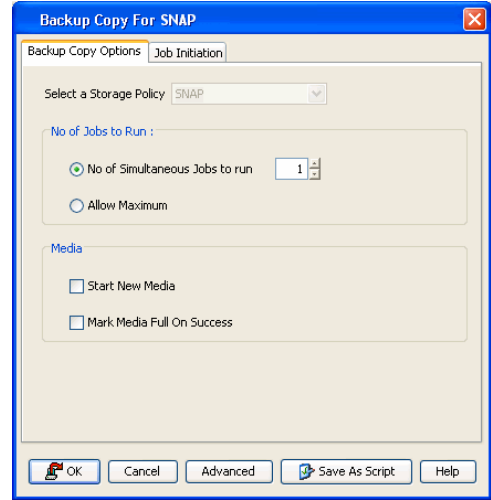
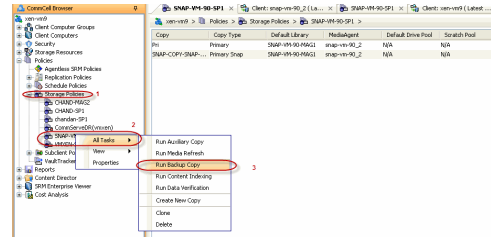


#### OFFLINE BACKUP COPY

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 - 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**.

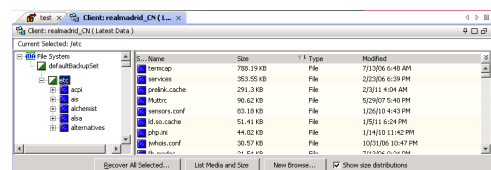
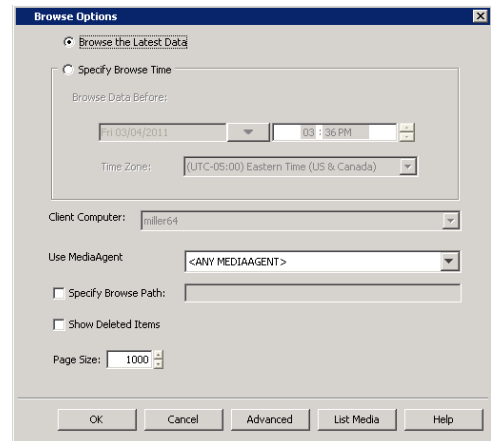
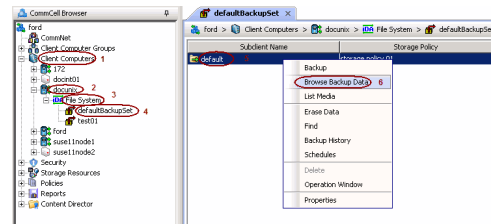
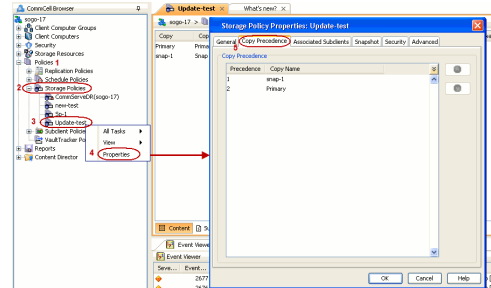
- Click **OK**.

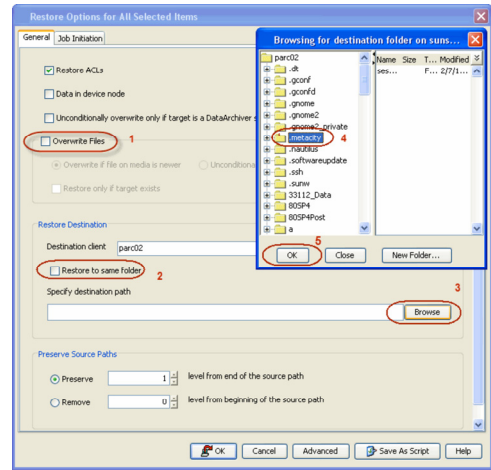
- Expand the **defaultBackupSet** and navigate to **etc** folder.
  - Select the **etc** folder.
  - Click **Recover All Selected**.

If you attempt to restore a running executable file, the application may crash and core dump.

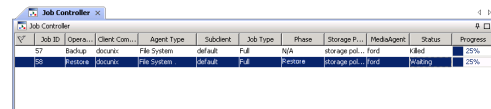
- Clear the **Overwrite Files** and **Restore to same folder** options.
  - Specify the destination path by clicking **Browse** button.
  - This will ensure that the existing files are not overwritten.
  - Click **OK**.

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**.



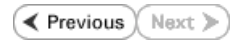
7. Once the File System is restored, verify that the restored files/folders are available in the restore destination

```
[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.

## 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**.

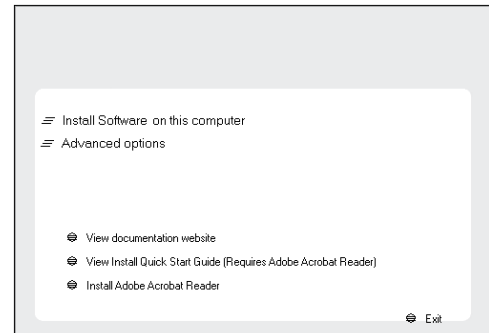
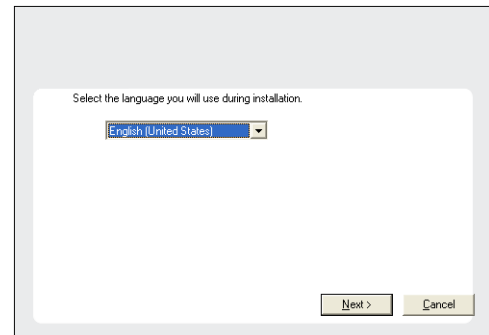
## BEFORE YOU BEGIN

### Download Software Packages

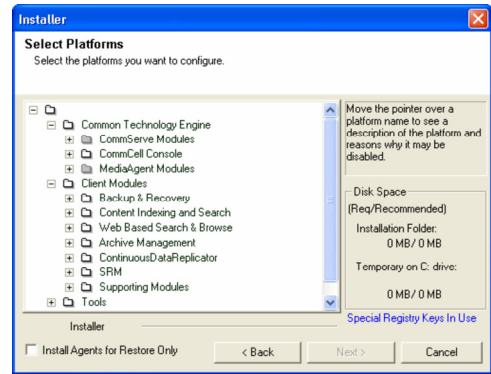
Download the latest software package to perform the install.

### SnapProtect Support - Platforms

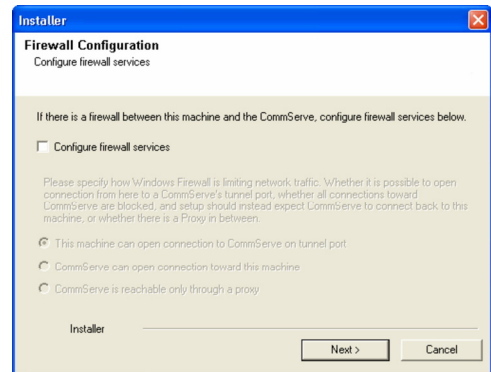
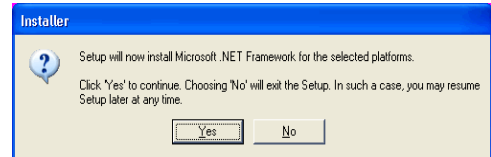
Make sure that the computer in which you wish to install the software satisfies the minimum requirements.



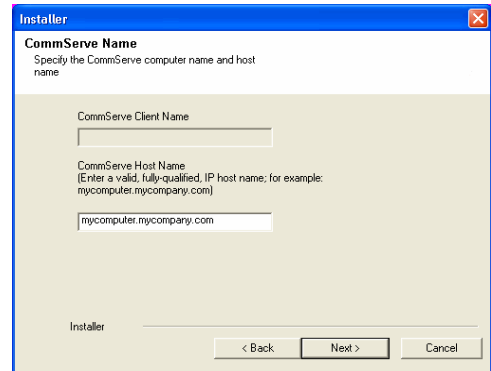
6. Click **YES** to install Microsoft .NET Framework package.
  - This prompt is displayed only when Microsoft .NET Framework is not installed.
  - Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.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



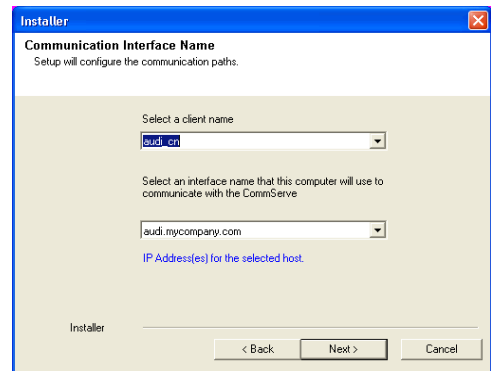
8. Enter the fully qualified domain name of the **CommServe Host Name**.  
 Click **Next**.  
 Do not use space and the following characters when specifying a new name for the CommServe Host Name:  
`\ | ` ~ ! @ # $ % ^ & * ( ) + = < > / ? , [ ] { } ; : ; " ' " "`



9. Click **Next**.



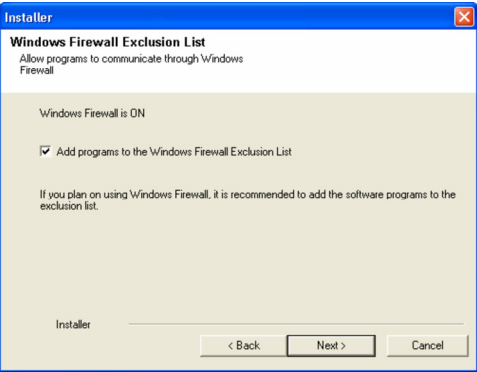
10. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.



Click **Next**.

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

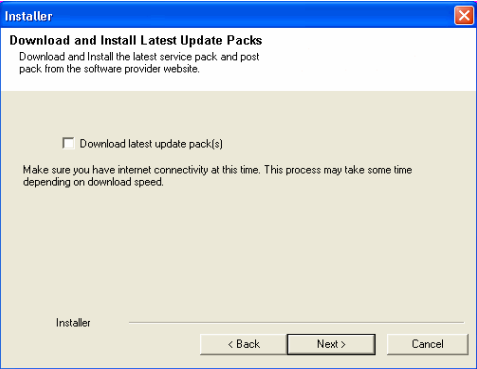
It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.



11. Click **Next**.

**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.

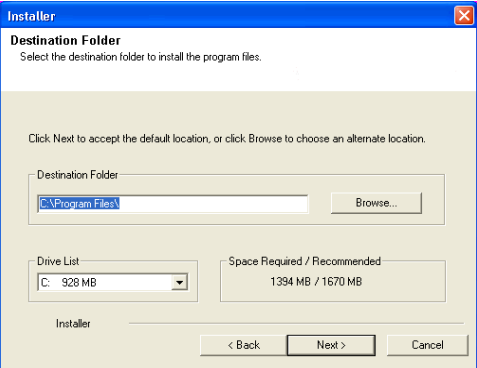
Click **Browse** to change the default location.

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:

/ : \* ? " < > | #

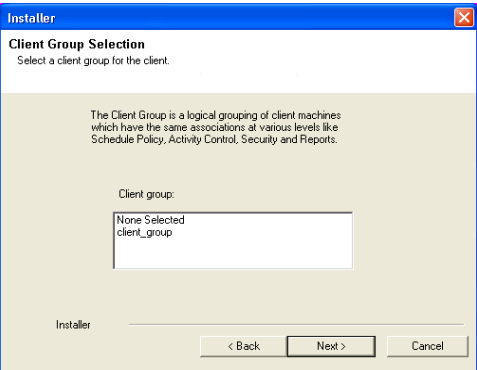
It is recommended that you use alphanumeric characters only.



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**.

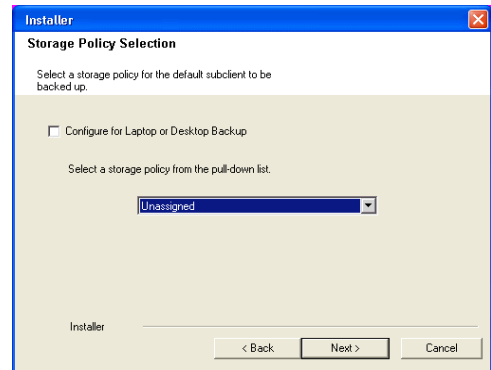
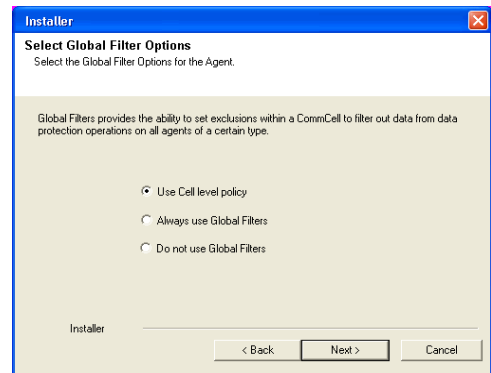
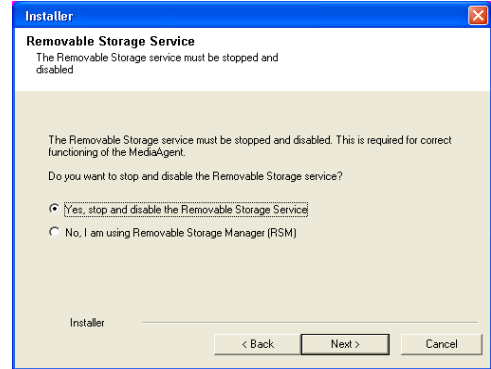
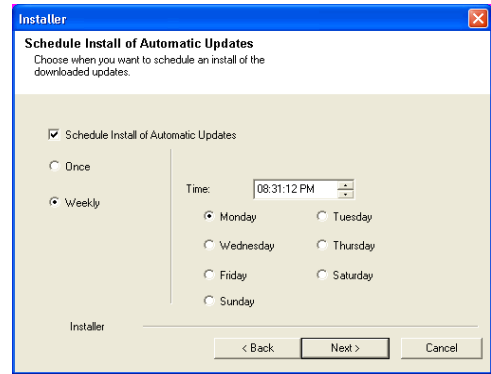
15. Select **Yes** to stop Removable Storage Services on the MediaAgent.  
Click **Next**.

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

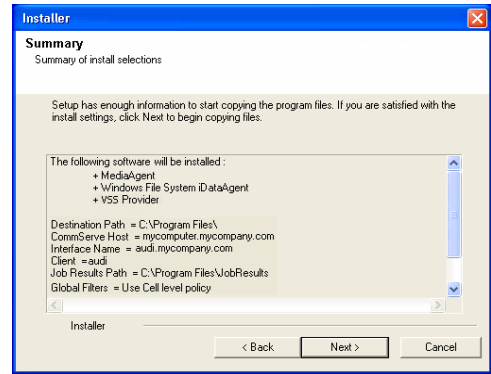
16. Click **Next**.

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

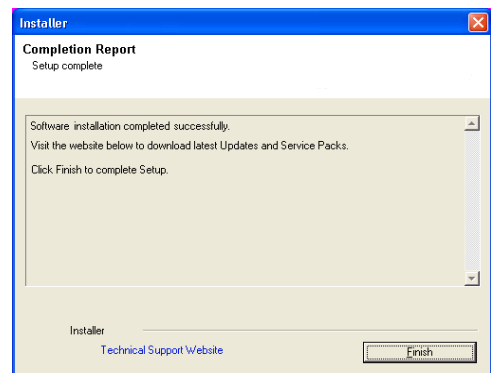
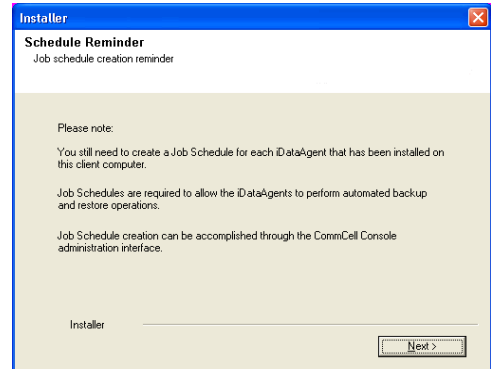
18. Click **Next**.



19. Click **Next**.



20. Click **Finish**.



# Getting Started - Windows File System Configuration

◀ Previous Next ▶

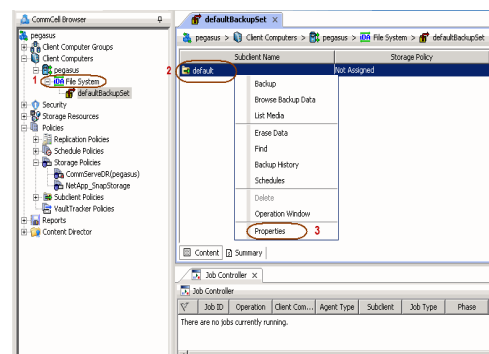
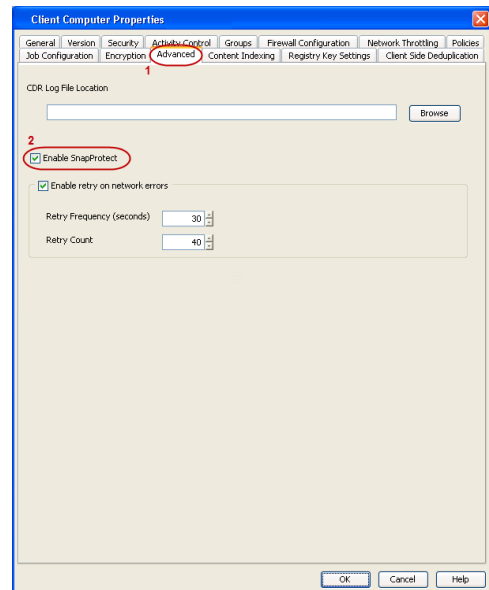
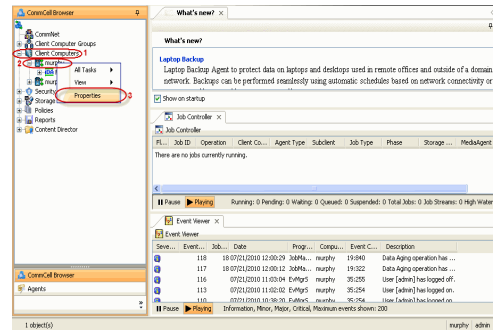
## PRE-REQUISITES

- 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

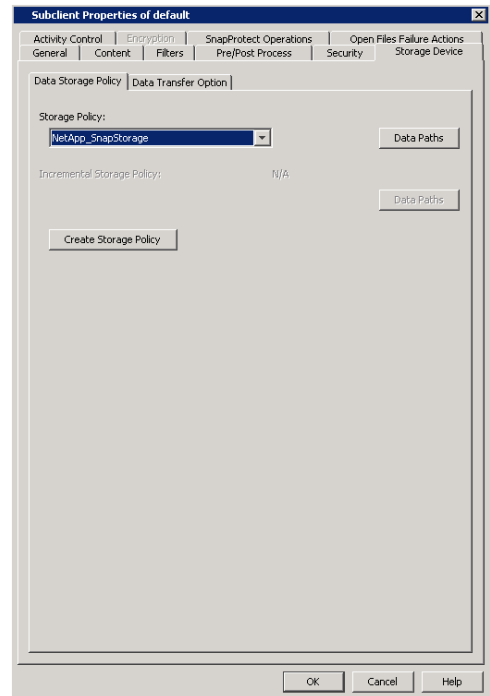
Once installed, the Windows File System *FileAgent* requires some additional configuration before running your first SnapProtect backup. Follow the steps given below to complete the configuration for this Agent.

- 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.

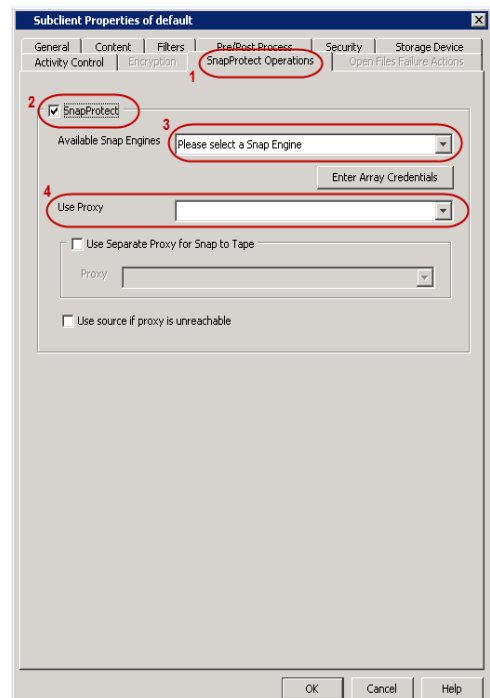


5.
  - Click the **SnapProtect Operations** tab.
  - Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
  - Select the storage array from the **Available Snap Engine** drop-down list.
  - From the **Use Proxy** list, select the MediaAgent where SnapProtect and backup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

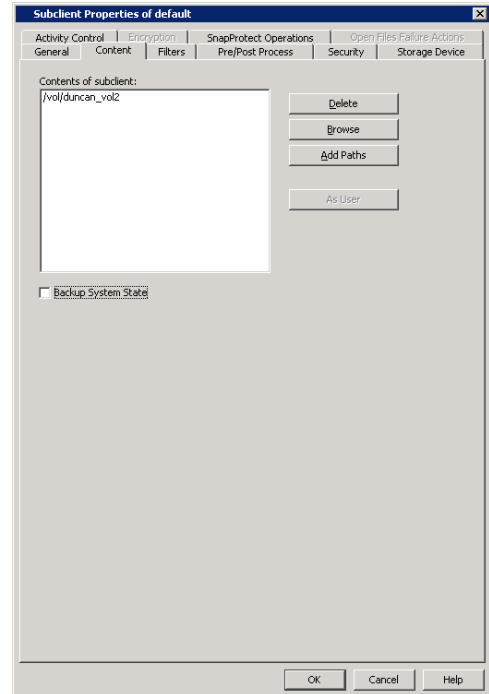
- Click **Use Separate Proxy for Snap to Tape** if you want to perform backup copy operations in a different MediaAgent.

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.

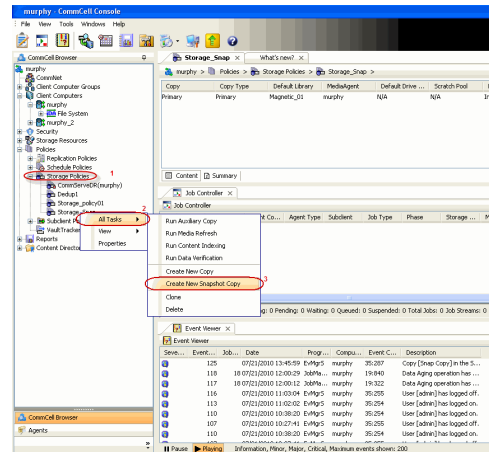
Click **Next** ➤ to Continue.

### CREATE A SNAPSHOT COPY

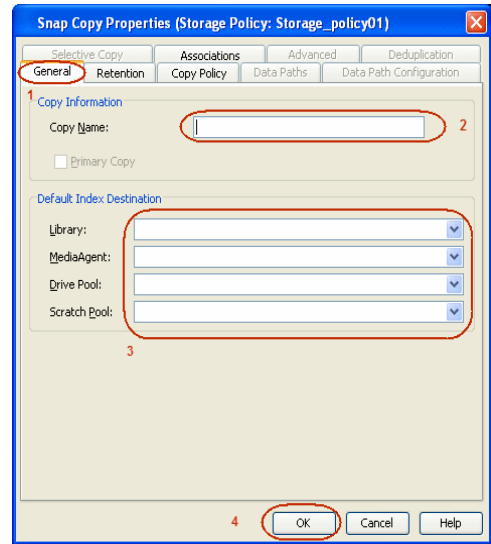
Next ➤

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**.



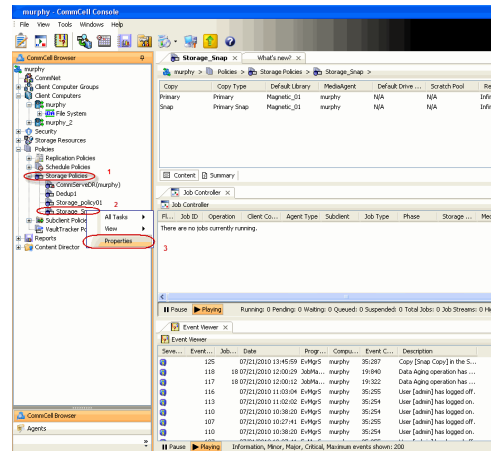
- Enter the copy name in the **Copy Name** field.
  - Select the **Library**, **MediaAgent**, master **Drive Pool** and **Scratch Pool** from the lists (not applicable for disk libraries).
  - Click **OK**.



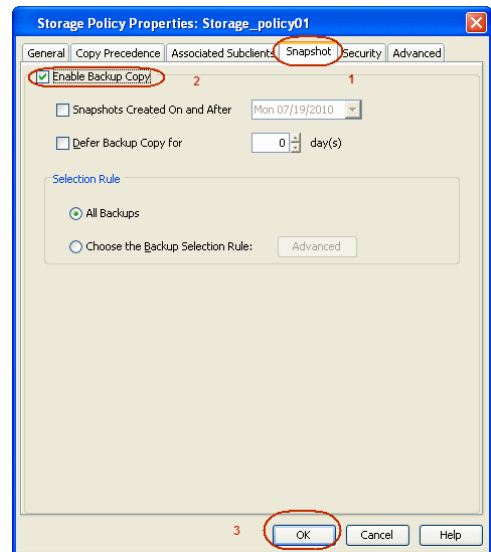
## CONFIGURE BACKUP COPY

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



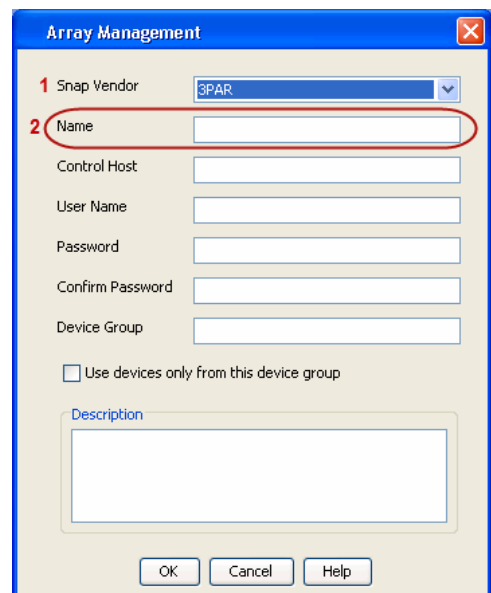
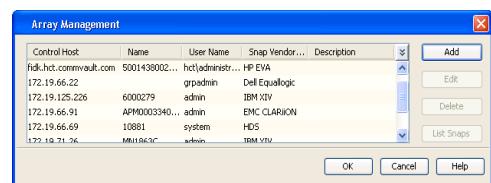
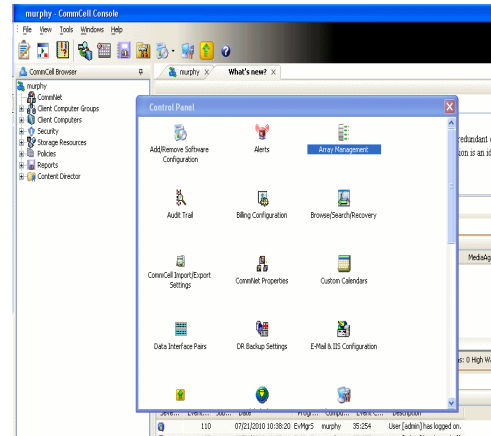
## PRE-REQUISITES

- 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

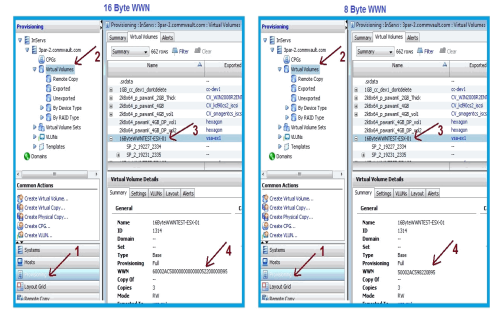
where  $\text{DevID.substr}(26,6)$  is the next 6 digits after the twenty sixth digit from the WWN number

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

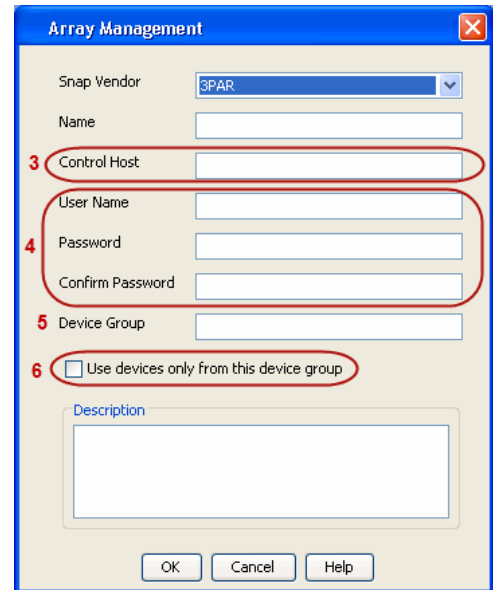
After adding all the values, the resulting array name is 2FF70002AC000B95.



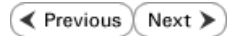
- Enter the IP address of the array in the **Control Host** field.
  - Enter the access information of a local 3PAR Management user with administrative privileges in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the CPG group created on the array to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

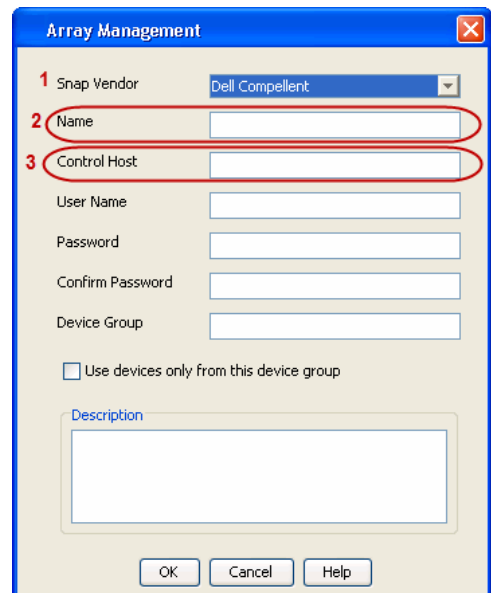
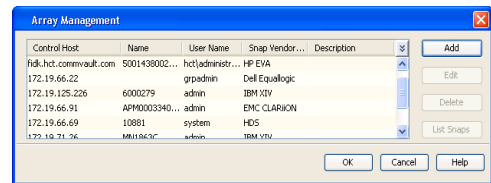
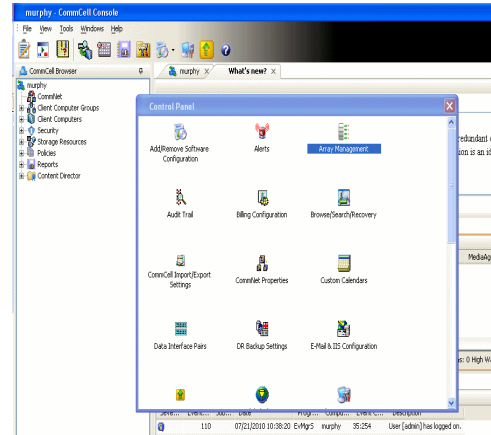
- Dell Compellent requires the Data Instant Replay license.
- Ensure that all members in the Compellent array are running firmware version Storage Center 5.5.14 and above for 5.x and 6.2.2 and above for 6.x.

## SETUP THE ARRAY INFORMATION

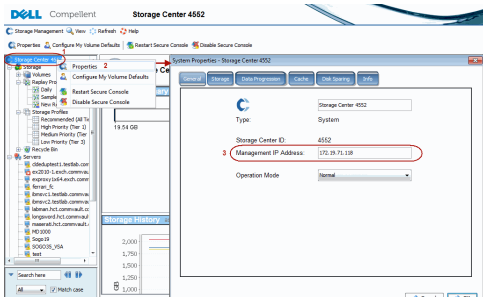
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

- 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.

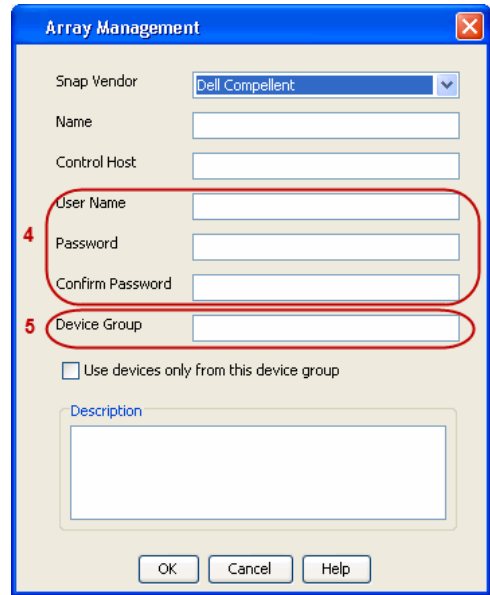
The Management IP address is also referred as the Storage Center IP address.



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.

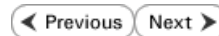


- 4.
- Enter the user access information of the application administrator in the **Username** and **Password** fields.
  - In the **Device Group** field, type *none* as this array does not use device groups for snapshot operations.
  - Use the **Description** field to enter a description about the entity. 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

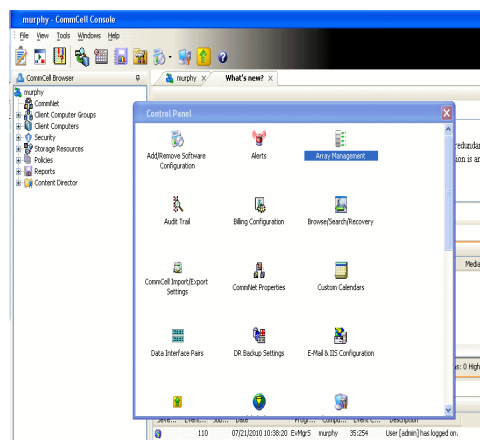
- Ensure that all members in the EqualLogic array are running firmware version 4.2.0 or higher.
- After upgrading the firmware, do either of the following:
  - Create a new group administration account in the firmware, and set the desired permissions for this account.
  - If you plan to use the existing 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.

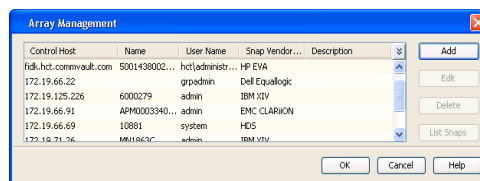
## SETUP THE ARRAY INFORMATION

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**.



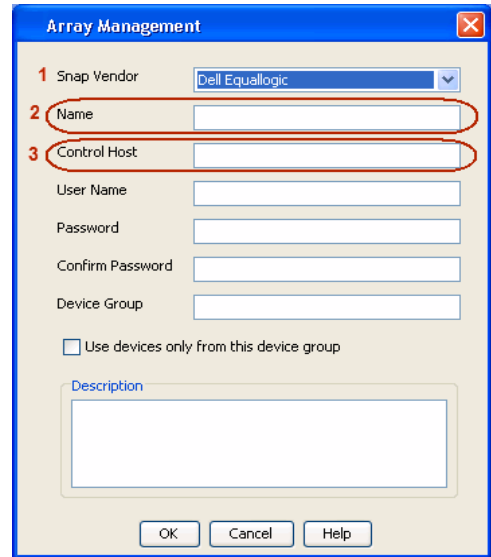
2. Click **Add**.



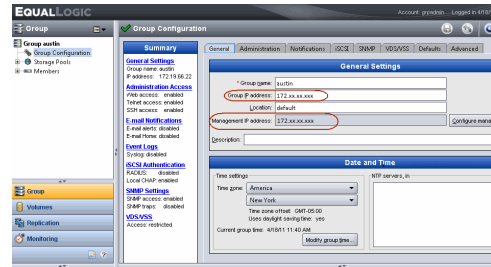
3.
  - Select **Dell Equallogic** from the **Snap Vendor** list.
  - Specify the Management IP address in the **Name** field.

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

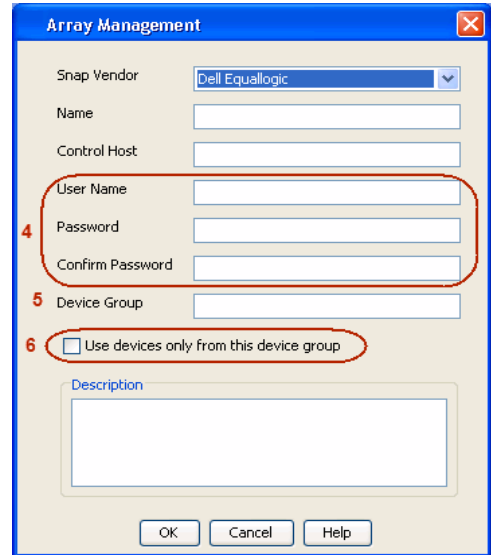
- Specify the Group IP address in the **Control Host** field.



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.

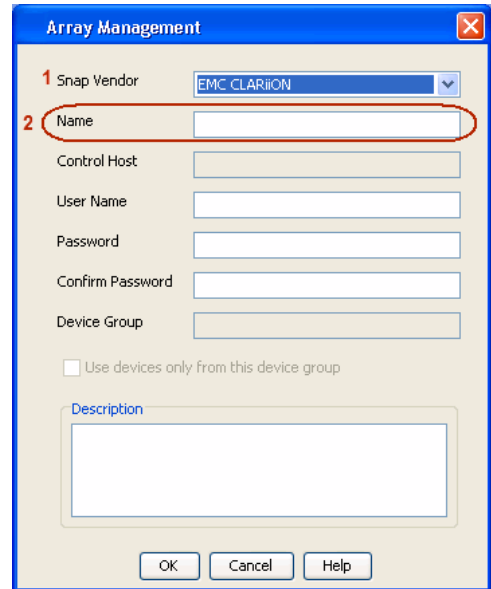
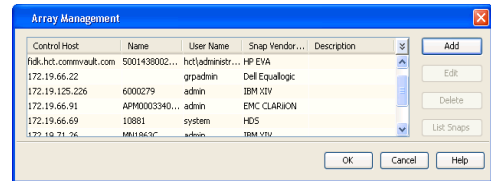
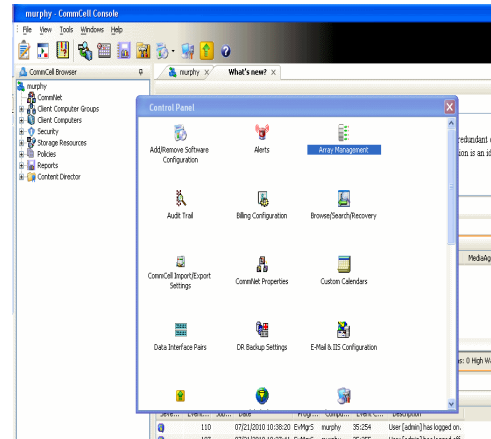
## SETUP THE ARRAY INFORMATION

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

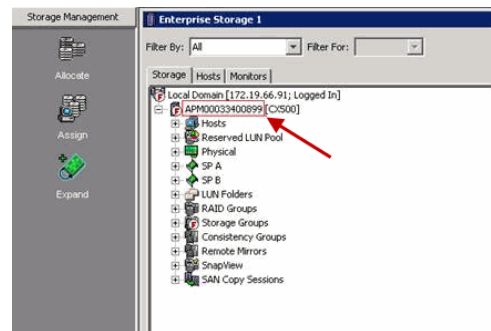
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.

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** [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

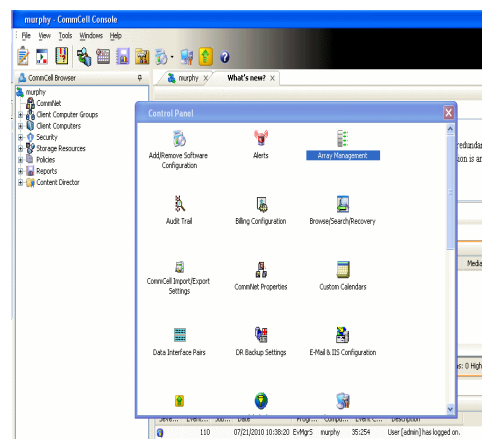
If you have the SYMCLI software installed, it is recommended that you test your local Symmetrix environment by running the following command to ensure that the Symmetrix database is successfully loaded:

```
symcfg discover
```

## SETUP THE ARRAY INFORMATION

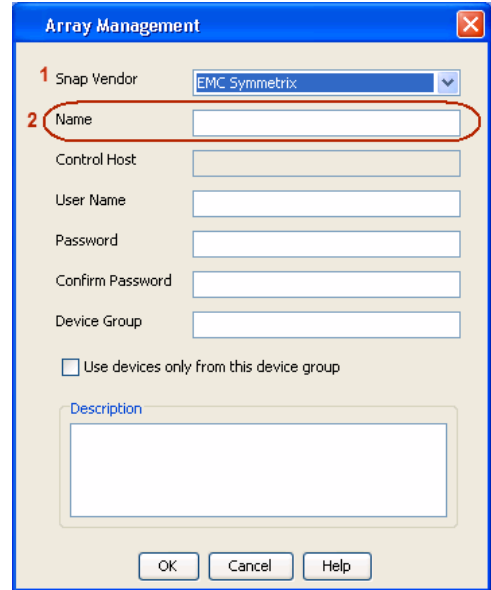
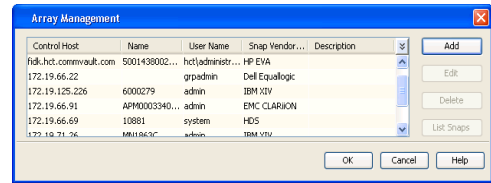
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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

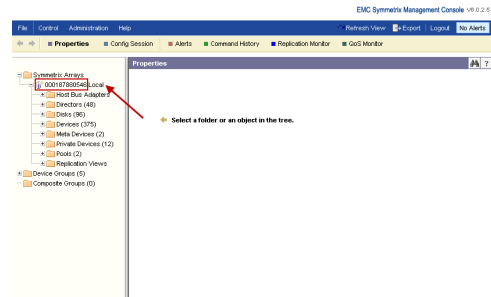


2. Click **Add**.

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

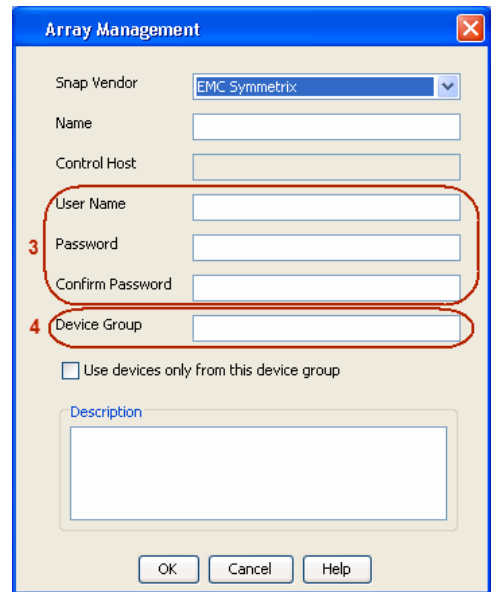


For reference purposes, the screenshot on the right shows the Symmetrix array ID (Symm ID) for the EMC Symmetrix storage device.



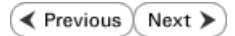
4.
  - If Symcfg Authorization is enabled on the Symmetrix Management Console, enter the access information for the Symmetrix Management Console in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the device group created on the client and proxy computer. 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



## 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

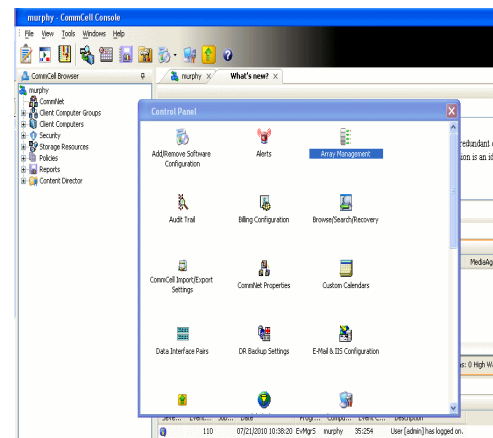
If pre-paired sessions are not available, destination volumes are automatically created for clone snapshots. If a non-existing device group is specified during array configuration in the CommCell Console, a destination volume is created based on the source volume type. However, if a valid device group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

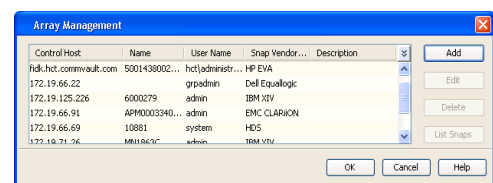
## SETUP THE ARRAY INFORMATION

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**.

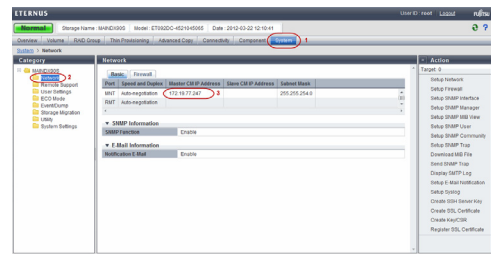
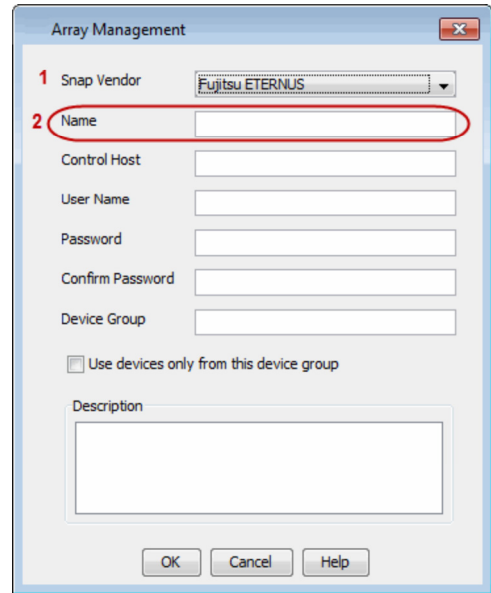


2. Click **Add**.

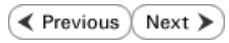
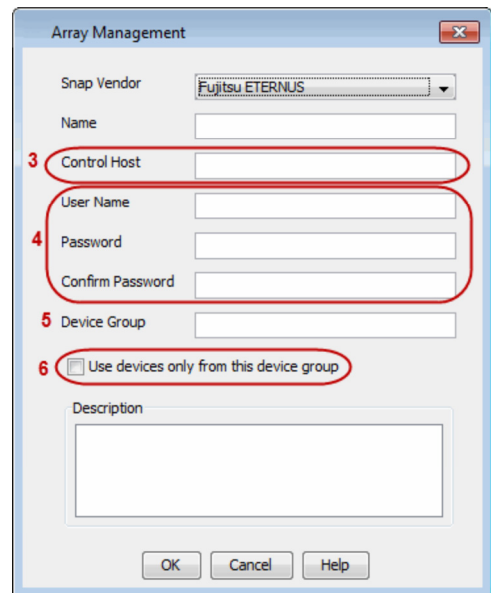


3.
  - Select **Fujitsu ETERNUS** from the **Snap Vendor** list.
  - Specify the CM IP Address of the array in the **Name** field.

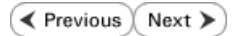
For reference purposes, the screenshot on the right shows the CM IP Address for the Fujitsu storage device.



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



## 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

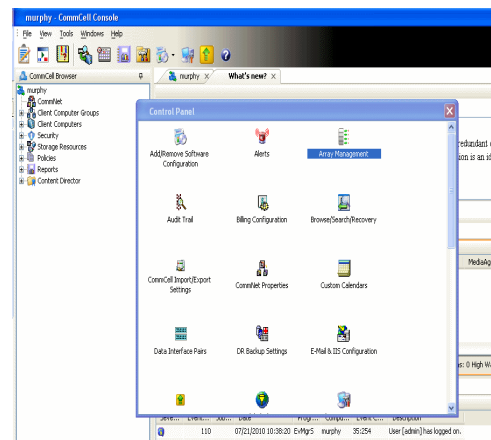
When performing SnapProtect operations on VMware using HDS as the storage array, ensure the following:

- 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.

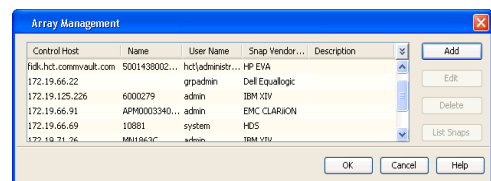
## SETUP THE ARRAY INFORMATION

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

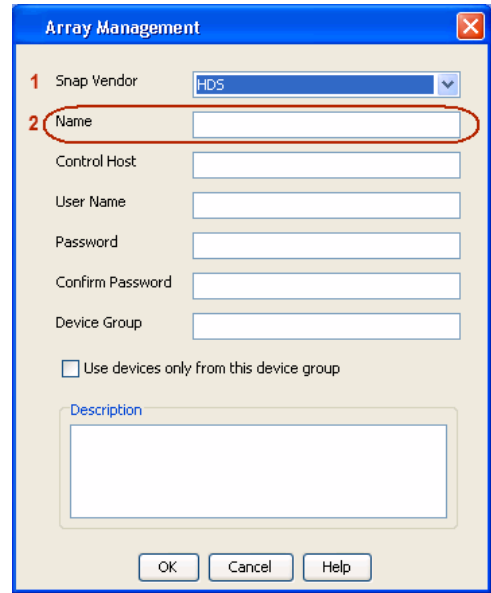
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



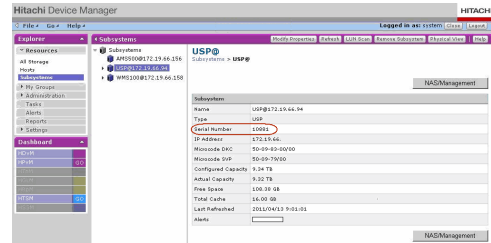
2. Click **Add**.



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.



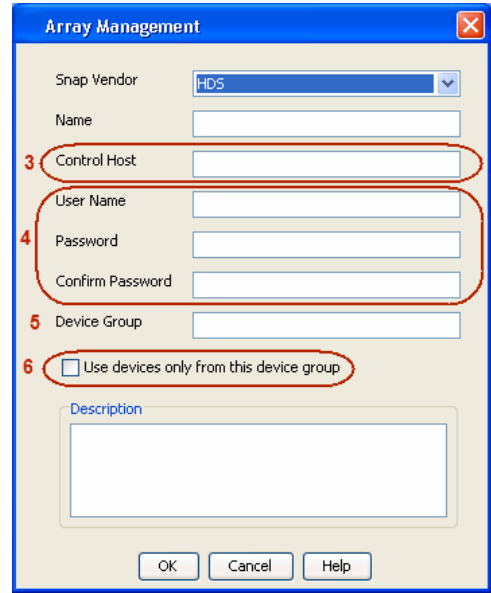
4.
  - Enter the IP address or host name of the Device Manager Server in the **Control Host** field.
  - Enter the user access information in the **Username** and **Password** fields.
  - In the **Device Group** field, specify the name of the hardware device group created on the array to be used for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

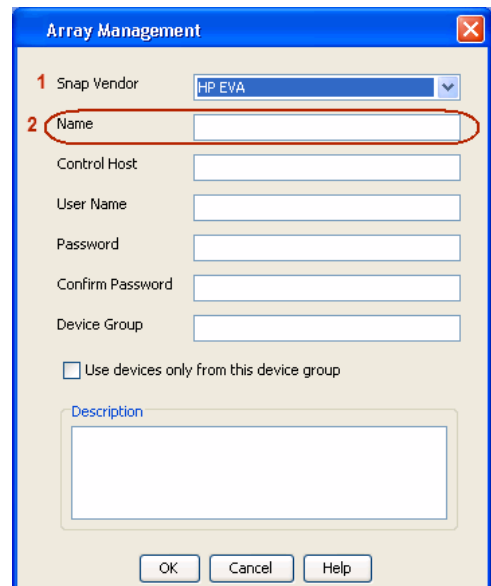
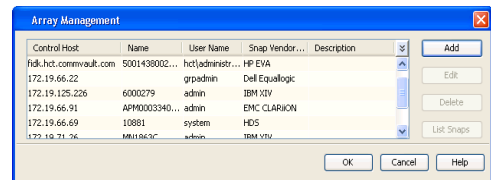
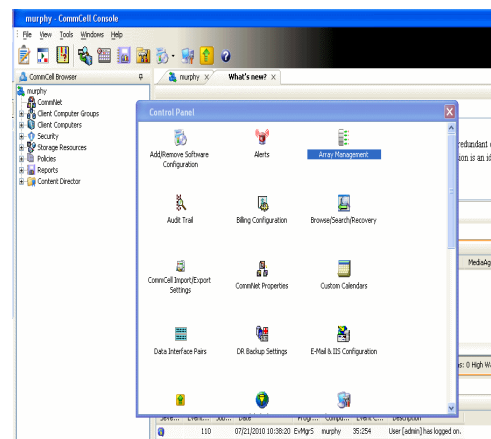
The following steps provide the necessary instructions to setup the HP EVA:

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

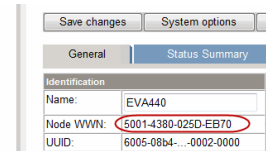
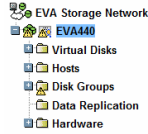
Provide the identification information for the array to ensure access. The following section provides step-by-step instructions for setting the array information.

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 ▶

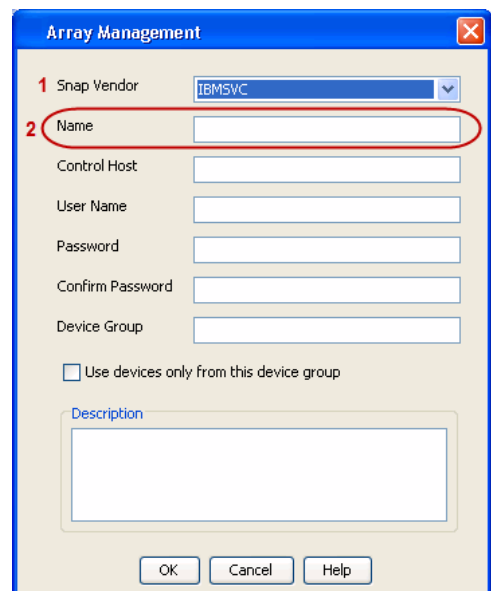
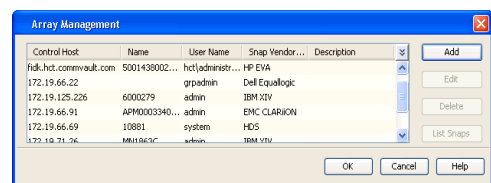
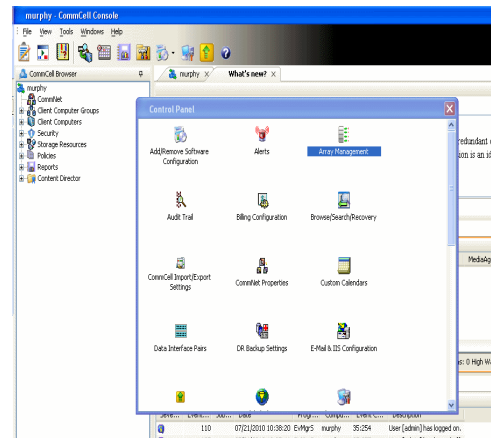
## PRE-REQUISITES

- 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.

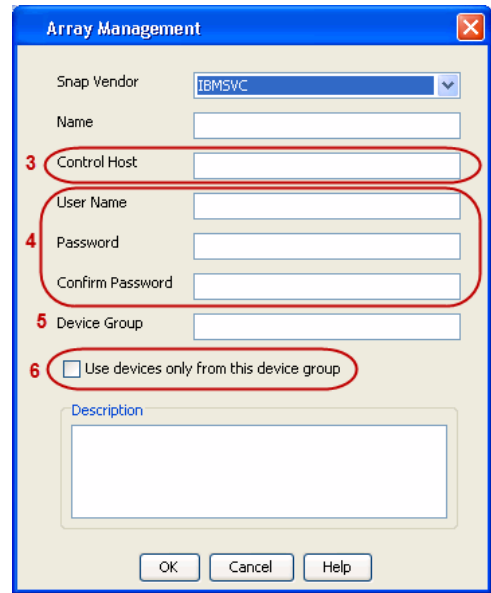
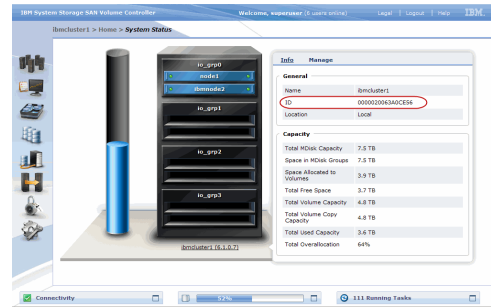
- From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.
- Click **Add**.
- Select **IBMSVC** from the **Snap Vendor** list.
  - Specify the 16-digit ID of the storage device in the **Name** field.



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

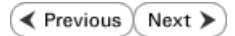
4.

- 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



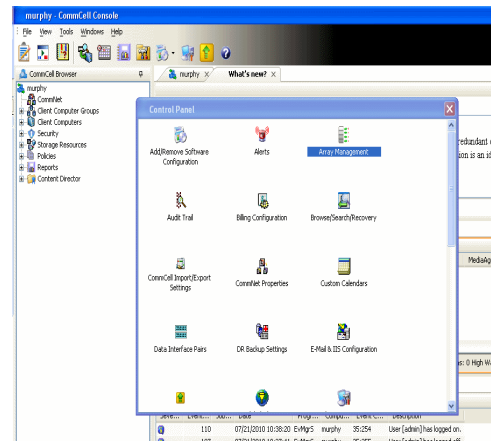
## PRE-REQUISITES

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.

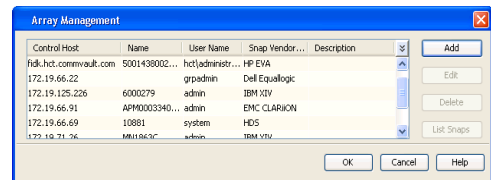
## SETUP THE ARRAY INFORMATION

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

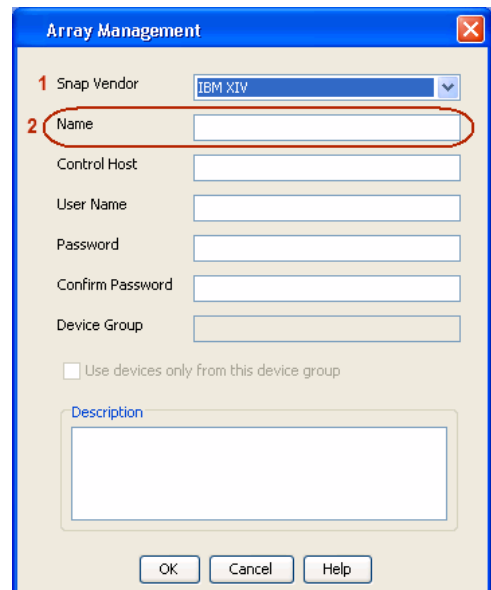
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.



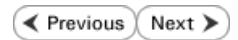
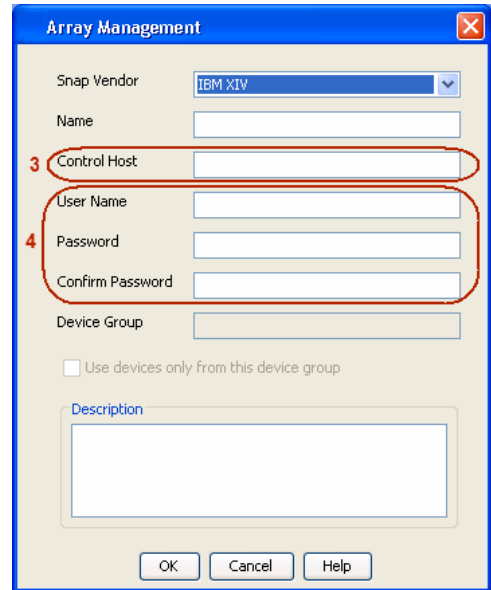
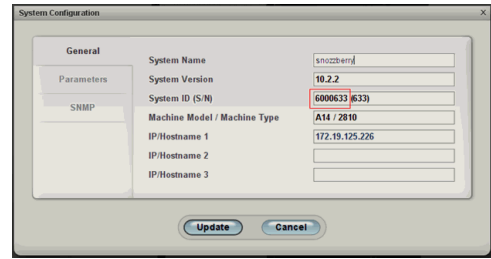
3.
  - Select **IBM XIV** from the **Snap Vendor** list.
  - Specify the 7-digit serial number for the array in the **Name** field.



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.

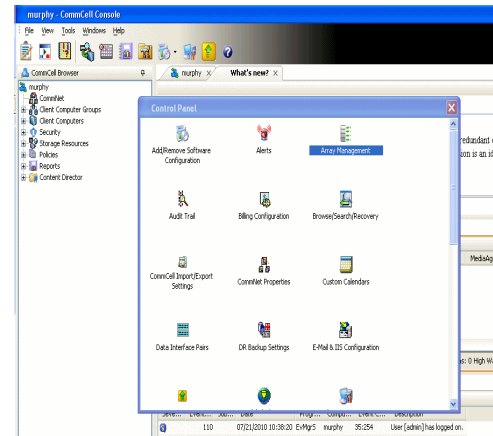
## ADDITIONAL REQUIREMENTS FOR VMWARE

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.

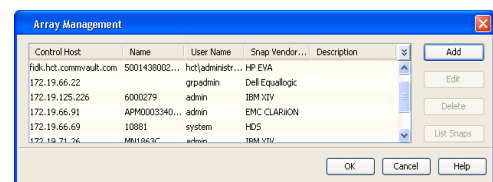
## SETUP THE ARRAY INFORMATION

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

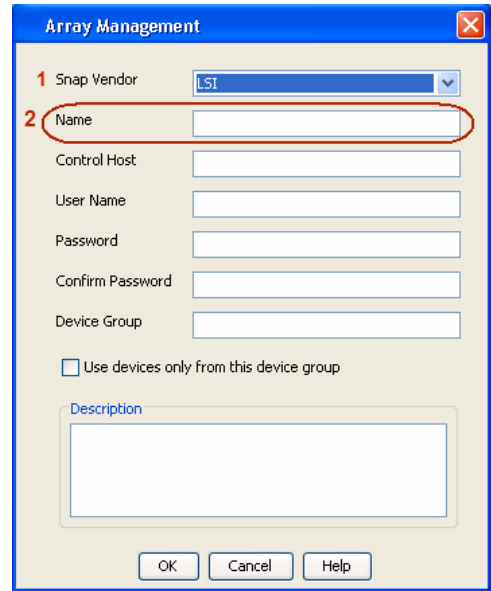
1.
  - From the CommCell Console, navigate to **Tools | Control Panel**.
  - Click **Array Management**.



2. Click **Add**.

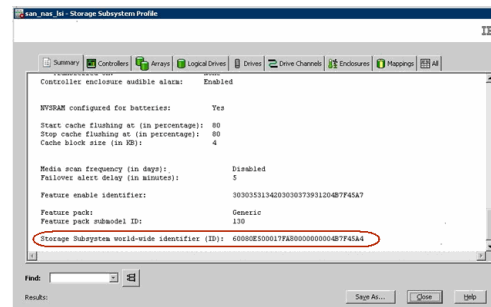


3.
  - Select **LSI** from the **Snap Vendor** list.
  - Specify the serial number for the array in the **Name** field.



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

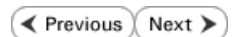
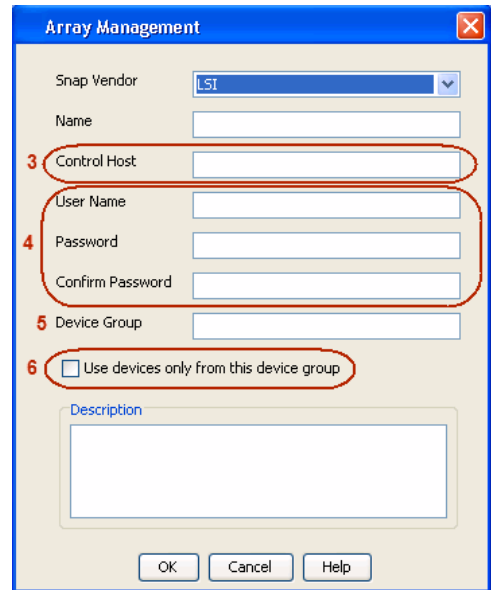
Use the SANtricity Storage Manager software to obtain the array name by clicking **Storage Subsystem Profile** from the **Summary** tab. See the screenshot on the right for reference.



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

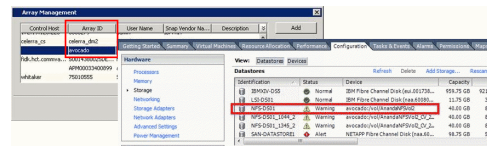
### LICENSES

- 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.

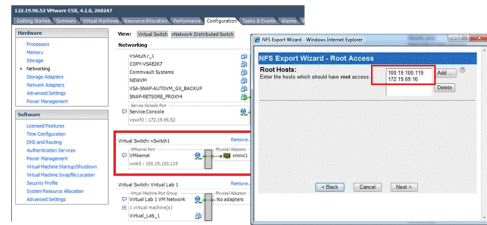
## ADDITIONAL REQUIREMENTS FOR VMWARE

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.



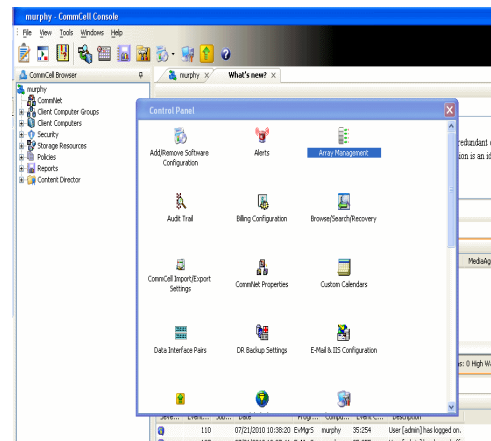
The VMkernel IP address of all ESX servers that are used for mount operations should be added to the root Access of the NFS share on the source storage device. This needs to be done because the list of all root hosts able to access the snaps are inherited and replicated from the source storage device.



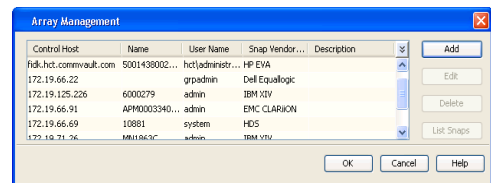
## SETUP THE ARRAY INFORMATION

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

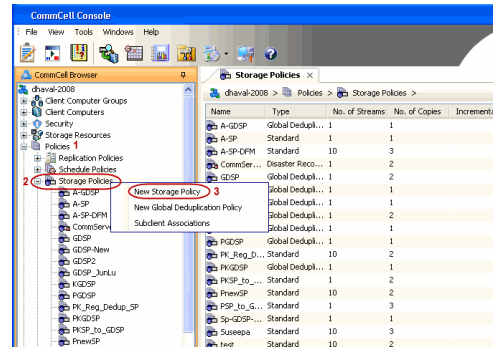
## CONFIGURATION

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

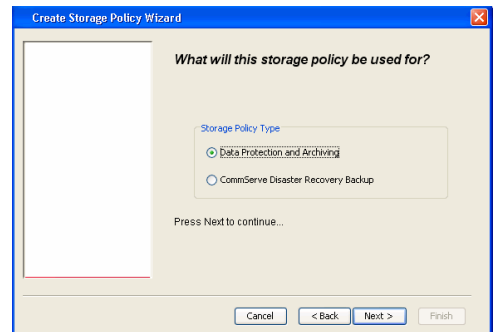
## CREATE STORAGE POLICY

Use the following steps to create a storage policy.

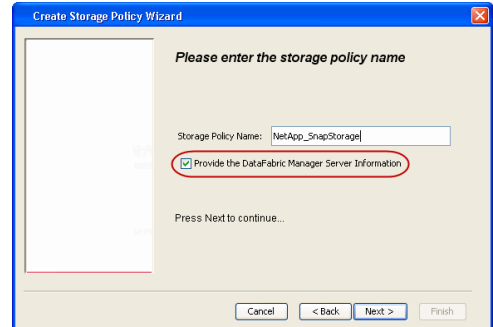
1.
  - From the CommCell Browser, navigate to **Policies**.
  - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



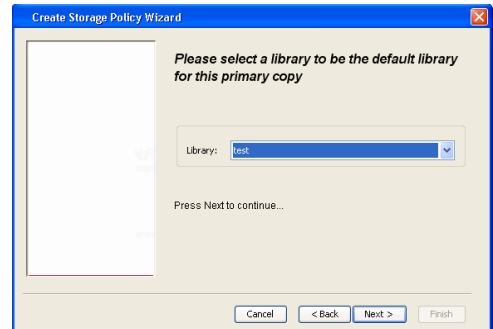
3.
  - Specify the name of the **Storage Policy** in the **Storage Policy Name** box.
  - Select **Provide the DataFabric Manager Server Information**.
  - Click **Next**.



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.

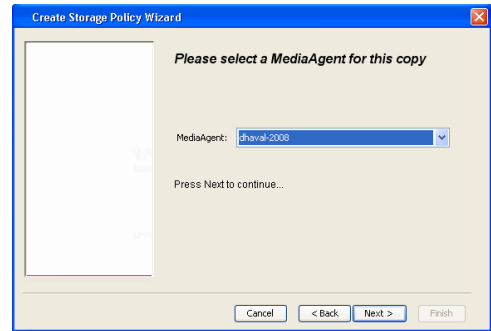
- Click **Next**.



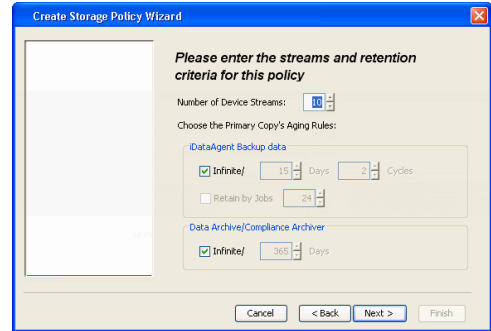
5.
  - Select a MediaAgent from the **MediaAgent** list.
  - Click **Next**.



6. Click **Next**.

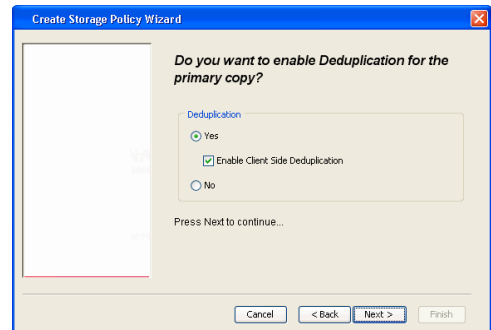


7. Click **Next**.



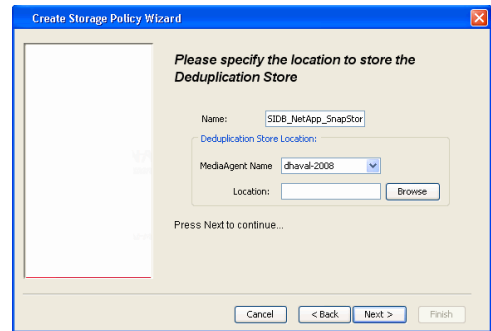
8. 

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

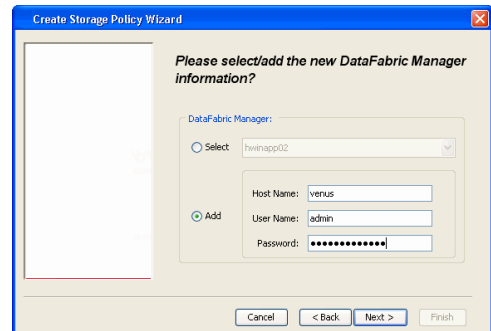


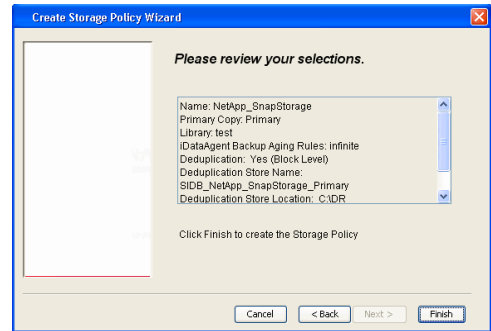
9. 

- 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**.



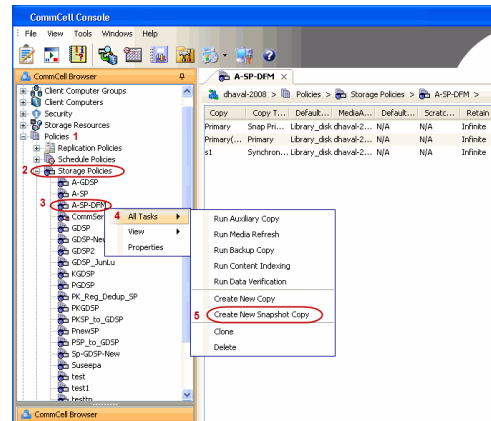


11. The new Storage Policy creates the following:
  - **Primary Snap Copy**, used for local snapshot storage
  - **Primary Classic Copy**, used for optional data movement to tape, disk or cloud.

### CREATE A SECONDARY SNAPSHOT COPY

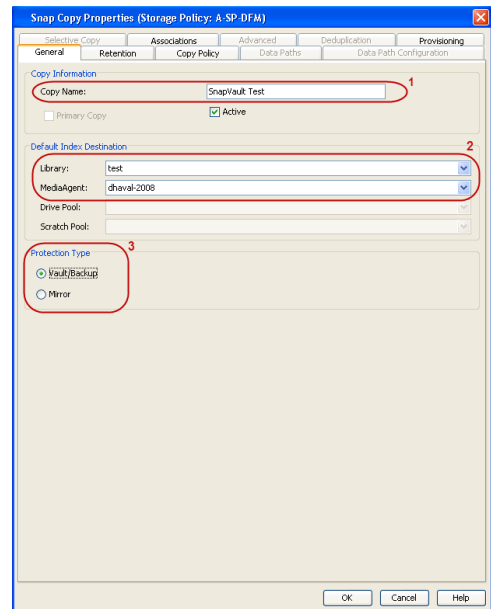
After the Storage Policy is created along with the Primary Snap Copy, the Secondary Snap Copy must be created on the new Storage Policy.

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.

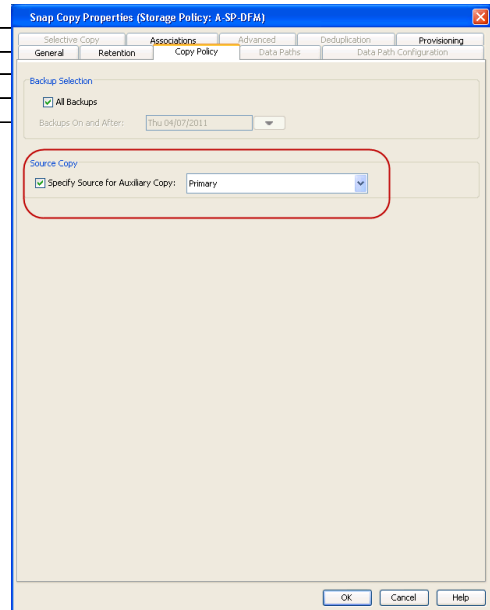


3.
  - Click the **Copy Policy** tab.
  - Depending on the topology you want to set up, click **Specify Source for Auxiliary Copy** and select the source copy.

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

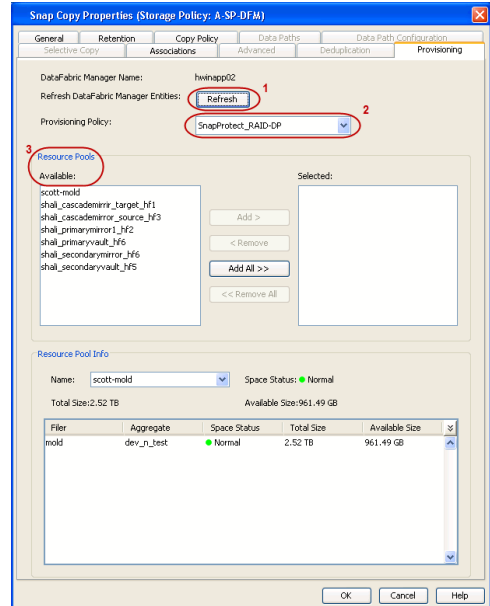
| TOPOLOGY | SOURCE COPY |
|----------|-------------|
|----------|-------------|

|                       |         |
|-----------------------|---------|
| 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.

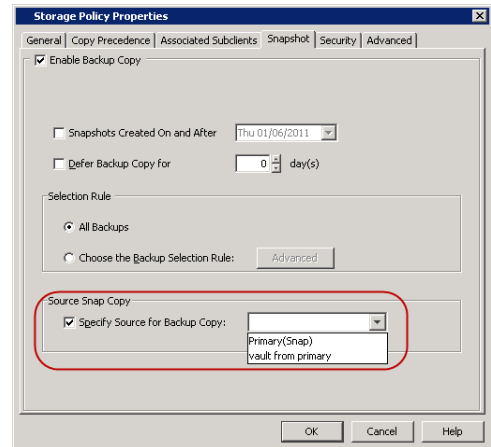
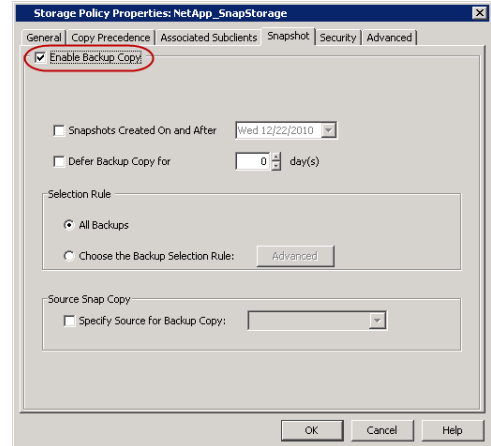
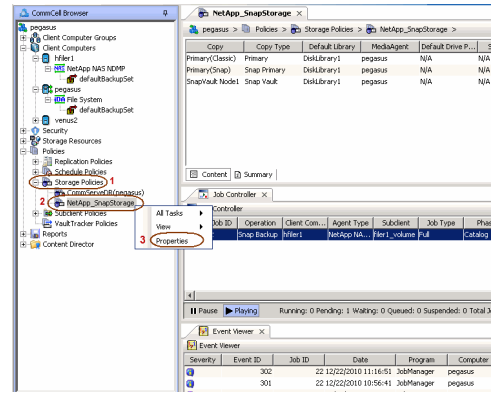
## CONFIGURE BACKUP COPY

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.

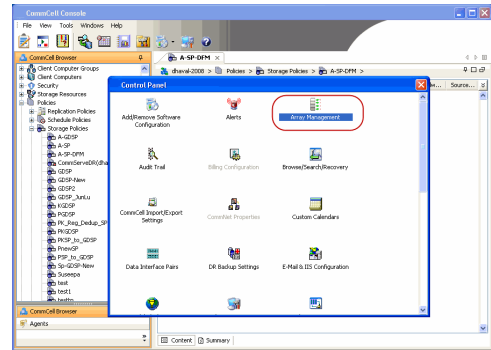


## SETUP THE ARRAY INFORMATION

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**.

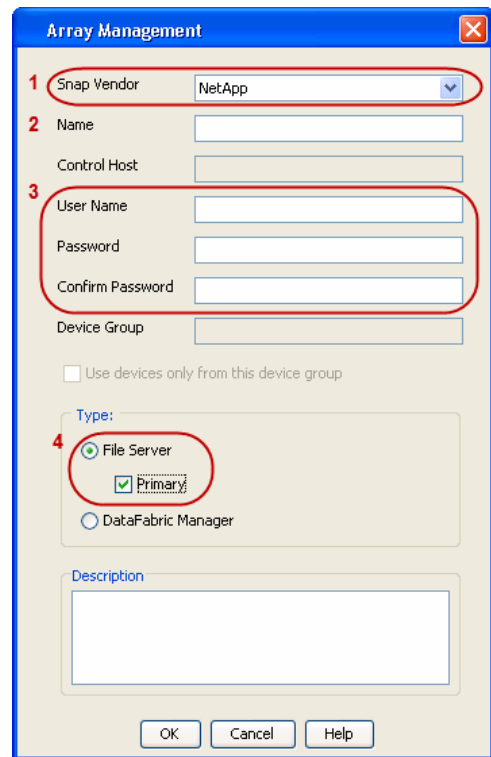
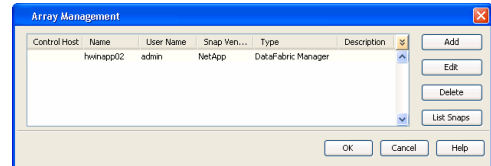


3.
  - Select **NetApp** from the **Snap Vendor** list.
  - Specify the name of the primary file server in the **Name** field.

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.

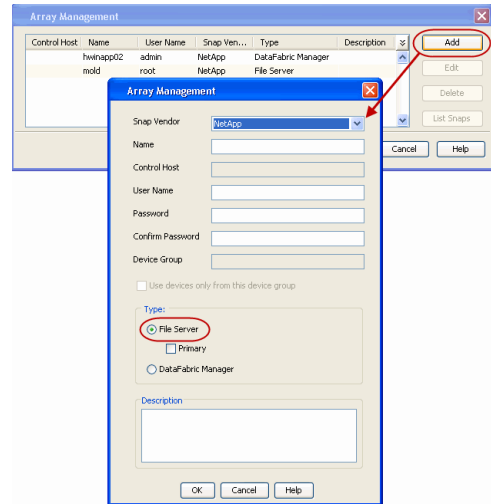
- Enter the user access information in the **Username** and **Password** fields.
- Select **File Server**, then click **Primary** for the array type.
- Use the **Description** field to enter a description about the entity. This description can include information about the entity's content, cautionary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

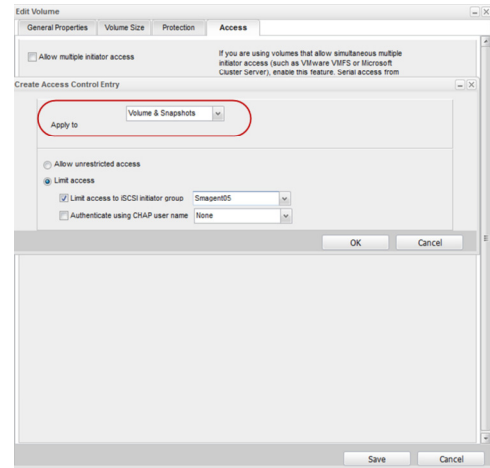
Provides the steps to import the configuration details of the DataFabric Manager server into the Simpana software.

# SnapProtect™ Backup - Nimble



## PREREQUISITES

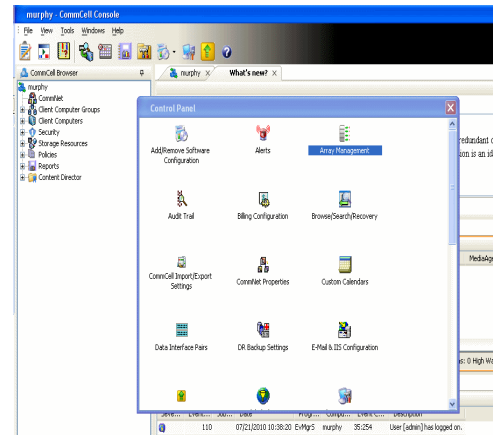
- From the Nimble storage array console, ensure that the **Access Control Entry** for the client initiator group is set to **Volume and Snapshots**.
- In case you are using a proxy computer for SnapProtect operations, add the initiator group for the proxy computer and set the **Access Control Entry**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



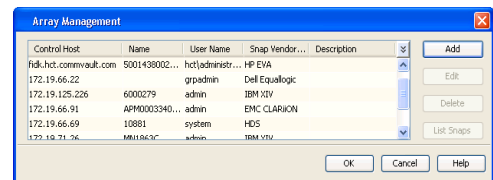
## SETUP THE ARRAY INFORMATION

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.

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.



**Array Management**

Snap Vendor: Nimble

Name: \_\_\_\_\_

Control Host: \_\_\_\_\_

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Confirm Password: \_\_\_\_\_

Device Group: \_\_\_\_\_

Use devices only from this device group

Type:

- File Server
- Primary
- DataFabric Manager

Description: \_\_\_\_\_

OK Cancel Help

< 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.

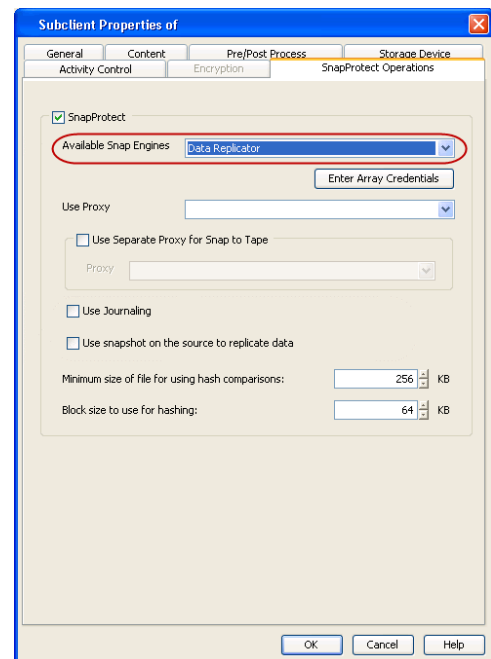
### STORAGE POLICY REQUIREMENTS

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

- 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 ▶

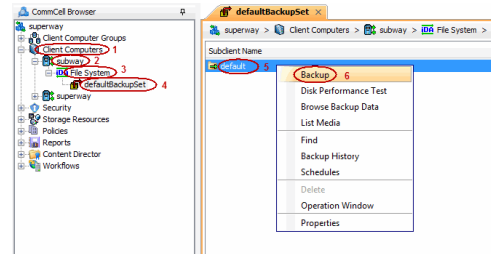
# Getting Started - Windows File System Backup

## PERFORM A BACKUP

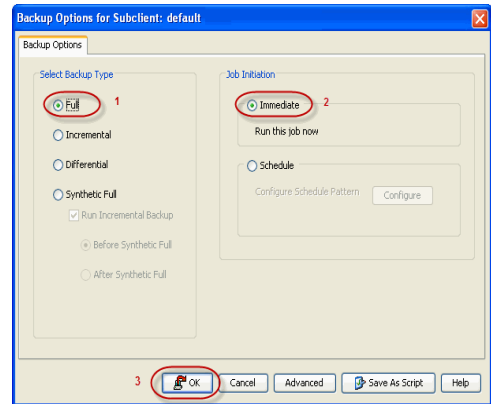
Once the storage policy is configured, you are ready to perform your first backup.

The following section provides step-by-step instructions for performing your first backup:

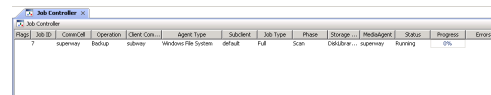
- From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.
  - Right-click the default subclient and click **Backup**.



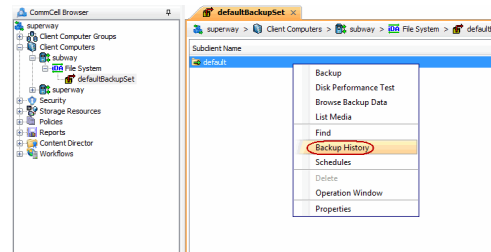
- Click **Full** as backup type and then click **Immediate**.
  - Click **OK**.



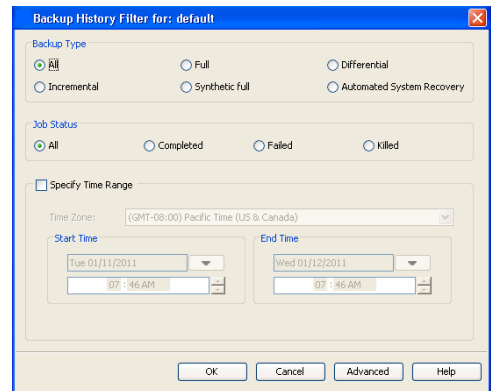
- You can track the progress of the job from the **Job Controller** window of the CommCell console.



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

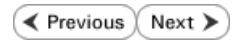
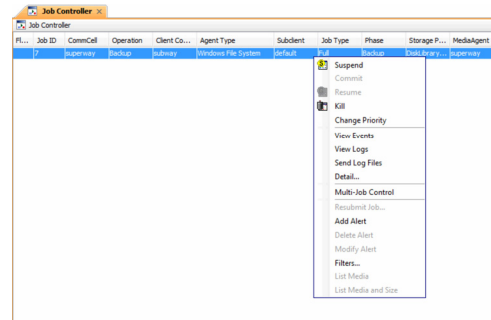


- Click **OK**.



- 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

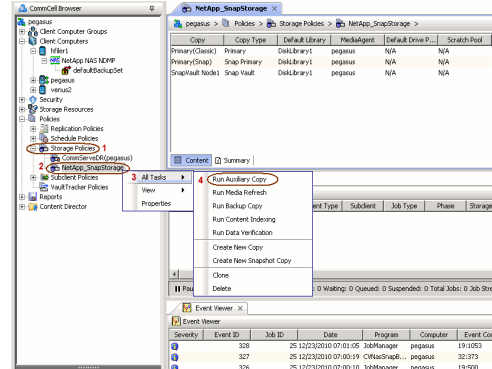
**SKIP THIS PAGE IF YOU ARE NOT USING NETAPP WITH SNAPVAULT/SNAPMIRROR.**

Click **Next** ▶ to Continue.

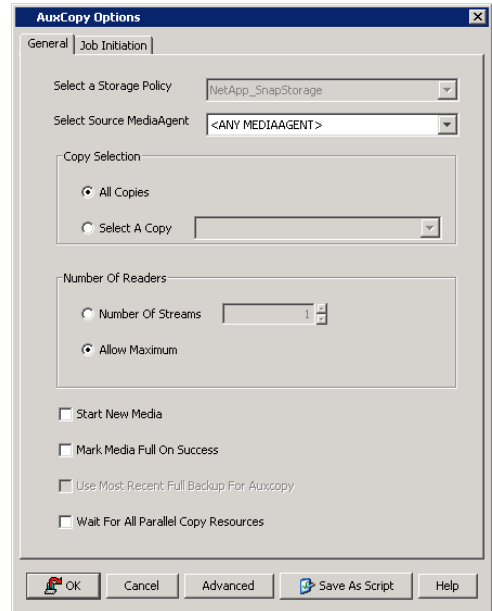
## INITIATE VAULT/MIRROR COPY

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**.

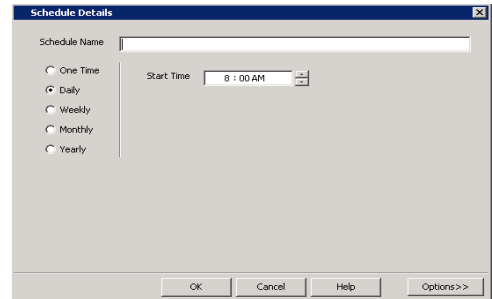


- Select the desired options and click the **Job Initiation** tab.
  - Select **Schedule** to configure the schedule pattern and click **Configure**.



- 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.

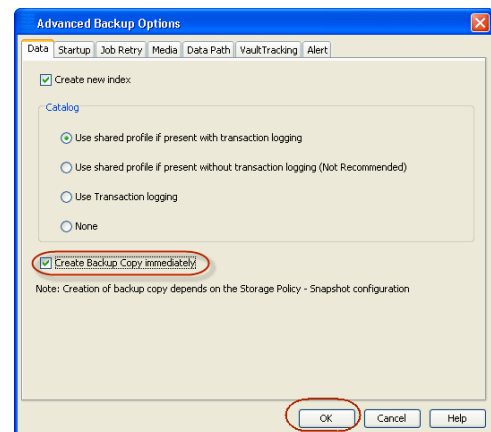
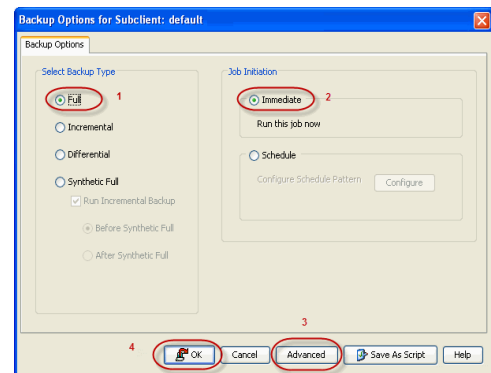
Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again.

#### 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**.

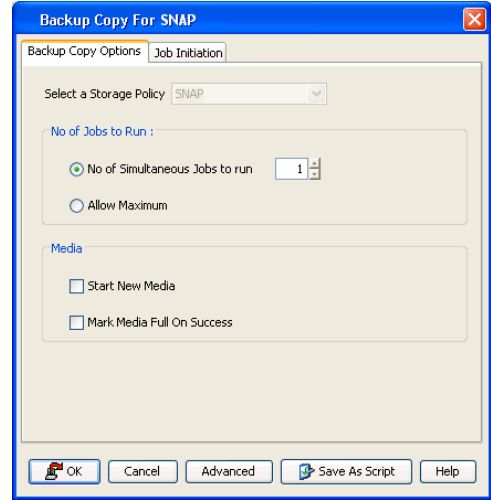
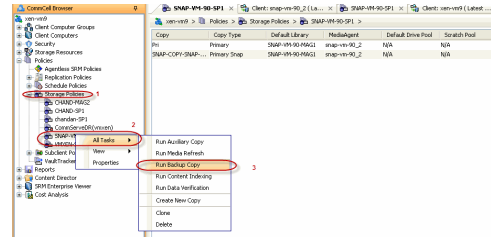


#### OFFLINE BACKUP COPY

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 - Windows File System Restore

## PERFORM A RESTORE

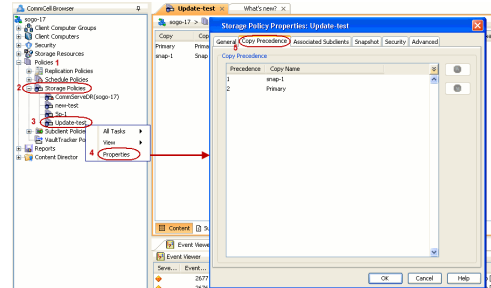
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after your first full backup to understand the process.

The following sections explain the steps for restoring the backup data from copies.

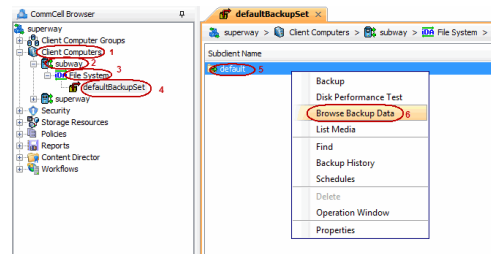
- From the CommCell Console, navigate to **Policies | Storage Policies**.
  - Right-click the **<storage policy>** and click **Properties**.
  - Click the **Copy Precedence** tab.
  - By default, the snapshot copy is set to 1 and is used for the operation.

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.

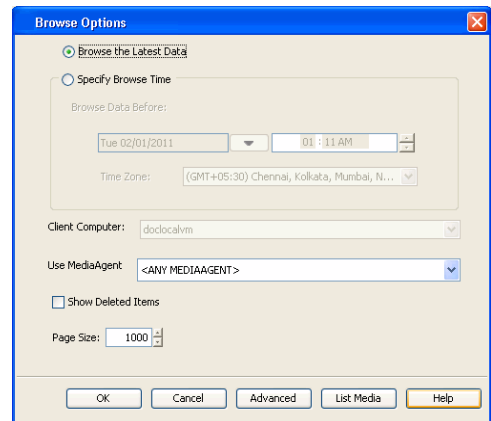
- Click **OK**.



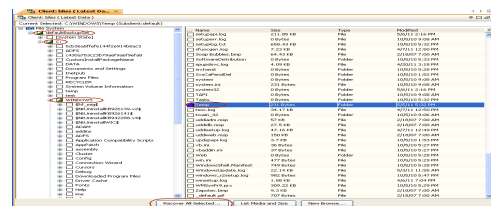
- From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.
  - Right-click the default subclient and then click **Browse Backup Data**.



- Click **OK**.



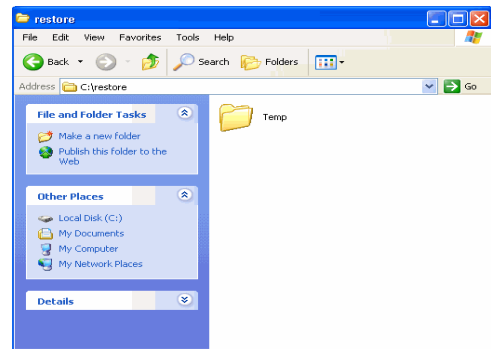
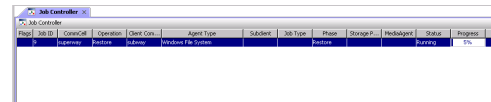
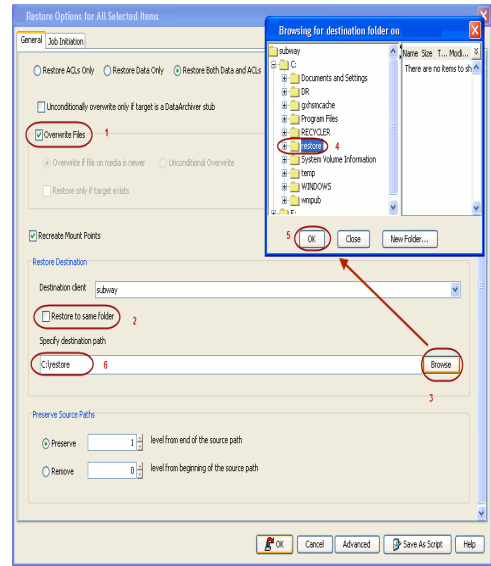
- Expand the **defaultBackupSet** and navigate to **Documents and Settings** folder.
  - Select the **Documents and Settings** folder.
  - Click **Recover All Selected**.



- 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**.



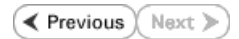
6. You can monitor the progress of the restore job in the **Job Controller** window of the CommCell Console.
7. Once the File System is restored, verify that the restored files/folders are available in the restore destination.



**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.



# Advanced - VMware SnapProtect™ Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert Virtual Machine from a Snapshot

### Configuring User Accounts

- Virtual Center Credentials
- Permissions for Custom User Accounts

### Configuring Auto-Discovery by Datastore Affinity of Virtual Machines

### Configuring Subclients through the Command Line

### Truncating SQL Database Logs

### Verify SnapProtect Backups

### Choosing Restore Types

### Restore to a Different ESX server

### Restoring Files and Folders

### Restore Files from a Snapshot (Live Browse)

### Restore Data from a Backup Copy

### Data Aging for SnapProtect Snapshots

- Retention by Number of Jobs

### Options not supported for VMware

### Using a Separate ESX Server for a Backup Copy

- Configuring a Subclient to Use a Separate Proxy Client
- Specifying Secondary ESX Server for Backup Copy Operations
- Restoring Virtual Machines from a Snapshot Mounted on the Secondary ESX Server

### Disabling VMware Quiesce

### Pre/Post Processing using VMware Tools

### Additional Options

## MANAGING SNAPSHOTS

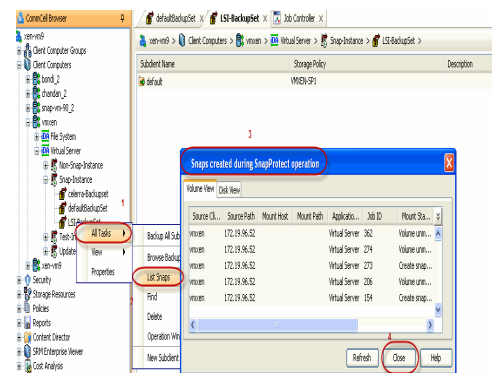
The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, or delete.

### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers | Virtual Server | <Instance>**.
2. Right-click **<backup set>** and click **All Tasks | List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.



### MOUNT SNAPSHOTS

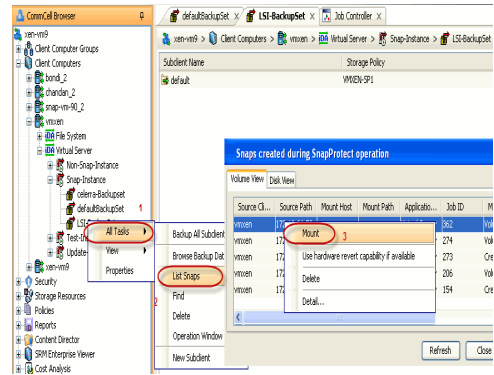
You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

If the niSCSIEnable registry key is configured, SnapProtect backup will always try to mount using iSCSI method. If

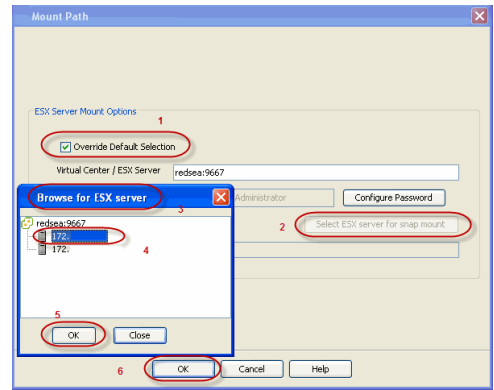
this key is not configured, SnapProtect backup will try to mount using the FC method first.

1. From the CommCell Browser, navigate to **Client Computers | Virtual Server | <Instance>**.
2. Right-click **<backup set>** and click **All Tasks | List Snaps**.
3. From the **Snaps created during SnapProtect operation** dialog box, right-click the snapshot that you wish to mount and select **Mount**.

You can also open the **Snaps created during SnapProtect operation** dialog box by right clicking the snapshot copy in a storage policy. However, if you open the dialog box by this method, you can only view the list of snapshots and cannot mount the snapshots.



4. From the **Mount Path** dialog box, you can select a different ESX server for mounting the snap by choosing the **Select ESX server for snap mount** option.
5. Select the appropriate ESX server from the **Browse for ESX Server** dialog box.
5. Click **OK** to close the **Browse for ESX Server** dialog box.
6. Click **OK** to close the **Subclient Properties** dialog box.

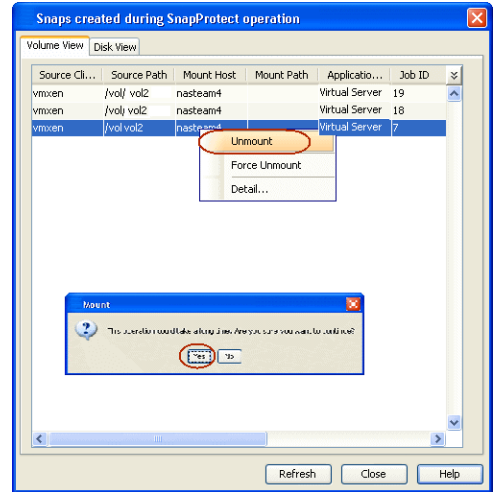


**UNMOUNT SNAPSHOTS**

Follow the steps given below to Unmount Snapshots:

1. From the CommCell Browser, navigate to **Client Computers | Virtual Server | <Instance>**.
2. Right-click **<backup set>** and click **All Tasks | List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.

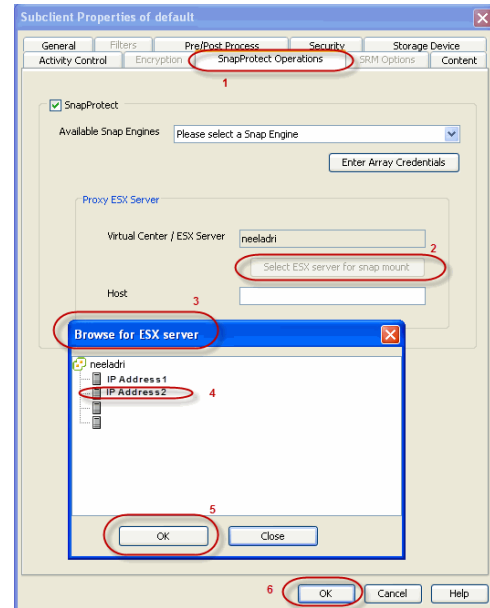


**SNAP MOUNT TO A DIFFERENT ESX SERVER**

While performing mount operations you can use a temporary ESX server to reduce the load on the production server.

1. From the CommCell Console, right-click the subclient for which you wish to perform a SnapProtect backup and click **Properties**.
2. Click the **SnapProtect Operations** tab.
3. Select the **SnapProtect** option to enable SnapProtect backup for the selected subclient.
4. You can select a different ESX server for mounting the snap by choosing the **Select ESX server for snap mount** option.
5. Select the appropriate ESX server from the **Browse for ESX Server** dialog box.
6. Click **OK** to close the **Browse for ESX Server** dialog box.
7. Click **OK** to close the **Subclient Properties** dialog box.

By default the snapshot will be exposed to the first Host Bus Adapter (HBA) on the ESX Server. If you want to expose the snapshot to a specific HBA, configure the sPortInfo registry key.



## DELETE SNAPSHOTS

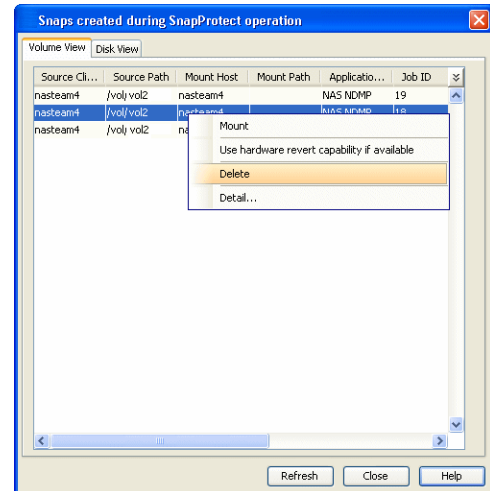
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



## REVERT VIRTUAL MACHINE FROM A SNAPSHOT

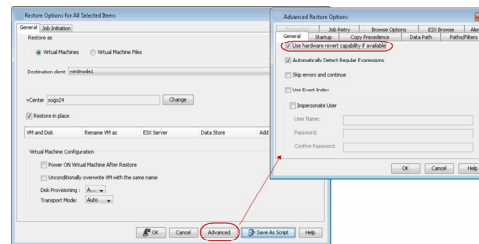
You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created.

Revert operations for a virtual machine are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. Other file servers are not supported. To perform a revert operation, the SnapRestore license is required on the NetApp file server.

Before performing revert operation, ensure that all the disks reside on the NFS data store. If the data does not reside on the NFS data store, you cannot perform the revert operation.

It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.

1. From the CommCell Browser, navigate to **Client Computers | Virtual Server | <Instance>**
2. Right-click **<backup set>** and click **All Tasks | Browse Backup Data**.
3. From the **Browse Options** dialog box, select **Container Restore** and click **OK**.
4. Select the virtual machine that you want to revert and click **Recover All Selected**.
5. From the **Restore Options** dialog box, click **Advanced**.
6. Select the **Use hardware revert capability if available** option.
7. Click **OK** to confirm the revert operation.
8. Click **OK** from the **Advanced Restore Options** dialog box.
9. Click **OK** to start the revert.



For NetApp NFS configurations:

- This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
- A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
- If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

## CONFIGURING USER ACCOUNTS

The Virtual Server iDataAgent requires user accounts that have sufficient privileges for the software to:

- Access the Virtual Center and ESX Servers
- Access virtual machines
- Access volumes, files, and folders within virtual machines

An administrative account configured with the **VCB Role** and the following additional privileges can be used:

- Virtual Machine
- Resource
- Datastore

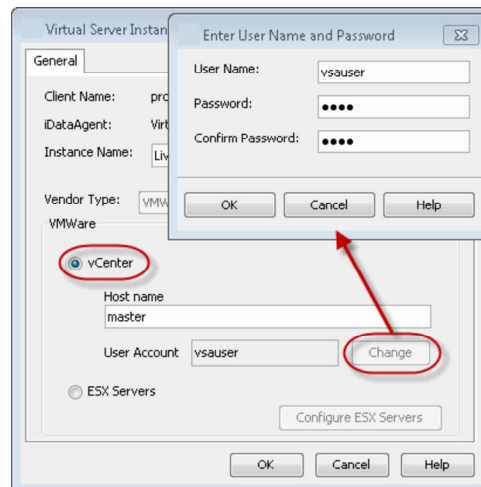
User-defined roles can also be created provided the above-mentioned privileges are included in those roles.

The following sections provide the steps necessary to configure user accounts for Virtual Centers and ESX Servers.

### VIRTUAL CENTER CREDENTIALS

1. Navigate to **Client Computers | <Client> | Virtual Server**.
2. Right-click the instance and click **Properties**.
3. In the **VMware | vCenter** area, click the **Change** button.
4. Enter the username and password.
 

The password must not contain single-quote (') or double-quote (") characters.
5. Click **OK** to save your changes.
6. Click **OK**.



### PERMISSIONS FOR CUSTOM USER ACCOUNTS

You can create a separate account for backup and restore operations. When you create a user account, following system privileges are automatically added to account:

| <b>CATEGORY</b> | <b>AVAILABLE PERMISSIONS</b> |
|-----------------|------------------------------|
| System          | Anonymous<br>Read<br>View    |

Ensure that the following permissions are assigned to the user account:

#### **BACKUP PERMISSION REQUIREMENTS**

| <b>Category</b>                                                                  | <b>Available Permissions</b>                                                                                                                                   |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Datastore                                                                        | Allocate space<br>Browse datastore<br>Configure datastore<br>Low level file operations<br>Remove datastore<br>Rename datastore<br>Update virtual machine files |
| Global                                                                           | Disable methods<br>Enable methods<br>Licenses                                                                                                                  |
| Host - Configuration                                                             | Advanced settings<br>Connection<br>Storage partition configuration<br>System Management                                                                        |
| Virtual machine - Configuration                                                  | Add existing disk<br>Add new disk<br>Add or remove device<br>Change resource<br>Disk change tracking<br>Disk lease<br>Remove disk<br>Settings                  |
| Virtual machine - Provisioning                                                   | Allow read-only disk access<br>Allow virtual machine download<br>Clone virtual machine                                                                         |
| Virtual machine - Snapshot Management ("Virtual machine - State" in vSphere 4.1) | Create snapshot<br>Remove Snapshot                                                                                                                             |

#### **RESTORE PERMISSION REQUIREMENTS**

| <b>Category</b>                 | <b>Available Permissions</b>                                                                                                      |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Datastore                       | Allocate space<br>Browse datastore<br>Configure datastore<br>Remove datastore<br>Rename datastore<br>Update virtual machine files |
| Host - Configuration            | Advanced settings<br>Connection<br>Storage partition configuration<br>System Management                                           |
| Network                         | Assign network                                                                                                                    |
| Resource                        | Assign vApp to resource pool<br>Assign virtual machine to resource pool                                                           |
| Virtual machine - Configuration | Add existing disk<br>Add new disk<br>Add or rRemove device                                                                        |

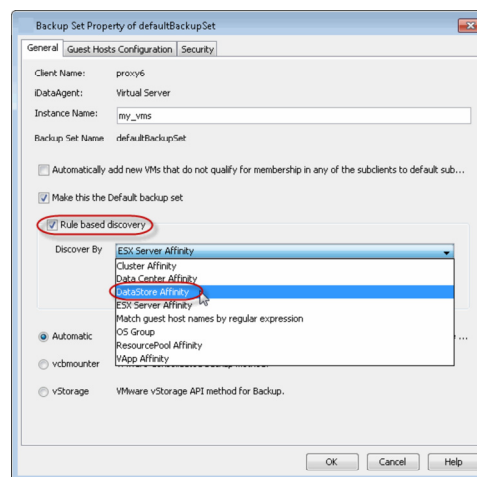
|                                                                                  |                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                  | Advanced<br>Change CPU count<br>Change resource<br>Disk change tracking<br>Disk lease<br>Host USB device<br>Memory<br>Modify device settings<br>Raw device<br>Reload from path<br>Remove disk<br>Rename<br>Reset guest information<br>Settings<br>Swapfile placement<br>Upgrade virtual machine compatibility ("Upgrade virtual hardware " in vSphere 4.1") |
| Virtual machine - Interaction                                                    | Power Off<br>Power On                                                                                                                                                                                                                                                                                                                                       |
| Virtual machine - Inventory                                                      | Create new<br>Register<br>Remove<br>Unregister                                                                                                                                                                                                                                                                                                              |
| Virtual machine - Provisioning                                                   | Allow disk access<br>Allow read-only disk access<br>Allow virtual machine download<br>Mark as template (to restore VM template)                                                                                                                                                                                                                             |
| Virtual machine - Snapshot Management ("Virtual machine - State" in vSphere 4.1) | Create snapshot<br>Remove Snapshot<br>Revert to snapshot                                                                                                                                                                                                                                                                                                    |

## CONFIGURING AUTO-DISCOVERY BY DATASTORE AFFINITY OF VIRTUAL MACHINES

It is recommended to configure automatic discovery of virtual machines by data store affinity if you have a large VMware environment with many virtual machines, ESX servers and datastores.

When configured, new virtual machines found in the datastore are automatically assigned to the desired subclient and backed up when backup operations on the subclient are performed.

1. From the CommCell Browser, right-click the backup set for which you want to discover guest hosts and then click **Properties**.
2. Select **Rule-Based Discovery**.
3. Click **Discover By** drop-down box and select **DataStore Affinity**.
4. Click **Configure**.
5. From the **Datastore Configuration for Auto Discover** dialog box, click **Discover Data Stores**.
6. From the **Auto Discover Data Stores** dialog box, locate the datastores you wish to configure for auto discovery and select the subclient you wish to associate each with.  
To exclude a select number of datastores from being backed up, choose the **Do Not Backup** option in the **Subclient** column.
7. Click **OK** to save your changes.
8. Click **OK** from the **Datastore Configuration for Auto Discover** dialog box.



## CONFIGURING SUBCLIENTS THROUGH THE COMMAND LINE

Use the following steps to configure a subclient with SnapProtect properties:

1. Download the update\_subclient\_add\_template.xml file and save it on the computer from where the command will be executed.

2. Select the operation that you want to run from the sections below, and execute the command from the <Software\_Installation\_Directory>/Base folder after substituting the parameter values.

#### SET BACKUP TYPE

```
qoperation execute -af update_subclient_add_template.xml -appName 'Virtual Server' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -backupType xxxxx
```

#### USE PROXY TO PERFORM SNAPPROTECT BACKUPS

```
qoperation execute -af update_subclient_add_template.xml -appName 'Virtual Server' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -useProxy/clientName xxxxx
```

#### SET THE TRANSPORT MODE FOR VMWARE

```
qoperation execute -af update_subclient_add_template.xml -appName 'Virtual Server' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -transportModeForVMWare xxxxx
```

#### SET THE PROXY FOR THE ESX HOST

```
qoperation execute -af update_subclient_add_template.xml -appName 'Virtual Server' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -isSnapBackupEnabled true -proxyESXHost xxxxx
```

#### ENABLE APPLICATION AWARE BACKUPS AND TRUNCATE EXCHANGE DATABASE LOGS

```
qoperation execute -af update_subclient_add_template.xml -appName 'Virtual Server' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -isSnapBackupEnabled true -backupForGranularRecovery true -truncateExDBLogs true
```

#### USE SEPARATE PROXY FOR SNAP TO TAPE OPERATION

```
qoperation execute -af update_subclient_add_template.xml -appName 'Virtual Server' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -isSnapBackupEnabled true -useSeparateProxyForSnapToTape true -separateProxyForSnapToTape/clientName xxxxx
```

#### SET THE STORAGE ARRAY TYPE

```
qoperation execute -af update_subclient_add_template.xml -appName 'Virtual Server' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -isSnapBackupEnabled true -snapShotEngineName 'xxxxx'
```

#### AVAILABLE PARAMETERS FOR SUBCLIENTS

The following table describes the parameters used in the above sections.

| PARAMETER                     | DESCRIPTION OF PARAMETER VALUES                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clientName                    | Name of the client computer.                                                                                                                                                                                                                                                                                        |
| backupsetName                 | Name of the backup set. If the backup set name is not specified in the command query, the default backup set is used by default.                                                                                                                                                                                    |
| appName                       | Name of the application. In this case it would be 'Virtual Server'.                                                                                                                                                                                                                                                 |
| subclientname                 | Name of the subclient.                                                                                                                                                                                                                                                                                              |
| backupType                    | Option to set the backup level at which the SnapProtect backup should run. Valid values are: <ul style="list-style-type: none"> <li>• FILE_LEVEL</li> <li>• VOLUME_LEVEL</li> <li>• DISK_LEVEL</li> </ul>                                                                                                           |
| useProxy/clientName           | Name of the client computer that will behave as the proxy. This is useful when you want a different computer to perform the backups.                                                                                                                                                                                |
| transportModeForVMWare        | Option to set the transport mode of your environment. Valid values are: <ul style="list-style-type: none"> <li>• AUTO, to allow the software to automatically set the transport mode based on your setup.</li> <li>• SAN</li> <li>• HOT_ADD</li> <li>• NAS</li> <li>• NBD_SSL</li> <li>• NBD</li> </ul>             |
| isSnapBackupEnabled           | Option to enable the SnapProtect configuration on the subclient.<br>Valid values are true/false.                                                                                                                                                                                                                    |
| backupForGranularRecovery     | Option to enable the application aware backup operation to allow granular recovery of files. Valid values are true/false.<br>When this option is set to <b>true</b> , you can also truncate the Exchange Database logs using the <b>truncateExDBLogs</b> parameter. Valid values for this parameter are true/false. |
| useSeparateProxyForSnapToTape | Option to enable the use of a proxy computer to perform SnapProtect operations in a different Virtual Server client. Valid values are true/false.<br>When this option is set to <b>true</b> , you also need to specify proxy computer using the <b>separateProxyForSnapToTape/clientName</b> parameter.             |
| snapShotEngineName            | Name of the storage array to be configured with the subclient. Valid values are:                                                                                                                                                                                                                                    |



The name of the storage array should match with the name displayed in the **Available Snap Engine** list in the subclient properties.

- Data Replicator
- 3PAR Clone
- 3PAR Snap
- Dell Compellent Snap
- Dell Equallogic Clone
- Dell Equallogic Snap
- EMC Celerra
- EMC CLARiiON SnapView Clone
- EMC CLARiiON SnapView Snap
- EMC TimeFinder BCV
- EMC TimeFinder Clone
- EMC TimeFinder Snap
- EMC CLARiiON SnapView Snap
- Fujitsu ETERNUS DX Clone
- Fujitsu ETERNUS DX Snap
- HDS Copy on Write Snapshot
- HDS Shadow Image
- HP EVA Clone
- HP EVA Snapshot
- IBM XIV Snap
- IBM SVC FlashCopy
- IBM SVC Space-efficient FlashCopy
- LSI Snapshot
- LSI Volume Copy
- NetApp
- Nimble Storage CS-Series Snap

## TRUNCATING SQL DATABASE LOGS

When you are using Virtual Server iDataAgent to create the snapshot of a SQL server, you can truncate the SQL server database logs before creating the snapshot. Follow the steps given below to truncate the SQL server database logs:

1. Install the Microsoft SQL Server iDataAgent for restore only on the virtual machine which has the SQL server. For more information, refer to Installing Restore Only Agents.

Once you install the agent, the CvSQLBackupUtility will be available in the <Base> folder under <Installation Directory> on the virtual machine. This utility will be used to truncate the SQL server database logs.

2. Create batch file with name <post-thaw-script.bat > and type the following command in the batch file. as below

```
CvSQLBackupUtility.exe -server <SQL Server> -database <databasename> -op <operation>
```

This command will execute the SQL command to truncate logs.

For example:

```
<Install Directory>\Base\CvSQLBackupUtility.exe" -server VSA_SQL2 -database ReportServer -op truncatelog
```

3. Create directory backupScripts.d under C:\Program Files\VMware\VMware Tools and copy the above batch file to this location.

The post-thaw-script location varies based on ESX versions For more information refer to [http://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=1006671](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006671).

When you perform the SnapProtect backup of the SQL server, the batch file will be executed while creating the snapshot and the SQL database logs will be truncated.

## VERIFY SNAPPROTECT BACKUPS

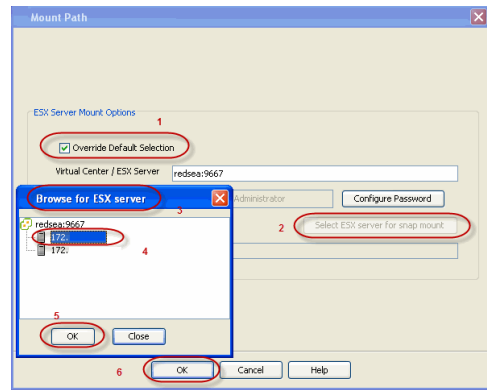
You can verify a backup to ensure that you can restore the virtual machine.

The recovery verification recreates the virtual machine to ensure backed up application and data are available as expected.

### MOUNT THE SNAPSHOT

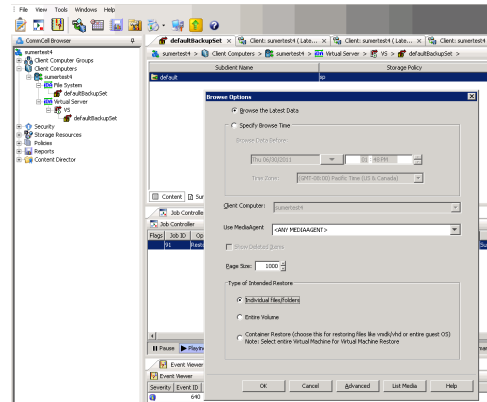
1. From the CommCell Browser, right-click the subclient that contains the virtual machine backup that you want to verify, click **All Tasks | List Snaps**.

2. Right-click the snapshot that you wish to verify and select **Mount**.
  3. From the **Mount Path** dialog box, click the **Select ESX server for snap mount** option.
  4. Select an ESX server from the **Browse for ESX Server** dialog box.
- As this ESX server will be used to create the virtual machine, it is recommended that you select a non-production server.
5. Click **OK**.



**BROWSE THE DATA**

6. From the CommCell Browser, right-click the subclient that contains the backup that you want to verify and click **All Tasks | Individual files/folders**.
7. Click **OK**.

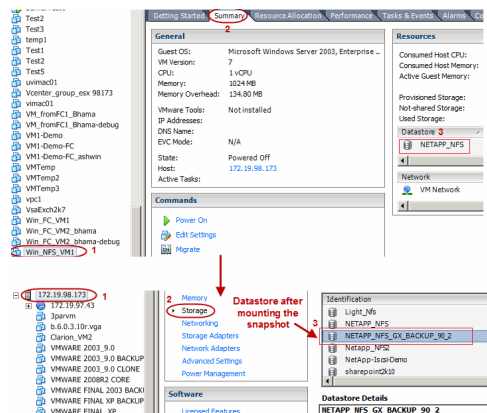


**BROWSE NEW DATASTORE AND REGISTER THE VIRTUAL MACHINE**

8. From the VI client, ensure that the new virtual machine from the backup is registered. The virtual machine name will be in the [OriginalVMName]\_[BackupJobID]\_GX\_BACKUP format.

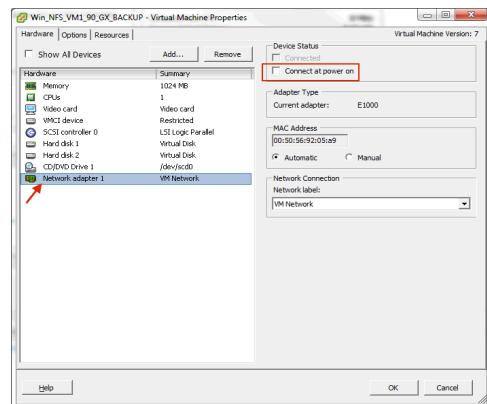
If the virtual machine is not registered, follow the steps given below to browse the new datastore that is created and register the virtual machine.

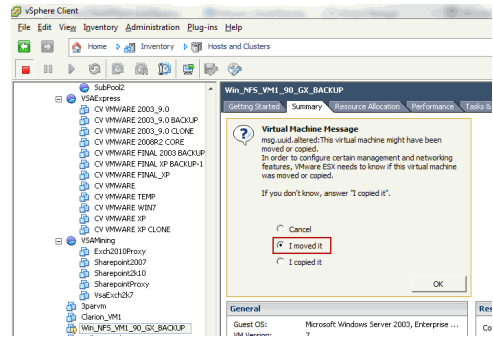
- i. Click the virtual machine you want to register and click the **Summary** tab to see the datastore name.
- ii. Click the ESX server you selected in Step 4, and click the **Storage** option.
- iii. Identify the new datastore created after mounting the snapshot and register the virtual machine. The new datastore will have the following name:  
[OriginalDatastoreName]\_GX\_BACKUP\_[BackupJobID]
- iv. Specify a name for the virtual machine.



**VERIFY THE DATA USING VI CLIENT**

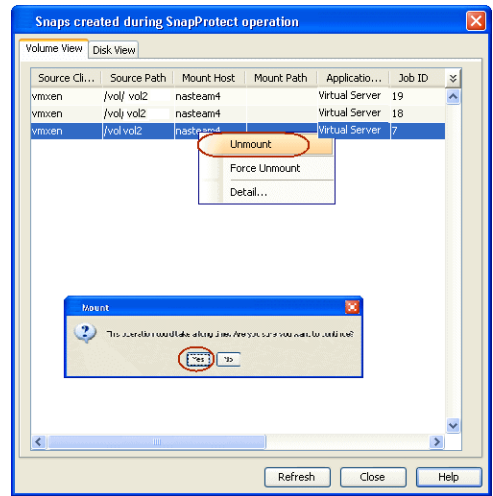
9. Right-click the virtual machine and select **Edit Settings**. Click **Network adapters**.
10. Clear the **Connect at power on** checkbox in the **Virtual Machine Properties** dialog box for all the available network adapters.
11. Click **OK**.
12. Turn on the virtual machine.
13. Click the **Summary** tab and select the **I moved it** option.
14. Login to the virtual machine and verify the applications and data.
15. After verification is complete, power off the virtual machine.
16. Right-click the virtual machine and select the **Remove from inventory** option.





**UNMOUNT THE SNAPSHOT**

17. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, click **All Tasks** | **List Snaps**.
18. Right-click the snapshot that you wish to unmount and select **Unmount**.



**CHOOSING RESTORE TYPES**

When restoring VMware data, it is important to consider the backup level that was originally performed. The following table illustrates the types of restores available for each backup level:

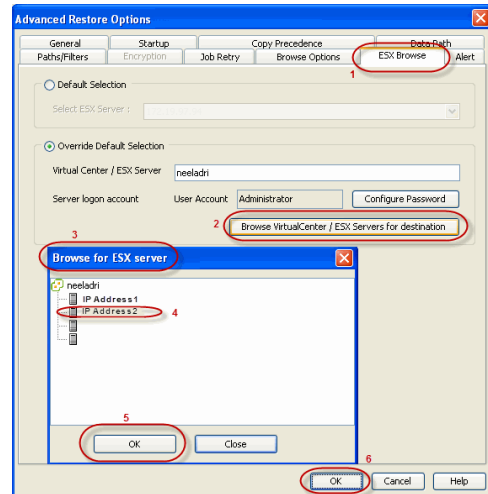
| BACKUP LEVEL                                              | RESTORE LEVEL FROM SNAP                                                                                                                                            | RESTORE FROM TAPE                                                                                  | NOTES                                                                                       |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Disk-Level                                                | Disk-Level (as virtual machine)<br>Disk Level (as VMDK file)                                                                                                       | Disk-Level (as virtual machine)<br>Disk Level (as VMDK file)                                       |                                                                                             |
| Disk-Level with <b>Enable Granular Recovery</b> enabled   | Disk-Level (as virtual machine)<br>Disk-Level (as VMDK file)<br>Volume-Level (as physical volume)<br>Volume-Level (as VHD)<br>Volume-Level (as VMDK)<br>File-Level | Disk-Level (as virtual machine)<br>Disk-Level (as VMDK file)<br>File-Level                         |                                                                                             |
| Volume-Level                                              | Disk-Level (as virtual machine)<br>Disk Level (as VMDK file)                                                                                                       | Volume-Level (as physical volume)<br>Volume-Level (as VHD)<br>Volume-Level (as VMDK)               | Supported only with volumes formatted with the NTFS file system.                            |
| Volume-Level with <b>Enable Granular Recovery</b> enabled | Disk-Level (as virtual machine)<br>Disk-Level (as VMDK file)<br>Volume-Level (as physical volume)<br>Volume-Level (as VHD)<br>Volume-Level (as VMDK)<br>File-Level | Volume-Level (as physical volume)<br>Volume-Level (as VHD)<br>Volume-Level (as VMDK)<br>File-Level | Supported only on Windows-based VMware virtual servers formatted with the NTFS file system. |
| File-Level                                                | File-Level<br>Disk-Level (as virtual machine)<br>Disk-Level (as VMDK file)<br>Volume-Level (as physical volume)<br>Volume-Level (as VHD)                           | File-Level                                                                                         | For file level restores, select <b>Enable Granular Recovery</b> option.                     |

Volume-Level (as VMDK)

## RESTORE TO A DIFFERENT ESX SERVER

You can override the default restore selection by choosing a different Virtual Centre or ESX Server to restore, by following the steps given below:

1. From the CommCell Console, right-click the **Subclient** and select **Browse Backup Data**.
2. Click **OK** and select the virtual machine under the backupset. Its entire contents will be automatically selected in the right pane. Click **Recover All Selected**.
3. Click **Advanced** from the **Restore Options** dialog box.
4. Select the **ESX Browse** tab.
5. The **Default Selection** has the IP address of the ESX Server pre-populated.
6. Select **Override Default Selection** to locate a different destination.
7. Enter appropriate credentials to logon to the server using **Configure Password** button.
8. Click **Browse VirtualCentre/ESX Servers for destination** to provide the ESX Server path to which the virtual machine will be restored.
9. Select the appropriate ESX server.
10. Click **OK** to close the **Browse for ESX Server** dialog box.
11. Click **OK** to close the **Advanced Restore Options** dialog box.



## RESTORING FILES AND FOLDERS

To restore files and folders to a Windows client, the client must have one of the following components installed:

- Windows File System iDataAgent
- Restore Only Agent for Windows File System.

Consider that the following before restoring files and folders from a virtual machine:

- The virtual machine has the MBR partition. If the virtual machine has GPT partition, you can restore files from a backup copy. For more information, refer to Restore Data from a Backup Copy.
- You must perform the backup using the **VMware Storage API method**. For more information, refer to Configuring Backups for vSphere VADP Environments.
- You cannot restore any archived files and folders.
- It is recommended to perform the file-level restores from disk or volume-level backups only when you are restoring small files. For example, restoring a 2GB file from a disk-level backup is not recommended.

You can restore files from NTFS file systems with the following limitations:

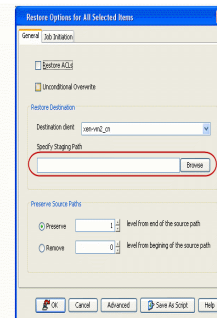
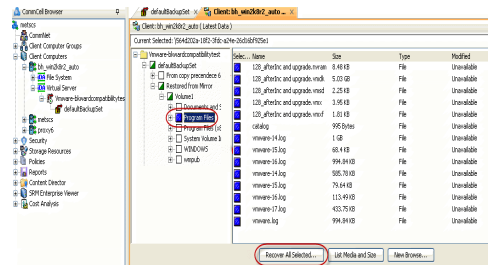
- The formatted cluster size (allocation unit) must be 1024 or greater.
- You cannot restore any archived files and folders.
- You cannot restore any file that has zero bytes, symbolic links, or hard links associated with it.
- You cannot restore files that have been dehydrated by Windows 2012 dedup.
- You cannot restore files from volumes created on Windows Storage Spaces.

If you cannot restore a file, you can restore the complete virtual machine or the disk that contains the file.

When restoring a file or folder on a virtual machine, the **Enable Granular Recovery** must have been selected when the backup was performed.

1. From the CommCell Console, perform a **Browse and Restore** operation.
2. In the **Browse Options** window, click **Individual files/folders**.
3. Click **OK**.
4. In the **Browse** window, click a file or folder in the right pane, and then click **Recover All Selected**.
5. From the **General** tab, specify a **Staging Path**. This is the destination path to which the file will be restored.
6. Click **OK**.

The **Preserve Source Path/Remove Source Path** feature is supported for File level restores from File level backup jobs. It is not relevant for Volume Level and Disk Level backups and restores.



## RESTORE FILES FROM A SNAPSHOT (LIVE BROWSE)

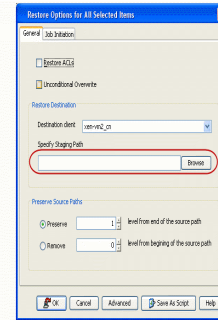
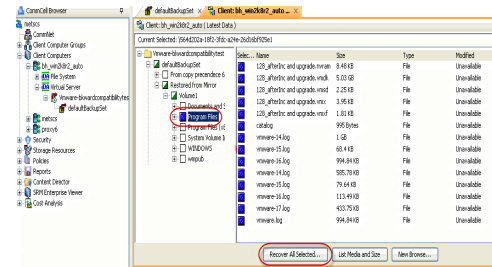
You can restore files and folders from a snapshot when a backup is performed without enabling the **Enable Granular Recovery** advanced backup option.

Before performing the browse and restore from a snapshot, note the following:

- This feature is available for Windows-based VMware virtual machines but not available for any other operating system.
- This feature is available for the MBR partition. If the virtual machine has GPT partition, you can restore files from a backup copy. For more information, refer to Restore Data from a Backup Copy.
- You must perform the backup using the **VMware Storage API method**. For more information, refer to Configuring Backups for vSphere VADP Environments.

Follow the steps given below to perform the browse and restore from a snapshot:

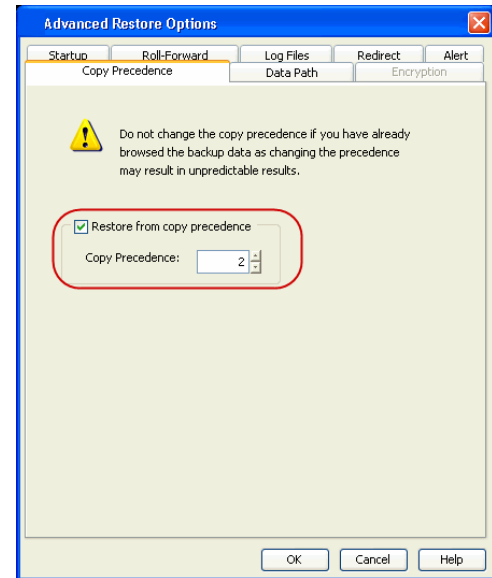
1. From the CommCell Browser, navigate to **Client Computers | <Client> | Virtual Server | <Instance>**.
2. Right-click the subclient that contains the data that you want to restore and click **Browse Backup Data**.
3. In the **Browse Options** window, click **Individual files/folders**.
4. Click **OK**.
5. Select the virtual machine that contains the files that you wish to restore.  
Depending on the hardware configuration, it may take some time to mount the snapshot on the ESX server before displaying the files and folders.
6. In the **Browse** window, right-click a file or folder in the right pane and click **Recover All Selected**.
7. From the **General** tab, specify a **Staging Path**. This is the destination path to which the file will be restored.
8. Click **OK**.



## RESTORE DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** dialog box and start the restore job.



## DATA AGING FOR SNAPPROTECT SNAPSHOTS

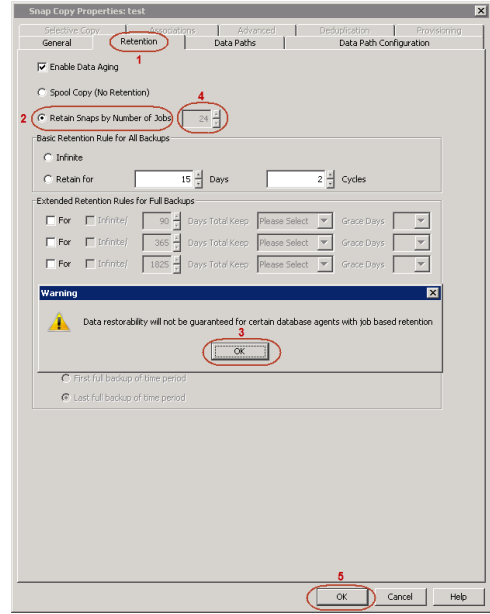
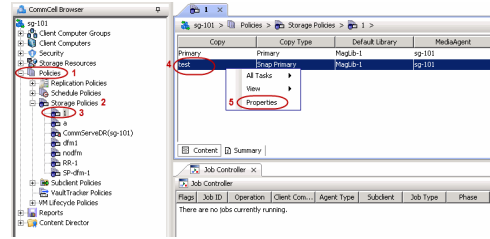
The following procedures describe the available retention configurations for snapshots. For movement to media retention, refer to Data Aging - Getting Started.

### RETENTION BY NUMBER OF JOBS

By default, snapshots are pruned based on the number of retention days and cycles specified in the storage policy. You can configure your snapshot copy to retain a defined number of SnapProtect backup jobs. When the total number of jobs goes above the specified retention number, the remaining jobs will be pruned. This configuration is recommended for File System and File System like Agents. This feature is supported for SnapProtect operations performed using the NetApp storage array.

The **NetApp Snap Management** license is required for retaining snaps by number of jobs.

1.
  - From the CommCell Console, navigate to **Policies | Storage Policies | <Storage Policy>**.
  - Right-click the primary snapshot copy and click **Properties**.
  
2.
  - Click the **Retention** tab.
  - Click **Retain Snaps by Number of Jobs**.
  - Click **OK** to the warning dialog box.
  - Specify the number of jobs to be retained for the primary copy.
  - Click **OK**.



## OPTIONS NOT SUPPORTED FOR VMWARE

The following options are not supported for SnapProtect backup for Virtual Server iDataAgent - VMware:

- Physical RDMs.
- Virtual RDMs
- Virtual machines including Local disks.
- Virtual machines should have all disks on the same storage array, e.g. if you are using NetApp as the storage array, then all disks of the virtual machine under backup should reside on the NetApp file server.

## USING A SEPARATE ESX SERVER FOR A BACKUP COPY

The backup copy is an additional standby copy of data. It can be created during the SnapProtect backup or at a later time. You can use a separate proxy client and ESX Server to create a backup copy. If you want to reduce the time required for mounting the snapshot, you must use a local Proxy client and ESX server for backup copy operations.

The backup copy can be an inline backup copy, offline backup copy or netapp's vault or mirror copies.

For example: The default proxy client and ESX Server is in location A and you want to use the backup copy of the data from location B. In such scenario, you can use an ESX server in location B for creating backup copy and then restore virtual machines from the backup copy.

## CONFIGURING A SUBCLIENT TO USE A SEPARATE PROXY CLIENT

Follow the steps given below to use a separate proxy for creating the backup copy:

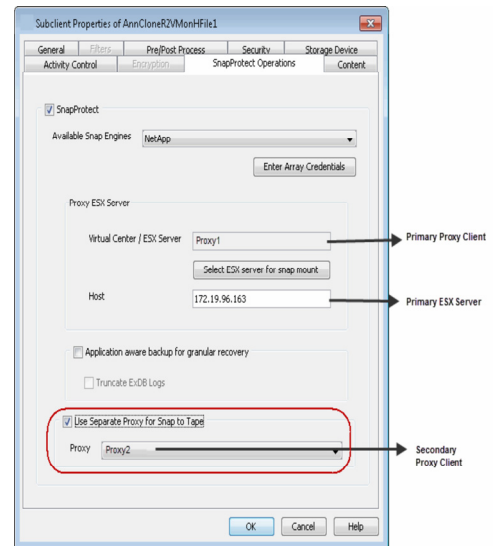
1. From the CommCell Browser, navigate to **Client Computers | <Client> | Virtual Server | <Instance>**.
2. Right-click the subclient and select **Properties**.
3. Click the **SnapProtect Operations** tab.

The Proxy ESX Server section will display the Primary proxy client and Primary ESX Server.

4. Click **Use Separate Proxy for Snap To Tape** check box.
5. Select a Proxy client from the **Proxy** list.
6. Click **OK**.

The selected Proxy client will be treated as a secondary proxy client. It will be used to perform the Inline Backup copy, Offline Backup copy, NetApp Vault or NetApp Mirror operations.

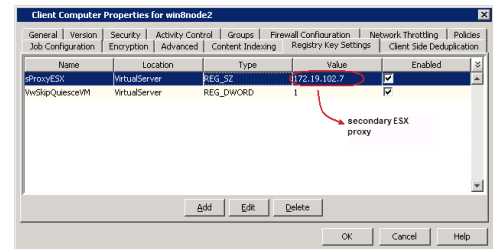
You can use the default ESX Server to create backup copy or you can specify a secondary ESX Server for the backup copy.



## SPECIFYING SECONDARY ESX SERVER FOR BACKUP COPY OPERATIONS

Follow the steps given below to specify a secondary ESX Server. The snapshots will be mounted to the specified ESX proxy and not to the Primary proxy.

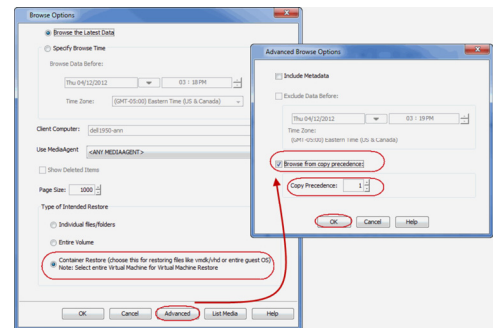
1. From the CommCell Browser, navigate to **Client Computers**.
2. Right click the Secondary Proxy client and click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type sProxyESX.
6. In the **Location** list, type HKEY\_LOCAL\_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\
7. In the **Type** list, select **REG\_SZ**.
8. In the **Value** field, type the Host name or IP address of the secondary ESX Server.
9. Click **OK**.



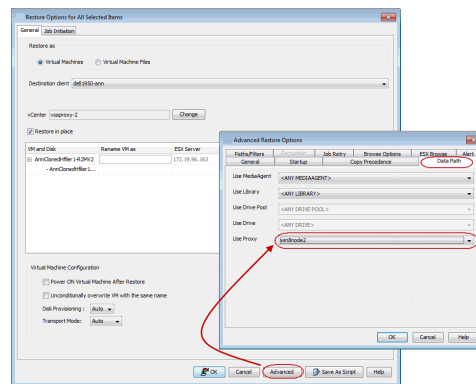
## RESTORING VIRTUAL MACHINES FROM A SNAPSHOT MOUNTED ON THE SECONDARY ESX SERVER

Follow the steps given below to perform the browse and restore from a snapshot mounted on the alternate ESX Server:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Virtual Server | <Instance>**.
2. Right-click the subclient that contains the data that you want to restore and click **Browse Backup Data**.
3. Select the **Type of Intended Restore**.  
If you haven't selected the **Enable Granular Recovery** option while performing the backup, select the secondary proxy in the **Use MediaAgent** list.
4. Click **Advanced**.
5. Select the **Browse from copy precedence** check box.
6. Enter the **Copy Precedence** of the snapshot copy.  
You can find out the copy precedence of the snapshot copy from the **Copy Precedence** tab of the **Storage Policy Properties** dialog box.
7. Click **OK**.
8. Click **OK**.  
The data from the snapshot mounted on the secondary ESX server will be displayed.
10. Select the virtual machine that you want to restore and Click **Recover All Selected**.
11. From the **General** tab, click **Advanced**.



12. Click the **Data Path** tab.
  13. Select the secondary proxy client from the **Use Proxy** list.
  14. Click **OK**.
- The secondary ESX server will be used to restore the virtual machine.



## DISABLING VMWARE QUIESCE

Quiescing indicates pausing or altering the state of running processes on a computer, particularly those that might modify information stored on disk during a backup, to guarantee a consistent and usable backup.

For windows Microsoft VSS inside the guest will be used to quiesce the file system and applications. This ensures that the data consistency of the file system and all VSS supported applications. By default VMware will engage all of the VSS writers that are configured inside the guest. If it is necessary to exclude a writer please refer to <http://kb.vmware.com/kb/1031200>

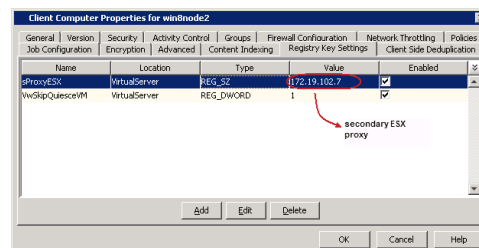
For Linux, the vmsync driver will be used to quiesce the file system and applications. This is included with VMware tools. The vmsync driver ensures that the file system is in a consistent state prior to the vmware snapshot being created. The vmsync driver is only supported with vSphere 5.0 and above.

Consider the following before enabling or disabling the quiescing during the backup:

- **Hardware Snapshot with Quiescing** - When you perform the IntelliSnap backup of a subclient, a hardware snapshot of all the virtual machines is created. Before the snapshot creation, the quiescing will be performed automatically for the operating system and applications on all the virtual machines in the subclient.
- **Crash consistent hardware snapshot** - The backup process may slow down because of the quiescing. If you do not want to perform quiescing before the snapshot creation, you can disable the quiescing. If you disable the quiescing, the crash consistent hardware snapshot will be created.

You can disable quiescing to reduce the backup time. If you disable quiescing, you can perform backup of the virtual machines which has .vmdks with same name.

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right click the Proxy client and click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type VwSkipQuiesceVM.
6. In the **Location** list, type HKEY\_LOCAL\_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\
7. In the **Type** list, select **REG\_DWORD**.
8. In the **Value** field, type 1.
9. Click **OK**.



## PRE/POST PROCESSING USING VMWARE TOOLS

You can use the VMware tools to perform the any operations before or after the backup. For example: A virtual machine hosts a oracle database and you want to enable the Hot backup of the database before performing the backup, you can run a script using the VMware Tools.

For more information about running scripts on Windows virtual machines, refer to <http://kb.vmware.com/kb/1006671>

On the Linux virtual machines, the script /usr/sbin/pre-freeze-script will be executed when the software snapshot is created and /user/sbin/post-freeze-script will be executed when the software snapshot is removed. Ensure that these scripts are executable by the VMware tools user.

The following scripts are available to perform the Pre/Post processes using VMware tools:

| OPERATION                                                                                                                                                                               | PROCEDURE                                                                                             | SCRIPTS                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------|
| The scripts can be used to take snapshot of a VM with DB2 Application. This script allows VMWARE to suspend I/O updates to DB2 database till VMWARE LINUX guest snap shot is completed. | 1. On a Linux virtual machine, copy the pre-freeze-script and post-thaw-script to /usr/bin directory. | pre-freeze-script.sh<br>post-thaw-script.sh |



|                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                               | <ol style="list-style-type: none"> <li>Copy write_suspend and write_resume scripts to a location where DB2 database can execute it. (Preferably to a directory under DB2 home)</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>write_resume.sh<br/>write_suspend.sh</p>                                                                                                  |
| The scripts can be used to take snapshot of a VM with MAXDB Application. This script allows VMWARE to suspend I/O updates to MAXDB database till VMWARE LINUX guest snap shot is completed.   | <ol style="list-style-type: none"> <li>On a Linux virtual machine, copy the pre-freeze-script and post-thaw-script to /usr/bin directory.</li> <li>Copy suspend_logwriter and resume_logwriter scripts to a location where MAXDB database can execute it. (Preferably to a directory under MAXDB home)</li> </ol>                                                                                                                                                                                                                                                                                                                                             | <p>pre-freeze-script.sh<br/>post-thaw-script.sh<br/>resume_logwriter.sh<br/>suspend_logwriter.sh</p>                                         |
| The scripts can be used to take snapshot of a VM with Oracle Application. This script allows VMWARE to suspend I/O updates to Oracle database till VMWARE LINUX guest snap shot is completed. | <ol style="list-style-type: none"> <li>On a Linux virtual machine, copy the pre-freeze-script and post-thaw-script to /usr/bin directory.</li> <li>Copy pre-freeze-script.sql and post-thaw-script.sql scripts to a location where Oracle database can execute it. (Preferably to a directory under Oracle home)</li> </ol> <p>These scripts change the entire database to backup mode. If the virtual machine has Oracle iDataAgent installed on it, you can also use the consistent-archivelog-backup.rman script as a sample to run archivelog backup. This will get a consistent snap and also all the latest archived logs and current control file.</p> | <p>pre-freeze-script.sh<br/>post-thaw-script.sh<br/>pre-freeze-script.sql<br/>post-thaw-script.sql<br/>consistent-archivelog-backup.rman</p> |
| The scripts can be used to take snapshot of a VM with Sybase Application. This script allows VMWARE to suspend I/O updates to Sybase database till VMWARE LINUX guest snap shot is completed. | <ol style="list-style-type: none"> <li>On a Linux virtual machine, copy the pre-freeze-script and post-thaw-script to /usr/bin directory.</li> <li>Copy pre-freeze-script.sql and post-thaw-script.sql scripts to a location where Sybase database can execute it. (Preferably to a directory under Sybase home)</li> </ol> <p>These scripts execute sybase quiesce commands which will stop updates to databases.</p>                                                                                                                                                                                                                                        | <p>pre-freeze-script.sh<br/>post-thaw-script.sh<br/>pre-freeze-script.sql<br/>post-thaw-script.sql</p>                                       |

## ADDITIONAL OPTIONS

Several additional options are available to further refine your backup and restore operations. The following table describes the additional options:

| OPTION                              | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | RELATED TOPICS                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>Job Results Directory</b>        | <p>Ensure that the full path name for the Job Results Directory, combined with the VMDK file name, is no greater than 255 characters in length.</p> <ol style="list-style-type: none"> <li>From the CommCell Browser, right-click the icon of the client computer whose job results path you want to change, then click <b>Properties</b>.</li> <li>From the <b>Job Configuration</b> tab of the <b>Client Computer Properties</b> dialog box, click <b>User Name/Password</b> to establish or change the Impersonate User account to access the Job Results Directory. Click <b>OK</b> once you have administered the account.</li> <li>From the <b>Job Configuration</b> tab, type a new job results path in the <b>Job results path</b> field.<br/>You can also click <b>Browse</b> to browse to a new job results path from the <b>Browse for Job Result Path</b> dialog box. Click <b>OK</b>.</li> <li>Click <b>OK</b> to save your changes.</li> </ol> | Refer to Job Management.                                                     |
| <b>Pre/Post Commands</b>            | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>        | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol>                                                                                                                                              |                                                                              |
| <b>Select a Job for Backup Copy</b> | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View</b></li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                              |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                     |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
|                                             | <p><b>Jobs.</b></p> <p>2. Right-click the job and then click <b>Pick for Backup Copy.</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                     |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <p>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs.</b></p> <p>2. Right-click the job and then click <b>Do not Backup Copy.</b></p>                                               |                                                     |
| <b>Offline Snap Copy Job Summary Report</b> | Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.                                                                                                                                                                                                                                                                                                                                                                                                                                                 | See Backup Copy Job Summary Report for more details |
| <b>Find</b>                                 | <p>Use Find to search and locate files or folders from a SnapProtect backup. If you want to restore a specific file or folder from a backup set or subclient, you can search the file or folder in the backup set or subclient.</p> <p>Before searching the subclient, ensure that all the files and folders in the subclient are included in the index. The files and folders are included in the index when you perform the <b>File Level</b> backup or <b>Enable Granular Recovery</b> before performing the <b>Volume Level</b> or <b>Disk Level</b> backup.</p> | See Finding and Restoring for more details.         |

[Back to Top](#)

# Advanced - Microsoft Exchange Database SnapProtect™ Backup

## TABLE OF CONTENTS

### Proxy Configuration

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Pause Consistency Checks During Backups

### Restoring a Database

### Restoring VSS-Enabled Backups

- Restoring to a Storage Group
- Restoring to a Different Disk Location

### Restoring Data from a Backup Copy

### Additional Options

## PROXY CONFIGURATION

A proxy configuration interacting with Exchange Databases allows you to execute an ESE Integrity check against the Exchange Database. For the proxy to validate the Microsoft Exchange Database files, follow the steps below:

1. Install the proper version of the Microsoft Exchange Management Tools from the Exchange installation media on the proxy computer. This will allow you to select the proxy computer from the **Use Proxy** option when configuring your Exchange subclient.
2. When scheduling a SnapProtect backup job, click **Advanced** and ensure the **Perform Consistency Check** option is enabled to perform the integrity check upon snapshot index completion.

## MANAGING SNAPSHOTS

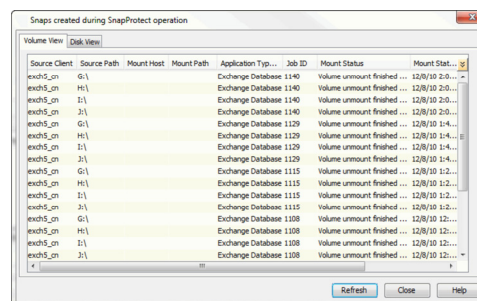
The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete, or revert.

### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
2. Right-click **Exchange Database** and click **All Tasks** | **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the Exchange Agent. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.



### MOUNT SNAPSHOTS

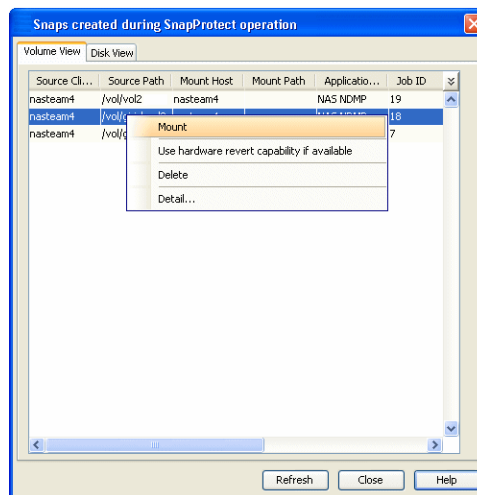
You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
2. Right-click **Exchange Database** and click **All Tasks** | **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.

On a Windows platform, enter a **CIFS Share Name** for the Agent.

6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

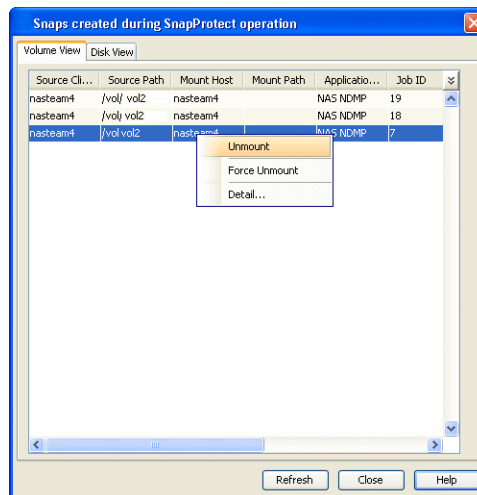


### UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers | <Client>**.
2. Right-click **Exchange Database** and click **All Tasks | List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



### DELETE SNAPSHOTS

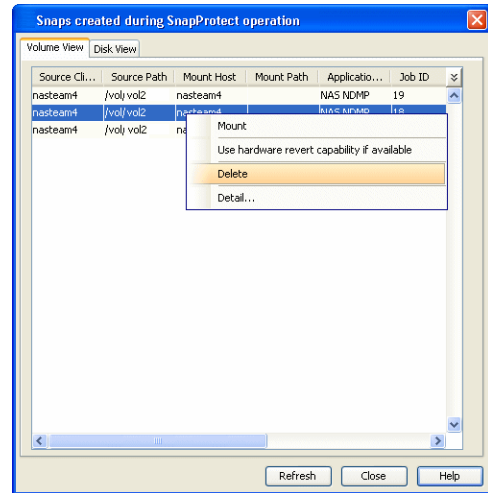
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers | <Client>**.
2. Right-click **Exchange Database** and click **All Tasks | List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

- Revert operations are not supported on Windows clustered disks.
- All the data stores should be manually dismounted.
- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.
  - It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
  - If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

## PERFORM AN APPLICATION AWARE REVERT

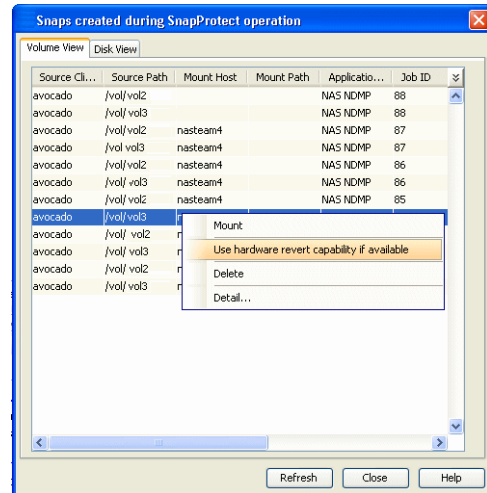
1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.
  - An application aware revert operation reverts back all the volumes included in the backup.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the application.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

## PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers | <Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, `confirm`.

5. Click **OK**.

- A hardware specific revert operation reverts back the volume included in the snapshot.
- For NetApp NFS configurations:
  - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
  - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
  - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



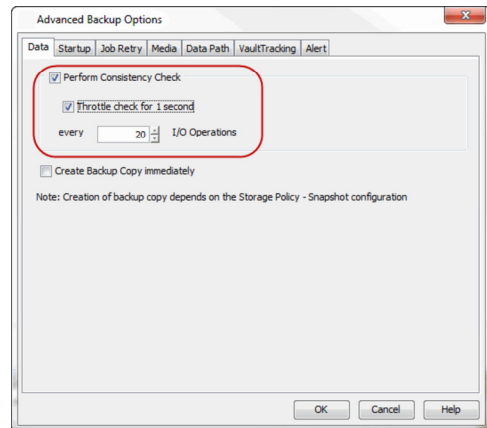
## SNAP RECONCILIATION

Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

## PAUSE CONSISTENCY CHECKS DURING BACKUPS

Pause points allow Exchange system resources to be made available periodically to other processes (e.g. send and receive e-mail messages) during the following:

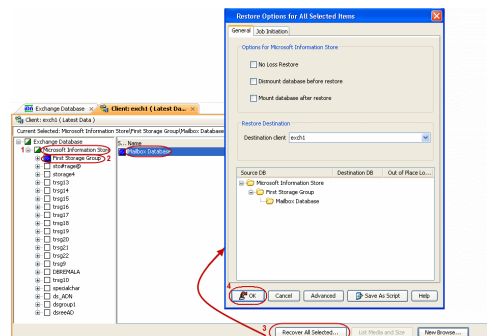
- Prolonged consistency checks of large databases
  - High load on the Exchange Server
1. From the CommCell Browser, navigate to **<Client> | Exchange Database**.
  2. Right click the **<Subclient>** and click **Backup**.
  3. Click **Advanced**.
  4. Click the **Data** tab and select the **Perform Consistency Check** option.
  5. Select the **Throttle check for 1 second** option and enter the number of I/O operations to complete before the throttle check is performed.
  6. Click **OK**.



## RESTORING A DATABASE

By default the database is restored to the same client from which it is backed up. Follow the steps given below to perform the in-place restore:

1. Ensure the database is marked for overwrite on the Exchange Server prior to performing the restore.
2. From the CommCell Console, navigate to **Client Computers | <Client>**.
3. Right-click **Exchange Database** and click **All Tasks | Browse Backup Data**.
4. Click **OK**.
4. In the left pane of the **Client Browse** window, navigate to **Exchange Database | Microsoft Information Store | <Storage Group>**.
5. Select the database to be restored in the right pane and click **Recover All Selected**.
6. Click **OK** to start the restore.
7. Manually mount the stores after the restore.



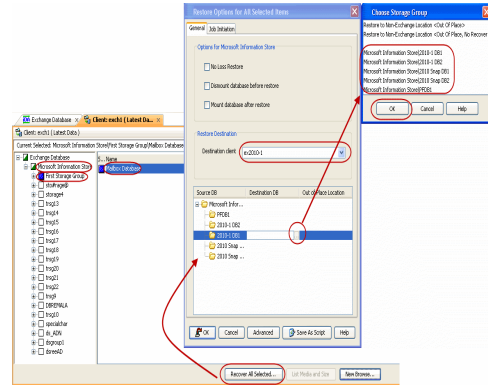
## RESTORING VSS-ENABLED BACKUPS

Use one of the methods below to restore VSS-Enabled backups for Exchange Server 2007 and 2010. When restoring VSS-enabled backups, the options **No Loss Restore** and **Mount database after restore** do not apply.

### RESTORING TO A STORAGE GROUP

You can restore the database stores to a different storage group (including Recovery Storage Groups) on the same Exchange Server, or to a different Exchange Server within the same Exchange organization.

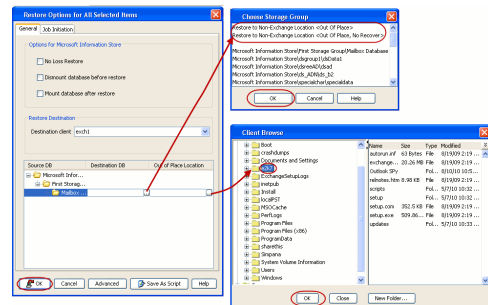
1. Ensure the database you want to restore is dismounted and marked for overwrite.
2. From the CommCell Console, navigate to **Client Computers | <Client>**.
3. Right-click **Exchange Database** and then click **All Tasks | Browse Backup Data**.
4. Click **OK**.
5. In the left pane of the **Client Browse** window, navigate to **Exchange Database | Microsoft Information Store | <Storage Group>**.
6. Select the database to be restored in the right pane and click **Recover All Selected**.
7. Select the **Destination client**.
8. Select the **Source DB** and double-click in the **Destination DB** column.
9. Click **..** and select a **Storage Group**.
10. Click **OK**.
11. Click **OK** to start the restore.
12. Manually mount the stores after the restore.



### RESTORING TO A DIFFERENT DISK LOCATION

You can restore the database stores to be a physically different location on disk (i.e., non-Exchange location) with a choice of whether or not to replay the logs.

1. From the CommCell Console, navigate to **Client Computers | <Client>**.
2. Right-click **Exchange Database** and then click **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. In the left pane of the **Client Browse** window, navigate to **Exchange Database | Microsoft Information Store | <Storage Group>**.
5. Select the database to be restored in the right pane and click **Recover All Selected**.
6. Select the **Destination client**.
7. Select the **Source DB** and double-click in the **Destination DB** column.
8. Click **..** and select one of the following options in the **Storage Group** dialog box:
  - o **Restore to Non-Exchange Location <Out of Place>** - The database will be restored to the specified location and the logs will be replayed.
  - o **Restore to Non-Exchange Location <Out of Place, No Recover>** - The database will be restored to the specified location and the logs will not be replayed.
9. Double click in the **Out of Place Location** column and click **..** to specify the fully-qualified destination.
10. Select the destination folder from the Destination client.
11. Click **OK**.
12. Click **OK** to start the restore.
13. Manually mount the stores after the restore.

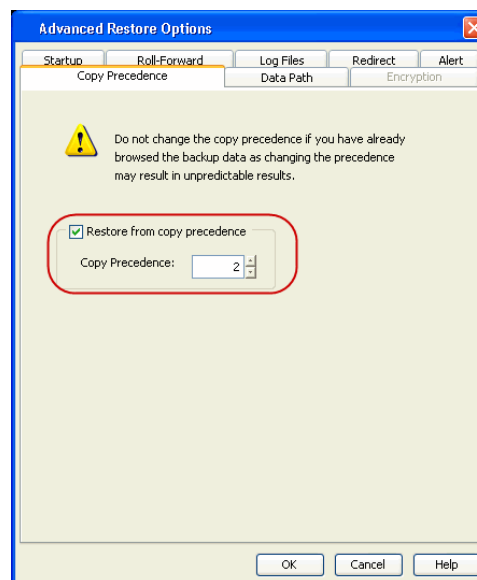


## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.

4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                                      | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | RELATED TOPICS                                                               |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>SCSI Reservation</b>                     | <p>SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key nSCSIReserveForSnap to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).</p> <p>If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail.</p>                                                                                                                                                                                                                                                                                                                                                                                     | For more information on registry keys, Registry keys                         |
| <b>Pre/Post Commands</b>                    | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                                                                                                                | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>                | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol> |                                                                              |
| <b>Select a Job for Backup Copy</b>         | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                          |                                                                              |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                      |                                                                              |
| <b>Offline Snap Copy Job Summary Report</b> | <p>Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | See Backup Copy Job Summary Report for more details                          |



[Back to Top](#)

# Advanced - Oracle SnapProtect™ Backup

## TABLE OF CONTENTS

### Configuring Offline Backup

### Configuring Log Backup

- Pruning the Logs After Backup Using RMAN

### Configuring Selective Online Full Backup

### Configuring Table Backups

### Configuring an ASM Instance

### Scheduling a Backup

### Disabling Verification of Datafiles During SnapProtect Backup

### Configuring SnapProtect Operations Using Command Line

### NFS SnapProtect for Oracle

### Configuring Oracle RAC Database SnapProtect Operations

- Configuring SnapProtect Operations Using a Single Node
- Configuring Online Backups for SnapProtect Subclients
- Configuring RMAN Backup Copy for SnapProtect Operations
- Disabling SP File Backup during Backup Copy Operations

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Restoring data From a SnapProtect Backup

- Restore Data from Snapshot Using RMAN
- Restore Data from Snapshot Using a Proxy Computer
- Restoring and Recovering an Entire Database to the Same Host
- Reverting an Entire Database to the Same Host
- Restoring and Recovering an Entire Database to a Previous Point-in-Time
- Restoring and Recovering an Entire Database to a new host
- Restoring Individual Datafiles/Tablespaces
- Restoring Archive Logs
- Restoring Database Tables to the Source Database
- Restoring Tables to a Different Database on the Same Host
- Setting up the Auxiliary Instance
- Using a User-defined Auxiliary Instance
- Disabling Clean-up of Auxiliary Instance after Restore
- Restoring Tables with Non-English Characters
- Exporting Table Objects
- Selecting/De-Selecting Dependent/Referenced Tables
- Including all Dependencies to the Dependent/Referenced Tables
- Deleting Existing Tables during a Restore
- Automatically Switching the Database Mode before a Restore
- Setting the Database Incarnation
- Enhancing Restore Performance
- Restoring from a SnapProtect and RMAN Mixed Environment

### Backup Copy Operations

- File System
- RMAN

### Restoring Data from Backup Copy

- Using File System
- Using RMAN

### Oracle Multi Instance Snap Optimization

- Configuring Multiple Instances using a Shared Storage On a Client
- SnapProtect Backup for Multiple Instances
- Restoring a database or datafiles /table spaces from a database
- Revert from a SnapProtect Job
- Backup Copy for Multiple Instances Using a Shared Storage on a Client

### Supported Volume Managers

### Options not applicable for Oracle SnapProtect

## Options not applicable for Oracle Snap Restore

### Additional Options

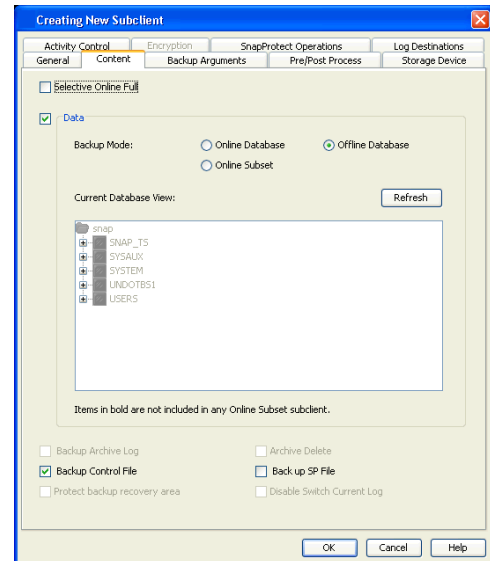
## CONFIGURING OFFLINE BACKUP

Offline backups can be performed when the database is in offline or online mode. If the database is online, it shuts down the database, performs the backup and then brings up the database back.

1. From the CommCell Browser, navigate to **<Client> | Oracle**.
2. Right-click the **<Instance>** and click **All Tasks | New Subclient**.
3. In the **Subclient Name** box, type a name.
4. Click the **Content** tab.
5. Select the **Offline Database** checkbox.
6. Click the **Storage Device** tab.
7. In the **Data Storage Policy** box, select a storage policy name.
8. Click the **SnapProtect Operations** tab.
9. Click **SnapProtect** to enable SnapProtect backup for the selected subclient.
10. Select the storage array from the **Available Snap Engine** drop-down list.
11. 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.

12. Click **OK**.

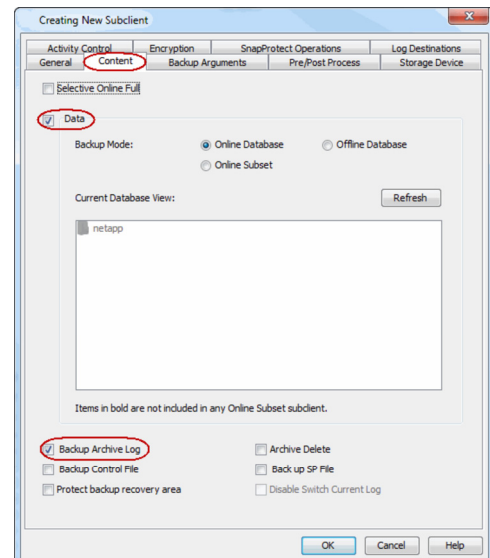


## CONFIGURING LOG BACKUPS

Once you perform a SnapProtect backup, perform a log backup. You will need to create a separate subclient for log backups. By default, the system will use data storage policy for SnapProtect backups and backup copy. If you create a log specific subclient, the log specific storage policy is used for SnapProtect backups and backup copies.

Use the following steps to configure log backups.

1. From the CommCell Browser, navigate to **<Client> | Oracle**.
2. Right-click the **<Instance>** and click **All Tasks | New Subclient**.
3. In the **Subclient Name** box, type a name.
4. Click the **Content** tab.
5. Click to clear the **Data** checkbox.
6. Select the **Backup Archive Log** checkbox.
7. If you have multiple log locations, click **Log Destinations** tab.
8. Select **Log Destinations for Backup** and click **Add**.
9. Type the path to the log files to be backed up.
10. Click **OK**.



## PRUNING THE LOGS AFTER BACKUP USING RMAN

You can customize the pruning of archive logs after the backup using RMAN Scripts. If applicable, you will also need to specify the connect target string and connect string for a recover catalog for a full RMAN script.

## FILE SYSTEM MOVEMENT TO TAPE

RMAN will not know which archive logs have been backed up for file system movement to tape. Hence, we need to prune all the backed up archive logs. Use the following command to prune the logs for file system movement to tape:

```
connect target sys/****@oracledb
connect catalog catuser/****@catalog
DELETE NOPROMPT ARCHIVELOG ALL COMPLETED BEFORE 'SYSDATE-XX'
rman cmdfile</path/to/rman.script>
```

Example:

```
connect target sys/syspw@oracledb
connect catalog catuser/syspw@catalog
DELETE NOPROMPT ARCHIVELOG ALL COMPLETED BEFORE 'SYSDATE-2'
rman cmdfile</path/to/rman.script>
```

If you run the command in the above example, RMAN will remove all archive logs on the disk that are older than 2 days.

### RMAN MOVEMENT TO TAPE

You can use the same command used for file system movement to tape to prune all archive logs. In addition, you can also use the following command to delete the archive logs that have been backed up multiple times, if you are saving multiple copies of archive logs to optimize your database recovery:

```
connect target sys/****@oracledb
connect catalog catuser/****@catalog
DELETE NOPROMPT ARCHIVELOG ALL BACKED UP XX TIMES TO DEVICE TYPE sbt;
rman cmdfile</path/to/rman.script>
```

Example:

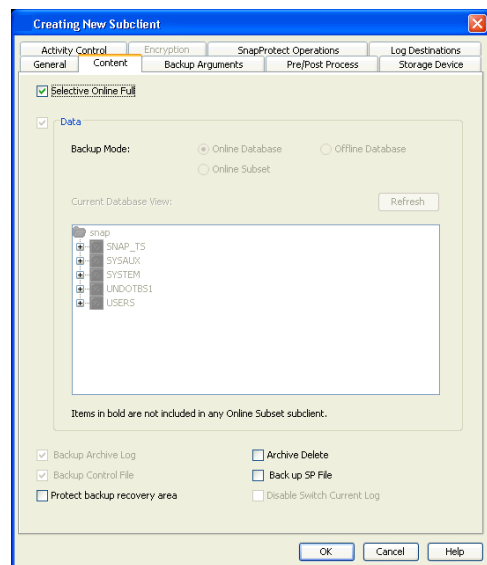
```
connect target sys/****@oracledb
connect catalog catuser/****@catalog
DELETE NOPROMPT ARCHIVELOG ALL BACKED UP 2 TIMES TO DEVICE TYPE sbt;
rman cmdfile</path/to/rman.script>
```

If you run the command in the above example, RMAN will remove all archive logs that have been backed up at least 2 times to device type 'sbt'.

## CONFIGURING SELECTIVE ONLINE FULL BACKUP

Selective Online Full backup is a full backup taken when Oracle database is online, and the backup data is copied to a selective copy (during an auxiliary copy operation) from which it can be restored.

1. From the CommCell Browser, navigate to **<Client> | Oracle**.
2. Right-click the **<Instance>** and click **All Tasks | New Subclient**.
3. In the **Subclient Name** box, type a name.
4. Click the **Content** tab.
5. Select the **Selective Online Full** checkbox.
6. A message indicating that you need to use a separate Storage Policy for Selective Online Full backups is displayed. Click **OK**.
7. Click the **Storage Device** tab.
8. In the **Data Storage Policy** box, select a storage policy name.
9. Click the **SnapProtect Operations** tab.
10. Click **SnapProtect** to enable SnapProtect backup for the selected subclient.
11. Select the storage array from the **Available Snap Engine** drop-down list.
12. 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.
13. Click **OK**.



## CONFIGURING TABLE BACKUPS

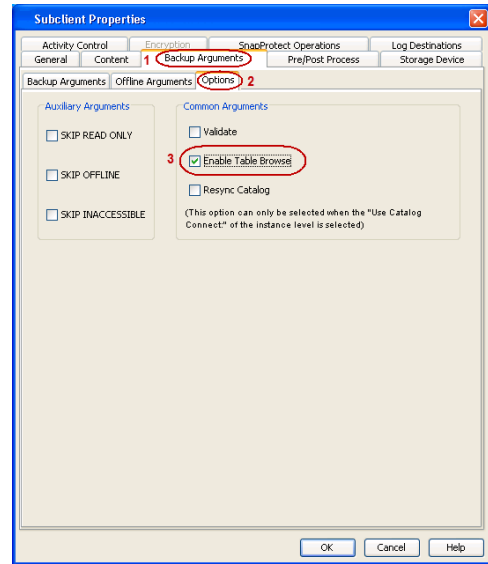
When a table backup is performed, all database tables are gathered in order to present the backup data in a table view during a browse operation.

Use the following steps to configure table backups:

1. From the CommCell Browser, navigate to **<Client> | Oracle | <Instance>**.

2. Right-click the subclient and click **Properties**.
3. Click the **Backup Arguments | Options** tab.
4. Click the **Enable Table Browse** option.
5. Click **OK**.

After running a SnapProtect backup with table browse enabled on the subclient, you can restore database tables.



## CONFIGURING AN ASM INSTANCE

If Oracle home of ASM instance and RDBMS instance are different, then make sure to separately configure ASM instance on the CommCell Console in additions to RDBMS instance.

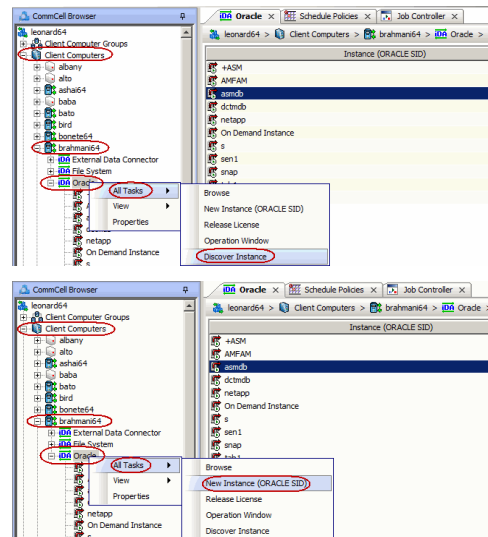
Make sure that the kfed utility resides under <Oracle ASM Home>/bin location. If the kfed utility do not exist, then build the kfed utility as shown in the following example:

- cd <Oracle ASM Home>/rdbms/lib
- make -f ins\_rdbms.mk ikfed

Ensure that the ASM disk string is not empty. Use the following steps to configure the ASM instance:

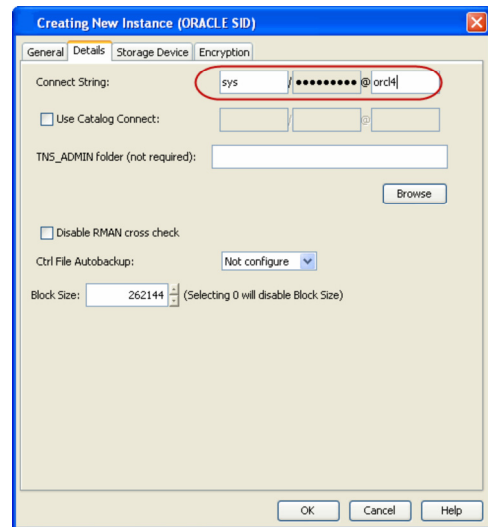
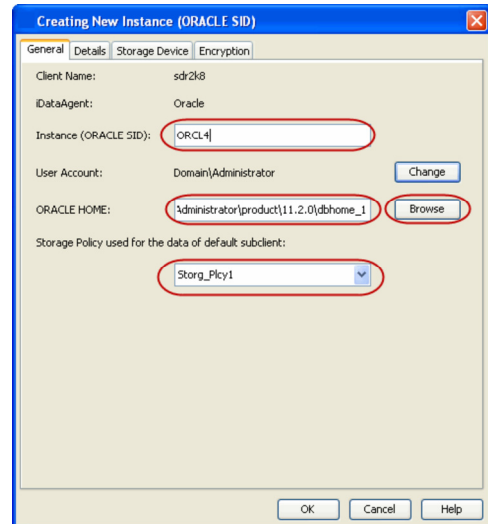
1. From the CommCell Browser, navigate to **Client Computers | <Client>**.
2. Right-click **Oracle**, point to **All Tasks** and then click **Discover Instance**.
3. Click **Yes**.

If your +ASM instance and RDBMS instance is not discovered automatically, you may have to manually add the instance.



4. From the CommCell Browser, navigate to **Client Computers | < Client >**.
5. Right-click **Oracle**, point to **All Tasks**, and then click **New Instance (ORACLE SID)**.
6. In the **Instance (ORACLE SID)** box, type the Instance name.
7. In the **User Account** box, type the login credentials to access the Oracle client.
8. In the **ORACLE HOME** box, type the Oracle application install path.
9. In the **Storage Policy used for the data of default subclient** box, select a storage policy name.
10. Click the **Storage Device** tab.
11. In the **Storage Policy used for user command backup of data** box, select a storage policy.
12. Click the **Log Backup** tab.
13. In the **Storage Policy used for all Archive Log backups** box, select a storage policy name.
14. Click **OK**.

15. Click the **Details** tab.
16. In the **Connect String** box, type the credentials to access the Oracle database. For example, `sys/pwd12@orcl4`.
17. Click the **Storage Device** tab.
18. In the **Storage Policy used for user command backup of data** box, select a storage policy.
19. In the **Storage Policy used for all Archive Log backups** box, select a storage policy.
20. Click **OK**. You can now create a subclient and perform SnapProtect jobs.

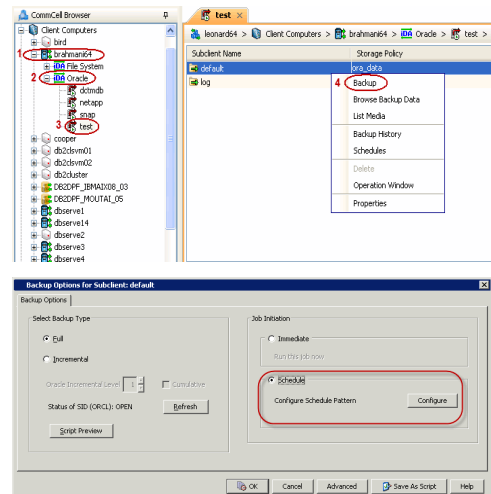


If the ASM disks are from persistent snap engine, then you need to disable the snap integrity. Refer Disabling Verification of Datafiles during SnapProtect Backup for more information.

## SCHEDULING A BACKUP

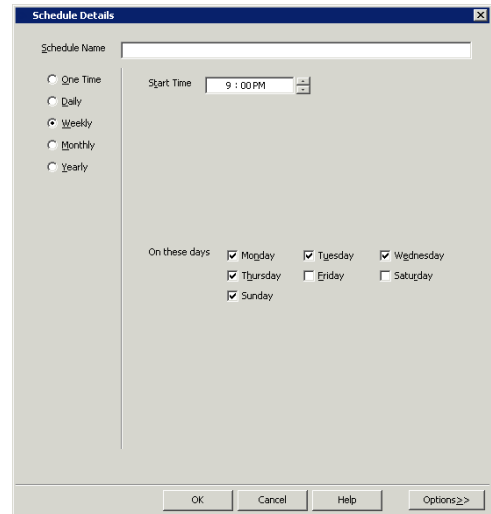
Use the following steps to schedule a backup. When scheduling backups, ensure that you schedule the log backups soon after a SnapProtect backup.

1.
  - From the CommCell Console, navigate to **<Client> | Oracle | <Instance>**.
  - Right-click the **Subclient** and click **Backup**.
2.
  - Select the **Backup type**.
  - Click **Schedule** to schedule the backup for a specific time.
  - Click **Configure** to set the schedule for the backup job. The Schedule Details dialog displays.



3. Select the appropriate scheduling options. For example:
  - Click **Weekly**.
  - Check the days you want the run the backup job.
  - Change the Start Time to 9:00 PM.
  - Click **OK** to close the Schedule Details dialog.
  - Click **OK** to close the Backup Options dialog.

The backup job will execute as per the schedule.



## DISABLING VERIFICATION OF DATAFILES DURING SNAPPROTECT BACKUP

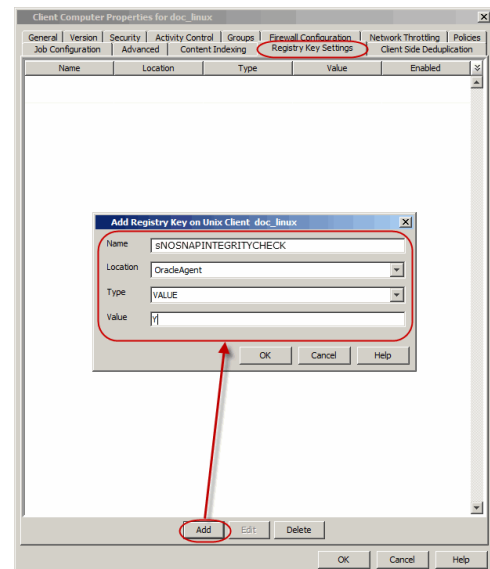
The following steps are performed automatically when you perform a SnapProtect backup:

1. The database is placed in a quiesced state.
2. A snapshot is created for data volumes.
3. The database is placed in a unquiesced state.
4. The snapshot is mounted on source and cataloging of datafiles is performed from mounted snapshot.
5. The snapshot is created for log volumes
6. The snapshot is mounted on source and cataloging is performed for mounted log files.

Cataloging is performed to verify whether all the datafiles are properly captured during a SnapProtect backup. RMAN catalog datafilecopy will check the datafile header and verify its authenticity before cataloging it.

Use the following steps to disable the cataloging operation:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<Client>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type sNOSNAPINTEGRITYCHECK.
6. In the **Location** box, select or type OracleAgent from the list.
7. In the **Type** box, select **Value**.
8. In the Value box, type **Y**, and then click **OK**.
8. Click **OK**.



## CONFIGURING SNAPPROTECT OPERATIONS USING COMMAND LINE

### ENABLING SNAPPROTECT BACKUP

1. Download the update\_sc.xml file and save it on the computer from where the command will be executed.

- Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameter values.

```
goperation execute -af update_sc.xml -clientName <clientname> -instanceName <oraclesid> -subclientName <subclientname>
-storagePolicyName <storagepolicyname> -isSnapBackupEnabled true
```

## SELECTING SNAP ENGINE

- Download the update\_sc.xml file and save it on the computer from where the command will be executed.
- Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameter values.

```
goperation execute -af update_sc.xml -clientName <clientname> -instanceName <oraclesid> -subclientName <subclientname>
-storagePolicyName <storagepolicyname> -isSnapBackupEnabled true -snapShotEngineName <Snapshot engine>
```

## SELECTING A PROXY CLIENT FOR MOVEMENT TO TAPE:

- Download the update\_sc.xml file and save it on the computer from where the command will be executed.
- Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameter values.

```
goperation execute -af update_sc.xml -clientName <clientname> -instanceName <oraclesid> -subclientName <subclientname>
-storagePolicyName <storagepolicyname> -isSnapBackupEnabled true -snapShotEngineName <Snapshot engine> -
snapToTapeProxyToUse/clientName <proxy client>
```

## SELECTING RMAN BACKUP COPY

- Download the update\_sc.xml file and save it on the computer from where the command will be executed.
- Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameter values.

If you select RMAN for backup copy, you should install the Oracle iDataAgent and the oracle instance configured in CommCell browser should be identical to the instance in the source computer.

```
goperation execute -af update_sc.xml -clientName <clientname> -instanceName <oraclesid> -subclientName <subclientname>
-storagePolicyName <storagepolicyname> -isSnapBackupEnabled true -snapShotEngineName <Snapshot engine> -
snapToTapeProxyToUse/clientName <proxy client> -isRMANEnableForTapeMovement true
```

## DISABLING SNAPPROTECT BACKUP

- Download the update\_sc.xml file and save it on the computer from where the command will be executed.
- Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameter values.

You must perform a full backup job after enabling/disabling SnapProtect backup.

```
goperation execute -af update_sc.xml -clientName <clientname> -instanceName <oraclesid> -subclientName <subclientname>
-storagePolicyName <storagepolicyname> -isSnapBackupEnabled false
```

## AVAILABLE PARAMETERS FOR SNAPPROTECT OPERATIONS

The following table displays all the parameters you can use with the commands mentioned in the above sections. To add a parameter to your command, use the following syntax: (A example is provided at the end of the table.)

```
goperation execute -af <template XML file> -<parameter name> <value>
```

| PARAMETER                                        | DESCRIPTION OF PARAMETER VALUES                                   |
|--------------------------------------------------|-------------------------------------------------------------------|
| clientName                                       | Name of the client computer, as displayed in the CommCell Browser |
| instanceName                                     | Name of the oracle instance                                       |
| subclientName                                    | Name of the Subclient used for SnapProtect operations             |
| storagePolicyName                                | Name of the storage policy used for SnapProtect operations        |
| isSnapBackupEnabled<br>(true/false)              | To enable/disable a SnapProtect backup                            |
| snapShotEngineName                               | To define the engine to be used for a SnapProtect backup          |
| snapToTapeProxyToUseSource<br>(true/false)       | To enable/disable using source if proxy is unreachable            |
| snapToTapeProxyToUse<br>clientName="client_name" | To define proxy client to be used of backup copy operations.      |
| isRMANEnableForTapeMovement<br>(true/false)      | To enable/disable using RMAN for backup copy                      |

## EXAMPLES

The following example shows how to add a parameter for a command:



|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enabling SnapProtect Backup</b>                   | Enable SnapProtect backup for instance name under client brahmani64.<br><pre>./qoperation execute -af update_sc.xml -clientName brahmani64 -instanceName dctmdb - subclientName command_test1 -storagePolicyName 9815 -isSnapBackupEnabled true</pre>                                                                                                                                                                                         |
| <b>Selecting Snap Engine</b>                         | Select a Snap engine for instance name <i>dctmdb</i> under client brahmani64 and subclient name <i>command_test1</i> .<br><pre>./qoperation execute -af update_sc.xml -clientName brahmani64 -instanceName dctmdb - subclientName command_test1 -storagePolicyName 9815 -isSnapBackupEnabled true - snapshotEngineName &lt;Snapshot engine&gt;</pre>                                                                                          |
| <b>Selecting A Proxy Client For Movement To Tape</b> | Select a proxy client for brahmani64 for movement to tape.<br><pre>./qoperation execute -af update_sc.xml -clientName brahmani64 -instanceName dctmdb - subclientName command_test1 -storagePolicyName 9815 -isSnapBackupEnabled true - snapshotEngineName &lt;Snapshot engine&gt; -snapToTapeProxyToUse/clientName &lt;proxy client&gt;</pre>                                                                                                |
| <b>Selecting RMAN Backup Copy</b>                    | Select a Snap engine for instance name <i>dctmdb</i> under client brahmani64 and subclient name <i>command_test1</i> .<br><pre>./qoperation execute -af update_sc.xml -clientName brahmani64 -instanceName dctmdb - subclientName command_test1 -storagePolicyName 9815 -isSnapBackupEnabled true - snapshotEngineName &lt;Snapshot engine&gt; -snapToTapeProxyToUse/clientName &lt;proxy client&gt; - isRMANEnableForTapeMovement true</pre> |
| <b>Disabling SnapProtect Backup</b>                  | Disable SnapProtect operation for instance name <i>dctmdb</i> under client brahmani64.<br><pre>./qoperation execute -af update_sc.xml -clientName brahmani64 -instanceName dctmdb - subclientName command_test1 -storagePolicyName 9815 -isSnapBackupEnabled false</pre>                                                                                                                                                                      |

## NFS SNAPPROTECT FOR ORACLE

You can perform a SnapProtect backup for Oracle when the database is on a NFS Volume. However, you will require a root access in the storage device's NFS configuration to be able to read and write on the accessible Oracle files i.e., the host on which the NFS Volume is mounted.

You can also perform SnapProtect backups for Oracle if the database resides on a Direct NFS volume. SnapProtect backups supports volumes using the Oracle Direct NFS (dNFS) protocol.

File level reverts can also be performed when the database is on a NFS volume by using the `sUSE_FILE_LEVEL_REVERT` registry key. Do not perform the file level revert when the database resides on a NFS with regular LUNs.

Consider the following while performing a SnapProtect backup for data or databases that reside on a NFS Volume:

- The export name on the storage device should be the same as the storage path on the storage device.  
E.g., if the storage path of the storage device is `/vol/Volume/Qtrees`, use `/vol/Volume/Qtrees` as the export name and not an alias such as `/ExportName`.
- You can use the exports both at the root of a NetApp volume and at subdirectory levels below the root of the volume.
- Make sure that the storage device is accessible from the source and proxy machine (even if they exist in different domains) using the storage device's short name while mounting NFS exports from the storage device. Make sure to enter the storage device credentials using its short name. Do not use an IP address or the fully qualified domain name.  
E.g., use a short name for the server such as `server1` or `server2`.

## CONFIGURING ORACLE RAC DATABASE SNAPPROTECT OPERATIONS

You can perform SnapProtect operations for a single node Oracle RAC setup. When configuring the Oracle RAC components for a SnapProtect backup, ensure the following:

- The Oracle instance should be configured on one of the physical nodes for the Oracle RAC Agent.
- If the data and archive logs do not reside on a shared location, create a user-defined subclient for the archive logs and run a backup using RMAN. The original subclient should only include the data volume in order to perform a SnapProtect backup.
- The **Use RMAN for Tape Movement** option is selected during the subclient configuration if you plan to backup the archive logs.
- The ASM Oracle Database should be located on a ASM disk group, and the underlying disks should be snap-able.

### CONFIGURING SNAPPROTECT OPERATIONS USING A SINGLE NODE

You must select a physical client and a RAC instance under such physical client for scheduling SnapProtect operations. It is recommended to configure the RMAN catalog prior to performing a SnapProtect backup.

Use the following steps to configure a RAC instance for SnapProtect operations using a single node:

1. From the CommCell Browser, navigate to **Client Computers | <RAC Physical Client>**.
2. Right-click the **<Oracle Agent>**, point to **All Tasks** and then click **New Instance (Oracle SID)**.
  - In the Instance (ORACLE SID) box, type the RAC Instance name.
  - In the ORACLE USER box, type the user account name for RAC Instance.
  - In the ORACLE HOME box, type the Oracle home path for RAC instance. Alternatively, you can click **Browse** to select the location.

- o Select the Storage Policy for the data of a default subclient from the list.

3. Click the **Details** Tab.
4. In the Connect String box, type the Connect String (SYS login): <sys>/<syspassword>@<Oracle service>  
Example: sys/password1@racdb1
5. In the **TNS\_ADMIN Folder** box, type the TNS ADMIN folder name. Alternatively, click **Browse** to select the location.
6. Click the **Storage Device** tab.
7. In the **Storage Policy used for user command backup of data** box, select a storage policy.
8. Click the **Log Backup** tab.
9. In the **Storage Policy used for all Archive Log backups** box, select a storage policy name.
10. Click **OK**.

Make sure that the kfed utility resides under the following location:

```
<Oracle ASM Home>/bin
```

If the kfed utility do not exist, build the kfed utility as shown in the example:

```
cd <Oracle ASM Home>/rdbms/lib
make -f ins_rdbms.mk ikfed
```

You must configure an ASM instance since Oracle RAC SnapProtect operations support only ASM instances (In case of a first node, it is +ASM1).

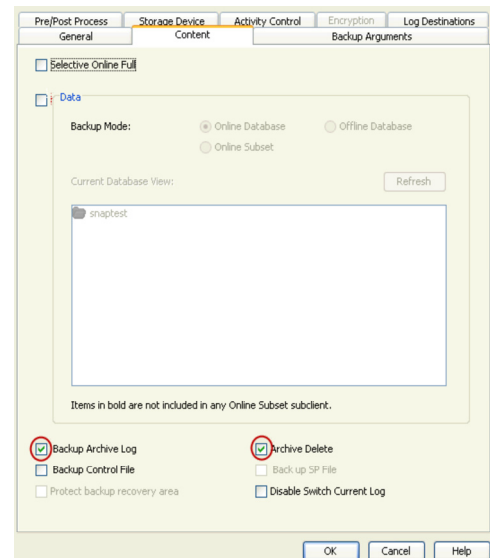
## CONFIGURING ONLINE BACKUPS FOR SNAPPROTECT SUBCLIENTS

When you perform a SnapProtect backup for online databases, ensure you also backup the archive logs. The archive log destination should be shared among all RAC instances. If the log destination is not shared among all RAC instances, you need to separately schedule the archive log backups using a user-defined subclient.

When you backup archive logs, you can specify the location (archive log destinations) from where log backups should be performed. Oracle RAC database will be distributed across many physical clients. These physical clients may or may not share archive log destinations for all instances.

Use the following steps to configure backups for online databases if the archive log destination is shared among all RAC instances:

1. From the CommCell Browser, navigate to **<Client> | Oracle | Instance**.
2. Right-click the **<Subclient>** and click **Properties**.
3. Click the **Content** tab.
4. Select the **Backup Archive Log** checkbox. If you want the archive log files to be deleted after they are backed up, select the **Archive Delete** checkbox.
5. If you have multiple log locations, click **Log Destinations** tab.
6. Select **Log Destinations for Backup** and click **Add**.
7. Type the path to the log files to be backed up.
8. Select **Log Destinations for Delete** and click **Add**.
9. Type the path to the log files to be deleted.
10. Click **OK**.



## CONFIGURING RMAN BACKUP COPY FOR SNAPPROTECT OPERATIONS

You can use RMAN for copying the data to the media in an Oracle RAC setup. When the data is moved to media, the RMAN backup interface is used for block level backup operations. Also, these backup operations are recorded on the RMAN catalog.

RMAN is required in the case of Automatic Storage Management (ASM) Oracle Databases, since ASM data is not available on the file system.

Prior to using RMAN for copying the data to the media, ensure the following:

- The Oracle (non RAC) instance on the proxy computer should have the same name as that in the source computer.
- For backups involving ASM instances, both ASM and the RDBMS instances have to be configured on the proxy computer.
- You must configure the Oracle instance and corresponding ASM instances under the proxy client.
- The Oracle user id/group id on the proxy computer should be identical to the user id/group id on the source computer
- The catalog user and the catalog database must be accessible by the source and the proxy Oracle instances. Catalog is mandatory for RMAN backups on proxy computer.
- The Oracle database installed on the proxy and source machine should be compatible.
- The proxy and source computer should have the same directory structure e.g. dump, diagnostic and data directories.
- Oracle database requires the ASM to be registered with Oracle Cluster Registry (OCR). It will ensure the RMAN to successfully mount the disk group.
- If multiple source client database instances are configured to run RMAN backup copy on the same proxy MediaAgent, the backup copy may fail due to instance and database name conflicts. The conflicting database and instances need to be moved to a different proxy MediaAgent in such cases.
- By default, during RMAN backup copy the data snaps are mounted in the same location as source on proxy MediaAgents. In case of ASM databases, the ASM Disk Groups are not renamed during RMAN backup copy. This is to facilitate incremental RMAN backup copy where the datafile paths need to be in the same path as source.

However, if you use the same proxy MediaAgent for multiple databases RMAN backup copy may fail if the file system mount points or ASM Disk Group names of different Oracle instances conflict with each other. In such cases, set the `sMANDATAFILECOPY` registry key to make the data snaps to be mounted on a different path or in case of ASM databases, to rename the ASM Disk Groups uniquely.

If you plan to use RMAN for copying the data to the media on the proxy computer, copy the Oracle parameter file (pfile) from the client to the proxy computer's `$ORACLE_HOME/dbs/` directory, and remove any parameter containing Oracle RAC related entries.

For example:

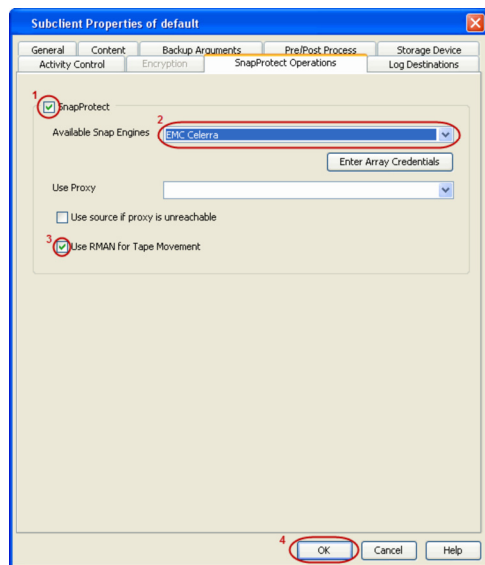
- `cluster_database_instances`
- `cluster_database`
- `<RAC Instance name>.thread`
- `<RAC Instance name>.local_listener`
- `<RAC Instance name>.instance_number`

Use the following steps to configure the RMAN backup copy for Oracle RAC setup:

1. From the CommCell Console, navigate to **Client Computers** | **<Client>** | **Oracle RAC** | **<Instance>**.
2. Right-click the subclient and click **Properties**.
3. Click the **SnapProtect Operations** tab.
4. Click **SnapProtect**.
5. Select the storage array from the **Available Snap Engine** drop-down list.
6. Click **Use RMAN for Tape Movement**.

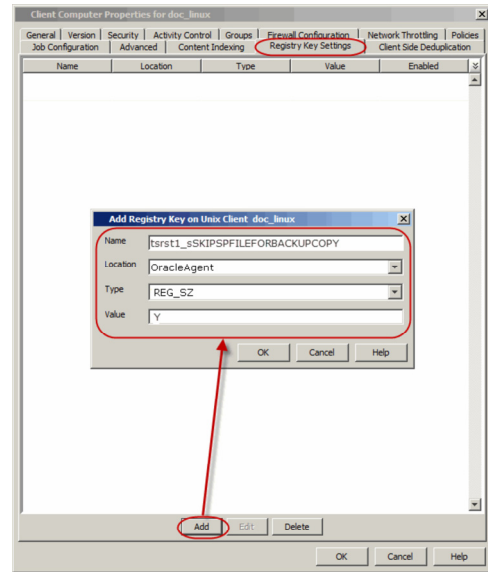
The **Use RMAN for Tape Movement** option is not supported for software snapshots.

7. Click **OK**.



## DISABLING SP FILE BACKUP DURING BACKUP COPY OPERATIONS

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<Client>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type `<ORACLE_SID>_sSKIPSPFILEFORBACKUPCOPY`.  
For example, `tsrst1_sSKIPSPFILEFORBACKUPCOPY`.
6. In the **Location** box, select or type `OracleAgent` from the list.
7. In the **Type** box, select **Value**.
8. In the Value box, type **Y** and then click **OK**.



## MANAGING SNAPSHOTS

The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete, or revert.

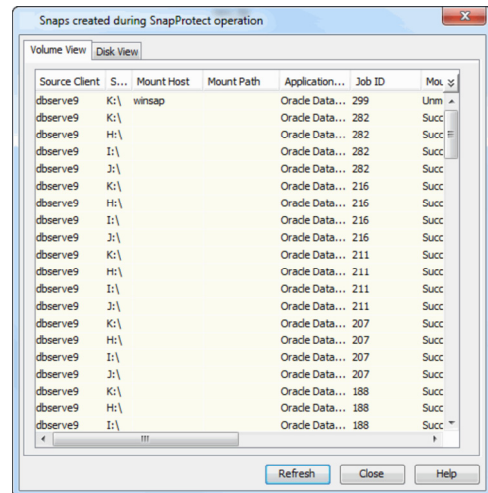
### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.

You can also browse snapshots at the instance level of the Oracle Agent.

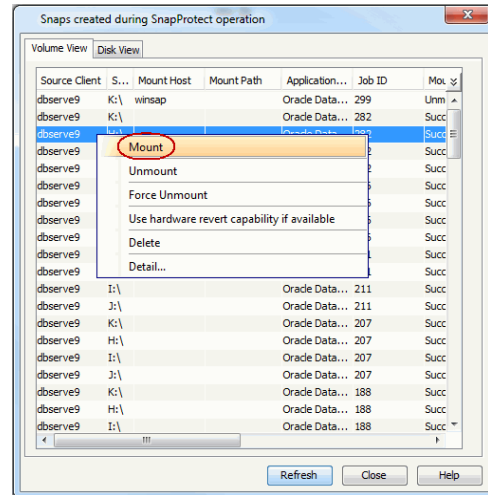


### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

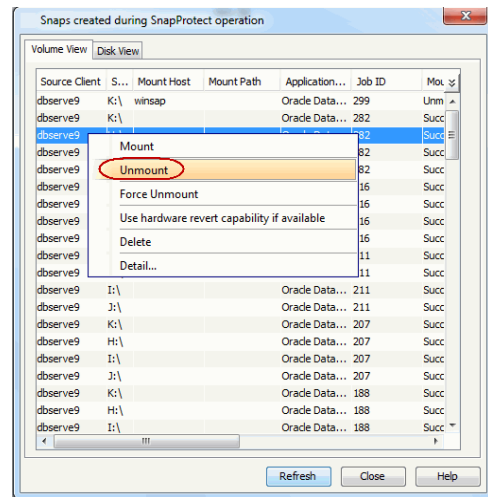


### UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



### DELETE SNAPSHOTS

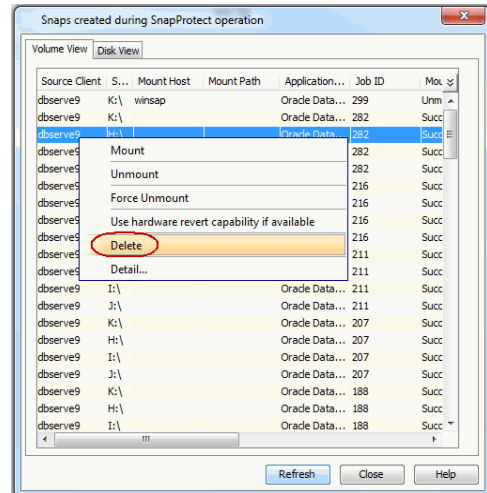
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

- It is recommended to perform an application aware revert operation to prevent a possible loss of data.
- Log revert is not supported.
- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.
- On Unix clusters, use pre/post scripts to freeze and unfreeze the cluster for revert operations. For example, on Red Hat Linux cluster, use the following command in the pre/post scripts:

```
clusvcadm -Z <group> to freeze the cluster
```

```
clusvcadm -U <group> to unfreeze the cluster
```

This is required because, during revert the application is shut down and corresponding volumes are unmounted. In that case, the cluster will automatically failover to another node thus preventing the revert operation.

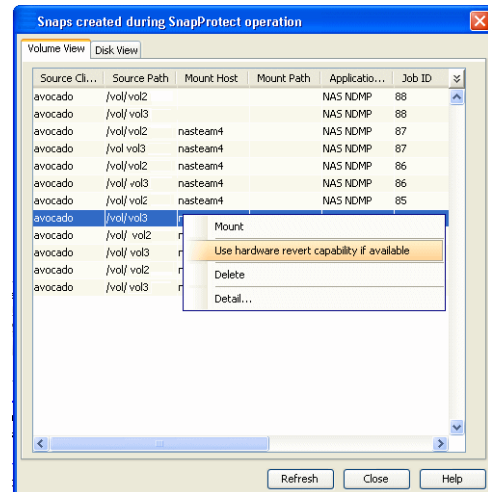
- It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
- If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

## PERFORM AN APPLICATION AWARE REVERT

1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.
  - An application aware revert operation reverts back all the volumes included in the backup.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the application.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

## PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers** | *<Client>*.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, `confirm`.
5. Click **OK**.
  - A hardware specific revert operation reverts back the volume included in the snapshot.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



## SNAP RECONCILIATION

Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

## RESTORING DATA FROM A SNAPPROTECT BACKUP

When restoring data from a snapshot, note the following:

- If the selected backup (latest or point-in-time) was a SnapProtect backup, the subsequent restore will be a SnapProtect restore.
- During Snapshot restore operations, the database is shutdown first and then the snapshots are restored. Once restored, the database is changed to mount mode for the recover operation.

Snapshots are mounted on the destination client where the restore is performed. Hence, destination client should have access to the storage array/filer where snapshot was taken. If the destination client does not have access to storage device, then you should restore the data from snapshot using proxy computer. You can restore an oracle database on a ASM disk group using RMAN.

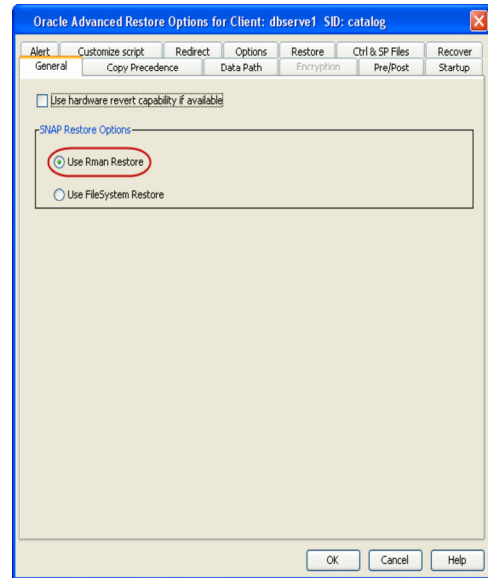
## RESTORE DATA FROM SNAPSHOT USING RMAN

Use the following steps to restore data from a snapshot using RMAN scripts:

1. From the CommCell Browser, navigate to **Client Computers** | *<Client>* | **Oracle**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks** | **Browse Backup Data**.

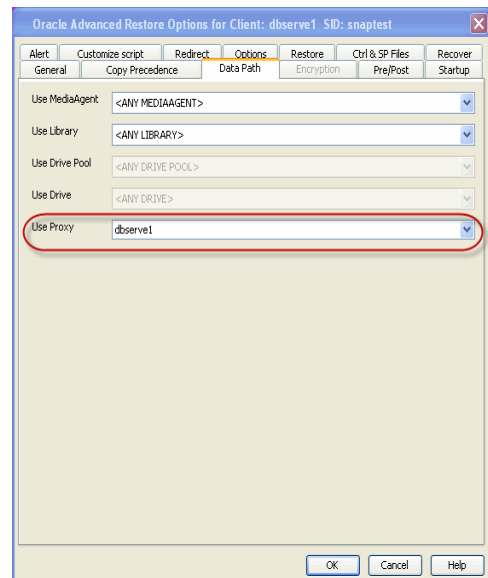
Restoring log data using RMAN is not supported.

3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, select the **Use Snap Restore** checkbox.
6. Click **Advanced**.
7. Select the **Use RMAN Restore** checkbox.
8. Click **OK** to save the settings and close the **Advanced Restore Options** window.
9. Click **OK** to close the **Restore Options** window and initiate the restore job.



## RESTORE DATA FROM SNAPSHOT USING A PROXY COMPUTER

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, select the **Use Snap Restore** checkbox.
6. Click **Advanced**.
7. Click the **Data Path** tab.
8. From the **Use Proxy** box, select the server that you want to use as proxy.  
The oracle restore will use the file system restore from snap if this option is selected.
9. Click **OK** to save the settings and close the **Advanced Restore Options** window.
10. Click **OK** to close the **Restore Options** window and initiate the restore job.



## RESTORING AND RECOVERING AN ENTIRE DATABASE TO THE SAME HOST

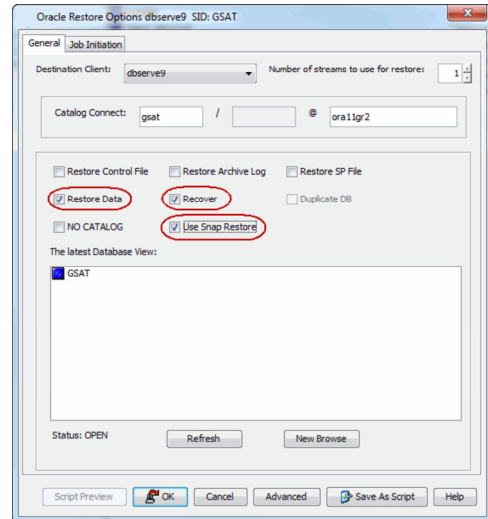
When the database is corrupted or lost, you can restore and recover it from the latest offline or online full backup (depending on how the subclient was configured for backups).

By default, the database is restored to the same location from where it was backed up. Once the database is restored, it is recovered to the current time.

Use the following steps to restore and recover a database to the same host:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **All Tasks** and then click **Restore**.
3. Verify that the **Restore Data** and **Recover** options are selected.
4. Select the **Restore Control File** check box.
5. Click **OK**.

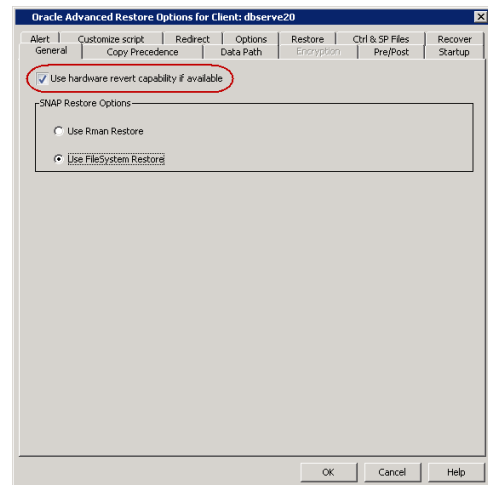




## REVERTING AN ENTIRE DATABASE TO THE SAME HOST

You can use the revert operation to bring the oracle database back to the point in time when the SnapProtect backup was taken. However, the log volume will not be reverted. Hence, you can use either the file system or RMAN to revert the logs after reverting the data volume.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
3. From the **Browse** window, navigate and select the database to be restored and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.



## RESTORING AND RECOVERING AN ENTIRE DATABASE TO A PREVIOUS POINT-IN-TIME

The point-in-time restore is useful in the following scenarios:

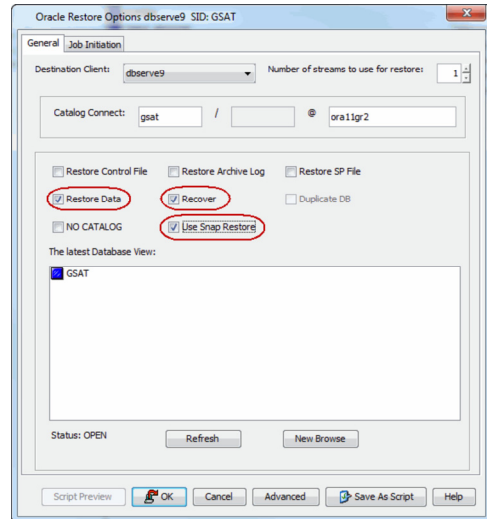
- If any undesired transaction occurs in the database, you can revert the database to a state just before the transaction.
- If a database fails, you can restore to the state just before the point of failure.

When you restore and recover an entire database to a previous point-in-time from an online backup or offline backup (depending on how the subclient was configured for backups) to the original host, it is recommended to use the control files.

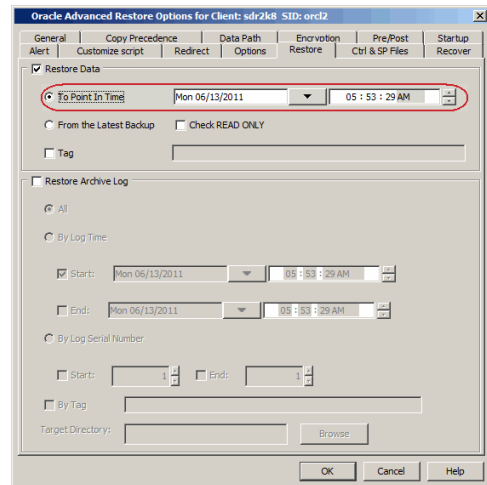
When you perform a point-in-time restore for a database, the next scheduled backup for that database will automatically convert to a full backup.

Use the following steps to restore and recover a database to a previous point-in-time:

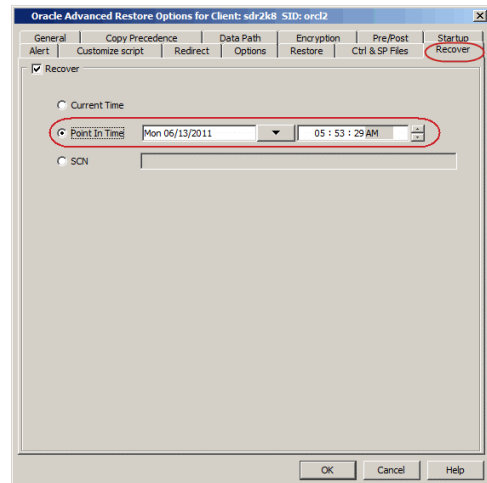
1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **All Tasks** and then click **Restore**.
3. Select **Restore Control File** check box, if you want to restore the control file(s).
4. Click **Advanced**.



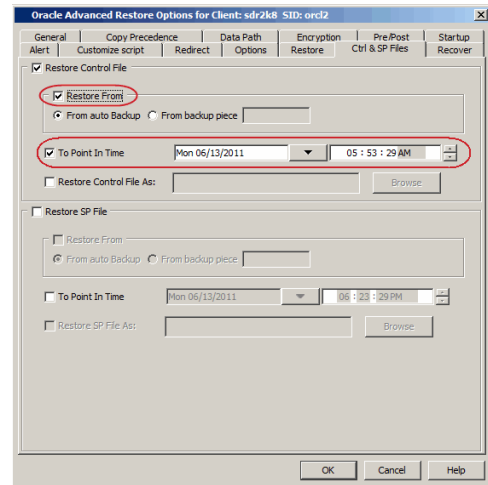
5. Click the **Restore** tab.
6. Click **To Point-In-Time** and select the data and time.



7. Click the **Recover** tab.
8. Click the **Point-In-Time** and select the data and time.



9. Click **Ctrl&SP Files** Tab, if you have selected to restore the control file(s).
10. Select **Restore From** check box.
11. Click the **Point-In-Time** and select the data and time.  
You must restore the control files to a point-in-time later than or equal to the point-in-time set in the **Restore** tab.
12. Click **OK**.



## RESTORING AND RECOVERING AN ENTIRE DATABASE TO A NEW HOST

If the computer on which you hosted a database is damaged or destroyed, you can restore and recover the lost database with the same directory structure on to a new host.

By default, the database is restored in the ARCHIVELOG mode, You can also choose to restore the db in NOARCHIVELOG mode.

Use the following steps to restore and recover a database to a new host with the same directory structure:

### PREREQUISITES

1. Verify the following in both the source and destination computers:
  - The connection specifications (host, service name, port) in the `tnsnames.ora` file on both the source and destination computers should be different.
  - The `<username>` you use for the destination computer is different than the username for the source computer.
  - Sufficient disk space is available on the destination computer to accommodate the restored database.
  - Both the source and destination computers should have the following similar features:
    - Operating systems
    - Oracle version
    - ORACLE\_SID
    - `init <SID>.ora` file
    - Processor (32-bit or 64-bit)
    - Datafile directory structures

### SETTING UP THE SOURCE AND DESTINATION HOSTS

2. Create a new user account with recovery catalog owner permission within the Recovery Catalog for the destination computer. Use a different `<username>`

```

SQL>create user <username> identified by <password>
2>temporary tablespace <temp_tablespace_name>
3>default tablespace <default_tablespace_name>
4>quota unlimited on <default_tablespace_name>;

Statement processed.

SQL>grant connect, resource, recovery_catalog_owner to
<username>;

Statement processed.

```
3. Manually transfer the Oracle password file `orapw<Oracle SID name>` from the source computer to the destination computer. Usually, this file resides in `ORACLE_HOME/dbs`.
4. Export the recovery catalog data for the catalog user.
 

For example, if the user ID for the recovery catalog owner is `user1`, you need to export the database backup information for `user1`.
5. Import the recovery catalog data to the new user account for the destination computer.

#### Example:

```

SQL>create user <username> identified by <password>
2>temporary tablespace <temp_tablespace_name>
3>default tablespace <default_tablespace_name>
4>quota unlimited on <default_tablespace_name>;

```

Statement processed.

```

SQL>grant connect, resource, recovery_catalog_owner to
<username>;

```

Statement processed.

#### Example using IMPORT CATALOG Command:

```

RMAN>IMPORT CATALOG user1/user1@src;

```

6. Copy the recovery catalog's connect string entry in the `tnsnames.ora` file from the source host to the destination host.
7. Make sure that the `ORACLE_SID` and `ORACLE_HOME` are appropriately configured on the destination computer.
8. Install the Oracle *iDataAgent* and configure it as client in the same CommServe in which the source computer resides.
9. Create and configure a new Oracle instance, similar to the one existing in the source computer on the destination computer. Ensure that this instance is in NOMOUNT mode.

```
<service_name> =
(DESCRIPTION =
(AADDRESS = (PROTOCOL = <protocol>)(HOST = <host>) (PORT
= <#>))
(CONNECT_DATA = (SID = <Recovery Catalog database>)))
```

**Example:**

**For Unix:**

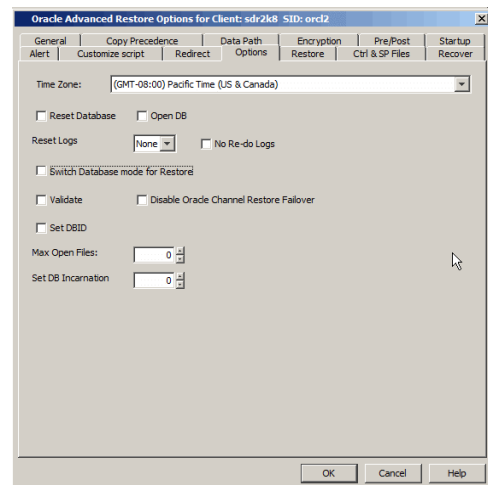
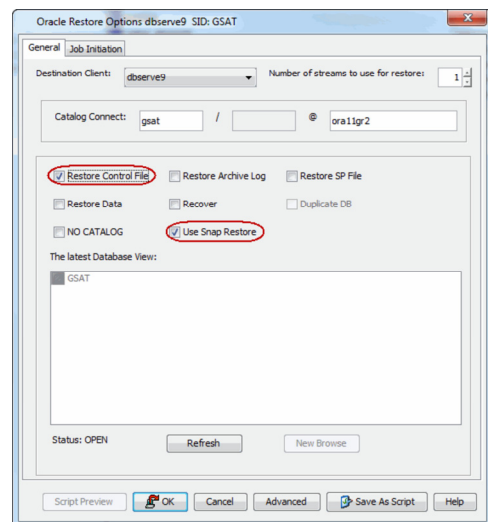
```
#export ORACLE_SID= <target database SID>
#export ORACLE_HOME= <Oracle home directory>
```

**For Windows:**

```
C:\set ORACLE_SID= <target database SID>
C:\set ORACLE_HOME= <Oracle home directory>
```

**RESTORING THE DATABASE**

10. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
11. Right-click the **<Instance>** point to **All Tasks** and then click **Restore**.
12. Select the name of the client computer from the **Destination Client** list.
13. Select **Restore Control File** check box.
14. Click **Advanced**.
15. Click the **Options** tab.
16. If the database is in NOARCHIVELOG mode, then select **No Redo Logs**.
17. Click **OK**.



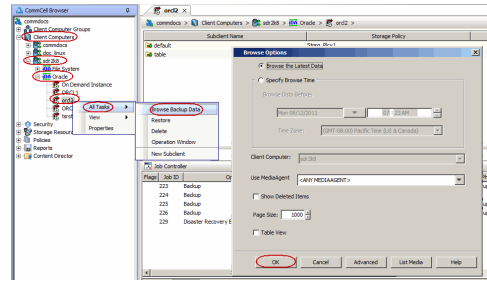
**RESTORING INDIVIDUAL DATAFILES/TABLESPACES**

In addition to restoring a database, you can also restore specific tablespaces or datafiles that were lost due to an error or corruption. By default, the selected tablespaces/datafiles are restored to the original location from the latest online backup.

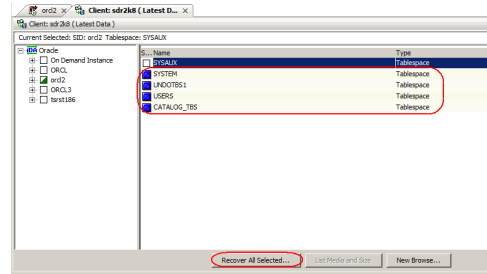
Use the following steps to restore the datafile(s) or tablespace(s):

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.

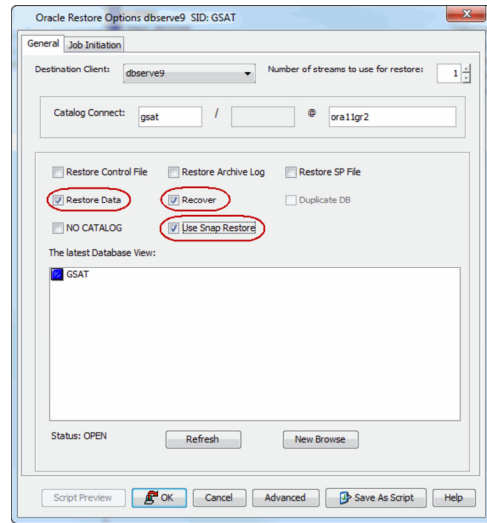
- Right-click the **<Instance>**, point to **All Tasks** and then click **Browse Backup Data**.
- Click **OK**.



- In the right pane of the Browse window, select the datafiles or tablespaces you want to restore and click **Recover All Selected**.



- Click **OK**.



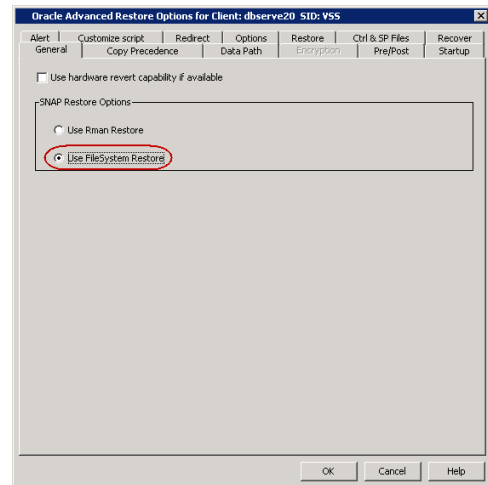
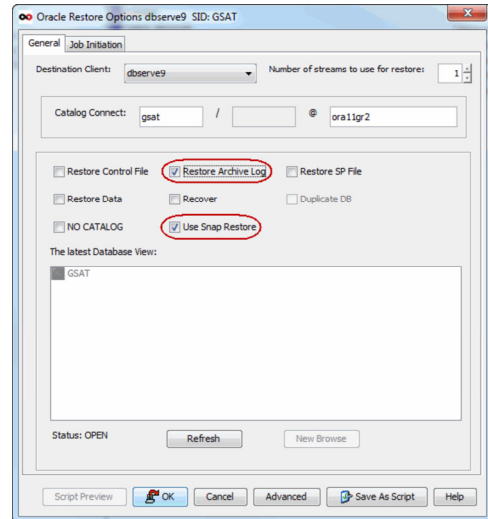
## RESTORING ARCHIVE LOGS

Archive logs can be restored separately or along with the database. If there is a database failure and you need to recover the database to the recent state, you will be able to restore all the logs along with the database.

Use the following steps to restore all the archived logs (note that this is the default option):

- From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
- Right-click the **<Instance>**, point to **All Tasks** and then click **Restore**.
- Select the **Restore Archive Log** check box.
- Click **Advanced**.

5. In the Snap Restore Options, select the **Use FileSystem Restore** Check box
6. Click **OK**.



## RESTORING DATABASE TABLES

Database tables can be restored from a SnapProtect backup using RMAN. In order to restore database tables, you need to perform a SnapProtect backup with table browse enabled.

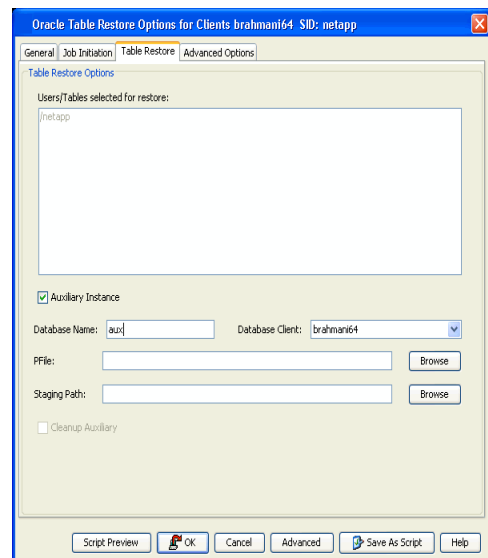
Use the following steps to restore database tables:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>** and click **All Tasks | Browse Backup Data**.
3. Select the **Table View** checkbox.
4. Click **OK**.
5. In the **Browse** window, select the tables that you want to restore and click **Recover All Selected**.
6. Click the **Table Restore** tab.
7. Select the **Auxiliary Instance** checkbox if you want to specify an auxiliary instance for the restore.

When specifying the auxiliary instance, ensure that the database is in NOMOUNT mode.

8. In the **Database Name** text box, type the auxiliary database name.
9. In the **PFile** textbox, type the path to the PFile. Alternatively, click **Browse** to locate the PFile.
10. In the **Database Client** box, select the client for the auxiliary instance.

When you provide an auxiliary instance, make sure that the `temp.dbf` file is removed from the operating system in the specified auxiliary instance datafile location.

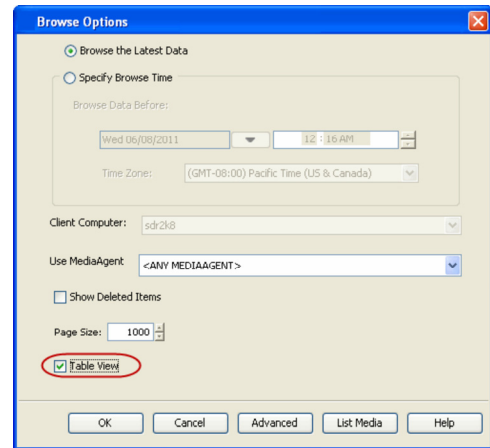


11. Click **OK**.

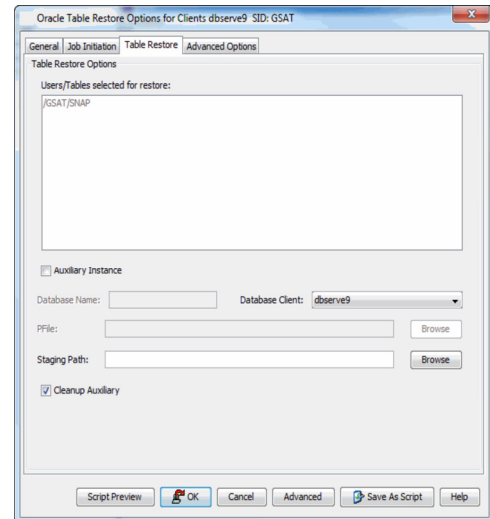
## RESTORING TABLES TO THE SOURCE DATABASE

If some of the tables in the database are lost or corrupted, you can restore those tables back to the same database using the following steps:

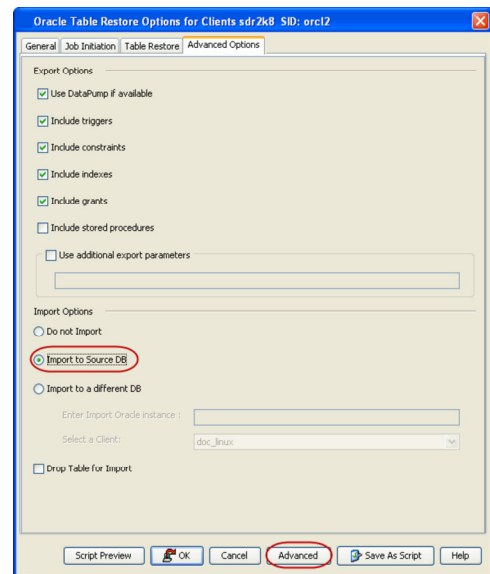
1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **All Tasks** and select **Browse Backup Data**.
3. Select the **Table View** check box and click **OK**.
4. From the **Browse** window, navigate and select the tables to be restored and click **Recover All Selected**.



5. Click the **Table Restore** tab.
6. In the **Staging Path** box, click **Browse** and select the location where the auxiliary instance will be created.
7. Click the **Advanced Options** tab.



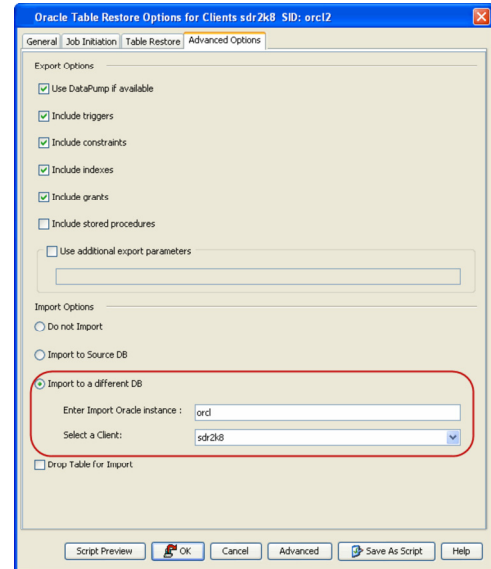
8. Select **Import to Source DB**.
9. Click **OK**.



## RESTORING TABLES TO A DIFFERENT DATABASE ON THE SAME HOST

Use the following steps to restore tables to a different database on the same host:

1. Add the destination instance name in the `Listener.ora` and `Tnsnames.ora` files.
2. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **Oracle**.
3. Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
4. Select the **Table View** check box and click **OK**.
5. From the **Browse** window, navigate and select the tables to be restored and click **Recover All Selected**.
6. Click the **Table Restore** tab.
7. In the **Staging Path** box, type the location where the tables will be restored.
8. Click the **Advanced Options** tab.
9. Select **Import to a Different DB**.
10. In the **Enter Import Oracle Instance:** box, type the destination instance name.
11. In the **Select a Client** box, select the source client.
12. Click **OK**.



## SETTING UP THE AUXILIARY INSTANCE

By default, when you restore database tables to a target instance, the system automatically duplicates the source database to an auxiliary instance in a temporary staging location specified during the restore operation. The database will be automatically imported from this auxiliary instance after the restore.

Use the following steps to set up a specific database as an auxiliary instance. This is useful when you want to restore a table to a specific failure point.

1. Copy the `init<SID>.ora` file from the source database to the auxiliary database instance.
2. Update the database name and the database file locations in the `init<SID>.ora` file for the auxiliary database instance.
3. Add the `DB_FILE_NAME_CONVERT` and `LOG_FILE_NAME_CONVERT` parameters in the `init<SID>.ora` file. These parameters will redirect the datafiles, temp files, and log files to the auxiliary instance.
4. Add the `log_archive_dest_1` parameter is added to the `init<SID>.ora` file on the auxiliary instance.
5. Restart the Oracle Services, if using Windows clients.
6. Add the destination instance name in the `Listener.ora` and `Tnsnames.ora` files. If using a different host, add the duplicate database instance name in the `Listener.ora` file on the destination host and `Tnsnames.ora` files on the destination and source hosts. Also, add the original database name in the `Tnsnames.ora` file on the destination host.
7. Restart the Listener.
8. Ensure that the auxiliary instance is in NOMOUNT mode.

### Windows Clients:

```
DB_FILE_NAME_CONVERT=
('source_of_df_path/', 'dup_of_df_path/', 'source_of_temp_path/', 'dup_of_temp_path/', ...)
LOG_FILE_NAME_CONVERT=('source_of_log_path/redo', 'dup_of_log_path/redo')
```

### Unix Clients:

```
DB_FILE_NAME_CONVERT=
(source_of_df_path/, dup_of_df_path/, source_of_temp_path/, dup_of_temp_path/, ...)
LOG_FILE_NAME_CONVERT=(source_of_log_path/redo, dup_of_log_path/redo)
```

```
DUPDB = (DESCRIPTION =
(AADDRESS = (PROTOCOL = TCP) (HOST = powerpc02) (PORT = 1521))
(CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = dupdb) (UR=A)))
```

```
$!snrctl reload
```

```
sql> startup nomount;
```

## RESTORING TABLES USING A USER-DEFINED AUXILIARY INSTANCE

By default, when you restore database tables to a target instance, the system automatically duplicates the source database to an auxiliary instance in the specified temporary staging location. Once the database is duplicated, you can import the tables to the target instance.

However, if required, you can also use an user-defined auxiliary instance for the restore operation. This is used when you want to restore a table to a specific



failure point.

When restoring tables to a different host, if a user-defined auxiliary instance option is selected for the restore, you need to recover the database to a specified point-in-time or SCN number. You cannot recover the database to the current time using an user-defined auxiliary instance.

### SETTING UP THE AUXILIARY INSTANCE

1. Copy the `init<SID>.ora` file from the source database to the auxiliary database instance.
2. Update the database name and the database file locations in the `init<SID>.ora` file for the auxiliary database instance.
3. Add the `DB_FILE_NAME_CONVERT` and `LOG_FILE_NAME_CONVERT` parameters in the `init<SID>.ora` file. These parameters will redirect the datafiles, temp files, and log files to the auxiliary instance.
4. Add the `log_archive_dest_1` parameter is added to the `init<SID>.ora` file on the auxiliary instance.
5. Restart the Oracle Services, if using Windows clients.
6. Add the destination instance name in the `Listener.ora` and `Tnsnames.ora` files. If using a different host, add the duplicate database instance name in the `Listener.ora` file on the destination host and `Tnsnames.ora` files on the destination and source hosts. Also, add the original database name in the `Tnsnames.ora` file on the destination host.
7. Restart the Listener.
8. Ensure that the auxiliary instance is in NOMOUNT mode.

Windows Clients:

```
DB_FILE_NAME_CONVERT=
('source_of_df_path','dup_of_df_path','source_of_temp_path','dup_of_temp_path',...)
LOG_FILE_NAME_CONVERT=('source_of_log_path/redo','dup_of_log_path/redo')
```

Unix Clients:

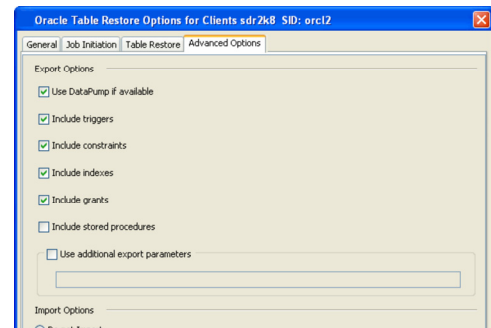
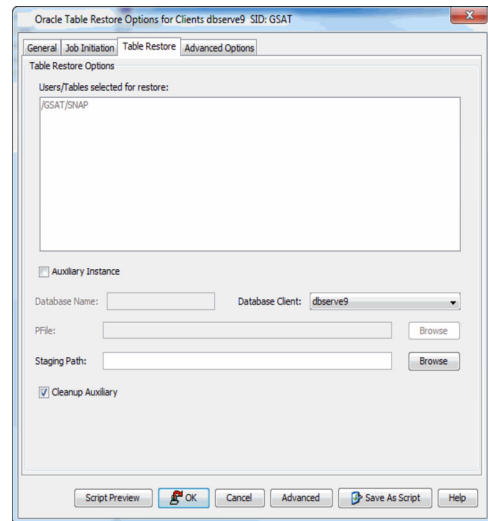
```
DB_FILE_NAME_CONVERT=
(source_of_df_path/dup_of_df_path/source_of_temp_path/dup_of_temp_path,...)
LOG_FILE_NAME_CONVERT=(source_of_log_path/redo,dup_of_log_path/redo)
```

```
DUPDB = (DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = powerpc02)(PORT = 1521))
(CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = dupdb) (UR=A)))
```

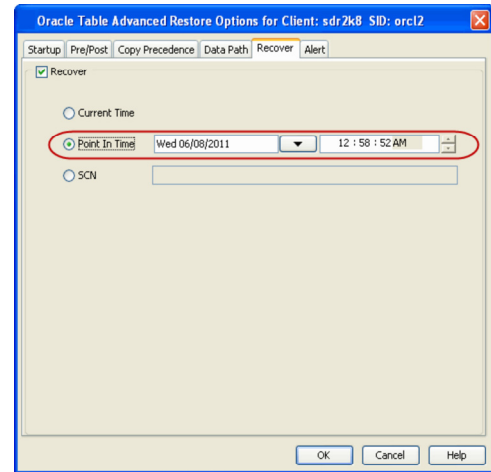
```
sql> sqlplus / as sysdba
sql> $!snrctl reload
sql> startup nomount;
```

### RESTORING THE TABLES USING THE AUXILIARY INSTANCE

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
3. Select the **Table View** check box and click **OK**.
4. From the **Browse** window, navigate and select the tables to be restored and click **Recover All Selected**.
5. Click the **Table Restore** tab.
6. Select the **Auxiliary Instance** checkbox.
7. In the **Database Instance** box, type the auxiliary instance name.
8. In the **Database Client** box, select the destination client for the auxiliary instance.
9. In the **PFile** box, type the path to the PFile of the auxiliary instance. Alternatively, click **Browse** to select the path.
10. In the **Staging Path** box, type the location where the auxiliary instance will be created. Alternatively, click **Browse** to select the path.
11. Click the **Advanced Options** tab.
12. Select **Import to a Different DB**.
13. In the **Enter Import Oracle Instance:** box, type the destination instance name.
14. In the **Select a Client** box, select the destination client.
15. Click **Advanced**.



16. Select the **Recover** tab.
17. Select **Point-In-Time** checkbox and specify the time range to which the the database need to be recovered.
18. Click **OK**.

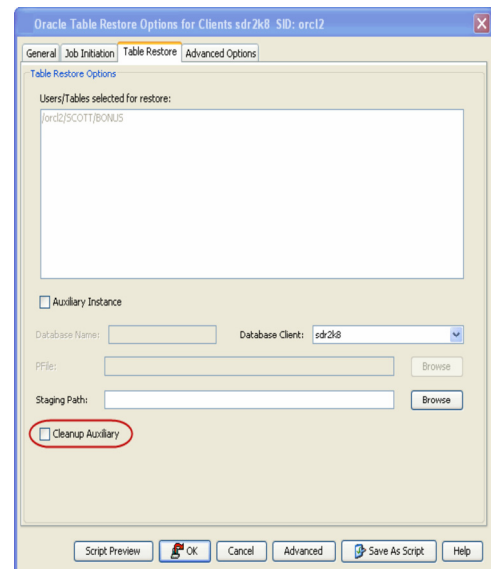


### DISABLING CLEAN-UP OF AUXILIARY INSTANCE AFTER RESTORE

By default, the system generated auxiliary instance is deleted automatically once the tables are imported to the destination instance.

Use the following steps to disable the clean-up of auxiliary instance after the restore:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
3. Select the **Table View** check box and click **OK**.
4. From the **Browse** window, navigate and select the tables to be restored and click **Recover All Selected**.
5. Click the **Table Restore** tab.
6. In the **Staging Path** box, type the location where the tables will be restored.
7. Clear the **Cleanup Auxiliary** checkbox.
8. Click **OK**.



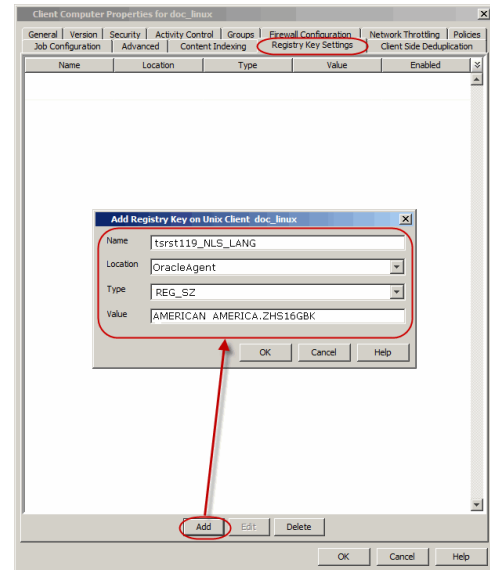
### RESTORING TABLES WITH NON-ENGLISH CHARACTERS

By default, you can restore the tables with English characters. Use the following steps to restore the non-English characters in the tables:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<Client>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type <ORACLE\_SID>\_NLS\_LANG. For example, tsrst119\_NLS\_LANG
6. In the **Location** box, select or type OracleAgent from the list.
7. In the **Type** box, select **Value**.
8. In the Value box, set the database's character set as per your database's character set and then click **OK**.

For example, if the database's nls character set value is ZHS16GBK, you can set NLS\_LANG registry key to AMERICAN\_AMERICA.ZHS16GBK. By default this value is set to AMERICAN\_AMERICA.US7ASCII.

- Click **OK**.



## EXPORTING TABLE OBJECTS

During table restores, the tables are exported from the auxiliary instance to the destination client and later imported to the target database. By default, the following data objects are exported along with the tables:

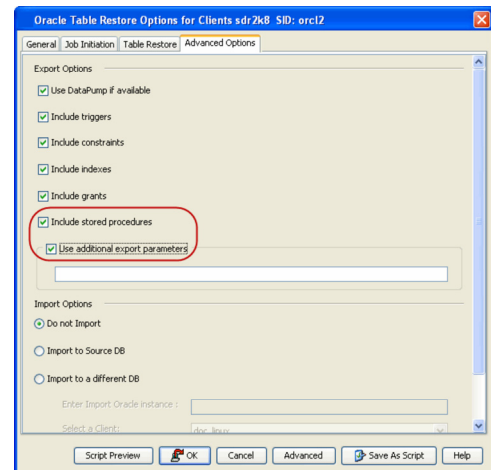
- Triggers
- Constraints
- Indexes
- Grants

However, the stored procedures associated with the selected tables are not exported by default. Use the following steps to export the stored procedures and additional export parameters, such as (COMPRESS or PARALLEL):

Stored procedures are restored from the Schema level. Schema is the collection of data objects created by the user to contain or reference their data. Hence, if one of the table within the schema is selected for restore, all the stored procedures for that schema will also get restored.

When exporting the tables, the datapump export utility is used if it is supported by the Oracle application. The datapump utility facilitates the export of stored procedures. In oracle versions that do not support datapump export utility, you will not be able to include stored procedures during export.

- From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
- Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
- Select the **Table View** check box and click **OK**.
- From the **Browse** window, navigate and select the tables to be restored and click **Recover All Selected**.
- Click the **Table Restore** tab.
- In the **Staging Path** box, type the location where the auxiliary instance will be restored.
- Click the **Advanced Options** tab.
- Select the **Include Stored Procedures** checkbox.
- Select **Use additional export parameters** checkbox and type the parameters to be exported.
- Click **OK**.



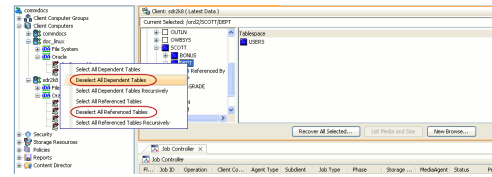
## SELECTING/DE-SELECTING DEPENDENT/REFERENCED TABLES

When you browse using the table view, you can also view the dependent and referenced tables associated with the tables selected for the restore.

Dependent tables are the parent tables (containing the primary key) that the selected table (containing the foreign key) depends upon. Similarly, Referenced tables are the child tables (containing the foreign key) that references the selected table (containing the primary key).

By default, all the dependent and referenced tables will be included in the restore operation. Use the following steps to exclude the dependent/referenced tables:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
3. Select the **Table View** check box and click **OK**.
4. From the **Browse** window, navigate to the table to be restored.
5. Right-click the **<table>** and click **Select/Deselect All Dependent Tables** to exclude all the dependent tables.



Similarly, click **Deselect All Referenced Tables** to exclude all the referenced tables.

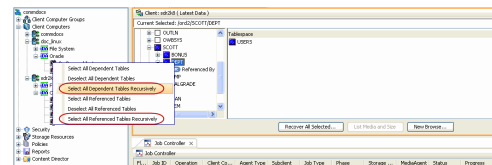
6. Click **Restore All Selected**.
7. Click the **Table Restore** tab.
8. In the **Staging Path** box, type the location where the auxiliary instance will be restored.
9. Click **OK**.

### INCLUDING ALL DEPENDENCIES TO THE DEPENDENT/REFERENCED TABLES

When restoring tables, you can include recursive dependency relationship of all the dependent/referenced tables.

Use the following steps to include all the dependent/referenced tables recursively:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
3. Select the **Table View** check box and click **OK**.
4. From the **Browse** window, navigate to the table to be restored.
5. Right-click the **<table>** and click **Select All Dependent Tables Recursively** to include recursive dependency of dependent tables.



Similarly, click **Deselect All Referenced Tables Recursively** to include recursive dependency of referenced tables.

6. Click **Restore All Selected**.
7. Click the **Table Restore** tab.
8. In the **Staging Path** box, type the location where the auxiliary instance will be restored.
9. Click **OK**.

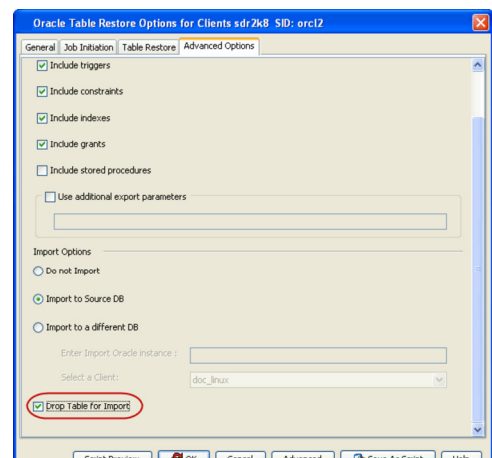
### DELETING EXISTING TABLES DURING A RESTORE

By default, the restore operation will overwrite the existing tables in the destination database during the restore. You can also configure the restore operation to delete the existing tables before performing the restore.

Manually drop/delete the existing tables at the destination instance and then import the tables.

Use the following steps to automatically delete existing tables on the destination instance during restore. Note that you can also manually drop/delete the existing tables at the destination instance and perform the restore without enabling this option.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to All Tasks and select **Browse Backup Data**.
3. Select the **Table View** check box and click **OK**.
4. From the **Browse** window, navigate and select the tables to be restored and click **Recover All Selected**.
5. Click the **Table Restore** tab.
6. In the **Staging Path** box, type the location where the tables will be restored.
7. Click the **Advanced Options** tab.
8. Select **Import to Source DB**.
9. Click **Drop Table for Import** checkbox.
10. Click **OK**.

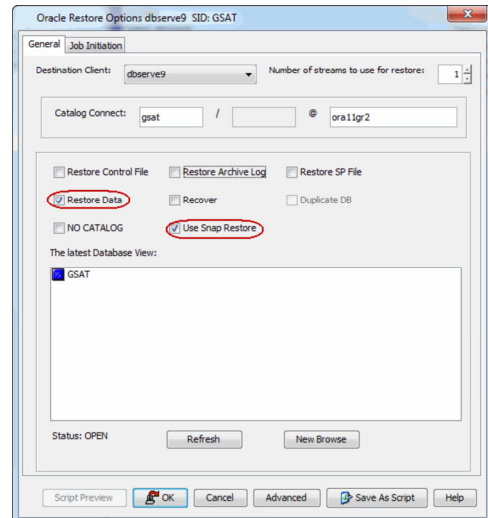


## AUTOMATICALLY SWITCHING THE DATABASE MODE BEFORE A RESTORE

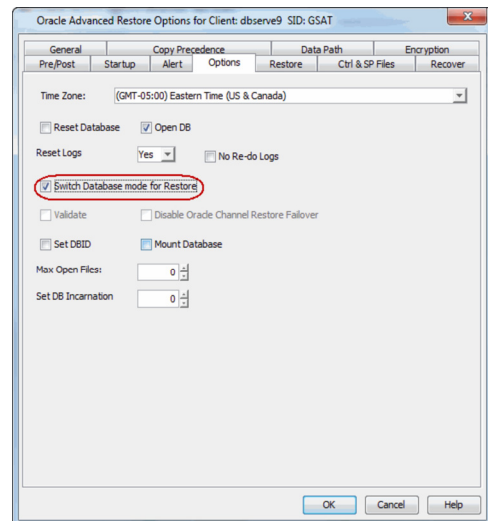
In order to perform a restore operation, the database should be in the MOUNT mode. If the database is not in mounted state, you are prompted to switch the database to the mounted state and then perform the restore.

Use the following steps to automatically switch the database to mount mode prior to restore:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **All Tasks** and then click **Restore**.
3. Click **Advanced**.



4. Click the **Options** tab.
5. Select **Switch Database mode for Restore**.
6. Click **OK**.

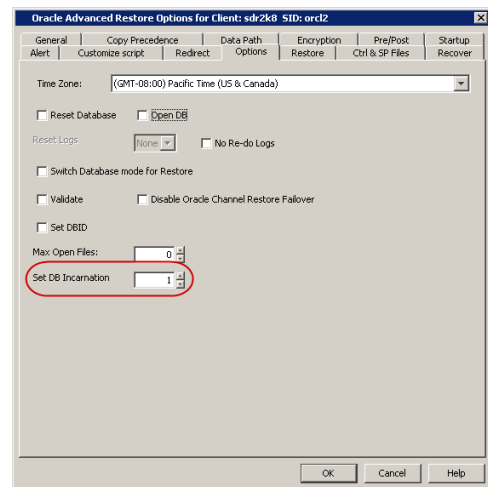
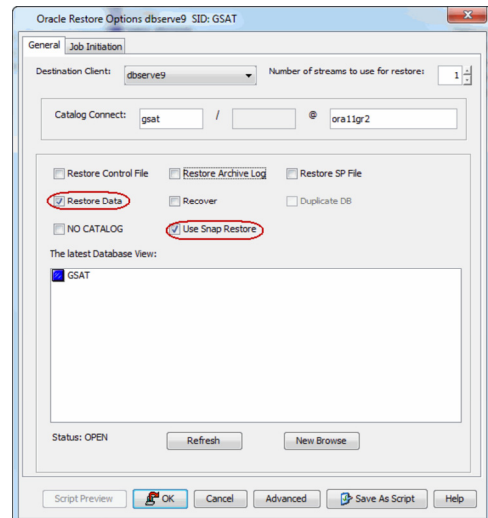


## SETTING THE DATABASE INCARNATION

When you perform a point-in-time recovery of an Oracle database with RESETLOGS, a new incarnation of the database is created. All archive log files generated after resetting the logs will be associated to the new incarnation. However, in order to perform a point-in-time recovery from a backup of a previous incarnation, you need to reset the current incarnation to the previous incarnation value. Use the following steps to set the incarnation value:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **All Tasks** and then click **Restore**.
3. Click **Advanced**.

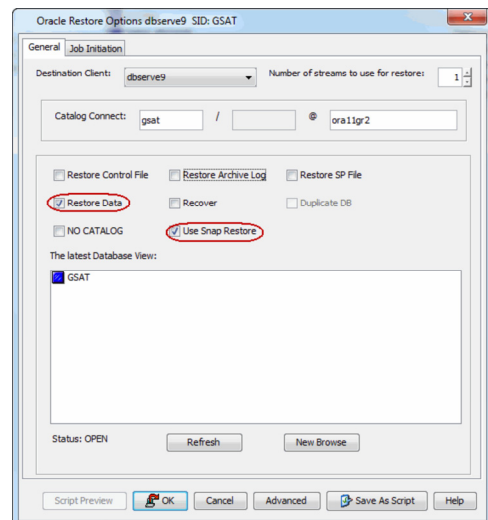
4. Click **Options** tab.
5. Select the database incarnation value from **Set DB Incarnation** list.
6. Click **OK**.



## ENHANCING RESTORE PERFORMANCE

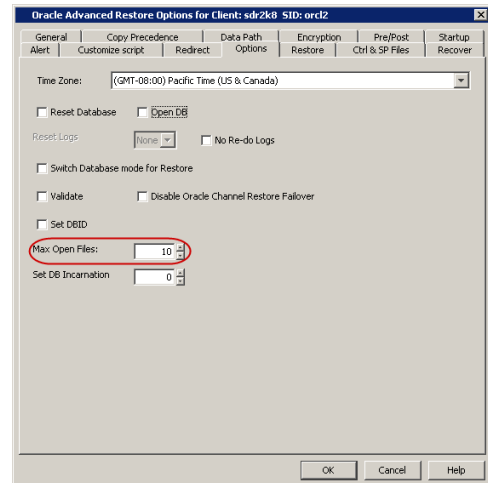
You can perform a restore operation faster when you set a maximum number of concurrent open datafiles for RMAN to read simultaneously. Use the following steps to enhance your restore operation:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **All Tasks** and then click **Restore**.
3. Click **Advanced**.



4. Click **Options** tab.
5. Select the number of open files from **Max Open Files** list.

6. Click **OK**.
7. Click **OK** to start the restore.



## RESTORING FROM A SNAPPROTECT AND RMAN MIXED ENVIRONMENT

When restoring from a SnapProtect and RMAN mixed environment, the data can be restored from a SnapProtect or RMAN backup jobs depending on the browse time and whether the database full backup is a SnapProtect or RMAN backup job.

Consider the following scenarios:

### Scenario 1

The backup jobs are performed in the following sequence:

1. Full SnapProtect backup job
2. RMAN archive log job

In this scenario, when you restore a control file, SP file from autobackup or backup piece, the restore is always performed from the full SnapProtect backup job.

Similarly, when restoring only the archive logs, the logs are restored from the SnapProtect backup job instead of the latest archive log backup.

### Scenario 2

The backup jobs are performed in the following sequence:

1. Full SnapProtect backup job
2. Full RMAN backup job
3. RMAN archive log job

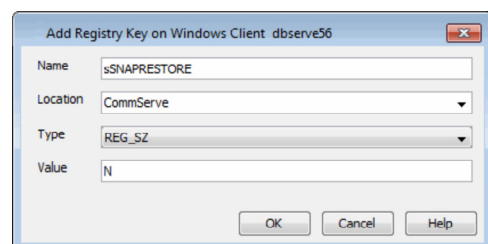
In this scenario, the restores are performed from the latest backup job (SnapProtect or RMAN) depending on the specified time.

If the SnapProtect full backup job and RMAN full backup job were executed in parallel, by default, the SnapProtect full backup job is used for the restore operation.

## ENABLING RESTORES FROM RMAN BACKUPS

In a SnapProtect and RMAN mixed environment, you can configure to restore certain database components, such as control file, SP file, or archive logs from RMAN backup jobs by creating the sSNAPRESTORE registry key on the CommServe using the following steps. Once the restore is complete, make sure to delete this key to enable restores from SnapProtect backups.

1. From the CommCell Browser, right-click the <CommServe>, and then click **Properties**.
2. Click the **Registry Key Settings** tab.
3. Click **Add**.
4. In the **Name** box, type sSNAPRESTORE.
5. In the **Location** box, type or select CommServe from the list.
6. In the **Type** box, select **REG\_SZ**.  
On Unix clients, select **Value**.
7. In the Value box, type **N** and then click **OK**.



## RESTORE AND RECOVER THE DATABASE TO A POINT IN TIME

In a mixed mode environment, you can restore and recover the database to a point in time using the following steps:

1. Enable restores from RMAN backup by creating the `sSNAPRESTORE` registry key on the CommServe.
2. Restore the Control File from Autobackup/Backup Piece or point in time
3. Enable restores from SnapProtect backups by deleting the `sSNAPRESTORE` registry key.
4. Restore and recover the database to a point in time from SnapProtect backup.

## BACKUP COPY OPERATIONS

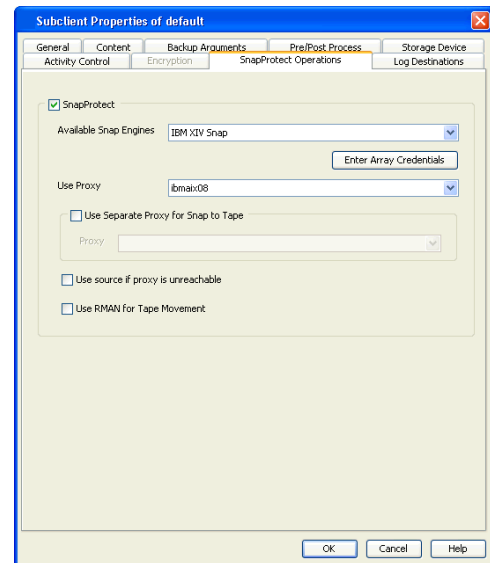
The following sections describe the additional modes of Backup Copy Operations:

### FILE SYSTEM

By default, the system will use the File System for copying the data to the media. The system will scan the file, generate and read the collect file, extract the file list and copies the data on to the tape using MediaAgent's data mover.

In order to perform the file system snap to tape copy on a proxy computer, ensure that the MediaAgent and File System iDataAgent are installed on the proxy computer.

1. From the CommCell Console, navigate to **Client Computers** | **<Client>** | **Oracle** | **<Instance>**.
2. Right-click the subclient and click **Properties**.
3. Click **SnapProtect Operations**.
4. Select **SnapProtect**.
5. Click **Available Snap Engines** drop-down box and select the storage array.
6. Click **OK**.



### RMAN

You can also use RMAN for copying the data to the media.

When data is moved from snap to media, the RMAN backup interface is used for block level backup operations. Also, these backup operations are recorded on the RMAN catalog. RMAN is required in the case of Automatic Storage Management (ASM) Oracle Databases, since ASM data is not available on the file system. You can also run RMAN restores/reports from these backups.

Prior to using RMAN for copying the data to the media, ensure the following:

- The Oracle iDataAgent must be installed on the proxy computer.
- The Oracle instance on the proxy computer should have the same name as that in the source computer.
- The Oracle database installed on the proxy and source computers should be compatible.
- For backups involving ASM instances, both ASM and the RDBMS instances have to be configured on the proxy computer.
- The catalog user and the catalog database must be accessible by the source and the proxy Oracle instances.
- The proxy and source computer should have the same directory structure e.g. dump, diagnostic and data directories.
- Oracle database requires the ASM to be registered with Oracle Cluster Registry (OCR), since the ASM instance is a resource in CRS repository. It will ensure the RMAN to successfully mount the disk group.
- If multiple source client database instances are configured to run RMAN backup copy on the same proxy MediaAgent, the backup copy may fail due to instance and database name conflicts. The conflicting database and instances need to be moved to a different proxy MediaAgent in such cases.

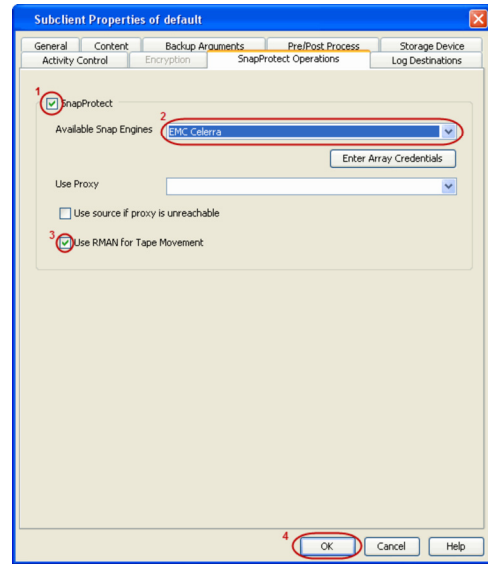
1. From the CommCell Console, navigate to **Client Computers** | **<Client>** | **Oracle** | **<Instance>**.
2. Right-click the subclient and click **Properties**.



3. Click **SnapProtect Operations**.
4. Select **SnapProtect**.
5. Select the storage array from the **Available Snap Engine** drop-down list.
6. Select **Use RMAN for Tape Movement**.

The **Use RMAN for Tape Movement** option is not supported for software snapshots.

7. Click **OK**.



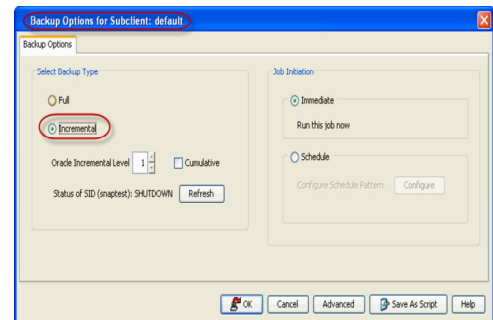
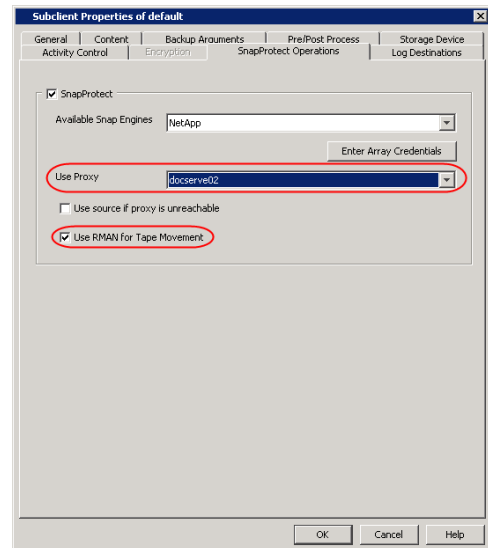
### RMAN INCREMENTAL BACKUP COPY

Oracle RMAN incremental backup copy can be performed on a proxy server.

Prior to performing the RMAN incremental backup copy, ensure the following:

- The database physical schema is the same in both the snap and the current backup (i.e. no addition or deletion of tablespaces between time of snap and current backup).
- The Oracle user ID/group ID on source and proxy should be the same otherwise the RMAN backup copy will fail due to permission issues.

1. Copy the Oracle parameter file (pfile) and password file from the source to the proxy computer's \$ORACLE\_HOME/dbs/ directory.
2. Create the bdump, udump, adump, cdump and diagnostic\_dest directories. Ensure that the directories are in the same location as the source.
3. Create the DB\_CREATE\_FILE\_DEST and LOG\_ARCHIVE\_DEST directories. If there are multiple archive destinations, then create the directories for each of the archivelog destinations.
4. Copy the catalog connection information from the source to the proxy in the tnsnames.ora.
5. Startup the proxy instance in NOMOUNT mode.
6. Configure the proxy Oracle Instance on the CommCell Console.
7. Click **Use Proxy** drop-down box and select the configured proxy from the dropdown list.
8. Select **Use RMAN for Tape Movement** and click **OK**.
9. The **Incremental** option is now available for backup.



### PREVENTING RMAN BACKUP COPY FAILURES DUE TO MOUNT POINT/ ASM DISK GROUP NAME CONFLICTS ON A PROXY MEDIAAGENT

By default, during RMAN backup copy the data snaps are mounted in the same location as source on proxy MediaAgents. In case of ASM databases, the ASM

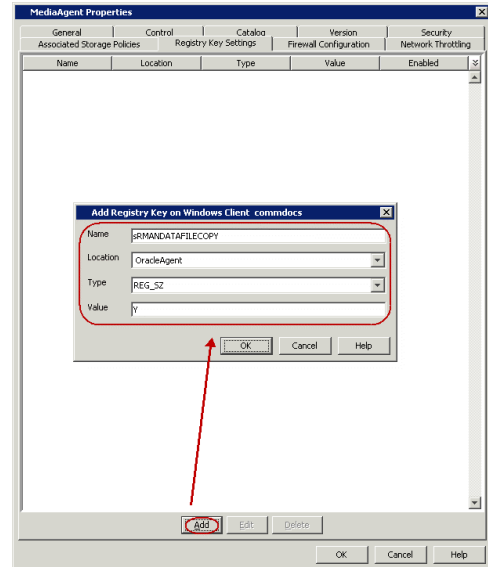
Disk Groups are not renamed during RMAN backup copy. This is to facilitate incremental RMAN backup copy where the datafile paths need to be in the same path as source.

However, if you use the same proxy MediaAgent for multiple databases RMAN backup copy may fail if the file system mount points or ASM Disk Group names of different Oracle instances conflict with each other.

In such cases, use the following steps to make the data snaps to be mounted on a different path or in case of ASM databases, to rename the ASM Disk Groups uniquely:

1. From the CommCell Browser, navigate to **Storage Resources | MediaAgents**.
2. Right-click the **<Proxy MediaAgent>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type `SRMANDATAFILECOPY`.
6. In the **Location** box, type or select `OracleAgent` from the list.
7. In the **Type** box, select **REG\_SZ**.  
On Unix clients, select **Value**.
8. In the Value box, type **Y** and then click **OK**.

RMAN incremental backups will not be possible if we set this registry key as we use `BACKUP DATAFILECOPY` syntax in this case.

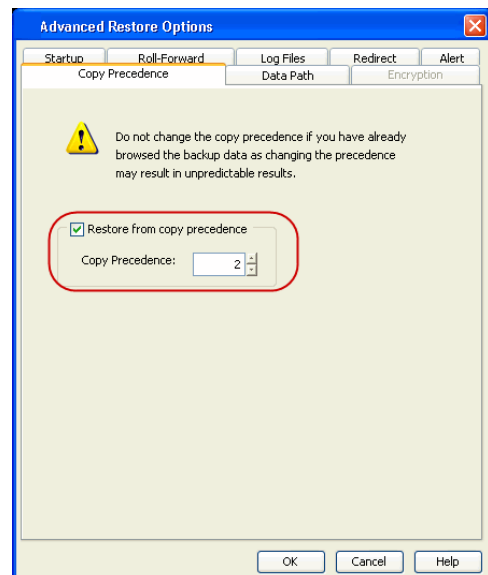


## RESTORING DATA FROM BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number. Use the following steps to restore the data from backup copy using the File System backup:

### RESTORE DATA FROM BACKUP COPY USING FILE SYSTEM

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Select the **General** tab.
9. Select the **Use File System Restore** checkbox.
10. Click **OK**.

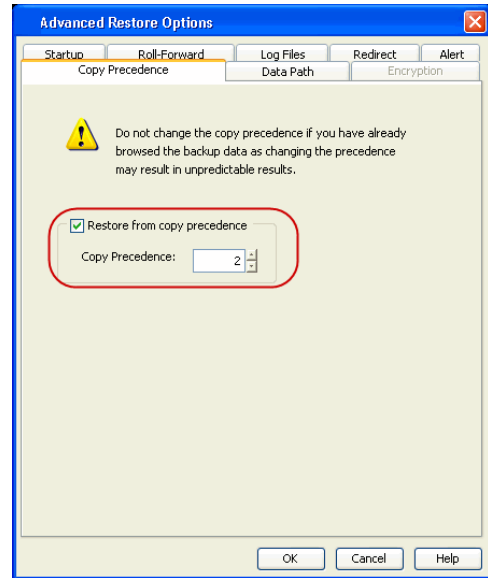


### RESTORE DATA FROM BACKUP COPY USING RMAN

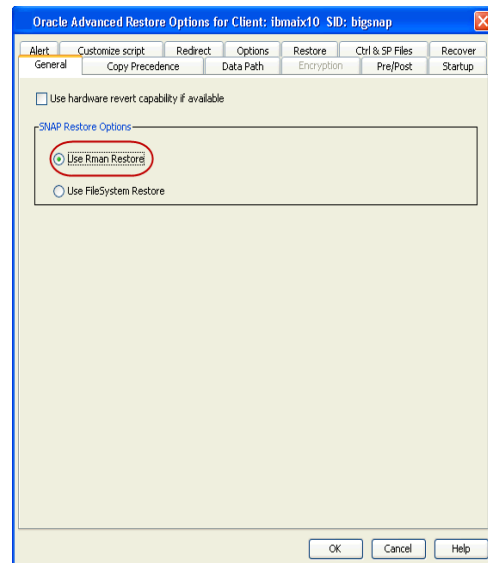
Use the following steps to restore the data from backup copy using RMAN. Refer *Advanced Restore - Oracle /DataAgent* for regular restore operations.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.

2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.



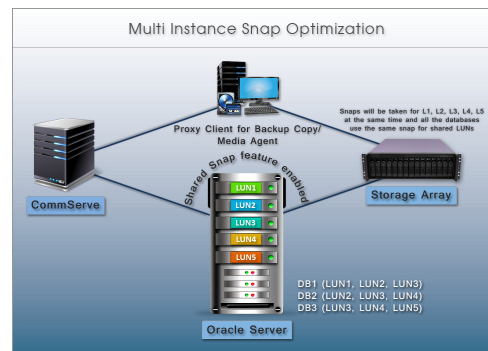
8. Click the **General** tab.
9. Select the **Use RMAN Restore** checkbox.
10. Click **OK**.



## ORACLE MULTI INSTANCE SNAP OPTIMIZATION

During a SnapProtect backup, snapshots will be created for each LUN associated with a database. Snapshots will be created even when multiple database instances share one or more LUNs. In such a case, the shared LUNs will be backed up multiple times - once as part of every instance using the LUN. When you enable the optimization and group all instances that share a set of LUNs into a single schedule policy, each shared LUN will be backed up only once. This will reduce the number of snapshots on the storage, thus saving time and storage resources.

Since multiple databases use one set of snapshots for backup, you can revert all the LUNs and databases in a single revert job. Without this optimization, reverting one database may corrupt data files of another database that shares the LUN(s).



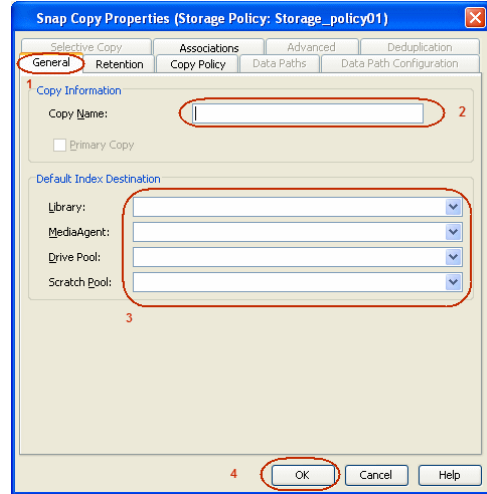
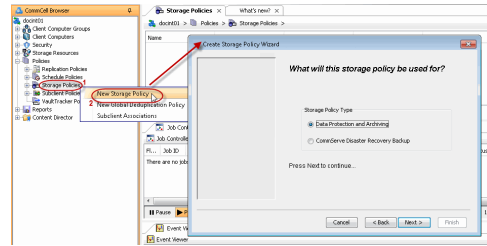
## CONFIGURING MULTIPLE INSTANCES USING A SHARED STORAGE ON A CLIENT

Follow the steps given below to configure multiple instances using a shared storage on a client:

1. Ensure that you have installed the Oracle *i*DataAgent and MediaAgent on all the source and proxy clients. See Oracle *i*DataAgent and MediaAgent deployment for

step-by-step procedure on how to install the oracle iDataAgent and MediaAgent.

2. Configure the client and instance using the steps described in Getting Started - Oracle Configuration. Ensure that you perform a manual discovery of instances.
3. Create a storage policy to perform SnapProtect operations. See Create a Storage Policy for step-by-step instructions for creating a storage policy. See Create a Snapshot Copy to enable a snapshot on the copy.

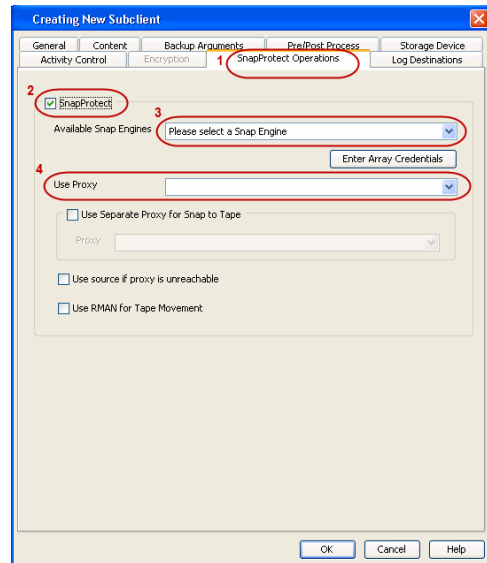


4. Create a schedule policy to perform SnapProtect operations. See Creating an Agent-Specific Data Protection Schedule Policy for step-by-step instructions.
5. Create and configure a new subclient manually as follows:

- o From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
- o Right-click the **<Instance>**, point to **All Tasks**, and then click **New Subclient**.
- o In the **Subclient name** box, type the subclient name.
- o Click the **SnapProtect Operations** tab.
- o Click **SnapProtect** option to enable SnapProtect backup for the selected subclient.
- o Select the storage array from the **Available Snap Engine** drop-down list.
- o By default, the system will perform a File System backup copy. Select **Use RMAN Movement to Tape** if you want to use RMAN backup copy.

If you are using NoArchiveLog mode Database, do not select **Use RMAN Movement to Tape**.

- o Select the proxy client from the **Use Proxy** drop-down list.
- See Configuring Proxy for RMAN Backup Copy, if you want to use a proxy for RMAN backup copy.



6. Select the storage policy from the storage device tab of the subclient created for snaps.
  - o From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle | <Instance>**.
  - o Right-click the subclient created for snaps and then click **Properties**
  - o Click the **Storage Device** tab.
  - o In the **Data Storage Policy** list, select a Storage Policy name.
  - o Click **OK** to convert the next backup as a full backup.

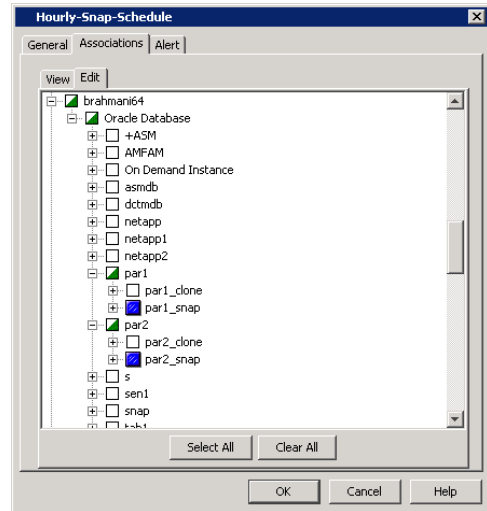
- o Click **OK**.

7. You must create and configure a subclient as shown in step-5 for all the instances included in the shared storage on a client.

Once the subclients for snaps are created for other instances, you must assign a storage policy as shown in step-6 to them.

8. Add all the subclients that are included in this shared storage environment to the schedule policy.

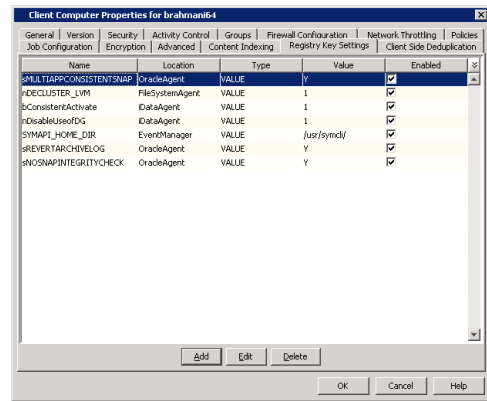
See Automatic Subclient Creation and Configuration to automatically create and configure subclients using the qscripts.



9. Ensure that all the following additional requirements are satisfied on all the clients for successful snap or clone operations in a shared LUN environment:

- o All the subclients of a client in the same schedule policy should use the same storage policy.
- o All the subclients of a client in the same schedule policy should use the same proxy client.
- o Use the sMULTIAPPCONSISTENTSAP registry key set to Y on all the clients to perform a snap for multiple databases in the same job.
- o Configure the nDECLUSTER\_LVM registry key on all the nodes and Proxy machine if cluster is configured and set it to 1.
- o If the storage array is EMC clariion or EMC Symmetrix, use the SYMAPI\_HOME\_DIR registry key to the directory where the Symmetrix SYMAPI library is present on all the clients and restart the Calypso services. In case of EMC Symmetrix, all the source devices should be in the same device group for consistency.
- o Enable the bConsistentActivate registry key on all the clients, if the array is EMC clariion or EMC Symmetrix. For Symmetrix storage array, you can enable the bSymmSmartClone, if you do not want to wait till the background copy completes for clone.
- o REDO Log for No archive log database should be on the volume for which snap should be supported.
- o Data and log volumes should not be shared and each database should have unique paths on the volumes like /data/db1, /data/db2, /log/db1, /log/db2 etc.
- o Execute the following Qscript to enable the multi instance snap optimization:

```
goperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si
EnableOracleMultiInstanceSnap -si y -si 1
```



For clone operations, perform the following in addition to the above configuration:

- While creating a new subclient, select the clone engine from the **Available Snap Engine** drop-down list in the **SnapProtect Operations** tab.
- Create a separate schedule policy for clone operations.

### AUTOMATIC SUBCLIENT CREATION AND CONFIGURATION

- Once the instances are created or discovered, execute the following QScript to create and configure the subclients:

```
goperation execscript -sn OraMultiDBCSSnapConfig -si <ClientComputerGroup> -si <hourly/snap schedule policy> -si
<daily/clone schedule policy> -si <y/n>(FullScan)
```

#### ARGUMENTS

|                             |                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------|
| Client Computer Group       | Create one client group and add all the clients for which snap/clone jobs will be performed |
| Hourly/snap schedule policy | Create hourly schedule policy which will be used to run snap jobs for every hour            |

|                             |                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Daily/clone schedule policy | Create daily schedule policy which will be used to run clone jobs once for daily.                                                                                                                                                                                                                                           |
| FullScan (Y/N)              | If the value is "n", then it is incremental scan and as part of incremental scan it will check only newly created/discovered instances. subclients will be created for them only. Otherwise it will check all the instances in that client group and create subclients if any instance do not have the required subclients. |

When you execute the script, the system will check all the instances in that client group and perform the following steps:

1. If the subclients are not already created, it will create the following two subclients for snap and clone correspondingly:

```
<instancename>_snap
```

```
<instancename>_clone
```

2. It will assign EMC TimeFinder Snap Snap Engine to <instancename>\_snap subclient and **EMC TimeFinder Clone** to **<Instancename>\_clone** subclient. See Modify Snap Engine for a subclient section to change the Snap Engine.
3. By default, the system will perform a File System backup copy. **Use RMAN Movement to Tape** is also selected for these subclients.

If you are using NoArchiveLog mode Database, disable Use RMAN Movement to Tape.

4. It will add all the snap subclients(<instancename>\_snap) to hourly schedule policy and all clone subclients(<instancename>\_clone) to daily schedule policy.

If you want to exclude instances from creating subclients and associating them to shared schedule policy, update the instance description with **exclude with cvsnap schedule**. Then the above script will not create subclients for those instances. See **Update instance description** to change the instance description using command line.

Once you execute the script, assign the storage policy and proxy client to all the subclients using the CommCell Console or command line.

Example:

Executing configuration script:

```
[root@brahmani64 Base]# ./qoperation execscript -sn OraMultiDBCGSnapConfig -si CVLT -si hourly -si daily -si n
QScript[OraMultiDBCGSnapConfig] CS[leonard64] DB[CommServ] Source[SQL File]
```

Qscript Output:

```
Changed database context to 'CommServ'.
Created snap subclients for:
Client [brahmani64] Instance [par1]
Client [brahmani64] Instance [par2]
OraMultiDBCGSnapConfig completed at Aug 8 2012 11:48PM. ErrorCode (0).
Qscript Execution Succeeded!
```

#### MODIFY SUBCLIENT USING COMMAND LINE

Download the update\_subclient\_template.xml file and save it on the computer from where the command will be executed.

#### ASSIGN A STORAGE POLICY TO A SUBCLIENT

Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameters and attributes.

```
qoperation execute -af update_subclient_template.xml -clientName brahmani64 -instanceName par1 -subclientName par1_snap -
storagePolicyName snapSP
```

#### ASSIGN A PROXY TO A SUBCLIENT

Make sure that the proxy is configured correctly before assigning a proxy to a subclient.

- Refer Configuring Proxy for RMAN Movement to Tape.
- Install the File System and MediaAgent for FS Movement to tape.

Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameters and attributes.

```
qoperation execute -af update_subclient_template.xml -clientName brahmani64 -instanceName par1 -subclientName par1_snap -
storagePolicyName snapSP -snapToTapeProxyToUse/clientName dbcs
```

#### DISABLE USE RMAN MOVEMENT TO TAPE

You must disable Use RMAN movement to tape for NOARCHIVELOG databases.

Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameters and attributes.

```
qoperation execute -af update_subclient_template.xml -clientName brahmani64 -instanceName par1 -subclientName par1_snap -
storagePolicyName snapSP -snapToTapeProxyToUse/clientName dbcs -isRMANEnableForTapeMovement false
```

### MODIFY SNAP ENGINE FOR A SUBCLIENT

Download the update\_snapengine\_template.xml file and save it on the computer from where the command will be executed.

Execute the following command from the <Software\_Installation\_Directory>/Base folder after substituting the parameters and attributes.

```
qoperation execute -af update_snapengine_template.xml -clientName brahmani64 -instanceName parl -subclientName parl_snap -
storagePolicyName snapSP - snapShotEngineName "EMC CLARiiON Snapview Snap"
```

### UPDATE INSTANCE DESCRIPTION

Execute the following command to change the instance description after substituting the parameters and attributes:

```
[root@brahmani64 Base]#./qoperation execscript -sn SetOracleInstanceProperties.sql -si brahmani64 -si 'Q_ORACLE' -si parl
-si 'User Description' -si 'exclude from cvsnap schedule' -si 1
```

### CONFIGURING PROXY FOR RMAN BACKUP COPY

When you configure a proxy for RMAN backup copy, make sure to satisfy the following requirements:

- Make sure that the data, log, diag, FRA and all the dump directories on the proxy are identical to the source.
- Oracle gid and uid should match the source computer's oracle user.
- Oracle instances on the proxy should be configured similar to those at source and should be in started mode. You need to configure the instances on the CommCell console.
- You can also use sRMANDATAFILECOPY registry key for RMAN backup copy. See RMAN Backup Copy Operationsns for more information.

## SNAPPROTECT BACKUP FOR MULTIPLE INSTANCES

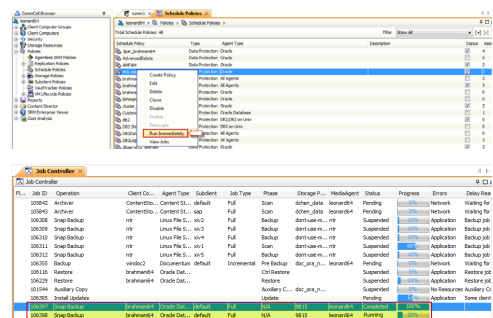
A snap or clone operation is performed for all the instances at the same time in a shared LUN environment using the schedule policy created specifically for this purpose. You can perform a snap or clone operation immediately or at a scheduled time.

When you perform a SnapProtect backup or a clone operation, the system performs the following:

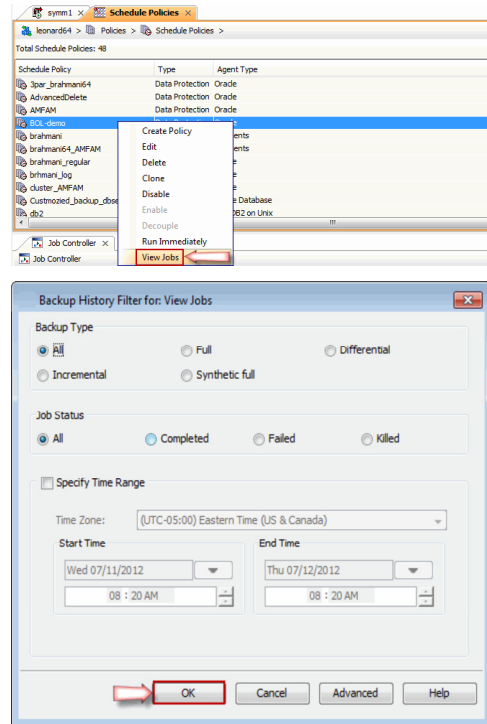
- A single job among multiple jobs will be selected and this job becomes the master job.
- Master job will collect all the data mount points for all the databases which are included in the schedule policy and performs the following:
  - If the database is in archive log mode and open, it will be change it to a hot backup mode. This will be performed for all the archive log databases.
  - If the database is in noarchive log mode and open, it will completely depend on consistent option provided by snap engine and will also take a snap for REDO log location.
  - If the database is noarchive log DB, it will not change the database to a hot backup mode..
  - If one of the databases is down or in started mode, it will skip that database for snap operation.
- SnapProtect will be performed for all the data mount points at the same time. After Snap operation, the databases are changed from hot backup mode.
- Master job switches the log for archive log DB and will take the backup of controlfile to archive log location or data file location for archive log DB and No archive log DB correspondingly.
- Similar to data, all the mount points for log will be collected and snaps will be performed.
- Once archive indexing is completed, the master job is marked as complete.
- Once the master job is completed, all the other jobs will continue and verify whether the snaps are already taken. If they know that the snaps are already taken, they just clone the archive files, perform archive index and completes the job.

Use the following steps to perform a SnapProtect backup:

1. From the CommCell Browser, navigate to **Policies | Schedule Policies**.
2. Right-click the **<Schedule Policy>** in the right pane and click **Run Immediately**.
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 **Schedule Policy** and select **View Jobs**.

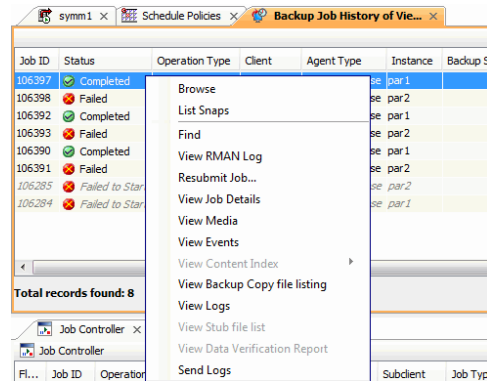


5. Click **OK**.



6. Right-click the job to:

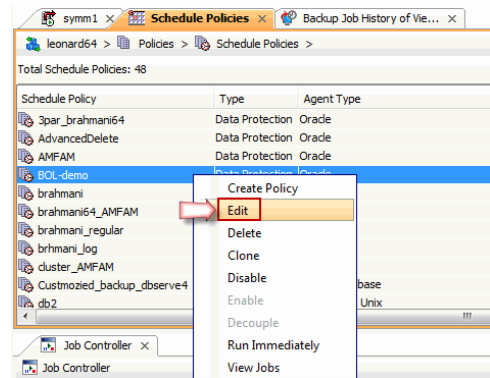
- Browse the databases that were backed up.
- List Snaps
- View RMAN Logs.
- Resubmit the job.
- View job details.
- View media associated with the job.
- View events associated with the job.
- View or send the log file that is associated with the job.



### SCHEDULING A SNAPPROTECT BACKUP FOR ALL THE INSTANCES IN A SHARED LUN ENVIRONMENT

Use the following steps to schedule a SnapProtect backup for all the instances in a shared LUN environment:

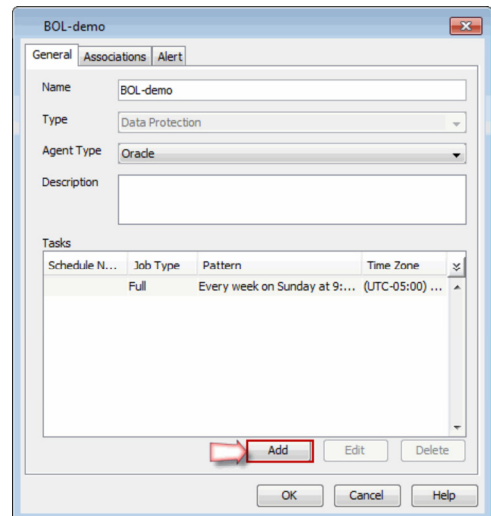
1.
  - From the CommCell Browser, navigate to **Policies | Schedule Policies**.
  - Right-click the **<Schedule Policy>** in the right pane and click **Edit**.



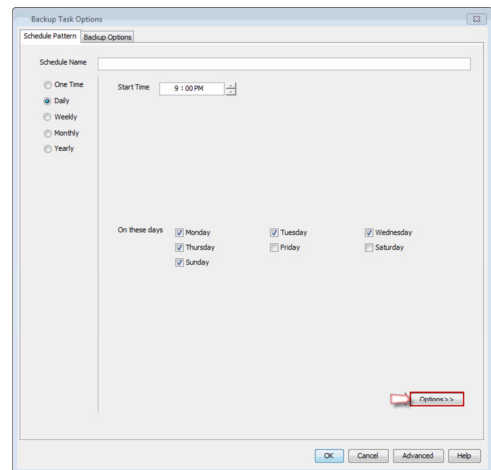
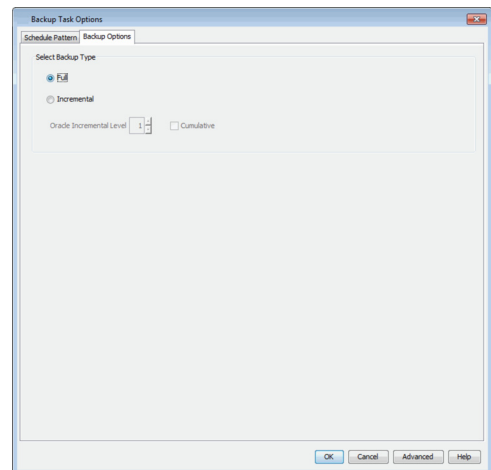
2. Click **Add** button.



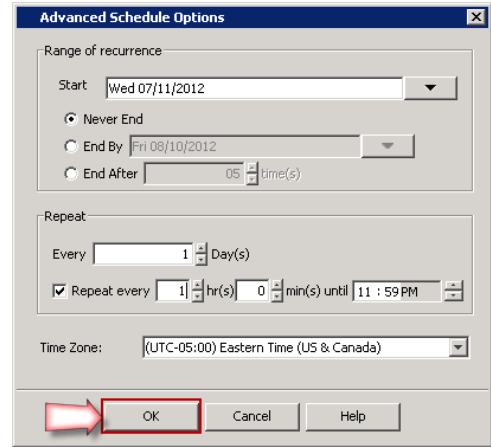
3.
  - Click the **Backup Options** tab.
  - Click **Full**.



4. Select the appropriate scheduling options.  
For example:
  - Click **Daily**.
  - Check the days you want to run the SnapProtect backup job.
  - Change the Start Time to 9:00 PM.
  - Click **Options**.



5. Select the appropriate advanced schedule options.  
For example:
  - Click **Start date**.
  - Select the end dates or times after which you want to stop the scheduled job.
  - Change the Repeat Times.
  - Specify the **Time Zone** for the schedule.
  - Click **OK**.



6.
  - Click **OK** to close the **Backup Task Options** dialog box.
  - Click **OK** to close the **Scheduled Policy** dialog box.

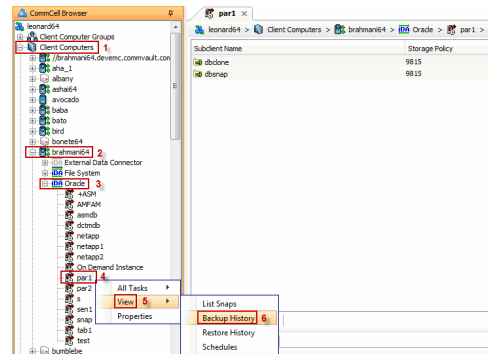
The SnapProtect backup job for instances in a shared storage will execute as per the schedule.

## RESTORING A DATABASE OR DATAFILES /TABLE SPACES FROM A DATABASE

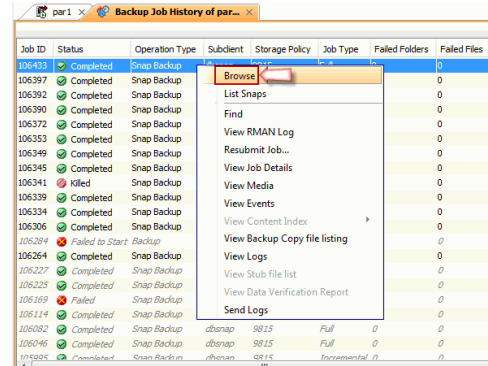
You can restore each database or some of the datafiles/table spaces from one database on a client.

Use the following steps to restore a database:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **View** and then click **Backup History**.
3. In the Backup History Filter for <Instance> dialog box, click **OK**.

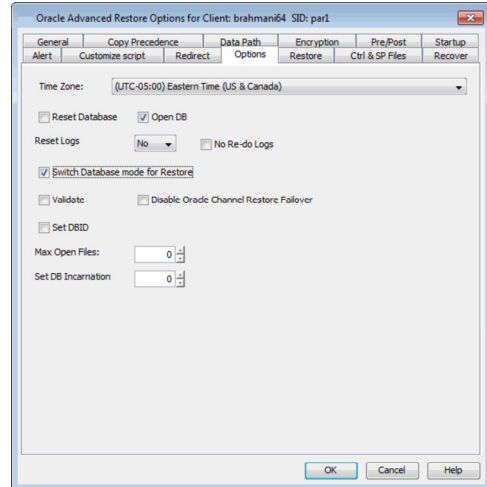
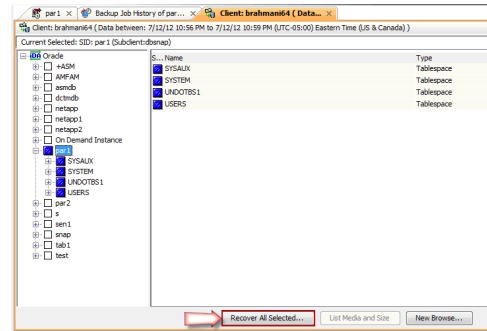


4. Right-click the SnapProtect job you want to restore and click **Browse**.
5. In the **Browse Options** dialog box, click **OK**.



6. In the right pane of the Browse window, select an entire instance or the datafiles or tablespaces you want to restore and click **Recover All Selected**.

7. In the **Restore Options** dialog box, click **Advanced**.
8. Click the **Options** tab.
9. Select **None** from the **Reset Logs** list.  
For No archive log database, select **Yes** from the **Reset Logs** list as the restore will always be Point-in-time restore and REDO logs which were existing in snap/clone will only be applied. You should perform a full database restore for no archive log database.
10. Select **Switch Database mode for Restore** check box.
11. Click **OK**.

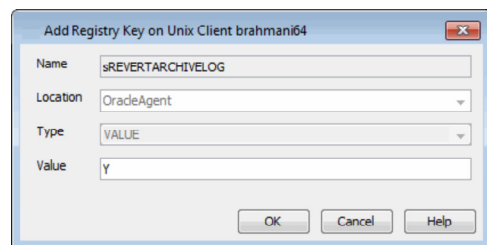


## REVERT FROM A SNAPPROTECT JOB

If you perform a revert from a SnapProtect job from a schedule policy, it will revert all the databases which were snapped in that SnapProtect backup job to the same point-in-time. Ensure that you have performed a SnapProtect backup for all the databases which share the same LUNs.

Ensure that both the data and log volumes are reverted for successful revert operation. By default, the data volumes only are reverted. Perform the following to revert the log volumes also in addition to data volumes:

1. From the CommCell console, navigate to **Client Computers | <Client>**
2. Right-click the **<client>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type `sREVERTARCHIVELOG`.
6. In the **Location** box, type or select `OracleAgent` from the list.
7. In the **Type** box, select **Value**.
8. In the **Value** box, type **Y** and then click **OK**.



Use the following steps to revert a SnapProtect job:

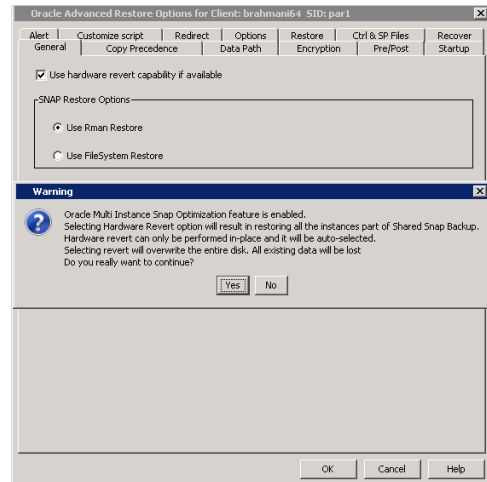
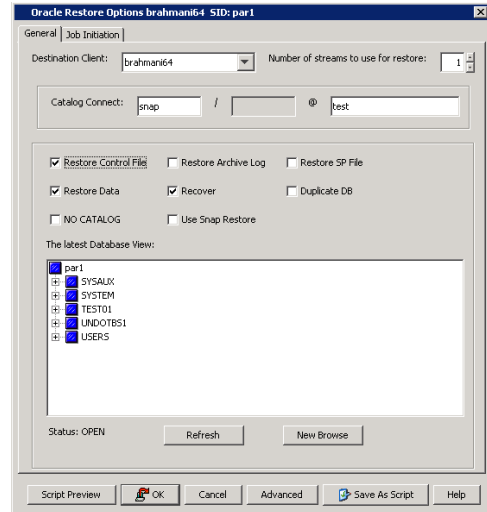
1. From the CommCell Browser, navigate to **Client Computers | <Client> | Oracle**.
2. Right-click the **<Instance>**, point to **All Tasks** and then click **Browse Backup Data**.
3. From the **Browse Options** dialog box, click **OK**.
4. Select the data you want to revert and click **Recover All Selected**.

Even if you select one instance, it will revert all the databases that are included in the SnapProtect job.

5. From the **Restore Options** dialog box, select **Restore Control File**.
6. Click **Advanced**.

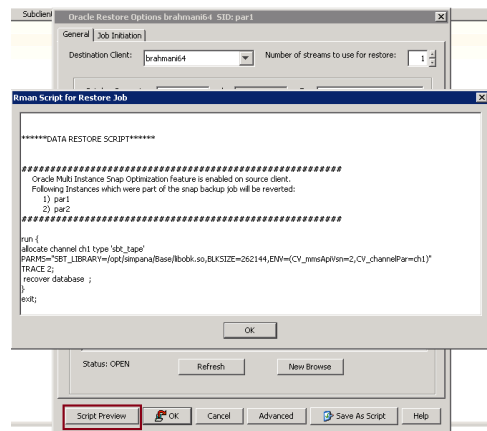
7. Select the **Use hardware revert capability if available** option.

A warning message displaying that the oracle multi instance snap optimization feature is enabled and selecting hardware revert option will result in restoring all the instances which are included in the shared snapprotect backup. The message informs you that the hardware revert can only be performed in-place and it will be automatically selected. The message will also warn you that the selection of revert option will overwrite the entire disk and all the existing data will be lost. Select **Yes** if you still want to continue. Select **No** if you do not want to continue.



8. Click **Options** tab.
9. Select **Yes** from the **Reset Logs** list.
10. Select **Switch Database mode for Restore**.
11. Click **OK** to confirm the revert operation.
12. Click **OK** from the **Advanced Restore Options** dialog box.
13. Click **Script Preview** to verify the instances that are being reverted in the current revert operation.
14. Click **OK** to start the revert operation.

if the database is in mount mode while taking a SnapProtect backup, then the same status is preserved even after the revert operation.



Once a revert is completed, resync the catalog using RMAN to register the new incarnation.

Example:

```
[oracle@brahmani64 ~]$ export ORACLE_SID=par2
```

```
[oracle@brahmani64 ~]$ rman target / catalog snap/snap@test
```

```
Recovery Manager: Release 10.2.0.4.0 - Production on Fri Jul 13 10:04:19 2012
```

```
Copyright (c) 1982, 2007, Oracle. All rights reserved.
```

```
connected to target database: PAR2 (DBID=1259990815)
```

connected to recovery catalog database

```
RMAN> resync catalog;
```

starting full resync of recovery catalog

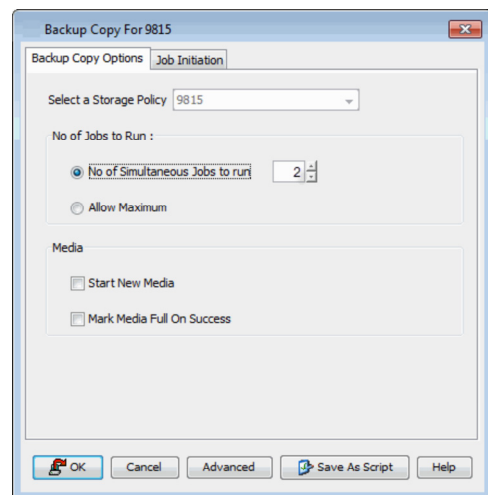
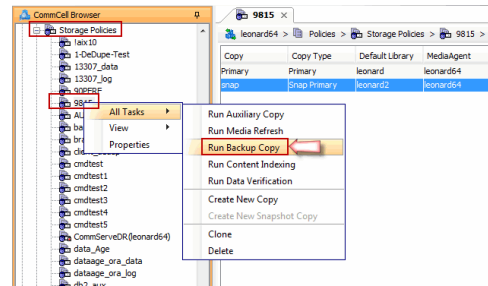
full resync complete

```
RMAN>
```

## BACKUP COPY FOR MULTIPLE INSTANCES USING A SHARED STORAGE ON A CLIENT

Once the SnapProtect jobs are completed, you can perform or schedule backup copy jobs. You can run parallel backup copy for all the SnapProtect jobs which are performed using a schedule policy in one operation. In case of parallel backup copy, mount all the snaps in the first backup copy job itself. The other jobs will use these mount points and backup their corresponding databases.

1. From the CommCell Browser, navigate to **Policies | Storage Policies**.
2. Right-click the **<Storage Policy>** in the right pane, point to **All Tasks** and click **Run Backup Copy**.
3. Select **Number of simultaneous jobs to run** from the list.
4. Click **Job Initiation** tab.
5. Select **Immediate** to perform the backup copy job. You can also click **Schedule** to perform the job at a scheduled time.
6. Click **OK**.



See Backup Copy Operations and Restoring Data from Backup Copy for more information on backup copy operations.

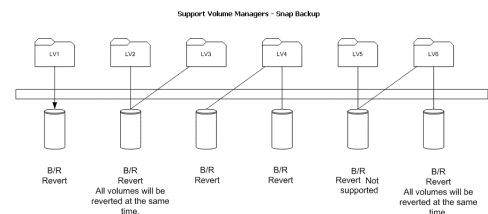
## SUPPORTED VOLUME MANAGERS

- 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.

### OPTIONS NOT APPLICABLE FOR ORACLE SNAPPROTECT

The following options do not apply to SnapProtect backup for Oracle iDataAgent:

| DIALOG BOX                         | TABS/OPTIONS NOT APPLICABLE                                                                                                                                                                                                                                                                                           |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Backup Options dialog box | <ul style="list-style-type: none"> <li>• Delete Archive Logs tab</li> <li>• Custom RMAN Script tab                             <ul style="list-style-type: none"> <li>○ Customize Script</li> </ul> </li> </ul>                                                                                                       |
| Subclient Properties dialog box    | <ul style="list-style-type: none"> <li>• Archive Delete option in Content tab</li> <li>• Log Destinations tab                             <ul style="list-style-type: none"> <li>○ Select ArchiveLog Destinations for Delete</li> </ul> </li> <li>• Backup Arguments tab (applicable for RMAN backup copy)</li> </ul> |

### OPTIONS NOT APPLICABLE FOR ORACLE SNAP RESTORE

The following options do not apply to snap restore for Oracle iDataAgent:

| DIALOG BOX                          | TABS/OPTIONS NOT APPLICABLE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Oracle Restore Options dialog box   | <ul style="list-style-type: none"> <li>• General tab                             <ul style="list-style-type: none"> <li>○ Duplicate DB</li> </ul> </li> <li>• Script Preview</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Advanced Restore Options dialog box | <ul style="list-style-type: none"> <li>• Customize Script tab</li> <li>• Redirect tab</li> <li>• Restore tab                             <ul style="list-style-type: none"> <li>○ Restore Archive Log By Log Time</li> <li>○ Restore Archive Log By Log Serial Number</li> <li>○ Restore Archive Log to Target Directory</li> </ul> </li> <li>• Options tab                             <ul style="list-style-type: none"> <li>○ Set DBID</li> <li>○ Max Open Files (applicable for RMAN backup copy)</li> <li>○ Validate</li> <li>○ Disable Oracle Channel restore Failover</li> </ul> </li> </ul> |

### ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | RELATED TOPICS                                                               |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| SCSI Reservation      | <p>SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key nSCSIReserveForSnap to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).</p> <p>If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail.</p>                                                                                                                                                                                                                                                                                      | For more information on registry keys, Registry keys                         |
| Pre/Post Commands     | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                 | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| View Snapshot Details | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> </ol> |                                                                              |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
|                                             | 3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                     |
| <b>Select a Job for Backup Copy</b>         | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                     |                                                     |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol> |                                                     |
| <b>Offline Snap Copy Job Summary Report</b> | Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.                                                                                                                                                                                                                                                                                                                                                                                                                                                | See Backup Copy Job Summary Report for more details |

[Back to Top](#)

# Advanced - Microsoft SQL Server SnapProtect™ Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Restoring Data from a Backup Copy

### Additional Options

## MANAGING SNAPSHOTS

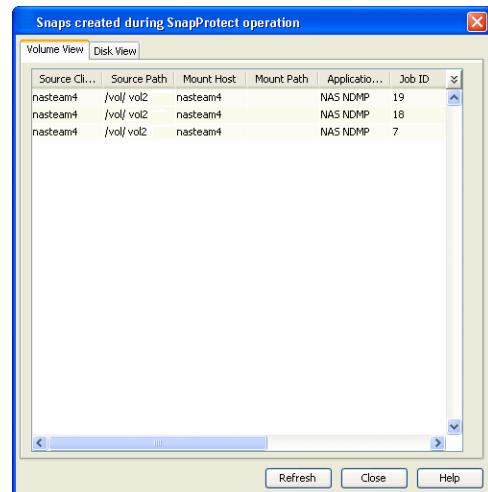
The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete, or revert.

### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

- From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **SQL Server**.
- Right-click **<Instance>** and click **All Tasks** | **List Snaps**.
- The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the SQL Agent. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.

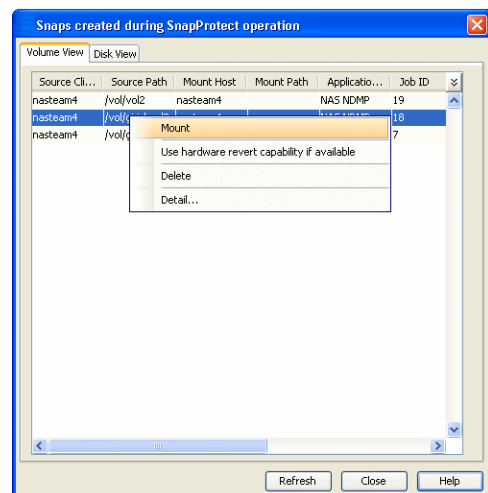


### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

- From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **SQL Server**.
- Right-click **<Instance>** and click **All Tasks** | **List Snaps**.
- Right-click the snapshot that you wish to mount and click **Mount**.
- Click **Yes**.
- In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
- If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
- Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.



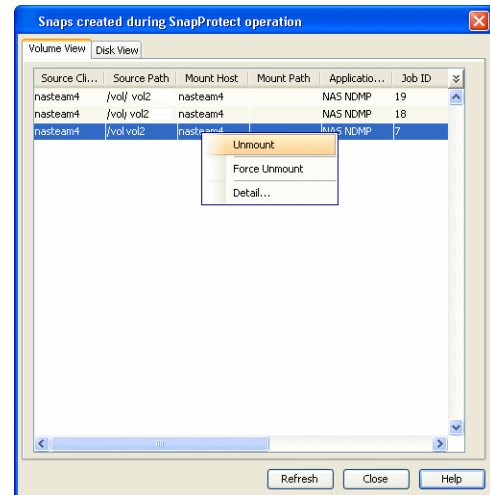


## UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **SQL Server**.
2. Right-click **<Instance>** and click **All Tasks** | **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



## DELETE SNAPSHOTS

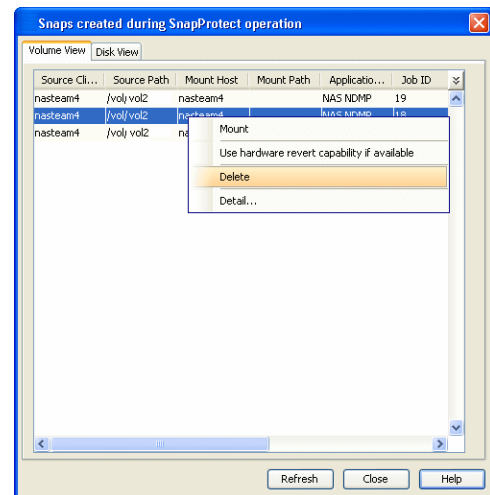
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **SQL Server**.
2. Right-click **<Instance>** and click **All Tasks** | **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

- `RevertSnapVolume` has been set to 1.
- Ensure that the archived redo log files and their mirror log files reside on the same array volume.
- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.
- Revert operations are not supported on Windows clustered disks.
- All the databases on a volume must be backed up using SnapProtect backup, failing which the revert operation will make the data inconsistent.

- All the databases on a volume must be selected for the revert operation. Also, the databases must be backed up using a single SnapProtect backup job.
- Ensure that the **Unconditionally Overwrite** restore option is selected for SQL Server *iDataAgent*. If this option is not selected, restores of SnapProtect backup data will fail.
- After performing a revert operation, you must restart the SQL Server service so that the databases are re-linked to the data files.
  - It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
  - If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

### PERFORM AN APPLICATION AWARE REVERT

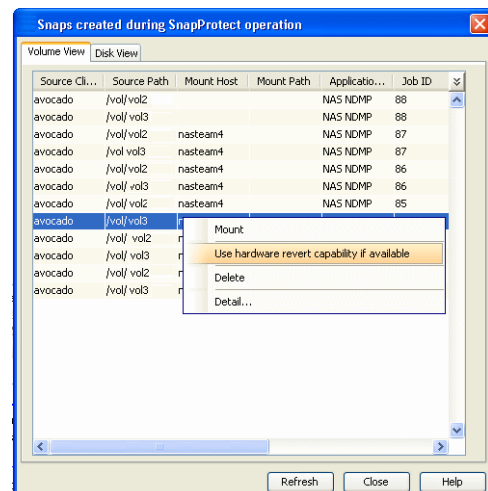
1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.

- An application aware revert operation reverts back all the volumes included in the backup.
- For NetApp NFS configurations:
  - This operation reverts all data on the file server volume, not just the data that is associated with the application.
  - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
  - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

### PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers | <Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, *confirm*.
5. Click **OK**.

- A hardware specific revert operation reverts back the volume included in the snapshot.
- For NetApp NFS configurations:
  - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
  - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
  - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



## SNAP RECONCILIATION

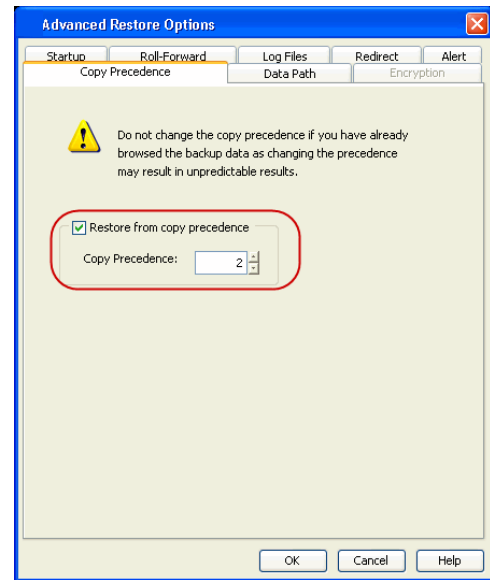
Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy

precedence number.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                                      | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | RELATED TOPICS                                                               |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>SCSI Reservation</b>                     | <p>SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key nSCSIReserveForSnap to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).</p> <p>If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail.</p>                                                                                                                                                                                                                                                                                                                                                                                     | For more information on registry keys, Registry keys                         |
| <b>Pre/Post Commands</b>                    | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                                                                                                                | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>                | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol> |                                                                              |
| <b>Select a Job for Backup Copy</b>         | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                          |                                                                              |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                      |                                                                              |
| <b>Offline Snap Copy Job Summary Report</b> | <p>Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | See Backup Copy Job Summary Report for more details                          |

[Back to Top](#)

# Advanced - NAS SnapProtect™ Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert Snapshots

### Restoring Data from a Backup Copy

### Restricting the Number of Backup Jobs Running on a File Server

- Enabling for all Clients
- Enabling for A Specific Client
- Additional Operations

### Data Aging for SnapProtect Snapshots

- Retention by Number of Jobs
- Retention using Spool Copy

### Additional Options

## MANAGING SNAPSHOTS

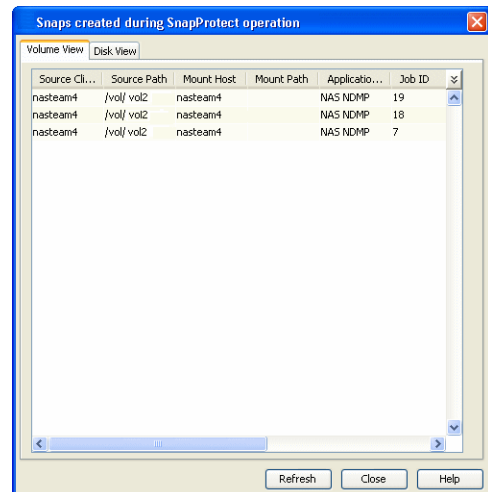
The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete or revert.

### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.

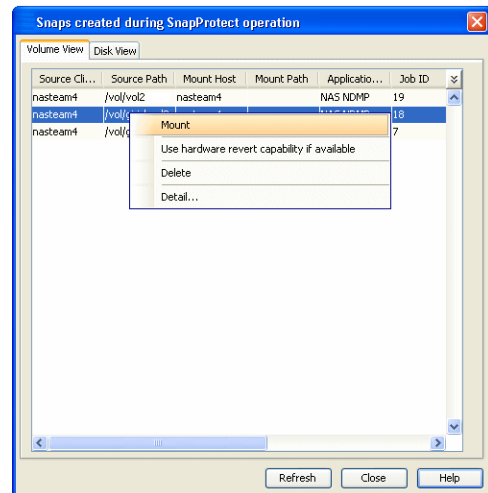


### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. Specify the destination client and the path on the client in **Destination Client** field.
6. Enter a **CIFS Share Name**.
7. Click **OK**.
8. Click **OK** to close the **Subclient Properties** dialog box.

The mounting of snapshots is supported for Unix MediaAgents if NetApp volume security model is a Unix type.

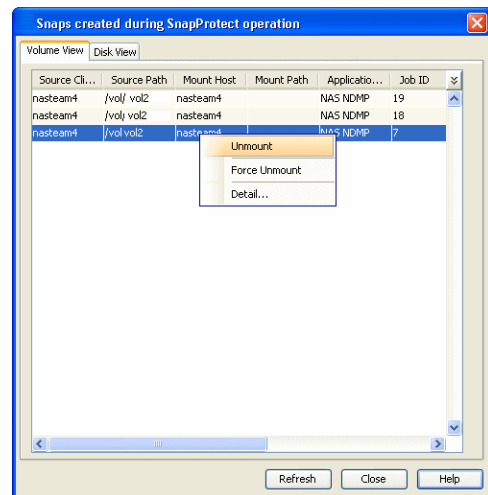


## UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



## DELETE SNAPSHOTS

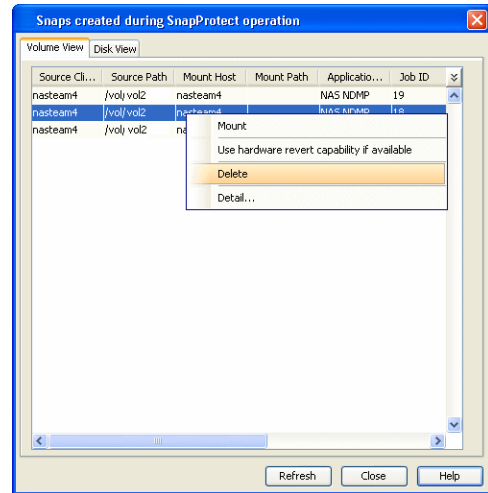
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



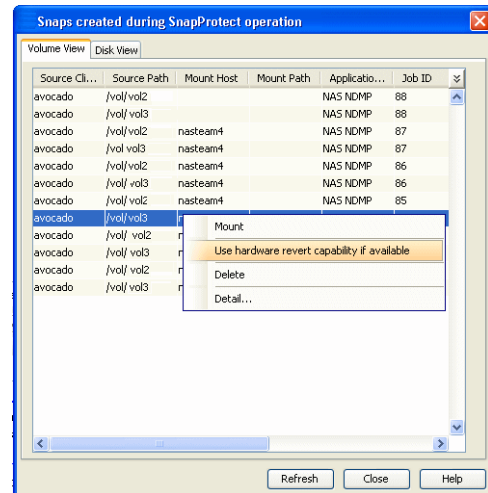
## REVERT SNAPSHOTS

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

- It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
- If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

### PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers** | **<Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, *confirm*.
5. Click **OK**.
  - A hardware specific revert operation reverts back the volume included in the snapshot.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

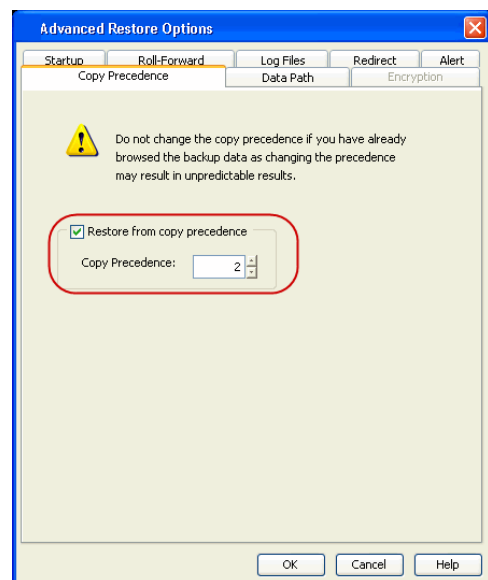


## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks** | **Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.

5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## RESTRICTING THE NUMBER OF BACKUP JOBS RUNNING ON A FILE SERVER

You can restrict the number of backup jobs that can run on the file server. The jobs exceeding the number specified will be queued and will be processed as soon as any running job completes.

### ENABLING FOR ALL CLIENTS

Use the following command line operations to enable/disable this feature for all clients:

1. To run command line operations, you must first login to the CommServe.

From Command prompt, navigate to <Software\_Installation\_Directory>/Base and run the following command:

```
qlogin -cs <commserve name> -u <user name>
```

For example, to log on to CommServe 'server1' with username 'user1':

```
qlogin -cs server1 -u user1
```

2. To enable the restriction of number of backups on a file server.

```
qoperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si ThrottleJobsFeature -si y -si 1
```

3. To set the limit the number of backup jobs that can run on a client.

If you want to limit the number of jobs to 5, then <number of jobs> should be replaced by 5 in the command.

```
qoperation execscript -sn SetLimitRunningJobs.sql -si 'myclient' -si 'DataCount' -si <number of jobs>
```

### ENABLING FOR A SPECIFIC CLIENT

Use the following command line operations to enable/disable this feature for a specific client:

1. To run command line operations, you must first login to the CommServe.

From Command prompt, navigate to <Software\_Installation\_Directory>/Base and run the following command:

```
qlogin -cs <commserve name> -u <user name>
```

For example, to log on to CommServe 'server1' with username 'user1':

```
qlogin -cs server1 -u user1
```

2. To enable the option to restrict the number of running jobs for a specific client.

```
qoperation execscript -sn SetLimitRunningJobs.sql -si 'myclient' -si 'LimitJobs' -si 1
```

3. To set the limit the number of backup jobs that can run on a client.

If you want to limit the number of jobs to 5, then <number of jobs> should be replaced by 5 in the command.

```
qoperation execscript -sn SetLimitRunningJobs.sql -si 'myclient' -si 'DataCount' -si <number of jobs>
```



## ADDITIONAL OPERATIONS

After logging in to the CommServer, you can perform different operations.

| OPERATIONS                                                    | COMMAND                                                                                 |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Disabling for all Clients                                     | qoperation exectuption -sn SetKeyIntoGlobalParamTbl.sql -si ThrottleJobsFeature -si n   |
| Disabling for a Specific Client                               | qoperation exectuption -sn SetLimitRunningJobs.sql -si 'myclient' -si 'LimitJobs' -si 0 |
| Enabling the Exclusion of Running Jobs for a Specific Client  | qoperation exectuption -sn SetLimitRunningJobs.sql -si 'myclient' -si 'Exclude' -si 1   |
| Disabling the Exclusion of Running Jobs for a Specific Client | qoperation exectuption -sn SetLimitRunningJobs.sql -si 'myclient' -si 'Exclude' -si 0   |
| Viewing the Current Setting on a Specific Client              | qoperation exectuption -sn SetLimitRunningJobs.sql -si 'myclient' -si 'View             |

## DATA AGING FOR SNAPPROTECT SNAPSHOTS

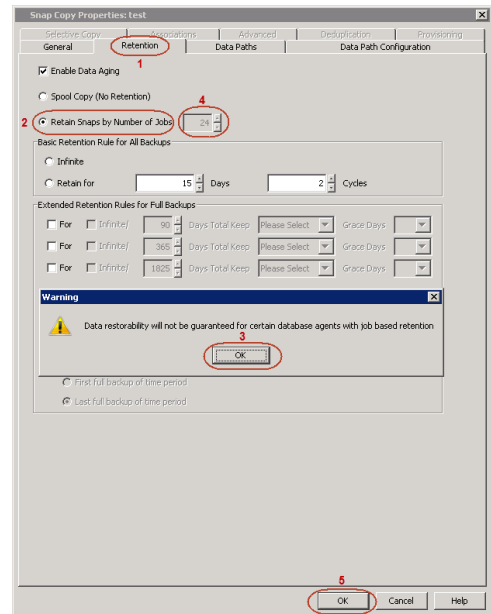
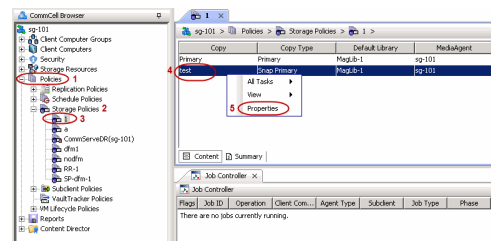
The following procedures describe the available retention configurations for snapshots. For movement to media retention, refer to Data Aging - Getting Started.

### RETENTION BY NUMBER OF JOBS

By default, snapshots are pruned based on the number of retention days and cycles specified in the storage policy. You can configure your snapshot copy to retain a defined number of SnapProtect backup jobs. When the total number of jobs goes above the specified retention number, the remaining jobs will be pruned. This configuration is recommended for File System and File System like Agents. This feature is supported for SnapProtect operations performed using the NetApp storage array.

The **NetApp Snap Management** license is required for retaining snaps by number of jobs.

- From the CommCell Console, navigate to **Policies | Storage Policies | <Storage Policy>**.
  - Right-click the primary snapshot copy and click **Properties**.
- Click the **Retention** tab.
  - Click **Retain Snaps by Number of Jobs**.
  - Click **OK** to the warning dialog box.
  - Specify the number of jobs to be retained for the primary copy.
  - Click **OK**.



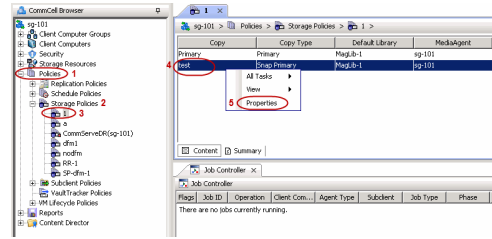
### RETENTION USING SPOOL COPY

By default, snapshots are aged based on the retention criteria specified in the storage policy. If you do not want the snapshot copy to retain your snapshot data, you can use a spool copy to temporarily retain the snapshots on the primary copy. Once the snapshot data is copied to an active synchronous copy, the

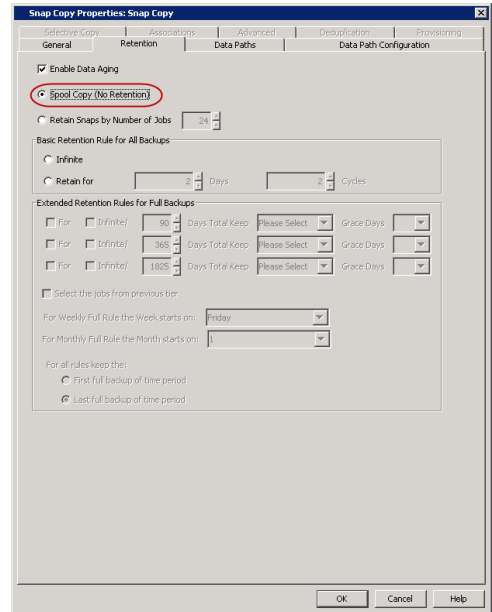
data on the primary copy is aged.

By default, a spool copy has a retention rule of 0 days and 0 cycles. For NAS snapshots, this copy has a retention rule of 0 days and 1 cycle.

1.
  - From the CommCell Console, navigate to **Policies | Storage Policies | <Storage Policy>**.
  - Right-click the primary snapshot copy and click **Properties**.



2.
  - Click the **Retention** tab.
  - Click **Spool Copy (No Retention)**.
  - Click **OK**.



## ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                                    | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | RELATED TOPICS                                                               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>Skip Catalog Phase for Snap Backup</b> | <p>This option allows you to accelerate backup jobs by skipping the indexing of snapshot data. When enabled, browse and restore operations should be performed from the backup copy. If other copies are used, the browse and restore operation will not work.</p> <p>You can still mount or revert the snapshot after enabling this option.</p> <p>If you want to perform a browse and restore using a different copy, follow the steps below.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, navigate to <b>&lt;Client&gt;   NAS NDMP</b>.</li> <li>2. Right click the subclient and click <b>Backup</b>.</li> <li>3. From the <b>Backup Options</b> dialog box, click <b>Advanced</b>.</li> <li>4. Clear the <b>Skip Catalog Phase for Snap Backup</b> checkbox.</li> <li>5. Click <b>OK</b>.</li> </ol> |                                                                              |
| <b>Pre/Post Commands</b>                  | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>              | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol>              |                                                                              |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                            |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| <b>Select a Job for Backup Copy</b>         | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                     |                                                            |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol> |                                                            |
| <b>Offline Snap Copy Job Summary Report</b> | <p>Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>See Backup Copy Job Summary Report for more details</p> |

[Back to Top](#)

# Advanced - Microsoft Hyper-V SnapProtect™ Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Restoring Data from a Backup Copy

### Data Aging for SnapProtect Snapshots

- Retention by Number of Jobs

### Additional Options

## MANAGING SNAPSHOTS

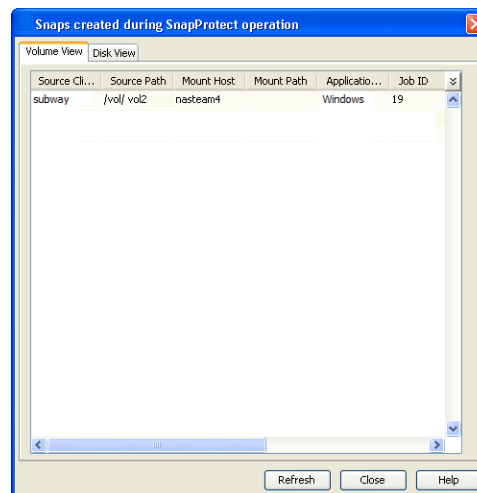
The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete, or revert.

### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.

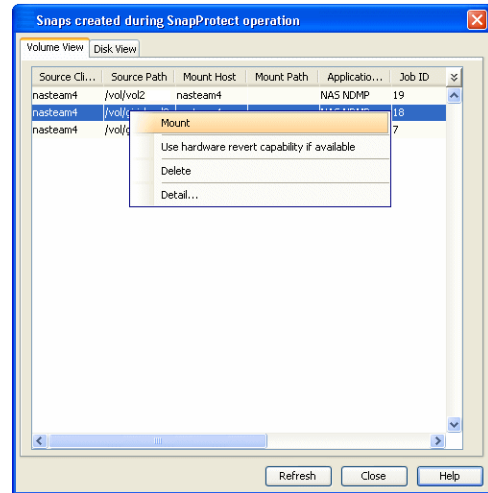


### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

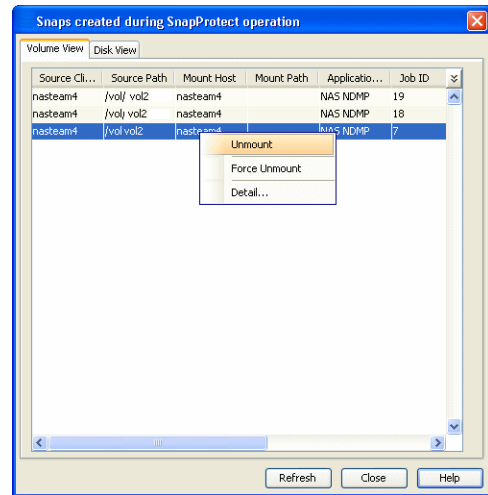


## UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



## DELETE SNAPSHOTS

Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

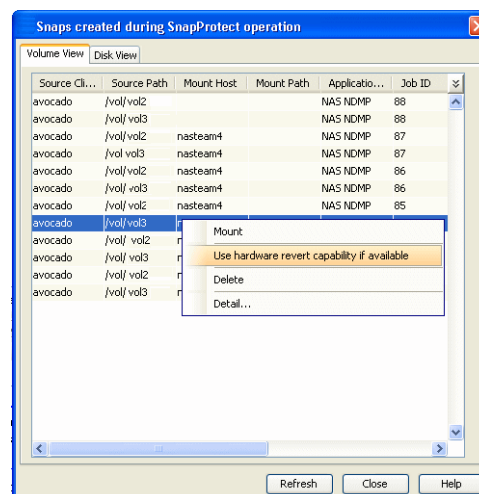
- Revert operations are not supported on Windows clustered disks.
- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.
  - It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
  - If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

## PERFORM AN APPLICATION AWARE REVERT

1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.
  - An application aware revert operation reverts back all the volumes included in the backup.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the application.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

## PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers | <Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, `confirm`.
5. Click **OK**.
  - A hardware specific revert operation reverts back the volume included in the snapshot.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



## SNAP RECONCILIATION

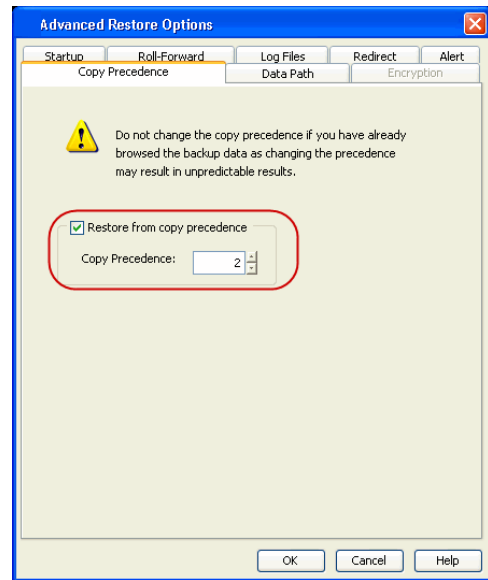
Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.

5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## DATA AGING FOR SNAPPROTECT SNAPSHOTS

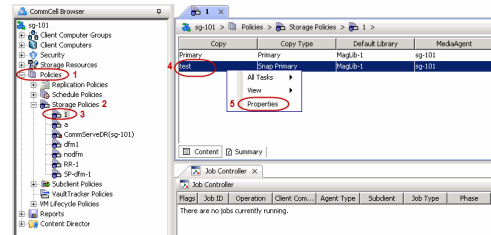
The following procedures describe the available retention configurations for snapshots. For movement to media retention, refer to Data Aging - Getting Started.

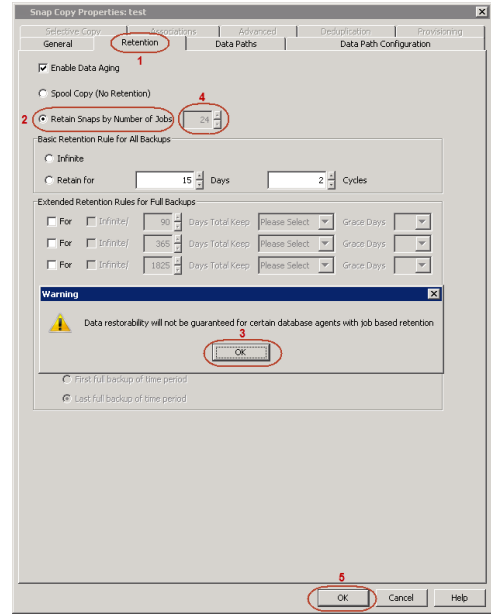
### RETENTION BY NUMBER OF JOBS

By default, snapshots are pruned based on the number of retention days and cycles specified in the storage policy. You can configure your snapshot copy to retain a defined number of SnapProtect backup jobs. When the total number of jobs goes above the specified retention number, the remaining jobs will be pruned. This configuration is recommended for File System and File System like Agents. This feature is supported for SnapProtect operations performed using the NetApp storage array.

The **NetApp Snap Management** license is required for retaining snaps by number of jobs.

1.
  - From the CommCell Console, navigate to **Policies | Storage Policies | <Storage Policy>**.
  - Right-click the primary snapshot copy and click **Properties**.
  
2.
  - Click the **Retention** tab.
  - Click **Retain Snaps by Number of Jobs**.
  - Click **OK** to the warning dialog box.
  - Specify the number of jobs to be retained for the primary copy.
  - Click **OK**.





## ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                              | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | RELATED TOPICS                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>Job Results Directory</b>        | <p>Ensure that the full path name for the Job Results Directory, combined with the VMDK file name, is no greater than 255 characters in length.</p> <ol style="list-style-type: none"> <li>From the CommCell Browser, right-click the icon of the client computer whose job results path you want to change, then click <b>Properties</b>.</li> <li>From the <b>Job Configuration</b> tab of the <b>Client Computer Properties</b> dialog box, click <b>User Name/Password</b> to establish or change the Impersonate User account to access the Job Results Directory. Click <b>OK</b> once you have administered the account.</li> <li>From the <b>Job Configuration</b> tab, type a new job results path in the <b>Job results path</b> field.<br/>You can also click <b>Browse</b> to browse to a new job results path from the <b>Browse for Job Result Path</b> dialog box. Click <b>OK</b>.</li> <li>Click <b>OK</b> to save your changes.</li> </ol> | Refer to Job Management.                                                     |
| <b>SCSI Reservation</b>             | <p>SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key nSCSIReserveForSnap to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).</p> <p style="text-align: center;">If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | For more information on registry keys, Registry keys                         |
| <b>Pre/Post Commands</b>            | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p style="text-align: center;">Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>        | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol>                                                                                                                                              |                                                                              |
| <b>Select a Job for Backup Copy</b> | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                              |



|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                            |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
|                                             | <p>move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                                                                  |                                                            |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol> |                                                            |
| <b>Offline Snap Copy Job Summary Report</b> | <p>Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>See Backup Copy Job Summary Report for more details</p> |

[Back to Top](#)

# Advanced - SAP for Oracle SnapProtect™ Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Restoring Data from a Backup Copy

### SnapProtect Backup Using SAP Command Line

### NFS SnapProtect for SAP for Oracle

- Enabling Volume Level Reverts on NFS Volumes

### Supported Volume Managers

### Options not applicable for SAP for Oracle

### Additional Options

## MANAGING SNAPSHOTS

The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete, or revert.

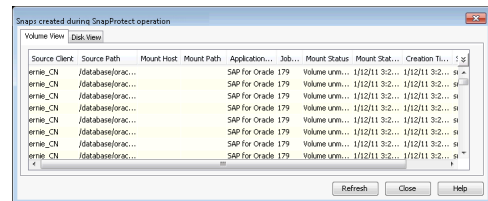
### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.

You can also browse snapshots at the instance level of the SAP for Oracle Agent.

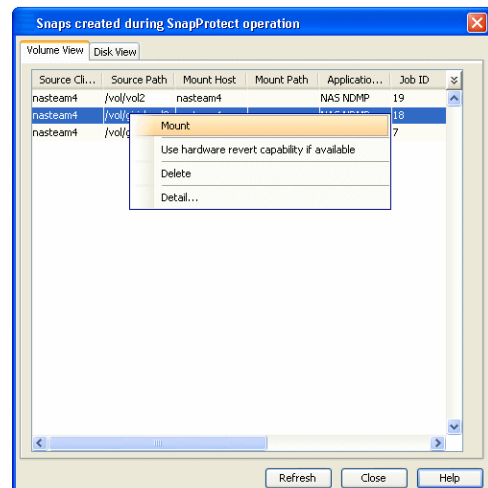


### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

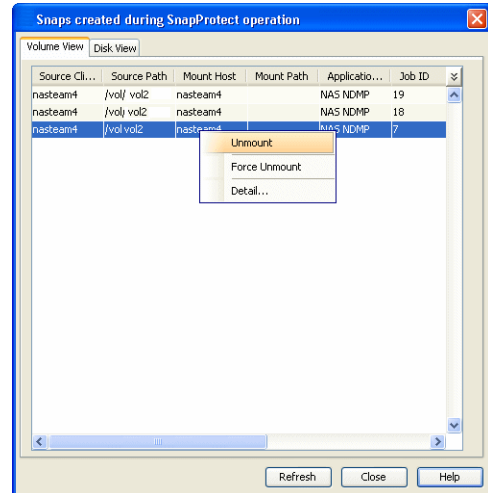


## UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



## DELETE SNAPSHOTS

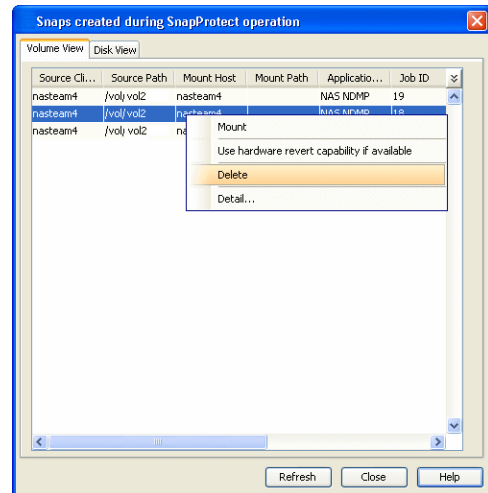
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

- As only the data volumes can be reverted, ensure that the database and other SAP data volumes reside on separate LUNs or drives. For example, sapdata (1-#) volumes and other volumes like sapbackup, saparch, sapreorg, dbs should reside on separate LUNs or drives.
- On Unix clusters, use pre/post scripts to freeze and unfreeze the cluster for revert operations. For example, on Red Hat Linux cluster, use the following command in the pre/post scripts:

```
clusvcadm -Z <group> to freeze the cluster
```

```
clusvcadm -U <group> to unfreeze the cluster
```

This is required because, during revert the application is shut down and corresponding volumes are unmounted. In that case, the cluster will automatically failover to another node thus preventing the revert operation.

## PERFORM A SAP ORACLE REVERT RESTORE OPERATION USING THE COMMAND LINE INTERFACE

Review the following before performing a revert operation:

- Set RevertSnapVolume to 1 at the following location:

```
$ORACLE_HOME/dbs/init<SID>.utl
```

- Ensure that the archived redo log files and their mirror log files reside on the same array as data.
- Run the following to perform Revert Restore of Database:

```
./brrestore -d util_file -m all -b last
```

- After a successful revert restore operation, you must also run the following command to restore control files:

```
./brrestore -d util_file -b last -m 0
```

- After the data and Cntrl File restore, perform recover as "recover database using backup controlfile until cancel" or recover using brrecover tool.
- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.

It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.

## PERFORM SAP ORACLE REVERT RESTORE USING COMMCELL CONSOLE

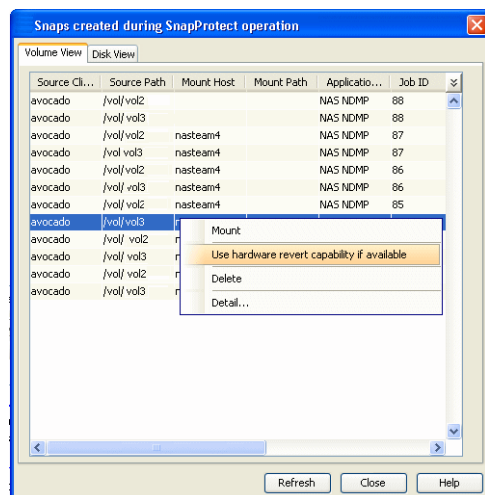
1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.

An application aware revert operation reverts back all the volumes included in the backup.

## PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers | <Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, *confirm*.
5. Click **OK**.

- A hardware specific revert operation reverts back the volume included in the snapshot.
- For NetApp NFS configurations:
  - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
  - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
  - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



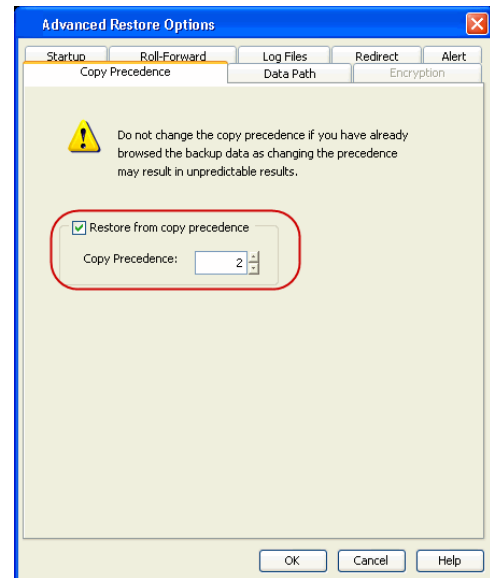
## SNAP RECONCILIATION

Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## SNAPPROTECT BACKUP USING SAP COMMAND LINE

In addition to CommCell Console, you can perform SnapProtect backups from the Command Line Interface using the `BRBACKUP` command.

```
brbackup -t offline/online -d util_file/rman_util/util_file_online -m full/incr
```

where the `BRBACKUP` command can backup control files and data files within one or more table spaces, and (if necessary) log files. `BRBACKUP` can backup all of these file types with the database either online or offline. Also, `BRBACKUP` saves the profiles and logs relevant to the backup.

### PARAMETER FILE

Before you run backups from the SAP command line, ensure that the appropriate parameter file containing information regarding the instance and the client is in place. Be sure to include at least the `CVInstanceName` parameter name followed by the name of the instance and also the `CVClientName` parameter name followed by the name of the client.

- For SAP for Oracle on Unix include this information in the `init.utl` file under the `$ORACLE_HOME/dbs` directory.
- For any SAP for Oracle version, if your backups and restores will be using the SAP utility files, be sure to modify the `init<SID>.utl` file by adding values for the following parameters. Note that some parameters are optional.
- `snapBackup`, which specifies that the SnapProtect backup is enabled. Default value is 0.
- `RestoreSnapToTape`, which specifies the source copy for restore. Default value is 0, which means that media will be used for restores.
- `RevertSnapVolume`, which specifies that the revert operation is enabled. Default value is 0, which means that revert is disabled.

It is recommended, that after reverting the data volumes, control file restores, log restores, and recovery you should reset the value of `RevertSnapVolume` to 0 to ensure that a revert operation is not unintentionally performed.

## NFS SNAPPROTECT FOR SAP FOR ORACLE

You can perform a SnapProtect backup for SAP for Oracle when the database is on a NFS Volume. However, you will require a root access in the storage device's NFS configuration to be able to read and write on the accessible SAP for Oracle files i.e., the host on which the NFS Volume is mounted.

File level revert is performed by default when revert restore is run on NFS volumes. For Volume Level revert on NFS volumes, use the `SUSE_FILE_LEVEL_REVERT` registry key. File level revert cannot be performed when the database resides on regular SAN Volumes (LUNs).

Consider the following while performing a SnapProtect backup for data or databases that reside on a NFS Volume:

- The export name on the storage device should be the same as the storage path on the storage device.

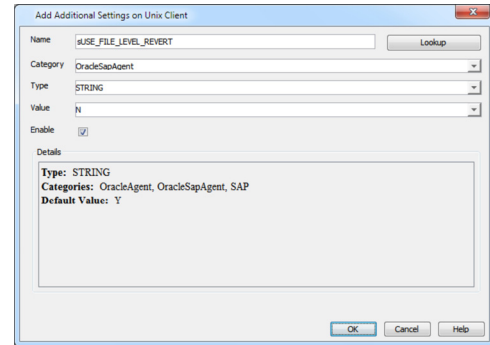
E.g., if the storage path of the storage device is `/vol/Volume/Qtrees`, use `/vol/Volume/Qtrees` as the export name and not an alias such as `/ExportName`.

- You can use the exports both at the root of a NetApp volume and at subdirectory levels below the root of the volume.
- Make sure that the storage device is accessible from the source and proxy machine (even if they exist in different domains) using the storage device's short name while mounting NFS exports from the storage device. Make sure to enter the storage device credentials using its short name. Do not use an IP address or the fully qualified domain name.

E.g., use a short name for the server such as `server1` or `server2`.

### ENABLING VOLUME LEVEL REVERTS ON NFS VOLUMES

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<Client>**, and then click **Properties**.
3. Click **Advanced** and then click **Additional Settings** tab.
4. Click **Add**.
5. In the **Name** field, type `sUSE_FILE_LEVEL_REVERT`.  
The **Category** and **Type** fields are populated automatically.
6. In the **Value** field, type `N`.
7. Click **OK**.



### SUPPORTED VOLUME MANAGERS

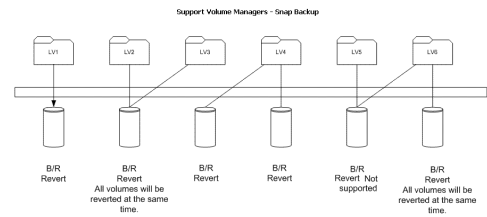
- Logical Volume Manager
  - All versions supported on AIX and Linux
  - Versions 1.0 and 2.x supported on HP-UX
- VERITAS Volume Manager (VxVM) 5.0 for AIX, Linux and Solaris
- Solaris ZFS Mirror
- Solaris Volume Manager

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.



### OPTIONS NOT APPLICABLE FOR SAP FOR ORACLE

The following options do not apply to SnapProtect backup for SAP for Oracle `iDataAgent`:

#### Backup Options dialog box

- Save as a Script

### ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                   | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                | RELATED TOPICS                                           |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <b>SCSI Reservation</b>  | SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key <code>nSCSIReserveForSnap</code> to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).<br><br>If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail. | For more information on registry keys, Registry keys     |
| <b>Pre/Post Commands</b> | The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog                                                                                                                                                                                                                                             | For more information on using the Pre/Post commands, see |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                     |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                      | <p>box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Pre/Post Processes. |
| <b>View Snapshot Details</b>         | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol> |                     |
| <b>Select a Job for Backup Copy</b>  | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                          |                     |
| <b>Disable a Job for Backup Copy</b> | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                      |                     |

[Back to Top](#)

# Advanced - DB2 SnapProtect Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Excluding the Online Log Volumes During SnapProtect Backup

### Restoring Database from a Point in Time

### Restoring Data from a Backup Copy

### NFS SnapProtect for DB2

### Supported Volume Managers

### Options not applicable for DB2

### Additional Options

## MANAGING SNAPSHOTS

The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete, or revert.

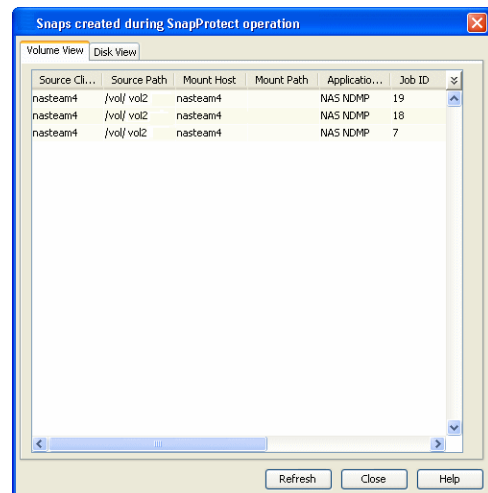
### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. `SP_2_79_1286222629`.

You can also browse snapshots at the instance level of the DB2 Agent.



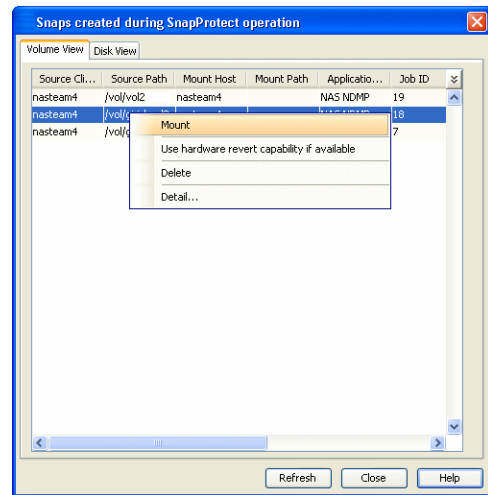
### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.



If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

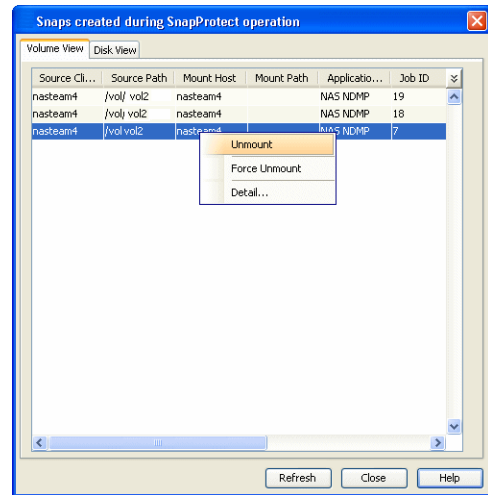


### UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



### DELETE SNAPSHOTS

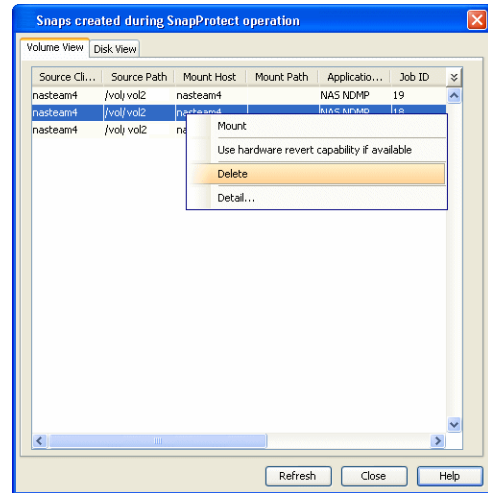
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

- `RevertSnapVolume` has been set to 1.
- Ensure that the archived redo log files and their mirror log files reside on the same array volume.
- After a revert or restore operation is completed successfully, you must also run the `./brrestore -d util_file -b last -m 0` job to restore control files.
- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.
- On Unix clusters, use pre/post scripts to freeze and unfreeze the cluster for revert operations. For example, on Red Hat Linux cluster, use the following command in the pre/post scripts:

```
clusvcadm -Z <group> to freeze the cluster
```

```
clusvcadm -U <group> to unfreeze the cluster
```

This is required because, during revert the application is shut down and corresponding volumes are unmounted. In that case, the cluster will automatically failover to another node thus preventing the revert operation.

- It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
- If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

## PERFORM AN APPLICATION AWARE REVERT

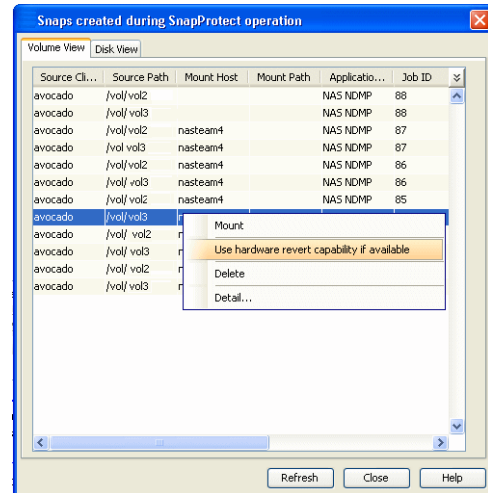
1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.

- An application aware revert operation reverts back all the volumes included in the backup.
- For NetApp NFS configurations:
  - This operation reverts all data on the file server volume, not just the data that is associated with the application.
  - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
  - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the

SnapVault/SnapMirror copy operation no longer works.

## PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers** | **<Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, `confirm`.
5. Click **OK**.
  - A hardware specific revert operation reverts back the volume included in the snapshot.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



## SNAP RECONCILIATION

Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

## EXCLUDING THE ONLINE LOG VOLUMES DURING SNAPPROTECT BACKUP

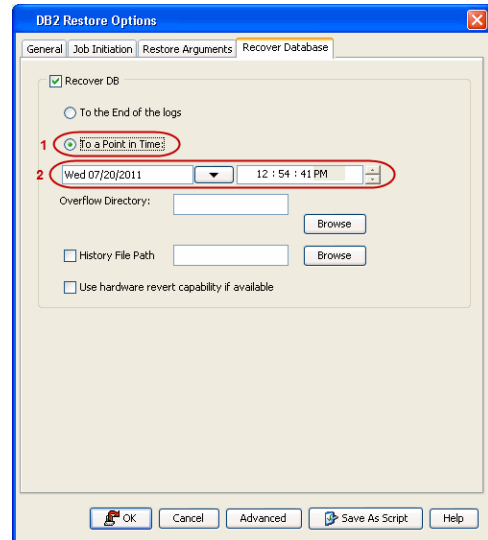
Use `sSKIPONLINELOGSNAP` registry key to exclude the online logs during the snap backup if the log volumes are separated from data volumes in DB2 database.

1. From the **CommCell Browser**, navigate to the **Client Computers**.
2. Right-click the **<Client>**, and then click Properties.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type `sSKIPONLINELOGSNAP`.
6. In the **Location** box, select or type DB2 Agent from the list.
7. In the **Type** box, select String as value.
8. In the **Value** box, type `y` or `Y` and then click **OK**.

## RESTORING DATABASE FROM A POINT IN TIME

You can restore a database from a point in time. This is useful if you want to restore certain configurations/contents in the database that are not reflected in the latest backup. For example, you can use this option to restore a SnapProtect backup if your latest backup was a traditional backup.

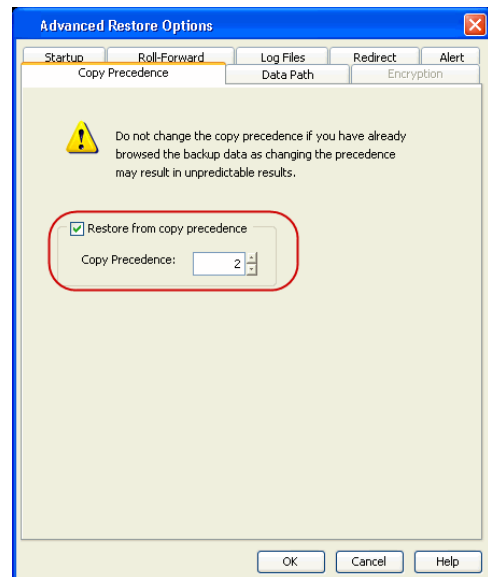
1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **DB2**.
2. Right-click the backup set and then click **All Tasks** | **Restore**.
3. Click the **Recover Database** tab.
4. Select **To a point in Time**.
5. Select the date and time of the backup you want to restore.
6. Click **OK**.



## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## NFS SNAPPROTECT FOR DB2

You can perform a SnapProtect backup for DB2 when the database is on a NFS Volume. However, you will require a root access in the storage device's NFS configuration to be able to read and write on the accessible DB2 files i.e., the host on which the NFS Volume is mounted.

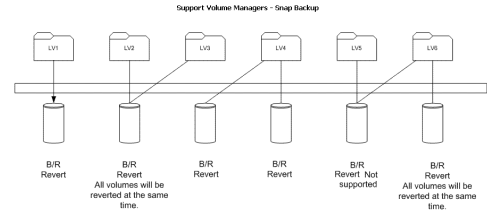
Consider the following while performing a SnapProtect backup for data or databases that reside on a NFS Volume:

- The export name on the storage device should be the same as the storage path on the storage device.  
E.g., if the storage path of the storage device is `/vol/Volume/Qtree`, use `/vol/Volume/Qtree` as the export name and not an alias such as `/ExportName`.
- You can use the exports both at the root of a NetApp volume and at subdirectory levels below the root of the volume.
- Make sure that the storage device is accessible from the source and proxy machine (even if they exist in different domains) using the storage device's short name while mounting NFS exports from the storage device. Make sure to enter the storage device credentials using its short name. Do not use an IP address or the fully qualified domain name.  
E.g., use a short name for the server such as `server1` or `server2`.

## 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.

**OPTIONS NOT APPLICABLE FOR DB2**

The following options do not apply to snap restore for the DB2 iDataAgent:

**DB2 Restore Options dialog box**

- General tab
  - Database Subset (for partial restore)
- Recover Database tab
  - History File Path

**DB2 Advanced Restore Options dialog box**

- Redirect tab
- Roll-Forward tab

**ADDITIONAL OPTIONS**

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                              | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | RELATED TOPICS                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>SCSI Reservation</b>             | SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key nSCSIReserveForSnap to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).<br><br>If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail.                                                                                                                                                                                                                                                                                                                                       | For more information on registry keys, Registry keys                         |
| <b>Pre/Post Commands</b>            | The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.<br><br>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.                                                                                                                                                                                                                                                                                                                  | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>        | You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.<br><br>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b> .<br><br>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.<br><br>3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties. |                                                                              |
| <b>Select a Job for Backup Copy</b> | You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                              |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
|                                             | <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                  |                                                     |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol> |                                                     |
| <b>Offline Snap Copy Job Summary Report</b> | Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.                                                                                                                                                                                                                                                                                                                                                                                                                                                | See Backup Copy Job Summary Report for more details |

[Back to Top](#)

# Advanced - Unix File System Agents SnapProtect™ Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Enabling Backups on Linux Clusters

### Reducing Snapshot Creation Time On Unix

### Restoring Data from a Backup Copy

### Data Aging for SnapProtect Snapshots

- Retention by Number of Jobs

### NFS SnapProtect for Unix

### Supported Volume Managers

### Additional Options

## MANAGING SNAPSHOTS

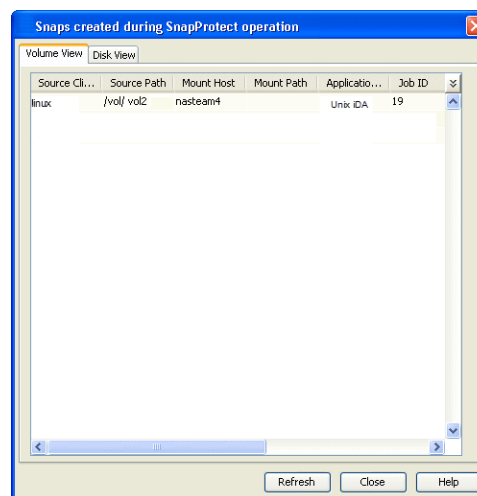
The snapshots of the data created by the SnapProtect backup are also available for various other operations like list, mount, unmount, delete, or revert.

### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.

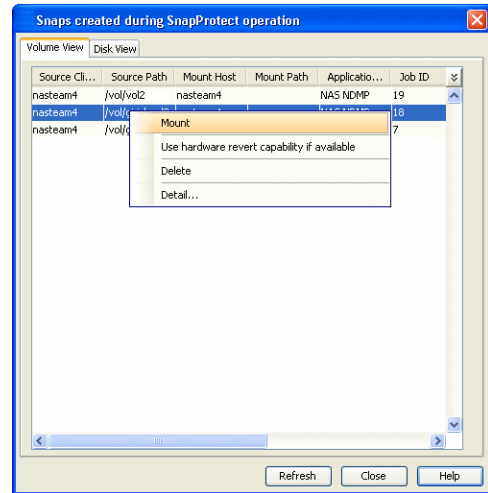


### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

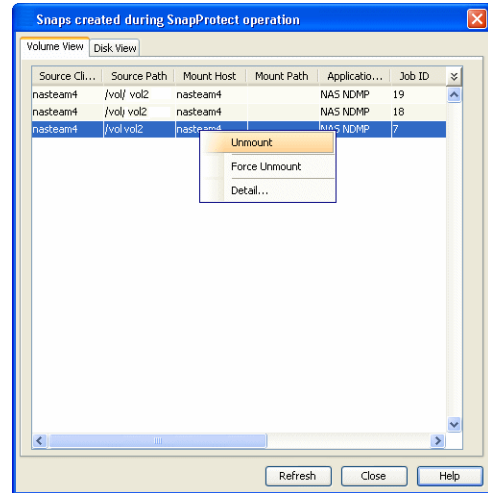


### UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



### DELETE SNAPSHOTS

Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

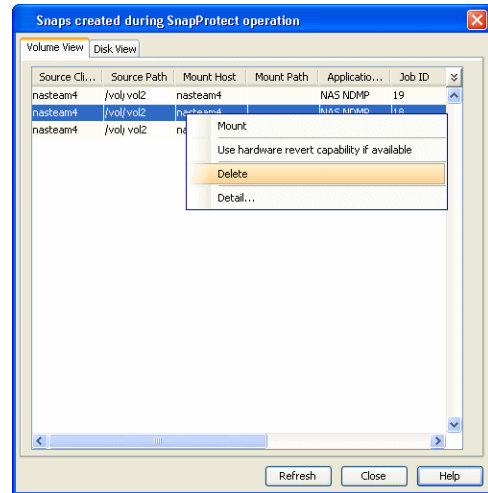
- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.





## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.
- Prior to performing a revert operation for ZFS LVM, consider the following:
  - The source Zpool should contain the same set of disks that were available during SnapProtect backup.
  - The entire Zpool will be reverted.
- Revert operation is not supported for mirrored volumes.
- Volumes to be reverted should not be monitored using DC. In case of LVM volumes, all the volumes in the volume group where the source volume resides should not be monitored using DC.
- On Unix clusters, use pre/post scripts to freeze and unfreeze the cluster for revert operations. For example, on Red Hat Linux cluster, use the following command in the pre/post scripts:

```
clusvcadm -z <group> to freeze the cluster
```

```
clusvcadm -U <group> to unfreeze the cluster
```

This is required because, during revert the application is shut down and corresponding volumes are unmounted. In that case, the cluster will automatically failover to another node thus preventing the revert operation.

- It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
- If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

## PERFORM AN APPLICATION AWARE REVERT

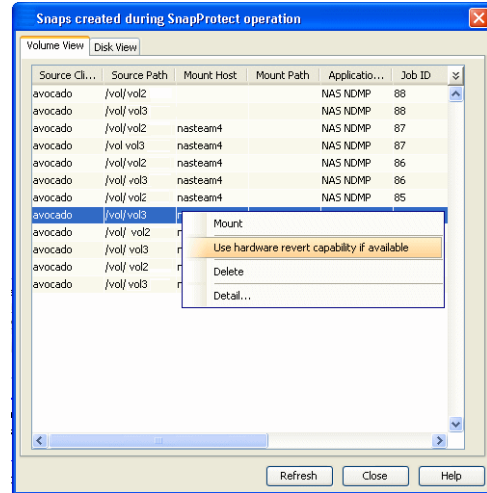
1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.

- An application aware revert operation reverts back all the volumes included in the backup.
- For NetApp NFS configurations:
  - This operation reverts all data on the file server volume, not just the data that is associated with the application.

- A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
- If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

**PERFORM A HARDWARE SPECIFIC REVERT**

1. From the CommCell Console, navigate to **Client Computers** | **<Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.
4. Enter the confirmation text string, `confirm`.
5. Click **OK**.
  - A hardware specific revert operation reverts back the volume included in the snapshot.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



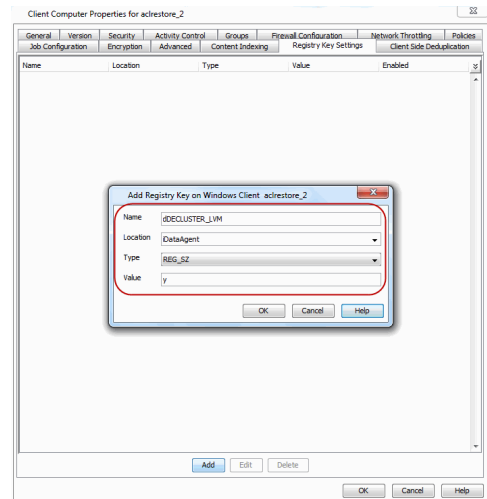
**SNAP RECONCILIATION**

Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

**ENABLING BACKUPS ON LINUX CLUSTERS**

Use the following steps to enable SnapProtect backups on Linux cluster nodes:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<Client>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type `nDECLUSTER_LVM`.
6. In the **Location** box, select or type `iDataAgent` from the list.
7. In the **Type** box, select **REG\_SZ**.
8. In the Value box, type **Y**, and then click **OK**.
9. Click **OK**.



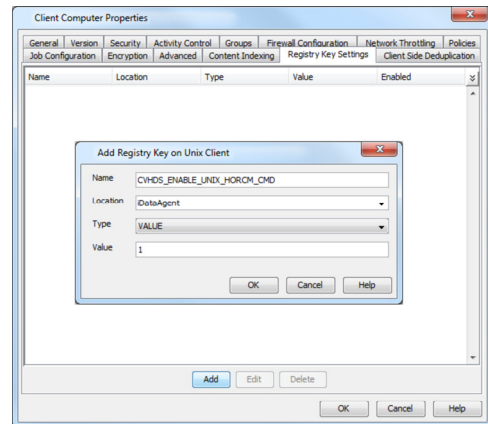
**REDUCING SNAPSHOT CREATION TIME ON UNIX**

The snapshot creation time on Unix platform can be reduced by enabling the `CVHDS_ENABLE_UNIX_HORCM_CMD` registry key which enables the usage of Command Control Interface instead of XML API.

Use the following steps to reduce the Snapshot creation time on Unix:

1. From the CommCell Browser, navigate to **Client Computers**.

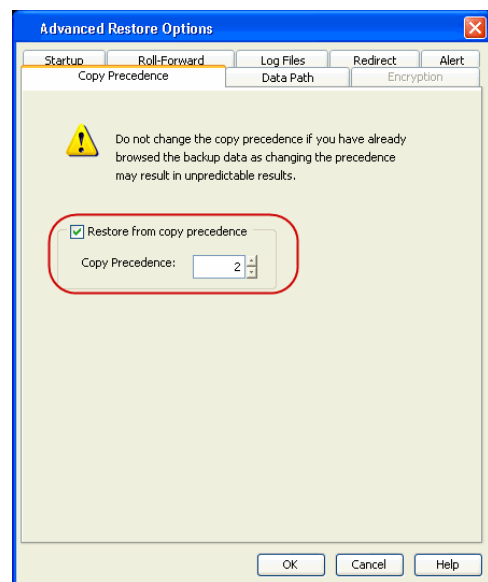
2. Right-click the **<Client>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type CVHDS\_ENABLE\_UNIX\_HORCM\_CMD.
6. In the **Location** box, select or type iDataAgent from the list.
7. In the **Type** box, select **Value**.
8. In the Value box, type **1**.
9. Click **OK**.



## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## DATA AGING FOR SNAPPROTECT SNAPSHOTS

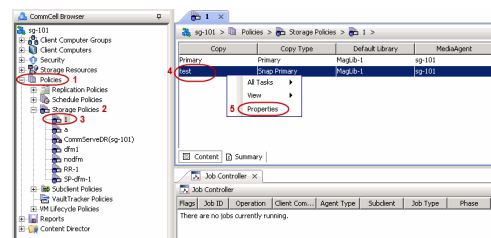
The following procedures describe the available retention configurations for snapshots. For movement to media retention, refer to Data Aging - Getting Started.

### RETENTION BY NUMBER OF JOBS

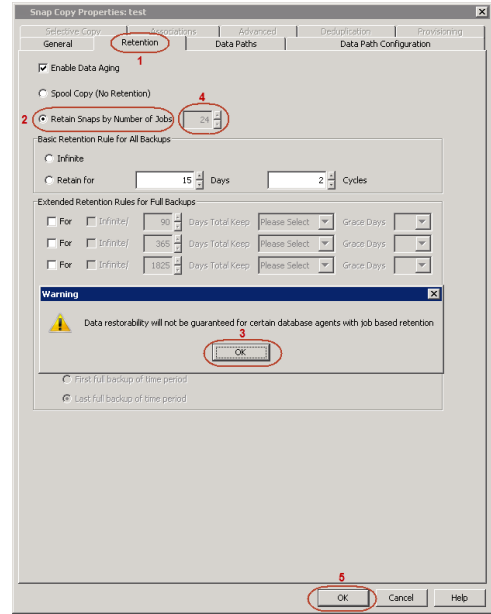
By default, snapshots are pruned based on the number of retention days and cycles specified in the storage policy. You can configure your snapshot copy to retain a defined number of SnapProtect backup jobs. When the total number of jobs goes above the specified retention number, the remaining jobs will be pruned. This configuration is recommended for File System and File System like Agents. This feature is supported for SnapProtect operations performed using the NetApp storage array.

The **NetApp Snap Management** license is required for retaining snaps by number of jobs.

1.
  - From the CommCell Console, navigate to **Policies | Storage Policies | <Storage Policy>**.
  - Right-click the primary snapshot copy and click **Properties**.
2.
  - Click the **Retention** tab.
  - Click **Retain Snaps by Number of Jobs**.
  - Click **OK** to the warning dialog box.



- Specify the number of jobs to be retained for the primary copy.
- Click **OK**.



## NFS SNAPPROTECT FOR UNIX

You can perform a SnapProtect backup for Unix when the database is on a NFS Volume. However, you will require a root access in the storage device's NFS configuration to be able to read and write on the accessible Unix files i.e., the host on which the NFS Volume is mounted.

Consider the following while performing a SnapProtect backup for data or databases that reside on a NFS Volume:

- The export name on the storage device should be the same as the storage path on the storage device.  
E.g., if the storage path of the storage device is `/vol/Volume/Qtree`, use `/vol/Volume/Qtree` as the export name and not an alias such as `/ExportName`.
- You can use the exports both at the root of a NetApp volume and at subdirectory levels below the root of the volume.
- Make sure that the storage device is accessible from the source and proxy machine (even if they exist in different domains) using the storage device's short name while mounting NFS exports from the storage device. Make sure to enter the storage device credentials using its short name. Do not use an IP address or the fully qualified domain name.  
E.g., use a short name for the server such as `server1` or `server2`.

## SUPPORTED VOLUME MANAGERS

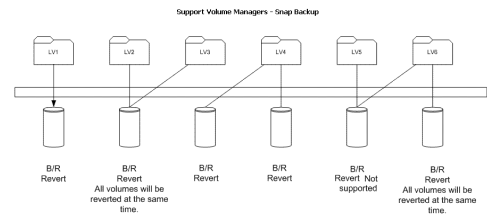
- Logical Volume Manager
  - All versions supported on AIX and Linux
  - Versions 1.0 and 2.x supported on HP-UX
- VERITAS Volume Manager (VxVM) 5.0 for AIX, Linux and Solaris
- Solaris ZFS Mirror
- Solaris Volume Manager

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.



## ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

|  |  |  |
|--|--|--|
|  |  |  |
|--|--|--|

| OPTION                                      | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | RELATED TOPICS                                                               |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>SCSI Reservation</b>                     | <p>SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key nSCSIReserveForSnap to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).</p> <p>If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail.</p>                                                                                                                                                                                                                                                                                                                                                                                     | For more information on registry keys, Registry keys                         |
| <b>Pre/Post Commands</b>                    | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                                                                                                                | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>                | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol> |                                                                              |
| <b>Select a Job for Backup Copy</b>         | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Pick for Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                          |                                                                              |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol>                                                                                                                                                                                                                                                      |                                                                              |
| <b>Offline Snap Copy Job Summary Report</b> | Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | See Backup Copy Job Summary Report for more details                          |

Back to Top

# Advanced - Windows File System SnapProtect™ Backup

## TABLE OF CONTENTS

### Managing Snapshots

- List Snapshots
- Mount Snapshots
- Delete Snapshots
- Revert a Snapshot
- Snap Reconciliation

### Restoring Data from a Backup Copy

### Data Aging for SnapProtect Snapshots

- Retention by Number of Jobs

### Additional Options

## MANAGING SNAPSHOTS

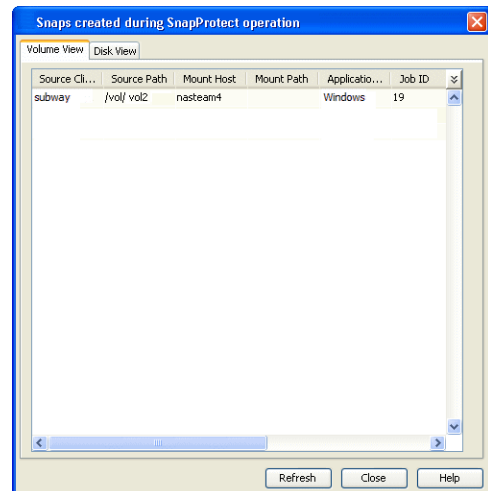
The following sections provide step-by-step instructions on all operations that can be performed on the snapshots created.

### LIST SNAPSHOTS

The browse operation provides the capability to see the snapshots created for an agent, job, or a snapshot copy. The list of the snapshots displayed is corresponding to the entity selected for the browse operation, for e.g., browsing the snapshots for an agent will display all the snapshots created for the selected agent. You can view volume or disk related information for the snapshots. Follow the steps given below to browse snapshots.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots created for the selected subclient. It also displays important information about each snapshot, including the source month path, snap mount path, the storage array, and the source client.

Click the **Disk View** tab to display the snapshot name, e.g. SP\_2\_79\_1286222629.

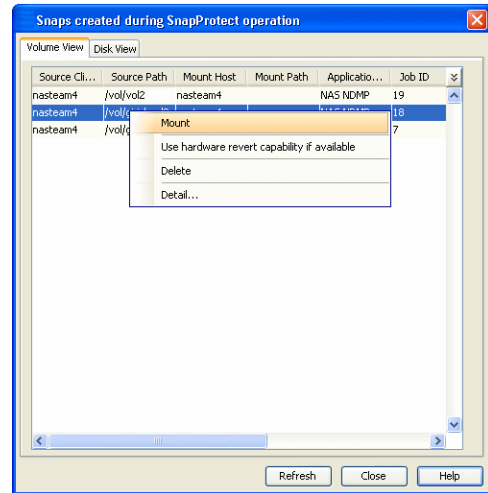


### MOUNT SNAPSHOTS

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

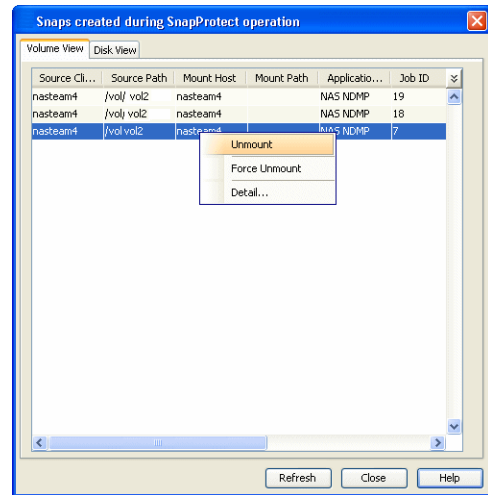


## UNMOUNT SNAPSHOTS

Follow the steps given below to unmount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to unmount and click **Unmount**.
4. Click **Yes** when prompted if you want to continue.

If the snapshot does not get unmounted, select the **Force Unmount** option to mark the snapshot as unmounted.



## DELETE SNAPSHOTS

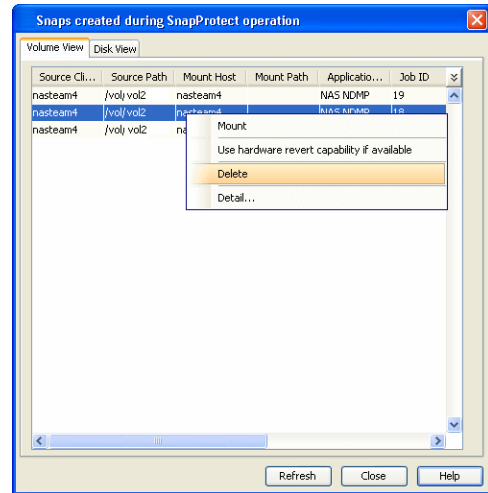
Snapshots can either be deleted using job-based pruning or from the list of displayed snapshots when browsing snapshots. Data Aging can also be used to define the retention rules and pruning of snapshots. Follow the steps given below to delete snapshots:

- Manual deletion of snapshots is not recommended. When a snapshot is deleted, it is no longer possible to perform data recovery operations from the snapshot copy. However, if a backup copy was created from the snapshot, data recovery operations can be performed from the backup copy.
- Ensure that the snapshot to be deleted is not mounted.

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **<Agent>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot you wish to delete.

Ensure all snapshots with the same **Job ID** are selected for a successful deletion operation.

4. Click **Delete**.
5. Enter the confirmation text string, `erase snapshots`.
6. Click **OK**.



## REVERT A SNAPSHOT

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is available if the storage arrays that you are using supports revert. Revert operations are supported on NetApp File Servers but not from SnapVault or SnapMirror snapshots. You can either perform an application aware revert or a hardware specific revert.

Review the following before performing a revert operation:

- Revert operations are not supported on Windows clustered disks.
- For Full System SnapProtect backup, the revert operation is not supported.
- When using HP EVA Clone or Data Replicator for SnapProtect backup, the revert operation is not supported.
- Revert operations are not supported when using Nimble storage array.
  - It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
  - If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

## PERFORM AN APPLICATION AWARE REVERT

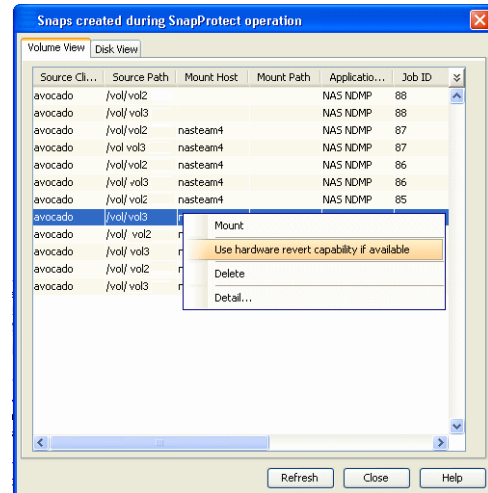
1. From the CommCell Browser, right-click the entity that contains the data you want to restore, and click **All Tasks | Browse Backup Data**.
2. From the **Browse Options** dialog box, click **OK**.
3. Select the data you want to revert and click **Recover All Selected**.
4. From the **Restore Options** dialog box, click **Advanced**.
5. Select the **Use hardware revert capability if available** option.
6. Click **OK** to confirm the revert operation.
7. Click **OK** from the **Advanced Restore Options** dialog box.
8. Click **OK** to start the revert.
  - An application aware revert operation reverts back all the volumes included in the backup.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the application.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.

## PERFORM A HARDWARE SPECIFIC REVERT

1. From the CommCell Console, navigate to **Client Computers | <Client>**.
2. Right-click the subclient and click **List Snaps**.
3. Right-click the snapshot that you wish to delete and click **Use hardware revert capability if available**.



4. Enter the confirmation text string, `confirm`.
5. Click **OK**.
  - A hardware specific revert operation reverts back the volume included in the snapshot.
  - For NetApp NFS configurations:
    - This operation reverts all data on the file server volume, not just the data that is associated with the snapshot.
    - A volume revert deletes all snapshots that were created after the snapshot to which you are reverting.
    - If you perform a volume revert on the source for a SnapVault/SnapMirror copy, and the snapshot to which you are reverting was created before the most recent snap moved to the SnapVault/SnapMirror copy, then the SnapVault/SnapMirror copy operation no longer works.



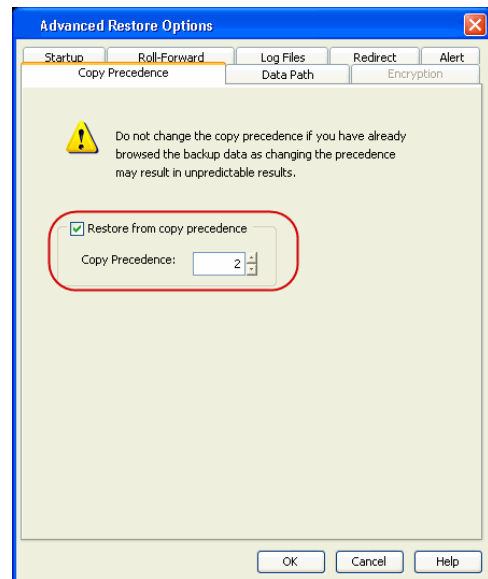
## SNAP RECONCILIATION

Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. You can use the `nRunSnapRecon` registry key to start snap reconciliation to check for missing snapshots once in every 24 hours and marks jobs corresponding to the missing snapshots as invalid.

## RESTORING DATA FROM A BACKUP COPY

You can perform a restore from the backup copy by setting the appropriate copy precedence number.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>**.
2. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse Backup Data**.
3. Click **OK**.
4. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.
5. From the **Restore Options for All Selected Items** window, click **Advanced**.
6. Click the **Copy Precedence** tab and select the **Restore from Copy Precedence** checkbox.
7. In the **Copy Precedence** box, type the copy precedence number for the backup copy.
8. Click **OK**.
9. Click **OK** to close the **Restore Options** window and start the restore job.



## DATA AGING FOR SNAPPROTECT SNAPSHOTS

The following procedures describe the available retention configurations for snapshots. For movement to media retention, refer to Data Aging - Getting Started.

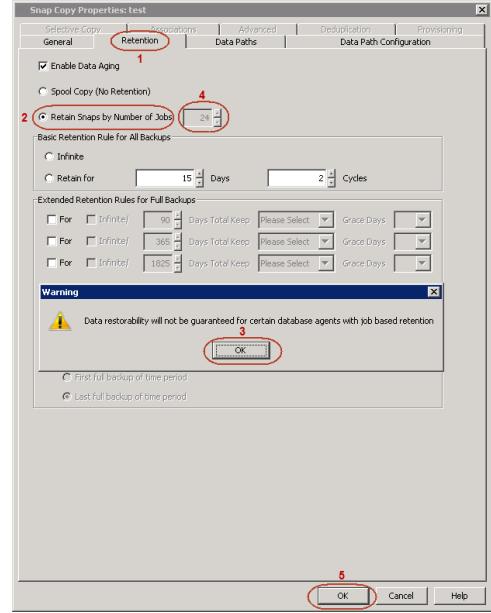
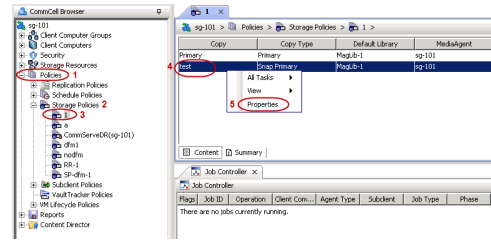
### RETENTION BY NUMBER OF JOBS

By default, snapshots are pruned based on the number of retention days and cycles specified in the storage policy. You can configure your snapshot copy to retain a defined number of SnapProtect backup jobs. When the total number of jobs goes above the specified retention number, the remaining jobs will be pruned. This configuration is recommended for File System and File System like Agents. This feature is supported for SnapProtect operations performed using the NetApp storage array.

The **NetApp Snap Management** license is required for retaining snaps by number of jobs.

1.
  - From the CommCell Console, navigate to **Policies | Storage Policies | <Storage Policy>**.
  - Right-click the primary snapshot copy and click **Properties**.

2.
  - Click the **Retention** tab.
  - Click **Retain Snaps by Number of Jobs**.
  - Click **OK** to the warning dialog box.
  - Specify the number of jobs to be retained for the primary copy.
  - Click **OK**.



## ADDITIONAL OPTIONS

Several additional options are available to further refine your backup operations. The following table describes the additional options:

| OPTION                              | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | RELATED TOPICS                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>SCSI Reservation</b>             | <p>SCSI reservation can be enabled for SnapProtect backup for all the agents. Use the registry key nSCSIReserveForSnap to enable SCSI reservation. Enabling SCSI Reservation prevents other applications (SCSI3 compliant) from using the reserved SCSI Device (i.e. the mounted snapshot).</p> <p>If this option is enabled and the hardware does not support this type of operation, subsequent data protection jobs may fail.</p>                                                                                                                                                                                                                                                                                                                                                                                     | For more information on registry keys, Registry keys                         |
| <b>Pre/Post Commands</b>            | <p>The Pre/Post commands for SnapProtect backup can either be executed on the proxy or the source computer. You can use the <b>Pre/Post Process</b> tab of the <b>Subclient Properties</b> dialog box to select where you wish to execute the Pre/Post commands. SnapProtect backup supports Pre/Post commands for the agents that support it.</p> <p>Use of Pre/Post Snap commands is not supported when using Data Replicator as the storage array.</p>                                                                                                                                                                                                                                                                                                                                                                | For more information on using the Pre/Post commands, see Pre/Post Processes. |
| <b>View Snapshot Details</b>        | <p>You can view the details of a snapshot for an agent, job, or a snapshot copy. When you right-click any of these entities, you will be able to browse all the snapshots corresponding to the selected entity.</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, right-click the entity that contains the snapshots you want to browse, and click <b>All Tasks   List Snaps</b>.</li> <li>2. The <b>Snaps created during SnapProtect operation</b> dialog box displays a list of all the snapshots created for the selected entity and displays important information about each snapshot, including the source mount path, snap mount path, the storage array, and the source client.</li> <li>3. Right-click the snapshot and click <b>Details</b> to view the snapshot properties.</li> </ol> |                                                                              |
| <b>Select a Job for Backup Copy</b> | <p>You can select a specific job for creating backup copy. Once selected, the Move Snap to Tape field for the specific job will be changed to Picked (i.e., the next backup copy operation will move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs, and then click <b>View Jobs</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                              |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
|                                             | 2. Right-click the job and then click <b>Pick for Backup Copy</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                     |
| <b>Disable a Job for Backup Copy</b>        | <p>You can prevent a job from being moved to media. You can apply this option to those jobs that were previously selected for moving to media. On selecting this option, the Move Snap to Tape field for the specific job will be changed to Not Picked (i.e., the next backup copy operation will not move this job to media).</p> <ol style="list-style-type: none"> <li>1. Right-click a storage policy containing SnapProtect backup jobs and then click <b>View Jobs</b>.</li> <li>2. Right-click the job and then click <b>Do not Backup Copy</b>.</li> </ol> |                                                     |
| <b>Offline Snap Copy Job Summary Report</b> | Offline Snap Copy Job Summary Report provides job summary details of backup copy jobs for moving snapshots to media.                                                                                                                                                                                                                                                                                                                                                                                                                                                | See Backup Copy Job Summary Report for more details |

[Back to Top](#)

# Advanced - 3PAR

## TROUBLESHOOTING

### SNAPPROTECT BACKUP OPERATIONS ARE FAILING

Review the following scenarios to troubleshoot snapshot failures:

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CIM Service is down on the 3PAR array</b>                          | <p>To verify if the service is up and running, try the following telnet command:</p> <pre>telnet &lt;3PAR Service IP&gt; 5988</pre> <p>If the telnet command gives you a time-out error, check the network connectivity between the 3PAR array and the client. However, if you get a connection-refused error, perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Perform an ssh connection with the array service IP: <pre>ssh &lt;3PAR Service IP&gt;</pre> </li> <li>2. Run the <code>showcim</code> command to check the service status. An example of the output you may get is shown below: <pre>-Service -State -SLP -SLPport -HTTPPort -HTTPS -HTTPSPort -PGVer -CIMVer Disabled Active Enabled Enabled 5988 Enabled 5989 2.9.1 3.1.1</pre> </li> <li>3. Run the following command to start the service: <pre>&lt;3PAR Array IP or Hostname&gt; cli% startcim</pre> <p>The CIM server will start in 90 seconds.</p> </li> </ol> |
| <b>Virtual volumes were created using the 3PAR Management Console</b> | <p>When creating a virtual volume using the 3PAR Management console, ensure that a Common Provisioning Group (CPG) is selected for copy space. This space will store copies of all changes to the user data since the last snapshot of the volume.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>A Thin Provision clone was created for a subclient</b>             | <p>If you created a Thin Provision clone for a subclient with Fully Provisioned physical disk, ensure that you specify a device group for the array to prevent the 3PAR clone from failing.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## FAQ

### CAN I SELECT THE OPTION TO PROTECT A SNAPSHOT DURING MOUNT?

No. The **Protect Snapshot during mount** option is not applicable for 3PAR snapshots. These snapshots are considered non-persistent because any modifications made to the snapshots cannot be saved during mount. However, for 3PAR clones, you can use this option to ensure that the changes made to the snapshot during mount are not retained when the snapshot is unmounted.

## BEST PRACTICES

- iSCSI Initiator must be configured on the client and proxy computers to access the storage array.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the `sSNAP_UseINITIATOR` registry key to the desired initiator address.

# Advanced - Dell Compellent

## TABLE OF CONTENTS

### Troubleshooting

### Best Practices

## TROUBLESHOOTING

### SNAPSHOT CREATION FAILS WITH DEVICE ERROR

If snapshot creation returns the following error, your Compellent array may not be properly defined in Array Management:

```
<device_name> is not a Compellent Device
```

Review the following workarounds to resolve this issue:

- Check the **User Name** specified for the array in Array Management. Remember that this field is case-sensitive.
- Ensure the IP of your Compellent array matches the Management IP Address. From the Management Console, right-click the **Storage Center** node and then click **Properties** to verify the Management IP.

### MEDIA AGENT CRASHES

Media agent crashes if the Simpana array list contains a Storage Center that is unreachable due to a network error.

Resolution

The CVSE was modified to handle the situation.

### CVSE PREVIOUSLY CREATED PERSISTENT SNAPSHOTS FOR ALL SNAPSHOT TYPES

CVSE previously created persistent snapshots for all snapshot types. These persistent snapshots were backed up by a view volume which consumes resources on the Storage Center.

Resolution

Now all snapshots are non-persistent.

### MANUALLY DELETING SNAPSHOTS FOR MULTIPLE VOLUMES RESULTS IN AN ERROR BEING DISPLAYED IN THE GUI

The error resulted when snaps were deleted that could not be found on the Storage Center.

Resolution

Deletion logic now returns success message if the snapshot cannot be found.

## BEST PRACTICES

- Use Boot from SAN volumes for supported server operating systems. However, it is recommended to avoid saving application data (such as Exchange or SQL Server data) on Boot from SAN volumes.
- SnapProtect backups should be performed on data volumes that are mapped to the server.
- Use Storage Center replication for supported server operating systems.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the sSNAP\_UseINITIATOR registry key to the desired initiator address.

### BACKING UP VMWARE ESXI 5.0 ENVIRONMENTS

- Datastores should be created on non-Boot from SAN volumes.
- It is recommended to create a single subclient for each VMware datastore as Calypso processes each subclient as its own job. This will allow jobs to run in parallel when backing up many subclients, providing higher performance.
- The proxy server must be connected to the Storage Center where the VMware datastore volumes reside. A corresponding server object must also exist in the Storage Center for the proxy server.
- You can increase the speed of proxy mounting by having a low number of LUNs connected to the ESX proxy server.
- It is recommended to spread virtual machines over multiple datastores to improve backup performance. For heavily used virtual machines, ensure there are fewer virtual machines per datastore.

---

## **BACKING UP SQL SERVERS**

To perform a SnapProtect backup of SQL virtual instances running ESX(i), it is recommended that:

- Dell Compellent volumes are present in the virtual machine as physical Raw Device Mappings (RDMs) from the ESX(i) host.
- SQL databases are installed on Dell Compellent volumes.

---

## **BACKING UP EXCHANGE SERVERS**

To perform a SnapProtect backup of Exchange virtual instances running ESX(i), it is recommended that:

- Dell Compellent volumes are present in the virtual machine as physical Raw Device Mappings (RDMs) from the ESX(i) host.
- Exchange databases are installed on Dell Compellent volumes.

---

## **BACKING UP A WINDOWS FILE SYSTEM**

When performing SnapProtect backups of file system data, you must use the Microsoft Volume Shadow Copy Service (VSS) or the operation will fail.

# Advanced - Dell EqualLogic

## TROUBLESHOOTING

---

### THE RESERVED SNAPSHOT VOLUME IS FULL AND THE OLDER SNAPSHOTS ARE GETTING DELETED

The Snapshot space recovery policy on the Dell EqualLogic array is by default set to delete the older snapshots when the reserved snapshot volume is out of disk space. You can change this option and select to set the volume and its snapshots offline when the reserved snapshot volume exceeds the allotted disk space.

## FAQ

---

### SHOULD I SELECT THE OPTION TO PROTECT A SNAPSHOT DURING MOUNT?

Yes, you should use the **Protect Snapshot during mount** option to ensure that the changes made to the snapshot during mount are not retained when the snapshot is unmounted. By default, the changes made to the mounted snapshots are retained when the snapshot is unmounted.

## BEST PRACTICES

- Ensure that enough disk space is available for snapshot operations and the disk space used by snapshots is monitored. The space requirement for snapshots created during SnapProtect backup can vary based on your environment. The space utilization is dependent on the number of snapshots created and the retention period defined for the snapshots.
- If you have SELinux enabled on the client computer, run the following commands as a root user before performing any snap operations:
  - `chcon -t texrel_shlib_t /opt/<software installation directory>/Base/libManageEquallogic.so`
  - `chcon -t texrel_shlib_t /opt/<software installation directory>/Base/libpsapi.so.4`
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the sSNAP\_UseINITIATOR registry key to the desired initiator address.

# Advanced - EMC Clariion, VNX

## TABLE OF CONTENTS

Troubleshooting

FAQ

Best Practices

## TROUBLESHOOTING

### SNAPSHOTS ARE NOT BEING CREATED

It is recommended that multiple SnapProtect backups using the same host must be run one after the other. Multiple SnapProtect backups running at the same time may cause the snapshot creation to fail due to the database lock.

### UNABLE TO PERFORM CLONING OPERATION

For clone operations, ensure that Clone Private LUN (CPL) is created for each storage processor prior to performing the snapshot operations.

### CLARIION DISCOVERY COMMAND FAILS WITH ERROR

The `symcfg discover -clariion` command fails with the following error:

```
Invalid certificate encountered - End-of-chain encountered without finding a trusted certificate
```

The discovery command fails because there is no LUN coming from the Clariion array to the proxy computer. To solve this issue, consider the following scenario:

If you have two storage arrays (Clariion 1 and Clariion 2) and a proxy computer, where the proxy has access to the LUN in Clariion 2 and your source LUN comes from Clariion 1. Clariion 1 does not have any LUN on the proxy. For the discovery operation to be successful, you must add a LUN to Clariion 1 and mount it to the proxy computer to allow connectivity. It is recommended to perform this workaround instead of using the Clariion discovery command.

## FAQ

### WHAT SHOULD BE THE SIZE OF FREE LUN?

Free LUN should be of the same size as the clone source and this LUN should not be a part of any storage group.

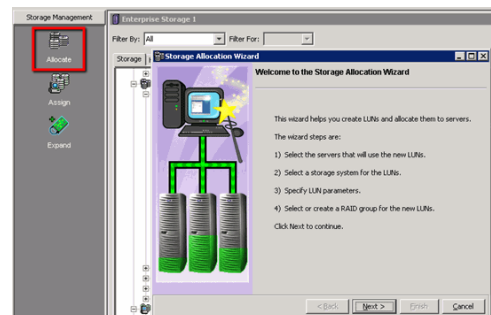
### HOW TO ASSIGN A NEW LUN TO A SPECIFIC HOST?

Before you proceed to assign a new LUN, ensure the following:

- Proper hardware zoning has been completed for the Hot Bus Adaptors (HBAs) of the server to provide visibility to a storage processor.
- The NaviAgent is installed to allow connectivity to the Navisphere Server.

Follow the steps below:

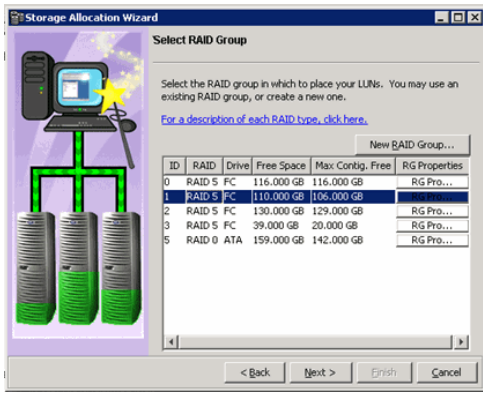
1. Allocate a new LUN.



2. Select the Clariion system and host to be configured. You can either create a new RAID Group or use an existing one.

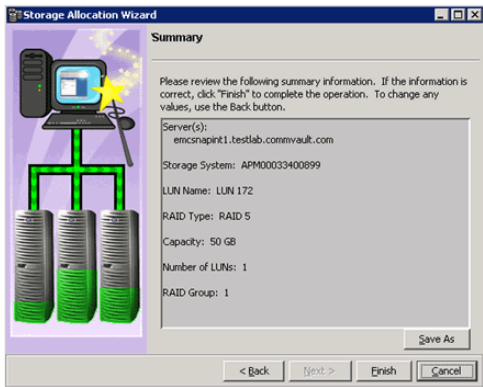
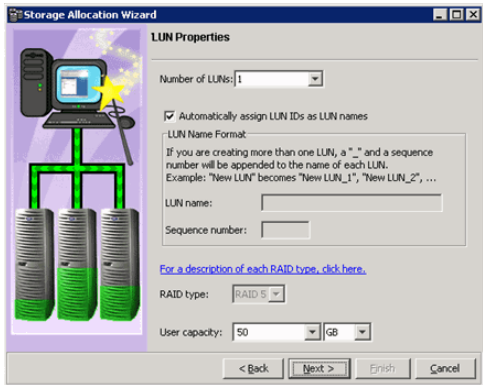


3. Select a specific LUN parameter. You can also use the option for automatic configuration of the LUN ID to the host.



4. Verify your selections and click **Finish**.

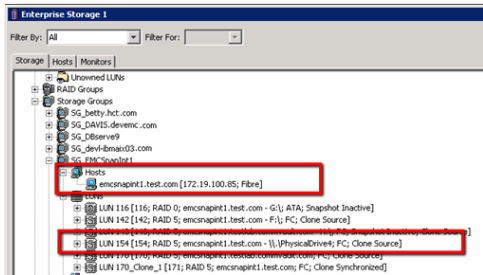
Check that the specified LUN has been created under the correct Storage Group for the host.

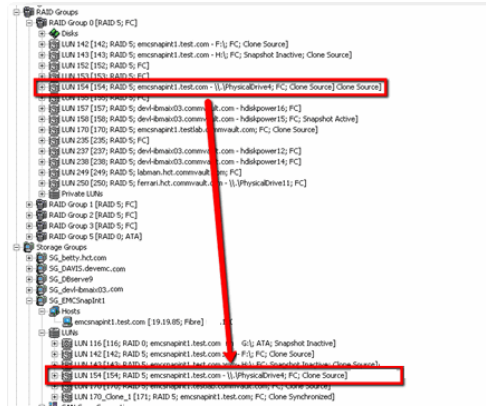


## HOW TO VERIFY THAT A LUN IS MAPPED TO A HOST THAT REQUIRES PROTECTION ?

To check if the LUN is already assigned to the server, check the following under Navisphere:

1. The LUN that was created based on the RAID Group must be present to the Host through Access Logix Storage Groups.
2. From the Clariion Storage Group configuration, you should be able to see the LUN. For example, LUN 154 is based on RAID Group-0, which has RAID-5 configuration.





## HOW DOES SNAPPROTect WORK WITH SNAPVIEW/CLONE?

Calypso always runs a synchronization process to Clone target columns. The example on the right shows where the Clone SnapProtect job ran from Job ID #2748 from Navisphere. The example on the right also shows that the Clone is:

- Consistent: Synchronization was completed.
- Fractured: Clone is available to be mounted to the host (production or proxy computer).

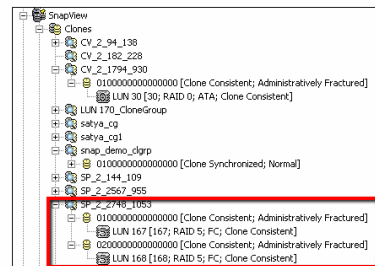
Calypso uses the following naming convention for the SnapProtect jobs:

SP\_<commcell id as per the CSDB>\_<Job\_ID>\_XXX

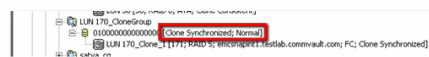
When a SnapProtect job is running, you will notice that a synchronization is required for SnapView/Clone before the Clone can be fractured as shown in the example.

You must have enough space on the Clone target RAID group or enough Clone Private LUN for SnapProtect operations to run successfully.

Consistent Clones:



Synchronized Clones:



## HOW DOES SNAPPROTect WORK WITH SNAPVIEW/SNAP?

Unlike Clones, SnapView/Snap does not need synchronization as it will copy any blocks that have been modified based on the Copy-On-Write model. Once a snapshot has been taken, you can see in Navisphere that a new snapshot was created as shown in the example on the right.

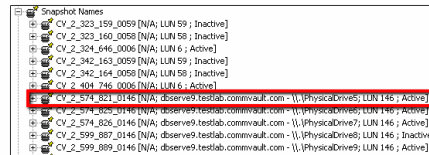
Calypso uses the following naming convention for the SnapProtect jobs:

SP\_<commcell id as per the CSDB>\_<Job\_ID>\_XXX\_<Original LUN ID>

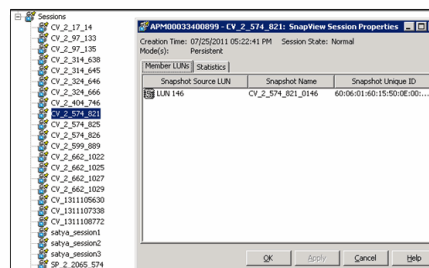
You will also notice that a Sessions that starts when the snapshot is created as seen in the image. Sessions are created based on the snapshot to allow:

- Tracking on which snapshot the session is present and on which reserved or source volume.
- Tracking of blocks that have been modified.

New snapshot:



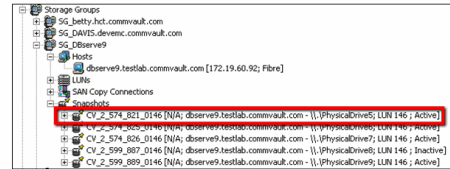
SnapView Session:



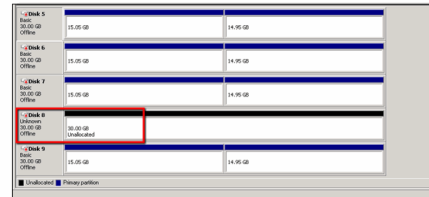
Once a snapshot has been activated to the host computer, it is available for the host that is specified with the Storage Group as shown in the example on the right.

Also, once the snapshots have been defined, they will remain inactive until they are activated again to run the SnapView session.

**Active snapshot:**



**Inactive snapshot:**



## BEST PRACTICES

- Ensure that the client and proxy computers are configured and have access to the array.
- Ensure that sufficient number of Save Area devices are configured to meet your retention requirements.
- Ensure that enough disk space is available for snapshot operations and the disk space used by snapshots is monitored. The space requirement for snapshots created during SnapProtect backup can vary based on your environment. The space utilization is dependent on the number of snapshots created and the retention period defined for the snapshots.
- For any EMC Clariion operations to work, the SYMAPI\_HOME\_DIR registry key must be set to the directory where the Symmetrix SYMAPI library is located.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the sSNAP\_UseINITIATOR registry key to the desired initiator address.

# Advanced - EMC Symmetrix

## TABLE OF CONTENTS

BCV Devices Requirement

Troubleshooting

FAQ

Best Practices

## BCV DEVICES REQUIREMENT

Use the following matrix to calculate the number of target devices required for performing SnapProtect operations.

| AGENT                                                      | TARGET DEVICE REQUIREMENTS (BUSINESS CONTINUANCE VOLUMES/ SHADOW IMAGE VOLUMES)                                                                                                                                                         |                                                          | NOTES                                                                              |                                                                                                                                                                                                    |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | FULL BACKUP                                                                                                                                                                                                                             | INCREMENTAL BACKUP                                       |                                                                                    | DIFFERENTIAL BACKUP                                                                                                                                                                                |
| <b>DB2</b>                                                 | [Number of devices where data resides] + [Number of devices where the online log resides] + [Number of devices where the 'LOCAL_DB_DIRECTORY' resides] + [Number of devices where the 'DBPATH' resides]                                 | N/A                                                      | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Exchange Database</b>                                   | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      | [Number of devices where the log resides]                | [Number of devices where the log resides]                                          | For example, if your data resides on 2 devices, logs reside on 1 devices. Full backup will require 3(2+1) target devices, Incremental/Differential backup will require 1 target devices.           |
| <b>Microsoft SQL Server</b>                                | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      |                                                          | [Number of devices where data resides] + [Number of devices where the log resides] | For example, if your file system data resides on 3 devices you will require 3 target devices.<br>SQL log backup does not require any target device.                                                |
| <b>Microsoft Windows File System</b>                       | Number of devices on which the file system data resides                                                                                                                                                                                 | Number of devices on which the file system data resides  | Number of devices on which the file system data resides                            |                                                                                                                                                                                                    |
| <b>NAS NDMP</b>                                            | Number of devices on which the file system data resides                                                                                                                                                                                 |                                                          |                                                                                    |                                                                                                                                                                                                    |
| <b>Oracle</b>                                              | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      |                                                          | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Oracle – Data and logs residing on the same devices</b> | 2x[Number of devices where data and logs reside]                                                                                                                                                                                        |                                                          | N/A                                                                                | For example, if your data and logs reside on 3 devices, you will require 6 target devices.                                                                                                         |
| <b>Applications running on JFS</b>                         | [Number of devices where application data resides] + [Number of devices where JFS logs reside] + [No. of devices on which logs reside]                                                                                                  |                                                          | N/A                                                                                | For example, if your application data resides on 2 devices, logs reside on 1 devices, data and logs share one device, and JFS logs reside on 1 device, you will require 6 (2+1+2+1) target devices |
| <b>SAP for Oracle - Data and logs</b>                      | [Number of devices where data resides] + [Device where the 'sapbackup' directory resides] + [Number of devices where the log resides] + [Device where the 'saparch' directory resides] + 2 x [Device where the 'dbs' directory resides] | N/A                                                      | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Unix File System</b>                                    | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      |                                                          |                                                                                    |                                                                                                                                                                                                    |
| <b>Unix File System on JFS</b>                             | [Number of devices on which the file system data resides ] + [No. of devices on which file system logs reside]                                                                                                                          |                                                          |                                                                                    | For example, if your file system data resides on 2 devices and file system log resides on 1 device, you will require 3 target devices.                                                             |
| <b>VMware</b>                                              | Number of luns on which the datastore for the VM resides                                                                                                                                                                                | Number of luns on which the datastore for the VM resides | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Microsoft Hyper-V</b>                                   | Number of luns on which vhd and configuration files of VM reside                                                                                                                                                                        | Number of luns on which vhd and                          | N/A                                                                                |                                                                                                                                                                                                    |

|                                  |
|----------------------------------|
| configuration files of VM reside |
|----------------------------------|

## TROUBLESHOOTING

### SNAPSHOTS ARE NOT BEING CREATED

It is recommended that multiple SnapProtect backups using the same host must be run one after the other. Multiple SnapProtect backups running at the same time may cause the snapshot creation to fail due to the database lock.

### SNAPPROTECT BACKUP FAILED

SnapProtect backup may fail when EMC Solutions Enabler software does not clean the SYMAPI database locks during abnormal termination of any process using SYMAPI. Additionally, this also causes the subsequent snapshot operations to hang indefinitely. As a workaround for this issue, reset the SYMAPI database locks using the EMC utilities or any other procedures provided by EMC.

### DEVICE DISCOVERY FAILED WITH ERROR 7143

If you run the `symcfg discover` command the Symmetrix CLI and completes with the following error in the MediaAgent log file, then the Symmetrix database was not successfully loaded:

```
C:\SYMAPI::Discover() - SYMAPI - SymDiscover() failed with error (7143)
```

In the Symmetrix logs, you will also find the following error message:

```
Gatekeeper for the Symmetrix (Symm ArrayID) cannot be opened by the base daemon
```

As a workaround, ensure the Symmetrix gatekeeper is assigned from the array specified in the above error message. If the gatekeeper is assigned to the correct array ID, then set the MPIO policy as `FALLOVER` in the MPIO properties of the gatekeeper devices.

If you have multiple Symmetrix arrays, then a gatekeeper should be assigned for each array.

## FAQ

### HOW MANY LUNS CAN BE ASSIGNED TO A SINGLE PORT?

Ensure that there are not be more than 255 LUNs assigned to any single port, especially for Windows.

### WHAT ARE DEVICE GROUPS?

Device Groups are a technique for grouping specific BCV and VDEV devices for clone or snapshot use. An example of Device Groups with a single BCV is shown on the right.

Device groups that are local to every client should have the following configuration:

- The Device Group name must be the same for every client as during the array configuration you cannot specify more than one Device Group.
- The source LUN and the BCV/VDEV devices must be part of the same Device Group.

```
C:\> symdg show test
Group Name: test
Group Type : REGULAR
Valid : Yes
SymmetrixID : 000187980546
Group Creation Time : Thu May 19 23:48:22 2011
VendorID : CommVault
ApplicationID : Galaxy_Ent_2000

Number of STD Devices in Group : 1
Number of Locally-associated BCV's : 1
Standard(STD) Devices (1):

LdevName PdevName Sym Cap Dev Alt Sts (MB)

DEV001 \\PHYSICALDRIVE22 006C RW 14400

BCV Devices Locally-associated (1):

LdevName PdevName Sym Cap Dev Alt Sts (MB)

SP_2_453_292 \\PHYSICALDRIVE23 008B RW 14400
```

### CAN I USE MULTIPLE DEVICE GROUPS?

When you configure an array using the CommCell Console, the Calypso software allows you to use one Device Group name. You can use multiple device groups by enabling the `nDisableUseOfDG` or `nDisableDGChange` registry key. Based on your environment, use the following configuration scenarios to use multiple device groups:

When using the registry keys, source and target devices will not be moved from the groups where they reside. Also, no new device groups will be created.

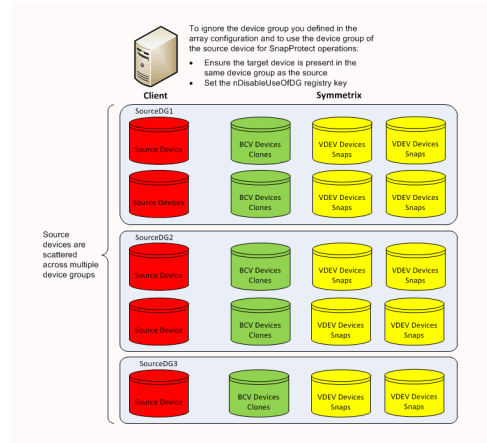
#### CONFIGURATION 1: USE THE DEVICE GROUP OF THE SOURCE DEVICE

Enable the `nDisableDGChange` registry key to ignore the device group you defined in the CommCell Console and to use the device group of the source device for SnapProtect operations. Before using this key, ensure the target device is present in the same device

group as the source device.

This key is useful in the following scenarios:

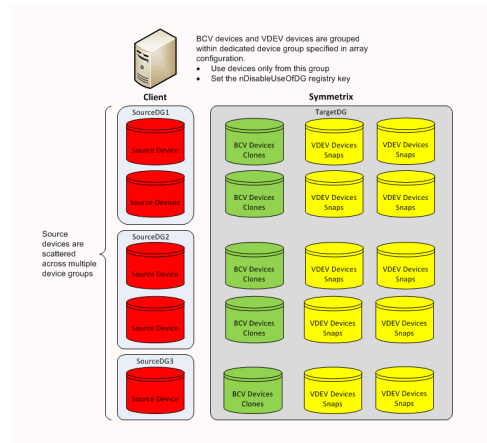
- You have device groups named differently on each client computer.
- You have multiple device groups on the client computer. Each device group has source-target device pairs.



### CONFIGURATION 2: USE TARGET DEVICE FROM DIFFERENT DEVICE GROUP

Enable the nDisableUseOfDG registry key to use a target device from a different device group other than the source device group. The name of the devices group containing the target devices should be specified in Array Management.

This key is useful when you have all target devices in one device group and the source devices are scattered across multiple device groups.



### HOW DOES THE BCV DEVICE SELECTION HAPPEN?

Calypso requires BCV and VDEV devices of the same block size to be created before performing SnapProtect operations. The BCV device selection occurs based on the following precedence:

- Currently established BCVs
- Masked BCV's to a proxy or source that are currently established
- Split source BCVs
- Split source BCVs masked to a proxy or source
- Non-established BCVs

### HOW TO VERIFY THAT A LUN IS MAPPED TO A HOST THAT REQUIRES PROTECTION?

To check if the LUN is already assigned to the server, run the following command on the server:

```
C:\> symdev -sid <symm_ID>
```

The physical device name may be displayed as "Not Visible" even if everything has been configured correctly (see image on the right). This may happen if you have multiple hosts that are doing the device management or if the SYMAPI DB has not been refreshed. You can try the following:

- Check the Device Manager and Kernel Messages to ensure the disk is visible.
- Refresh the SYMAPI DB using the following command:

```
C:\> symcfg discover
```

If you still do not see the device properly, then you may need to configure/map the LUNs to the Host Adapter to make it visible to the Production Host.

```
C:\> symdg show test
```

```
Group Name: test
Group Type : REGULAR
Valid : Yes
Symmetrix ID : 000187880546
Group Creation Time : Thu May 19 23:48:22 2011
Vendor ID : CommVault
Application ID : Galaxy_Ent_2000

Number of STD Devices in Group : 1
Number of Locally-associated BCVs : 1
Standard (STD) Devices (1):

LdevName PdevName Sym Cap Dev Att. Sts (MB)

DEV001 \\PHYSICALDRIVE22 006C RW 14400

BCV Devices Locally-associated (1):

LdevName PdevName Sym Cap Dev Att. Sts (MB)

SP_2_453_292 \\PHYSICALDRIVE23 008B RW 14400
```

### HOW TO ASSIGN A NEW LUN TO A FIBER CHANNEL DIRECTOR?

Before you proceed to assign a new LUN, ensure that proper hardware zoning has been completed for the Hot Bus Adaptors (HBAs) of the server to provide visibility to a Host Adapter.

The following example assumes that you are zoning the required HBA with Fiber Channel Director 10a / Port 1. Use the steps below to assign Symmetrix VOL 94 to LUN 0x31 - 49 (decimal) on FA-10a/Port 1:

1. Check if the device is unassigned or if it shows as "Not Visible":

```
C:\> symdev -sid 0546 list
```

```
C:\> symdev -sid 0546 list
Symmetrix ID: 000187880546

Device Name Directors Device

Sym Physical SA :P DA :IT Config Cap Attribute Sts (MB)

0094 Not Visible ????:? 06C:D2 2-Way Mir Grp'd RW 2048
```

2. Create a text file (e.g., test.txt) with the following content:

```
map dev 0094 to dir 10A:1 lun=31
```

3. Verify that the format of the text file has the correct syntax:

```
C:\> symconfigure -sid 0546 -f test.txt preview
```

```
C:\> symconfigure -sid 0546 -f test.txt preview
Execute a symconfigure operation for symmetrix '000187880546' (y/n)? y
A Configuration Change operation is in progress. Please wait...
Establishing a configuration change session..... Established.
Processing symmetrix 000187880546
Performing Access checks..... Allowed.
Checking Device Reservations..... Allowed.
Submitting configuration changes..... Submitted
Locking devices..... Locked.
Validating configuration changes..... Validated.
Closing configuration change request..... Closed.
Terminating the configuration change session..... Done.
The configuration change session has completed successfully.
```

4. Prepare Symmetrix for the configuration change. Check if there any locks (usually not for LUN mappings) to avoid making multiple configuration changes at the same time:

```
C:\> symconfigure -sid 0546 -f test.txt prepare
```

```
C:\> symconfigure -sid 0546 -f test.txt prepare
Execute a symconfigure operation for symmetrix '000187880546' (y/n)? y
A Configuration Change operation is in progress. Please wait...
Establishing a configuration change session..... Established.
Processing symmetrix 000187880546
Performing Access checks..... Allowed.
Checking Device Reservations..... Allowed.
Submitting configuration changes..... Submitted
Locking devices..... Locked.
Validating configuration changes..... Validated.
Initiating PREPARE of configuration changes..... Queued.
PREPARE requesting required resources..... Obtained.
Step 004 of 017 steps..... Executing.
Step 009 of 017 steps..... Executing.
Step 013 of 017 steps..... Executing.
Step 014 of 017 steps..... Executing.
Step 016 of 017 steps..... Executing.
Local: PREPARE..... Done.
Closing configuration change request..... Closed.
Terminating the configuration change session..... Done.
The configuration change session has completed successfully.
```

5. Commit the configuration changes:

```
C:\> symconfigure -sid 0546 -f test.txt commit
```

During the configuration change, a script runs on Symmetrix to load the new Configuration Files (IMPL) and allow device #0094 to be mapped to FA-10a / Port 1.

```
C:\> symconfigure -sid 0546 -f test.txt commit
Execute a symconfigure operation for symmetrix '000187880546' (y/n)? y
A Configuration Change operation is in progress. Please wait...
Establishing a configuration change session..... Established.
Processing symmetrix 000187880546
Performing Access checks..... Allowed.
Checking Device Reservations..... Allowed.
Submitting configuration changes..... Submitted
Locking devices..... Locked.
Validating configuration changes..... Validated.
Initiating PREPARE of configuration changes..... Queued.
PREPARE requesting required resources..... Obtained.
Step 004 of 017 steps..... Executing.
Step 011 of 017 steps..... Executing.
Step 013 of 017 steps..... Executing.
Step 015 of 017 steps..... Executing.
Local: PREPARE..... Done.
Initiating COMMIT of configuration changes..... Queued.
COMMIT requesting required resources..... Obtained.
Step 003 of 079 steps..... Executing.
Step 046 of 079 steps..... Executing.
Step 061 of 116 steps..... Executing.
Step 108 of 116 steps..... Executing.
Step 112 of 116 steps..... Executing.
Local: COMMIT..... Done.
Terminating the configuration change session..... Done.
```

6. Confirm that device #0094 has been mapped to Host Adapter FA-10a / Port 1 as LUN 0x31 (49):

```
C:\> symdev -sid 000187880546 list
```

```
C:\> symdev -sid 000187880546 list
Symmetrix ID: 000187880546

Device Name Directors Device

Sym Physical SA :P DA :IT Config Cap Attribute Sts (MB)

0094 Not Visible 10A:1 06C:D2 2-Way Mir Grp'd RW 2048
```

```
C:\> symdev -sid 0546 list -SA 10A -p 1
Symmetrix ID: 000187880546

Device Name Directors Device

Sym Physical SA :P DA :IT Config Cap Attribute Sts (MB)

0000 \\\PHYSICALDRIVE20 10A:1 01C:C2 2-Way Mir N/Grp'd VCM WD 23
0094 Not Visible 10A:1 06C:D2 2-Way Mir Grp'd RW 2048
```

7. Make LUN mask device #0094 visible to HBA and assign it to WWN 21:00:00:E0:8B:07:A0:BC:

```
C:\> symmask -sid 0546 -wwn 210000E08B07A0BC -dir 10a -p 1 add devs 0094
```

Refresh the SYMAPI DB and verify the device is displayed properly as shown in the example.

```
C:\> symmask -sid 0546 -wnn 21000E08B07A0BC -dir 10a -p 1 add devs 0094

C:\> symmask -sid 0546 refresh

Refresh Symmetrix FA/SE directors with contents of SymMask database 000187880546
(y/N)? y

Symmetrix FA/SE directors updated with contents of SymMask Database 000187880546

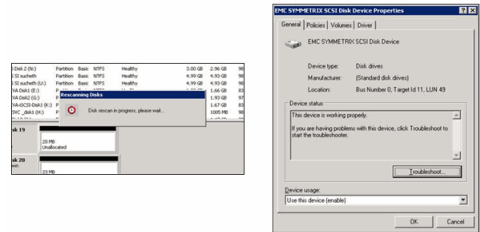
C:\> symmaskdb -sid 0546 list database -dir 10a -p 1

Symmetrix ID : 000187880546
Database Type : Type4
Last updated at : 06:50:34 AM on Fri May 20,2011
Director Identification: FA-10A
Director Port : 1

User-generated
Identifier Type Node Name Port Name Devices

210000e08b07a0bc Fibre 210000e08b07a0bc210000e08b07a0bc 006C:006D
0094
```

8. Make the LUN available to the host by refreshing the device manager.



SYMCLI shows you the correct Operating System level disk:

```
C:\> syminq
```

| Device            | Product | Device    |                |         |          |
|-------------------|---------|-----------|----------------|---------|----------|
| Name              | Type    | Vendor ID | Rev            | Ser Num | Cap (KB) |
| \\PHYSICALDRIVE12 | EMC     | SYMMETRIX | 56714600094000 | 2096640 |          |

## HOW DOES SNAPPROTECT WORK WITH TIMEFINDER/MIRROR?

Calypso always runs an Incremental Establish on BCV volumes. If there has been no prior TimeFinder operations on the BCV, then the Incremental automatically converts into a Full. See the following SYMAPI logs snippet which shows an Incremental Establish:

```
05/24/2011 05:21:15.056 7160 1436 STARTING a BCV 'INCREMENTAL ESTABLISH' operation for 1 [SRC-TGT] Pair:
05/24/2011 05:21:15.181 7160 1436 Symm 000187880546 Number of Pairs: 1 Operation Flags: MultiEstablish
05/24/2011 05:21:15.196 7160 1436 Source-Target Devices: [006C-008B]
05/24/2011 05:21:15.462 7160 1436 The BCV 'INCREMENTAL_ESTABLISH' operation SUCCEEDED.
```

Assuming that device #006C is used as the Primary LUN to the production host, the following steps describe how to create a new TimeFinder/Mirror relationship with SnapProtect:

1. Create a new Device Group "test" to be used for SnapProtect.

```
C:\> symdmg create test -type ANY

C:\> symld -g test -sid 0546 add dev 006C

C:\> symdmg show test

Group Name: test
Group Type : ANY
Device Group in GNS : No
Valid : Yes
Symmetrix ID : 000187880546
Group Creation Time : Thu May 19 14:39:08 2011
VendorID : EMC Corp
Application ID : SYMCLI

Number of STD Devices in Group : 1
Number of Associated GK's : 0
Number of Locally-associated BCV's : 0
Number of Locally-associated VDEV's : 0
Number of Locally-associated TGT's : 0
Number of Remotely-associated VDEV's(STD RDF): 0
Number of Remotely-associated TGT's(TGT RDF): 0
Number of Remotely-associated BCV's(STD RDF): 0
Number of Remotely-associated BCV's(BCV RDF): 0
Number of Remotely-associated BCV's(RBCV RDF): 0
Number of Remotely-associated BCV's(Hop-2 BCV): 0
Number of Remotely-associated VDEV's(Hop-2 VDEV): 0
Number of Remotely-associated TGT's(Hop-2 TGT): 0
Number of Composite Groups : 0
Composite Group Names : N/A

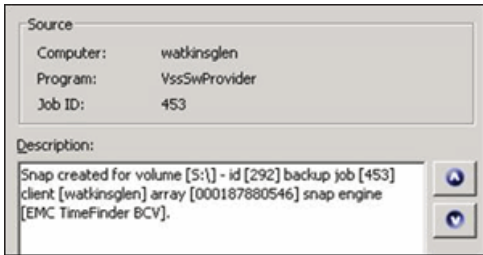
Standard(STD) Devices(1):
{

LdevName PdevName Sym Device Dev Config Cap Att. Sts (MB)
DEV001 N/A 006C 2-Way Mir RW 14400
}
```

2. Assign the BCV volumes to the "test" device group.
3. Using the CommCell Console, create a new subclient for the LUN:
  - During the subclient configuration, ensure to select **EMC TimeFinder BCV** as the storage array.
  - Run a Full/Incremental backup job.

```
C:\> symbcv -g test associate dev xxxx
```





- 4. During the SnapProtect backup job, the "test" device group gets created, and during the snapshot creation, a synchronization is performed.

A BCV device cannot split until the synchronization completes. You can if the device is ready to split using the following command:

```
C:\> symmir -g test split
```

```
C:\> symdg show test
Group Name: test

Group Type : REGULAR
Device Group in GNS : No
Valid : Yes
Symmetrix ID : 000187880546
Group Creation Time : Thu May 19 23:48:22 2011
Vendor ID : CommVault
Application ID : Galaxy_Ent_2000

Number of STD Devices in Group : 1
Number of Associated GK's : 0
Number of Locally-associated BCV's : 1
Number of Locally-associated VDEV's : 0
Number of Locally-associated TGT's : 0
Number of Remotely-associated VDEV's (STD RDF): 0
Number of Remotely-associated BCV's (STD RDF): 0
Number of Remotely-associated TGT's (TOT RDF): 0
Number of Remotely-associated BCV's (BCV RDF): 0
Number of Remotely-associated RBCV's (RBCV RDF): 0

Standard (STD) Devices (1):
{

LdevName PdevName Sym Cap Dev Att Sts (MB)

DEV001 \\PHYSICALDRIVE22 006C RW 14400
}

BCV Devices Locally-associated (1):
{

LdevName PdevName Sym Cap Dev Att Sts (MB)

SP_2_453_292 \\PHYSICALDRIVE23 008B RW 14400
}

```

- 5. Once the synchronization completes, the "split" operation is automatically issued by the Calypso software.

```
C:\> symmir -g test query
Device Group (DG) Name: test
DG's Type : ANY
DG's Symmetrix ID : 000187880546

Standard Device BCV Device State

Logical Inv. Sym Tracks Logical Inv. Sym Tracks STD <=> BCV

DEV001 006C 0 BCV001 008B * 329805 SyncdnProg
Total
Track(s) 0 329805
MB(s) 0.0 10306.4

```

```
C:\> symmir -g test query
Device Group (DG) Name: test
DG's Type : ANY
DG's Symmetrix ID : 000187880546

Standard Device BCV Device State

Logical Inv. Sym Tracks Logical Inv. Sym Tracks STD <=> BCV

DEV001 006C 0 BCV001 008B * 0 Synchronized
Total
Track(s) 0 0
MB(s) 0.0 0.0

```

Legend:  
 (\*) The paired BCV device is associated with this group.

```
C:\> symmir -g test query
Device Group (DG) Name: test
DG's Type : REGULAR
DG's Symmetrix ID : 000187880546

Standard Device BCV Device State

Logical Inv. Sym Tracks Logical Inv. Sym Tracks STD <=> BCV

DEV001 006C 0 SP_2_453_292 008B * 0 Split
Total
Track(s) 0 0
MB(s) 0.0 0.0

```

Legend:  
 (\*) The paired BCV device is associated with this group.

- 6. During the cataloging phase, the host LUN mapping is adjusted for the BCV device #008D.

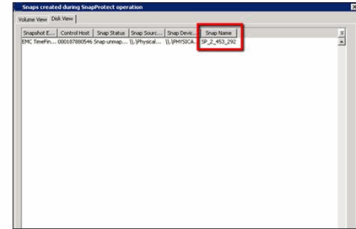
- The BCV device is "un-masked". From the CommCell Console, you can see the snapshots created during the the SnapProtect job.

```
C:\> symmaskdb -sid 0546 list database -dir 10a -p 1

Symmetrix ID : 000187880546
Database Type : Type4
Last updated at : 08:50:34 AM on Fri May 20,2011
Director Identification: FA-10A
Director Port : 1

User-generated
Identifier Type Node Name Port Name Devices

210000e08b07a0bc Fibre 210000e08b07a0bc 210000e08b07a0bc 006C:006D
008B
```



```
C:\> symmir -g test query

Device Group (DG) Name: test
DG's Type : REGULAR
DG's Symmetrix ID : 000187880546

StandardDevice BCV Device State

Logical Inv. Tracks Logical Inv. Tracks STD <=> BCV
Sym Sym

DEV001 006C 0 SP_2_453_292 008B * 0 Spilt

Total
Track(s) 0 0
MB(s) 0.0 0.0

Legend:
(*) The paired BCV device is associated with this group.
```

### HOW DOES SNAPPROTECT WORK WITH TIMEFINDER/SNAP?

Similar to TimeFinder/Mirror, Calypso always require a new or recycled VDEV relationship to a single Production volume for each SnapProtect job. However, TimeFinder/Snap allows the LUN to be available to the production host by using the Copy-On-Write mechanism.

Assuming that device #0094 is used as the Primary LUN to the production host, the following steps describe how to create a new TimeFinder/Snap relationship with SnapProtect:

- Create a new Device Group "test" to be used for SnapProtect.
- You must have a SAVE pool for VDEV volumes. You may use the DEFAULT\_POOL.

In the example shown on the right, you can see that the DEFAULT\_POOL has few devices and plenty of space. If you require further SAVE devices, you can create a text file (e.g., new\_save\_pool.txt) with the following content:

```
add dev 81:82 to pool DEFAULT_POOL, type=savedev, member_state=enable;
```

After creating the text file, run the following commands to add the extra devices to the SAVE:

```
C:\> symconfigure -sid 0546 -f c:\new_save_pool.txt -v -nop commit
```

- Assign a VDEV volume to be used for TimeFinder/Snap.

```
C:\> symdev -sid 0546 list -savedev

Symmetrix ID: 000187880546

Device Name Directors Device

Sym Physical SA P DA IT Config Cap Attribute Sts (MB)

0079 Not Visible ???-? 02D:C2 2-Way Mir N/A (SV) RW 14400
007A Not Visible ???-? 15A:C2 2-Way Mir N/A (SV) RW 14400
007B Not Visible ???-? 12D:C2 2-Way Mir N/A (SV) RW 14400
007C Not Visible ???-? 05A:C2 2-Way Mir N/A (SV) RW 14400
007D Not Visible ???-? 02B:C2 2-Way Mir N/A (SV) RW 14400
007E Not Visible ???-? 15C:C2 2-Way Mir N/A (SV) RW 14400
007F Not Visible ???-? 01A:C2 2-Way Mir N/A (SV) RW 14400
0080 Not Visible ???-? 16D:C2 2-Way Mir N/A (SV) RW 14400
0081 Not Visible ???-? 11C:C2 2-Way Mir N/A (SV) RW 14400
0082 Not Visible ???-? 06B:C2 2-Way Mir N/A (SV) RW 14400
```

```
C:\> symsnap list -svp DEFAULT_POOL -savedevs

Symmetrix ID: 000187880546

SNAP SAVE DEVICES

Device SaveDevice Total Used Free Full
Sym Emulation PoolName Tracks Tracks Tracks (%)

0079 FBA DEFAULT_POOL 460800 21076 439724 4
007B FBA DEFAULT_POOL 460800 19835 440965 4
007C FBA DEFAULT_POOL 460800 20130 440670 4
007E FBA DEFAULT_POOL 460800 20326 440474 4
007F FBA DEFAULT_POOL 460800 20499 440301 4
0080 FBA DEFAULT_POOL 460800 20965 439835 4

Total
Tracks 2764800 122831 2641969 4
MB(s) 86400.0 3838.5 82561.5
```

```
C:\> symid -g test -sid 0546 add dev 009E -vdev
C:\> symdg show test
Group Name: test

Group Type : REGULAR
Device Group in GNS : No
Valid : Yes
Symmetrix ID : 000187880546
Group Creation Time : Mon May 23 07:01:30 2011
Vendor ID : EMC Corp
Application ID : SYMCLI

Number of STD Devices in Group : 1
Number of Associated GK's : 0
Number of Locally-associated BCV's : 0
Number of Locally-associated VDEV's : 1
Number of Locally-associated TGT's : 0
Number of Remotely-associated VDEV's (STD RDF): 0
Number of Remotely-associated BCV's (STD RDF): 0
Number of Remotely-associated TGT's (TGT RDF): 0
Number of Remotely-associated BCV's (BCV RDF): 0
Number of Remotely-associated RBCV's (RBCV RDF): 0

Standard (STD) Devices (1):
{

LdevName PdevName Sym Cap Dev Att Sts (MB)

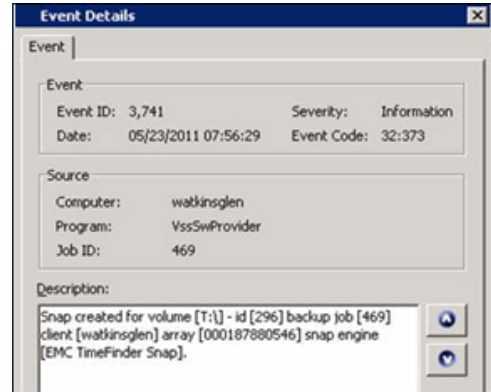
DEV001 W:\PHYSICALDRIVE12 0094 RW 2048
}

VDEV Devices Locally-associated (1):
{

LdevName PdevName Sym Cap Dev Att Sts (MB)

```

4. Using the CommCell Console, create a new subclient for the LUN:
  - During the subclient configuration, ensure to select **EMC TimeFinder Snap** as the storage array.
  - Run a Full/Incremental backup job.



5. During the snapshot creation, Copy-On-Write operations are performed. Once the snapshot is created, the snapshot will be mounted and cataloged, and the VDEV device will be "un-masked".

```
C:\> symsnap -g test_snap query

Device Group (DG) Name: test
DG's Type : REGULAR
DG's Symmetrix ID : 000187880546

Source Device Target Device State Copy

Protected Changed
Logical Sym Tracks Logical Sym G Tracks SRC <=> TGT (%)

DEV001 0094 65520 SP_2_469_296 009E X 0 CopyOnWrite 0

Total
Track(s) 65520 0
MB(s) 2047.5 0.0

Legend:
(G): X = The Target device is associated with this group,
 . = The Target device is not associated with this group.
```

**WHAT ARE THE SYMCLI ENVIRONMENT VARIABLES I CAN USE?**

There are many environment variables that may aid in troubleshooting and potentially change some of the SnapProtect behavior. Please use these variables with caution. Consult with your EMC Storage Consultant if you are unsure of the impact these variable may cause.

Use the following command to retrieve the list of SYMCLI variables:

```
C:\> symcli -env
```

**IF I HAVE RDF DEVICES THAT ARE NOT PAIRED, HOW CAN I USE THEM FOR SNAPPROTECT BACKUP?**

To use the RDF devices that are not paired, follow the steps given below:

1. Create a RDF device group.
2. Ensure that the source RDF device is a part of the device group created on the same machine.
3. Add the Target VDEV/BCV to the same device group. Use the `symdg add` with `-tgt` option to add the target devices to the RDF device group.

**HOW DO I BACK UP ALL OF THE DEVICES THAT BELONG TO A PARTICULAR APPLICATION?**

Enable the `bConsistentActivate` registry key to create a consistent point-in-time image of the devices distributed across multiple sites. The key is used during

activate operation for TimeFinder/Snap and TimeFinder/Clone and during Split operation for TimeFinder/Mirror. This is helpful while backing up all of the devices that belong to a particular application or backing up multiple devices distributed across multiple sites.

---

### **CAN I USE A DIFFERENT SAVE DEVICE POOL FOR TIMEFINDER/SNAP?**

By default, TimeFinder Snap uses DEFAULT\_POOL as the SAVE Device Pool for saving changed tracks from the source device.

Enable the `sSaveDevicePool` registry key to change the default SAVE Device Pool and use a different pool. The specified SAVE Device Pool Name is used with `-svp` option to TimeFinder/Snap create command.

### **BEST PRACTICES**

- Ensure that masking is configured.
- We recommend that all the VDEV and BCV devices are mapped to all the available ports.
- Ensure that gatekeepers are configured for each host connected to the Symmetrix array.
- Ensure that enough disk space is available for snapshot operations and the disk space used by snapshots is monitored. The space requirement for snapshots created during SnapProtect backup can vary based on your environment. The space utilization is dependent on the number of snapshots created and the retention period defined for the snapshots.
- SnapProtect backup uses any available previously synchronized BCVs.
- For any EMC Symmetrix operations to work, the `SYMAPI_HOME_DIR` registry key must be set to the directory where the Symmetrix SYMAPI library is located.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the `sSNAP_UseINITIATOR` registry key to the desired initiator address.

# Advanced - Fujitsu Eternus DX

## BEST PRACTICES

- It is important not to perform any configurations on the ETERNUS Console while running snapshot operations in the CommCell Console.
- For SnapOPC snapshots, the SDV volume should be pre-paired with the source before performing snapshot operations.
- For EC (clone) snapshots, the destination volume should be pre-paired with the source before performing snapshot operations. After pre-pairing, the destination volume should not be left in a suspended state.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the sSNAP\_UseINITIATOR registry key to the desired initiator address.

## FAQ

---

### WHAT ARE THE TARGET VOLUME SELECTION RULES?

The target volume selection rules for Clone and Snap Snapshots are discussed below:

#### FOR CLONE SNAPSHOTS

1. The first priority is given to pre-paired sessions in the following order:
  - If special name is set by the registry key ETERNUS\_USE\_VOLUME\_LABEL, then pre-paired session with target volume having special name will be given preference. If no such pre-paired session found, any existing pre-paired session will be picked.
  - If the registry key ETERNUS\_USE\_VOLUME\_LABEL is not set, pre-paired sessions with volumes named as iSnapR\_<xyz> will be given preference. If no such pre-paired session found, any existing pre-paired session will be picked.
2. If pre-paired sessions are not available, preference is given to target volumes with a special name set by the registry key ETERNUS\_USE\_VOLUME\_LABEL. If there are no suitable volumes with the special name, the backup job will fail. If there are more than one volumes with the special name, preference will be based on the source volume type. If source volume is a standard volume, preference will be given to standard volumes otherwise thin provisioning volume.
3. If no target volumes are available, a volume will be created using the specified destination pool.

#### FOR SNAP SNAPSHOTS

1. The first priority is given to pre-paired sessions in the following order:
  - If special name is set by the registry key ETERNUS\_USE\_VOLUME\_LABEL, then pre-paired session with target volume having special name will be given preference. If no such pre-paired session found, any existing pre-paired session will be picked.
  - If the registry key ETERNUS\_USE\_VOLUME\_LABEL is not set, pre-paired sessions with volumes named as iSnapR\_<xyz> will be given preference. If no such pre-paired session found, any existing pre-paired session will be picked.
2. If pre-paired sessions are not available, preference is given to target volumes with a special name set by the registry key ETERNUS\_USE\_VOLUME\_LABEL. If there are no suitable volumes with the special name, the backup job will fail.
3. If no target volumes are available, the job will fail.

# Advanced - Hitachi Data Systems

## TABLE OF CONTENTS

BCV Devices Requirement

Troubleshooting

FAQ

Best Practices

## BCV DEVICES REQUIREMENT

Use the following matrix to calculate the number of target devices required for performing SnapProtect operations.

| AGENT                                                      | TARGET DEVICE REQUIREMENTS (BUSINESS CONTINUANCE VOLUMES/ SHADOW IMAGE VOLUMES)                                                                                                                                                         |                                                          | NOTES                                                                              |                                                                                                                                                                                                    |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | FULL BACKUP                                                                                                                                                                                                                             | INCREMENTAL BACKUP                                       |                                                                                    | DIFFERENTIAL BACKUP                                                                                                                                                                                |
| <b>DB2</b>                                                 | [Number of devices where data resides] + [Number of devices where the online log resides] + [Number of devices where the 'LOCAL_DB_DIRECTORY' resides] + [Number of devices where the 'DBPATH' resides]                                 | N/A                                                      | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Exchange Database</b>                                   | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      | [Number of devices where the log resides]                | [Number of devices where the log resides]                                          | For example, if your data resides on 2 devices, logs reside on 1 devices. Full backup will require 3(2+1) target devices, Incremental/Differential backup will require 1 target devices.           |
| <b>Microsoft SQL Server</b>                                | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      |                                                          | [Number of devices where data resides] + [Number of devices where the log resides] | For example, if your file system data resides on 3 devices you will require 3 target devices.<br>SQL log backup does not require any target device.                                                |
| <b>Microsoft Windows File System</b>                       | Number of devices on which the file system data resides                                                                                                                                                                                 | Number of devices on which the file system data resides  | Number of devices on which the file system data resides                            |                                                                                                                                                                                                    |
| <b>NAS NDMP</b>                                            | Number of devices on which the file system data resides                                                                                                                                                                                 |                                                          |                                                                                    |                                                                                                                                                                                                    |
| <b>Oracle</b>                                              | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      |                                                          | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Oracle – Data and logs residing on the same devices</b> | 2x[Number of devices where data and logs reside]                                                                                                                                                                                        |                                                          | N/A                                                                                | For example, if your data and logs reside on 3 devices, you will require 6 target devices.                                                                                                         |
| <b>Applications running on JFS</b>                         | [Number of devices where application data resides] + [Number of devices where JFS logs reside] + [No. of devices on which logs reside]                                                                                                  |                                                          | N/A                                                                                | For example, if your application data resides on 2 devices, logs reside on 1 devices, data and logs share one device, and JFS logs reside on 1 device, you will require 6 (2+1+2+1) target devices |
| <b>SAP for Oracle - Data and logs</b>                      | [Number of devices where data resides] + [Device where the 'sapbackup' directory resides] + [Number of devices where the log resides] + [Device where the 'saparch' directory resides] + 2 x [Device where the 'dbs' directory resides] | N/A                                                      | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Unix File System</b>                                    | [Number of devices where data resides] + [Number of devices where the log resides]                                                                                                                                                      |                                                          |                                                                                    |                                                                                                                                                                                                    |
| <b>Unix File System on JFS</b>                             | [Number of devices on which the file system data resides ] + [No. of devices on which file system logs reside]                                                                                                                          |                                                          |                                                                                    | For example, if your file system data resides on 2 devices and file system log resides on 1 device, you will require 3 target devices.                                                             |
| <b>VMware</b>                                              | Number of luns on which the datastore for the VM resides                                                                                                                                                                                | Number of luns on which the datastore for the VM resides | N/A                                                                                |                                                                                                                                                                                                    |
| <b>Microsoft Hyper-V</b>                                   | Number of luns on which vhd and configuration files of VM reside                                                                                                                                                                        | Number of luns on which vhd and                          | N/A                                                                                |                                                                                                                                                                                                    |

## TROUBLESHOOTING

### HARDWARE REVERT OF VSP VOLUMES FAILS

Hardware specific revert operations of VSP volumes may fail if system MODE 80 and MODE 87 options are set to ON in the array. It is recommended to have these modes always OFF for hardware reverts to succeed.

Please note that by default MODE 80 and MODE 87 are set to OFF. After installing the storage array software, all system modes are set to their default values by default. System modes can only be changed by a Hitachi Data Systems representative.

#### MODE 80

- If set to ON, normal restore and/or reverse copy is performed.
- If set to OFF, quick restore is performed.

#### MODE 87

- If set to ON, quick resynchronization is performed.
- If set to OFF, normal copy is created.

## FAQ

### CAN I SWITCH BETWEEN HDS SNAP AND HDS CLONE ON THE SAME DISK?

You cannot switch between HDS Snap and HDS Clone on the same disk; even after deleting the existing snaps.

### WHAT IS THE MAXIMUM NUMBER OF SNAPSHOTS CREATED FOR USP VOLUMES?

The maximum number of snapshots created for a USP volume is 3.

### CAN I REUSE A DELETED SHADOW IMAGE?

Yes, you can reuse a deleted Shadow Image by creating the `CVHDS_USE_DELETED_SHADOWIMAGE` registry key if you encounter one of the following scenarios:

- When the expected changes to the source volume are less than 50% between the old and new Shadow Image.
- When you decide to use a spool copy.

### HOW IS THE DEVICE POOL FOR COW ON HUS SELECTED?

For P-VOL, the first COW pair creation determines the device pool selection. The pool-id specified during the first COW pair is used for all the remaining COW pairs created using the same P\_VOL. If you specify another pool-id during the creation it will be ignored and the pool-id specified during the first COW pair creation will be used.

## BEST PRACTICES

- Ensure that the client and proxy computers are configured and have access to the array.
- The V-VOL (COW snapshot) should be created prior to performing the SnapProtect backup operations.
- Same size unallocated P-VOL (Primary Volume) will be chosen to be converted into an S-VOL while doing a shadow image operation for a P-VOL.
- Ensure that sufficient number of V-VOL (COW snapshot) and destination P-VOL (S-VOL - Shadow Image) devices are configured to meet your retention requirements.
- Ensure that command devices are configured for each host connected to the HDS array.
- After mapping a device and adding a drive letter, you should perform a Host refresh on the Device Manager Server.
- Ensure that enough disk space is available for snapshot operations and the disk space used by snapshots is monitored. The space requirement for snapshots created during SnapProtect backup can vary based on your environment. The space utilization is dependent on the number of snapshots created and the retention period defined for the snapshots.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the `sSNAP_UseINITIATOR` registry key to the desired initiator address.

# Advanced - HP StorageWorks EVA

## TROUBLESHOOTING

---

### SNAPSHOTS ARE NOT BEING CREATED

Snapshots cannot be created when the source disk is:

- a snapshot
- is in the process of normalizing (clone in progress) or being deleted

---

### CLONES ARE NOT BEING CREATED

Clones cannot be created when the source disk is:

- a snapshot
- a disk that has a snapshot
- in the process of normalizing (clone in progress) or being deleted

---

### SNAPPROTECT BACKUP IS FAILING FOR HP-UX

Ensure that the kernel tunable (MAXVGS) value are set based on the number of volume groups on the client computer.

## BEST PRACTICES

- Snapshots/clones are included in the maximum number of virtual disks per array.
- The maximum number of snapshots per source varies based on the array controller software version. For more information, see the HP StorageWorks Enterprise Virtual Array compatibility reference.
- Ensure that the client and proxy computers are configured and have access to the array.
- Ensure that enough disk space is available for snapshot operations and the disk space used by snapshots is monitored. The space requirement for snapshots created during SnapProtect backup can vary based on your environment. The space utilization is dependent on the number of snapshots created and the retention period defined for the snapshots.
- By default, SnapProtect backup uses the first FC adapter that it detects. To use a different FC adapter, use the sSNAP\_UseINITIATOR registry key.



## Advanced - IBM SAN Volume Controller (SVC)

### BEST PRACTICES

- Prior to performing a revert operation for a Flash Copy, ensure that:
  - you do not have any Space-Efficient Flash Copies created on the volume prior to creating the Flash Copy.
  - copy operations for the Flash Copy have completed.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the sSNAP\_UseINITIATOR registry key to the desired initiator address.

## Advanced - IBM XIV

### BEST PRACTICES

- For Fibre Channel, by default, SnapProtect backup uses the first FC adapter that it detects. To use a different FC adapter, use the sSNAP\_UseINITIATOR registry key.
- If a fiber channel adapter is found on the Windows or UNIX client, then by default, the fiber channel will be attempted for mounting snapshots. Set the sSNAP\_IsISCSI registry key to use iSCSI even when a fiber channel adapter is detected.

# Advanced - LSI

## TROUBLESHOOTING

### SNAPPROTECT BACKUP IS FAILING

If multiple paths are available and multipath is not configured properly SnapProtect backup job may fail due to intermittent path failures. In case of improper multipath configuration, the SnapProtect backup chooses preferred path while performing mapping but preferred path may change due to failovers. Verify if the array you are using supports multi paths.

### UNABLE TO CONFIGURE LSI ARRAY FROM OEM VENDORS

If you are unable to configure LSI array from OEM vendors, such as Dell, IBM, etc., make sure to set the LSI\_VENDOR\_NAME and LSI\_PRODUCT\_ID registry keys on the source and proxies if available.

## FAQ

### WHAT IS THE MAXIMUM NUMBER OF SNAPSHOTS THAT CAN BE CREATED?

The maximum number of snapshot created for each source volume is 4.

### HOW CAN I AUTHENTICATE LSI ARRAY PASSWORD WITH SMIS SERVER PASSWORD?

You can authenticate the LSI array password with SMIS (Storage Management Initiative Specification) server using `CvSMISTool` for successful snap creation.

Use the following steps to set the password:

1. From the command prompt, navigate to `<Software Installation Directory>\Base` folder.
2. Type `CvSMISTool.exe`.
3. Type **2** to set the password.

```
1) Test SMIS Server
2) Set LSI Array Password
Select option 1 or 2, for Quit, default [1]: 2
```

4. Specify host name or IP address of the device manager where the array is configured.

```
Enter SMIS server HostName or IP : <Server_Name>
```

5. Specify the user name of the SMIS server.

```
Enter SMIS server User Name : <User Name>
```

6. Specify password for SMIS server.

```
Enter SMIS server Password : <Password>
```

7. Specify the number corresponding to the array that you wish to select and press **Enter**.

```
1) Array Name : iscsi-lsi-1
Array UUID : *****1A2X

2) Array Name : san_nas_lsi
Array UUID : *****26B4
Select option : [1 - 2] to quit, default [1]: 1
```

8. Specify password of LSI Array.

```
Enter LSI Array Password:
Re-enter LSI Array Password:
Password modified successfully
```

## BEST PRACTICES

- Ensure that enough disk space is available for snapshot operations and the disk space used by snapshots is monitored. The space requirement for snapshots created during SnapProtect backup can vary based on your environment. The space utilization is dependent on the number of snapshots created and the retention period defined for the snapshots.
- While Volume Copy operation is in progress, read-write to the source volume should be frozen until volume copy operation completes.

- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the sSNAP\_UseINITIATOR registry key to the desired initiator address.

# Advanced - NetApp

## TABLE OF CONTENTS

Troubleshooting

FAQ

Best Practices

## TROUBLESHOOTING

---

### ERROR MESSAGE: NO SUCH SNAPSHOT

#### PROBLEM

You may get this error message when mounting a snapshot from a Vault Copy for a destination volume that has Deduplication enabled.

#### SOLUTION

To resolve the issue, setup the following registry keys on the Client computer:

- For LUN mount operation, create the sNETAPPCLONELUNBYSNAPTIMESTAMP registry key
- For NFS mount operation, create the sNETAPPREVERTVOLUMEBYSNAPTIMESTAMP registry key

---

### SNAP CREATION FAILS WITH A BUSY LUN ERROR

A snapshot enters a busy state in the following scenarios:

- When there are LUN clones backed up in the snapshot
- When snapshots are mounted manually outside of the SnapProtect backup, through the CommCell Console, or for SnapProtect backup operations such as backup copy creation

Busy snapshots may cause SnapProtect backups to go pending. If you have busy snapshots, consider the following:

- Delete the snapshots in the reverse order they were created in.
- Do not mount a volume and create another SnapProtect backup for the volume.

The SnapProtect backup software will detect busy snapshots and will not allow an additional snapshot to be created until there are no busy snaps. To avoid this snapshot dependency, do not manually create a snapshot of a volume while you have a snapshot mounted.

- If you have a situation where the busy snapshot is no longer mounted but still shows as busy, proceed to delete all the additional snaps that were created while the busy snap was mounted. The snapshot will no longer be busy.

To avoid the snap dependency for NetApp ONTAP version 7.3, use the snapshot\_clone\_dependency volume option to enable the system to lock the backup of snapshot copies for the active LUN clone. You will be able to delete the base Snapshot copy without having to first delete all of the more recent backing Snapshot copies.

If you are using any other applications on the LUN, review the documentation for impacts caused by using the snapshot\_clone\_dependency volume option. If you delete the snapshot cloned by the LUN with the volume option enabled, you will not be able to restore the clone from one of the later snaps. The SnapProtect backup will detect if the dependency option is enabled and will allow additional snapshots to be created, even if the snapshot is mounted.

## FAQ

---

### WHAT IS THE MAXIMUM NUMBER OF SNAPSHOTS CREATED FOR EACH VOLUME?

The maximum number of snapshot created for each volume is 255.

---

### CAN I CREATE ADDITIONAL PROVISIONING POLICIES FOR SECONDARY COPIES AND USE THEM FOR SNAPPROTECT?

Additional provisioning policies for secondary copies can be added to the DataFabric Manager. Any provisioning policy with a name starting with "SnapProtect\_" (case in-sensitive) will be displayed in the SnapProtect GUI for use in storage policy copies.

---

### CAN I USE A NON ROOT USER TO CONFIGURE AN ARRAY OR NDMP?

You can use a Non-Root user for the Array configuration and NDMP configurations.

To configure the array with a non-root user, execute the following commands:

```
NetApp1> useradmin role add snapprotectrole -c "[SnapProtect Management Role]" -a login-ndmp,login-http-admin,api-*
```

```
NetApp1> useradmin group add snapprotectgroup -c "[SnapProtect Management Group]" -r snapprotectrole
NetApp1> useradmin user add snapprotectuser -c "[SnapProtect Management Account]" -n "S Admin" -g snapprotectgroup
```

For example:

```
NetApp1> useradmin role add snapprotectrole -c "SP Mgmt Role" -a login-ndmp,login-http-admin,api-*
NetApp1> useradmin group add snapprotectgroup -c "SP Mgmt Group" -r snapprotectrole
NetApp1> useradmin user add snapprotectuser -c "SP Mgmt Account" -n "S Admin" -g snapprotectgroup
```

The first command creates the SnapProtect Role with the proper rights; the second command adds this role to a newly created SnapProtect group; and the third command creates the user to for the Array credential field in the Calypso Control Panel.

**USE THE SAME CREDENTIALS FOR NDMP**

You can use the same credentials for NDMP that you use for the array.

To configure NDMP with the same credentials, enter the encrypted password in the following command, and then execute it:

```
NetApp1> ndmpd [password] snapprotectsuser
```

For example:

```
NetApp1> ndmpd pswdl snapprotectsuser
```

**HOW DO I VERIFY THAT THE DESTINATION FILER HAS SNAPMIRROR ACCESS TO THE SOURCE FILER?**

To ensure that SnapMirror jobs run, the destination filer must have SnapMirror access to the source filer. If the name or IP address of the SnapMirror filer appears in "/etc/snapmirror.allow", then the destination filer has access.

To add entries to "/etc/snapmirror.allow" execute the following command:

```
source-filer> wrfile /etc/snapmirror.allow
destination-filer
<Ctrl+C>

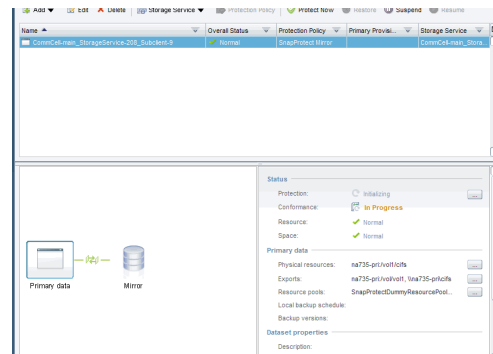
source-filer> rdfile /etc/snapmirror.allow
destination-filer
```

Alternatively, you can go into each of the hosts in DataFabric Manager and configure the the proper security rights for source and destination in the Fabric-Attached Storage settings.

**HOW DOES THE SNAPMIRROR PROCESS WORK?**

1. To get the full, detailed Snap Management plan so that SnapMirror/SnapVault can run, NetApp runs a conformation check during the first auxiliary copy job.

On NetApp



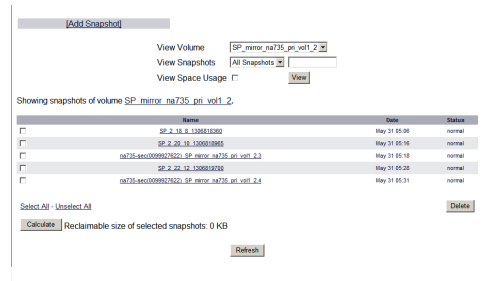
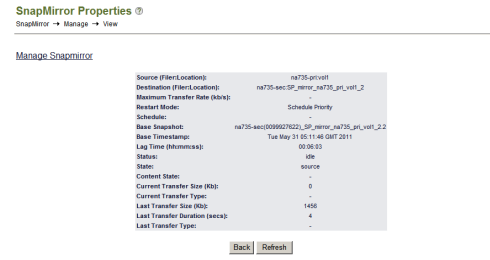
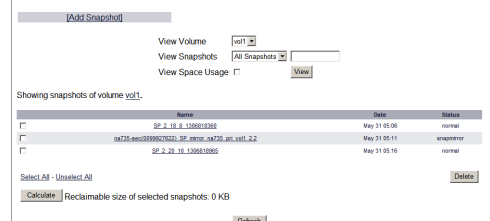
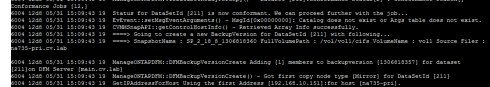
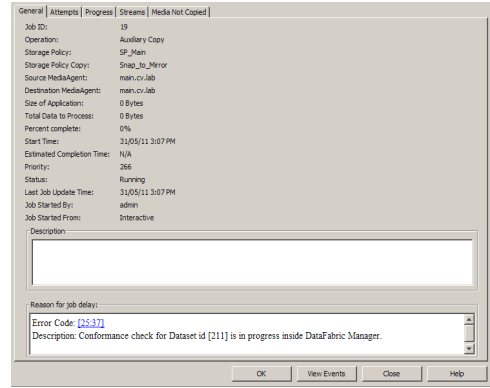
On Calypso

- During each SnapMirror auxiliary copy job, SnapMirror creates a "BackupVersion," which is a new Snapshot of the entire volume that requires replication.
- Once a new Snapshot for SnapMirror is available, the Snapshot is listed under the volume on the Primary Filer.
- The new Snapshot also appears in the current SnapMirror session.

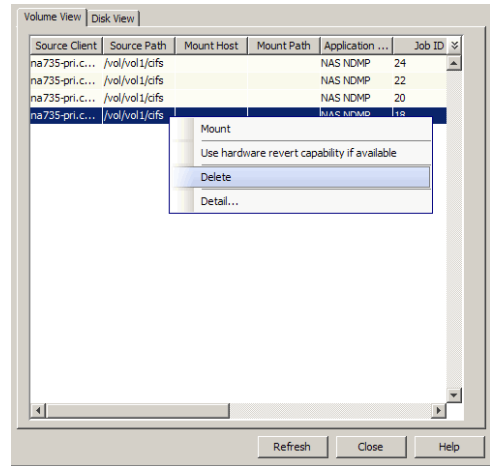
- On the destination filer site, the same Snapshot appears. In addition, if there were any previous SnapMirror on-demand jobs run, only the very last one remains on the target box.
- NetApp calls this a "Swizzling Process". That is, the primary Fabric-Attached Storage (FAS) creates a delta set between the original snapshot used from the previous SnapMirror job and the new snapshot created for the current SnapMirror job. Only the details of the snapshot and the deltas are sent to the destination FAS, and refer to the previous snapshot, which was formerly the target SnapMirror session. The volume is updated to match what is in the primary FAS. The previous snapshot is not deleted because the entire process is a background job.

**HOW DOES DATA AGING WORK WITH SNAPMIRROR?**

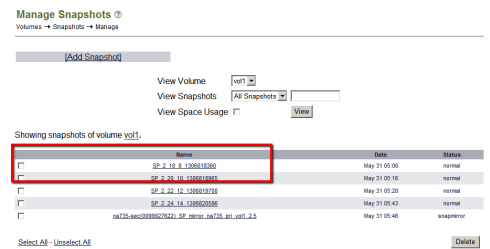
- Once a job has been Data-Aged or manually deleted, the job no longer appears in the SnapMirror target either. SnapVault is not affected by this process.



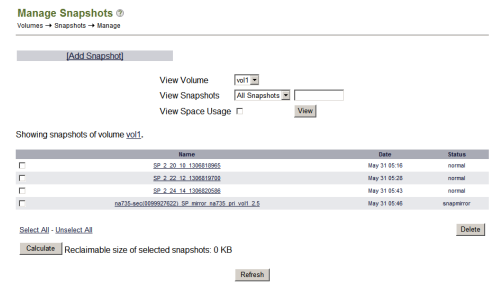
**BEFORE DELETION ON CALYPSO**



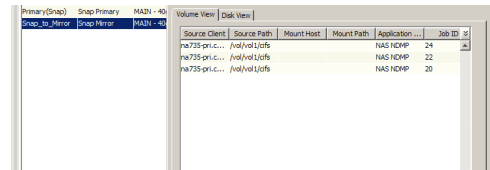
**BEFORE DELETION ON SNAPMIRROR**



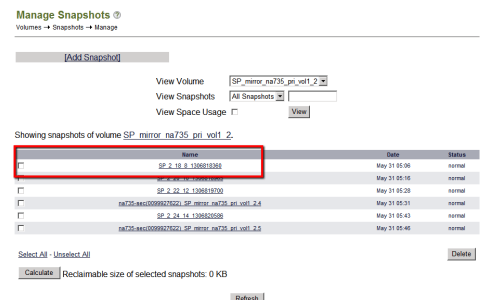
**AFTER DELETION ON PRIMARY FAS**



**AFTER DELETION ON CALYPSO**



**AFTER DELETION ON THE SECONDARY FAS**



- The DataAging process does not remove this snapshot either. Only the next auxiliary copy job deletes this snapshot. After a new job runs, AuxCopy reports that there is no

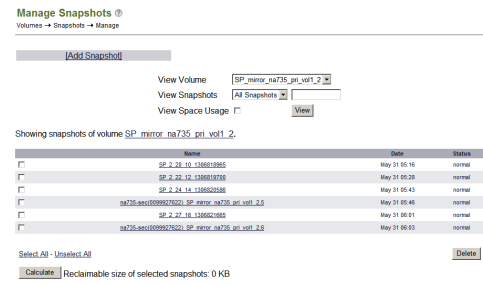
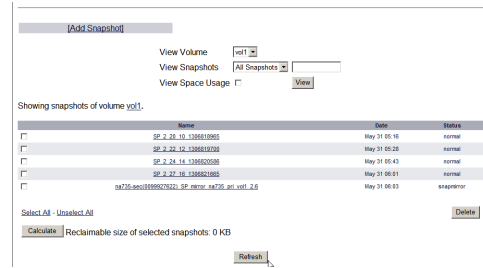


new data to move.

The primary FAS shows that a new snapshot is used for SnapMirror.

3. The secondary FAS shows the new snapshot here, but the process has not removed the volume snapshot that pertained to Job 18.

Now the job has been deleted from Calypso. This won't affect the SnapMirror relationship until the next job runs and another auxiliary copy job runs. The latest SnapMirror snapshot that was synchronized to the secondary FAS is responsible for deleting the snapshot on the destination FAS box.



## BEST PRACTICES

- For any ONTAP version, it is recommended to provide the host name or IP address of a data port (e.g., e0A, e0B) during the NAS client or storage array configuration instead of using the management port (e.g., e0M). If you are using the management port, you must reassign the host name or IP address of the management port to a data port on the file server.
- It is recommended that you do not use the system volume (typically vol0) for user data.
- Ensure that enough disk space is available for snapshot operations and the disk space used by snapshots is monitored. The space requirement for snapshots created during SnapProtect backup can vary based on your environment. The space utilization is dependent on the number of snapshots created and the retention period defined for the snapshots.
- It is recommended that you do not install the CommServe and DataFabric Manager on the same computer.
- To perform snapshots and backup to tape operations in parallel for the same data, use two backupsets.
- When planning for Snapshots, group LUNs according to their rate of change. For example, group LUNs with a high rate of change in the same volume and group LUNs with a low rate of change in another, separate volume. When calculating the size of volumes, use the rate of change to determine the amount of space necessary for Snapshots.
- SnapProtect provides the full suite of capabilities for recovery regardless of the Volume to LUN relationship and ratio. However, a 1 to 1, Volume to LUN, relationship might simplify storage and application management. It is also best to ensure that each LUN resides within a Qtree in SnapMirror and SnapVault configurations. Thin Provisioned Volumes with LUNS make your storage provisioning and snapshot management flexible.
- Disable the native NetApp schedule for snapshots on volumes that Calypso manages. This ensures snapshot retention and storage use is in line with the policies defined within Calypso. Using the default setting for internal snapshot scheduling might cause contention problems if multiple calls to create snapshots occur at the same time. To change the default setting, you can clear the Scheduled checkbox for the volume from Filer View or System Manager.
- In order to use a specific initiator for accessing snapshots during SnapProtect backup set the sSNAP\_UseINITIATOR registry key to the desired initiator address.

# Advanced - Data Replicator

## TABLE OF CONTENTS

### Overview

#### How it Works

#### Use a Different Replication Process

#### Use Hardware snapshot

Enable Use of Hardware Snapshot

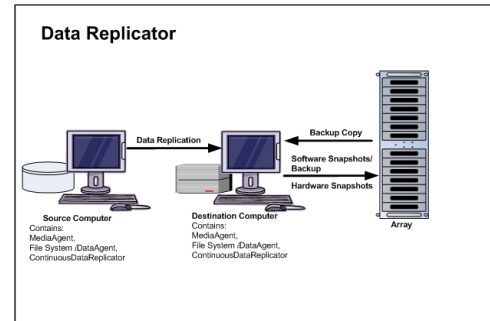
Setup the Array Information

## OVERVIEW

Data Replicator provides the snapshot functionality without the need for any specialized hardware.

The use of Data Replicator with SnapProtect backup provides the following key capabilities:

- Identify precise changes to the data protected on the source computer and transfer only the modified data during backup. This reduces the amount of data transferred over the network enabling faster backup cycles.
- Protect application data in a consistent state and restore to a point-in-time upon recovery.
- Protect highly dynamic application data environments without compromising system performance. An effective way to backup live data is to temporarily quiesce it, take a snapshot, and then resume live operations.
- Compression and encryption of source data during backup for network efficiency and data security.
- Move backup data on the destination to secondary storage and also restore back data from the secondary storage to the source computer when required.
- The flexibility to engage hardware or software storage arrays for performing backup operations. Use hardware or software storage arrays to perform SnapProtect backup. For e.g., you can use a hardware array like NetApp or a software storage array like Data Replicator to perform the data protection operations.



## HOW IT WORKS

When you select data replicator as a storage array, the data on the source computer is replicated to the destination computer. A snapshot of the replicated data is created and used for various data protection and recovery operations. After an initial data replication of data from source to destination computer, only the new or changed data on the source computer will be replicated to the destination computer.

You can either use the hardware or the software storage arrays to create snapshots of the replicated data to be used for various data protection operations.

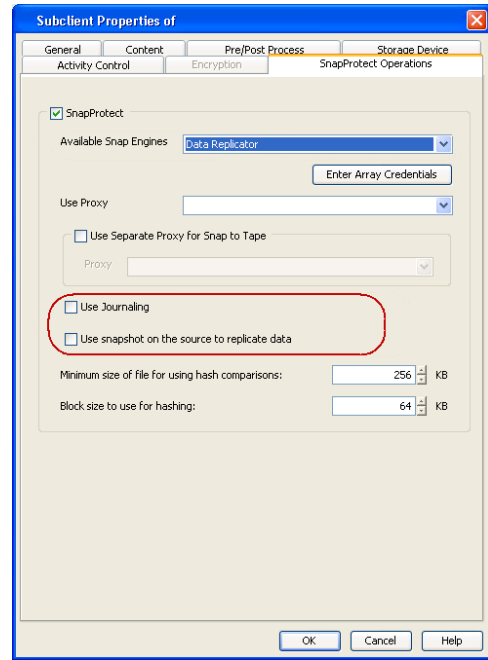
## USE A DIFFERENT REPLICATION PROCESS

There are other replication methods you can select from while configuring a subclient to use the Data Replicator storage array.

By default, the data on the source will be compared with the replicated data on the destination computer in order to transfer new or changed data to the destination for replication.

Follow the steps below to use a different replication method:

1. From the CommCell Console, navigate to **<Client> | <Agent>**.
2. Right-click the subclient and click **Properties**.
3. Click the **SnapProtect Operations** tab.
4. Click **Use Journaling** if you want to continuously track any change made on the source computer since the last SnapProtect backup. All the changes will be stored in the database and will be transferred for replication to the destination computer once the next backup starts.
5. Click **Use snapshot on the source to replicate data** if you want the snapshot of the replicated data to be created on the source computer. This method will follow the default replication process. However, snapshots may not be supported on the source computer e.g., root volumes.
6. Click **OK**.



## USE HARDWARE SNAPSHOT

You can choose to use hardware storage arrays to perform SnapProtect operation of the replicated data on the destination computer. The following section provides the steps to be performed for using hardware storage arrays for the SnapProtect operations.

### ENABLE USE OF HARDWARE SNAPSHOT

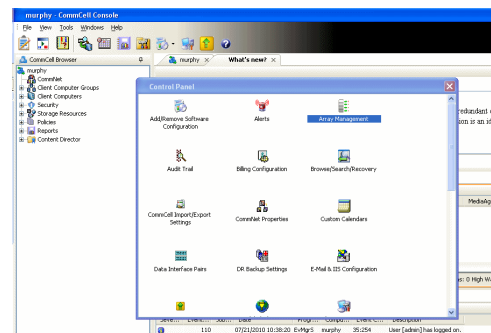
When using a hardware snapshot engine for performing SnapProtect operations, use the steps given below to configure use of hardware storage array.

1. From the CommCell Browser, right-click the snapshot copy that you wish to use for SnapProtect operations and select **Properties**.
2. From the **Data Path Configuration** tab, select the **Use Hardware Snapshot** option to use a hardware storage array to perform SnapProtect backup of the replicated data.
4. Click **OK**.

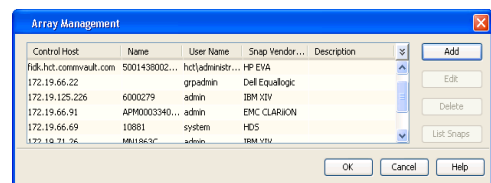
### SETUP THE ARRAY INFORMATION

When using a hardware storage array for performing SnapProtect operations, you need to provide the identification information for the array to ensure access to the array. 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 the hardware storage array from the list of **Snap Vendor** list.

The screenshot shows the 'Array Management' dialog box. The 'Snap Vendor' dropdown menu is highlighted with a red circle. The dialog box contains the following fields: Snap Vendor (dropdown), Name (text), Control Host (text), User Name (text), Password (text), Confirm Password (text), Device Group (text), and a checkbox for 'Use devices only from this device group'. There is also a 'Description' text area and buttons for 'OK', 'Cancel', and 'Help'.

4. Specify the identification information for the array in the **Name** field. The identification information for the array will be based on the storage array that you are using. For example:
- Dell EqualLogic: Specify the Management IP address of the array in this field.
  - EMC Symmetrix/EMC Clariion/IBM XIV/HDS/LSI: Specify the array's serial number in this and the **Control Host** fields.
  - HP EVA: Specify the storage array WWN (for e.g., 50014380025DEB70) in this field.
  - NetApp: Specify the hostname of the array in this field.

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

The screenshot shows the 'Array Management' dialog box. The 'Name' text field is highlighted with a red circle. The dialog box contains the following fields: Snap Vendor (dropdown), Name (text), Control Host (text), User Name (text), Password (text), Confirm Password (text), Device Group (text), and a checkbox for 'Use devices only from this device group'. There is also a 'Description' text area and buttons for 'OK', 'Cancel', and 'Help'.

- 5.
- If applicable, specify the name of the device manager server where the array was configured in the **Control Host** field.
  - Enter the user access information in the **Username** and **Password** fields.
  - If applicable, 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 specify a device group, the default device group will be used for snapshot operations.

For Dell EqualLogic Clone, specify the name of the Storage Pool where you wish to create the clones.

Array Management

Snap Vendor [dropdown]

Name [text box]

Control Host 1 [text box]

User Name 2 [text box]

Password [text box]

Confirm Password [text box]

Device Group 3 [text box]

Use devices only from this device group

Description [text area]

OK Cancel Help

- 6.
- If applicable, 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**.

Array Management

Snap Vendor [dropdown]

Name [text box]

Control Host [text box]

User Name [text box]

Password [text box]

Confirm Password [text box]

Device Group [text box]

1  Use devices only from this device group

2 Description [text area]

3 OK Cancel Help

# Advanced - Nimble

## FAQ

---

### **CAN I REVERT A SNAPSHOT?**

No. When using Nimble storage array, you cannot revert a snapshot.

# SnapProtect™ Backup - Snaptest Tool

## TABLE OF CONTENT

### Overview

#### Usage

Setup Array Configuration  
 Exercise Vendor Snap Engine  
 Detect Snap Engine Type  
 Show HBA/iSCSI Address  
 Send SCSI inquiry to mount point  
 Mount Snapshot on Proxy

## OVERVIEW

The SnapTest tool is used to test the basic snap engine operations like creating, deleting, mounting snapshots etc. It can also be used as a diagnostic tool to verify the host and array connections. The SnapTest tool is capable of working with multiple mount points for each operation and supports an interactive and command line mode.

## USAGE

You can use the SnapTest tool to derive the HBA/iSCSI, the vendor, product, and version details for an array. You can also use the Snaptest tool to:

- create, mount, unmount, delete, revert snapshots for an array.
- test proxy computers by mounting snapshots.

---

## SETUP ARRAY CONFIGURATION

Follow the steps given below to setup array information:

1. Navigate to `<installed_directory>\Base` and double-click **SnapTest.exe**.

2. Press **Enter**.

This tool helps to perform operations such as...

```
-> Automatic Snap Tests
-> Individual Snap Tests
-> Hardware Snapshot Engine Detection
-> SCSI Inquiry
-> Scan HBA/iQN Adapters
```

NOTE: Please make sure that the mount points used for this test are not being used by any other application. If they are in use, it may cause data corruption or data loss. Please refer to our online documentation for list of supported Operating systems, Hardware Snapshot engines and File systems.

Press <ENTER> to continue...

3. Type **2** press **Enter**.

```
SnapTest Version Main Menu

```

Perform automatic snap tests or launch Advanced Operations such as Array Configuration, Snapshot Engine Detection etc. Automatic snap tests take one or more source mounts to snap and performs series of Snap related operations on them. In order to perform these snap operations, array configuration such as array id, control host and user credentials is required. If no array configuration is found, Automatic Snaptests takes you to Array Configuration screen.

```
1. Automatic Snap Tests
2. Advanced Operations
0. Exit
```

Choose your option [1]:

```
SnapTest Version Advanced Operations

```

From this screen you can launch Array Configuration screen or Miscellaneous tasks screen.

4. Type **2** and press **Enter**.

5. Press **Enter** to add a new array.

1. Perform Individual Snap Operations
2. Array Configuration
3. Miscellaneous Tasks
0. Exit

Choose your option [1]:

SnapTest Version      Configure Arrays

-----

All snap operations require array information such as Array ID, User Name and Password etc... Without this information, Snap operations will fail. Configuration changes performed in this screen can be saved to disk so that it is available when the tool is restarted. Password will be encrypted before writing to disk.

1. Add New Array
2. Delete Array
3. Show Existing Arrays
4. Save configuration (If not saved, changes will be lost.)
0. Exit

Choose your option [1]:

SnapTest Version      Add Array

-----

Choose the vendor of your array

1. CommVault
2. Dell Equallogic
3. EMC CLARiiON
4. EMC Celerra
5. EMC Symmetrix
6. HDS
7. HP EVA
8. IBM XIV
9. LSI
10. Native
11. NetApp
0. Exit

Enter Vendor Number [1]:

SnapTest                  Add Array

-----

Vendor : XXX

Enter array ID :

Enter control host name/ip :

Enter user name :

Enter password :

Enter password again :

Enter device group :

6. Specify the number corresponding to the snap engine vendor that you wish to add and press **Enter**.

7. Specify the following information for the detected array:
  - Array ID
  - Control host name/ip
  - User name
  - Password
  - Reenter password
  - Device group
  - Use only devices belonging to the above device group [y/n]

---

## EXERCISE VENDOR SNAP ENGINE

Use the following steps to create, mount, unmount, delete, revert snapshots for an array.

1. Navigate to **<installed\_directory>\Base** and double-click **SnapTest.exe**.
2. Press **Enter**.

This tool helps to perform operations such as...

-> Automatic Snap Tests

-> Individual Snap Tests



3. Type **2** and press **Enter**.

```
-> Hardware Snapshot Engine Detection
-> SCSI Inquiry
-> Scan HBA/iQN Adapters
```

NOTE: Please make sure that the mount points used for this test are not being used by any other application. If they are in use, it may cause data corruption or data loss. Please refer to our online documentation for list of supported Operating systems, Hardware Snapshot engines and File systems.

Press <ENTER> to continue...

```
SnapTest Version Main Menu

```

Perform automatic snap tests or launch Advanced Operations such as Array Configuration, Snapshot Engine Detection etc. Automatic snap tests take one or more source mounts to snap and performs series of Snap related operations on them. In order to perform these snap operations, array configuration such as array id, control host and user credentials is required. If no array configuration is found, Automatic Snaptests takes you to Array Configuration screen.

- 1. Automatic Snap Tests
- 2. Advanced Operations
- 0. Exit

Choose your option [1]:2

4. Press **Enter**.

```
SnapTest Version Advanced Operations

```

From this screen you can launch Array Configuration screen or Miscellaneous tasks screen.

- 1. Perform Individual Snap Operations
- 2. Array Configuration
- 3. Miscellaneous Tasks
- 0. Exit

Choose your option [1]:

5. Specify the number corresponding to the snap engine that you wish to select and press **Enter**.

```
SnapTest Version Snap Engine Test

```

Choose the snap engine you would like to exercise. All the snap tests will use this engine till you choose a different one. If you do not know what engine to choose, choose 'Detect Engine' to find out what engine to choose.

- 1. Native
- 2. HDS Shadow Image
- 3. NetApp
- 4. EMC TimeFinder BCV
- 5. EMC TimeFinder Snap
- 6. EMC CLARiiON Snapview Snap
- 7. EMC CLARiiON Snapview Clone
- 8. HDS Copy on Write Snapshot
- 9. Dell Equallogic Snap
- 10. Data Replicator
- 11. Data Replicator
- 12. HP EVA Snapshot
- 13. HP EVA Clone
- 14. IBM XIV SNAP
- 15. Data Replicator
- 16. LSI Snapshot

6. Specify the operation that you wish to perform. For e.g., specify **1** if you wish to create a snapshot and press **Enter**.

```

17. LSI Volume Copy
18. Dell Equallogic Clone
19. EMC Celerra
20. IBMSVC Space-efficient FlashCopy
21. IBMSVC FlashCopy
22. 3PAR SNAP
23. 3PAR CLONE
24. LSI IBM Snap
25. LSI IBM Clone
26. LSI Dell Snap
27. LSI Dell Clone
28. LSI SGI Snap
29. LSI SGI Clone
30. LSI Sun Snap
31. LSI Sun Clone
32. Detect Engine
0. Exit

```

Enter Engine Number [32]:

```

SnapTest Version Snap Engine Test

```

From this screen, you can launch individual snap operations to exercise the snap engine selected in the previous screen. Exit from this screen to choose a different engine.

```

1. Create Snap
2. Delete Snap
3. Mount Snap
4. Unmount Snap
5. Revert to Snap
6. Save Snaps List
7. Load Snaps List
0. Exit

```

Choose your option [1]:

## DETECT SNAP ENGINE TYPE

Use the following procedure to detect the type of storage array in your environment:

1. Navigate to **<installed\_directory>\Base** and double-click **SnapTest.exe**.
2. Press **Enter**.

This tool helps to perform operations such as...

```

-> Automatic Snap Tests
-> Individual Snap Tests
-> Hardware Snapshot Engine Detection
-> SCSI Inquiry
-> Scan HBA/IQN Adapters

```

NOTE: Please make sure that the mount points used for this test are not being used by any other application. If they are in use, it may cause data corruption or data loss. Please refer to our online documentation for list of supported Operating systems, Hardware Snapshot engines and File systems. Press <ENTER> to continue...

3. Type **2** and press **Enter**.

```

SnapTest Version Main Menu

```

Perform automatic snap tests or launch Advanced Operations such as Array Configuration, Snapshot Engine Detection etc. Automatic snap tests take one or more source mounts to snap and performs series of

4. Type **3** and press **Enter**.

Snap related operations on them. In order to perform these snap operations, array configuration such as array id, control host and user credentials is required. If no array configuration is found, Automatic SnapTests takes you to Array Configuration screen.

- 1. Automatic Snap Tests
- 2. Advanced Operations
- 0. Exit

Choose your option [1]:2

```
SnapTest Version Advanced Operations

```

From this screen you can launch Array Configuration screen or Miscellaneous tasks screen.

- 1. Perform Individual Snap Operations
- 2. Array Configuration
- 3. Miscellaneous Tasks
- 0. Exit

Choose your option [1]:

5. Press **Enter**.

```
SnapTest Version Miscellaneous Tasks

```

From this screen you can launch various miscellaneous tasks that you might need to do while setting up snap feature. For example, you might need to find out HBA adapter address. Or you might need to scan for new devices upon zoning your client with your array. Such tasks can be performed from here.

- 1. Detect Snap Engine Type
- 2. Show HBA/iSCSI address
- 3. Send SCSI inquiry to mount point
- 4. Rescan Adapters
- 5. Delete Devices
- 0. Exit

Choose your option [1]:

6. Specify the source mount path or the device path and press **Enter**.  
The mount path should be specified as <drive>:\. For example, f:\.

```
SnapTest Version Snap Engine Detection

```

Enter source mount path or device path :

7. The snap engine type configured for the mount or device path is displayed.

```
SnapTest Version Snap Engine Detection

```

```
Mount Path : f:\
Underlying Devices : \\.\PhysicalDrive1
Snap Engine for \\.\PhysicalDrive1 : HP EVA Snapshot
Press <ENTER> to continue...
```

## SHOW HBA/iSCSI ADDRESS

Follow the steps given below to derive the HBA/iSCSI information for an array:

1. Navigate to <installed\_directory>\Base and double-click **SnapTest.exe**.
2. Press **Enter**.

This tool helps to perform operations such as...

- > Automatic Snap Tests
- > Individual Snap Tests
- > Hardware Snapshot Engine Detection
- > SCSI Inquiry
- > Scan HBA/iQN Adapters

NOTE: Please make sure that the mount points used for this test are not being used by any other

- 3. Type **2** and press **Enter**.

application. If they are in use, it may cause data corruption or data loss. Please refer to our online documentation for list of supported Operating systems, Hardware Snapshot engines and File systems.  
Press <ENTER> to continue...

```
SnapTest Version Main Menu
```

```

Perform automatic snap tests or launch Advanced
Operations such as Array Configuration, Snapshot
Engine Detection etc. Automatic snap tests take one
or more source mounts to snap and performs series of
Snap related operations on them. In order to perform
these snap operations, array configuration such as
array id, control host and user credentials is
required. If no array configuration is found,
Automatic Snaptests takes you to Array Configuration
screen.
```

- 1. Automatic Snap Tests
- 2. Advanced Operations
- 0. Exit

Choose your option [1]:2

- 4. Type **3** and press **Enter**.

```
SnapTest Version Advanced Operations
```

```

From this screen you can launch Array Configuration
screen or Miscellaneous
tasks screen.
```

- 1. Perform Individual Snap Operations
- 2. Array Configuration
- 3. Miscellaneous Tasks
- 0. Exit

Choose your option [1]:

- 5. Type **2** and press **Enter**.

```
SnapTest Version Miscellaneous Tasks
```

```

From this screen you can launch various
miscellaneous tasks that you might need to do while
setting up snap feature. For example, you might need
to find out HBA adapter address. Or you might need
to scan for new devices upon zoning your client with
your array. Such tasks can be performed from here.
```

- 1. Detect Snap Engine Type
- 2. Show HBA/iSCSI address
- 3. Send SCSI inquiry to mount point
- 4. Rescan Adapters
- 5. Delete Devices
- 0. Exit

Choose your option [1]:

- 6. Press **Enter** to list adapters for a specific array.

```
SnapTest Version List Adapters
```

```

Do you need adapters specific to an Array? [Y/N]
[Y] :
```

- 7. Enter the name of the snap engine.

```
SnapTest Version List Adapters
```

```

Do you need adapters specific to an Array? [Y/N]
[Y] : y
```

Enter Array name :

- 8. The HBA/iSCSI information including the WWPN number for the fiber card is displayed.

---

### SEND SCSI INQUIRY TO MOUNT POINT

Follow the steps given below to derive the vendor information for an array:

1. Navigate to **<installed\_directory>\Base** and double-click **SnapTest.exe**.
2. Press **Enter**.

This tool helps to perform operations such as...

- > Automatic Snap Tests
- > Individual Snap Tests
- > Hardware Snapshot Engine Detection
- > SCSI Inquiry
- > Scan HBA/iQN Adapters

NOTE: Please make sure that the mount points used for this test are not being used by any other application. If they are in use, it may cause data corruption or data loss. Please refer to our online documentation for list of supported Operating systems, Hardware Snapshot engines and File systems.

Press <ENTER> to continue...

3. Type **2** and press **Enter**.

SnapTest Version      Main Menu

-----

Perform automatic snap tests or launch Advanced Operations such as Array Configuration, Snapshot Engine Detection etc. Automatic snap tests take one or more source mounts to snap and performs series of Snap related operations on them. In order to perform these snap operations, array configuration such as array id, control host and user credentials is required. If no array configuration is found, Automatic Snaptests takes you to Array Configuration screen.

- 1. Automatic Snap Tests
- 2. Advanced Operations
- 0. Exit

Choose your option [1]:2

4. Type **3** and press **Enter**.

SnapTest Version      Advanced Operations

-----

From this screen you can launch Array Configuration screen or Miscellaneous tasks screen.

- 1. Perform Individual Snap Operations
- 2. Array Configuration
- 3. Miscellaneous Tasks
- 0. Exit

Choose your option [1]:

5. Type **3** and press **Enter**.

SnapTest Version      Miscellaneous Tasks

-----

From this screen you can launch various miscellaneous tasks that you might need to do while setting up snap feature. For example, you might need to find out HBA adapter address. Or you might need to scan for new devices upon zoning your client with your array. Such tasks can be performed from here.

- 1. Detect Snap Engine Type
- 2. Show HBA/iSCSI address
- 3. Send SCSI inquiry to mount point
- 4. Rescan Adapters
- 5. Delete Devices
- 0. Exit

Choose your option [1]:

6. Specify the drive letter of mount directory and press **Enter**.

SnapTest Version      Send SCSI Inquiry

-----

Enter Mount Point to send SCSI Inquiry :

7. The vendor information, source path, and the mount path details are displayed.

---

## MOUNT SNAPSHOT ON PROXY

Follow the steps below to create a snapshot on your source computer and mount it to a proxy computer:

1. On your source computer, navigate to **<installed\_directory>\Base** and double-click **SnapTest.exe**.
2. Press **Enter**.
3. Type **2** and press **Enter**.
4. Press **Enter**.
5. Specify the number corresponding to the storage that you wish to select and press **Enter**.

This tool helps to perform operations such as...

```
-> Automatic Snap Tests
-> Individual Snap Tests
-> Hardware Snapshot Engine Detection
-> SCSI Inquiry
-> Scan HBA/IQN Adapters
```

NOTE: Please make sure that the mount points used for this test are not being used by any other application. If they are in use, it may cause data corruption or data loss. Please refer to our online documentation for list of supported Operating systems, Hardware Snapshot engines and File systems.

Press <ENTER> to continue...

```
SnapTest Version Main Menu
```

```

```

Perform automatic snap tests or launch Advanced Operations such as Array Configuration, Snapshot Engine Detection etc. Automatic snap tests take one or more source mounts to snap and performs series of Snap related operations on them. In order to perform these snap operations, array configuration such as array id, control host and user credentials is required. If no array configuration is found, Automatic Snaptests takes you to Array Configuration screen.

```
1. Automatic Snap Tests
2. Advanced Operations
0. Exit
```

Choose your option [1]: 2

```
SnapTest Main Operations
```

```

```

From this screen you can perform individual snap operations or miscellaneous tasks.

```
1. Perform Individual Snap Operations
2. Miscellaneous Tasks
0. Exit
```

Choose your option [1]:

```
SnapTest Snap Engine Test
```

```

```

Choose the snap engine you would like to exercise. All the snap tests will use this engine till you choose a different one. If you do not know what engine to choose, choose 'Detect Engine' to find out what engine to choose.

```
1. Native
2. HDS Shadow Image
3. NetApp
4. EMC TimeFinder BCV
5. EMC TimeFinder Snap
6. EMC CLARiiON Snapview Snap
7. EMC CLARiiON Snapview Clone
8. HDS Copy on Write Snapshot
9. Dell Equallogic Snap
10. Data Replicator
11. Data Replicator
```

6. Specify the drive letter of mount directory and press **Enter**.  
 Enter all the mount points that you want to test. Ensure to specify two "\" after the drive letter e.g., E:\\.

7. Press **Enter**.

8. Type **0** and press **Enter** until you exit the tool.
9. Navigate to **<installed\_directory>\Base** and copy the `SnapTestSnapInfo.xml` file to a temporary location on the proxy computer.
10. Connect to the proxy computer and do the following:
- Rename the current `SnapTestSnapInfo` file to `SnapTestSnapInfo_old`.
  - Copy the new `SnapTestSnapInfo.xml` file to the **<installed\_directory>\Base** folder.
  - Double-click **SnapTest.exe** to start the tool.
11. Press **Enter**.

```

12. HP EVA Snapshot
13. HP EVA Clone
14. IBM XIV SNAP
15. Data Replicator
16. LSI Snapshot
17. LSI Volume Copy
18. Dell Equallogic Clone
19. EMC Celerra
20. IBMSVC Space-efficient FlashCopy
21. IBMSVC FlashCopy
22. Dell Compellent Snap
23. 3PAR SNAP
24. 3PAR CLONE
25. LSI IBM Snap
26. LSI IBM Clone
27. LSI Dell Snap
28. LSI Dell Clone
29. LSI SGI Snap
30. LSI SGI Clone
31. LSI Sun Snap
32. LSI Sun Clone
33. Detect Engine
0. Exit

```

```

Enter Engine Number [33]:
Mount points to snap (separate by commas, if more
than one): E:\\

```

```

SnapTest Create Snap

Mount points to snap (separate by commas, if more
than one): E:\\
Creating snapshot... SUCCESS
Press <ENTER> to continue...

```

```

This tool helps to perform operations such as...
-> Automatic Snap Tests
-> Individual Snap Tests
-> Hardware Snapshot Engine Detection
-> SCSI Inquiry
-> Scan HBA/IQN Adapters

NOTE: Please make sure that the mount points used
for this test are not being used by any other
application. If they are in use, it may cause data
corruption or data loss. Please refer to our online
documentation for list of supported Operating
systems, Hardware Snapshot engines and File systems.

Press <ENTER> to continue...

```

12. Type **2** and press **Enter**.

```

SnapTest Version Main Menu

Perform automatic snap tests or launch Advanced
Operations such as Array Configuration, Snapshot
Engine Detection etc. Automatic snap tests take one
or more source mounts to snap and performs series of
Snap related operations on them. In order to perform
these snap operations, array configuration such as
array id, control host and user credentials is
required. If no array configuration is found,
Automatic Snaptests takes you to Array Configuration
screen.

1. Automatic Snap Tests
2. Advanced Operations
0. Exit

Choose your option [1]: 2

```

13. Press **Enter**.

```

SnapTest Main Operations

-
From this screen you can perform individual snap
operations or miscellaneous tasks.

1. Perform Individual Snap Operations
2. Miscellaneous Tasks
0. Exit

Choose your option [1]:

```

14. Specify the number corresponding to the storage that you wish to select and press **Enter**.

```

SnapTest Snap Engine Test

Choose the snap engine you would like to exercise.
All the snap tests will use this engine till you
choose a different one. If you do not know what
engine to choose, choose 'Detect Engine' to find out
what engine to choose.

1. Native
2. HDS Shadow Image
3. NetApp
4. EMC TimeFinder BCV
5. EMC TimeFinder Snap
6. EMC CLARiiON Snapview Snap
7. EMC CLARiiON Snapview Clone
8. HDS Copy on Write Snapshot
9. Dell Equallogic Snap
10. Data Replicator
11. Data Replicator
12. HP EVA Snapshot
13. HP EVA Clone
14. IBM XIV SNAP
15. Data Replicator
16. LSI Snapshot
17. LSI Volume Copy
18. Dell Equallogic Clone
19. EMC Celerra
20. IBMSVC Space-efficient FlashCopy
21. IBMSVC FlashCopy
22. Dell Compellent Snap
23. 3PAR SNAP
24. 3PAR CLONE
25. LSI IBM Snap
26. LSI IBM Clone

```



15. Type **3** and press **Enter**.

```

27. LSI Dell Snap
28. LSI Dell Clone
29. LSI SGI Snap
30. LSI SGI Clone
31. LSI Sun Snap
32. LSI Sun Clone
33. Detect Engine
0. Exit
Enter Engine Number [33]:

```

```

SnapTest Snap Engine Test

-

```

```

From this screen, you can launch individual snap
operations to exercise the snap engine selected in
the previous screen. Exit from this screen to choose
a different engine.

```

```

1. Create Snap
2. Delete Snap
3. Mount Snap
4. Unmount Snap
5. Revert to Snap
6. Save Snaps List
7. Load Snaps List
0. Exit

```

```

Choose your option [1]: 3

```

16. Type the number corresponding to the snapshot you want to mount and press **Enter**.

```

Snap numbers to mount (Separate by commas, if more
than one): 1

```

17. Specify the destination path for the snapshot to be mounted and press **Enter**.

```

Enter Mount point for snapshot 1: c:\mylocation

```

18. Press **Enter**.

```

SnapTest Mount Snap


```

The snapshot is successfully mounted on the proxy computer.

```

Snap numbers to mount (Separate by commas, if more
than one): 1

```

```

Enter Mount point for snapshot 1: c:\mylocation

```

```

Mounting snapshot... SUCCESS
Press <ENTER> to continue...

```

19. Do the following to remove the snapshot after perform the test:

- Type **0** and press **Enter** until you exit the tool.
- Navigate to **<installed\_directory>\Base** and remove the SnapTestSnapInfo.xml file you copied.
- Rename the SnapTestSnapInfo\_old file to SnapTestSnapInfo.

Back to Top

# Best Practices - SnapProtect™ Backup

## VIRTUAL SERVER (VMWARE)

- A separate initiator group must be used for the client, and proxy computers and LUNs should be added to both.
- In case the Virtual Server iDataAgent is no longer required to run data protection operations, it is recommended to release the Virtual Server iDataAgent's license instead of uninstalling it. If the iDataAgent is uninstalled then you will not be able to do the following:
  - Perform Live-Browse.
  - Unmount any Virtual Server iDataAgent mounted snapshots.
- It is recommended that the Virtual Server iDataAgent and MediaAgent be installed on a physical computer in environments leveraging fiber channel storage (required for HDS).
- Storage for iSCSI and NFS must be entered in array management in the same format that it is presented to the ESX servers. (i.e. should storage be connected by IP on the ESX it must be entered by IP in Array Management.)
- When leveraging NFS storage an entry for each IP used will need to be entered into the array management. Entering only a single IP for a management interface is not sufficient.
- The Virtual Server iDataAgent proxy must have access to the storage network. If you have an isolated network, an additional network connection must be added to the proxy.
- It is recommended to use a short name for an NFS datastore. When you perform the SnapProtect backup of an NFS datastore, Calypso can append up to 20 characters with the name of NFS datastore to create the volume label. The ESX server supports a volume label of 42 characters.
- If you have configured datastore affinity for a subclient and if the datastore contains some virtual machines with large disks, the SnapProtect backup of the subclient may take considerably longer time. Also, deleting the snapshots created by the subclient may take long time. In such scenario it is recommended to exclude these virtual machines from the subclient configured with the datastore affinity. To exclude any virtual machine, select the **Do Not Backup** option from the **Guest Host Configuration** dialog box.

You can create a separate subclient under a different backupset to backup these virtual machines.

- It is recommended to create multiple backupsets for the same ESX server or vCenter when using Virtual Server iDataAgent with hardware snapshots. You can configure multiple backupsets as follows:

BackupSet 1 - Use this backupset only for snapshots and not for backup copies. This backupset will provide multiple recovery points and fast recovery from any point-in-time.

BackupSet2 - Use this backupset for regular backups. After performing the first full backup, you can keep on performing incremental backups. You can enable the DASH copy option while creating the secondary copy. The VMware's Change Block Tracking feature is used internally during regular backups. The Change Block Tracking and DASH copy enable faster backups.

This configuration has following advantages:

- A dedicated ESX proxy is not required for creating the backup copy.
- ESX proxy is required only for restoring data from the snapshots.
- You can perform the regular incremental backups and still you will get all benefits of a SnapProtect backup.
- No additional impact on production server or storage.

## ORACLE

- SnapProtect backup for Oracle databases will fail if the mount points are created as symbolic links; so ensure that a mount point is a directory created on the client computer and not a symbolic link.
- Consider the following for ASM based SnapProtect backups:
  - Movement to media is always performed using RMAN.
  - For ASM based SnapProtect backup or movement to media operations, when SnapProtect backup is enabled for RDBMS instance for a subclient, the **Use RMAN for Tape Movement** option is not selected by default. As a work around for this issue, refresh the Client properties or select the **Use RMAN for Tape Movement** option before saving the subclient properties.
  - Before executing any ASM based Snapshot or Movement to media jobs, run the following commands:

```
cd $ORACLE_HOME/rdbsms/lib
```

```
gmake -f ins_rdbms.mk ikfed; ensure that kfed is specified in the path.
```

- Perform an inline backup copy operation prior to modifying the Oracle database schema. This will avoid any backup copy failures due to changes in Oracle database schema.
- If you want to use cross machine auxiliary instance for table level restores from snapshot, make sure that you do not have the database whose name is the same as the source database.
- It is recommended to select both data and log, if you select table browse option in a subclient.

- When you perform a SnapProtect backup, make sure to disable the SSKIPBACKUPBROWSE Registry key.
- When you perform a SnapProtect backup, do not use the same mount point or same LUN for data and logs.
- Static listener must be configured for snap backups, if connect string uses static listener.
- It is recommended to have the control files and redo log locations on a separate volume that is not included in the snap backups for data and logs. As a result, these files are not modified during revert operations thus enabling full complete recovery.

## MICROSOFT SQL SERVER

When performing SnapProtect backup for a SQL on cluster, a proxy server must be used for performing backup and restore operations.

## UNIX FILE SYSTEM

If you have SELinux enabled on the client computer, run the following commands as a root user before performing a SnapProtect backup:

```
chcon -t texrel_shlib_t /opt/<software installation directory>/Base/libIndexing.so
setsebool -P allow_execheap=1
```

## WINDOWS FILE SYSTEM

- When performing a SnapProtect backup, you can use Data Classification or Classic File Scan as the scan method. When using Data Classification, consider the following:
  - If you are using a Snap Proxy, the proxy must have Data Classification Enabler installed.
  - If the DC database is moved to another location, Data Classification will no longer be used as the scan method.
  - Data classification database must reside on the volume being backed up.
- When performing SnapProtect backup for a Windows Cluster, a proxy server must be used for performing backup and restore operations.
- When performing a full system SnapProtect backup for a Windows Server 2008 computer, even though the subclient content does not include any local drive, you should exclude any local drive containing system protected files by creating filters for the subclient. On Windows Server 2008, some of the software installation files are considered as system protected files and therefore the local drive where the software is installed must be excluded from the subclient content.

# Frequently Asked Questions - SnapProtect™ Backup

## TABLE OF CONTENTS

**General**

**Virtual Server (VMware)**

**Microsoft Hyper-V**

**Oracle**

**Microsoft SQL Server**

**NAS**

**SAP for Oracle**

**DB2 (Unix)**

**Unix File System**

**Windows File System**

## GENERAL

---

### HOW DOES THE SNAPPROTECT BACKUP OPERATION WORK?

When you run a SnapProtect backup operation, the Calypso software performs the operations listed below in the following sequence of events:

#### CREATE SNAPSHOT ON THE SOURCE

This event includes the following operations:

1. Device detection based on subclient content.

This operation gathers information from local volume managers, multipath devices and physical disks (including partitions). For example, information on UUIDs is retrieved from a local volume manager.

2. Take snapshot of detected devices

This operation invokes the snapshot functions from the file server and creates the snapshot. Once created, Calypso records the snapshot in the CommServe database along with metadata, which includes information about local volume managers, multipaths and physical disks.

#### MOUNT SNAPSHOT ON PROXY

This event includes the following operations:

1. Map LUNs to the MediaAgent

This operation invokes the file server functions to map clone devices to the proxy MediaAgent.

2. Recreate Storage Hierarchy

Based on the metadata collected during device detection and snapshot creation, Calypso recreates the storage hierarchy as follows:

- Devices are rescanned at the operating system level in order to allow the proxy to see the snapshot LUNs.
- For each device detected on the source, Calypso checks the partitions to determine if the device is accessible or if it is a multipath device. If it is a multipath device, then the operation fails as partitions on multipath are not supported. However, if it is not a multipath device, then the software will keep parsing the device name to retrieve the partition information.

When a partition number is detected, it is appended to the device name of the LUN. If no partition number is found, the full device name is used.

- If required, the hierarchy of the local volume manager is recreated based on the metadata collected during device detection and snapshot creation.
- File systems (LUNs and multipath disks) are mounted on the detected devices. Logical volumes are mounted in the case of logical volume managers.
- Index is created and the software moves the data to the media.

---

### WHAT PROVISIONING POLICIES CAN I USE?

Provisioning Policies are optional to use. During the creation of the secondary snapshot copy, the following Provisioning Policies are automatically created and available for selection in the CommCell Console:

- **SnapProtect\_RAID-DP**
- **SnapProtect\_Dedupe**
- **SnapProtect\_Mirror\_Destination**

If you need to create your own provisioning policy, ensure it is defined with the following naming convention in the DFM server:

SnapProtect\_<provisioning\_policy\_name>

where "SnapProtect\_" is the prefix required for the provisioning policy to be available in the SnapProtect software.

---

### WHAT HAPPENS WHEN A VAULT/MIRROR COPY IS CREATED?

During an Auxiliary Copy job, a new dataset is created or an existing dataset is modified with new data members, as explained in the following flow of events:

1. When the SnapProtect software assigns data to the service catalogue, a new baseline transfer may have started in the Data Fabric Manager (DFM) server.
2. The Auxiliary Copy job details display its status as the baseline transfer is in progress.
3. Once the baseline transfer is completed, the SnapProtect software adds the snaps to the backup list, and the backup starts with the DFM.
4. If SnapMirror is the destination copy, then the SnapProtect software sends a command to update the mirror.

The DFM job is monitored and marked as completed/failed depending on the DFM job status.

---

### HOW ARE SNAPSHOTS COPIED DURING A BACKUP COPY OPERATION?

The snapshots are copied to media in a sequential order. If you wish to perform an inline backup copy operation and a previously selected snapshot has not been copied to media, the current SnapProtect backup job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

---

### HOW CAN I BACK UP AND RESTORE ALL VIRTUAL MACHINES WITHIN A SPECIFIC DATASTORE?

All virtual machines in a specific datastore can be backed up and restored together as follows:

1. Create a new subclient that will be dedicated to the datastore containing the virtual machines you want to back up. Consider giving this subclient the name of the datastore you are backing up for easy identification in the CommCell Console. Refer to [Creating User-Defined Subclients](#) for complete step-by-step instructions.
2. From the backup set in which the new subclient is created, configure automatic discovery of virtual machines based on datastore affinity. You can then assign the desired datastore to the new subclient. Refer to [Discover by Datastore Affinity](#) for complete step-by-step instructions.
3. Schedule routine backups of the subclient. Refer to [Scheduling a Backup](#) for complete step-by-step instructions.
4. When a restore is needed, you can restore all virtual machines within the datastore by performing a browse operation on the subclient, selecting all virtual machines displayed in the **Browse** window, and selecting either the original datastore or a new datastore as the destination from the **Restore Options** dialog box.

Refer to the following for complete step-by-step instructions:

- Restoring Virtual Machines to Same Destination (In-Place Restore) - This procedure describes the steps in restoring the virtual machines to the exact location from which they were backed up.
- Restoring Virtual Machines to Different Destination (Out-of-place Restore) - Different Datastore - This procedure describes the steps in restoring the virtual machines to a different datastore of your choice.

The above-mentioned steps can also be customized to group backups and restores of other entities, such as ESX Server, Resource Pools, etc.

---

### WHAT SHOULD I TAKE INTO ACCOUNT WHEN USING RETENTION BY NUMBER OF JOBS?

Configuring a storage policy or snapshot copy with job based retention is recommended for File System and File System like Agents, and not for Database Agents.

Review the following scenarios if you are using the retention by number of jobs configuration:

- During a browse operation, deleted files may be displayed for recovery. If the jobs containing these files are pruned by the retention criteria, the deleted files will be irrecoverable.
- You may need to manually delete jobs from deconfigured clients. These clients will continue to retain the old jobs since new jobs will not run again on them.
- When you associate a new storage policy to a subclient, it is important to perform a full backup operation in order to be retained by the new storage policy. The old storage policy will continue to retain the old jobs until you manually delete them.

---

### WHAT UTF SETTING SHOULD BE USED FOR VOLUME LANGUAGE?

To successfully browse and restore files on a NetApp file server that contain Unicode characters, it is recommended to use the UTF-8 setting for volume language. Please consult with NetApp for implications of changing volume language.

---

### HOW IS THE DATA FABRIC MANAGER SERVER AFFECTED WHEN A SNAP COPY IS DELETED?

If you delete a snapshot copy, the following components in the DataFabric Manager server will be affected:

- The storage services associated to the snapshot copy will be deleted.

- Datasets associated with the deleted storage service will be deleted.

Secondary volumes/datasets are not deleted as they are stored in case you need to perform a restore operation from a deleted dataset. Secondary datasets can be removed manually, if needed.

- Any relationship associated with a dataset will be deleted within a configurable period of time defined in the DataFabric Manager server.
- Base snapshot copies remain available.

### IS MULTI INSTANCING SUPPORTED?

No. Multi Instancing is not supported for SnapProtect backup.

### CAN I USE MEDIA EXPLORER TO RESTORE DATA?

No. Restore of SnapProtect backup data using Media Explorer is not supported. However, Media Explorer can be used to restore SnapProtect backup data from the Primary Copy.

### HOW DO I DETERMINE THE NUMBER OF STREAMS TO BE USED FOR A RESTORE OPERATION FROM A SNAPPROTECT BACKUP?

For DB2, SAP for Oracle, and Oracle iDataAgents, when restoring from a snapshot using file system, the number of streams depends on the number of mount points used for the restore operation. Similarly, when restoring from a backup copy using file system, the number of streams depends on the number of media groups used for the restore operation.

### CAN I PERFORM A SNAPPROTECT BACKUP OF RDM DISKS FOR AN AGENT FROM A VIRTUAL MACHINE HOST?

Yes. It is supported to run a SnapProtect backup operation of Raw Device Map (RDM) disks for any Windows-based Agent configured in a virtual machine. Ensure the iSCSI Initiator is configured on the client computer to access the storage device in order to perform a successful SnapProtect operation.

### WHAT ARE THE COMMANDS USED FOR DEVICE DISCOVERY?

During a SnapProtect backup job, the Calypso software runs a set of commands to discover storage devices.

The following table displays the commands that are used to list, rescan and delete adapters/devices for each operating system:

| OPERATING SYSTEM | LIST FIBRE CHANNEL ADAPTERS | RESCAN FIBRE CHANNEL ADAPTERS                                                                                                                                                                                                                                                | RESCAN ISCSI DEVICES                                                                                                                                                                                                                                                                                                 | DELETE DEVICE                                                                                                                                                                                                                                                                                                                   |
|------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AIX</b>       | <Base>/scan_fc_adapters.sh  | cfgmgr -l <hba_name>                                                                                                                                                                                                                                                         | cfgmgr -l <iscsi_adapter>                                                                                                                                                                                                                                                                                            | rmdev -d -l <hdisk_name>                                                                                                                                                                                                                                                                                                        |
| <b>HP-UX</b>     | <Base>/scan_fc_adapters.sh  | <ol style="list-style-type: none"> <li>1. Obtain the path for the host bus adapter (HBA):<br/>ioscan -unfc fc</li> <li>2. Scan the HBA path<br/>ioscan -H &lt;HBA_path&gt;</li> </ol>                                                                                        |                                                                                                                                                                                                                                                                                                                      | For Legacy HP-UX (earlier than 11.2):<br>rmsf -a <device><br><br>For non-Legacy HP-UX:<br><ol style="list-style-type: none"> <li>1. Obtain persistent name mapping<br/>ioscan -m dsf</li> <li>2. Check device availability:<br/>ioscan -kNF &lt;device&gt;</li> <li>3. Delete the device:<br/>rmsf -H &lt;device&gt;</li> </ol> |
| <b>LINUX</b>     | <Base>/scan_fc_adapters.sh  | <ol style="list-style-type: none"> <li>1. Perform the hardware loop initialization (LIP):<br/>echo 1<br/>&gt; /sys/class/fc_host/&lt;host&gt;/issue_lip</li> <li>2. Perform a SCSI mid-level rescan:<br/>echo '---'<br/>&gt; /sys/class/fc_host/&lt;host&gt;/scan</li> </ol> | <ul style="list-style-type: none"> <li>• For Red Hat 4 computers:<br/>/sbin/iscsi -rescan</li> <li>• For SuSE Linux 9 computers:<br/>/etc/init.d/iscsi reload /bin/rescan-scsi-bus.sh -r -L 512 -w -c -- nooptscan</li> <li>• For SuSE Linux 10 and Red Hat 5 computers:<br/>/sbin/iscsiadm -m session -R</li> </ul> | echo 1<br>> /sys/block/<device>/device/de                                                                                                                                                                                                                                                                                       |
| <b>SOLARIS</b>   | <Base>/scan_fc_adapters.sh  | cfgadm -c configure <controller>                                                                                                                                                                                                                                             | devfsadm -i iscsi                                                                                                                                                                                                                                                                                                    | devfsadm -C -c disk                                                                                                                                                                                                                                                                                                             |

## CAN I CREATE MY OWN COMMANDS TO PERFORM DEVICE DISCOVERY?

Yes, you can customize the device deletion and the rescan logic by creating the following registry keys:

| KEY          | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeleteDevice | <p>This key will trigger a custom script which will perform an OS level device deletion. Once all the devices are removed, the Calypso software will remove the LUNs from the storage arrays.</p> <p>Use this key if you need to unmount snapshots that are mapped to either the proxy or source machine. The key will delete all devices mapped to the machine.</p> <p>Follow the steps below to create this registry key:</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, navigate to <b>Client Computers</b>.</li> <li>2. Right-click the &lt;<b>Client</b>&gt;, and the click <b>Properties</b>.</li> <li>3. Click the <b>Registry Key Settings</b> tab.</li> <li>4. Click <b>Add</b>.</li> <li>5. In the <b>Name</b> box, type DeleteDevice.</li> <li>6. In the <b>Location</b> box, select or type the iDataAgent.</li> <li>7. In the <b>Type</b> box, select <b>Value</b>.</li> <li>8. In the <b>Value</b> box, type the full path to the script. The device name will be passed as an argument.</li> <li>9. Click <b>OK</b>.</li> </ol> |
| RefreshBus   | <p>This key will trigger a custom script for each host bus adapter that needs to be rescanned.</p> <p>Use this key if you need to rescan the machine for any new devices each time a snapshot is mounted or unmounted.</p> <p>Follow the steps below to create this registry key:</p> <ol style="list-style-type: none"> <li>1. From the CommCell Browser, navigate to <b>Client Computers</b>.</li> <li>2. Right-click the &lt;<b>Client</b>&gt;, and the click <b>Properties</b>.</li> <li>3. Click the <b>Registry Key Settings</b> tab.</li> <li>4. Click <b>Add</b>.</li> <li>5. In the <b>Name</b> box, type RefreshBus.</li> <li>6. In the <b>Location</b> box, select or type the iDataAgent.</li> <li>7. In the <b>Type</b> box, select <b>Value</b>.</li> <li>8. In the <b>Value</b> box, type the full path to the script. The WWPN of the adapter will be passed as an argument.</li> <li>9. Click <b>OK</b>.</li> </ol>                                                                                                                                     |

After creating the above registry keys, you can use the following script examples:

### ON LINUX COMPUTERS

```
#-----
#Example 1: Linux Rescan Script to be used by RefreshBUS key
#-----
#!/bin/sh
hba_wwpn=$1
#This line sets $Fc_adapter. (See o/p of scan_fc_adapters.sh)
eval ` /opt/simpana/Base/scan_fc_adapters.sh | grep $hba_wwpn | awk '{print $1}' `

#Add your own custom commands here.

#Perform scsi midlevel rescan. (May not be needed if you have your custom scan command above).
echo '- - -' > /sys/class/scsi_host/${Fc_adapter}/scan
exit 0

#-----
```

### ON AIX COMPUTERS

```

#-----
#Example 1: AIX Rescan Script to be used by RefreshBUS key
#-----
#!/bin/sh
hba_wwpn=$1
#This line sets $Fc_adapter. (See o/p of scan_fc_adapters.sh)
eval ` /opt/simpana/Base/scan_fc_adapters.sh | grep $hba_wwpn | awk '{print $1}' `

#Add your own custom commands here.

#Perform scan using cfgmgr (May not be needed if you have your custom scan command above).
cfgmgr -l $Fc_adapter
exit 0

#-----

```

## HOW DOES CALYPSO SELECT TARGET DEVICES DURING CLONE/SNAP OPERATIONS?

When you configure an storage device using Array Management in the CommCell Console, the **Device Group** text box defines the target device group where Calypso will move the source and target devices during SnapProtect backup operations. This option does not specify the source device group (from where a device should be found during Snap/Clone operations).

The following table explains the default behavior for selecting a Snap or Clone target device:

| SCENARIOS BASED ON ARRAY MANAGEMENT OPTIONS                                                            | TARGET DEVICE IS SELECTED FROM...                 | SOURCE AND TARGET DEVICES ARE MOVED TO...         |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------|---------------------------------------------------|
| <b>Device Group</b> is not specified and <b>Use devices only from this device group</b> is not checked | Any device in the array                           | CV_PROTECTION_GROUP device group                  |
| <b>Device Group</b> is not specified but <b>Use devices only from this device group</b> is checked     | CV_PROTECTION_GROUP device group                  | CV_PROTECTION_GROUP device group                  |
| <b>Device Group</b> is specified but <b>Use devices only from this device group</b> is not checked     | Any device in the array                           | The device group specified in <b>Device Group</b> |
| <b>Device Group</b> is specified and <b>Use devices only from this device group</b> is checked         | The device group specified in <b>Device Group</b> | The device group specified in <b>Device Group</b> |

## CAN I BACKUP PHYSICAL RDMs IN A VIRTUAL MACHINE USING SNAPPROTTECT?

Yes. You can use File System *iDataAgent* and perform the SnapProtect operation to backup the physical RDMs in the following scenario:

- The datastore of the physical RDM is located on a NetApp storage array.
- The host of the virtual machine has ESX server version 5.0
- The MediaAgent, used for a SnapProtect operation, is installed on a physical computer and not on a virtual machine.
- The virtual machine has File System *iDataAgent* and Exchange Database *iDataAgent* installed on it.

## VIRTUAL SERVER (VMWARE)

### CAN I USE A DIFFERENT ESX SERVER FOR SNAP MOUNT DURING RESTORES OR MOVING TO TAPE?

Yes, you can override the default restore selection by choosing a different Virtual Centre or ESX Server to restore or moving to tape, by following the steps given below:

1. From the CommCell Console, right-click the **Subclient** and select **Browse Backup Data**.
2. Click **OK** and select the virtual machine under the backupset. Its entire contents will be automatically selected in the right pane. Click **Recover All Selected**.
3. Click on the **Advanced** from the **Restore Options** dialog box.
4. Select the **ESX Browse** tab.
5. The **Default Selection** has the IP address of the ESX Server pre-populated.
6. Select **Override Default Selection** to locate a different destination.
7. Enter appropriate credentials to logon to the server using **Configure Password** button.
8. Click **Browse VirtualCenter/ESX Servers for destination** to provide the ESX Server path to which the virtual machine will be restored.
9. Select the appropriate ESX server.
10. Click **OK** to close the **Browse for ESX Server** dialog.



- Click **OK** to close the **Advanced Restore Options** dialog.

### DOES A VIRTUAL SERVER CLIENT SUPPORT ADVANCED TRANSPORT MODES FOR SNAPPROTECT OPERATIONS?

Yes, the Virtual Server client can support advanced transport modes like SAN during restores and mounting operations, if configured as follows:

- The Virtual Server client machine should be physical server.
- LUNs on which the virtual machine is created should be exposed to the Virtual Server proxy client.
- The Virtual Server client is connected through iSCSI or Fiber Channel.

### HOW DO BACKUP AND RESTORE OPERATIONS HANDLE INDEPENDENT/RDM DISKS?

If a virtual machine undergoing a backup job includes independent disks, physical or virtual RDMs, these disks will be skipped. During a full VM restore the independent disk/Physical or virtual RDMs will get restored as a regular disk with 0MB data.

If a subclient contains virtual machines with independent disks/physical or virtual RDMs, the backup job will always complete with the status "Completed w/ one or more errors". However, if you create the IgnoreUnsupportedDisks registry key on the proxy computer, the backup job will complete successfully.

### HOW DO BACKUP AND RESTORE OPERATIONS HANDLE VIRTUAL RDM DISKS?

Virtual RDMs are protected by the backup job (but not during IntelliSnap backup). However at the time of restore, the data is restored as a regular VMDK on a datastore. A virtual RDM is not re-created and the data is not restored to the virtual RDM's device.

### CAN I PERFORM A SNAPPROTECT BACKUP OF A WINDOWS 2008 R2 VIRTUAL MACHINE?

Yes. To successfully run a SnapProtect backup of a virtual machine with Windows 2008 R2, ensure that if the virtual machine resides on a single datastore it is not spread across multiple folders.

If the virtual machine is spanned across multiple datastores, you can run SnapProtect backups for virtual machines with ESX version 4.1 (or higher) by configuring the VM using the steps below:

- Power off the virtual machine.
- From the VI client, right-click the virtual machine and select **Edit Settings**.
- Click the **Options** tab.
- From the list of settings, select **General** located under the **Advanced** setting. Then click the **Configuration Parameters** button on the right pane.
- From the **Configuration Parameter** dialog box, click the `Disk.EnableUUID` parameter and set it to false.
- Click **OK**.

### CAN I CONFIGURE THE VIRTUAL MACHINE TO INCLUDE THE ROOT VOLUME OF A FILE SERVER?

No, data that resides on the root volume cannot be part of the virtual machine content.

### CAN I CONFIGURE ARCHIVE LOG DESTINATION WITH A DIFFERENT PATTERN FOR SNAP PROTECT OPERATIONS?

No. The archive log destination should be a valid directory for snap. Snap protect operation will not work if you configure the archive log destination with a different pattern such as `log_Archive_dest_1='location=/archivelog/db_'`.

### HOW IS VM BACKUP SIZE CALCULATED FOR CAPACITY LICENSING?

For VM backups, capacity licensing is based on the total backup size, calculated as the sum of backup sizes for all VM backup jobs after white spaces (blocks of zeros) are removed. The license counts the backup size of all configured subclients; virtual machines that are included in multiple subclients will be counted multiple times. The backup size is measured for usage tracking and shown on the Backup Job Summary Report.

The backup size can be different from the guest host size or used space value shown for the VM in the disk properties dialog by Microsoft Windows.

The following factors can affect the backup size calculation:

- The presence of virtual machine snapshots.
- The presence of sparse files or deleted files in the guest can cause the backup size to vary.
- The backup size reported for VMDKs in a VM can vary depending on white space and change allocation tracking for that VM.

For example:

- A Windows VM with a single volume of 80 GB has 30 GB occupied and 50 GB free.
- The guest size would be 30 GB.
- The backup size is the amount of data transferred and written for that backup, which can be up to 80 GB.

The backup size reflects the size after eliminating white spaces; but data that was written and deleted still counts as reserved (allocated) space. The layering effects of multiple virtual file systems can cause differences between the size reported by the guest host running within the VM and the reported backup size. Frequent deletion of large files can easily cause these numbers to be out of sync.

Version 9.0 reports on all allocated blocks in the VM. The amount reported for allocated blocks can be the same size or larger than what is actually in use and can contain reserved space for deleted items. For each VMware instance, Version 9.0 has an additional reporting column of the actual size of VMs.

The following measures can help reduce backup size:

- Delete or move unnecessary data before virtualizing physical machines. This saves resources and time, and ensures that new VMs only contain used blocks.
- If you already have a large number of VMs with significant reserved and unused blocks, use a tool such as the Windows SDelete utility to release reserved space on VMs, as described in SDelete v1.61.
- Ensure that VM templates used for provisioning do not contain unreferenced blocks in the VMDK.
- Wherever possible, configure virtual machine disks with the VMware Thin Provisioned disk option enabled. Thin provisioning ensures only valid blocks occupy space in the VMDK file. With thin provisioned VMs, VMware APIs only return occupied blocks.

## MICROSOFT HYPER-V

### HOW IS VM BACKUP SIZE CALCULATED FOR CAPACITY LICENSING?

For VM backups, capacity licensing is based on the total backup size, calculated as the sum of backup sizes for all VM backup jobs after white spaces (blocks of zeros) are removed. The license counts the backup size of all configured subclients; virtual machines that are included in multiple subclients will be counted multiple times. The backup size is measured for usage tracking and shown on the Backup Job Summary Report.

The backup size can be different from the guest host size or used space value shown for the VM in the disk properties dialog by Microsoft Windows.

The following factors can affect the backup size calculation:

- The presence of virtual machine snapshots.
- The presence of sparse files or deleted files in the guest can cause the backup size to vary.
- The backup size reported for VMDKs in a VM can vary depending on white space and change allocation tracking for that VM.

For example:

- A Windows VM with a single volume of 80 GB has 30 GB occupied and 50 GB free.
- The guest size would be 30 GB.
- The backup size is the amount of data transferred and written for that backup, which can be up to 80 GB.

The backup size reflects the size after eliminating white spaces; but data that was written and deleted still counts as reserved (allocated) space. The layering effects of multiple virtual file systems can cause differences between the size reported by the guest host running within the VM and the reported backup size. Frequent deletion of large files can easily cause these numbers to be out of sync.

Version 9.0 reports on all allocated blocks in the VM. The amount reported for allocated blocks can be the same size or larger than what is actually in use and can contain reserved space for deleted items. For each VMware instance, Version 9.0 has an additional reporting column of the actual size of VMs.

The following measures can help reduce backup size:

- Delete or move unnecessary data before virtualizing physical machines. This saves resources and time, and ensures that new VMs only contain used blocks.
- If you already have a large number of VMs with significant reserved and unused blocks, use a tool such as the Windows SDelete utility to release reserved space on VMs, as described in SDelete v1.61.
- Ensure that VM templates used for provisioning do not contain unreferenced blocks in the VMDK.
- Wherever possible, configure virtual machine disks with the VMware Thin Provisioned disk option enabled. Thin provisioning ensures only valid blocks occupy space in the VMDK file. With thin provisioned VMs, VMware APIs only return occupied blocks.

## ORACLE

### CAN I USE THE ORACLE AGENT TO PERFORM A SNAPPROTECT BACKUP OF AN ORACLE RAC CLIENT?

Yes, you can perform SnapProtect operations for a single node Oracle RAC setup. The following configurations are required:

- When configuring the Oracle RAC components for the first SnapProtect backup, ensure that:
  - The Oracle instance is configured on one of the physical nodes for the Oracle RAC agent.
  - If the data and archive logs do not reside on a shared location, create a user-defined subclient for the archive logs and run a backup using RMAN. The original subclient should only include the data volume in order to perform a SnapProtect backup.
  - The **Use RMAN for Tape Movement** option is selected during the subclient configuration if you plan to backup the archive logs.
- The ASM Oracle Database should be located on a ASM disk group, and the underlying disks should be snap-able.
- If you plan to use RMAN for copying the data to the media on the proxy computer, copy the Oracle parameter file (pfile) from the client to the proxy

computer's \$ORACLE\_HOME/dbs/ directory, and remove any parameter containing Oracle RAC related entries. For example:

- cluster\_database\_instances
- cluster\_database
- <RAC Instance name>.thread
- <RAC Instance name>.local\_listener
- <RAC Instance name>.instance\_number

### **CAN I USE A SEPARATE PROXY TO PERFORM A BACKUP COPY?**

No. The **Use Separate Proxy for Snap to Tape** option in Subclient Properties is not supported for the Oracle iDataAgent.

### **CAN WE RESTORE A POINT IN TIME SNAPPROTECT BACKUP, IF COPY PRECEDENCE IS NOT SELECTED?**

Generally, we can set copy precedence for storage policy. The copy that is set to a copy precedence of 1 will be restored. However, if a snapprotect backup job is available, then it won't consider the copy precedence and restores only from the snapprotect backup.

### **CAN I PERFORM AN INCREMENTAL BACKUP COPY?**

Yes. You can perform an incremental backup copy using RMAN.

### **IF THE DATABASE AND INSTANCE NAME ARE DIFFERENT, CAN I PERFORM A TABLE LEVEL RESTORE?**

No. The table level restores will not work, if the database and instance names are different.

### **CAN WE PREVENT THE SINGLE VOLUME REVERT WHEN THE DATABASE IS SPANNED ACROSS THE MULTIPLE VOLUMES?**

No. You cannot prevent a single volume revert when the database is spanned across multiple volumes. When you perform a hard revert, the database will not be restored as the reversion happens at LUN level and the other source paths related to this database are not reverted. Hence, we recommend Restore by Revert which is application aware instead of regular revert using the CommCell Console (GUI).

The following steps explain the current process of reversion for a single volume when the database is spanned across multiple volumes:

1. Create two Logical Unit Numbers (LUNs) from the same volume and another LUN from a different Volume.
2. Create host volume from each LUN or two LUNs from the same volume. Create two LUNs from a different Volume and host volumes (partitioned disks) from each LUN.
3. Create multiple mount points and mount the File System created from above LUNs.
4. Create a database on these mount points and create table spaces spanned across these locations.
5. Perform a SnapProtect backup for the database.
6. Perform a SnapProtect backup after adding data and tables.
7. Select all source paths related to LUN at previous Job ID and perform the hardware revert.

### **CAN I CONFIGURE THE ORACLE DATABASE TO INCLUDE THE ROOT VOLUME OF A FILE SERVER?**

No. The data that resides on the root volume cannot be part of the Oracle database content.

### **CAN I PERFORM A LOG ONLY RESTORE FOR ASM DATABASE?**

No. Log Only restore is not supported for ASM database.

### **IS THE SOFTLINK PATH SUPPORTED FOR SNAPPROTECT OPERATION?**

No. Softlinks are not supported for this iDataAgent's datafile paths and archive log location. you should use the real paths.

You can create alias device using `mknod` for raw devices.

### **HOW DO I DETERMINE THE SUPPORTED INTELLISNAP OPERATIONS BASED ON THE LOCATION OF THE ORACLE APPLICATION, DATA AND LOG VOLUMES ON THE CLIENT?**

The following table displays the supported IntelliSnap operations based on the location of the Oracle Application, Data and Log volumes on the client :

| OPERATION | ORACLE APPLICATION / DATA / LOG ARE ON THE | ORACLE APP IS ON DIFFERENT DEVICE / | ORACLE APPLICATION, DATA AND LOG ARE ON | NOTES |
|-----------|--------------------------------------------|-------------------------------------|-----------------------------------------|-------|
|           |                                            |                                     |                                         |       |

|                                     | <b>SAME PHYSICAL<br/>DISK/VOLUME GROUP</b> | <b>VOLUME GROUP BUT<br/>ORACLE DATA AND LOG<br/>ON SAME PHYSICAL<br/>DISK / VOLUME GROUP</b> | <b>DIFFERENT PHYSICAL<br/>DISKS / VOLUME<br/>GROUPS (RECOMMENDED<br/>CONFIGURATION)</b> |                                                                                                                                   |
|-------------------------------------|--------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| IntelliSnap Backup                  | Supported                                  | Supported                                                                                    | Supported                                                                               |                                                                                                                                   |
| Backup Copy                         | Supported                                  | Supported                                                                                    | Supported                                                                               |                                                                                                                                   |
| IntelliSnap Restore                 | Supported                                  | Supported                                                                                    | Supported                                                                               |                                                                                                                                   |
| Volume level Revert                 | Not Supported                              | Supported (based on Array Support)                                                           | Supported                                                                               | For NetApp array, if data and log are on the same volume, log snap will be deleted automatically after reverting the data volume. |
| File Level Revert (NetApp NFS only) | Supported                                  | Supported                                                                                    | Supported                                                                               |                                                                                                                                   |

If data and logs are on same volume/disk, multiple snaps will be taken in data phase and log phase separately.

## Multi Instance Snap Optimization

### CAN WE REVERT FROM SNAP, IF THE SNAP AND CLONE ARE PRESENT ON THE SAME DEVICE?

If the SnapProtect backup and Clone exist for the same source device in the case of EMC Symmetrix, the revert operation from SnapProtect backup will work. However, the revert from clone will not work until all the snap sessions are terminated.

### CAN WE PERFORM A LOG ONLY SNAPPROTECT BACKUP IN A MULTIPLE INSTANCES ENVIRONMENT USING A SHARED STORAGE ON A CLIENT?

No. Currently, the Log only SnapProtect backup is not supported for multiple instances using a shared storage on a client

### CAN WE PERFORM A TABLE LEVEL AND ASM SNAPPROTECT BACKUPS IN A MULTIPLE INSTANCES ENVIRONMENT USING A SHARED STORAGE ON A CLIENT?

No. Currently, the table level and ASM SnapProtect backups are not supported in a multiple instances environment using a shared storage on a client.

## MICROSOFT SQL SERVER

### ARE THERE ANY CONSIDERATIONS FOR A SQL DATABASE BACKUP?

- Transactional Log backups always use the traditional backup method. Log backups are stored in the Primary (classic) copy.
- The SQL Writer does not support the following:
  - Log Backups
  - File and filegroup backup
  - Page Restore

## NAS

### CAN I BACKUP DATA RESIDING ON A VFILER?

Yes. If the data you want to backup resides on a vFiler, set it up as follows:

1. Add the vFiler as a NAS client as explained in the Getting Started - NAS Configuration procedure.
  - If you plan to add more vFilers as NAS clients, ensure they have unique names. vFilers with the same name are not supported.
2. During the NAS client configuration, ensure not to include the vFiler root volume in the subclient content.
3. When performing a backup, indexing is supported if the physical file server (where the vFiler resides) has been specified in Array Management. If not, ensure you select the **Skip Catalog phase for SnapProtect** option during backup as indexing will not be supported.
4. To restore the data, create a backup copy as explained in the Snap Movement to Media procedure and restore the files and volumes from the backup copy.
5. Other operations you can also perform with the snapshot are mount and revert operations.

### CAN I CONFIGURE A SUBCLIENT TO INCLUDE THE ROOT VOLUME OF A FILE SERVER?

No, data that resides on the root volume cannot be part of the NAS subclient content.

**CAN I USE A VFILER AS DESTINATION FOR SNAPVAULT/SNAPMIRROR COPIES?**

No. vFilers cannot be the destination location for SnapVault/SnapMirror copies as it is not supported by the DataFabric Manager.

**CAN I USE THE FILE SYSTEM NRE FOR NAS RESTORES?**

No. Restore of NAS data to a Windows or Unix computer using File System NDMP Restore Enabler (NRE) is not supported for NAS iDataAgent snapshots.

**CAN I ENABLE THE IMAGE BACKUP SET OPTION ON A SNAPVAULT COPY?**

Yes, you can enable the **Image Backup Set** option (for SnapMirror to Tape) on a backup set containing the SnapVault copy. However, the image backup of the SnapVault copy will not exactly match the primary (source) volume. For example, the non-qtrees data on the primary volume will be in a qtree on the SnapVault copy; the SnapVault copy may also contain data from other primary volumes.

**CAN I RESTORE TO A CLIENT FROM A NAS SNAPSHOT?**

No. Restores from NAS Snapshots are not supported. You can restore to a client from a NAS backup copy.

**SAP FOR ORACLE****HOW CAN I INCREASE THE NUMBER OF SNAPSHOTS CREATED FOR A USP VOLUME?**

The maximum number of snapshots created for a USP volume is 3. When using the HDS storage array with SAP for Oracle, you can have up to 4 snapshots on the same volume if you store the Data (\$SAPDATA\_HOME) and Config (\$ORACLE\_HOME/dbs) directories in the same volume.

**IS THE SOFTLINK PATH SUPPORTED FOR SNAPPROTECT OPERATION?**

No. Softlinks are not supported for this iDataAgent's datafile paths and archive log location. you should use the real paths.

**DB2 (UNIX)****CAN I RESTORE DATA AND LOG FILES?**

No. During a SnapProtect backup, log files are not moved to the snapshot copy even if the **Backup Log Files** option is selected on the subclient where the backup operation is being performed. Log files always use the traditional backup method, not the SnapProtect backup.

Running a restore operation from the snapshot copy will fail because the log data will not be found. If you want to restore both data and logs, modify the copy precedence to restore from the **Primary(Classic)** copy.

**IS THE SOFTLINK PATH SUPPORTED FOR SNAPPROTECT OPERATION?**

No. Softlinks are not supported for this iDataAgent's datafile paths and archive log location. you should use the real paths.

**UNIX FILE SYSTEM****CAN I INCLUDE ROOT FOLDER (/) AS SUBCLIENT CONTENT FOR SNAPPROTECT?**

No, root folder (/) should not be included as subclient content for SnapProtect.

**WHAT NON-NATIVE FC DRIVERS ARE SUPPORTED?**

Qlogic SANSurfer CLI on SuSE Linux Enterprise Server 10 SP2.

**CAN I PERFORM A CROSS PLATFORM RESTORE OF ACLS?**

No, the restore of ACLs from one operating system to another is not supported.

**CAN I RESTORE ACLS FROM ONE FILE SYSTEM TYPE TO ANOTHER?**

The restore of ACLs from one file system type to another may fail as the ACLs restore is dependent on the file system implementation. For example, ACLs which are backed up from ext3 cannot be restored to NFS and vice versa. Also, if you attempt to restore data from one file system type to another with ACLs included, but the file system is mounted without ACLs, the restore operation will fail. To workaround this issue ensure that the file system is mounted with ACLs before attempting a restore operation.

To prevent the restore operation from failing you can restore data without the ACLs included.

## **HARDWARE REVERTS FOR AIX LOGICAL VOLUMES. WHAT HAPPENS DURING THIS OPERATION?**

When you revert all the logical volumes in the AIX Logical Volume Manager, the revert operation supports all logical volume types and all their attributes are preserved. However, for revert operations on single logical volumes, striped volumes are not supported.

The following table displays the logical volume attributes that are preserved when you revert a single volume:

| <b>ATTRIBUTE NAME</b>           | <b>DESCRIPTION</b>                                                                            |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| <b>INTER</b>                    | Inter-physical volume allocation policy                                                       |
| <b>INTRA</b>                    | Intra-physical volume allocation policy                                                       |
| <b>LABEL</b>                    | Volume label                                                                                  |
| <b>RELOCATABLE</b>              | Defines if relocation is allowed during reorganization of the logical volume                  |
| <b>STRICTNESS</b>               | Strict allocation policy                                                                      |
| <b>TYPE</b>                     | Logical volume type                                                                           |
| <b>UPPERBOUND</b>               | Upper-bound on the physical volume used for new allocations                                   |
| <b>PERMISSION</b>               | Access permission of the logical volume                                                       |
| <b>MIRROR WRITE CONSISTENCY</b> | Defines if mirrored copies are in a consistent/active state                                   |
| <b>SERIALIZE IO</b>             | Defines if logical volumes are overlapping I/O serialized                                     |
| <b>SCHED POLICY</b>             | Defines which scheduling policy is being used when more that one logical partition is written |
| <b>BB POLICY</b>                | Bad block relocation policy                                                                   |
| <b>WRITE VERIFY</b>             | Defines if all verified write operations are followed by a follow up read operation           |

## **IS THE SOFTLINK PATH SUPPORTED FOR SNAPPROTECT OPERATION?**

No. Softlinks are not supported for SnapProtect operation. you should use the real paths.

You can create alias device using `mknod` for raw devices.

## **WINDOWS FILE SYSTEM**

### **WHAT HAPPENS TO MY BACKUP IF THE TIMESTAMP ON THE COMMSERVE AND CLIENT COMPUTER IS DIFFERENT?**

The incremental or differential backup will run as full backup and include all the files located on the source in the backup, even though these backups will be displayed as incremental or differential in the Job Manager.

### **WHICH SCAN METHODS ARE SUPPORTED FOR SCANNING FILES DURING A SNAPPROTECT BACKUP?**

You can enable the classic scan or Data Classification to scan files during a SnapProtect backup. If you select the Data Classification as the scanning method, ensure that the meta database is located on the same volume for which you are performing the snap backup.

# Troubleshooting - SnapProtect™ Backup

## TABLE OF CONTENTS

Virtual Server (VMware)

Oracle

SAP for Oracle

NAS

Virtual Server (Hyper-V)

DB2

Unix File System

## VIRTUAL SERVER (VMWARE)

### COMPLETED WITH ONE OR MORE ERRORS

Backup jobs from Virtual Server /DataAgent will be displayed as "Completed w/ one or more errors" in the Job History in the following cases:

- If the virtual machine, virtual machine disk, or virtual machine configuration file fails to back up.
- If one or more virtual machines in a backup job fail to back up.
- If communication fails with vCenter.
- If a disk included in a backup is not supported (i.e., independent disks or physical RDM).

If the meta data collection operation fails during a snap backup job, the job will be displayed as "Completed" in the **Backup Job History** of the subclient. You can create the bCWEJobMDDataFails registry key if you want to display the status as "Completed w/ one or more errors" in such scenario.

### WHILE PERFORMING A SNAPPROTECT BACKUP ON A LINUX VM, THE METADATA COLLECTION IS NOT INCLUDED IN THE BACKUP

To get the file level details of a Linux VM, follow the steps given below:

1. Perform a Disk Level SnapProtect backup.
2. Perform a Backup Copy operation.
3. Perform a File level Browse operation using the Primary Copy. You can specify the copy precedence by clicking **Advanced** on the **Browse Options** dialog box.

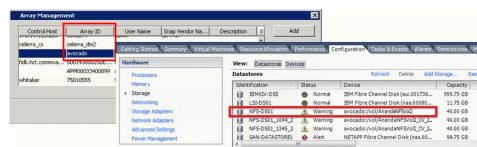
### RESTORING INDEPENDENT DISK/PHYSICAL RDM RESULTS IN VM NOT POWERING ON

If the virtual machine under backup includes independent disks/physical RDMs, these disks will be skipped. During a full restore the independent disk/Physical RDM gets restored with OMB, and the virtual machine cannot be powered on. As a work around, prior to powering on, manually remove the independent disks/Physical RDMs and then power on the restored virtual machine.

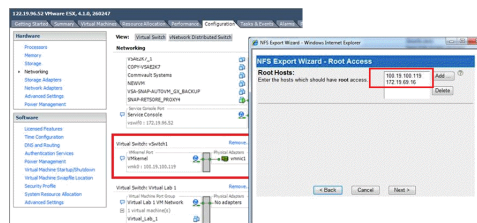
### MOUNT OPERATIONS ON AN ESX SERVER ARE FAILING USING NFS PROTOCOL

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.



### REVERT OPERATION IN PENDING STATE

**SYMPTOM**

The Revert job may go to Pending state with the following error:

```
File level revert is not supported for a Virtual Machine [%VMNAME%] which is on VMFS datastore. [Datastore(s) [%DatastoreName%] does not support file level revert.
```

**CAUSE**

The virtual machine may have NFS and iSCSI disks. Ensure that all the disks reside on the NFS data store. If the data does not reside on the NFS data store, you cannot perform the revert operation.

**SOLUTION**

Perform the conventional **Container Restore** to bring the data back to the point-in-time.

**REVERT OPERATION FAILS**

Before starting the revert operation, ensure that the Snapshot which you are using to perform the revert operation is not mounted.

**EXCHANGE MINING OPERATION FAILS****SYMPTOM**

Exchange Snap Mining operation may fail if SAN mode is used to perform the backup and snapshots were exposed in read-only mode.

**SOLUTION**

It is recommended to use NBD mode for Exchange Snap Mining backup. However, if you want to use SAN mode, ensure that all the disks exposed to the proxy computer have read and write permissions.

Follow the steps give below to clear read-only attributes of any SAN shared disk:

1. Open the Command Prompt on the proxy computer.
2. Enter the following commands:

```
diskpart
san policy=onlineall
```

**VIRTUAL MACHINE REGISTRATION FAILS DURING THE BACKUP COPY OPERATION****SYMPTOM**

During the backup copy operation, the registration of a virtual machine fails with the following error:

```
The Operation is not allowed in the current state
```

**CAUSE**

The ESX server which hosts the virtual machine is in the maintenance mode.

**SOLUTION**

Before initiating the backup copy operation, ensure that the ESX server is not in the maintenance mode. If you are performing an inline backup copy, before initiating the SnapProtect operation, ensure that the any host involved in the backup, is not in the maintenance mode.

**BACKUP JOB GOES TO PENDING STATE****SYMPTOM**

The SnapProtect backup job goes to pending state.

**CAUSE**

You cannot perform the SnapProtect backup of a template virtual machine. If the subclient for which you are performing the SnapProtect backup, contains the template virtual machine, the backup job goes to pending state.

**SOLUTION**

Set the SkipTemplateVM registry key to 1 and perform the backup of the subclient which contains the template virtual machine. The template virtual machine will not be included in the backup and the backup job will complete successfully.

**LIVE BROWSE FAILS TO DOWNLOAD VMX FILES WITH HTTP ERROR 403**



### **SYMPTOM**

You may get following error when you are restoring files and folders from a virtual machine:

Failed to download config file

### **SOLUTION**

Disable the Symantec End Point Protection on the computer where you have installed Virtual Server iDataAgent and MediaAgent and perform the file level restore.

---

## **BACKUP FAILS TO DOWNLOAD VMX FILES**

### **SYMPTOM**

The backup operation fails with a error: Unable to download config files.

### **CAUSE**

The name of the datastore contains + or @.

### **SOLUTION**

1. Check if the datastore of any virtual machine included in the backup contains + or @ characters in its name.
2. Rename the datastore and remove + and @ characters from the name.
3. Perform the backup operation.

---

## **UNABLE TO MOUNT THE SNAPSHOT**

### **SYMPTOM**

When you are mounting any snapshot on a host, you may get following error:

Discovery Failed. Unable to access host

### **CAUSE**

The **Snaps created during SnapProtect operation** dialog box displays a list of all the snapshots on a storage array. If you open the **Snaps created during SnapProtect operation** dialog box by one of the following methods, you can only view the list of snapshots and cannot mount the snapshots:

- Right click the snapshot copy of a storage policy and select **List Snaps**.
- From the Control Panel, double click Array Management. Select the required array in the Array Management dialog box and click **List Snaps**.

### **SOLUTION**

For more information about correct method mounting a snapshot, refer to Mount Snapshots.

---

## **NFS DATASTORE BECOMES INACCESSIBLE AFTER MOUNTING THE SNAPSHOT**

### **SYMPTOM**

Successfully mounted datastore becomes inaccessible when the browse operation is performed or data is accessed.

### **CAUSE**

This issue is caused by incorrect MTU settings between ESX proxy host and NFS storage.

### **SOLUTION**

To check if the issue is occurring due to incorrect MTU settings, use ping command with DF "do not fragment" option by providing different MTU values and check if Ping is working as expected.

---

## **FILE-LEVEL RESTORE FAILS WHEN DESTINATION CLIENT HAS A MEDIA AGENT**

---

### **SYMPTOM**

A file-level restore fails when restoring from an IntelliSnap backup to a destination client that has a media agent.

---

### **CAUSE**

When mounting the virtual machine, the restore operation tries to use the media agent on the destination client rather than the media agent on the source client, and the mount fails.

---

## RESOLUTION

1. Initiate the restore.
2. During the restore operation, select the content to be restored and the destination client.
3. On the **Restore Options** dialog, click **Advanced**, then click the **Data Path** tab.
4. In the **Use MediaAgent** field, select the media agent for the source client.
5. In the **Use Proxy** field, select the source proxy.
6. Complete the restore.

When the source media agent is used, the mount succeeds and the file-level restore completes successfully.

---

## VIRTUAL MACHINE CLIENT NAMES ARE GETTING CREATED WITH '\_1' APPENDED TO THE ORIGINAL CLIENT NAME

---

### SYMPTOM

When viewing virtual machines in the Client Computers list, you may see duplicated client names (for example, *<ClientName>* and *<ClientName>\_1*).

---

### CAUSE

Virtual machine information is added to the database during the discovery phase of a backup. If information changes, a new client is discovered during the discovery phase.

Making changes to information such as the virtual machine fully qualified domain name (FQDN), the GUID, or the host name can cause this issue.

---

## RESOLUTION

### TO AVOID DUPLICATE CLIENT ENTRIES CAUSED BY DIFFERENT CLIENT OR HOST NAME:

Use the install software option for the client level in the CommCell Console (rather than interactively installing software to the virtual machine Guest Operating System).

### TO CORRECT EXISTING CLIENTS:

If duplicate clients are created with '\_1' appended to the original client name, you can perform the following steps to merge the duplicate client back into the original:

1. At a command prompt, navigate to the software installation path, log in to the CommServer, and run the following script:

```
operation execscript -sn QS_SetVMClient -si @sourceClient='<ClientName>_1' -si @destClient='<ClientName>'
```

where *<ClientName>* is the original client name and *<ClientName>\_1* is the duplicate.

This script reassigns all backup history from *<ClientName>\_1* to *<ClientName>*. This enables you to view backup history, and to generate Job Summary Reports with the **Include Protected VMs** option enabled.

2. Remove the duplicate clients:
  - a. In the CommCell Console, go to **Control Panel | User Preferences**.
  - b. Click the **Client Computer Filter** tab.
  - c. Select the **Show Virtual Server Discovered Clients** option.
  - d. Delete the duplicate clients from the CommCell Browser.

---

## FAILED TO START THE VIRTUAL MACHINE

### SYMPTOM

When a virtual machine has been replicated in vSphere and backed up, and a full VM restore is performed from the backup, the following status message might be displayed in vCenter:

```
Failed to start the virtual machine.
```

### CAUSE

If the **Power ON Virtual Machine After Restore** option is selected when performing a full VM restore, VMware attempts to power on the restored VM before disabling replication.

### RESOLUTION

Clear the **Power ON Virtual Machine After Restore** option when initiating the restore. VMware automatically disables replication when the restore is completed, and you can power on the virtual machine manually.

---

## UNABLE TO BROWSE FILES ON SNAPSHOT FOR WINDOWS 2008 R2 VIRTUAL MACHINE - DISK:[<NAME>] FILTERED DURING SNAP PROTECT OPERATION

### SYMPTOM

A user is unable to browse files on a snapshot for a Windows 2008 R2 virtual machine (ESXi or ESX 4.1 and higher).

The following message appears in the **cvd.log** file:

```
Disk:[<Name>] filtered during snap protect operation
```

### CAUSE

File-level browse of a virtual machine snapshot fails if the page files for the VM are filtered out. The virtual machine snapshot cannot be mounted because it needs the page file for the VM. The page file is unavailable because it resides on a datastore that is filtered for backup.

This issue occurs when the **disk.EnableUUID** attribute is set to true for the virtual machine. The **disk.EnableUUID** attribute enables application-level quiescing. If the UUID is not enabled, VMware performs file-system consistent quiescing.

### RESOLUTION

During the restore, file-level browsing succeeds if the user selects a MediaAgent that has the Virtual Server Agent installed and has access to the datastore that contains the page files. On the **Advanced Restore Options** dialog, go to the **Data Path** tab to specify a MediaAgent.

To resolve this issue, set the **disk.EnableUUID** attribute to **false** and run the IntelliSnap backup again on the virtual machines where page files were filtered.

To modify the UUID setting in vSphere 5.1:

1. Select the VM and power it off.
2. On the **Summary** tab, click **Edit Settings**.
3. On the **Virtual Machine Properties** dialog, go to the **Options** tab.
4. Select the **General** field under **Advanced**.
5. Click the **Configuration Parameters** button.
6. Enter the **disk.EnableUUID** attribute and set the value to **false**.

As long as there is not a backup copy or auxiliary copy in progress, users should be able to browse files from the VM snapshot.

Disabling the UUID attribute does not affect applications that do not use Volume Shadow Copy Services (VSS), such as Microsoft SQL, Microsoft Exchange, or Active Directory.

### ADDITIONAL INFORMATION

See the following articles:

- Cannot take a quiesced snapshot of Windows 2008 R2 virtual machine (1031298)
- Volume Shadow Copy Service Quiescing
- Enabling and disabling Windows 2008 application-consistent quiescing on ESXi/ESX (1028881)

---

## CANNOT RESTORE FILES FROM A WINDOWS 2012 VIRTUAL MACHINE USING DEDUPLICATION

### SYMPTOM

When restoring from a backup of a Windows 2012 virtual machine that has deduplication enabled, a file-level restore completes successfully but only creates stub files.

### CAUSE

File-level restores are not supported for deduplicated volumes from a Windows 2012 VM.

### RESOLUTION

To retrieve files from a backup for a Windows 2012 VM using deduplication, restore the disk that contains the file.

Alternatively, you can install a local file system agent on the Windows 2012 VM to enable file-level restores.

---

## BACKUP COPY FAILS WITH MOUNT ERRORS: "UNABLE TO MOUNT THE VOLUMES."

### SYMPTOM

When mounting a snapshot to an existing datastore for a Backup Copy job, the mount operation fails with the following error:

```
Unable to mount the volumes.
```

#### CAUSE

When mounting a snapshot to an existing datastore, the string '\_gx\_backup', the job ID, and the archive file ID are added to the datastore name.

If the combined name is more than 42 characters, the mount operation fails.

#### RESOLUTION

Ensure that the combined name is less than 42 characters. In most cases, if the datastore name is 20 characters or less, the combined name will be under 42 characters.

## ORACLE

---

### FAILURE DURING SNAPPROTECT BACKUPS

SnapProtect Backup operations fail if the database is in the NOARCHIVELOG mode. Alter the database to ARCHIVELOG mode and then perform the SnapProtect backups.

```
SQL>startup mount;
SQL>alter database archiveolog;
SQL>alter database open;
```

Sometimes, the SnapProtect backup operations may fail if you enable the `SSKIPBACKUPBROWSE` registry key. Ensure to disable it.

---

### SNAPPROTECT BACKUP JOB RUNS INDEFINITELY

SnapProtect Backup operations run indefinitely if the archive log location is full. In such cases, you have to either clear the archive logs to make enough space available or specify a different archive log location.

---

### ORACLE RMAN SNAP TO TAPE INCREMENTAL COPY FAILS ON THE PROXY COMPUTER

When performing an Oracle RMAN incremental snap to tape copy, note the following:

1. The Oracle database installed on the proxy machine should be of the same version as the source. For example if Oracle 10.2.0.4 is installed on source then the proxy also should be of the same version i.e. 10.2.0.4
2. Oracle user ID/group ID on source and proxy should be the same otherwise the RMAN backup copy will fail with permission issues.
3. Copy the Oracle parameter file pfile from the source to the proxy (say the instance only as spfile)

```
sqlplus <username/password@servicename> as sysdba << EOF
Create pfile from spfile;
Exit;
EOF
```

Copy the pfile `init<instance name>.ora` to the proxy computer and the destination location should be `$ORACLE_HOME/dbs/` with oracle user permissions. Also, copy the oracle password file from the source to the proxy computer's `$ORACLE_HOME/dbs/` directory.

4. Create the `bdump`, `udump`, `adump`, `cdump` and `diagnostic_dest` directories. Please note that the directories should be in the same location as the source.
5. Create the directories `DB_CREATE_FILE_DEST`, `LOG_ARCHIVE_DEST` and any other directory required for starting the database in `NOMOUNT` mode. If there are multiple archive destinations, then create the directories for each of the archive destinations.
6. Copy `$ORACLE_HOME/network/admin/tnsnames.ora` configuration from source to proxy. If the entire content cannot be copied then copy at least the configuration related to catalog connection.
7. Startup the proxy instance in `NOMOUNT` mode.
8. Now configure the proxy Oracle Instance on the CommServer Console and status should be started. Now you are all set to do Oracle RMAN snap to tape incremental

Note that for incremental backup, snap clone will be mounted in the same location as the source mount-point of the source database. For example, if the data mount-point is `/netapp/data` then on the proxy too it will be mounted in `/netapp/data`, similarly for the archive log location chosen for the SnapProtect backup. Therefore, ensure that on the proxy this mount-point is free and there is no such directory existing on the proxy computer ( even if it exists it should be empty).

---

### SNAP PROTECT BACKUP COPY OF AN ORACLE ASM DATABASE FAILS ON THE PROXY COMPUTER

When performing SnapProtect operations on a backup copy of an Oracle ASM database, note the following:

- The Oracle iDataAgent must be installed on the proxy computer.
- The Oracle database installed on the proxy and source computers should be compatible.
- If you create an ASM instance manually in Oracle 11gRelease2, it must be registered to Central Repository Server (CRS). From Oracle 11gRelease2 onwards, ASM instance is a resource in CRS repository.

1. Run the following command as Oracle ASM user from ASM \$ORACLE\_HOME/bin to register ASM database to OCR:

```
> srvctl status asm
PRCR-1001 : Resource ora.asm does not exist
```

2. Run the following command to add the resource to the configuration, If resource does not exist:

```
> srvctl add asm -p $ORACLE_HOME/dbs/init${ORACLE_SID}.ora
> srvctl status asm
ASM is not running.
```

3. Run the following command to start the ASM instance:

```
> srvctl start asm
or
> sqlplus "/ as sysasm"
startup
```

4. Run the following command to verify the Status:

```
> srvctl status asm
```

5. Now, you will see the following message:

```
ASM is running on <proxy>
```

---

## SNAP PROTECT BACKUP COPY ON PROXY FAILS

**SOMETIMES, THE BACKUP COPY ON PROXY FAILS WITH THE FOLLOWING ERROR:**

**ORA-7217 SLTLN: ENVIRONMENT VARIABLE CANNOT BE EVALUATED.**

Example:

If RMAN configuration parameters contain \$s as shown below:

```
RMAN> show all;
```

RMAN configuration parameters for database with db\_unique\_name CVLT are:

```
CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 0 DAYS;
CONFIGURE BACKUP OPTIMIZATION ON;
CONFIGURE DEFAULT DEVICE TYPE TO DISK; # default
CONFIGURE CONTROLFILE AUTOBACKUP OFF;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '$ORACLE_BKUP/$ORACLE_SID/controlfile%F.f';
CONFIGURE DEVICE TYPE DISK PARALLELISM 2 BACKUP TYPE TO COMPRESSED BACKUPSET;
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '$ORACLE_BKUP/$ORACLE_SID/%d_df_%t_b%s_p.p.rmf' MAXPIECESIZE 2000 M;
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ENCRYPTION FOR DATABASE OFF; # default
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default
CONFIGURE COMPRESSION ALGORITHM 'BASIC' AS OF RELEASE 'DEFAULT' OPTIMIZE FOR LOAD TRUE ; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO '$ORACLE_BKUP/$ORACLE_SID/snapcf_CVLT.f';
ORA-7217 sltln: environment variable cannot be evaluated
```

Perform one of the the following steps to resolve this issue:

- Configure “/” as connect string on proxy and set the environment variables specified for snapshot control file path in cvprofile residing in Base directory.
  - a. Edit /opt/calypso/Base/cvprofile
  - b. export ORACLE\_BKUP=/tmp
  - c. calypso restart
- Change the configuration parameters on source to remove environment variables (\$ORACLE\_BKUP etc).

**SOMETIMES, THE BACKUP COPY ON PROXY FAILS WITH THE FOLLOWING ERROR EVEN THOUGH THE CONTROL FILE COPY IS CATALOGED INTO RECOVERY CATALOG:**

RMAN-03002: failure of backup command at 04/11/2012 13:44:03

RMAN-06004: ORACLE error from recovery catalog database: RMAN-20220: control file copy not found in the recovery catalog

RMAN-06090: error while looking up control file copy: +DATA/backupctl.galaxy

RMAN>

Perform the following to resolve this failure:

- Unregister and then reregister the source database to recovery catalog.
- Resume the backup copy job.

**SOMETIMES THE SNAP PROTECT OPERATION AND A BACKUP COPY ON PROXY FOR ASM DATABASE WILL FAIL WITH THE FOLLOWING ERRORS:**

**FOR SNAP:**

**ERROR CODE: [19:1335]**

Description: Oracle Backup [GetASMLogDisks Failed.]

**FOR BACKUP COPY:**

**ERROR CODE: [19:1335]**

Description: Oracle Backup [Mounting snap or renaming ASM DiskGroup operation failed with an error. Please check the logs for more details.]

30156 f48b7410 04/18 13:00:37 97550 OraObject::GetOraMode() - oraMode = SHUTDOWN.

30156 f48b7410 04/18 13:00:37 97550 OraObject::GetOraMode() - oraMode = SHUTDOWN: return Error.

30156 f48b7410 04/18 13:00:37 97550 OraInfoBase::GetInfo() - CheckOraMode() failed: oraError=301989906

30156 f48b7410 04/18 13:00:37 97550 ASMSnapUtil::runSqlWithScript() - Failed while getting the Oracle version

30156 f48b7410 04/18 13:00:37 97550 ASMSnapUtil::runSqlWithScript() - Writing into file [/@/opt/calypso/Base/Temp/tmp\_asm\_30156.sql] sql = [select 'U,||' state from v\$asm\_diskgroup where name = 'DATADG1'

/

]

30156 f48b7410 04/18 13:00:37 97550 ASMSnapUtil::runSqlWithScript() - Executing SQL select 'U,||' state from v\$asm\_diskgroup where name = 'DATADG1'

/

failed with an error Database is in SHUTDOWN mode

30156 f48b7410 04/18 13:00:37 97550 ASMSnapUtil::isASMDiskGroupMounted() - Failed while executing the sqlscript [select 'U,||' state from v\$asm\_diskgroup where name = 'DATADG1'

/

] output = []

30156 f48b7410 04/18 13:00:37 97550 ASMDiskGroup::renameASMDiskGroup() - Child change user=oracle, gid=501, uid=501

30156 f48b7410 04/18 13:00:37 97550 ClOraSnapAgent::RenameAndMountASMDiskGroup() - Successfully Renamed ASM DISK GROUPS

30156 f48b7410 04/18 13:00:37 97550 OraObject::GetOraMode() - strictSID = 0

30156 f48b7410 04/18 13:00:37 97550 OraChildProcess::SetPostForkParam() - Parent path = /oracle11gr2/product/11.2.0/dbhome\_1/bin/sqlplus

30156 f48b7410 04/18 13:00:37 97550 OraChildProcess::SetPostForkParam() - Parent oraUser = oracle

Perform the following to resolve this failure:

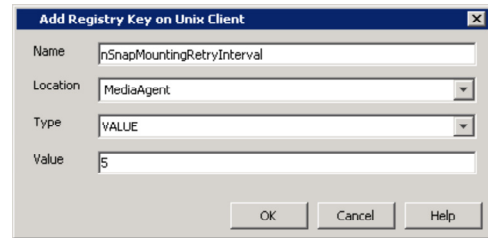
1. Log in to the CommCell Console.
2. Verify the Oracle +ASM instance status. The status should be in started mode.
3. Resume the Snap protect operation or the backup copy job that you need to perform.

**LATENCY OCCURS FOR RELEASING FILEDESCRIPTORS BY ASM INSTANCE DURING DISMOUNTING OF ASM DISKGROUPS**



Follow the steps given below to configure the time interval between two retries for mounting the snapshots:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<Client>**, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type `nSnapMountingRetryInterval`.
6. In the **Location** box, select or type `MediaAgent` from the list.
7. In the **Type** box, select **Value**.
8. In the Value box, type the value and then click **OK**.




---

### SYSTEM IS DISPLAYING ORA-01145: OFFLINE IMMEDIATE DISALLOWED UNLESS MEDIA RECOVERY ENABLED ERROR WHEN RECOVERING THE NO ARCHIVELOG DATABASE

When you see ORA-01145: offline immediate disallowed unless media recovery enabled error when recovering the no archivelog database, verify whether the catalog is in sync with the database. If the catalog is not in sync with the database, perform a resync.

---

### SYSTEM IS DISPLAYING ORA-01031: INSUFFICIENT PRIVILEGES ON THE PROXY

During the proxy setup the following error may occur after the Oracle password file is copied over the proxy

```
SQL> conn sys/<password>@orcl as sysdba;
ERROR:
ORA-01031: insufficient privileges
```

The listener uses the dynamic service information about the database and instance before using statically configured information in the listener.ora file. Configuration of static service information is necessary if you require remote database startup from a tool other than Oracle Enterprise Manager, or you have Oracle Database releases earlier than Oracle8i.

Also please note that the SID\_NAME is case sensitive. Listener.ora file on proxy

#### Cause:

```
SID_LIST_LISTENER=
(SID_LIST=
(SID_DESC=
(ORACLE_HOME=/u01/app/oracle/rdbms/11.2.0.3/dbhome_1)
(SID_NAME=prd1)
)
(SID_DESC=
(ORACLE_HOME=/u01/app/oracle/rdbms/11.2.0.3/dbhome_1)
(SID_NAME=orcl)
)
)
```

#### Solution:

```
SID_LIST_LISTENER=
(SID_LIST=
(SID_DESC=
(ORACLE_HOME=/u01/app/oracle/rdbms/11.2.0.3/dbhome_1)
(SID_NAME=PRD1)
)
(SID_DESC=
(ORACLE_HOME=/u01/app/oracle/rdbms/11.2.0.3/dbhome_1)
(SID_NAME=ORCL)
)
)
```

#### Verification:

```
SQL> conn sys@ORCL as sysdba
Enter password:
Connected.
```



## SEPARATE MEDIAAGENTS FOR PRIMARY AND SNAP BACKUP COPIES IS NOT SUPPORTED

Separate MediaAgents for Primary and Snap Backup Copies is not supported for SnapProtect operations. The backup copy operation fails in such configurations.

## CATALOG ERRORS DURING SNAPPROTECT BACKUP

During SnapProtect backup job, you may notice the following catalog errors:

File Name: /opt/calypso/MediaAgent/SnapVolumeMounts/SnapMnt\_1\_2\_26099/oradata/ONLINE/dbconf.cfg

RMAN-07517: Reason: The file header is corrupted

File Name: /opt/calypso/MediaAgent/SnapVolumeMounts/SnapMnt\_1\_2\_26099/oradata/ONLINE/initONLINE.ora

RMAN-07517: Reason: The file header is corrupted

File Name: /opt/calypso/MediaAgent/SnapVolumeMounts/SnapMnt\_1\_2\_26099/oradata/ONLINE/spfileONLINE.ora

RMAN-07518: Reason: Foreign database file DBID: 0 Database Name:

File Name: /opt/calypso/MediaAgent/SnapVolumeMounts/SnapMnt\_1\_2\_26099/oradata/ONLINE/GalaxyControlFile.Conf

RMAN-07517: Reason: The file header is corrupted

These error messages can be ignored. As part of the backup job, files such as spfile, pfile and backup controlfiles are copied to the archive log location. Oracle does not recognize these files as archive log files and hence displays the error messages.

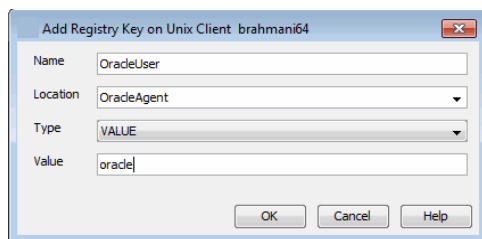
## RESTORE ERROR ON LINUX CLIENT WHEN SWITCH DATABASE MODE IS ENABLED

When restoring Oracle database on Linux clients, if the **Switch database mode for restore** option is selected to keep database in correct mode during restore, the database may not restart after switching the database mode. Also, the restore operation may fail with the following error message.

RMAN Script execution failed with error [RMAN-04014: startup failed: ORA-27137: unable to allocate large pages to create a shared memory segment]. Please check the Logs for more details.

This issue occurs if the oracle user has a higher ulimit configuration than the root user. To resolve this issue, apply the ulimit value of Oracle user for the restore using the following steps:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the <Client>, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type OracleUser.
6. In the **Location** box, select or type OracleAgent from the list.
7. In the **Type** box, select **Value**.
8. In the Value box, type the Oracle user name (eg., oracle) and then click **OK**.
9. Click **OK**.
10. Restart Calypso Services on the client.



## SAP FOR ORACLE

When you perform SnapProtect backup operation, snaps are performed twice on sapbackup directory, dbs folder etc. However, there is a limitation with Hitachi Data System (HDS). You can only create 3 S-VOL for a given P-VOL when you are using HDS shadow image snap engine. If we have the entire SAPDATA\_HOME on a single volume, all the 3 available S-VOL's may be exhausted.

Hence, you need to perform the following for SAP HDS:

- Perform the SnapProtect backup operation Data and Logs separately using 2 different subclients.

- Use the spool copy for every SnapProtect backup operation so that snaps can be aged once it is copied to disk / tape.

---

## SEPARATE MEDIAAGENTS FOR PRIMARY AND SNAP BACKUP COPIES IS NOT SUPPORTED

Separate MediaAgents for Primary and Snap Backup Copies is not supported for SnapProtect operations. The backup copy operation fails in such configurations.

## NAS

---

### SNAPVAULT/SNAPMIRROR COPIES ARE NOT CREATED WHEN BACKING UP VFILER DATA

When you configure a physical file server (vfiler0) as a NAS client and define vFiler volumes in the subclient content, auxiliary copy operations will fail to create the SnapVault/SnapMirror copies. You can resolve this issue by configuring each vFiler as a NAS client. During the client configuration, ensure not to include the vFiler root volume in the subclient content. You can also perform mount and revert operations with the snapshot.

---

### I CANNOT RESTORE FROM A SNAPSHOT AFTER SELECTING TO SKIP THE INDEXING PHASE DURING BACKUP

Restore operations from a snapshot are not supported if you selected the **Skip Catalog phase for SnapProtect** option in the **Advanced Backup Options** dialog box during backup. To restore your backed up data, you must create a backup copy as explained in the Snap Movement to Media procedure and restore your data from the backup copy.

---

### RESTORE FROM SNAPVAULT/SNAPMIRROR COPIES FAILS WITH AN ERROR INDICATING THE FILE SERVER IS NOT A NAS CLIENT

Restore operations will fail with the following error code if the file server used to backup Vault or Mirror copies is not added as a NAS client:

```
[39:279] The host <file_server_name> could not be found in the list of NAS Clients. Please add this host as NAS Client.
```

To resolve this issue, add the file server as a NAS client as well as any other NAS storage device used to back up secondary storage data.

## VIRTUAL SERVER (HYPER-V)

---

### SNAPPROTECT BACKUP FOR ONLINE VIRTUAL MACHINES IN HYPER-V CLUSTERS FAILS

You can resolve this issue by temporarily suspending the virtual machine during the SnapProtect operation.

---

### WHILE PERFORMING A RESTORE OPERATION, THE MEDIAAGENT DOES NOT HAVE ACCESS TO THE STORAGE DEVICE

If the storage policy uses a Media Agent that does not have access to the storage device where the snapshot was created, an additional step is required while selecting the options in the **Restore Options for all selected items** window.

- Click on the **Advanced** button.
- From the **Advanced Restore Options** window, click the **Data Path** tab.
- Select a proxy from the **Use Proxy** dropdown to mount the snapshot.
- Click **OK**.

---

### VIRTUAL MACHINES RESTORED FROM SNAPPROTECT ARE NOT POWERED ON AUTOMATICALLY

The virtual machine may have been in a running state during the SnapProtect backup. Consequently, the virtual machine is restored in a saved state. To resolve this issue:

1. Right-click the virtual machine in the Hyper-V Manager.
2. Click **Delete Saved State**.

---

### FILE-LEVEL RESTORE FAILS

The restore operation fails when you are restoring files or folders from a Disk Level backup. The restore will fail if the **Enable Granular Recovery** option is not selected before performing the backup or the Granular Recovery operation fails.

In such scenario, you can use following procedure to restore files and folders from a disk level backup:

1. Mount the snapshot that contains the data which you want to restore. For more information, refer to Mount Snapshots.
2. Browse the **Destination Path** which you selected while mounting the snapshot and locate the VHD file for the disk which contains the required files and folder.
3. Use the DiskManager to mount the VHD file on any Windows server. A new drive will be created on the Windows server.
4. Browse the files and folder on this drive and copy the required files and folders to a desired destination.

## CANNOT RESTORE FILES FROM A WINDOWS 2012 VIRTUAL MACHINE USING DEDUPLICATION

### SYMPTOM

When restoring from a backup of a Windows 2012 virtual machine that has deduplication enabled, a file-level restore completes successfully but only creates stub files.

### CAUSE

File-level restores are not supported for deduplicated volumes from a Windows 2012 VM.

### RESOLUTION

To retrieve files from a backup for a Windows 2012 VM using deduplication, restore the disk that contains the file.

Alternatively, you can install a local file system agent on the Windows 2012 VM to enable file-level restores.

## DB2

### SEPARATE MEDIAAGENTS FOR PRIMARY AND SNAP BACKUP COPIES IS NOT SUPPORTED

Separate MediaAgents for Primary and Snap Backup Copies is not supported for SnapProtect operations. The backup copy operation fails in such configurations.

## UNIX FILE SYSTEM

### FAILURE DURING MOUNT OF SECOND LOGICAL VOLUME HAVING THE FIRST LOGICAL VOLUME ALREADY MOUNTED

You have two logical volumes on the same physical volume group. After performing a SnapProtect backup on a subclient which has both logical volumes as content, you proceed to mount each logical volume. After successfully mounting the first volume, an error will be displayed while trying to mount the second one saying the mount operation failed during the volume group recreation. Although the mount operation was not successful, the second logical volume will show as mounted in the **Snaps created during SnapProtect operation** window of the CommCell Console. In this scenario, proceed to unmount the second logical volume.

- From the CommCell Console, right-click the entity that contains the snapshots you want to browse, and click **All Tasks | List Snaps**.
- From the **Snaps created during SnapProtect operation** window, right-click the logical volume and select **Unmount**.
- Click **Yes**.

To avoid this issue on future mount operations, it is recommended to mount one of the logical volumes, and not both.

### IOSCAN ERROR ON AN IA64 MACHINE RUNNING HP-UX 11.23

When running a SnapProtect backup on an IA64 machine running HP-UX 11.23, the below ioscan error in the logs can be safely ignored.

```
5774 16 02/14 14:14:57 ##### UXScsi::scanAgile() - "/usr/sbin/ioscan -kFnN" failed: ioscan: illegal option -- N
```

### SNAPPROTECT FAILURE AT THE VGIMPORT PHASE ON AN IA64 MACHINE RUNNING HP-UX

On an IA64 machine running HP-UX, SnapProtect job may fail at the vgimport phase with an error message if the maximum number of volume groups allowed on the machine is exhausted. For example,

```
<Failure during recreate VG. Error [Failed import: vgimport -v -
m /opt/calypso/Base/Temp/vg_test_1360887863.map /dev/vg_test_1360887863 /dev/dsk/c20t0d2 14672 Error: vgimport: Cannot open the control
file "/dev/vg_test_1360887863/group":
```

In such cases, use the following steps to increase the maximum number of volume groups and resume the job:

1. Check the maxvgs parameter using query:

```
kctune -v maxvgs
```

2. Check the maximum minor number, represented as NN, in the output below using the following command. For example,

```
ls -l /dev/vg_test_1360887863
crw-r----- 1 root dba 128 <0xNN0000> Dec 17 16:00 group
```

3. If the maximum value of the minor number determined in the previous step is equal to the maxvgs parameter then modify it to accommodate more volume groups. For example,

```
kctune maxvgs=50
```

4. Reboot the machine.

# Accessing Exchange Data from VMware Snapshots

## ACCESS EXCHANGE DATA ON A VIRTUAL MACHINE

Exchange data, such as mail messages, can be restored from an offline point-in-time virtual machine snapshot to reduce impact to the production Exchange Server. To mine Exchange data on a virtual machine, do the following:

- Setup Backup Proxy Computer and Exchange Server Virtual Machine
- Configure Virtual Server iDataAgent and Discover Exchange Server Virtual Machine
- Create Magnetic Library and Storage Policy
- Configure and Create Snapshot of Exchange Data
- Configure and Run Snap Mining Job
- Browse and Mine Exchange Data

---

## SETUP BACKUP PROXY COMPUTER AND EXCHANGE SERVER VIRTUAL MACHINE

The addresses of both computers must be network resolvable.

### BACKUP PROXY COMPUTER

The backup proxy computer is used to create the snapshot of the Exchange data on the virtual machine. It also is used to run the snap mining job. This proxy computer must satisfy certain requirements, as listed in System Requirements. In addition, ensure that the proxy computer and the Exchange Server virtual machine are members of the same domain.

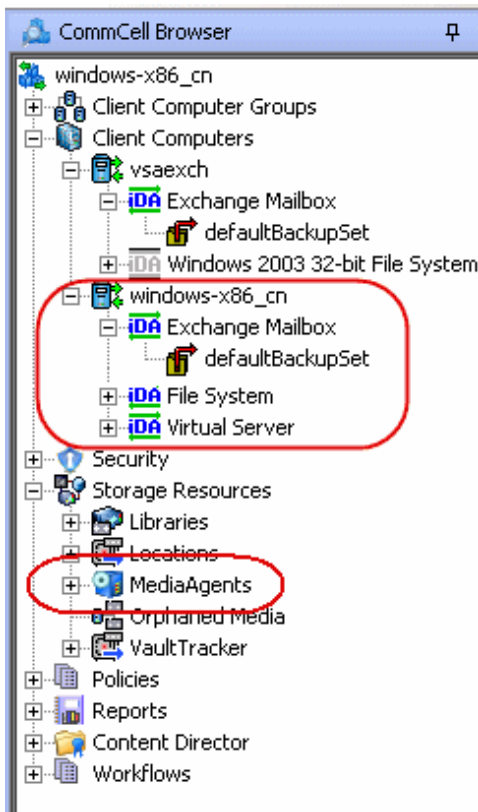
On this proxy computer, install the following:

- Virtual Server iDataAgent.  
See Getting Started - VMware Deployment for installation instructions.
- Exchange Mailbox iDataAgent (Restore Only).  
See Deployment - Microsoft Exchange Server Agents for installation instructions.

When prompted for the **Exchange Server Name**, enter the fully-qualified name of the Exchange Server (e.g., `exchange.vm.company.com`) installed on the Exchange Server virtual machine. Ensure you also select the correct **Exchange Server Version**, or else the snap mining job may fail.

- MediaAgent.  
See MediaAgent Deployment for installation instructions.
- Active Directory Lightweight Directory Services (AD LDS) Snap-Ins and Command-Line Tools. This feature is used to remotely manage Active Directory Domain Services.
- Microsoft Outlook.

After installing, the components in CommCell Console are displayed as follows:



#### EXCHANGE SERVER VIRTUAL MACHINE

This virtual machine has the Exchange data that you wish to mine. The Exchange Server has already been installed on this machine. Install the following:

- Exchange Mailbox *iDataAgent*.

See Deployment - Microsoft Exchange Server Agents for installation instructions.

When prompted for the **Exchange Server Name**, enter the fully-qualified name of the Exchange Server (e.g., `exchange.vm.company.com`) installed on the Exchange Server virtual machine. Ensure you also select the correct **Exchange Server Version**, or else the snap mining job may fail.

- Windows File System *iDataAgent* (Restore Only).

See Deployment - Windows File System *iDataAgent* for installation instructions.

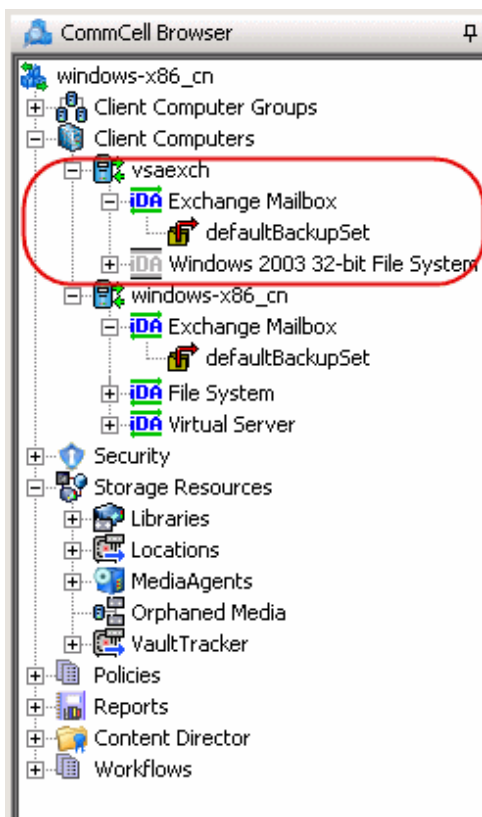
- VMware Tools (latest version).

See <http://downloads.vmware.com/> for more information.

- VSS Provider.

See VSS Provider for step-by-step installation instructions.

After installing, the components in CommCell Console are displayed as follows:

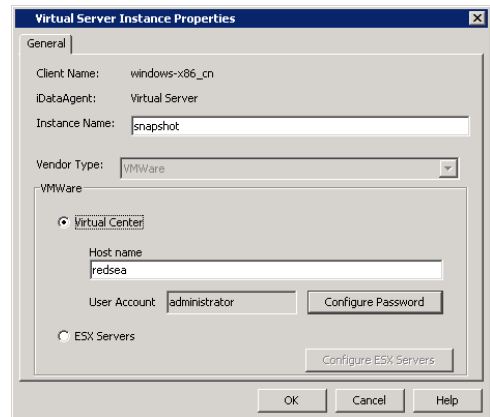


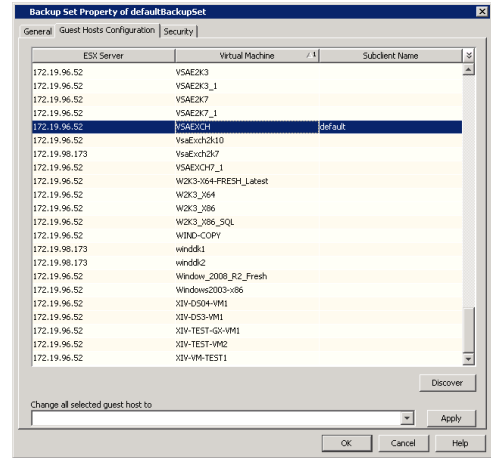
## CONFIGURE VIRTUAL SERVER IDATAAGENT AND DISCOVER EXCHANGE SERVER VIRTUAL MACHINE

The following steps are performed on the backup proxy computer.

1. Configure an instance of the Virtual Server iDataAgent as follows:
  1. From the CommCell Console, navigate to **Client Computers | Virtual Server**.
  2. Right-click the Agent and click **All Tasks | Create New Instance**.
  3. Enter an **Instance Name** and select **Vendor Type**.
  4. Click **Virtual Center**.
  5. Enter a valid **Host name** for the Virtual Center.
  6. Click **Configure Password** and enter User Name and Password of Virtual Server. Click **OK**.
  7. Click **OK**.
  
2. Discover the Exchange Server virtual machine as follows:
  1. From the CommCell Console, navigate to **Client Computers | Virtual Server**.
  2. Right-click the backupset and select **Properties**.
  3. Click the **Guest Hosts Configuration** tab.
  4. Click **Discover**.
  5. Scroll through the list and select the Exchange Server virtual machine you wish to mine.
  6. Click **OK**.

Click the **Virtual Machine** column to sort the machines alphabetically.





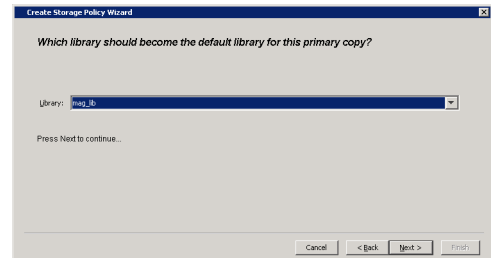
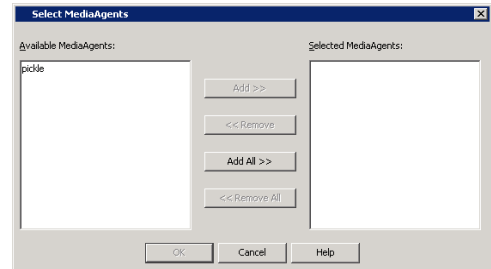
## CREATE MAGNETIC LIBRARY AND STORAGE POLICY

The following steps are performed on the backup proxy computer.

1. Create a magnetic library if one has not already been configured as follows:
  1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
  2. Double click **Library & Drive Configuration**.
  3. Select the MediaAgent(s) whose devices you want to detect or display, and then click **OK**.

**NOTES**

  - If a device has already been configured for the MediaAgent, the system displays the device in the **Library & Drive Configuration** window.
  4. Click **OK** to continue.
  5. Click **OK** again if prompted.
2. Create a storage policy as follows:
  1. From the CommCell Browser, right-click **Storage Policies | New Storage Policy**.
  2. Follow the prompts displayed in the Storage Policy Wizard:
    - Click **Data Protection and Archiving** for type of Storage Policy and click **Next**.
    - Click **No** for Legal Hold and click **Next**.
    - Enter a name in **Storage Policy Name** and click **Next**.
    - Enter the **Primary Copy** name and click **Next**.
    - Select the library that was created in Step 1 and click **Next**.
    - Select the MediaAgent and click **Next**.
    - Configure device stream and retention criteria (default is infinite) and click **Next**.
    - For deduplication, select **No** and click **Next**.
    - Confirm the selections and click **Finish**.



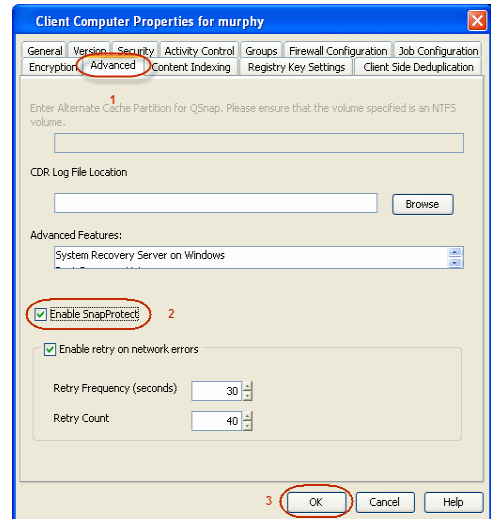
## CONFIGURE AND CREATE A SNAPSHOT OF EXCHANGE DATA

The following steps are performed on the backup proxy computer.

1. Enable SnapProtect as follows:
  1. From the CommCell Console, navigate to **<Client>**.
  2. Right-click the client and select **Properties**.
  3. Click on the **Advanced** tab.
  4. Select the **Enable SnapProtect** option to enable SnapProtect backup for the client.
  5. Click **OK**.

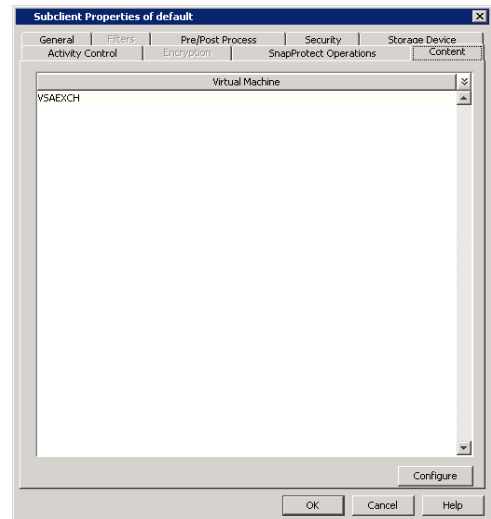
2. Configure the content of the subclient as follows:

1. From the CommCell Console, navigate to **Client Computers | Virtual Server**.
2. Right-click the subclient and click the **Content** tab.
3. Click **Configure**.
4. In the **Guest Hosts Configuration** dialog, select the Exchange Server virtual machine and click **OK**.
5. Click **OK**.



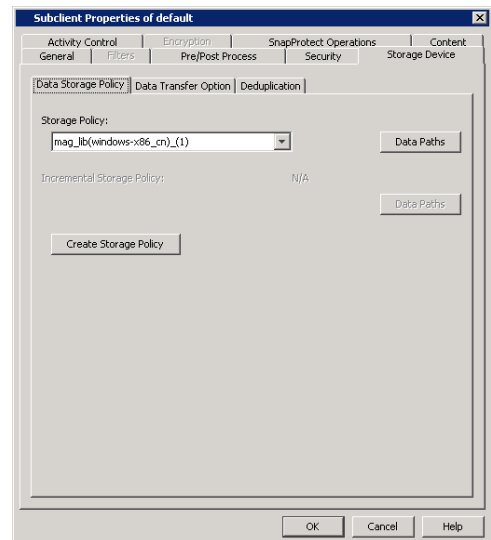
3. Assign the storage policy to the subclient as follows:

1. From the CommCell Console, navigate to **Client Computers | Virtual Server**.
2. Right-click the subclient and click **Properties**.
3. Click the **Storage Device** tab.
4. In **Storage Policy**, select the storage policy as created in Create Magnetic Library and Storage Policy.
5. Click **OK**.



4. Enable SnapProtect and snap mining for the subclient as follows:

1. From the CommCell Console, navigate to **Client Computers | Virtual Server**.
2. Right-click the subclient and click **Properties**.
3. Click the **SnapProtect Operations** tab.



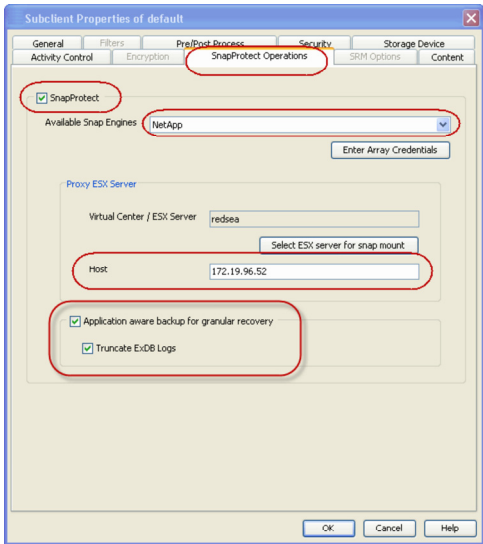


4. Select **SnapProtect** option to enable SnapProtect backup for the selected subclient.
5. Select the relevant snap engine from the **Available Snap Engines** drop-down list.

Ensure that the snap engine has been configured in Array Management. To configure it, click **Enter Array Credentials** and click **Add**.

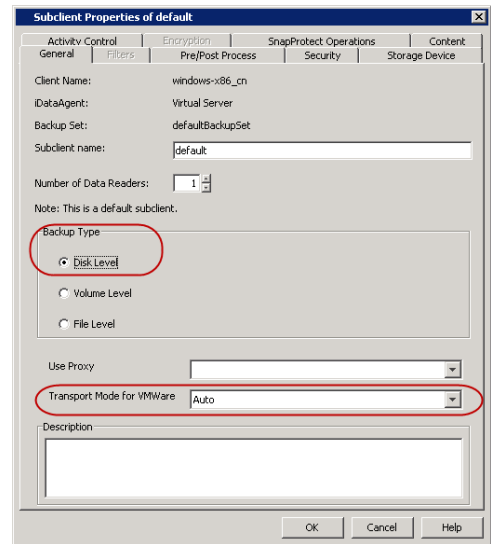
6. Specify the IP address of the Host by clicking **Select ESX server for snap mount**. Select a Host IP address and click **OK**.
7. Select **Application aware backup for granular recovery** option to enable snap mining for the selected subclient.
8. Optionally, select the **Truncate ExDB Logs** to prune Exchange Database logs that are no longer needed and prevent them from growing to an unmanageable size. This is recommended.
9. Click **OK**.

Keep in mind that once snap mining is enabled for a subclient, it cannot be reversed.



5. Configure the backup type and transport mode for the subclient as follows:

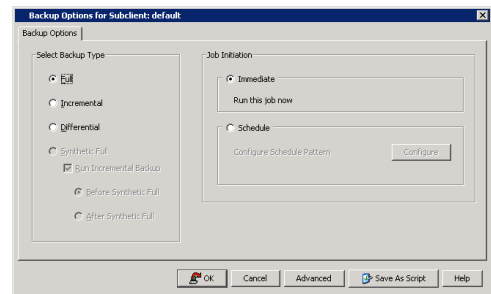
1. From the CommCell Console, navigate to **Client Computers | Virtual Server**.
2. Right-click the subclient and click **Properties**.
3. For **Backup Type**, select **Disk Level**.
4. In **Transport Mode for VMWare**, select **Auto**.
5. Click **OK**.



6. Run the SnapProtect backup job as follows:

1. From the CommCell Console, navigate to **Client Computers | Virtual Server**.
2. Right-click the subclient and click **Backup**.
3. Click **Full**.
4. Click **OK**.

In **Job Controller**, you can view the progress of the job. Double-click the job to view the job details.

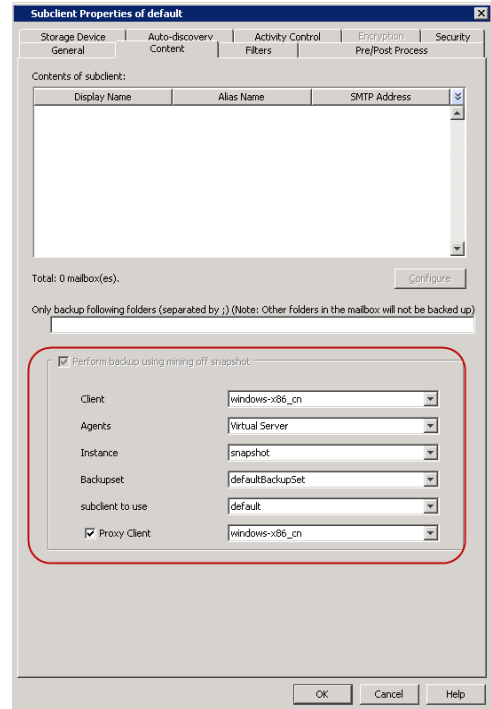


## CONFIGURE AND RUN SNAP MINING JOB

The following steps are performed on the Exchange Server virtual machine.

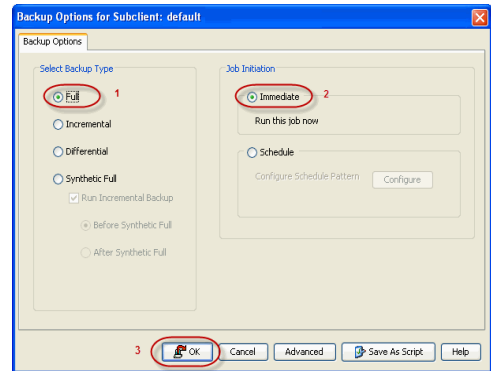
1. Configure the subclient of the Exchange Mailbox *iDataAgent* as follows:
  1. From the CommCell Console, navigate to **Client Computers | <Exchange server client> | Exchange Mailbox**.
  2. Right-click a subclient and click **Properties**.
  3. Click the **Content** tab.
  4. Click **Perform backup using mining off snapshot**.
  5. Choose the client computer on which the snapshot was created in **Client**.

6. Choose **Virtual Server** as the **Agent** that was used to create the snapshot.
7. Choose the **Instance** of the Virtual Server iDataAgent that was used to create the snapshot.
8. Choose the **Backupset** of the Virtual Server iDataAgent that was used to create the snapshot.
9. Choose the subclient of the Virtual Server iDataAgent in **subclient to use** that was used to create the snapshot.
10. Click **Proxy Client** and from the pulldown menu, select the proxy computer that will be used to run the snap mining data protection job. You must choose a proxy computer for running the data protection job; it cannot be run from the Exchange Server virtual machine itself. If desired, an additional proxy computer could be used for running the data protection job instead of the backup host proxy. It would have the same requirements as the backup host proxy.
11. Click **OK**.



2. Run the snap mining job as follows:

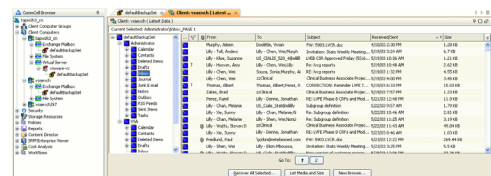
1. From the CommCell Console, navigate to **Client Computers | <Exchange server client> | Exchange Mailbox**.
2. Right-click a subclient and click **Backup**.
3. From the CommCell Console, right-click the subclient and click **Backup**.
4. Select **Full** as backup type and **Immediate** to run the job immediately.
5. Click **OK**.



## BROWSE AND MINE EXCHANGE DATA

The following steps are performed on the Exchange Server virtual machine.

1. Browse and mine Exchange data as follows:
  1. From the CommCell Browser, right-click the subclient and click **Browse Backup Data**.
  2. Click **OK**.
  3. Select data to restore in the Browse window and click **Recover All Selected...**
  4. Click one of the following in the **Restore Options** window:
    - Click **To Mailbox** to restore data to a mailbox. Choose whether to restore to original or different client computer and the same or different path.
    - Click **To PST** to restore the data to a PST file. Choose whether to restore the PST file to a local or network drive.
  5. Click **OK**.



Back to Top

# Accessing Exchange Data from Database Snapshots

## TABLE OF CONTENTS

### Overview

### Prerequisites

### Create a Snapshot

- Hardware Supported Storage Array
- Data Replicator

### Configure Snap Mining

- Mining on a Proxy
- Mining on a Single Computer

### Configuring Wait Time for Parallel Snap Mining

### Configuring for Parallel Snap Mining Preparation Timeout

### Run a Snap Mining Job

### View Job History

### Best Practices

### FAQ

## OVERVIEW

Snap mining allows you to protect data from an offline copy of the Exchange database. The offline copy is a point-in-time snapshot of the data to be used for data protection operations. With snap mining, impact to the Exchange Server can be reduced in a production environment thus improving performance.

## PREREQUISITES

The following are prerequisites to using this feature:

- Mailboxes that are mined from a Microsoft Exchange 2003 32-bit Server database requires the 32-bit Exchange Mailbox iDataAgent.
- Mailboxes that are mined from a Microsoft Exchange 2007 64-bit Server or Microsoft Exchange 2010 64-bit Server databases require the 64-bit Exchange Mailbox iDataAgent.
- Ensure that the Operating System on the computer on which the Exchange Server is installed and the computer where the snap is mounted is the same.

## CREATE A SNAPSHOT

A snapshot needs to be created for snap mining. It can be created before or after configuring the subclient for snap mining. Snapshots are created in one of these ways:

- Hardware supported storage array
- Software storage array (Data Replicator)

---

### HARDWARE SUPPORTED STORAGE ARRAYS

A snapshot can be created with SnapProtect backup using a supported storage array.

For step-by-step instructions on creating a snapshot with a hardware storage array, refer to SnapProtect Backup - Microsoft Exchange Database.

---

### DATA REPLICATOR

A snapshot can be created with SnapProtect backup when Data Replicator is selected as the storage array. Data Replicator provides the snapshot functionality without the need for any specialized hardware.

For step-by-step instructions on creating a snapshot with Data Replicator as the software storage array, refer to SnapProtect™ Backup - Data Replicator.

Data Replicator is not supported when mining a snapshot on a single source computer.

## CONFIGURE SNAP MINING

You can mine data from a snapshot directly on the computer hosting the snapshot or from a proxy computer.

- Method 1:** Mining on a Proxy
- Method 2:** Mining on a Single Computer

## RELATED TOPICS

**SnapProtect™ Backup - Exchange Database**  
Use SnapProtect backup to create a point-in-time snapshot of the data using hardware storage arrays to provide snapshot functionality for data protection operations.

## METHOD 1: MINING ON A PROXY

Running the data protection job on a proxy server improves performance as it offloads processing on the production Exchange server.

Select one of the following configurations to run a snap mining job on the proxy computer. Then configure the subclient of the Exchange Mailbox *iDataAgent*.

- Configure on Source but Mine on Proxy
- Configure on Proxy and Mine on Proxy

### CONFIGURE ON SOURCE BUT MINE ON PROXY

In this configuration, the Exchange Database *iDataAgent* creates the snapshot on the source computer. To run the snap mining job on a proxy but configure it on the source computer, install the following components:

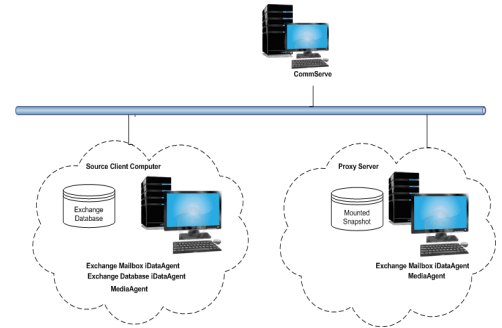
#### Source Computer

- Microsoft Exchange Server
- Exchange Database *iDataAgent*
- Exchange Mailbox *iDataAgent*
- MediaAgent
- VSS Provider (required for hardware storage arrays)
- ContinuousDataReplicator (if Data Replicator is the storage array)

#### Proxy Computer

- Exchange Mailbox *iDataAgent*
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

The Exchange Database and Exchange Mailbox Agents are installed on same source client. The Exchange Mailbox *iDataAgent* is also installed on the proxy server so that the subclient is configured on the source client. Mounting of the snapshot and backing it up are performed on the proxy computer.



### CONFIGURE ON PROXY AND MINE ON PROXY

In this configuration, the Exchange Database *iDataAgent* creates the snapshot on the source computer. To configure and run the snap mining job on a proxy computer, install the following components:

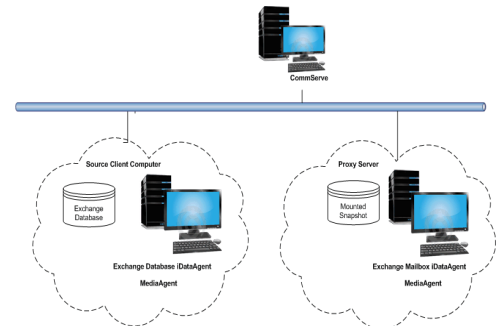
#### Source Computer

- Microsoft Exchange Server
- Exchange Database *iDataAgent*
- MediaAgent
- VSS Provider (required for hardware storage arrays)
- ContinuousDataReplicator (if Data Replicator is the storage array)

#### Proxy Computer

- Exchange Mailbox *iDataAgent*
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

The Exchange Mailbox *iDataAgent* is installed on the proxy server so configuration of the subclient content is performed on the proxy server. Mounting of the snapshot and backing it up are also performed on the proxy server.



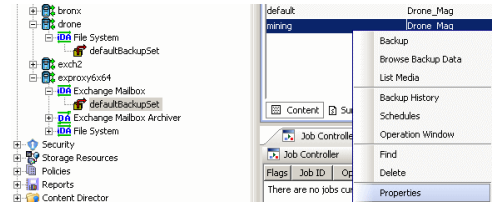
### CONFIGURE SUBCLIENT

A Snap Mining job is configured from a subclient of the Exchange Mailbox *iDataAgent*.

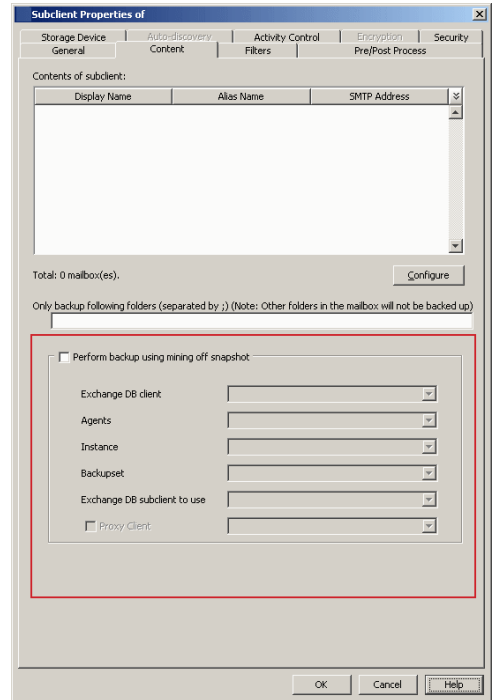
- Regardless of the settings in Agent properties (General tab), the Deleted Item Retention will always be protected in a snap mining operation.
- It is recommended to create one snap mining subclient for each database subclient, since only one subclient can mine from a snapshot at a time.
- It is not recommended to mix snap mining subclients and traditional subclients within the same backupset.
- Snap mining can be performed for databases configured in the subclient in which Snap Mining is enabled.
- Typically, the subclient is configured first before the snapshot is created. The only exception to this rule would be for NetApp snapshots that are discovered using External Data Connector. In this case, the subclient can be configured at any time.

Keep in mind that once snap mining is enabled for a subclient, it cannot be reversed.

- From the CommCell Browser, right-click a subclient of the Exchange Mailbox *iDataAgent* and select **Properties**.  
This subclient will be used to run the snap mining data protection job.



- Click the **Content** tab in **Subclient Properties**.
  - Click **Perform backup using mining off snapshot**.
  - Select the **Exchange DB client**. This is the source computer where the Exchange Database is installed and where the snapshot was created.
  - Select the **Agent** that was used to create the SnapProtect backup. In this case, it is **Exchange Database**.
  - Select the subclient on the source computer to use for mining the SnapProtect backup in **Exchange DB subclient to use**.
  - If you configured the snap mining job on a source computer but to be run on a proxy, select **Proxy Client** and select the proxy computer from the drop-down list.
    - The content of a subclient that will be used for snap mining should not be manually assigned. If any mailboxes are assigned to a subclient before running a snap mining data protection job, they may not be included in the job.
    - If the target database for the snap mining data protection job contains a mailbox that currently exists in another subclient, it will not be included in the data protection job. It is recommended to remove it from the other subclient's content so that the next snap mining data protection job will pick it up.
  - Click **OK** to save your changes.

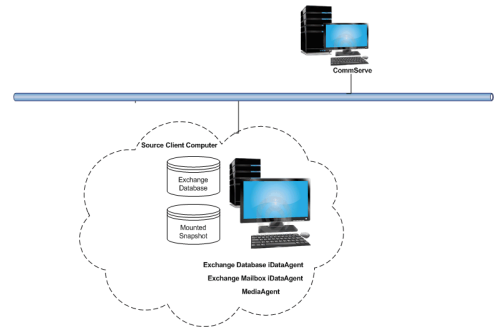


## METHOD 2: MINING ON A SINGLE COMPUTER

When running a snap mining job on a single computer, install the following components.

- Microsoft Exchange Server
- Exchange Database *iDataAgent*
- Exchange Mailbox *iDataAgent*
- VSS Provider (required for hardware storage arrays)
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

In this configuration, the Exchange Database and Mailbox *iDataAgents* are installed on the same computer, so creating the snapshot and configuring the subclient is performed on this computer. Mounting of the snapshot and backing it up are also performed on this computer.



### CONFIGURE SUBCLIENT

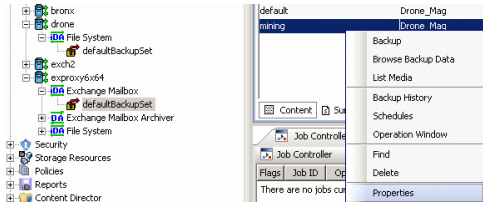
A Snap Mining job is configured from a subclient of the Exchange Mailbox *iDataAgent*.

- Regardless of the settings in Agent properties (General tab), the Deleted Item Retention will always be protected in a snap mining operation.
- It is recommended to create one snap mining subclient for each database subclient, since only one subclient can mine from a snapshot at a time.
- It is not recommended to mix snap mining subclients and traditional subclients within the same backupset.
- Snap mining can be performed for databases configured in the subclient in which Snap Mining is enabled.
- Typically, the subclient is configured first before the snapshot is created. The only exception to this rule would be for NetApp snapshots that are discovered using External Data Connector. In this case, the subclient can be configured at any time.

Keep in mind that once snap mining is enabled for a subclient, it cannot be reversed.

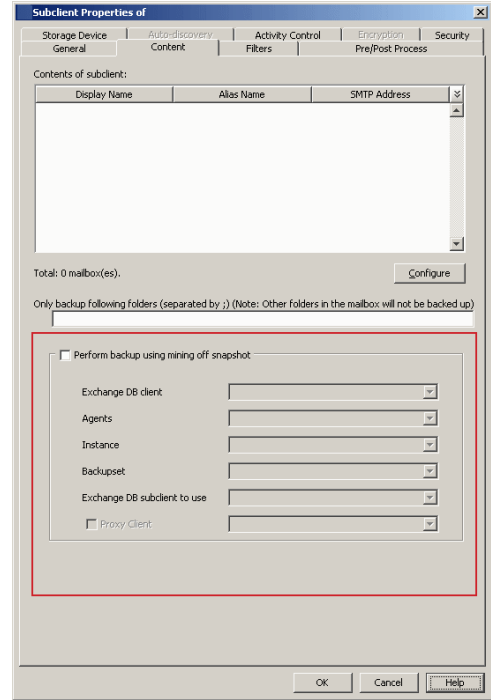
- From the CommCell Browser, right-click a subclient of the Exchange Mailbox *iDataAgent* and select **Properties**.

This subclient will be used to run the snap mining data protection job.



2. Click the **Content** tab in **Subclient Properties**.

- Click **Perform backup using mining off snapshot**.
- Select the **Exchange DB client**. This is the source computer where the Exchange Database is installed and where the snapshot was created.
- Select the **Agent** that was used to create the SnapProtect backup. In this case, it is **Exchange Database**.
- Select the subclient on the source computer to use for mining the SnapProtect backup in **Exchange DB subclient to use**.
- If you configured the snap mining job on a source computer but to be run on a proxy, select **Proxy Client** and select the proxy computer from the drop-down list.
  - The content of a subclient that will be used for snap mining should not be manually assigned. If any mailboxes are assigned to a subclient before running a snap mining data protection job, they may not be included in the job.
  - If the target database for the snap mining data protection job contains a mailbox that currently exists in another subclient, it will not be included in the data protection job. It is recommended to remove it from the other subclient's content so that the next snap mining data protection job will pick it up.
- Click **OK** to save your changes.



## CONFIGURING WAIT TIME FOR PARALLEL SNAP MINING

In cases where multiple Exchange Mailbox subclients are configured to mine from the same Exchange Database subclient the first job will prepare the snapshot to be used by all other concurrently running jobs. While this preparation is ongoing the other subclients will wait for preparation to complete. By default they will check the status of preparation every 15 minutes.

Once the snapshot is prepared the remaining subclients can continue with the backup phase. To change the frequency for checking the preparation status the key WAITTIME\_PARALLEL\_SNAPMINING can be created on the client for the appropriate agent.

- From the CommCell Browser, navigate to **Client Computers**.
- Right-click the <Client> in which you want to add the registry key, and then click **Properties**.
- Click the **Registry Key Settings** tab.
- Click **Add**.
- Enter WAITTIME\_PARALLEL\_SNAPMINING in the **Name** field.
- Enter <Instance Root>\MSExchangeMBAgent in the **Location** field (For Exchange Mailbox iDataAgent).
- Enter REG\_DWORD in the **Type** field.
- Enter *n* in the Value field.

Where *n* is the number of minutes the other jobs will wait before checking for the availability of metadata for snap mining.

- Click **OK**.

## CONFIGURING FOR PARALLEL SNAP MINING PREPARATION TIMEOUT

It is also advisable to set up a timeout value in case of parallel snap mining. This timeout value specifies the amount of time after which the mailbox subclients waiting for the snap preparation will start their own snap preparation process.

- From the CommCell Browser, navigate to **Client Computers**.
- Right-click the <Client> in which you want to add the registry key, and then click **Properties**.
- Click the **Registry Key Settings** tab.
- Click **Add**.
- Enter TIMEOUT\_PREPARATION\_PARALLEL\_SNAPMINING in the **Name** field.

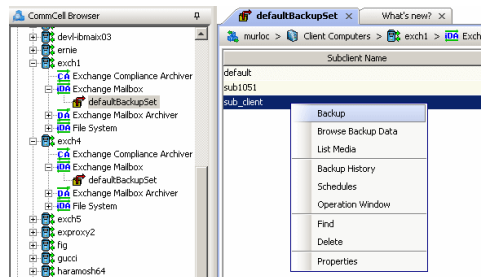
- Enter <Instance Root>\MSEExchangeMBAgent in the **Location** field (For Exchange Mailbox iDataAgent).
- Enter REG\_DWORD in the **Type** field.
- Enter *n* in the Value field.  
Where *n* is the number of minutes after which the jobs in the waiting state will timeout.
- Click **OK**.

## RUN A SNAP MINING JOB

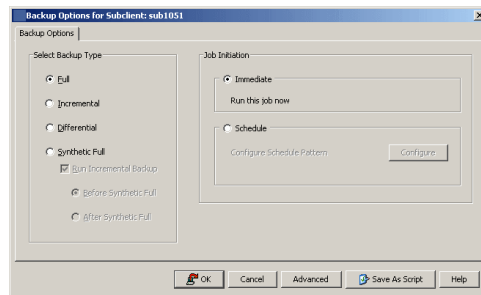
Run a snap mining job by selecting the subclient that was configured.

The procedure to run a snap mining data protection job is the same for all configurations, except for the configuration where the subclient is configured on the proxy server instead of the source computer.

1. Right-click the subclient that was configured and select **Backup**.



2. Click **Full** backup type.

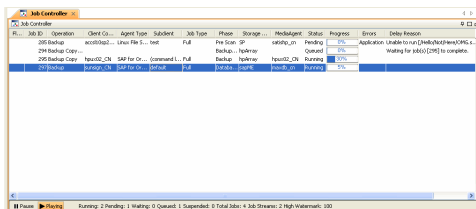


3. Click **OK**.

You can track the progress of the backup job from the **Job Controller** window.

If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically. Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

Once completed, the details of the job can be viewed in the **Job History** window.



4. Run a Browse and Restore operation.

## VIEW JOB HISTORY

Once a snap mining job has completed, it may be useful to view specific historical information about the job, such as the following:

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

This information can be viewed in the Job History window. The history provided depends on the entity from which the job history is viewed. For example, viewing job history from the subclient level will yield information for the jobs performed for that subclient. Conversely, viewing job history from the instance level will yield information for jobs run from all subclients within that instance.

To view the backup job history:

1. From the CommCell Browser, right-click the entity (client computer, iDataAgent, instance, or subclient) whose backup history you want to view, click **View**, and then click **View Job History**.

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

The system displays the Job History window.

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

To view the additional options discussed above, right-click the desired job choose the appropriate option.

4. Click **OK**.

## BEST PRACTICES

It is not recommended to use Regular Expression or Active Directory group auto-discovery affinity on a backupset which contains subclients configured for Snap Mining as the subclient content association may not behave as expected and some mailboxes may fail to be protected. In this case, it is recommended to use Database affinity as the auto-discovery method.

## FAQ

- Exchange 2010 message moderation approval requests may fail to restore if they were protected by a Snap Mining operation.
- Mailbox Quotas are not supported by Snap Mining.

---

## KEYWORDS

Snap Mining, Mining Exchange Data, Exchange Snap Mining.

[Back to Top](#)



# Accessing Archived Exchange Data from Database Snapshots

## TABLE OF CONTENTS

### Overview

### Prerequisites

### Create a Snapshot

- Hardware Supported Storage Array
- Data Replicator

### Configure Snap Mining

- Mining on a Proxy
- Mining on a Single Computer

### Configuring Wait Time for Parallel Snap Mining

### Configuring for Parallel Snap Mining Preparation Timeout

### Run a Snap Mining Job

### View Job History

### Best Practices

### FAQ

## OVERVIEW

Snap mining allows you to protect data from an offline copy of the Exchange database. The offline copy is a point-in-time snapshot of the data to be used for data protection operations. With snap mining, impact to the Exchange Server can be reduced in a production environment thus improving performance.

## PREREQUISITES

The following are prerequisites to using this feature:

- Mailboxes that are mined from a Microsoft Exchange 2003 32-bit Server database requires the 32-bit Exchange Mailbox iDataAgent.
- Mailboxes that are mined from a Microsoft Exchange 2007 64-bit Server or Microsoft Exchange 2010 64-bit Server databases require the 64-bit Exchange Mailbox iDataAgent.
- Ensure that the Operating System on the computer on which the Exchange Server is installed and the computer where the snap is mounted is the same.

## CREATE A SNAPSHOT

A snapshot needs to be created for snap mining. It can be created before or after configuring the subclient for snap mining. Snapshots are created in one of these ways:

- Hardware supported storage array
- Software storage array (Data Replicator)

---

### HARDWARE SUPPORTED STORAGE ARRAYS

A snapshot can be created with SnapProtect backup using a supported storage array.

For step-by-step instructions on creating a snapshot with a hardware storage array, refer to SnapProtect Backup - Microsoft Exchange Database.

---

### DATA REPLICATOR

A snapshot can be created with SnapProtect backup when Data Replicator is selected as the storage array. Data Replicator provides the snapshot functionality without the need for any specialized hardware.

For step-by-step instructions on creating a snapshot with Data Replicator as the software storage array, refer to SnapProtect™ Backup - Data Replicator.

Data Replicator is not supported when mining a snapshot on a single source computer.

## CONFIGURE SNAP MINING

You can mine data from a snapshot directly on the computer hosting the snapshot or from a proxy computer.

- Method 1:** Mining on a Proxy
- Method 2:** Mining on a Single Computer

## RELATED TOPICS

**SnapProtect™ Backup - Exchange Database**  
Use SnapProtect backup to create a point-in-time snapshot of the data using hardware storage arrays to provide snapshot functionality for data protection operations.

## METHOD 1: MINING ON A PROXY

Running the data protection job on a proxy server improves performance as it offloads processing on the production Exchange server.

Select one of the following configurations to run a snap mining job on the proxy computer. Then configure the subclient of the Exchange Mailbox Archiver Agent.

- Configure on Source but Mine on Proxy
- Configure on Proxy and Mine on Proxy

### CONFIGURE ON SOURCE BUT MINE ON PROXY

In this configuration, the Exchange Database *iDataAgent* creates the snapshot on the source computer. To run the snap mining job on a proxy but configure it on the source computer, install the following components:

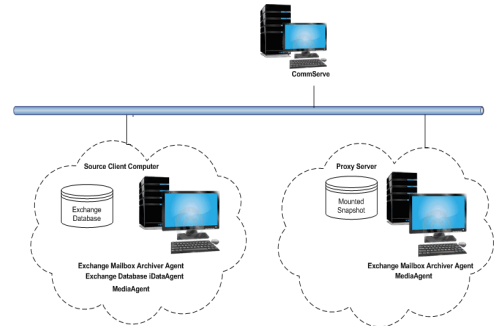
#### Source Computer

- Microsoft Exchange Server
- Exchange Database *iDataAgent*
- Exchange Mailbox Archiver Agent
- MediaAgent
- VSS Provider (required for hardware storage arrays)
- ContinuousDataReplicator (if Data Replicator is the storage array)

#### Proxy Computer

- Exchange Mailbox Archiver Agent
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

The Exchange Database and Exchange Mailbox Archiver Agents are installed on same source client. The Exchange Mailbox Archiver Agent is also installed on the proxy server and in this case, the configuration of the subclient is configured on the source client. Mounting of the snapshot and backing it up are performed on the proxy server.



### CONFIGURE ON PROXY AND MINE ON PROXY

In this configuration, the Exchange Database *iDataAgent* creates the snapshot on the source computer. To configure and run the snap mining job on a proxy computer, install the following components:

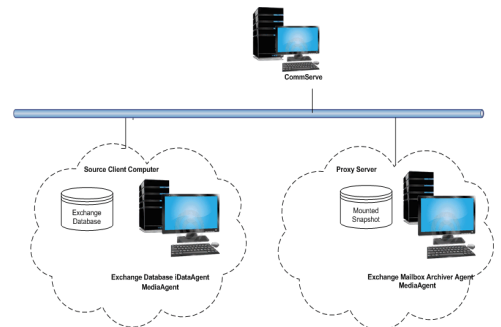
#### Source Computer

- Microsoft Exchange Server
- Exchange Database *iDataAgent*
- MediaAgent
- VSS Provider (required for hardware storage arrays)
- ContinuousDataReplicator (if Data Replicator is the storage array)

#### Proxy Computer

- Exchange Mailbox Archiver Agent
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

The Exchange Mailbox Archiver Agent is installed on the proxy server so configuration of the subclient content is performed on the proxy server. Mounting of the snapshot and backing it up are also performed on the proxy server.



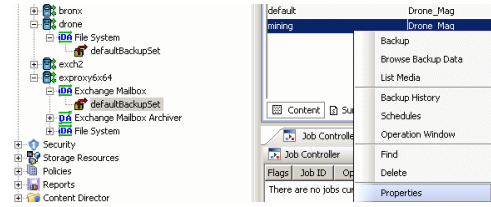
### CONFIGURE SUBCLIENT

A Snap Mining job is configured from a subclient of the Exchange Mailbox Archiver Agent.

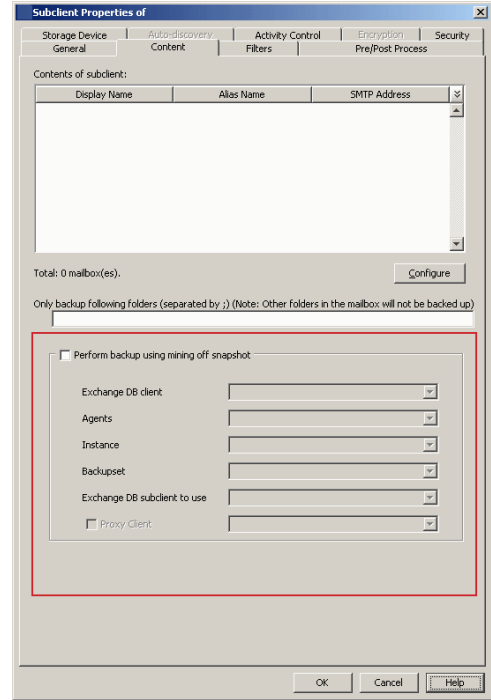
- It is recommended to create one snap mining subclient for each database subclient, since only one subclient can mine from a snapshot at a time.
- It is not recommended to mix snap mining subclients and traditional subclients within the same backupset.
- Snap mining can be performed for databases configured in the subclient in which Snap Mining is enabled.
- Typically, the subclient is configured first before the snapshot is created. The only exception to this rule would be for NetApp snapshots that are discovered using External Data Connector. In this case, the subclient can be configured at any time.

Keep in mind that once snap mining is enabled for a subclient, it cannot be reversed.

1. Right-click a subclient of the Exchange Mailbox Archiver Agent and select **Properties**.  
This subclient will be used to run the snap mining data protection job.



2. Click the **Content** tab in **Subclient Properties**.
  - Click **Perform backup using mining off snapshot**.
  - Select the **Exchange DB client**. This is the source computer where the Exchange Database is installed and where the snapshot was created.
  - Select the **Agent** that was used to create the SnapProtect backup. In this case, it is **Exchange Database**.
  - Select the subclient on the source computer to use for mining the SnapProtect backup in **Exchange DB subclient to use**.
  - If you configured the snap mining job on a source computer but to be run on a proxy, select **Proxy Client** and select the proxy computer from the drop-down list.
    - The content of a subclient that will be used for snap mining should not be manually assigned. If any mailboxes are assigned to a subclient before running a snap mining data protection job, they may not be included in the job.
    - If the target database for the snap mining data protection job contains a mailbox that currently exists in another subclient, it will not be included in the data protection job. It is recommended to remove it from the other subclient's content so that the next snap mining data protection job will pick it up.
  - Click **OK** to save your changes.



## METHOD 2: MINING ON A SINGLE COMPUTER

When running a snap mining job on a single computer, install the following components.

- Microsoft Exchange Server
- Exchange Database *iDataAgent*
- Exchange Mailbox Archiver Agent
- VSS Provider (required for hardware storage arrays)
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

In this configuration, the Exchange Database and Exchange Mailbox Archiver Agents are installed on the same source client, so the configuration of the subclient is configured on the source client. Mounting of the snapshot and backing it up are also performed on this client.

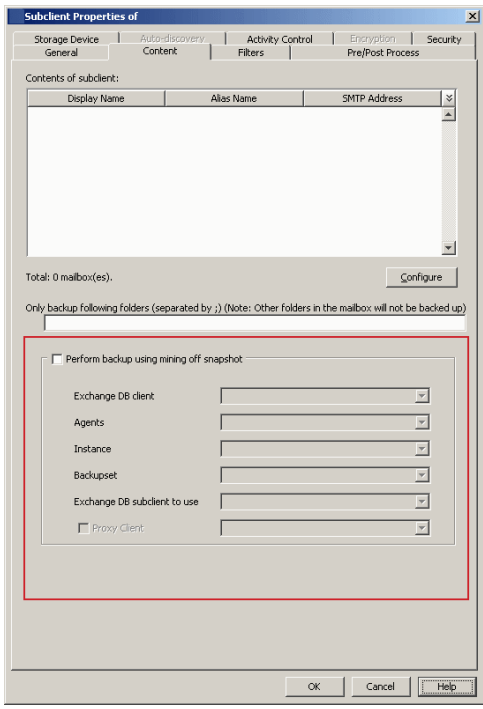
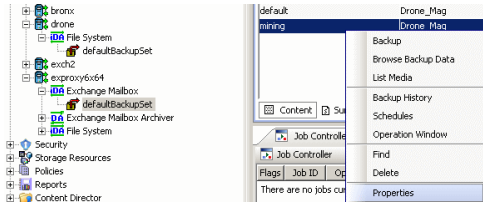
### CONFIGURE SUBCLIENT

A Snap Mining job is configured from a subclient of the Exchange Mailbox Archiver Agent.

- It is recommended to create one snap mining subclient for each database subclient, since only one subclient can mine from a snapshot at a time.
- It is not recommended to mix snap mining subclients and traditional subclients within the same backupset.
- Snap mining can be performed for databases configured in the subclient in which Snap Mining is enabled.
- Typically, the subclient is configured first before the snapshot is created. The only exception to this rule would be for NetApp snapshots that are discovered using External Data Connector. In this case, the subclient can be configured at any time.

Keep in mind that once snap mining is enabled for a subclient, it cannot be reversed.

1. Right-click a subclient of the Exchange Mailbox Archiver Agent and select **Properties**.  
This subclient will be used to run the snap mining data protection job.



2. Click the **Content** tab in **Subclient Properties**.
  - Click **Perform backup using mining off snapshot**.
  - Select the **Exchange DB client**. This is the source computer where the Exchange Database is installed and where the snapshot was created.
  - Select the **Agent** that was used to create the SnapProtect backup. In this case, it is **Exchange Database**.
  - Select the subclient on the source computer to use for mining the SnapProtect backup in **Exchange DB subclient to use**.
  - If you configured the snap mining job on a source computer but to be run on a proxy, select **Proxy Client** and select the proxy computer from the drop-down list.
    - The content of a subclient that will be used for snap mining should not be manually assigned. If any mailboxes are assigned to a subclient before running a snap mining data protection job, they may not be included in the job.
    - If the target database for the snap mining data protection job contains a mailbox that currently exists in another subclient, it will not be included in the data protection job. It is recommended to remove it from the other subclient's content so that the next snap mining data protection job will pick it up.
  - Click **OK** to save your changes.

## CONFIGURING WAIT TIME FOR PARALLEL SNAP MINING

In cases where multiple Exchange Mailbox subclients are configured to mine from the same Exchange Database subclient the first job will prepare the snapshot to be used by all other concurrently running jobs. While this preparation is ongoing the other subclients will wait for preparation to complete. By default they will check the status of preparation every 15 minutes.

Once the snapshot is prepared the remaining subclients can continue with the backup phase. To change the frequency for checking the preparation status the key WAITTIME\_PARALLEL\_SNAPMINING can be created on the client for the appropriate agent.

- From the CommCell Browser, navigate to **Client Computers**.
- Right-click the <Client> in which you want to add the registry key, and then click **Properties**.
- Click the **Registry Key Settings** tab.
- Click **Add**.
- Enter WAITTIME\_PARALLEL\_SNAPMINING in the **Name** field.
- Enter <Instance Root>\MSExchangeDMAgent in the **Location** field (For Exchange Mailbox Archiver).
- Enter REG\_DWORD in the **Type** field.
- Enter *n* in the Value field.

Where *n* is the number of minutes the other jobs will wait before checking for the availability of metadata for snap mining.

- Click **OK**.

## CONFIGURING FOR PARALLEL SNAP MINING PREPARATION TIMEOUT

It is also advisable to set up a timeout value in case of parallel snap mining. This timeout value specifies the amount of time after which the mailbox subclients waiting for the snap preparation will start their own snap preparation process.

- From the CommCell Browser, navigate to **Client Computers**.
- Right-click the <Client> in which you want to add the registry key, and then click **Properties**.
- Click the **Registry Key Settings** tab.
- Click **Add**.
- Enter TIMEOUT\_PREPARATION\_PARALLEL\_SNAPMINING in the **Name** field.

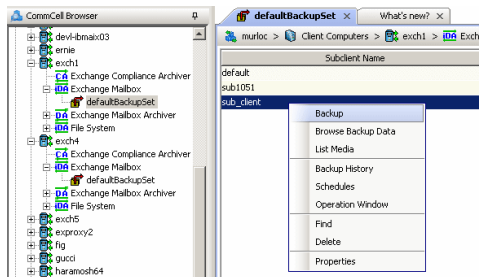
- Enter <Instance Root>\MSEExchangeDMAgent in the **Location** field (For Exchange Mailbox Archiver).
- Enter REG\_DWORD in the **Type** field.
- Enter *n* in the Value field.  
Where *n* is the number of minutes after which the jobs in the waiting state will timeout.
- Click **OK**.

## RUN A SNAP MINING JOB

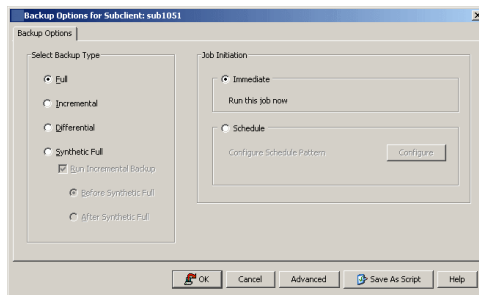
Run a snap mining job by selecting the subclient that was configured.

The procedure to run a snap mining data protection job is the same for all configurations, except for the configuration where the subclient is configured on the proxy server instead of the source computer.

1. Right-click the subclient that was configured and select **Backup**.



2. Click **Full** backup type.

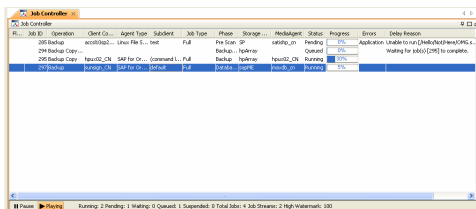


3. Click **OK**.

You can track the progress of the backup job from the **Job Controller** window.

If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically. Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

Once completed, the details of the job can be viewed in the **Job History** window.



4. Run a Browse and Restore operation.

## VIEWING JOB HISTORY

Once a snap mining job has completed, it may be useful to view specific historical information about the job, such as the following:

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

This information can be viewed in the Job History window. The history provided depends on the entity from which the job history is viewed. For example, viewing job history from the subclient level will yield information for the jobs performed for that subclient. Conversely, viewing job history from the instance level will yield information for jobs run from all subclients within that instance.

To view the backup job history:

1. From the CommCell Browser, right-click the entity (client computer, iDataAgent, instance, or subclient) whose backup history you want to view, click **View**, and then click **View Job History**.

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

The system displays the Job History window.

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

To view the additional options discussed above, right-click the desired job choose the appropriate option.

4. Click **OK**.

## **BEST PRACTICES**

It is not recommended to use Regular Expression or Active Directory group auto-discovery affinity on a archiveset which contains subclients configured for Snap Mining as the subclient content association may not behave as expected and some mailboxes may fail to be protected. In this case, it is recommended to use Database affinity as the auto-discovery method.

## **FAQ**

- Exchange 2010 message moderation approval requests may fail to restore if they were protected by a Snap Mining operation.
- Mailbox Quotas are not supported by Snap Mining operations.
- Exchange 2010 Archive Mailboxes are not supported for Snap Mining operations.

[Back to Top](#)

# Accessing SharePoint Data from SQL Database Snapshots

## TABLE OF CONTENTS

### Overview

#### Prerequisites

Microsoft SharePoint

#### Create a Snapshot

Hardware Supported Storage Array  
Data Replicator

#### Configure Snap Mining

Mining on a Proxy  
Mining on a Single Computer

#### Run a Snap Mining Job

#### View Job History

#### Mining a SnapProtect Backup from SharePoint

Mounting a Snapshot of a SharePoint Content Database  
Attaching the Snapshot to a Database on a SQL Server Instance  
Accessing the Snapshot from SharePoint Central Administration

#### Best Practices

## RELATED TOPICS

**SnapProtect™ Backup - Microsoft SQL Server**  
Use SnapProtect backup to create a point-in-time snapshot of the data using hardware storage arrays to provide snapshot functionality for data protection operations.

## OVERVIEW

Snap mining allows a granular-level SharePoint Document data protection job to be run from an offline snapshot of SharePoint SQL databases. With snap mining, performance is improved since processing calls are no longer required from the production back-end SQL Server during a data protection job of an offline SnapProtect backup. Processing also improves on SharePoint Front-End Web Servers when the data protection job is run on a proxy server.

## PREREQUISITES

The following are prerequisites to using this feature:

---

### MICROSOFT SHAREPOINT

These versions of Microsoft SharePoint are supported for snap mining:

- MOSS 2007
- WSS v3.0
- SharePoint 2010 Foundation
- SharePoint Server 2010

### CREATE A SNAPSHOT

A snapshot needs to be created for snap mining. It can be created before or after configuring the subclient for snap mining. Snapshots are created in one of these ways:

- Hardware supported storage array
- Software storage array (Data Replicator)
- NetApp snapshots

---

### HARDWARE SUPPORTED STORAGE ARRAYS

A snapshot can be created with SnapProtect backup using a supported storage arrays.

For step-by-step instructions on creating a snapshot with a hardware storage array, refer to SnapProtect Backup - Microsoft SQL Server.

---

### DATA REPLICATOR

A snapshot can be created with SnapProtect backup when Data Replicator is selected as the storage array. Data Replicator provides the snapshot functionality without the need for any specialized hardware.

For step-by-step instructions on creating a snapshot with Data Replicator as the software storage array, refer to SnapProtect™ Backup - Data Replicator.

Data Replicator is not supported when mining a snapshot on a single source computer.

## CONFIGURE SNAP MINING

You can mine data from a snapshot directly on the computer hosting the snapshot or from a proxy computer.

- **Method 1:** Mining on a Proxy
- **Method 2:** Mining on a Single Computer

### METHOD 1: MINING ON A PROXY

Select one of the following configurations to run a snap mining job on the proxy computer. Then configure the subclient of the SharePoint Server iDataAgent.

- Configure on Source but Mine on Proxy
- Configure on Proxy and Mine on Proxy

#### CONFIGURE ON SOURCE BUT MINE ON PROXY SERVER

The SQL Server iDataAgent creates the snapshot on the source computer. To run the snap mining job on a proxy but configure it on the source computer, install the following components:

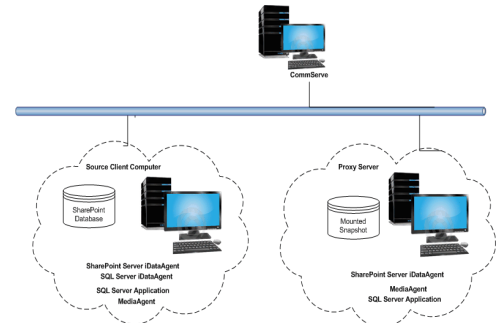
##### Source Computer

- SQL Server application
- SQL Server iDataAgent
- SharePoint Server iDataAgent
- MediaAgent
- VSS Provider (required for hardware storage arrays)
- ContinuousDataReplicator (if Data Replicator is the storage array)

##### Proxy Computer

- SQL Server application
- SharePoint Server iDataAgent
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

The configuration of the subclient content of the SharePoint Server iDataAgent is performed on the source client. Mounting of the snapshot and backing it up are performed on the proxy computer.



#### CONFIGURE ON PROXY AND MINE ON PROXY SERVER

The SQL Server iDataAgent creates the snapshot on the source computer. To configure and run the snap mining job on a proxy, install the following components:

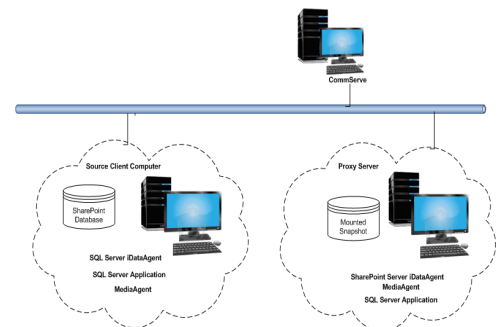
##### Source Computer

- SQL Server application
- SQL Server iDataAgent
- MediaAgent
- VSS Provider (required for hardware storage arrays)
- ContinuousDataReplicator (if Data Replicator is the storage array)

##### Proxy Computer

- SQL Server application
- SharePoint Server iDataAgent
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

The SharePoint Server iDataAgent is installed on the proxy server and configuration of the subclient content is performed on the proxy server. Mounting of the snapshot and backing it up are also performed on the proxy server.



### CONFIGURE SUBCLIENT

A Snap Mining job is configured from a subclient of the SharePoint Server iDataAgent.

- It is not recommended to mix snap mining subclients and traditional subclients within the same backupset.
- Snap mining can be performed for databases configured in the subclient in which Snap Mining is enabled.
- Typically, the subclient is configured first before the snapshot is created. The only exception to this rule would be for NetApp snapshots that are discovered using External Data Connector. In this case, the subclient can be configured at any time.

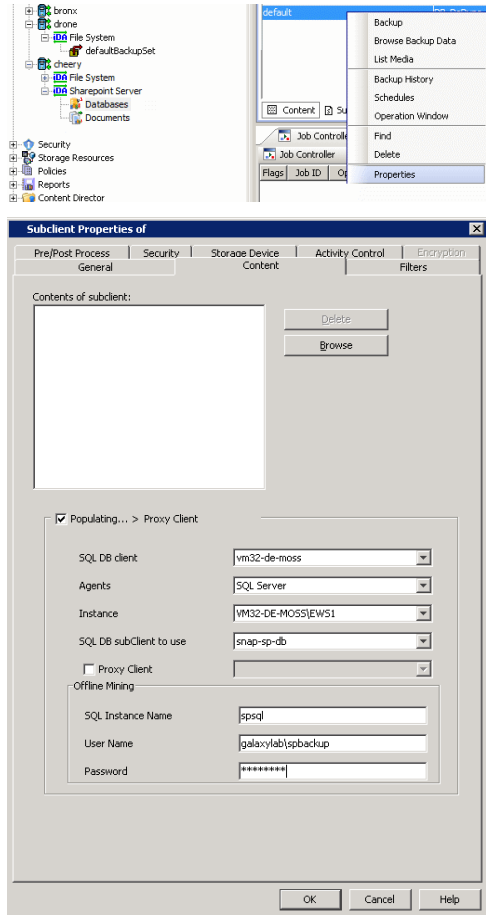


Keep in mind that once snap mining is enabled for a subclient, it cannot be reversed.

- From the CommCell Browser, right-click a subclient of the SharePoint Server iDataAgent and select **Properties**.

This subclient will be used to run the snap mining data protection job.

- Click the **Content** tab in **Subclient Properties**.
  - Click **Populating... > Proxy Client**.
    - Select the **SQL DB client**. This is the source client computer where the SharePoint Databases are located.
    - Select the **Agent** that was used to create the SnapProtect backup. In this case, it is **SQL Server**.
    - Select the **Instance** of the SQL Server iDataAgent used to create the SnapProtect backup.
    - Select the subclient on the source computer to use for mining the SnapProtect backup from the **SQL DB subclient to use** drop-down list.
    - If you are using a proxy computer to run the snap mining job, click **Proxy Client** and select the proxy computer.
  - In the **Offline Mining** section:
    - Specify the **SQL Instance Name** that will be used to mine the offline databases.
    - Enter the credentials in **User Name** and **Password** to access the offline databases so that the snapshot is successfully mounted and attached.
  - Click **OK** to save your changes.

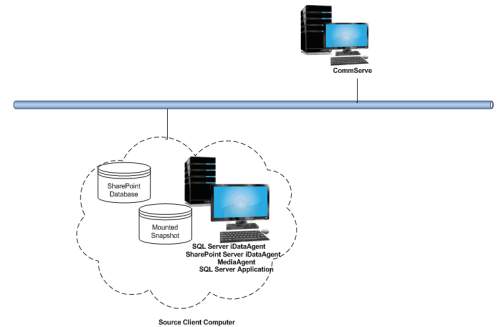


## METHOD 2: MINING ON A SINGLE COMPUTER

When running a snap mining job on a single computer, install the following components:

- SQL Server application
- SQL Server iDataAgent
- SharePoint Server iDataAgent
- VSS Provider (required for hardware storage arrays)
- MediaAgent
- ContinuousDataReplicator (if Data Replicator is the storage array)

In this configuration, the SQL Server and SharePoint Server iDataAgents are installed on the same computer, so creating the snapshot and configuring the subclient is performed on this computer. Mounting of the snapshot and backing it up are also performed on this computer.



### CONFIGURE SUBCLIENT

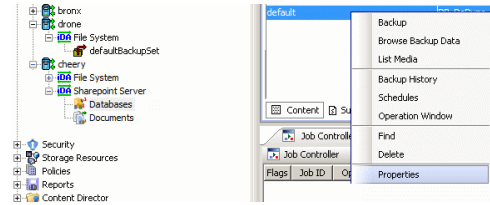
A Snap Mining job is configured from a subclient of the SharePoint Server iDataAgent.

- It is not recommended to mix snap mining subclients and traditional subclients within the same backupset.
- Snap mining can be performed for databases configured in the subclient in which Snap Mining is enabled.
- Typically, the subclient is configured first before the snapshot is created. The only exception to this rule would be for NetApp snapshots that are discovered using External Data Connector. In this case, the subclient can be configured at any time.

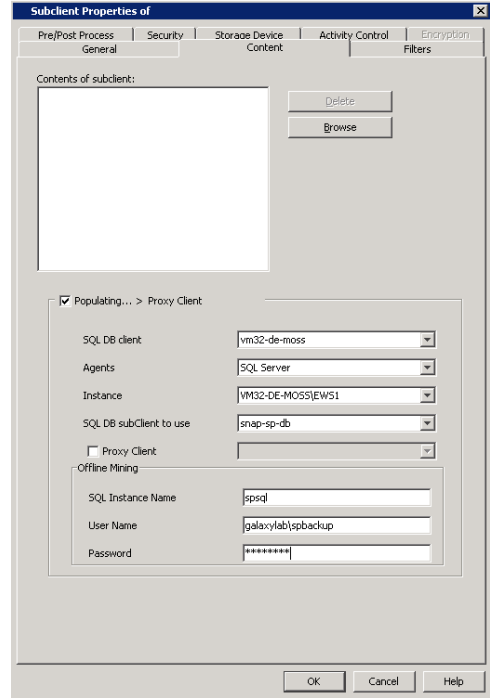
Keep in mind that once snap mining is enabled for a subclient, it cannot be reversed.

- From the CommCell Browser, right-click a subclient of the SharePoint Server iDataAgent and select **Properties**.

This subclient will be used to run the snap mining data protection job.



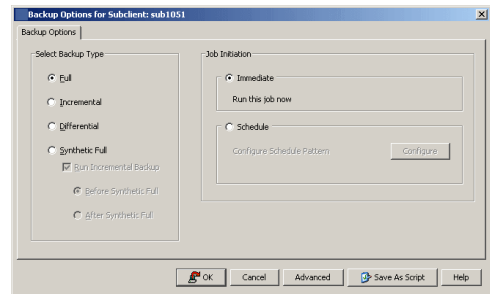
- Click the **Content** tab in **Subclient Properties**.
  - Click **Populating...> Proxy Client**.
    - Select the **SQL DB client**. This is the source client computer where the SharePoint Databases are located.
    - Select the **Agent** that was used to create the SnapProtect backup. In this case, it is **SQL Server**.
    - Select the **Instance** of the SQL Server iDataAgent used to create the SnapProtect backup.
    - Select the subclient on the source computer to use for mining the SnapProtect backup from the **SQL DB subclient to use** drop-down list.
    - If you are using a proxy computer to run the snap mining job, click **Proxy Client** and select the proxy computer.
  - In the **Offline Mining** section:
    - Specify the **SQL Instance Name** that will be used to mine the offline databases.
    - Enter the credentials in **User Name** and **Password** to access the offline databases so that the snapshot is successfully mounted and attached.
  - Click **OK** to save your changes.



## RUN A SNAP MINING JOB

Run a snap mining job by selecting the subclient that was configured.

- Right-click the subclient that was configured and select **Backup**.
- Click **Full** backup type.

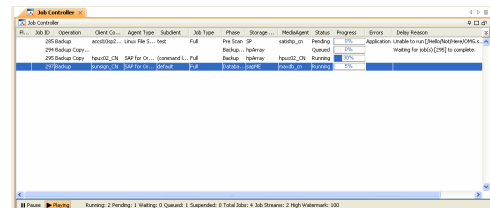


- Click **OK**.  
You can track the progress of the backup job from the **Job Controller** window.

If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically. Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

Once completed, the details of the job can be viewed in the **Job History** window.

- Run a Browse and Restore operation.



## VIEW JOB HISTORY

Once a snap mining job has completed, it may be useful to view specific historical information about the job, such as the following:

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

This information can be viewed in the Job History window. The history provided depends on the entity from which the job history is viewed. For example, viewing job history from the subclient level will yield information for the jobs performed for that subclient. Conversely, viewing job history from the instance level will yield information for jobs run from all subclients within that instance.

To view the backup job history:

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

The system displays the Job History window.

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

To view the additional options discussed above, right-click the desired job choose the appropriate option.

4. Click **OK**.

## MINING A SNAPPROTECT BACKUP FROM SHAREPOINT

You can restore a SnapProtect backup of a SharePoint content database without restoring a configuration database, and then mine the contents of the snapshot with SharePoint Central Administration.

1. Restore a snapshot of a SharePoint content database to a mount location.
2. Using SQL Server Management Studio, attach the snapshot of the SharePoint content database to a SQL server instance.
3. Using SharePoint Central Administration, browse or back up files from the snapshot of the SharePoint content database that are attached to the SQL server instance.

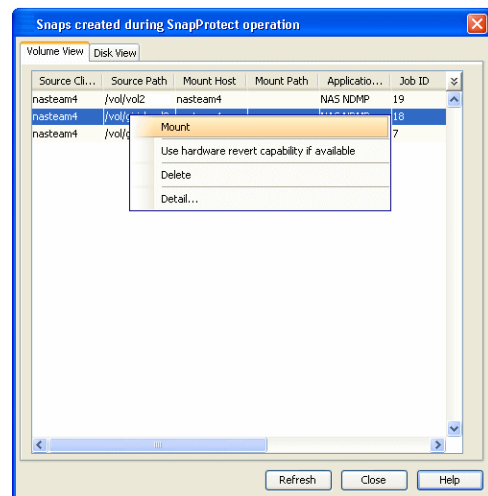
## MOUNTING A SNAPSHOT OF A SHAREPOINT CONTENT DATABASE

Perform the following operation on an SQL Server iDataAgent that contains a snapshot of a SharePoint content database.

You can mount any available snapshot to access the data included in the snapshot. It is recommended that you select the option to protect a snapshot when it is mounted, as this will ensure that the changes made to the snapshot when it is mounted are not retained when you unmount the snapshot and the snapshot is usable for data protection operations. Follow the steps given below to mount snapshots:

1. From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **SQL Server**.
2. Right-click **<Instance>**, point to **All Tasks**, and then click **List Snaps**.
3. Right-click the snapshot that you wish to mount and click **Mount**.
4. Click **Yes**.
5. In the **Mount Path** dialog box, specify the destination client and the path on the client in the **Destination Client** and **Destination Path** fields.  
On a Windows platform, enter a **CIFS Share Name** for the Agent.
6. If you do not wish to save any changes made to the mounted snapshot after the snapshot is unmounted, select **Protect Snapshot during mount**.
7. Click **OK**.

If you do not select **Protect Snapshot during mount**, the changes made to snapshot when it is mounted will be retained after the snapshot is unmounted and the snapshot can no longer be used for restore.

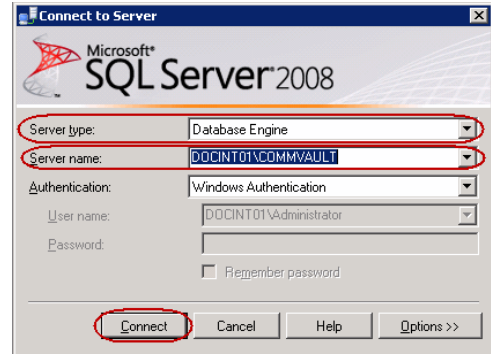


## ATTACHING THE SNAPSHOT TO A DATABASE ON A SQL SERVER INSTANCE

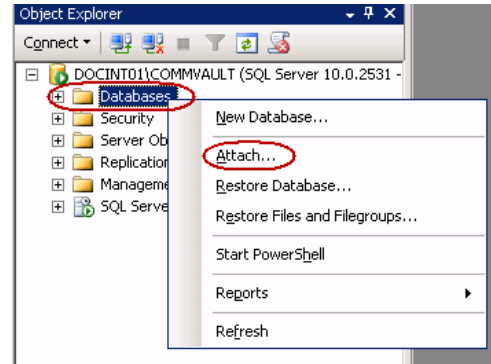
You must attach the snapshot of the SharePoint content database using SQL Server Management Studio.

To attach the snapshot to a database on a SQL server instance:

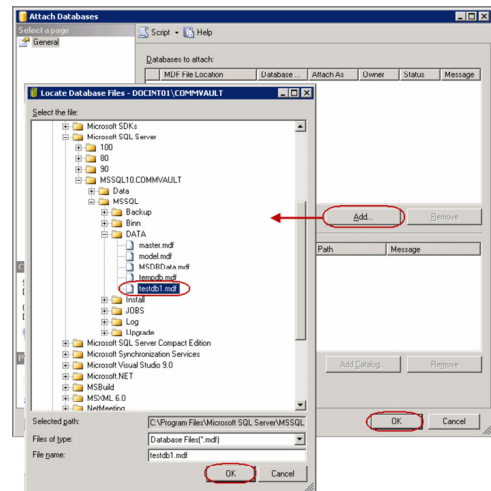
1. Open **Microsoft SQL Server Management Studio**.
2. From the **Server type** list, select **Database Engine**.



3. In the **Server name** list, specify a server, and then click **Connect**.
6. In **Object Explorer**, right-click **Databases**, and then click **Attach**.



7. In the **Attach Databases** dialog box, click **Add**.



8. In the **Locate Database Files** dialog box, navigate to the disk drive where the snapshot of the SharePoint content database resides, and then select the **.mdf** file for the snapshot.

9. Click **OK**.

10. Click **OK**.  
The snapshot is now attached to the SQL Server instance.

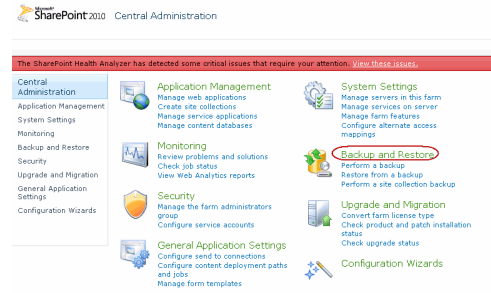
## ACCESSING THE SNAPSHOT FROM SHAREPOINT CENTRAL ADMINISTRATION

Once you have attached the SharePoint content database snapshot to a SQL server instance, you can then view, back up, or restore the contents. You must perform these steps inside SharePoint Central Administration.

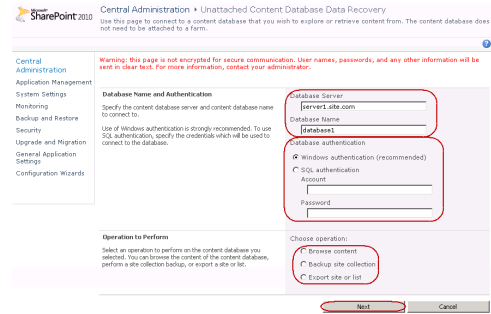
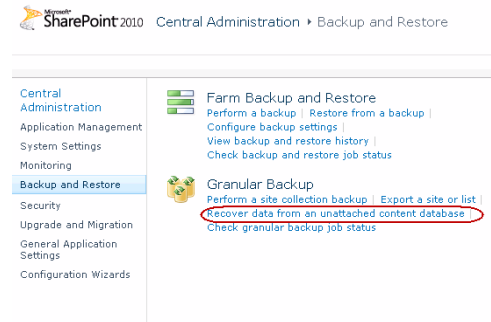
To access the SharePoint content database snapshot from the SharePoint Central Administration application:

1. Open the **SharePoint Central Administration** application.
2. Click **Backup and Restore**.

- Under **Granular Backup**, click **Recover data from an unattached content database**.



- In the **Database Server** box, enter the name of the Database Server where the content database is located.
- In the **Database Name** box, enter the name of the content database.
- Under **Database authentication**, select an authentication type, and if required, enter the appropriate credentials.
- Select one of the options, and then click **Next**.
  - To view the contents of the snapshot, select **Browse content**.
  - To back up the snapshot, select **Backup site collection**.
  - To restore the contents of the snapshot, select **Export site or list**.



## BEST PRACTICES

During snap mining backup, views that reside on a Web Server's file system will not be backed up.

Back to Top

