

Quick Start Guide - OSSV Plug-In

TABLE OF CONTENTS

OVERVIEW

NEW FEATURES

SYSTEM REQUIREMENTS

GETTING STARTED - SETUP THE NETAPP OSSV AGENT

GETTING STARTED - OSSV PLUG-IN DEPLOYMENT ON WINDOWS

GETTING STARTED - OSSV PLUG-IN ON UNIX

GETTING STARTED - OSSV PLUG-IN CONFIGURATION

GETTING STARTED - OSSV PLUG-IN BACKUP

GETTING STARTED - OSSV PLUG-IN RESTORE

Overview - OSSV Plug-In

TABLE OF CONTENTS

Introduction

Key Features

- Comprehensive Backup and Restore Capabilities
- Heterogeneous Environment Support
- Efficient Job Management and Reporting
- Block Level Deduplication

Add-On Components

- File System Restore Enabler

Terminology

INTRODUCTION

The OSSV Plug-In agent provides a simplified end-to-end backup and recovery solution for the data residing on a client computer. The OSSV Plug-In creates a relationship between the client and a secondary file server using the NetApp Open Systems SnapVault (OSSV) Agent and VSS/QSnap. This relationship allows the creation of an OSSV volume, which contains the data from the client, on the secondary file server. The MediaAgent takes the role of a Data Management Agent to allow the NetApp OSSV agent to transfer the data from the client to the file server.

In addition to complete protection of file system and application data, the OSSV Plug-In also provides more granular backup and recovery options that operate seamlessly with your data protection.

KEY FEATURES

The OSSV Plug-In offers the following key features:

COMPREHENSIVE BACKUP AND RESTORE CAPABILITIES

The OSSV Plug-In provides the flexibility to backup and restore the data residing on various client computers. You can perform one full backup of the entire data or many incremental backups. The backup data can be restored to different client computers.

The OSSV Plug-In also provides the capability to make a copy of the OSSV volume backup and send it to media. These copies use the NAS backup and restore process.

HETEROGENEOUS ENVIRONMENT SUPPORT

You can backup the data on LUNs from file servers other than NetApp (e.g., HDS or EMC). The OSSV Plug-In reads these LUNs on your client as local volumes, allowing you to perform regular backup and restore operations.

EFFICIENT JOB MANAGEMENT AND REPORTING

You can view and verify the status of the backup and recovery operations from the Job Controller and Event Viewer windows within the CommCell Console. You can also track the status of the jobs using reports, which can be saved and easily distributed. Reports can be generated for different aspects of data management. You also have the flexibility to customize the reports to display only the required data and save them to any specified location in different formats. For example, you can create a backup job summary report to view at-a-glance the completed backup jobs.

In addition, you can also schedule these reports to be generated and send them on email without user intervention.

BLOCK LEVEL DEDUPLICATION

You can perform deduplication on the OSSV volume created on the file server during backup. Deduplication provides a smarter way of storing data by identifying and eliminating the duplicate items in a data protection operation.

Deduplication at the data block level compares blocks of data against each other. If an object (file, database, etc.) contains blocks of data that are identical to each other, then block level deduplication eliminates storing the redundant data and reduces the size of the object in storage. This way dramatically reduces the backup data copies on both the disk and tapes.

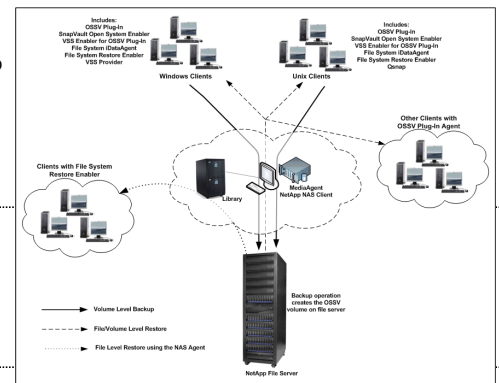
ADD-ON COMPONENTS

FILE SYSTEM RESTORE ENABLER

WHERE TO GO NEXT

Install the OSSV Plug-In

Walks you through the process of installing the OSSV Plug-In.



The File System Restore Enabler allows data that was backed up from a NetApp file server to be restored to a Windows or Unix computer. A file system restore is a cross-platform restore, where the data is restored to a computer with a different operating system e.g., data from a NetApp file server running ONTAP can be restored to a Windows computer.

TERMINOLOGY

The OSSV Plug-In documentation uses the following terminology:

CLIENT	The computer in which the Agent is installed and contains the data to be secured.
SUBCLIENT	The volume containing the client computer data used for backup and restore operations.
FILE SERVER	A device used for backup or archival purposes.
OSSV VOLUME	A volume created on the file server which contains the data from the client.
DATA MANAGEMENT AGENT	An agent that manages the OSSV backup process.
SNAPVAULT SNAPSHOT	A snapshot of the OSSV volume on the file server.

System Requirements - OSSV Plug-In

The following requirements are for the OSSV Plug-In:

OPERATING SYSTEM		PROCESSOR
LINUX	RED HAT ENTERPRISE LINUX	
	Red Hat Enterprise Linux 5.x with glibc 2.5.x	x64
	Red Hat Enterprise Linux 4.x with glibc 2.3.x	x64
	SUSE LINUX (SLES)	
	SuSE Linux 11 Enterprise Server with kernel 2.6.32.12-0.7 (Update 1)	x64
	SuSE Linux 11 Enterprise Server with kernel 2.6.27.19-5	x64
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.54.5 (Update 3)	x64
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.60-0.21 (Update 2)	x64
	SuSE Linux 10 Enterprise Server with kernel 2.6.16.46-0.12 (Update 1)	x64
SOLARIS	Solaris 9 with a minimum of Service Packs 111711-02	Sparc5 or higher recommended
	Solaris 10.x with a minimum of SunOS (Sparc) Patch 119963-14	Sparc5 or higher recommended
WINDOWS	WINDOWS 2008	
	Microsoft Windows Server 2008 32-bit and x64 Editions *Core Editions not supported	All Windows-compatible processors supported
	WINDOWS 2003	
	Microsoft Windows Server 2003 32-bit and x64 Editions with a minimum of Service Pack 1	All Windows-compatible processors supported

HARD DRIVE

LINUX AND SOLARIS

225 MB minimum of hard drive space for software.

100 MB of additional hard disk space for log file growth.

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

WINDOWS

101 MB minimum of hard disk space for software. The recommended space is 148 MB.

50 MB of additional hard disk space for log file growth.

725 MB of temp space required to install or upgrade (where the temp folder resides).

MEMORY

LINUX AND SOLARIS

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

Swap space = 2*RAM size

WINDOWS

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

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

NETWORK

TCP/IP Services configured on the computer.

MICROSOFT VISUAL C++

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

.NET FRAMEWORK

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

SELINUX

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

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

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

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

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

```
[root]# make backup_IDA.pp
Compiling targeted backup_IDA module
/usr/bin/checkmodule: loading policy configuration from tmp/backup_IDA.tmp
```

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

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

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

SELinux is now configured to work with this application.

DISCLAIMER

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

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

Getting Started - Setup the NetApp OSSV Agent

[< Previous](#) [Next >](#)

WHERE TO INSTALL

Install the NetApp Open System SnapVault (OSSV) Agent software on a client computer where you plan to install the OSSV Plug-In Agent. The client computer should have the NetApp Host Agent installed.

INSTALLATION

The NetApp OSSV Agent can be installed on the following operating systems:

WINDOWS

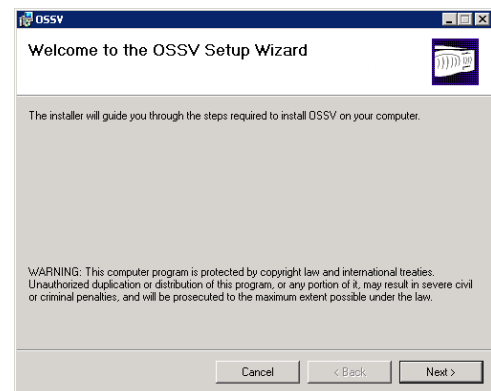
Use this procedure to install the software on a Windows client from the installation package and to configure the OSSV Configurator tool.

UNIX

Use this procedure to install the software on a Unix client from the installation package.

WINDOWS

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 **Disc 21**.
3. Click **Next**.



4. Select **I Agree**.
Click **Next**.



5.
 - Enter the NDMP account name and password.
The same NDMP credentials will be needed during the OSSV Plug-In Agent installation.
 - Click **Next**.

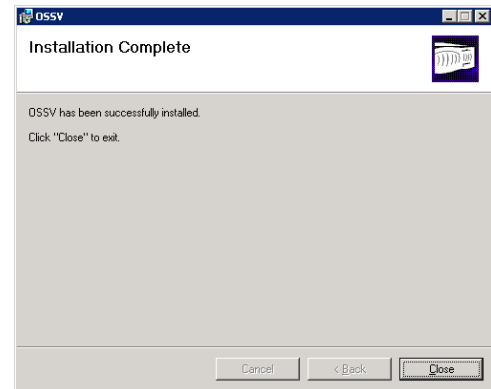
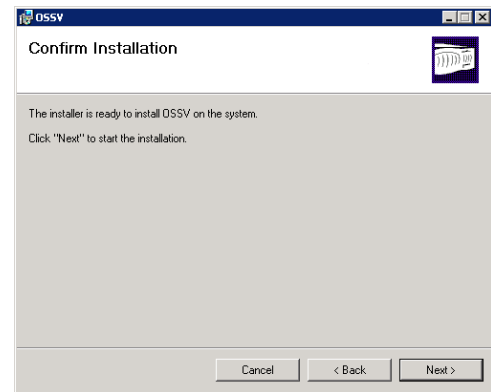
- 6.
- Enter the port to listen on for NDMP requests.
 - Click **Next**.

- 7.
- Enter the host name or IP address of a secondary storage system where you can back up the data from this client computer.
 - Click **Next**.

- 8.
- Specify the location for the NetApp OSSV Agent.
 - Click **Browse** to change directories.
 - Click **Next**.

9. Click **Next**.

10. Click **Close**.



UNIX

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. To install the software from CD, run the following command to mount the CD:
`mount -t iso9660,udf /dev/cdrom /mnt/cdrom`
Run the following command from the Software Installation Package or mount point:
`./install`
If you are installing on a Solaris computer, run the following command:
`pkgadd -d <software_path> ossv`
where `<software_path>` is the full path where the OSSV package is located.
3. Read the license agreement. Type **y** and press **Enter**.
4. Press **Enter** to accept the default location.
If you want to install to a different location, enter a path to modify the default location and press **Enter**.
5. Enter the NDMP account name and press **Enter**.
6. Enter the NDMP account password and press **Enter**.
The same NDMP credentials will be needed during the OSSV Plug-In Agent installation.
7. Press **Enter**.
8. Enter the host name or IP address of a secondary storage system where you can back up the data from this client computer.
Press **Enter**.
The installation completes successfully.

Please enter the path where you would like the SnapVault directory to be created [/usr/snapvault]:

Enter the User Name to connect to this machine via the NDMP protocol: [ndmp]

Enter the password to connect to this machine via the NDMP protocol:

Confirm password:

Enter the NDMP listen port [10000]:

Enter the hostname or IP address of the SnapVault secondary storage system(s) allowed to backup this machine. Multiple hostnames or IP addresses must be comma separated.

>:[mycomputer.mydomain.com]

Getting Started - OSSV Plug-In Deployment on Windows

◀ Previous Next ▶

WHERE TO INSTALL

Install the software on a client computer that satisfies the minimum requirements specified in the System Requirements and with the following configurations:

- NetApp SnapVault OSSV Agent v3.0.1P1 installed.
- Client computer is connected to a NetApp file server that you want to protect. The Windows Primary and Secondary Snap Vault licenses must be present on the file server.

To backup the data from OSSV volumes, you need to install the MediaAgent software which includes the NAS iDataAgent. If the library is attached to the MediaAgent, you need to install the NDMP Remote Server software.

INSTALLATION

The software can be installed using one of the following methods:

METHOD 1: INTERACTIVE INSTALL

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

METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

Use this procedure to install remotely on a client computer.

BEFORE YOU BEGIN

Download Software Packages

Download the latest software package to perform the install.

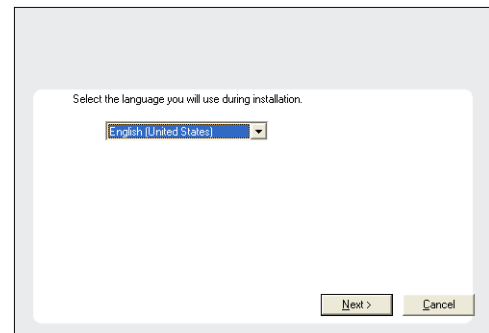
Verify System Requirements

Make sure that the computer in which you wish to install the software satisfies the System Requirements.

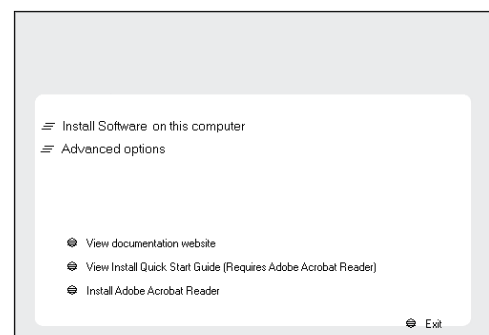
METHOD 1: INTERACTIVE INSTALL

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 **Common Technology Engine | MediaAgent Modules** and select **MediaAgent**.

If the library is attached to the MediaAgent, select **NDMP Remote Server**.

Expand **Client Modules | Backup & Recovery | File System** and select **Windows File System iDataAgent**.

Expand **Client Modules | OSSV Plug-In** and select **OSSV Agent**. The following are automatically selected:

- **VSS Enabler for OSSV Plug-In**
- **SnapVault Open System Enabler**
- **VSS Provider**
- **File System NDMP Restore Enabler**

Click **Next**.

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

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

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

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

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

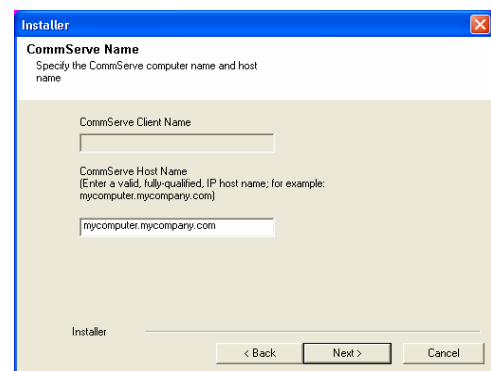
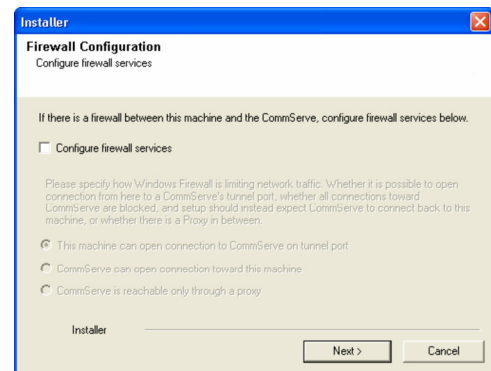
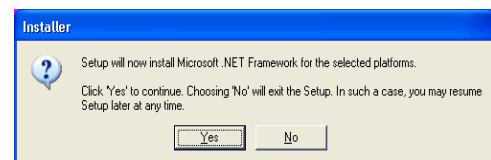
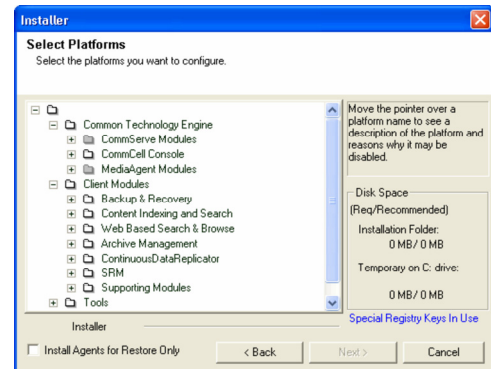
8. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

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

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

9. Click **Next**.



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

Click **Next**.

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

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

11. 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:

/ : * ? " < > | #

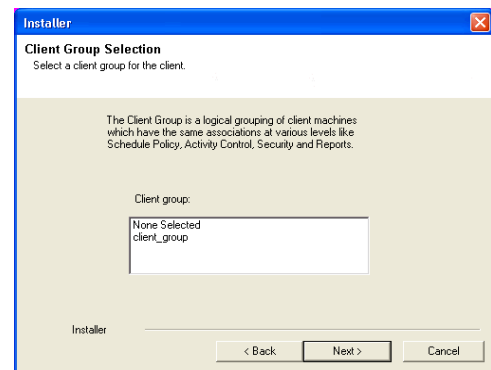
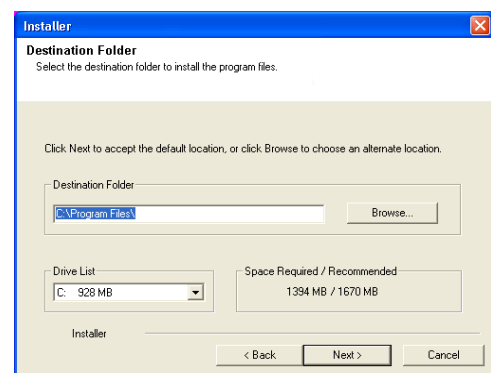
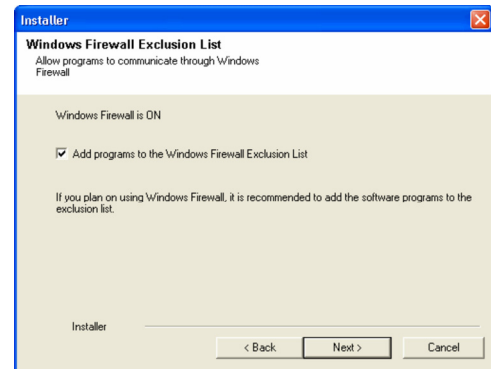
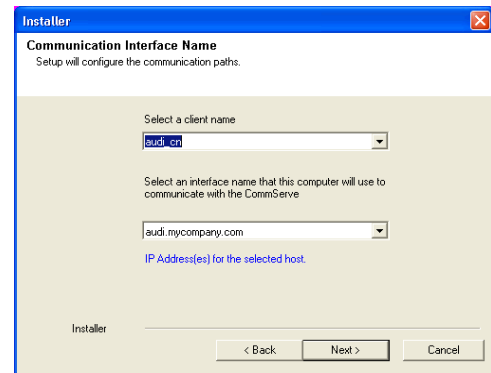
It is recommended that you use alphanumeric characters only.

12. Select a Client Group from the list.

Click **Next**.

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

13. Click **Next**.



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

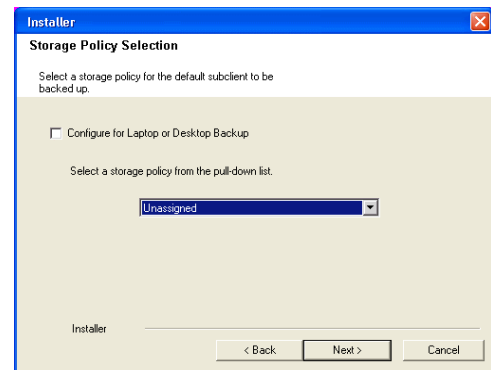
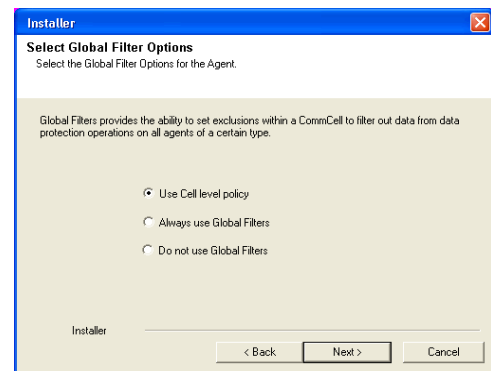
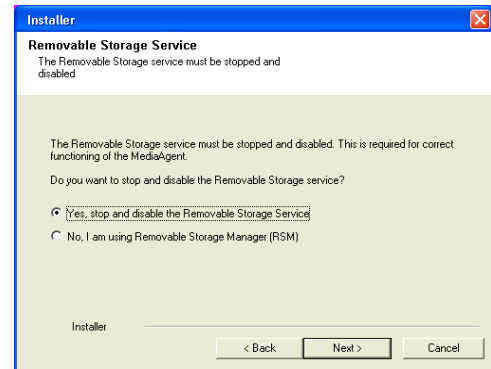
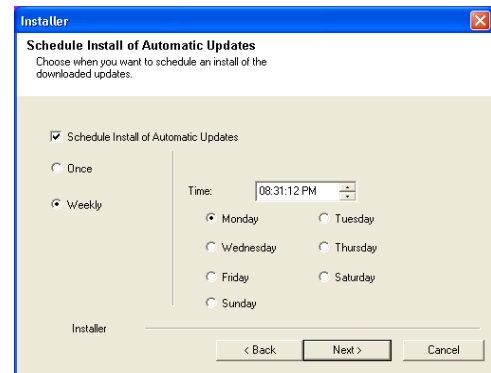
This prompt will not appear if Removable Storage Services are already disabled on the computer.

15. Click **Next**.

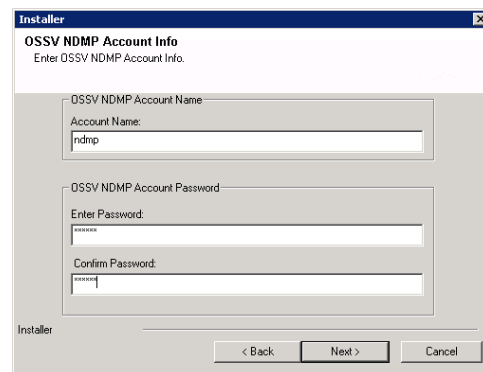
16. Select a **Storage Policy**.
Click **Next**.

You can create the Storage Policy later in step 21.

17. Enter the NDMP account name and password you provided during the NetApp SnapVault OSSV Agent installation.
Click **Next**.

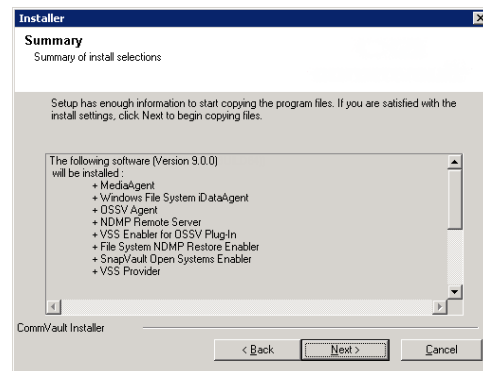


18. Click **Next**.



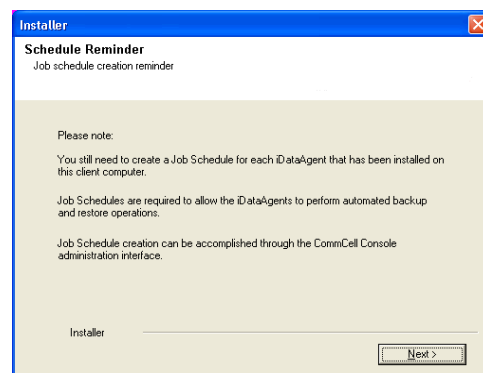
The dialog box is titled "Installer" and "OSSV NDMP Account Info". It prompts the user to "Enter OSSV NDMP Account Info." There are two main input sections: "OSSV NDMP Account Name" with a text field containing "ndmp", and "OSSV NDMP Account Password" with "Enter Password:" and "Confirm Password:" fields, both containing masked text. At the bottom, there are buttons for "< Back", "Next >", and "Cancel".

19. Click **Next**.

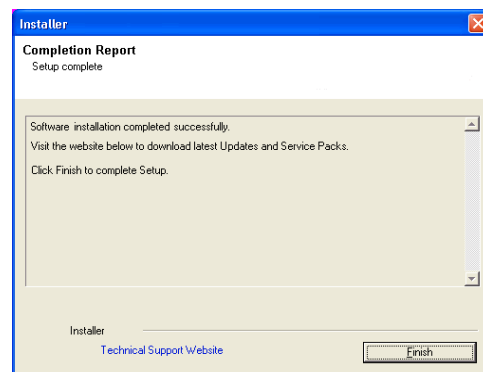


The dialog box is titled "Installer" and "Summary". It shows a "Summary of install selections". A message states: "Setup has enough information to start copying the program files. If you are satisfied with the install settings, click Next to begin copying files." Below this, a list of software to be installed (Version 9.0.0) is shown in a scrollable area: MediaAgent, Windows File System iDataAgent, OSSV Agent, NDMP Remote Server, VSS Enabler for OSSV Plug-In, File System NDMP Restore Enabler, SnapVault Open Systems Enabler, and VSS Provider. At the bottom, there are buttons for "< Back", "Next >", and "Cancel".

20. Click **Finish**.



The dialog box is titled "Installer" and "Schedule Reminder". It contains a "Job schedule creation reminder". A "Please note:" section states: "You still need to create a Job Schedule for each iDataAgent that has been installed on this client computer. Job Schedules are required to allow the iDataAgents to perform automated backup and restore operations. Job Schedule creation can be accomplished through the CommCell Console administration interface." At the bottom, there is a "Next >" button.



The dialog box is titled "Installer" and "Completion Report". It states "Setup complete". A scrollable area contains the message: "Software installation completed successfully. Visit the website below to download latest Updates and Service Packs. Click Finish to complete Setup." Below this, there is a "Finish" button and a link to the "Technical Support Website".



If you already have a storage policy selected in step 16, Click **Next** ► button available at the bottom of the page to continue.

If you do not have Storage Policy created, follow the steps below.

- 21 To create a storage policy, you must have configured a library in the CommCell.
- If you do not already have a library configured, go to Disk Library Creation.
 - If you have a library configured, go to Storage Policy Creation.

DISK LIBRARY CREATION:

1. From the CommCell Console, click the **Backup Target** button on **EZ Operations Wizard**.
2. Click **Disc Library (For backup to disc)** and click **Next**.
3. Click **Use Local Disk**.

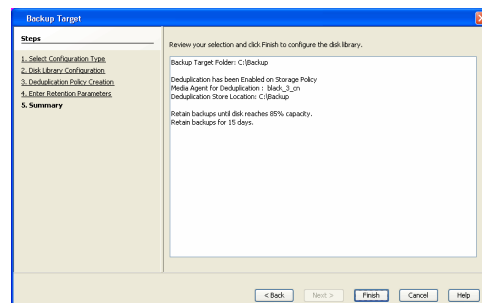
Type the name of the folder in which the disc library must be located in the **Enter backup destination folder** box or click the **Browse** button to select the folder.

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 **Next**.
5. Click **Finish**.

This will create a library and Storage Policy. Click the **Next** ➤ button available at the bottom of the page to continue.



STORAGE POLICY CREATION

1. From the CommCell Browser, navigate to **Policies**.
2. Right-click the **Storage Policies** and then click **New Storage Policy**.
3. 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**.

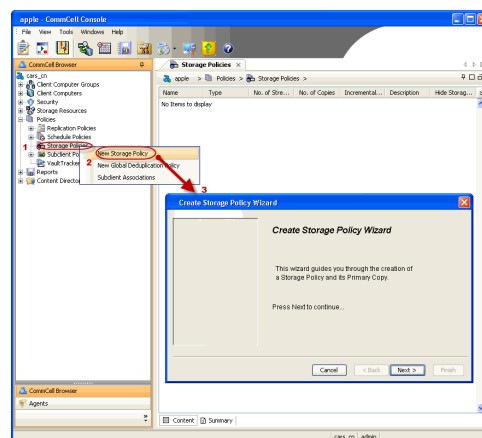
Ensure that you select a library attached to a MediaAgent operating in the current release.

- 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**.

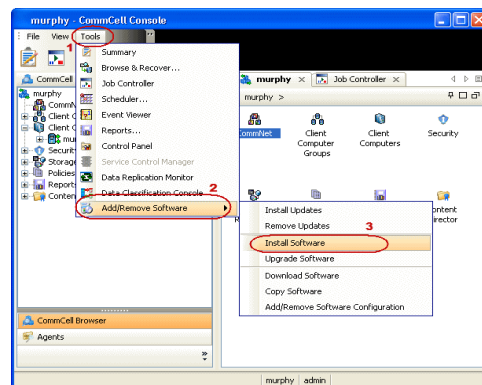
- o Review the details and click **Finish** to create the Storage Policy.

This will create a storage policy. Click the **Next** ➤ button available at the bottom of the page to continue.



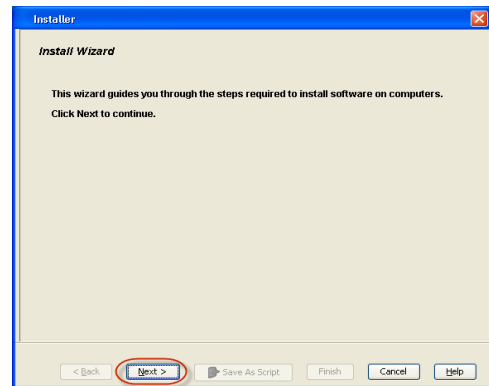
METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

1. From the CommCell Browser, select **Tools | Add/Remove Software | Install Software**.

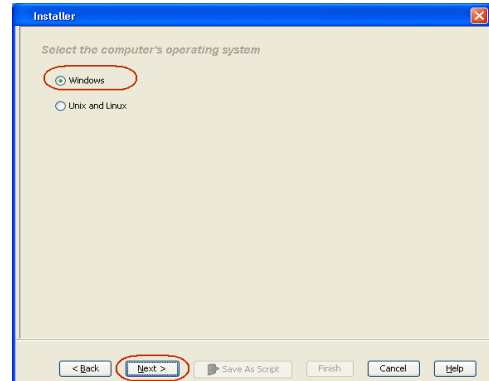


2. Click **Next**.

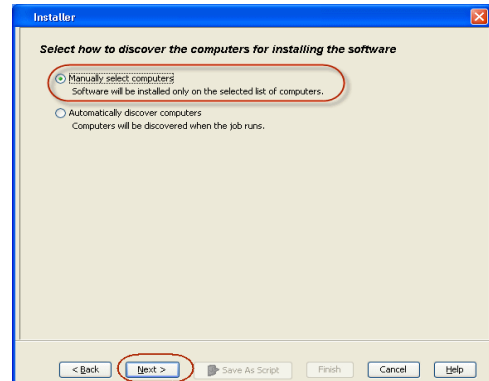
3. Select **Windows**.
Click **Next**.



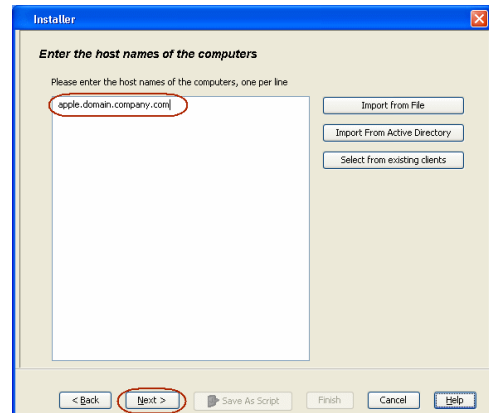
4. Select **Manually Select Computers**.
Click **Next**.



5. Enter the fully qualified domain name of the computer in which you wish to install the OSSV Plug-In.
For example: apple.domain.company.com
Click **Next**.



6. Click **Next**.



7. Specify **User Name** and **Password** that must be used to access the client computer. Click **Next**.

The user must be an Administrator or a member of the Administrator group on that computer.

8. Expand **Common Technology Engine | MediaAgent Modules** and select **MediaAgent**.

If the library is attached to the MediaAgent, select **NDMP Remote Server**.

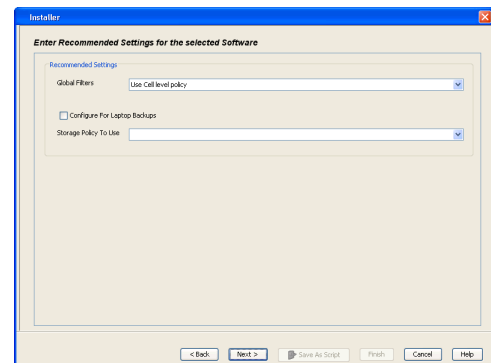
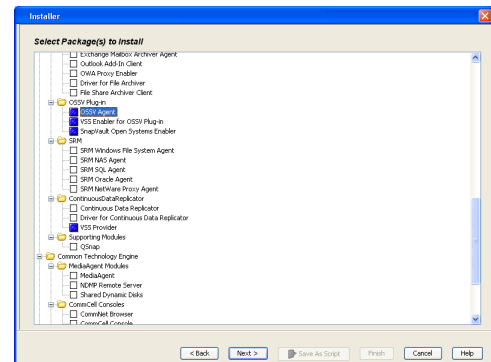
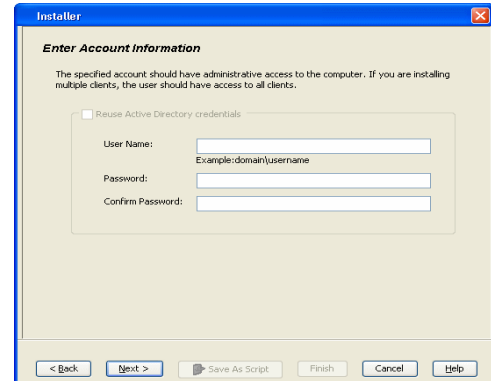
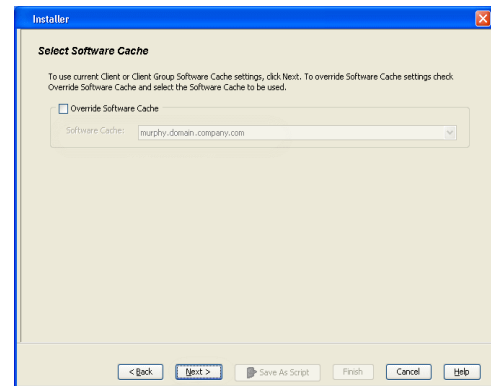
Expand **Client Modules | OSSV Plug-In** and select **OSSV Agent**. The following are automatically selected:

- **VSS Enabler for OSSV Plug-In**
- **SnapVault Open System Enabler**
- **VSS Provider**
- **Windows File System iDataAgent**
- **File System NDMP Restore Enabler**

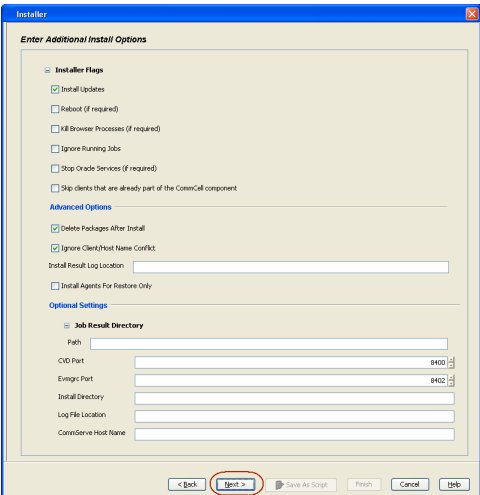
Click **Next**.

- 9.
- From **Storage Policy to Use** list, click storage policy.
 - Click **Next**.

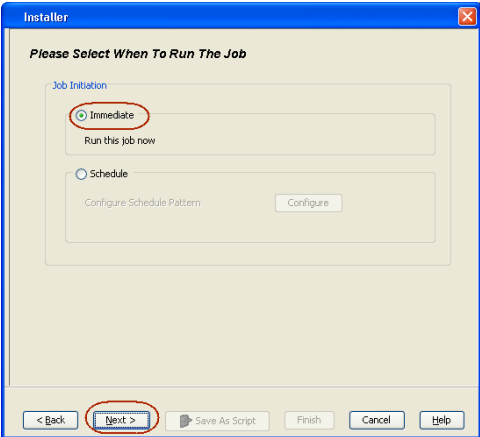
10. Click **Next**.



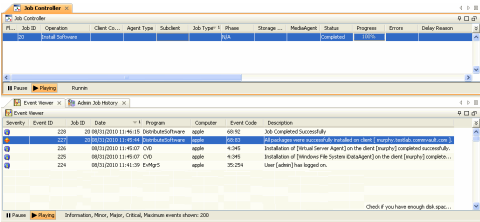
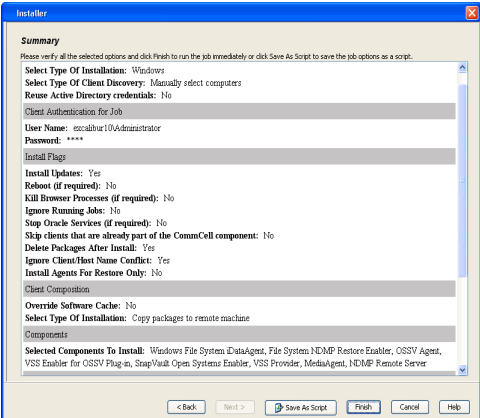
11.
- Click **Immediate**.
Click **Next**.



12.
- Click **Finish**.



13.
- You can track the progress of the job from the **Job Controller** or **Event Viewer** window.



Previous Next

ADDITIONAL INSTALLATION METHODS

Custom Package

Create a compact software package for quick deployment to multiple clients.

Decoupled Install

Install the software first and later register the client in the CommCell.

Remote Install

Deploy the software from CommCell Console on multiple clients.

Silent Install

Deploy the software silently on multiple clients.

Getting Started - OSSV Plug-In Deployment on a UNIX Computer

◀ Previous Next ▶

SKIP THIS PAGE IF YOU ARE NOT INSTALLING THIS AGENT ON A UNIX COMPUTER.

Click **Next** ▶ to continue with the deployment.

WHERE TO INSTALL

Install the software on a client computer that satisfies the minimum requirements specified in the System Requirements and with the following configurations:

- NetApp SnapVault OSSV Agent v3.0.1 installed.
- Client computer is connected to a NetApp file server that you want to protect. The Unix Primary and Secondary Snap Vault licenses must be present on the file server.

To backup the data from OSSV volumes, you need to install the MediaAgent software which includes the NAS iDataAgent. If the library is attached to the MediaAgent, you need to install the NDMP Remote Server software.

INSTALLATION

The software can be installed on a Linux or Solaris computer using one of the following methods:

METHOD 1: INTERACTIVE INSTALL

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

METHOD 2: INSTALL SOFTWARE FROM COMMCCELL CONSOLE

Use this procedure to remotely install the software on a client computer.

BEFORE YOU BEGIN

Download Software Packages

Download the latest software package to perform the install.

Verify System Requirements

Verify that the computer in which you wish to install the software satisfies the System Requirements.

METHOD 1: INTERACTIVE INSTALL

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 your are installing the software from CD, run the following command to mount the CD:

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


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

```
./cvpkgadd
```
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**.

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

Page 21 of 36

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** 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**.  
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**.

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

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]

18. 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.

19. 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.

20. Press **Enter**.

21. Enter the number associated with the storage policy you want use and press **Enter**.

22. Press **Enter**.

23. Make your selection and press **Enter**.

This prompt is displayed only if the directory identified in the previous Step does not exist.

24. Press **Enter** to grant this permission (recommended). Otherwise, type **no** and edit the affected `etc` system script as shown below.

For Red Hat Linux, update the `/etc/rc.d/rc.sysinit` file as follows:

```
/etc/init.d/cxbrf start
```

For SuSE Linux, update the `/etc/rc.d/boot.localfs` file as follows:

```
/etc/init.d/cxbrf start
```

For Solaris, update the `/etc/rc0` file as follows:

```
echo "Bull CXBF: updating the cxbrf on disk bitmaps."
/usr/sbin/cvsnaps -c "updatebitmaps"
```

25. Type the NDMP account name you provided during the NetApp SnapVault OSSV Agent installation.

26. Type the NDMP account password you provided during the NetApp SnapVault OSSV Agent installation.

27. Type **3** and press **Enter**.

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]

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]

For every snapshot taken CXBF driver creates a sparse file where it puts copy-on-write data blocks and block bitmap. These COW files are created in a dedicated directory that should satisfy a few requirements:

1) It should be a local directory for performance reasons,

2) It should have sufficient amount of space,

3) In case of Solaris UFS, it should have journaling turned off.

COW Cache Directory: [/space/opt/calypso2/CXBF/cache]

Directory "<dir\_name>" does not exist.

1) Create this directory and continue  
2) Retry input

Your choice: [1]

We now need to make some changes to your <etc file path> system script.

We can either make these changes ourselves at this time, or we can explain what has to be modified so that you can do it yourself.

Would you like us to modify <etc file> now? [yes]

Please enter OSSV NDMP Account Name.

Name:

Please enter OSSV NDMP Account Password.

Password:

Again:

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]

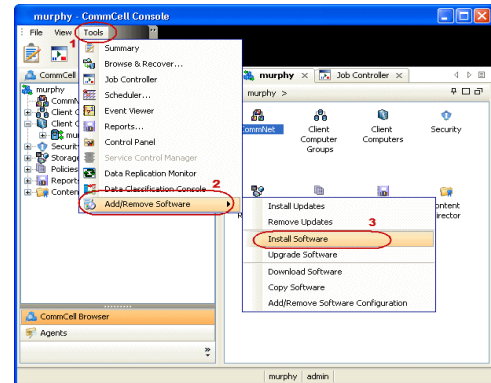


If you already have a storage policy selected in step 21, Click **Next** ➤ button available at the bottom of the page to continue.

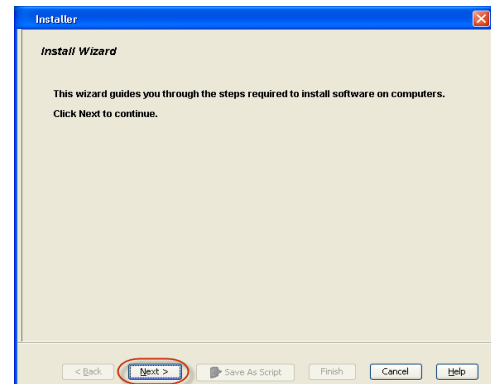
If you do not have Storage Policy created, follow the steps provided in the Create a Storage Policy procedure.

## METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

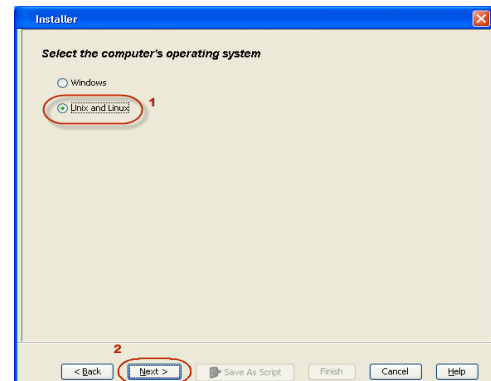
1. From the CommCell Browser, select **Tools | Add/Remove Software | Install Software**.



2. Click **Next**.



3. Select **Unix and Linux**.  
Click **Next**.



4. Select **Manually Select Computers**.  
Click **Next**.

5. Enter the fully qualified domain name of the computer in which you wish to install the OSSV Plug-In.

For example: apple.domain.company.com

Click **Next**.

6. Click **Next**.

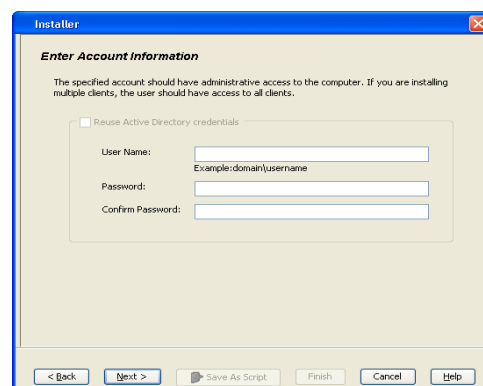
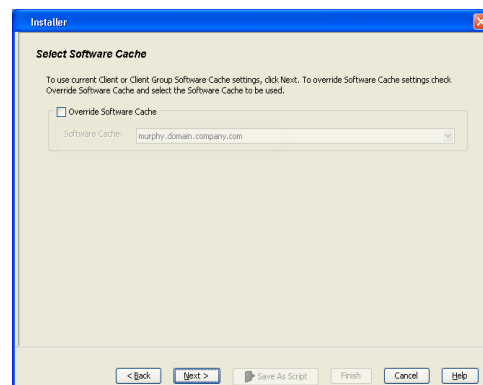
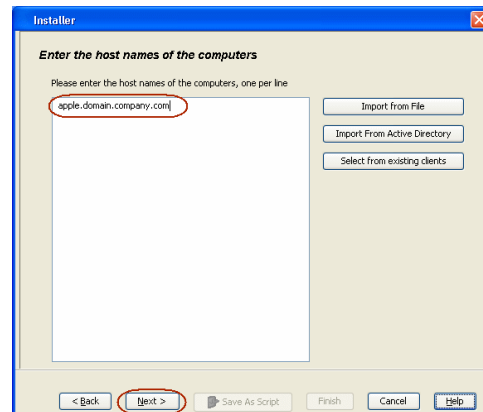
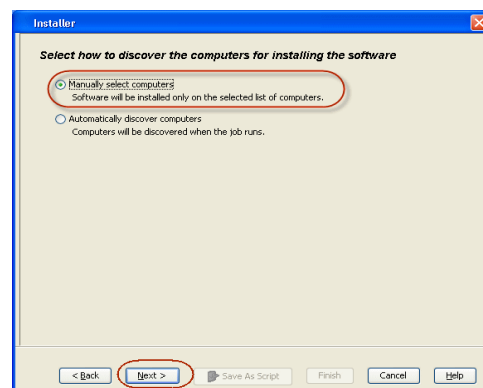
7. Specify **User Name** and **Password** that must be used to access the client computer. Click **Next**.

The user must be an Administrator or a member of the Administrator group on that computer.

8. Expand **Common Technology Engine | MediaAgent Modules** and select **MediaAgent**.

If the library is attached to the MediaAgent, select **NDMP Remote Server**.

Expand **Client Modules | Backup & Recovery | File System** and select the

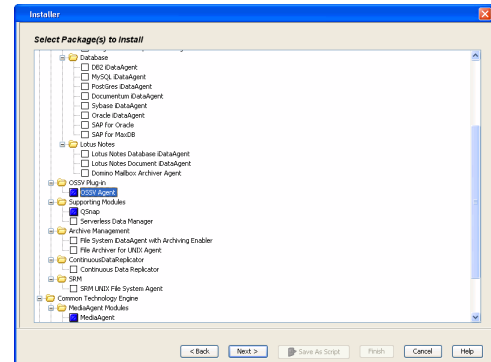


following:

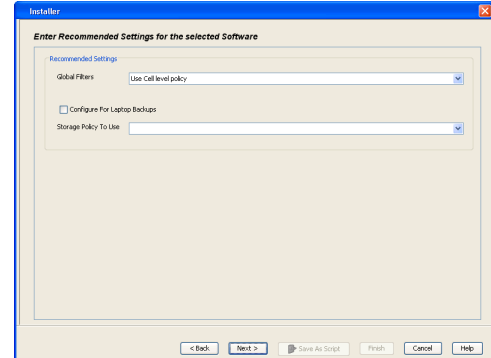
- **Unix File System iDataAgent**
- **File System NDMP Restore Enabler**

Expand **Client Modules | OSSV Plug-In** and select **OSSV Agent. QSnap** is automatically selected.

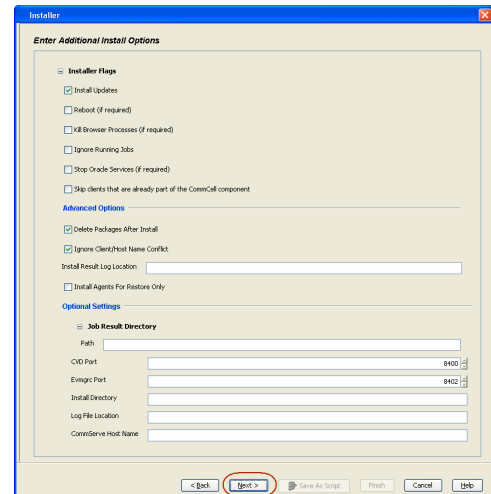
Click **Next**.



- 9.
- From **Storage Policy to Use** list, click storage policy.
  - Click **Next**.

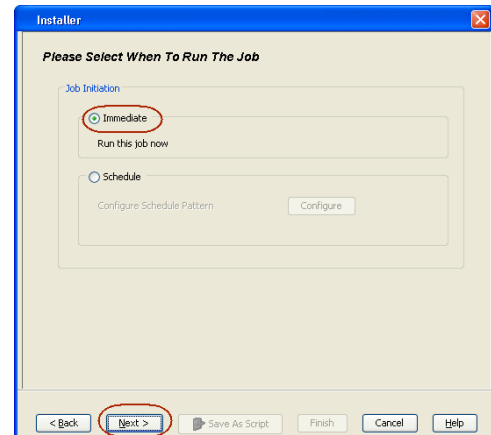


10. Click **Next**.



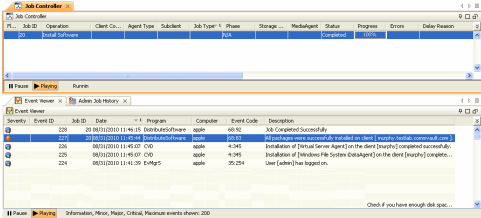
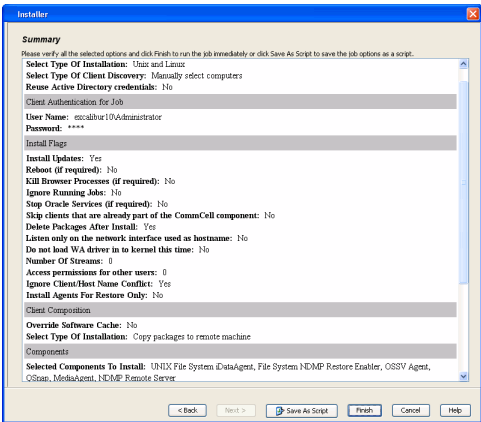
11. Click **Immediate**.

Click **Next**.



12. Click **Finish**.

13. You can track the progress of the job from the **Job Controller** or **Event Viewer** window.



Previous Next

## ADDITIONAL INSTALLATION METHODS

### Custom Package

Create a compact software package for quick deployment to multiple clients.

### Decoupled Install

Install the software first and later register the client in the CommCell.

### Remote Install

Deploy the software from CommCell Console on multiple clients.

### Silent Install

Deploy the software silently on multiple clients.

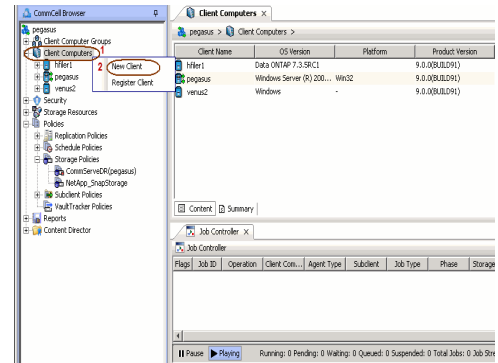
# Getting Started - OSSV Plug-In Configuration

◀ Previous   Next ▶

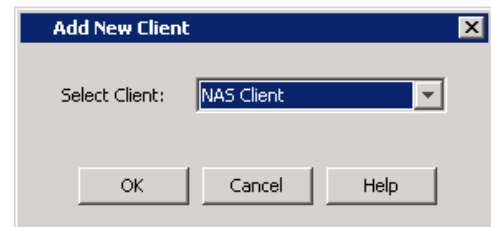
The following sections describe the steps required to configure the OSSV Plug-In Agent before creating the OSSV volume, which is created after running your first backup.

## ADD A NAS CLIENT

- From the CommCell Browser, right-click the **Client Computers** node and click **New Client**.



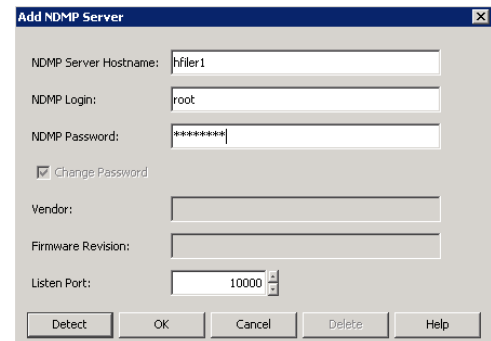
- Select **NAS Client** from the drop-down list.
  - Click **OK**.



- 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).

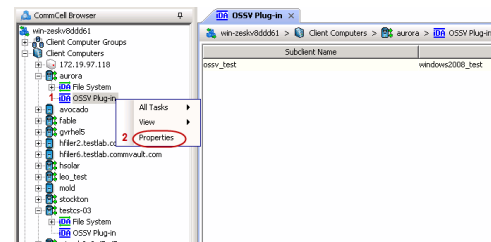
- Click **Detect**.
- Click **OK**.

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

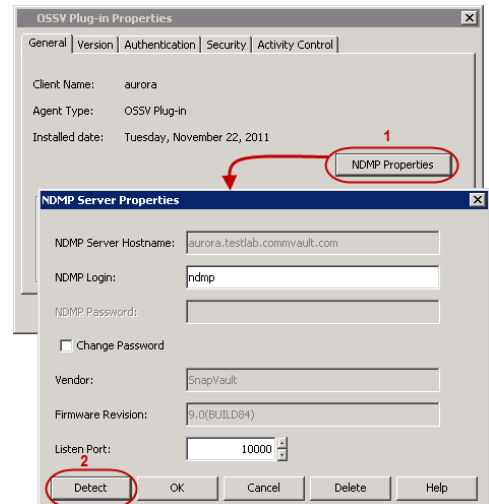


## VERIFY NDMP PROPERTIES FOR THE OSSV PLUG-IN

- From the CommCell Browser, navigate to **Client Computers | <Client>**.
  - Right-click the **OSSV Plug-In** and click **Properties**.

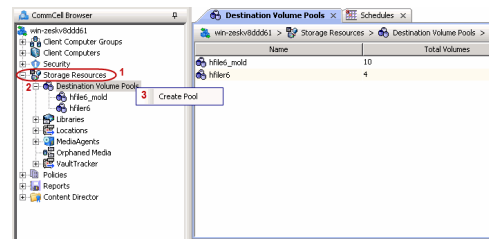


- Click **NDMP Properties**.
  - Click **Detect**. The OSSV NDMP credentials provided during installation will be used to detect the file server.
  - Click **OK**.

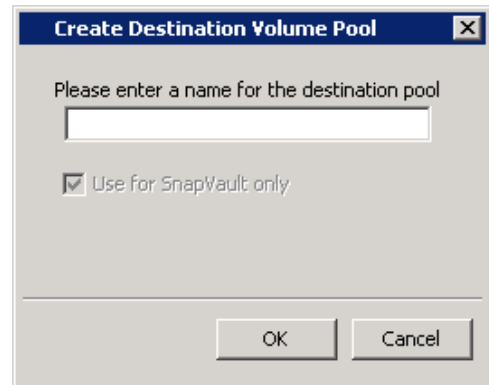


## CREATE A DESTINATION VOLUME POOL

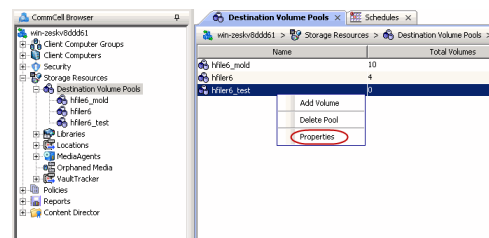
1.
  - From the CommCell Browser, navigate to **Storage Resources**.
  - Right-click the **Destination Volume Pools** node and click **Create Pool**.



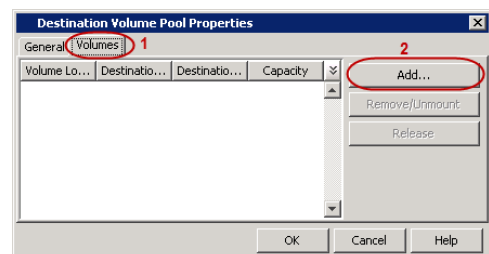
2.
  - Type a name for the new destination pool.
  - Click **OK**.



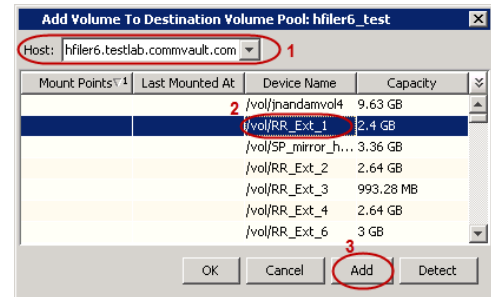
3. Right-click the new destination pool and click **Properties**.



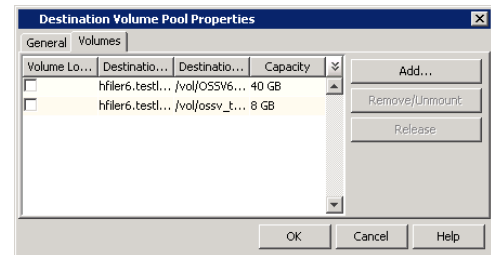
4. Click the **Volumes** tab and click **Add**.



5.
  - Select the NAS file server from the **Host** drop-down list. The volumes residing in the file server will be populated.
  - Select a volume you want to use as the destination volume for SnapVault operations and click **Add**. Repeat this step if more volumes need to be added.
  - Click **OK**.

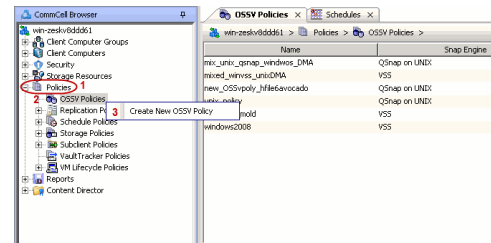


6. Click **OK**.



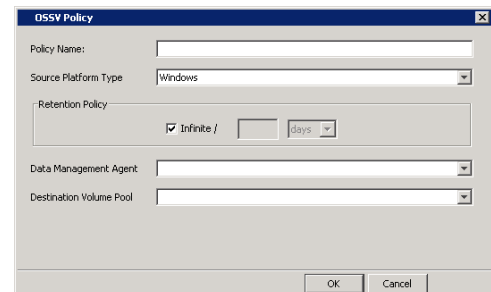
## CREATE AN OSSV POLICY

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



2.
  - Type a name for the new policy in the **Policy Name** box.
  - Select the operating system of the client computer where the OSSV Plug-In Agent resides from the **Source Platform Type** drop-down list.
  - Select the client computer where the OSSV Plug-In Agent resides from the **Data Management Agent** drop-down list.
  - Select the volume you recently created from the **Destination Volume Pool** drop-down list.
  - Click **OK**.

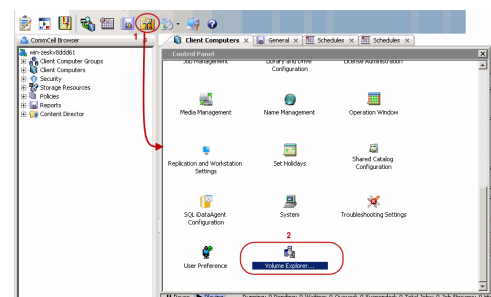
The OSSV Policy will determine which storage array and Agent (SnapVault Open Systems CopyManager) are used to create the snapshot.



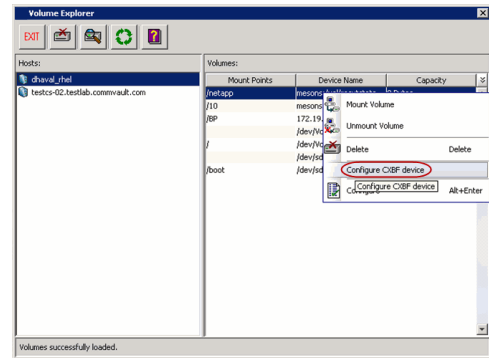
## CONFIGURE CXBF DEVICE (UNIX)

Skip this section if you are configuring a Windows client computer.

1.
  - From the toolbar in the CommCell Console, click **Control Panel**.
  - Double-click **Volume Explorer**.

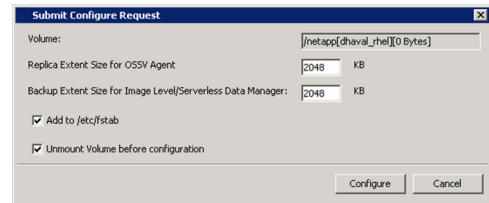


2.
  - Select your Unix client computer from the **Hosts** list in the left pane.
  - Right-click a mount point from the **Volumes** list in the right pane and then click **Configure CXBF device**.



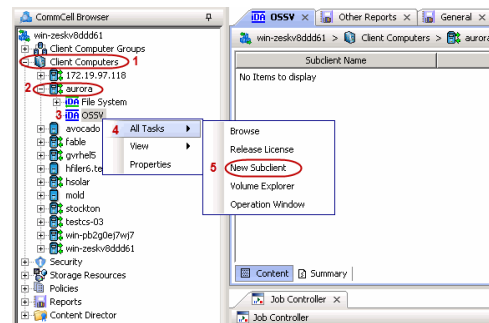
3. Click **Configure**.

Once the CXBF device is configured, it can be used as the subclient content for the OSSV volume creation.

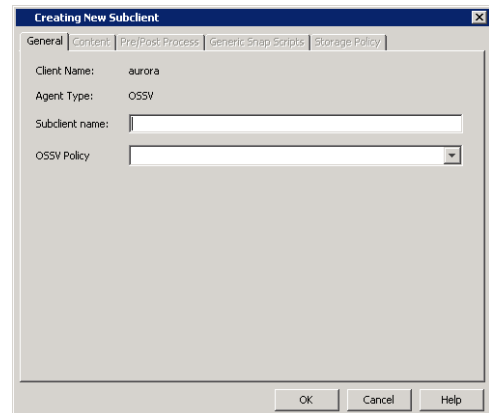


## CREATE A SUBCLIENT

1.
  - From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
  - Right-click the **OSSV Plug-In** and click **All Tasks** | **New Subclient**.



2.
  - Type a name for the new subclient in the **Subclient name** box.
  - Select the OSS policy you recently created from the **OSSV Policy** drop-down list.



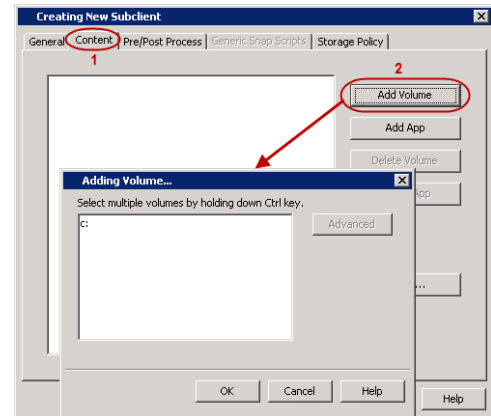
3. Click the **Content** tab.

Depending on the data you want to protect, you can add file system or application data.

For file system data:

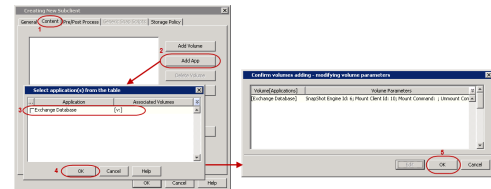
- Click **Add Volume**.
- From the **Adding Volume...** dialog box, select the volumes you want to add and click **OK**.

For Open Systems on Solaris, the source volumes must be CXBF devices.



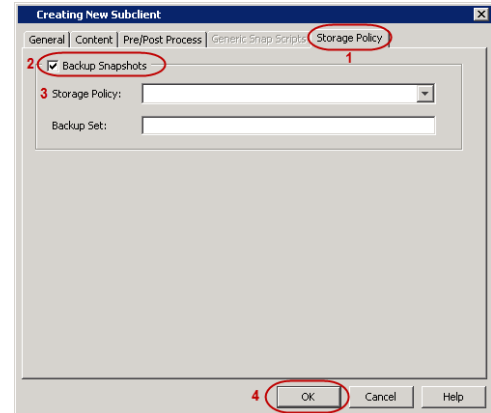
For application data:

- You must specify the user account to access the application server as explained in Configure Access to Supported Applications.
- Click **Add App**.
- Select the applications you want to add (e.g., Exchange Database) and click **OK**.
- Click **OK** to confirm the volumes to be added.



4.

- Click the **Storage Policy** tab.
- Click the **Backup Snapshots** check box.
- Select the storage policy you want to use to backup the snapshot to media from the **Storage Policy** drop-down list. The **Backup Set** box will be automatically populated.
- Click **OK**.



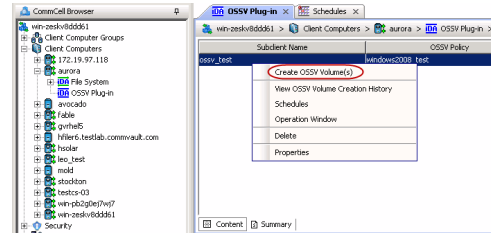
< Previous Next >

# Getting Started - OSSV Plug-In Backup

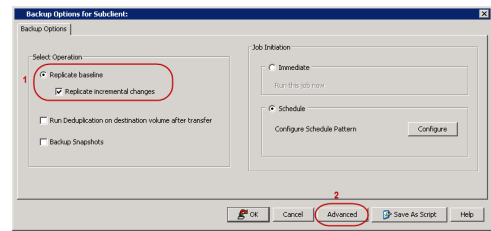
[< Previous](#)
[Next >](#)

| WHAT GETS BACKED UP               | WHAT DOES NOT GET BACKED UP |
|-----------------------------------|-----------------------------|
| All contents on the source volume |                             |

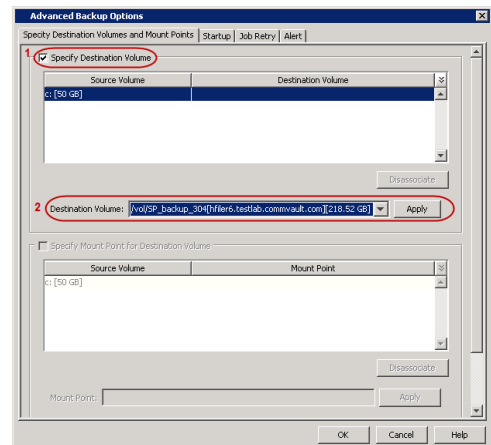
- From the CommCell Browser, navigate to **Client Computers** | **<Client>** | **OSSV Plug-In**
  - Right-click the subclient and click **Create OSSV Volume(s)**.



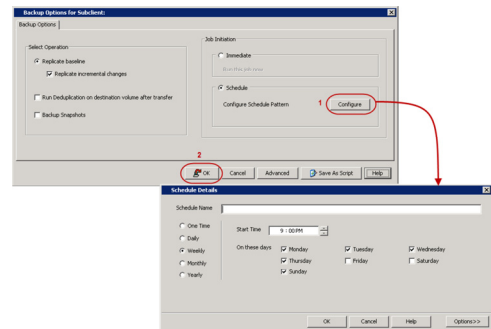
- Click **Advanced**.



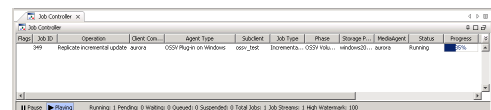
- Click the **Specify Destination Volume** check box.
  - Click the volume that needs a destination volume association from the **Source Volume** list.
  - Select the volume on the file server where all the data will be copied from the **Destination Volume** drop-down list and click **Apply**.
  - Click **OK**.



- Click **Configure** to schedule the next incremental backups after the OSSV volume is replicated on the file server.
  - Click **OK**.
  - Click **OK** to start the backup operation.



- 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 **OSSV Plug-In** Agent and click **View** | **OSSV Volume Creation**.

8. Right-click the job to:



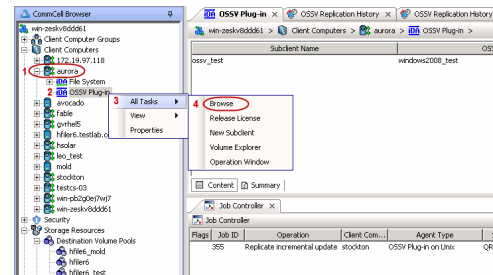
# Getting Started - OSSV Plug-In Restore

[< Previous](#) [Next >](#)

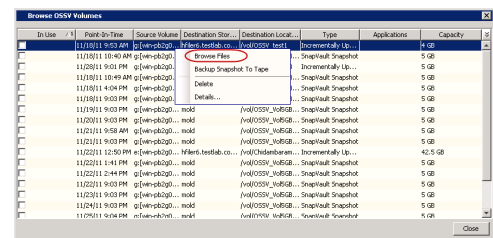
As restoring your backup data is very crucial, it is recommended that you perform a restore operation immediately after creating the OSSV volume on the destination to understand the process.

The following sections describe the steps for restoring the data of the OSSV volume to a different location.

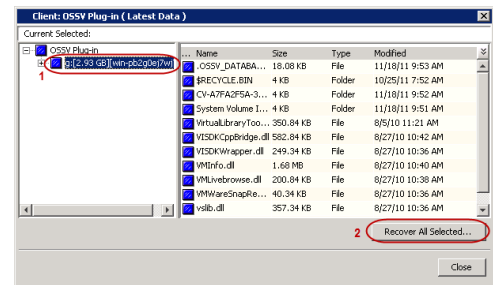
- From the CommCell Browser, navigate to **Client Computers** | **<Client>**.
  - Right-click the **OSSV Plug-In** Agent and click **All Tasks** | **Browse**.



- Right-click the snapshot you want to restore and then click **Browse Files**.



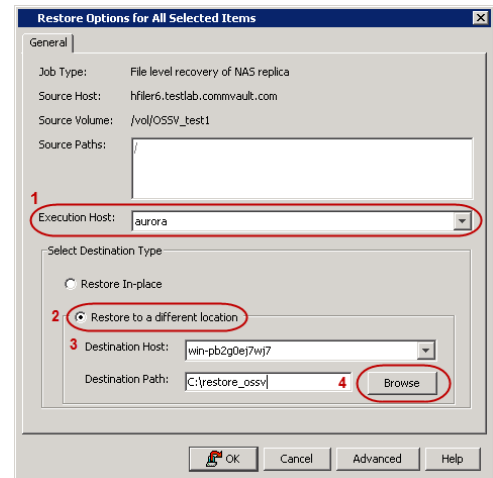
- Select the volume containing the data you want to restore in the left pane.
  - Click **Recover All Selected**.



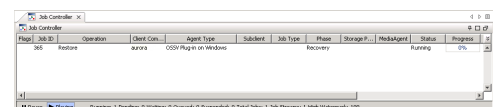
- Select the client computer that will start the restore process from the **Execution Host** drop-down list.
  - Click **Restore to a different location**.
  - Select the name of the client computer from the **Destination Host** drop-down list.
  - Specify the destination path by clicking **Browse**.

A UNC path should not be used as the destination path.  
The OSSV Plug-In does not support UNC paths as restore destinations.

- Click **OK**.



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



- Once the restore job has completed, right-click the **OSSV Plug-In** Agent and click **View** | **OSSV Volume Recovery**.

