NETAPP TECHNICAL REPORT

Open Systems SnapVault Best Practices Guide for Protecting Virtual Infrastructure

Chris Blackwood, NetApp
TR-3653

ABSTRACT

This document provides the information that you need to deploy Open Systems SnapVault® 2.6 in a VMware® virtual infrastructure. Many of the best practices that have been identified for previous versions of Open Systems SnapVault apply to this version as well. However, backup features that are new to this version require an additional level of best practices and design strategies.

TABLE OF CONTENTS

1 INTRODUCTION 3
1.1 REQUIREMENTS AND ASSUMPTIONS 3
1.2 INTENDED AUDIENCE 3
2 OVERVIEW 3
3 REQUIREMENTS 4
4 INSTALLATION 4
4.1 PREREQUISITES 4
4.2 INTERACTION WITH VIRTUALCENTER 4
4.3 INSTALLATION LOCATION 5
4.4 INSTALLATION EXAMPLE 5
4.5 CONFIGURING THE ESX FIREWALL 7
5 SETUP WITH PROTECTION MANAGER 8
5.1 ADDING AN ESX HOST 8
5.2 MODIFYING THE DEFAULT BACKUP POLICY 10
5.3 CREATING A DATA SET 11
5.4 ADDING A PROTECTION POLICY 13
5.5 RUNNING A MANUAL UPDATE 15
5.6 RESTORING THE DATA SET 15
6 BEST PRACTICES 16
6.1 MINIMUM MEMORY SIZE FOR VIRTUAL MACHINES 16
6.2 NUMBER OF VIRTUAL MACHINES TO PROTECT 16
6.3 SCHEDULING WITH VMOTION IN MIND 16
7 KNOWN BEHAVIORS 16
8 TROUBLESHOOTING 17
8.1 LOG FILE LOCATIONS 17
8.2 COMMON ERROR CONDITIONS 17
9 ADDITIONAL REFERENCES 18
10 APPENDIX 18
10.1 SINGLE FILE RESTORE 18
10.2 DISASTER RECOVERY, TEST, AND DEVELOPMENT 21

1 INTRODUCTION

Historically, Open Systems SnapVault has been a successful solution for backing up open system platforms such as Windows®, UNIX®, and Linux®. Its use of block-level incremental transfers makes it especially suitable for remote offices where slow network connections typically impede centralized backups.

Open Systems SnapVault 2.6 introduces support for VMware's ESX Server platform, which allows a new approach to backing up virtualized environments. This document contains information that is helpful in deploying Open Systems SnapVault 2.6 in the virtualized environment.

1.1 REQUIREMENTS AND ASSUMPTIONS

To take full advantage of the information in this document, you should be familiar with the following:

- Open Systems SnapVault backup solutions (A good resource for this information is the *Open Systems SnapVault Best Practices Guide*.)
- The *Open Systems SnapVault 2.6 Release Notes*
- The *Open Systems SnapVault 2.6 Installation and Administration Guide*
- VMware virtualization concepts and the ESX Server platform
- NetApp® system administration

1.2 INTENDED AUDIENCE

This internal document is intended for end users who are responsible for deploying Open Systems SnapVault in VMware environments.

2 OVERVIEW

The growing popularity of server virtualization presents new challenges for backup and recovery techniques. With Open Systems SnapVault 2.6, there are several ways to back up and recover a virtual machine. In previous versions, Open Systems SnapVault could back up a virtual machine just as it would any nonvirtualized server. For each virtual machine, an Open Systems SnapVault agent would be installed and configured independently on each guest operating system. But how is it possible to protect all virtual machines with just a single Open Systems SnapVault agent? That question is the focus of this document.

VMware virtual machines are made up of a series of files that reside on a data store. In many cases, this data store is a VMFS LUN presented to the ESX Server. In other cases, the data store lives on an NFS share. Either way, if you can back up those files from the ESX Server level, then you have another approach to backup and recovery in virtual environments.

You should be familiar with the following components of the VMware infrastructure:

- ESX Server
- Service Console
- Data Store
- VirtualCenter Server
- VMotion™

For descriptions of these components, refer to www.vmware.com.

Beginning with version 2.6, Open Systems SnapVault can be installed in the Service Console of the ESX Server, making it possible to back up each virtual machine as whole files. In other words, you can now back up .vmx, .vmdk, .nvram, and .log files that make up individual virtual machines, effectively allowing bare metal recoveries.

Open Systems SnapVault supports VMotion movement of virtual machines. When planning for backups in a VMotion environment, you should consider several things.

Both ESX Servers must be available in order for incremental updates to occur after a VMotion migration has taken place for a virtual machine. The ESX Server that originally processed the baseline backup will also process all subsequent incrementals, even if the virtual machine has been migrated to another host. If a VMotion migration has taken place due to a system outage, Open Systems SnapVault will not be able to complete a backup of any migrated virtual machines until the ESX outage has been resolved.

Checksum computations are done on the original ESX Server while a virtual machine is resident on an alternate host.

While OSSV is taking a snapshot, any VMotion migration attempts fail because VMotion is disabled during snapshot creation. When Open Systems SnapVault has completed the copy, VMotion can complete the migration.

If a VMotion migration is in progress, any Open Systems SnapVault backup attempt fails because the snapshot creation fails.

3 REQUIREMENTS

The following requirements apply to Open Systems SnapVault and protecting the virtual infrastructure. For more information, see the *Open Systems SnapVault 2.6 Release Notes.*

- ESX Server 3.0, 3.0.1, or 3.0.2
- Data ONTAP® 7.x
- Open Systems SnapVault 2.6
- A valid sv_vi_pri license key on the NetApp destination
- A valid sv_ontap_sec license key on the NetApp destination
- A valid NearStore® license on the NetApp destination
- Protection Manager 3.7 (optional but recommended)

4 INSTALLATION

For complete installation instructions, see the *Open Systems SnapVault 2.6 Installation and Administration Guide.* This section addresses additional considerations.

4.1 PREREQUISITES

The `/vmfs/volumes` directory structure must exist before installation. Otherwise the installation will fail.

4.2 INTERACTION WITH VIRTUALCENTER

A VirtualCenter host is not required for an Open Systems SnapVault deployment on an ESX Server. However, environments that use VMotion have a VirtualCenter host. This is standard practice from a VMware perspective. The installation process asks for information about this VirtualCenter host.

Additionally, the default protocol for communicating with the VirtualCenter host is HTTPS; NetApp does not recommend the use of HTTP. If you choose not to use HTTPS (you are asked during installation), you must complete some additional steps, These steps require you to modify VMware configuration files on the ESX Server as well as the VirtualCenter host. This procedure is documented in the following guides in the section "Modifying the Server Configuration to Support HTTP." The steps differ slightly depending on the version of VirtualCenter you are running.

- Developer's Setup Guide VMware Infrastructure SDK 2.0.1
- Developer's Setup Guide VMware Infrastructure SDK 2.5

Note: Using HTTP is likely to cause backups to fail. It can also prevent Protection Manager from being able to identify the virtual machines that are registered on the ESX Server.

4.3 INSTALLATION LOCATION

The default installation location is `/usr/snapvault`. You can change the location during the installation process if necessary.

4.4 INSTALLATION EXAMPLE

The following console output shows an example installation of Open Systems SnapVault 2.6 in the Service Console of an ESX Server.

```
# ls –l
-rwxr-xr-x    1 root     root     11406066 Mar 19 04:00 ossv_esx_v2.6.tar.gz

# gzip -dc ossv_esx_v2.6.tar.gz | tar xf –
# cd ossv
# ./install
Installer invoked in /var/tmp/ossv
Using default /tmp as the temporary directory
Expanding distribution file

OSSV
2_6_2008MAR10
Have you read and agreed to the terms of the license?
(y = yes, n = no, d = display license) (y n d) [d] : y

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 : root

Please 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.
> : vmcoe-fas2020-02b

Enter the Host Name or IP address of the
Virtual Center Host [localhost] : 192.168.10.100

Enter the User Name to connect to the
```

```
Virtual Center Host : administrator

Please enter the password to connect to the
Virtual Center Host :
Confirm password:

Should HTTPS be used to connect to the Virtual Center Host?
If you specify n, HTTP will be used (y n) [y] :y

Enter the HTTPS port [443] :443
checkinstall running
CHOSEN_CLASSES=ossvcore
PKG_BASE=/usr/snapvault
This is a new installation - not an upgrade
Trace Directory = /usr/snapvault/trace
Temp  Directory = /usr/snapvault/tmp
preinstall running
Installing ossvcore
Copying uninstallation scripts
postinstall running
HOST_OS=Esx
Creating Trace Directory /usr/snapvault/trace
NV_UPGRADE=FALSE
Creating database directory /usr/snapvault/db
Installing libraries
libsvdb.so
libsvndmp.so
libsvplugin.so
libsv.so
Creating symbolic links
Installing base npk's
Checking for components in /var/tmp/ossv/packages
Installing additional npk's
Install normal package
Installing vmware plugins
/lib/libcrypto.so.0.9.8 already exists. Not over-written
/lib/libssl.so.0.9.8 already exists. Not over-written
Creating link to libsvvim.so
Successfully installed '/var/tmp/ossv/packages/vmware0010.npk'
Install normal package
Successfully installed '/var/tmp/ossv/packages/ossv2300.npk'
Checking for extra components in /var/tmp/ossv/extrapackages
Copying non-installable additional npk's
Setting gathered configuration values
Installing OSSV Services
Will link to '/usr/snapvault/etc/startup.sh'
```

```
Starting OSSV Services
Checking install validity
SnapVault home directory: '/usr/snapvault'
SnapVault database directory: '/usr/snapvault/db'
SnapVault temporary directory: '/usr/snapvault/tmp'
SnapVault Database and Temporary directories have 70% space left (3464Mb)
SnapVault service is running
SnapVault listener is running
NDMP Server, on port 10000, details:
    Vendor     NetApp
    Product    SnapVault
    Version    2_6_2008MAR10
    Host       vmcoe-ppe01
    Host Id    493EB5670392E3A7FE91B9947036EAD1
    OS Type    ESX
    OS Version 2.4.21-47.0.1.ELvmnixEsx
SnapVault QSM Server is responding correctly
Validating filesystems:
   Mount point / (/dev/sda2) is suitable for backup
   Mount point /proc (none) is a special mount, unsuitable for backup
   Mount point /dev/pts (none) is a special mount, unsuitable for backup
   Mount point /proc/bus/usb (usbdevfs) is a special mount, unsuitable for backup
   Mount point /boot (/dev/sda1) is suitable for backup
   Mount point /dev/shm (none) is a special mount, unsuitable for backup
   Mount point /var/log (/dev/sda6) is suitable for backup
The vmware plugin loaded successfully.
SnapVault File Server is responding correctly

Check Succeeded

Installation appears valid
Installation completed successfully
```

4.5 CONFIGURING THE ESX FIREWALL

The internal firewall in the ESX Server operating system is enabled by default. Therefore you must modify the firewall to open the ports required for Open Systems SnapVault backup and restore operations. The following table shows the default port assignments.

Port	Description
10000	Default NDMP port (required for Protection Manager)
10555	FILESERVER port
10566	QSM port

Execute the following commands from the Service Console to open these required ports:

```
# /usr/sbin/esxcfg-firewall –o 10000,tcp,in,NDMP
```

```
# /usr/sbin/esxcfg-firewall –o 10000,tcp,out,NDMP
# /usr/sbin/esxcfg-firewall –o 10555,tcp,in,FILESERVER
# /usr/sbin/esxcfg-firewall –o 10555,tcp,out,FILESERVER
# /usr/sbin/esxcfg-firewall –o 10566,tcp,in,QSM
# /usr/sbin/esxcfg-firewall –o 10566,tcp,out,QSM
```

To view these open ports, run the following command:

```
# /sbin/service firewall status
```

5 SETUP WITH PROTECTION MANAGER

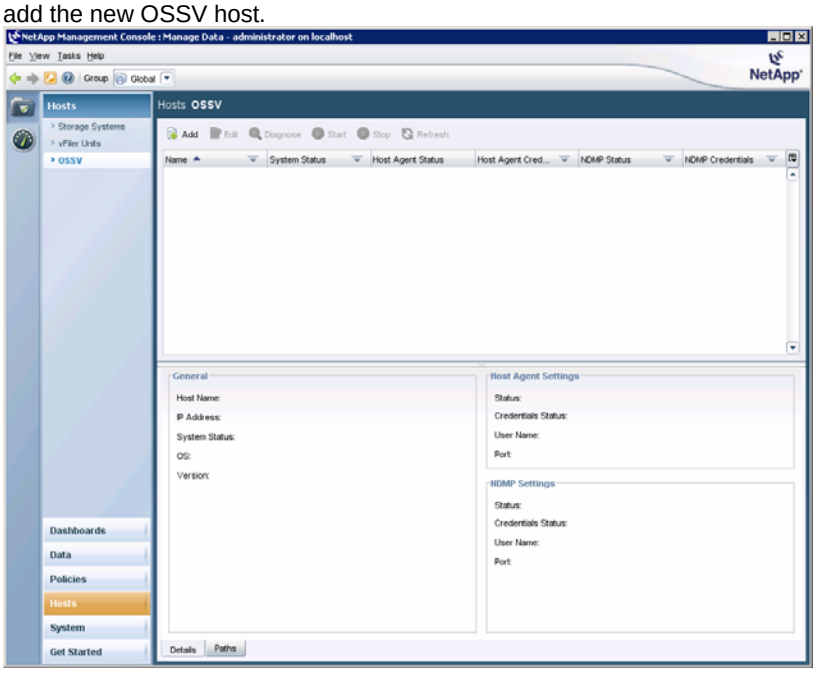
Although management functionality exists for Open Systems SnapVault using a command line interface, NetApp recommends the use of Protection Manager for simplified management. For information on command line syntax and options, see the *Open Systems SnapVault 2.6 Installation and Administration Guide.*

This section describes how to configure your virtual environment for backup and recovery by using Protection Manger.

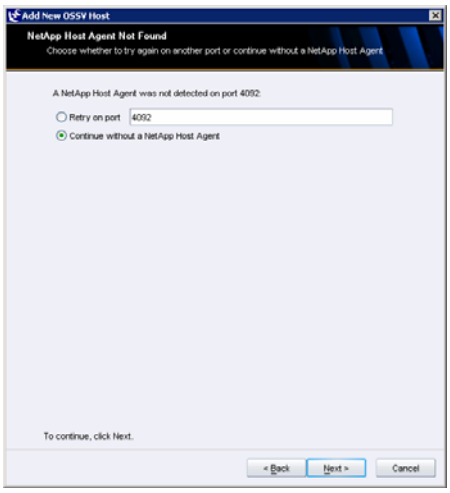
5.1 ADDING AN ESX HOST

To add an ESX host, follow these steps.

1. In the NetApp Management Console, Manage Data, selects Hosts > OSSV and then click Add to add the new OSSV host.

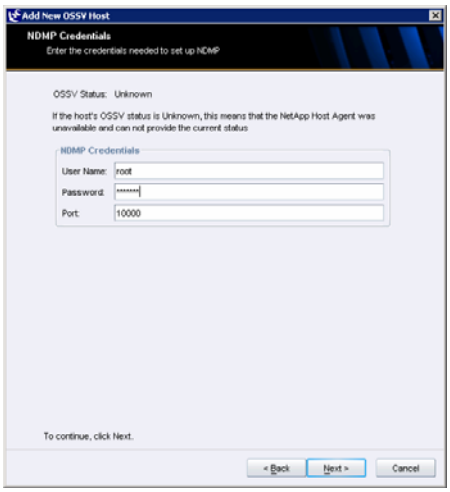


2. In the Add New OSSV Host wizard that is displayed, enter the name or IP address of the ESX Server and then click Next.
3. There is no NetApp Host Agent for ESX Server, so select Continue without a NetApp Host Agent and then click Next.



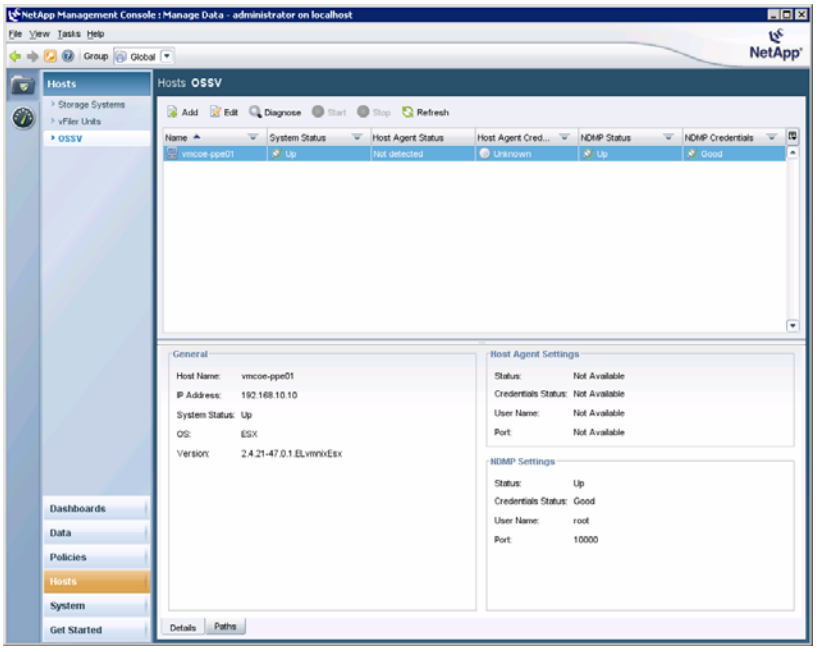
4. Enter the NDMP credentials required for the ESX Server and then click Next.

   NDMP is used for authentication and management.



5. On the Summary page, click Finish.

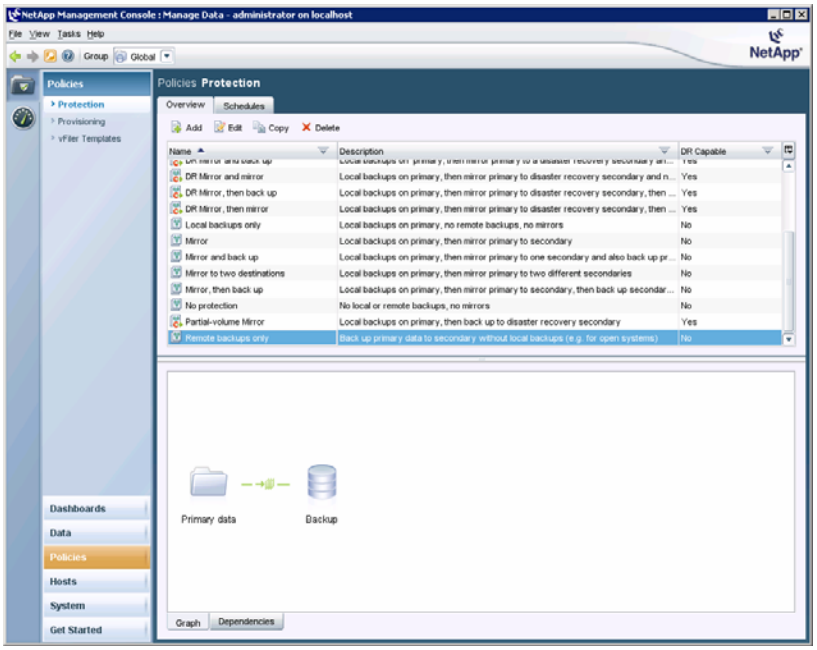
   The new host is added to the list of hosts.



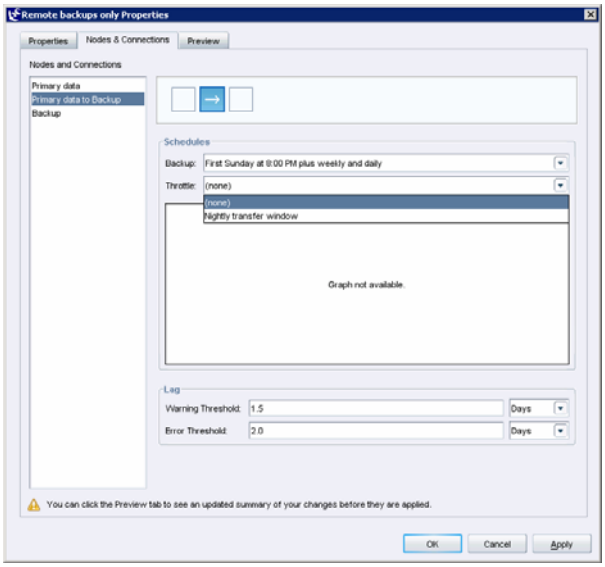
5.2 MODIFYING THE DEFAULT BACKUP POLICY

Open Systems SnapVault uses the “remote backups only” policy. By default, it is set to run only at night because of the default throttle for this policy. If you want the initial backup to run immediately after it is configured, follow these steps to change the throttle setting.

1. In the NetApp Management Console, Manage Data, select Policies > Protection > Remote Backups Only and then click Edit.



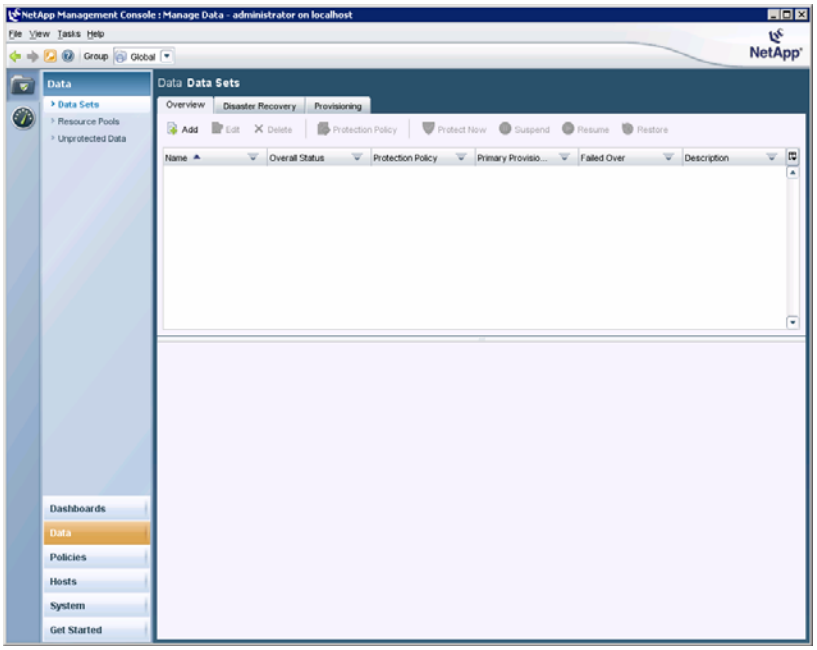
2. On the Nodes & Connections tab, select Primary Data to Backup. From the Throttle drop-down list, select (none) and then click OK.



5.3 CREATING A DATA SET

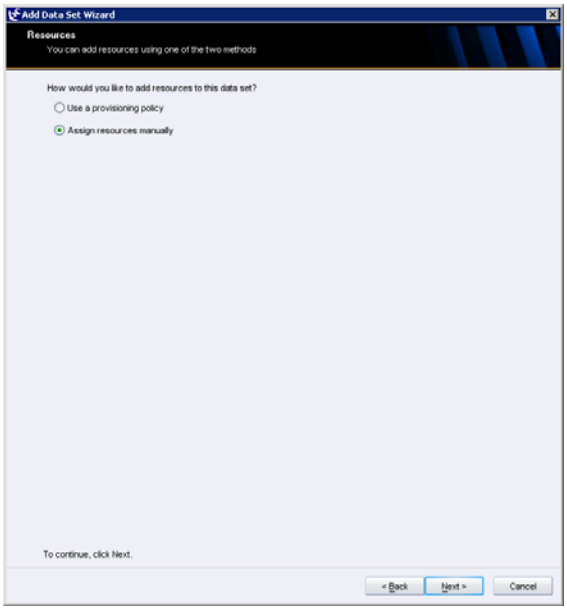
Next, you create a data set. In this case, a data set is a collection of virtual machines that you manage as a single unit. To create a data set, follow these steps.

1. In the NetApp Management Console, Manage Data, select Data > Data Sets and then click Add.

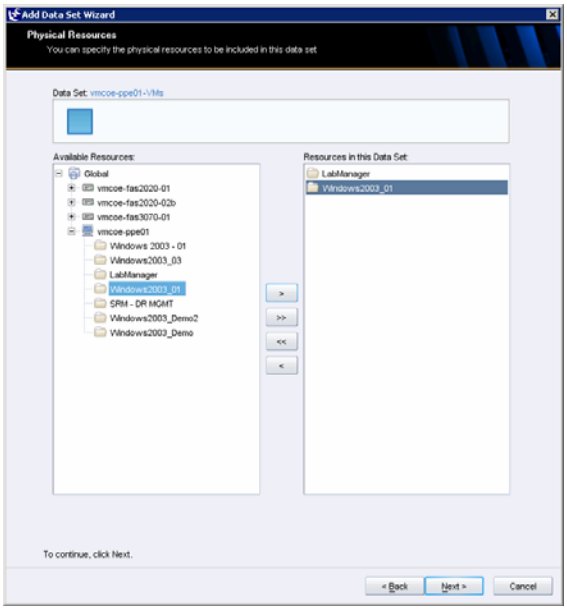


2. In the Add Data Set wizard that is displayed, give the data set a name.

3. Select Assign Resources Manually and then click Next.



4. Expand the ESX Server and select the virtual machines to protect in this data set. Move the selected virtual machines to the box on the right and then click Next.

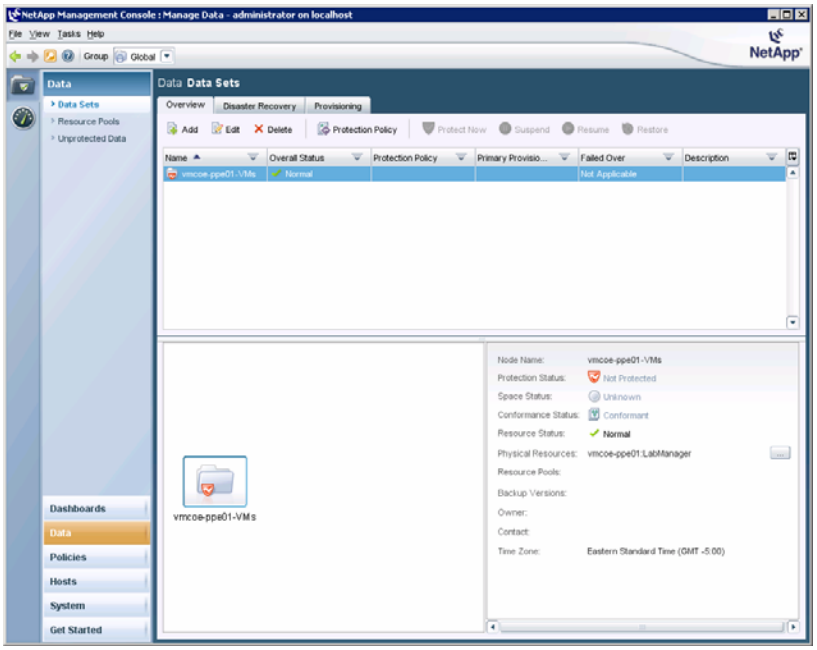


5. Continue through the rest of the wizard.

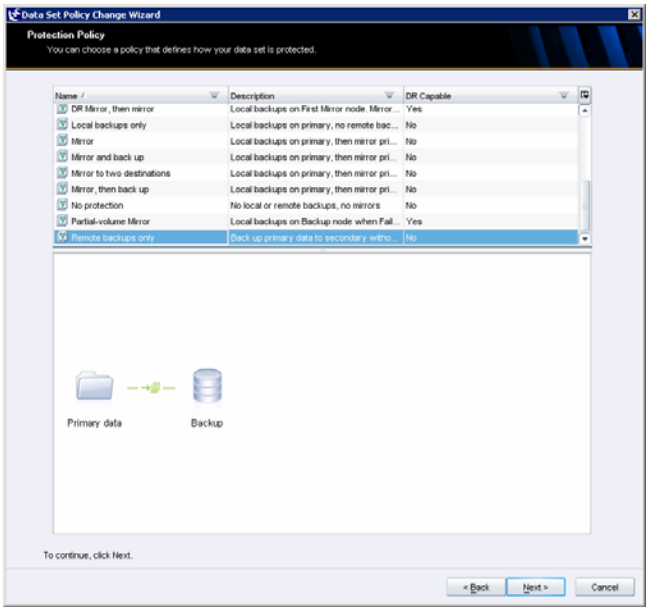
5.4 ADDING A PROTECTION POLICY

Follow these steps to add a protection policy.

1. In the NetApp Management Console, Manage Data, select Data > Data Sets. Select a data set and then click Protection Policy.

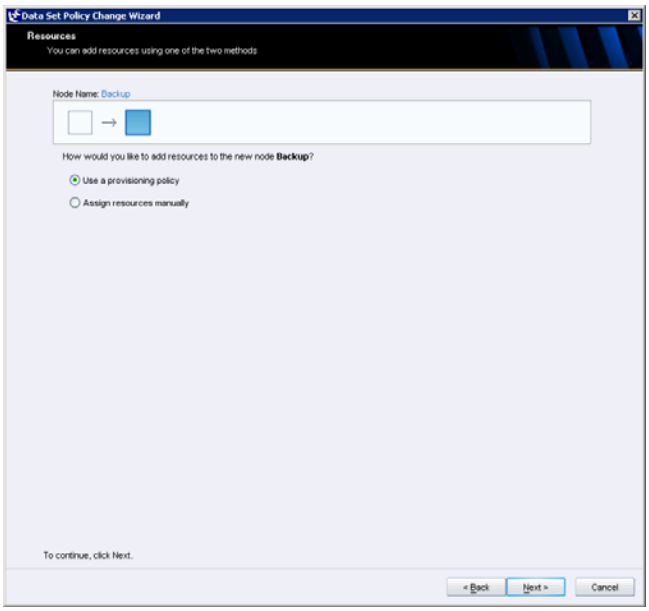


2. In the Data Set Policy Change Wizard that appears, select Remote Backups Only and then click Next.

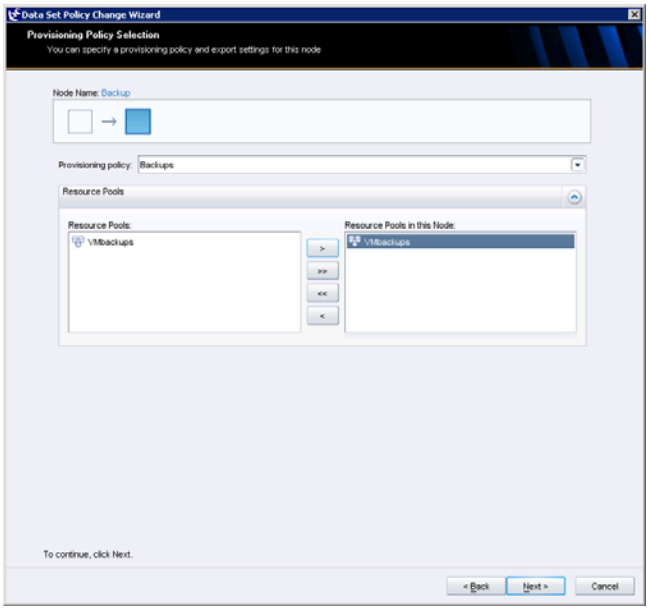


3. If a provisioning policy and a resource pool have already been established for destination storage, select Use a Provisioning Policy and then click Next.

   If a resource pool has not been created, select Assign Resources Manually and then select the destination location.



4. Select a provisioning policy and a resource pool. Click Next and continue through the wizard to provision flexible volumes.



After you have added the protection policy, the initial backup begins for the data set. To view the job progress, click System and then click Jobs.

5.5 RUNNING A MANUAL UPDATE

The Restore button is not available for a data set until a later update occurs.

- To manually run an update, select the data set and then click Protect Now. In the new window that opens, select a retention level for the backup and then click OK. When the backup is complete, the data set becomes available for restore operations.

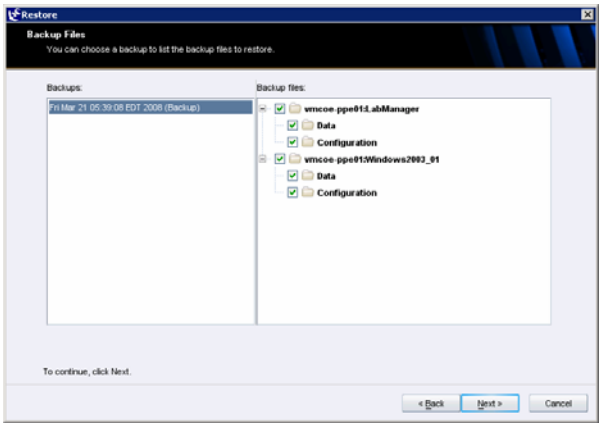
5.6 RESTORING THE DATA SET

To restore a data set, follow these steps.

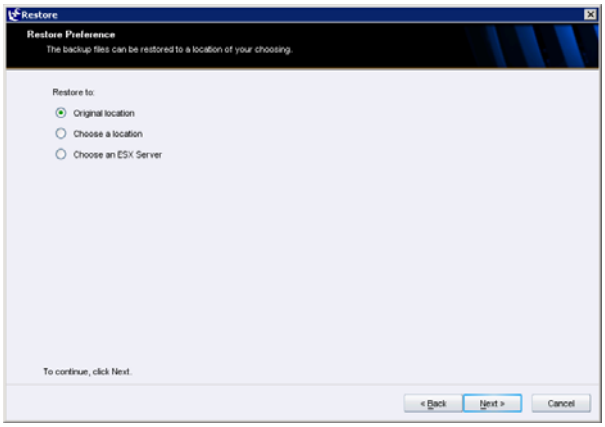
1. Select a data set and then click the Restore button to start the Restore wizard.

2. Select the virtual machines to restore. You can restore only the data (disk files) or both the data and the configuration (configuration files and log files).

   Note: If the virtual machine does not exist, you must select both the Data and Configuration options.



3. The following restore options appear.



- Select Original Location to restore the virtual machines to their original data store. When the restore is complete, VMware powers on the virtual machines.
- Select Choose a Location to browse the file systems of the ESX Servers and select the restore location.

Note: if you want the restore to become a usable virtual machine, you must direct the restore to a valid data store.

- The third option, Choose an ESX Server, is useful if all of the following are true:
  - The virtual machine has been lost or destroyed
  - The ESX Server that originally backed up the virtual machine has been lost or destroyed
  - You want to restore the virtual machine to an alternate ESX host

When you use the third option, the alternate ESX Server must have Open Systems SnapVault installed. It must also have shared access to the data store where the virtual machine was originally located. After the restore is complete, the virtual machine files must be imported into VMware.

4. Continue through the wizard to begin the restore transfers.

6 BEST PRACTICES

Many of the general best practices that have already been defined for Open Systems SnapVault apply to backups of whole virtual machines as well. However, there are a few more best practices to keep in mind.

6.1 MINIMUM MEMORY SIZE FOR VIRTUAL MACHINES

NetApp recommends that you assign each virtual machine at least 256MB of memory.

6.2 NUMBER OF VIRTUAL MACHINES TO PROTECT

Depending on the size of the virtual environment, it may not be a good idea to back up all virtual machines on an ESX Server at the same time. As more virtual machines are backed up at the same time, load increases on the server. This can cause post-backup deletion of VMware snapshots to timeout and eventually fail. If VMware can't delete a snapshot, subsequent backups for that virtual machine will fail until the snapshot is manually removed.

6.3 SCHEDULING WITH VMOTION IN MIND

When scheduling backups, keep in mind the backup schedules for any virtual machines that might migrate via VMotion. Here's an example. Suppose that you have two ESX Servers with three virtual machines each and that each ESX Server backs up all three virtual machines at 6 p.m. If you use VMotion to migrate all three virtual machines from one ESX Server to another, the load for that server is increased. At 6 p.m., all six of these virtual machines get backed up while hosted by a single server. This can cause performance degradation.

Also be aware that virtual machines may get migrated automatically in a VMware Distributed Resource Scheduler (DRS) environment.

7 KNOWN BEHAVIORS

This section describes limitations that have been identified. You should understand these limitations before deploying the product.

- Open Systems SnapVault backups fail if a VMware snapshot exists when the backup starts. Any existing snapshots must be deleted before backup.

- Virtual machines that contain disks of multiple modes must be powered off before they can be backed up. By default, these virtual machines are not powered off and are not backed up. You control this behavior by modifying the `vmware.poweroff_before_ss` variable by using the `svconfig` command. Independent and virtual RDM disks are not backed up regardless of whether or not the virtual machine is powered off.
- Virtual machines that contain physical RDMs are not backed up; the backup fails.
- Any changes to a virtual machine's uuid cause backups to fail.
- A virtual machine that is registered with an ESX Server different than the one initiating an Open Systems SnapVault backup is not supported for baseline transfers. Update transfers are supported.
- When a virtual machine has been migrated with VMotion to an alternate ESX Server, its original ESX Server must remain available in order for incremental updates to continue to function.
- NetApp deduplication is not currently supported for Open Systems SnapVault destination volumes.
- Open Systems SnapVault does not perform application backups. When a virtual machine is backed up, it is done so in a consistent state. Any applications hosted by that virtual machine are crash consistent unless they are shut down before the backup.

8 TROUBLESHOOTING

This section discusses some things to check if you encounter problems with Open Systems SnapVault 2.6 in an ESX environment.

8.1 LOG FILE LOCATIONS

The default log file locations are:

On the NetApp destination: `/etc/log/snapmirror`

On the ESX Server: `/usr/snapvault/etc/snapvault`

8.2 COMMON ERROR CONDITIONS

Errors when VMware snapshot exists before backup

Error on the storage system (snapmirror log):

```
Abort (could not read from socket)
```

Errors on the ESX Server (snapvault log):

```
Snapshot API failed or a snapshot exists(1) for VM
Error while trying to create VM snapshot
Failed to create volume snapshot
```

Error when the firewall is blocking ports

Error on the storage system (snapmirror log):

```
Abort (cannot connect to source filer)
```

Errors when VM is powered off and backup fails

Error on the NetApp destination (snapmirror log):

```
Abort (could not read from socket)
```

Errors on the ESX Server (snapvault log):

```
VM is not ON. Skip backup of this VM
Error while trying to create VM snapshot
Failed to create volume snapshot
```

Errors when HTTP is used and not properly configured

Error on the NetApp destination (snapmirror log):

```
Abort (source is not a valid name or qtree path)
```

Errors on the ESX Server (snapvault log):

```
Failed to Create Session
Failed to validate the given VM instance
Have not been supplied a valid application path
```

9 ADDITIONAL REFERENCES

Open Systems SnapVault (OSSV) Best Practices Guide

Open Systems SnapVault 2.6 Release Notes

Open Systems SnapVault 2.6 Installation and Administration Guide

VMware Introduction to Virtual Infrastructure

VMware Server Configuration Guide

10 APPENDIX

10.1 SINGLE FILE RESTORE

Although restores of virtual machines are inherently limited to whole restores, there is a way to restore a single file from a virtual machine backup. This process is outside of the scope of Protection Manager functionality.

To restore a single file from a virtual machine backup, create a FlexClone® copy of the destination volume. **Note:** The snapshot copy used for the FlexClone volume must not be more recent than the base snapshot copy.

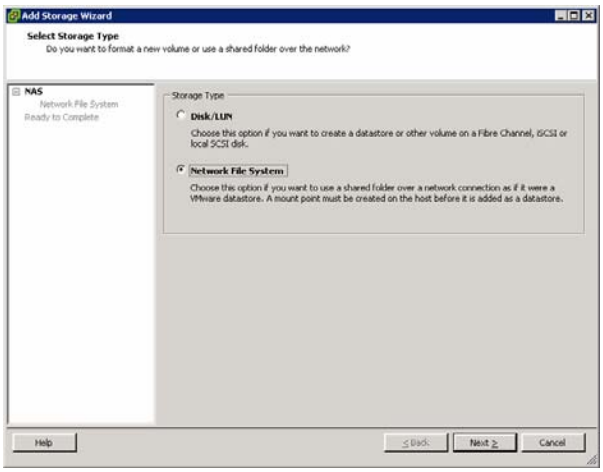
For example:

```
vmcoe-fas2020-01*> vol clone create VM_Recover -b dfpm_vmcoe_ppe01_VMs_SV_1206091033_3128
dfpm_windows2003-03.45.1206407247

Wed Mar 26 15:56:10 EST [vmcoe-fas2020-01: wafl.qtree.qsmBreak.base:error]: Breaking
snapmirrored qtree 1 in volume VM_Recover: base snapshot no longer exists. Use snapmirror
resync or initialize to re-establish the snapmirror.

Wed Mar 26 15:56:10 EST [vmcoe-fas2020-01: wafl.volume.clone.created:info]: Volume clone
VM_Recover of volume dfpm_vmcoe_ppe01_VMs_SV_1206091033_3128 was created successfully.

Creation of clone volume 'VM_Recover' has completed.
```

Verify that the FlexClone volume has been exported by NFS with read-write permissions.

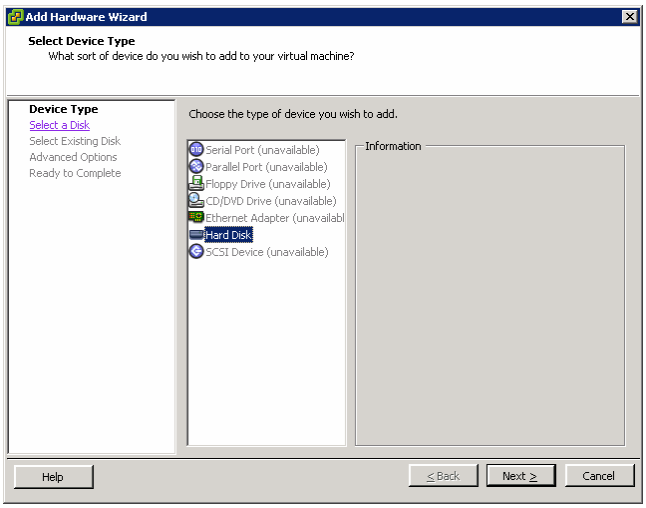
Next, using the VI Client, add the FlexClone volume as an NFS data store to the ESX Server.

- To add the data store, select the ESX Server and open the Configuration tab. Under the Hardware section, click Storage > Add Storage. Using the wizard, add the Network File System that points to the FlexClone volume.

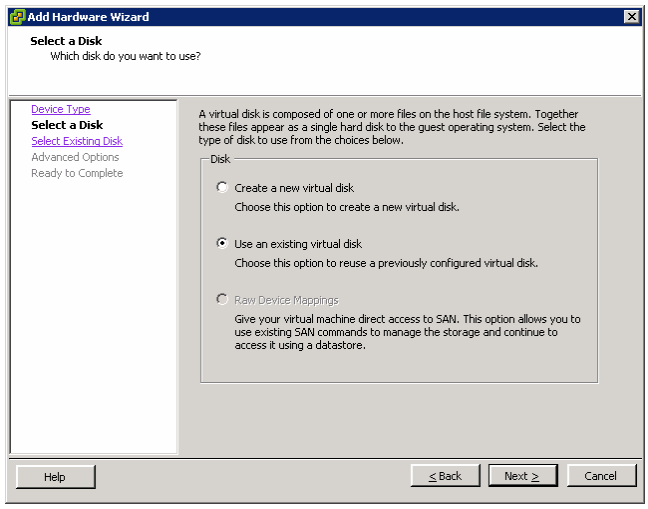


The next step is to add a new disk to one of the virtual machines. You can do this on the virtual machine to which you want to restore the file, or you can add it to a separate virtual machine. The new disk is the .vmdk file located in the data store that was previously cloned. To add a virtual disk, follow these steps.

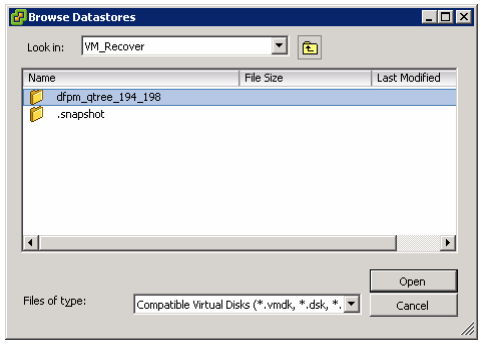
1. Select a virtual machine and then select Edit Settings from the Summary tab. On the Hardware tab, click Add.
2. Select Hard Disk and then click Next.



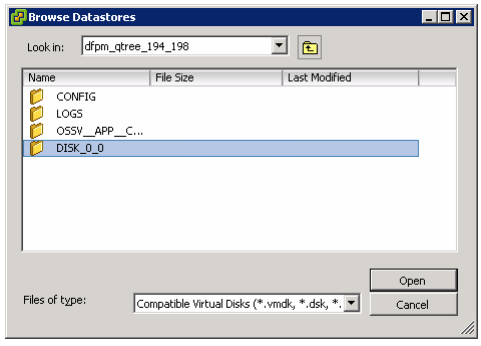
3. Select Use an Existing Virtual Disk and then click Next.



4. Browse the data store and select the qtree.



5. Navigate to the appropriate disk directory and choose the .vmdk file to add.



6. After you have added the disk to the virtual machine, you may need to run a disk rescan from within the OS of the virtual machine. Once the disk is available to the OS, the files to be restored can be accessed. You can then use file copy and network sharing techniques to restore the file to the proper location.

To remove the disk, follow these steps.

1. Power off the virtual machine.
2. Click Edit Settings and remove the hard disk.

To remove the data store, follow these steps.

1. Select the ESX Server and open the Configuration tab.
2. In the Hardware section, click Storage.
3. Select the data store and click Remove.
4. Remove the FlexClone volume by using the `vol offline <volume>` and `vol destroy <volume>` commands.

10.2 DISASTER RECOVERY, TEST, AND DEVELOPMENT

You can use the backup of a virtual machine to build a running copy of that virtual machine for test, development, or DR purposes. This copy can be brought online on any ESX Server that has NFS access to the destination storage. This is accomplished with minimal disk space by using FlexClone technology.

1. Create a FlexClone volume of the destination volume.

   Note: The snapshot copy used for the FlexClone volume must not be more recent than the base snapshot copy.

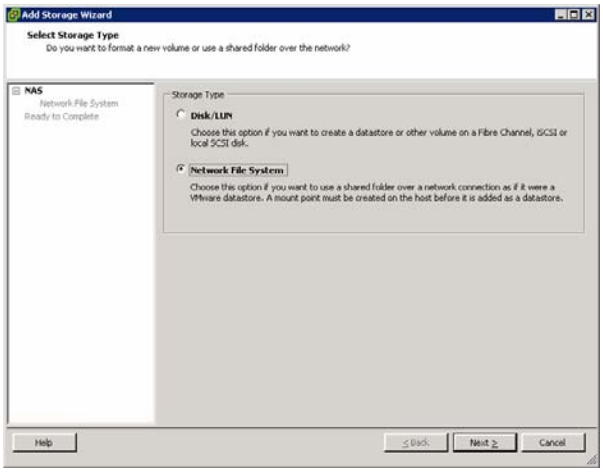
   For example:

   ```
   vmcoe-fas2020-01*> vol clone create VM_TESTDEV -b
   dfpm_vmcoe_ppe01_VMs_SV_1206091033_3128 dfpm_windows2003-03.46.1206493649

   Thu Mar 27 11:18:22 EST [vmcoe-fas2020-01: wafl.qtree.qsmBreak.base:error]:
   Breaking snapmirrored qtree 1 in volume VM_TESTDEV: base snapshot no longer
   exists. Use snapmirror resync or initialize to re-establish the snapmirror.

   Thu Mar 27 11:18:22 EST [vmcoe-fas2020-01: ems.engine.inputSuppress:info]: Event
   'wafl.volume.clone.created' suppressed 1 times since Thu Mar 27 10:48:24 EST 2008.

   Creation of clone volume 'VM_TESTDEV' has completed.

   vmcoe-fas2020-01*> Thu Mar 27 11:18:22 EST [vmcoe-fas2020-01:
   wafl.volume.clone.created:info]: Volume clone VM_TESTDEV of volume
   dfpm_vmcoe_ppe01_VMs_SV_1206091033_3128 was created successfully.
   ```

2. Make sure that the FlexClone volume has been exported by NFS with read-write permissions.

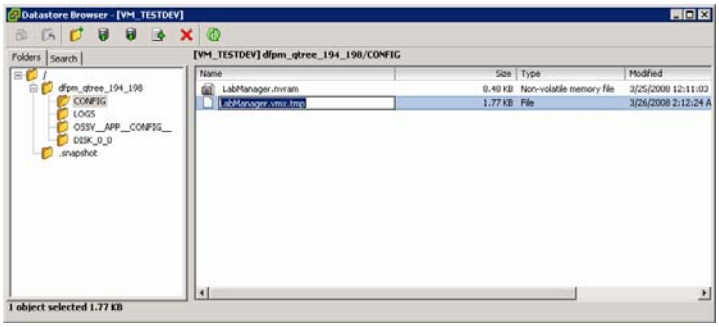
From the VI Client, follow these steps to add the FlexClone volume as an NFS data store to the ESX Server.

1. Select the ESX Server and open the Configuration tab.
2. In the Hardware section, select Storage > Add Storage.
3. Use the wizard to add the Network File System that points to the FlexClone volume.

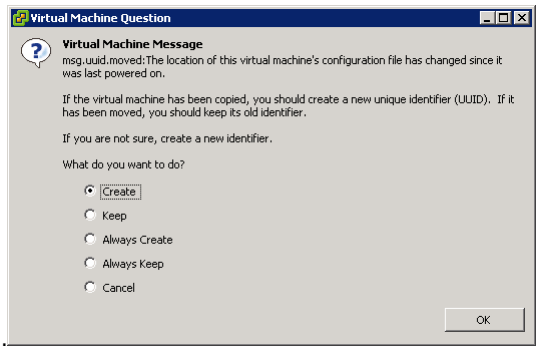


When the data store has been added, follow these steps to rename the vmx file to remove the .tmp extension.

1. Select an ESX Server and open the Configuration tab.
2. In the Hardware section, click Storage and then double-click the data store.
3. The .vmx file resides in the CONFIG directory in the qtree. Highlight the .vmx file and remove the .tmp extension.



4. Rename the file and then select Add to Inventory. Continue through the wizard to complete the import operation.
5. When the virtual machine has been imported, edit the settings for the virtual machine and remove Hard Disk from the Hardware tab.
6. Click Add and create a new hard disk from an existing virtual disk.
7. Browse the data store and select the .vmdk file.
8. Continue through the wizard.
9. Power on the virtual machine.
10. The following dialog box may appear. Select Create and then click OK. The virtual machine powers up.



To remove the virtual machine and the FlexClone volume, follow these steps.

1. Power off the virtual machine.
2. Right-click the virtual machine and select Remove from Inventory.
3. Remove the data store: Select the ESX Server and open the Configuration tab. In the Hardware section, select Storage. Select the data store and then click Remove.
4. Remove the FlexClone volume by using the `vol offline <volume>` and `vol destroy <volume>` commands.