HP OpenView Storage Data Protector 5.5/6.0

VMware ESX Server 2.x/3.0.2/3.5.0
Virtual disk snapshot capabilities
Integrated with Data Protector 5.5/6.0

Abstract

This document describes the integration of VMware ESX Server (2.X, 3.0.2/3.5.0) snapshot capabilities with Data Protector. The Data Protector version mentioned and tested here is Data Protector A.05.50 and A.06.00.

The backup methods explained in this whitepaper are:-

1. Backup the entire VMware ESX Server, virtual machines and VMFS for disaster recovery which is explained in the chapter Integration of VMware using snapshot capabilities.

2. Using data protector agents to backup individual virtual machines as independent clients or even cell managers which is explained in the chapter Using Data Protector Agents to backup/restore Virtual Machines as DP clients

Introduction

VMware ESX Server is server virtualization software. It consists of a small, Linux-based Server Console that provides working environment for several virtual machines (VMs). Virtual disks can be stored on raw disk partitions or on vmfs file system. The vmfs file system is designed to allow large files (well over 2 GB in size) and to store them efficiently for usage pattern imposed by virtual machines.

Virtual machines can be controlled (scripted) through supplied Perl interface. This includes (but is not limited to) enumeration of virtual machines, querying and controlling machine state and enumeration of used resources.

The Server Console can be backed up when the Data Protector Disk Agent is installed on it. It is possible to recreate the Server Console to a working state from scratch in less than half an hour, even if no backup is available. If a backup of the Server Console is available, then the desired Server Console's state can be restored. It is possible to back up the virtual machines using the full Data Protector functionalities when the machine is treated as a common physical machine.

Integration of DP with VMware using snapshot capabilities

This section describes steps integrating Data Protector with VMware ESX Server using VMware ESX Server's snapshot capabilities. This solution doesn't involve a special Data Protector agent, but is implemented using shell and Perl scripts that work with the respective Data Protector Agents.

Backing up the VMware ESX Server consists of two fundamentally different tasks. The first task is to back up the Server Console. The second task is to back up the virtual machines. The detailed steps for performing both the tasks are given in the following sections.

Installation of Data Protector

To utilize the scripts provided for Backup & Restore of VMware ESX Server, the machine hosting the Virtual Machines and Server Console must be first configured as a Data Protector client. This consists of installing the needed Data Protector agents i.e. Disk and Media Agent on the host adding the host into the Data Protector cell.

Steps to make ESX ready for DP

1. (on ESX) Update ***/etc/ssh/sshd_config*** file on the ESX server to permit *root* login by setting:

```
PermitRootLogin yes
```

2. (on ESX) Enable the SSH server service on the ESX server by entering (this service may already be enabled, in which case the *sshd PID* needs to be sent the *kill -HUP* signal):

```
# esxcfg-firewall -e sshServer
```

3: (on ESX) To be able to ftp to another system from the ESX server:

```
# esxcfg-firewall –AllowOutgoing
```

4: (on ESX)reboot ESX

```
#shutdown –r now
```

5: (on IS)Now test non key access first from IS to ESX

```
# ssh root@<ESX_Server>
```

Enter the ESX server password to register the login for the first time

Modify your bash shell rc file .bashrc

Add a few helpful aliases in order to see the hostname and current directory

```
# User specific aliases and functions

alias rm='rm -i'
alias cp='cp -i'
alias mv='mv -i'
alias ll='ls -l'
alias le='ls -lart|tail'
alias la='ls -la'

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi


PS1="[`whoami`@`hostname -s`]\$PWD
# "
        export PS1
```

Save the file and execute the rc file

```
[root@esxserver root]# . ./.bashrc
```

Configure ssh (not mandatory but recommended)

1. (on IS) A public-private key pair must be generated on the installation server by entering:

```
# ssh-keygen -t rsa
```

2: (from ESX to IS)The public key must be copied from the installation server to the ESX server. The key generated in step 1 was created as ***/root/.ssh/id_rsa.pub*** on the installation server. This key must be copied to he ESX server as ***/root/.ssh/authorized_keys*** by running the following on the installation server:

```
# scp /root/.ssh/id_rsa.pub <ESX_Server>:/root/.ssh/authorized_keys
```

3. (on IS) The ESX server must be added to the SSH list of known hosts on the installation server by running the following on the installation server:

```
# ssh root@<ESX_Server>
```

Set specific DP variables and parameters

1. (on IS) The ***OB2_SSH_ENABLED=1*** *omnirc* variable must be set to *1* on the installation server in ***/opt/omni/.omnirc***.

2. (on ESX) Port 5555 must be opened on the ESX server for incoming and outgoing Data Protector traffic as follows:

```
# esxcfg-firewall –o 5555,tcp,out,DP
# esxcfg-firewall –o 5555,tcp,in,DP
```

Disk agent

It is necessary to install the Disk agent on the ESX Server to be able to backup the virtual machines present on this host using the snapshot capabilities. The Media Agent can either be installed remotely or locally.

For detailed installation procedure of installing a Data Protector Disk Agent, please refer to the section “Procedure for Push Installation of DP Agents to ESX”.

Media agent

The Media agent can be installed either on the host where ESX Server is installed or on any other host in the Data Protector Cell, but for better performance it is recommended that the Media agent is installed on the host where a backup device is attached. Media agent can also be installed on the virtual machine, but it is not recommended as it cannot be used when the virtual machine is suspended. The Media Agent can either be installed remotely or locally.

For detailed installation procedure of installing a Data Protector Media Agent, please refer to the section “Procedure for Push Installation of DP Agents to ESX”.

Local install from DVD or iso image

Only when a physical DVD is available you can mount the e.g. B6961-10002 DVD (DP 6.00).

```
# mount –t auto /dev/cdrom /mnt/cdrom
```

Best is to make or download a iso image from the DVD B6961-10001 and B6961-10002 (both DP 6.00) and to ftp the files under */vmimages/iso_depot/DP_6.00*

Note: other iso images are available on http://www.hp.com/go/dataprotector (select evaluation downloads)

Mount the iso image file:

```
# mount -o loop /vmimages/iso_depot/DP_6.00/B6961-10002.iso /mnt/cdrom
```

Uncompress command

On ESX the uncompress command does not exist. Some older installations scripts are using this command and will fail. An easy workaround is available:

```
# cd /bin
# ln gzip uncompress
```

Install locally and import the agents

Go to /mnt/cdrom/LOCAL_INSTALL

```
# ./omnisetup.sh -source /mnt/cdrom -server cellserver.ind.hp.com -install da,ma
  No Data Protector/OmniBack software detected on the target system.


  Packets going to be (re)installed: omnicf  da ma

  Unpacking selected packets from CD, please wait (5-10 minutes)...
  Unpacking complete!

  Installing Core (omnicf)...

61831 blocks
Data Protector Software package successfully installed
  Installing Disk Agent (da)...

Data Protector Software package successfully installed
  Installing Media Agent (ma)...

Data Protector Software package successfully installed
  Importing client to cellserver.ind.hp.com...
Import host successful.

  Installation/Upgrade session finished.
```

Check the cell server

On the cell server verify the client

```
# omnicheck -patches -host esx_server
Patch level         Patch description
===========================================
Number of patches found: 0.
```

Install patches in order to update the DA and MA

When a **UNIX IS** available on the network, upgrade the agents however when only Windows systems are available a workaround is necessary.

Install the patches without UNIX IS on ESX server

The patches are the following packets you can extract from the latest UNIX IS patches for HP-UX PA / IA64 / Solaris and Linux. Untar the patch first.

E.G. This example is for DP 6.00 but the same principle is valid for 5.50.

CORE patch: PHSS_37173

```
…/opt/omni/databases/utils/gpl/i386/linux-x86/utils.tar
```

```
…/opt/omni/databases/vendor/omnicf/gpl/i386/linux-x86/A.06.00/packet.Z
```

Media Agent patch: PHSS_37175

```
…/opt/omni/databases/vendor/ma/gpl/i386/linux-x86/A.06.00/packet.Z
```

Disk Agent patch : PHSS_37881

…/opt/omni/databases/vendor/da/gpl/i386/linux-x86/A.06.00/packet.Z

Note : Since the name is the same for all packets please copy those into a repository as follow:

```
# ll
total 15152
-rw-r--r--    1 root     root     12078354 Mar  7 11:40 CORE_packet.Z
-rw-r--r--    1 root     root       730541 Mar  7 11:40 DA.packet.Z
-rw-r--r--    1 root     root      2660423 Mar  7 11:40 MA.packet.Z
-rw-r--r--    1 root     root        13875 Mar  7 11:40 utils.tar
```

Place the 4 files to /tmp
Note: those files are double zipped and have to be unzipped first!

```
# mv utils.tar utils.tar.Z
# uncompress  utils.tar.Z

# uncompress CORE_packet.Z
# mv CORE_packet  CORE_packet.Z
# uncompress DA.packet.Z
# mv DA.packet  DA.packet.Z
# uncompress MA.packet.Z
# mv MA.packet  MA.packet.Z
```

Make a dir omni_tmp under /tmp.

```
# mkdir omni_tmp
```

Copy the files into omni_tmp

```
utils.tar
CORE_packet.Z
DA.packet.Z
MA.packet.Z
```

In /tmp/omni_tmp

```
# tar xvf utils.tar
omni_chk_ds.sh
omni_chk_vers.sh
omni_de_inst.sh
omni_rinst.sh
```

install CORE first, then DA and optional MA

```
# ./omni_rinst.sh /tmp/omni_tmp/CORE_packet.Z core A.06.00 gpl/i386/linux-x86 /opt/omni
cellserver.ind.hp.com 5555

63429 blocks
Data Protector Software package successfully installed
# ./omni_rinst.sh /tmp/omni_tmp/DA.packet.Z da A.06.00 gpl/i386/linux-x86 /opt/omni
cellserver.ind.hp.com 5555

Data Protector Software package successfully installed
# ./omni_rinst.sh /tmp/omni_tmp/MA.packet.Z ma A.06.00 gpl/i386/linux-x86 /opt/omni
cellserver.ind.hp.com 5555

Data Protector Software package successfully installed
```

Check the patches on the CC

```
# omnicheck -patches -host  esxserver
Patch level         Patch description
===========================================
PHSS_37173/PHSS_37174/DPSOL_00315/DPLNX_00038 Core Component
PHSS_37881/PHSS_37882/DPSOL_00336/DPLNX_00051 Disk Agent
PHSS_37175/PHSS_37176/DPSOL_00316/DPLNX_00039 Media Agent
```

Patch analyse

```
# rpm -qa  | grep OB2
OB2-DA-A.06.00-1
```

```
OB2-CORE-A.06.00-1
OB2-MA-A.06.00-1

# rpm -qi OB2-DA-A.06.00-1
Name        : OB2-DA                       Relocations: (not relocatable)
Version     : A.06.00                           Vendor: (none)
Release     : 1                             Build Date: Thu 21 Feb 2008 04:07:15 PM CET
Install Date: Fri 07 Mar 2008 12:55:06 PM CET      Build Host: lxbld7.india.hp.com
Group       : Data-Protector                Source RPM: OB2-DA-A.06.00-1.src.rpm
Size        : 1732143                          License: Hewlett-Packard Company
Signature   : (none)
Summary     : HP OpenView Storage Data Protector Disk Agent
Description :
This package  contains the HP OpenView Storage Data Protector disk processing agents. These
run on all Data Protector nodes.

#  rpm -ql OB2-DA-A.06.00-1
/opt
/opt/omni
…
```

Integration scripts

The VMware ESX Server 2.x/3.0.2/3.5.0 is integrated with Data Protector using shell and Perl scripts. The prepared scripts are:

```
1.      DPvmware_config.sh_TMPL
2.      DPvmware_setup.sh
3.      DPvmware_preexec.sh
4.      DPvmware_postexec.sh
5.      Dpvmware_addredo.pl
6.      DPvmware_commitop.pl
7.      DPvmware_createsnapshot.pl
8.      DPvmware_removesnapshot.pl
9.      DPvmware_vmmapping.pl
10.   DPvmware_vmfs-mount.sh
11.   DPvmware_vmfs-umount.sh
```

Out of the above scripts, first four scripts are common for ESX server versions 2.x and 3.0.2/3.5.0.

DPvmware_addredo.pl, DPvmware_commitop.pl, DPvmware_vmfs-mount.sh, DPvmware_vmfs-umount.sh are specific to 2.x ESX server.

DPvmware_createsnapshot.pl, DPvmware_removesnapshot.pl and DPvmware_vmmapping.pl are specific to ESX server 3.0.2/3.5.0.

The scripts (DPvmware_preexec.sh and DPvmware_postexec.sh) should be used as backup pre-exec and post-exec scripts when configuring the Data Protector file-system backup specification (datalist). Refer Figure # 5. The DPvmware_preexec.sh script puts the selected virtual machines in suspended mode using the "vmware-cmd" tool, while the DPvmware_postexec.sh script returns them to the state as they were before the backup session. These scripts also call the Perl scripts for creating and committing the snapshots if required.

The Perl scripts are used for

1. Mapping the virtual machine configuration file to the display name (applicable for ESX 3.0.2/3.5.0 only).
2. Taking snapshot of the virtual machines.
3. Removing of snapshots after the backup.

These scripts use VMware Perl APIs, which are installed on VMware ESX Server when the VMware software is installed.

There is a configuration script (DPvmware_config.sh_TMPL) and a setup shell script (DPvmware_setup.sh) provided as part of this solution.

To install these scripts in their proper locations on ESX server, execute `DPvmware_setup.sh` as "root" user with –install option. This will perform following actions:

1. Places the new shell and Perl scripts in the proper locations as per the version of the Data Protector and sets the right permissions and ownerships for these scripts. It will overwrite the shell and Perl scripts currently installed in the client.
2. Places the configuration script DPvmware_config.sh_TMPL in "`/usr/omni/bin`" for Data Protector 5.5 or in "`/opt/omni/newconfig/etc/opt/omni/client`" for Data Protector 6.0. For DP 5.5 this file has to be copied to the same location i.e "/usr/omni/bin" with the name DPvmware_config.sh. And for DP 6.0 this file has to be manually copied to "/etc/opt/omni/client" with the name DPvmware_config.sh. If this installation is done upon an existing setup then you have to copy the DPvmware_config.sh file from the "/opt/omni/newconfig" directory to "/etc/opt/omni/client" directory.
3. Mounts the VMFS file systems on the Service Console.

NB:- If the VMware integration scripts are installed through the patch then the DPvmware_setup.sh will create only links for the preexec and postexec scripts.

With VMware ESX Server, the VMFS file systems are not mounted on the Service Console by default. Mounted VMFS file systems can be listed using the VMware specific "`vdf`" command (The VMFS file systems are not listed using the "`df`" command). Execution of the DPvmware_setup.sh with –install option would have mounted the VMFS file system. If the VMFS file systems are not already mounted on the service console, they can be mounted on the Service Console by running `DPvmware_setup.sh` with `--mount` option. This would ensure that the VMFS file systems are mounted at the time of VMware ESX Server startup and unmounted at the time of shutdown, ensuring that the VMFS file systems are accessible by the Data Protector Agents for backup and restore.

Procedure for Backup

The basic steps of backup are:

1. Identify the configuration data and virtual disks of the virtual machines to be backed up from the VMware ESX Server.
2. Create the Data Protector backup specification with the Virtual Machine's configuration files and virtual disk files selected for backup.
3. Update the DPvmware_config.sh script under "/etc/opt/omni/client" for DP 6.0 or "/usr/omni/bin" for DP 5.5 with the VM's configuration file

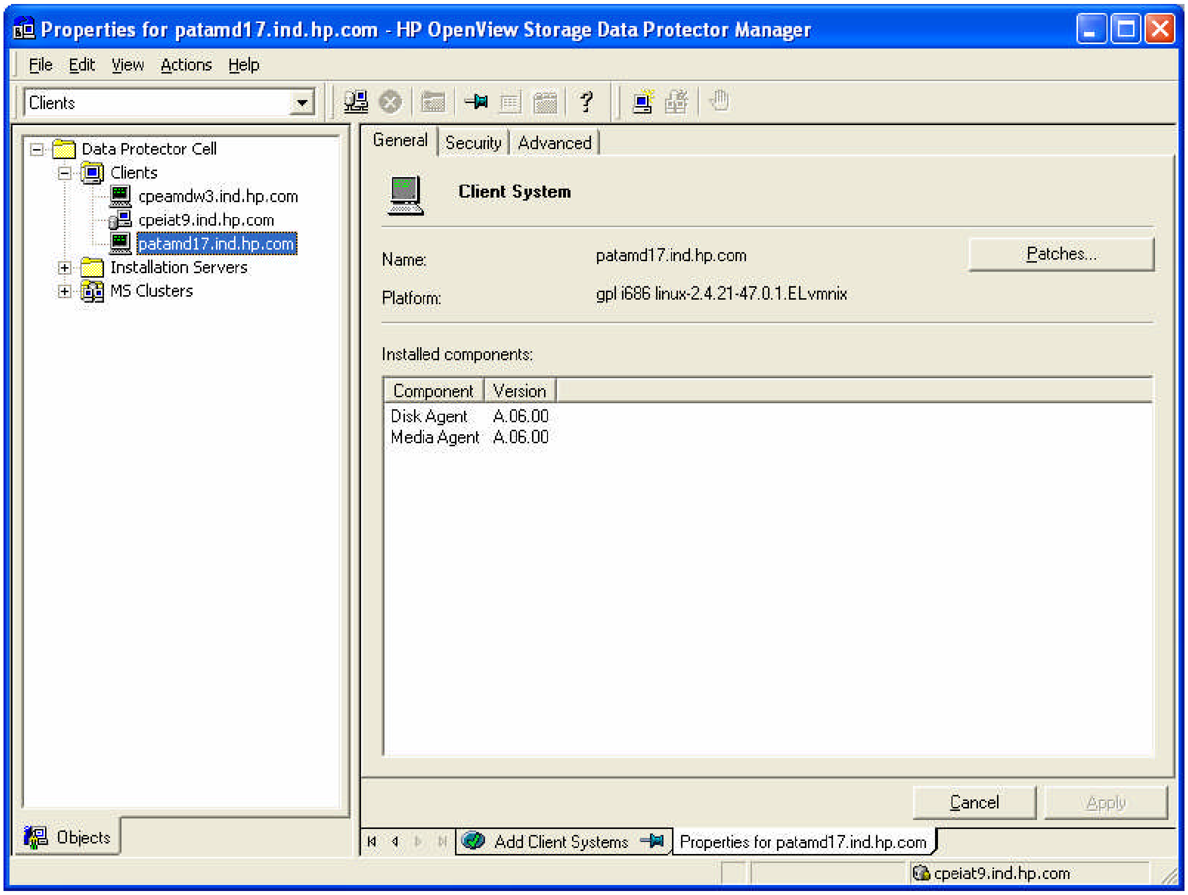
Configuring the Data Protector client

To identify the configuration data and virtual disks of the virtual machines to be backed up from the ESX Server, there are three steps involved, namely, identifying the host, identifying the virtual machines and identifying VMs' configuration.

Identify the host

The first step here is to identify the host hosting the virtual machines and add it to a Data Protector cell. The next step is to install the Data Protector Agents. Please refer to the earlier section regarding "Installation of Data Protector".

Example: As seen in Figure 1, `patamd7.ind.hp.com` hosts the Server Console and the VMs. Add it into Data Protector Cell and install the Disk and Media agents on it.



Name: patamd17.ind.hp.com

Platform: gpl i686 linux-2.4.21-47.0.1.ELvmnix

Installed components:

Component	Version
Disk Agent	A.06.00
Media Agent	A.06.00

Figure 1

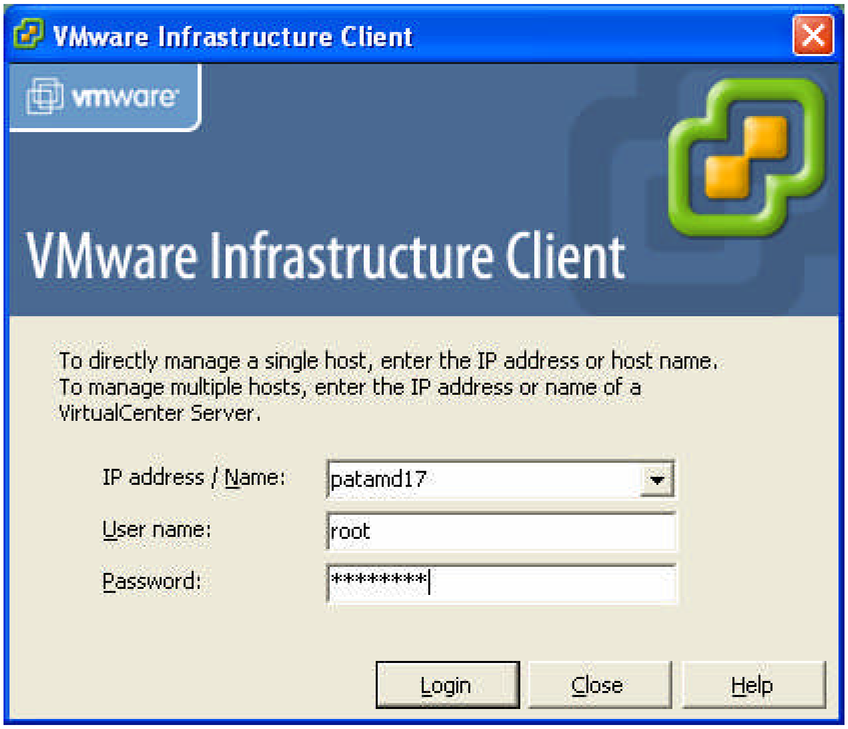
Identify the virtual machines

Next step is to identify the virtual machines to be backed up from the selected VMware ESX Server. To connect remotely to the VMware ESX Server http method can be used or Virtual Infrastructure client (VI) or VirtualCenter Server (VC) can be used. The screenshots provided in this document are of VI.

To access an ESX server through the VI or VirtualCenter Server (VC), you have to enter the ESX sever name, user and password.

Note: Virtual machines from the same VMware ESX Server should be configured and backed up in a single backup session.

Example: The figure below shows the login window for VMware ESX server `patamd17.ind.hp.com` through VI.



VMware Infrastructure Client

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a VirtualCenter Server.

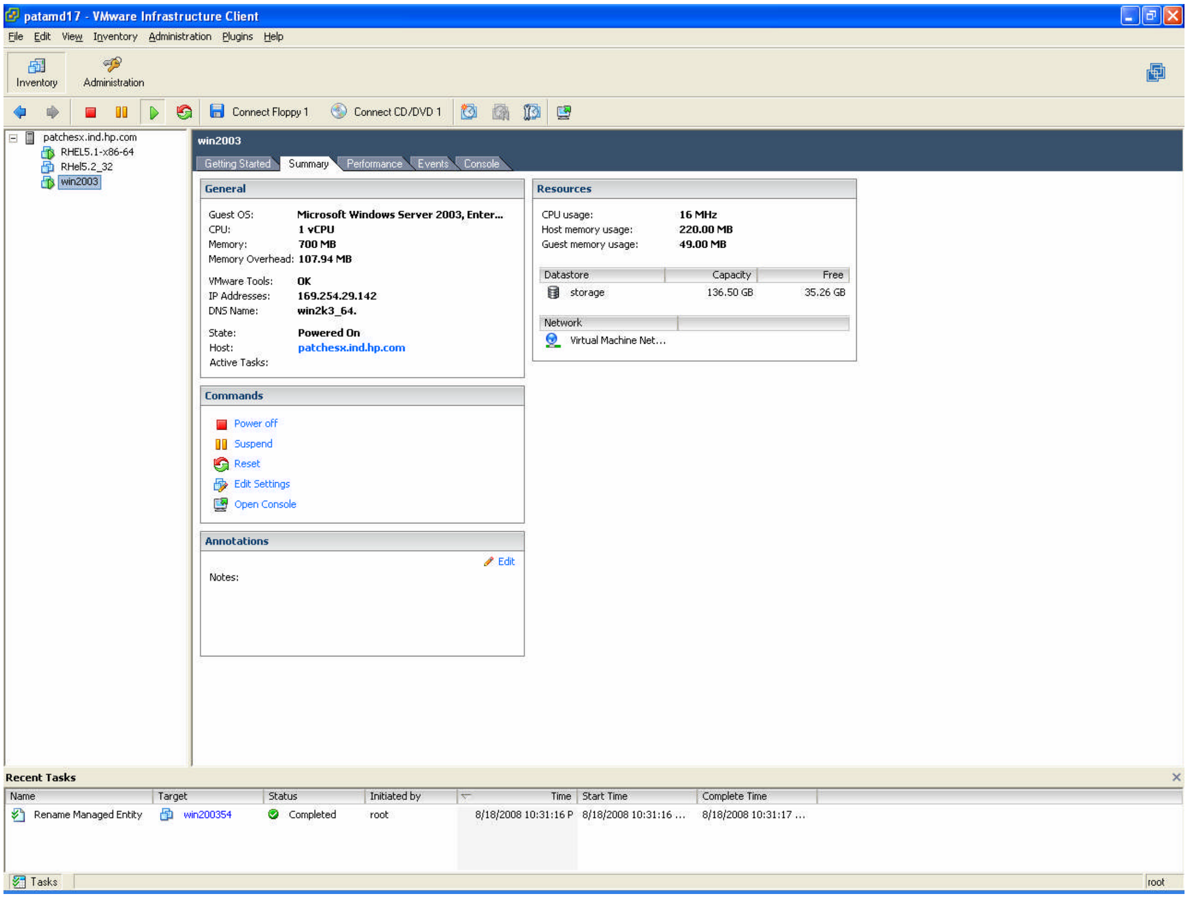
IP address / Name: patamd17

User name: root

Password: ********

Figure 2

After entering the username and password for the selected user, the configuration page of the virtual machines is accessed as shown in Figure 3.



General

Guest OS: Microsoft Windows Server 2003, Enter...
CPU: 1 vCPU
Memory: 700 MB
Memory Overhead: 107.94 MB

VMware Tools: OK
IP Addresses: 169.254.29.142
DNS Name: win2k3_64.

State: Powered On
Host: patchesx.ind.hp.com
Active Tasks:

Resources

CPU usage: 16 MHz
Host memory usage: 220.00 MB
Guest memory usage: 49.00 MB

Datastore	Capacity	Free
storage	136.50 GB	35.26 GB

Network
Virtual Machine Net...

Notes:

Recent Tasks

Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Rename Managed Entity	win200354	Completed	root	8/18/2008 10:31:16 P	8/18/2008 10:31:16 ...	8/18/2008 10:31:17 ...

Figure 3

Identifying the VM's configuration

Next step is to identify the virtual machine's configuration. There are following steps involved in this.

a. Identify full path of the configuration file.

The full path of the configuration file is required to configure the DPvmware_config.sh.

For ESX 3.x

To configure the "`DPvmware_config.sh`" either you can use the full path of the configuration file of the VM or the name of the VM that is displayed in the Virtual client or VI client. For example in the above mentioned Figure-3, the VM name is "`win2003`". If anytime the name of the VM modified then the DPvmware_config.sh has to be updated with the modified name. User can use the output of "`vmware-cmd –l`" to identify the registered virtual machine configuration file. Typically this location will be "`/vmfs/volumes/<UU-id>/virtualmachine/virtualmachine.vmx`".

For ESX 2.x

In case of ESX 2.x the DPvmware_config.sh has to be configured only with the full path of the configuration file. This location will be `/<username>/vmware/<platform>/<platform>.vmx`". Here the username is the owner of the VM (E.X: root user).

b. Identify the virtual disk's file name

Next step is to identify the virtual disk's file name for the selected virtual machine.

In “Hardware” tab under the “Virtual Disk” section, identify the `<VM_diskname>.dsk` file which represents the virtual disk of the VM. The filename and location of the virtual disk will be used later when configuring the Data Protector datalist. For ESX 3.0.2/3.5.0 and 2.5, the virtual machines are maintained in `.vmdk` and –flat.vmdk files. These files are placed in the same location as the configuration files in case of ESX server 3.0.2/3.5.0. But for ESX 2.x the location for virtual disk files is `“/<vmfs_mountpoint>/ “`.

Note: For ESX 2.1.x the name conventions for virtual disk file is VM_diskname>.dsk.

Creating the filesystem backup specification

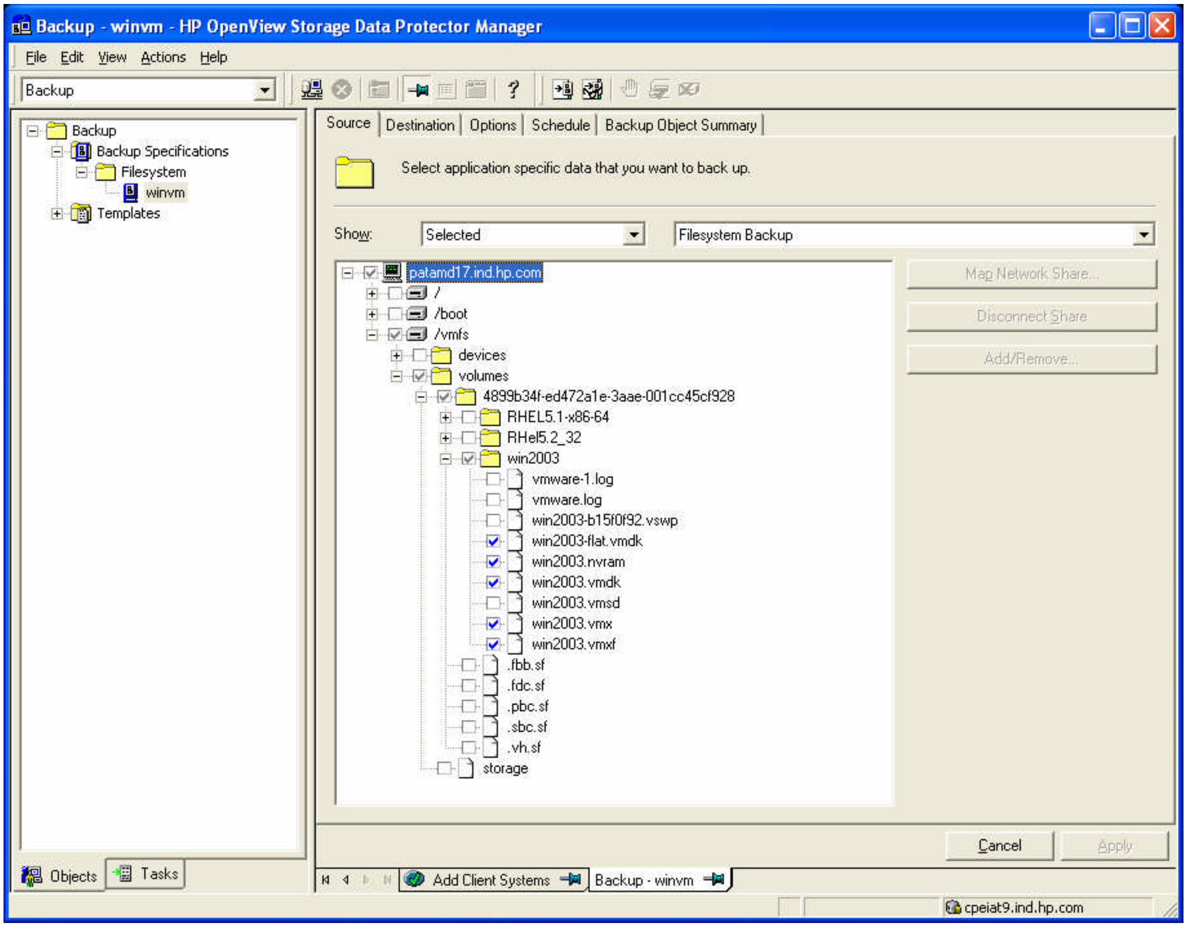
This section is described differently for ESX 2.x and 3.0.2/3.5.0.

For ESX 3.0.2/3.5.0 please follow the below procedure:-

On the selected VMware ESX Server which is DP client, select the configuration data for the Virtual Machine to be backed up. Select the `/vmfs/volumes/<UU-id>/virtual –machine/virtualmachine.vmx` and `/vmfs/volumes/<UU-id>/virtual machine /virtual machine.vmxf` which stores the configuration file for the selected virtual machine.

Select `/vmfs/volumes/<UU-id>/virtual machine /virtual machine .vmdk` which stores configuration information of virtual disk information along with `/vmfs/volumes/<UU-id>/virtual machine /virtual machine-flat .vmdk` which contains the virtual machine and `/vmfs/volumes/<UU-id>/virtual machine/virtualmachine.nvram` which contains BIOS information about the virtual machine. These files are selected via the Data Protector Backup Window GUI.

Example: As seen in figure 4, the “win2003” virtual machine runs on Windows 2003 platform. When backing up this virtual machine which is owned by user root from the “patamd17.ind.hp.com” VMware ESX Server, the corresponding configuration file, virtual disk file, BIOS information file of the virtual machine are selected for backup:



Select application specific data that you want to back up.

Show: Selected | Filesystem Backup

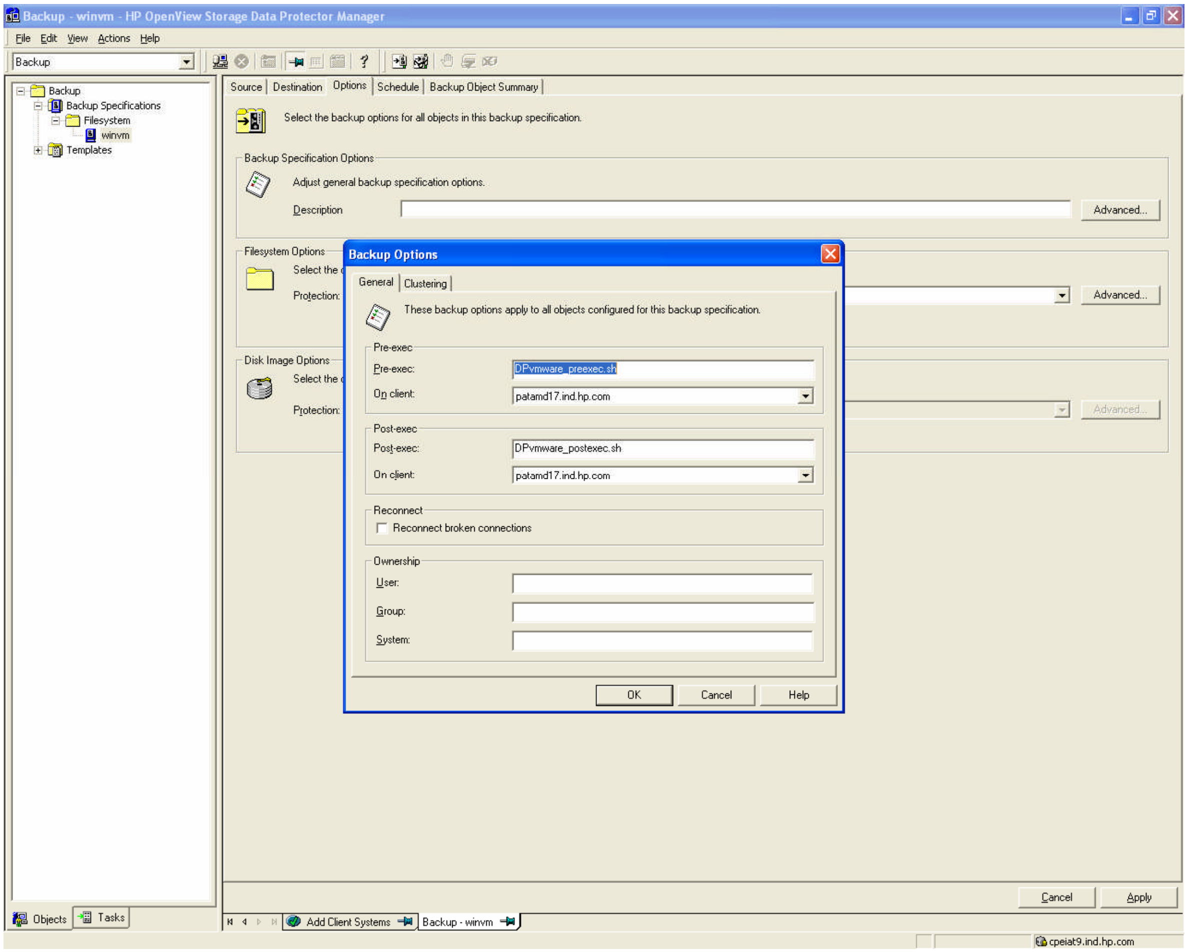
- ☑ patamd17.ind.hp.com
  - □ /
  - □ /boot
  - ☑ /vmfs
    - □ devices
    - ☑ volumes
      - ☑ 4899b34f-ed472a1e-3aae-001cc45cf928
        - □ RHEL5.1-x86-64
        - □ RHel5.2_32
        - ☑ win2003
          - □ vmware-1.log
          - □ vmware.log
          - □ win2003-b15f0f92.vswp
          - ☑ win2003-flat.vmdk
          - ☑ win2003.nvram
          - ☑ win2003.vmdk
          - □ win2003.vmsd
          - ☑ win2003.vmx
          - ☑ win2003.vmxf
        - □ .fbb.sf
        - □ .fdc.sf
        - □ .pbc.sf
        - □ .sbc.sf
        - □ .vh.sf
      - □ storage

Figure 4

After selecting the desired device to be used for backup, apply the pre-exec and post-exec script in the “Backup Specification Options”.

The supplied integration scripts should already be present in the appropriate locations `/usr/omni/bin` locations incase of Data Protector 5.5 `/opt/omni/lbin` incase if Data Protector 6.0 of the VMware ESX Server host. Select the `DPvmware_preexec.sh` as the pre-exec script and the `DPvmware_postexec.sh` as the post-exec script. And select the ESX server for the client tab.

Example: Figure 5 shows the pre-exec and post-exec script configuration for the VMware ESX Server named “`patamd17.ind.hp.com`”



Select the backup options for all objects in this backup specification.

Adjust general backup specification options.

These backup options apply to all objects configured for this backup specification.

Pre-exec: DPvmware_preexec.sh

On client: patamd17.ind.hp.com

Post-exec: DPvmware_postexec.sh

On client: patamd17.ind.hp.com

□ Reconnect broken connections

Figure 5

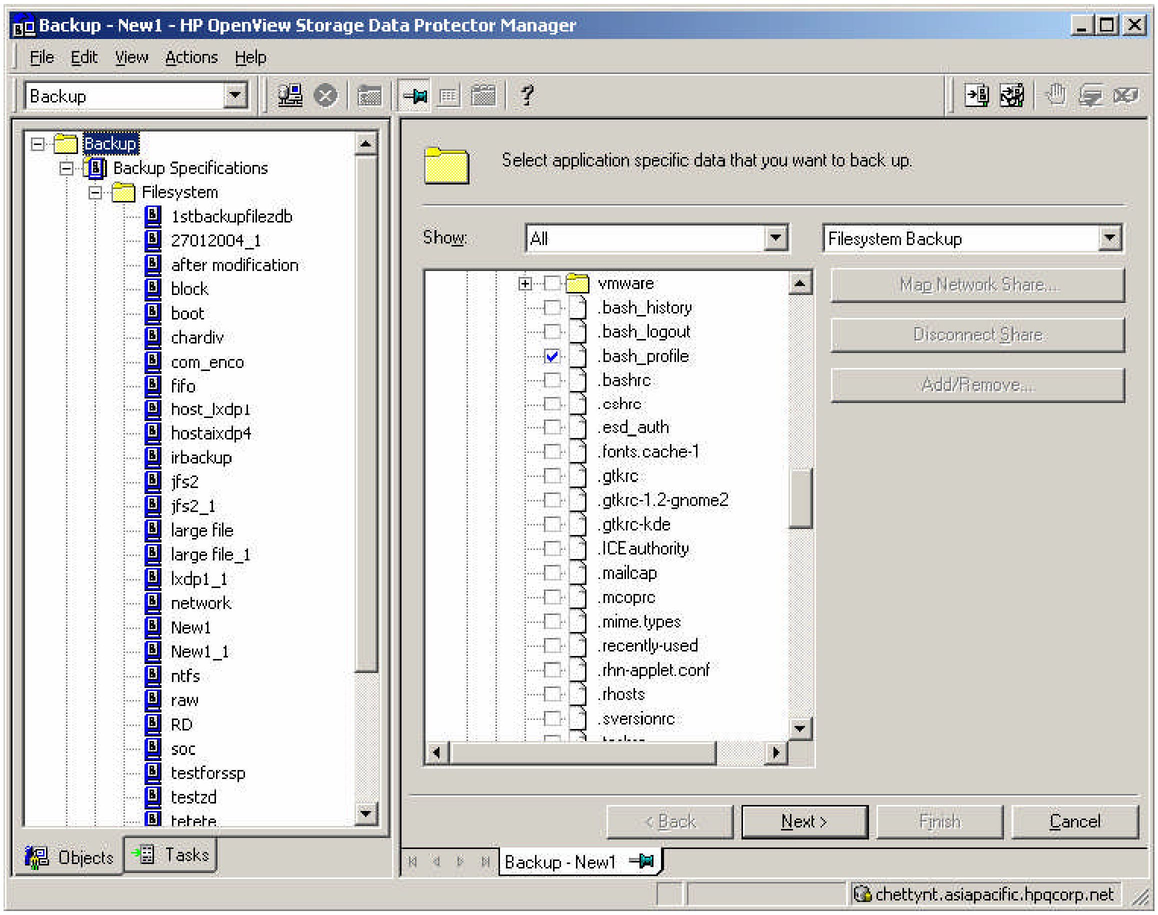
For ESX 2.X, Please follow the below procedure:-

On the selected VMware ESX Server client select the configuration data for the Virtual Machine to be backed up. Select the `/<username>/.vmware` location and the `/<username>/vmware/<platform>` location which stores the configuration file for the selected virtual machine.

Example: As seen in figure 6, the "W2k" virtual machine runs on Windows 2000 platform. When backing up the virtual machine named "W2k" owned by user root from the "`lxdp6.india.hp.com`" VMware ESX Server with the corresponding "`/root/vmware/win2000/win2000.vmx`" configuration file, the following configuration data is selected for backup:

`/root/.vmware`

`/root/vmware/win2000`



Select application specific data that you want to back up.

Show: All

Filesystem Backup

☑ .bash_profile

Figure 6

After selecting the desired device to be used for backup, apply the pre-exec and post-exec script in the “Backup Specification Options”.

The supplied integration scripts should already be present in the `/usr/omni/bin` location of the VMware ESX Server host. Select the `DPvmware_preexec.sh` as the pre-exec script and the `DPvmware_postexec.sh` as the post-exec script. And select the ESX server for the client tab.

Example: Figure 5 shows the pre-exec and post-exec script configuration for the VMware ESX Server named “`patamd17.ind.hp.com`”

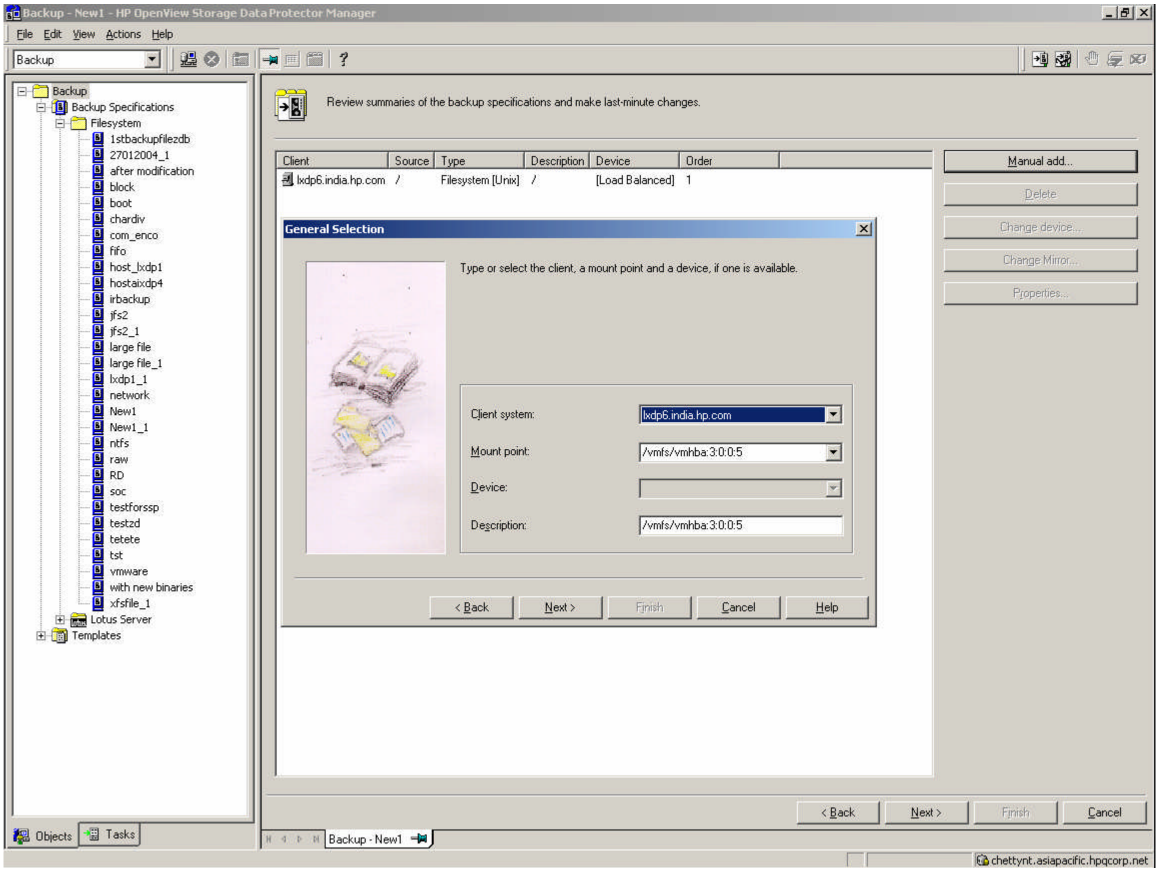
Under “Manual add” add the file representing the VM’s virtual disk. For this, click “`Manual Add`” -> “UNIX filesystem” and add the data corresponding to the file representing the virtual disk of your virtual machine. The virtual disk’s file is located on the vmfs filesystem on your VMware ESX Server and is represented as `/<vmfs_mountpoint>/<VM_diskname>.dsk` in case of ESX 2.1.x and `/<vmfs_mountpoint>/<VM_diskname>.vmdk` in case of ESX 2.5.x.

Example: `my_vmfs:test.dsk` is identified as the virtual disk for W2k VM. It means that the file representing the virtual disk is named `test.dsk` and located on the `/vmfs/my_vmfs` location. /vmfs is the default location where the vmfs filesystems created on the VMware ESX Server are mounted.

`/my_vmfs` is the soft link to the vmfs filesystem of the SCSI disk used for storing the virtual machine's virtual disks. On the Server Console execute the "`vdf`" ("`df`" with VMware ESX Server 2.x) command to get the mount point to the configured vmfs filesystem on the SCSI disk. Use this mount point as the full path to the virtual machine's virtual disk.

```
# df

Filesystem 1k-blocks Used Available Use% Mounted on

/dev/hda2 1510060 684884 748468 48% /

/dev/hda1 46636 9653 34575 22% /boot

none 63564 0 63564 0% /dev/shm

vmhba0:0:0:2 02400000 0 102400000 0% /vmfs

vmhba0:0:0:2 8896512 8842240 54272 100% /vmfs/vmhba0:0:0:2
```

The virtual machine's virtual disk is located on the /vmfs/vmhba0:0:02 mount point.



Review summaries of the backup specifications and make last-minute changes.

Client	Source	Type	Description	Device	Order
lxdp6.india.hp.com	/	Filesystem [Unix]	/	[Load Balanced]	1

Type or select the client, a mount point and a device, if one is available.

Client system: lxdp6.india.hp.com

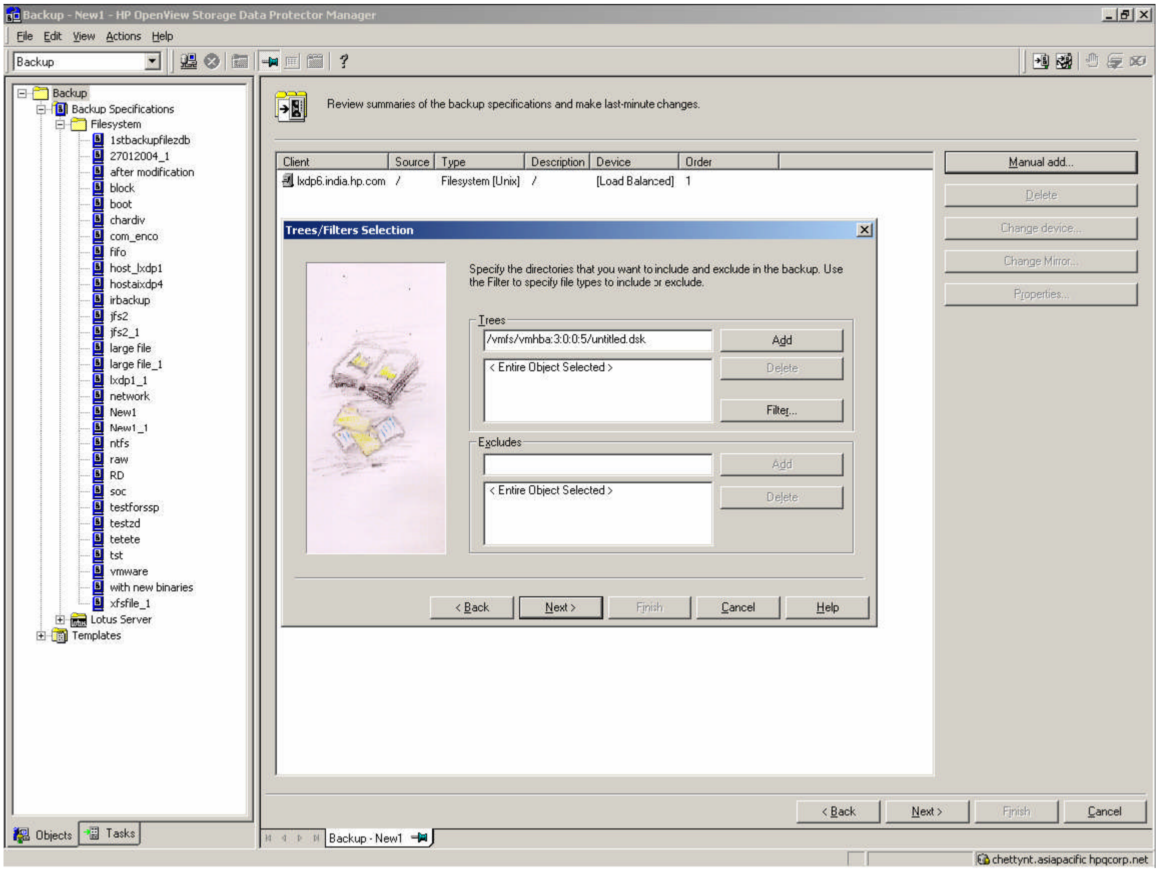
Mount point: /vmfs/vmhba:3:0:0:5

Device:

Description: /vmfs/vmhba:3:0:0:5

Figure 7

The client's name and the location of the virtual disk's filename are added as shown in Figure 7. By clicking next apply the full path to the virtual disk's file.



Backup - New1 - HP OpenView Storage Data Protector Manager

Review summaries of the backup specifications and make last-minute changes.

Client	Source	Type	Description	Device	Order
lxdp6.india.hp.com	/	Filesystem [Unix]	/	[Load Balanced]	1

Trees/Filters Selection

Specify the directories that you want to include and exclude in the backup. Use the Filter to specify file types to include or exclude.

Trees: /vmfs/vmhba:3:0:0:5/untitled.dsk

< Entire Object Selected >

Excludes:

< Entire Object Selected >

Figure 8

Enter the path `/vmfs/vmhba0:0:0:2/test.dsk`, which is the full path to the virtual disk's file and click "Add" to add the path in the list and then click "Next" as shown in Figure 8.

After completing the backup specification a new datalist appears on the Cell Manager at the location '`/etc/opt/omni/server/datalists`' in case of Unix Cell Manager or '`<Data Protector Home>\Config\Server\Datalists`' in case of Windows Cell Manager.

Typical Data Protector Datalist looks like following:

```
DATALIST "vmware-test"
DYNAMIC 1 5
PREEXEC "DPvmware_preexec.sh" -on_host lxdp6.india.hp.com
POSTEXEC "DPvmware_postexec.sh" -on_host lxdp6.india.hp.com
DEFAULTS
{
   FILESYSTEM
   {
   }
   RAWDISK
   {
   }
}
DEVICE "HP:Ultrium 1-SCSI_1_metla"
{
}
FILESYSTEM "/" lxdp6.india.hp.com:"/"
{
-trees
"/root/vmware/win2000"
"/root/.vmware"
}
FILESYSTEM "/vmfs/vmhba0:0:0:2" lxdp6.india.hp.com:"/vmfs/vmhba0:0:0:2"
{
-trees
"/vmfs/vmhba0:0:0:2/test.dsk"
}
```

Note: In ESX 2.5.x, the virtual disk's file name is changed to <VM_diskname>.vmdk, hence the last section of the datalist would look like:

```
FILESYSTEM "/vmfs/vmhba0:0:0:2" lxdp6.india.hp.com:"/vmfs/vmhba0:0:0:2"
{
-trees
"/vmfs/vmhba0:0:0:2/test.vmdk"
}
```

Updating the script on the backed up client

The supplied `DPvmware_config.sh` contains the information of which virtual machine should be put in suspended mode or snapshots of which virtual machine is to be taken. This file should already be present in /usr/omni/bin for Data Protector 5.5 or in `/etc/opt/omni/client` for Data Protector 6.0 of the ESX Server host.

The template `DPvmware_config.sh` script file looks like following:

```
      #SUSPEND_ALL_VMS="YES"
      #VMS_TO_SUSPEND="<vm-cfg-path1>.vmx,< vm-cfg-path4>.vmx"
      VMS_TO_SUSPEND=""
      #PUT_ALL_VMS_IN_HOT_MODE="YES"
      #VMS_IN_HOT_MODE="< vm-cfg-path2>.vmx,< vm-cfg-path3>.vmx"
      VMS_IN_HOT_MODE=""
```

The preceding template can be modified in following ways:

- In the VMS_TO_SUSPEND list, add the configuration file names of the virtual machines from the current VMware ESX Server to be suspended during the backup session. If there are no virtual machines for selection, then leave the list empty with an empty zero length string (for example, `VMS_TO_SUSPEND="")`.
- In the `VMS_IN_HOT_MODE` list, add the configuration file names of the virtual machines from the current VMware ESX Server that is to be put in hot mode during the backup session. If there are no virtual machines for selection, then leave the list empty with an empty zero length string (for example, `VMS_IN_HOT_MODE ="")`.
- If backup specification is configured in a way that all the virtual machines from the current VMware ESX Server are being backed up and they are to be suspended during the backup, then uncomment the line `SUSPEND_ALL_VMS="YES"` and comment all other lines.
- If backup specification is configured in the way that all the virtual machines from the current VMware ESX Server are being backed up and they are to be put in hot mode during the backup, then uncomment the line `PUT_ALL_VMS_IN_HOT_MODE ="YES"` and comment all other lines.

Notes

- Multiple values in the `VMS_TO_SUSPEND, VMS_IN_HOT_MODE` fields should be separated by a comma (","). This implies one limitation that the virtual machine name should not contain a comma or a double quote.
- For ESX Server 3.x, the user can either use the configuration file names or virtual machines' names in these variables. For the purpose of simplicity, use of the actual names of virtual machines is recommended. This white paper also uses the names of the virtual machines for, ESX server 3.x, instead of the configuration file names in the following examples.
- If the same virtual machine appears in the `VMS_TO_SUSPEND` and `VMS_IN_HOT_MODE` fields, then it is backed up in suspended mode. No snapshot mode backup is performed for such virtual machine.
- For snapshot backup, be sure that all the snapshots taken are committed to the virtual machine before starting the backup. If not, Data Protector will commit all the snapshots and proceed to the backup.
- `SUSPEND_ALL_VMS="YES`" and `PUT_ALL_VMS_IN_HOT_MODE="YES`" cannot be uncommented simultaneously. In such case, backup will not proceed.
- If the `DPvmware_postexec.sh` script fails to resume or commit the virtual machine for any reasons, it is possible to re-run `DPvmware_postexec.sh` manually.

Following are the examples of various backup options (suspended or hot mode).

The configuration file of the "rhel5" VM is identified as "`/vmfs/volumes/4574f99c-113aab61-e897-0017a44bc283/rhel5/rhel5.vmx`" or the display name (this option is applicable only for ESX Server 3.0.2/3.5.0) can be used for specifying the VM in DPvmware_config.sh.

Example 1: To put the “rhel5” VM in suspended mode during backup, update the `DPvmware_config.sh script` in the following way:

```
#SUSPEND_ALL_VMS="YES"

#VMS_TO_SUSPEND="< vm-cfg-path1>.vmx,< vm-cfg-path4>.vmx"

VMS_TO_SUSPEND="/vmfs/volumes/4574f99c-113aab61-e897-
0017a44bc283/rhel5/rhel5.vmx”

#PUT_ALL_VMS_IN_HOT_MODE="YES"

#VMS_IN_HOT_MODE="< vm-cfg-path2>.vmx,< vm-cfg-path3>.vmx"

VMS_IN_HOT_MODE=""
```

Or the same thing can be specified using display name (in this case “rhel5”)

```
VMS_TO_SUSPEND="rhel5”
```

Example 2: To put the “rhel5” VM in Hot mode during backup, update `DPvmware_config.sh` script in the following way:

```
#SUSPEND_ALL_VMS="YES"

#VMS_TO_SUSPEND="< vm-cfg-path1>.vmx,< vm-cfg-path4>.vmx"

VMS_TO_SUSPEND="”

#PUT_ALL_VMS_IN_HOT_MODE="YES"

#VMS_IN_HOT_MODE="< vm-cfg-path2>.vmx,< vm-cfg-path3>.vmx"

VMS_IN_HOT_MODE="/vmfs/volumes/4574f99c-113aab61-e897-
0017a44bc283/rhel5/rhel5.vmx”
```

Or the same thing can be specified using display name.

```
VMS_IN_HOT_MODE="rhel5”
```

Example 3: To suspend the first VM and put the second VM in hot mode during the backup, then the `DPvmware_config.sh` script is updated like this:

```
#SUSPEND_ALL_VMS="YES"

#VMS_TO_SUSPEND="< vm-cfg-path1>.vmx,< vm-cfg-path4>.vmx"

VMS_TO_SUSPEND="/vmfs/volumes/4574f99c-113aab61-e897-
0017a44bc283/rhel5/rhel5.vmx "

#PUT_ALL_VMS_IN_HOT_MODE="YES"

#VMS_IN_HOT_MODE="< vm-cfg-path2>.vmx,< vm-cfg-path3>.vmx"

VMS_IN_HOT_MODE="/vmfs/volumes/4574f99c-113aab61-e897-
0017a44bc283/sles10/sles10.vmx”
```

Sles10 is the second VM in the ESX server.

Example 4: To put two VMs in hot mode during the backup, then the `DPvmware_config.sh` script is updated like this using display names:

```
#SUSPEND_ALL_VMS="YES"
#VMS_TO_SUSPEND="< vm-cfg-path1>.vmx,< vm-cfg-path4>.vmx"
#VMS_TO_SUSPEND=" "
#PUT_ALL_VMS_IN_HOT_MODE="YES"
#VMS_IN_HOT_MODE="< vm-cfg-path2>.vmx,< vm-cfg-path3>.vmx"
VMS_IN_HOT_MODE="sles10,rhel5”
```

Supposing sles10 is the second VM in the ESX server. Specify the VMs separated by comma (,). Don't leave any spaces before and after the comma while specifying. Follow the same procedure to put multiple VMs in Suspended mode.

Example 5: To put all the VMs in hot mode during the backup uncomment the `PUT_ALL_VMS_IN_HOT_MODE="YES”` line in `the DPvmware_config.sh` script like this:

```
#SUSPEND_ALL_VMS="YES"
#VMS_TO_SUSPEND="< vm-cfg-path1>.vmx,< vm-cfg-path4>.vmx"
VMS_TO_SUSPEND=""
PUT_ALL_VMS_IN_HOT_MODE="YES"
#VMS_IN_HOT_MODE="< vm-cfg-path2>.vmx,< vm-cfg-path3>.vmx"
VMS_IN_HOT_MODE=""
```

To suspend all the VMs uncomment `SUSPEND_ALL_VMS="YES"`

NOTE: Before starting the backup session the user must make sure that all the backed up VMs from the backup specification are properly configured with their VM's configuration files in the DPvmware_config.sh script.

In case of VMware ESX 2.x, if the VM is put in hot mode, a snapshot of the VM is created and the changes are logged in the `<vmfs_mountpoint>/<VM_diskname>.dsk.REDO` file. This file is not backed up but is used for committing the changes when the VM is committed by the `DPvmware_postexec.sh` script. A VM can be put in hot mode when its virtual disk is configured in persistent, undoable or append mode.

The VMware Perl API commit command uses the following argument in our `DPvmware_commitop.pl` script:

```
$vm->commit($disk, 0, 0, 1);
```

It means that:

- This call commits a redo log file to a virtual disk while the virtual machines are running.
- `$disk` is the specified SCSI disk in the virtual machine configuration, such as scsi0:0. This disk must be an ESX Server virtual disk stored on VMFS.
- The topmost redo log file is committed.
- Virtual machine is not frozen while the redo log file is committed, though it will execute more slowly.
- The Perl call does not return until the commit has completed.

Procedure for Restore

The restore of the virtual machines is a common filesystem restore. Using the snapshot capabilities of the VMware ESX Server the entire virtual machine is backed up during the backup session, so the entire virtual machine is restored to a point in time during the restore session. The virtual machine must be powered off during the restore session.

Select for restore the same VM's data as selected for backup:

For ESX server 3.0.2/3.5.0:-

1. Virtual machine's configuration data:
   `/vmfs/volumes/<UU-id>/virtual machine/virtualmachine.vmx`
   `/vmfs/volumes/<UU-id>/virtual machine /virtual machine.vmxf`

2. Virtual machine's virtual disk's file:
   `/vmfs/volumes/<UU-id>/virtual machine/virtualmachine.vmdk`
   `/vmfs/volumes/<UU-id>/virtual machine/virtualmachine-flat.vmdk`

3. virtual machine BIOS configuration file:
   `/vmfs/volumes/<UU-id>/virtual machine/virtualmachine.nvram`

For ESX Server 2.x:-

1. Virtual machine's configuration data:
   - `“/<username>/.vmware” location`
   - `“/<username>/vmware/<platform>” location`

2. Virtual machine's virtual disk's file:
   - `In ESX 2.1.x - “/<vmfs_mountpoint>/<VM_diskname>.dsk” or`
   - `In ESX 2.5.x - “/<vmfs_mountpoint>/<VM_diskname>.vmdk”`

As the entire virtual machine is restored to a point in time, the “Destination -> File Conflict Handling” restore option must be set to “Overwrite”.

Please note that the virtual machine must be powered off during restore of entire virtual machine to a point in time.

Using Data Protector Agents to backup / restore Virtual Machines as DP clients

Data Protector Agents can be used to backup and restore the virtual machines as independent Data Protector Clients. The VMs have independent host names and IP addresses; hence the Data Protector Agents can be installed in the VM as one would install them in a normal system.

Even a Data Protector Cell Server can be installed on a virtual machine, but it is not recommended as it will not be accessible if the virtual machine is suspended.

Data protector can also backup the applications installed in a virtual machine, treating the virtual machines as normal DP client, provided the application and operating system combination is supported by Data Protector. For detailed installation procedure of installing and using Data Protector, please refer to the “HP OpenView Storage Data Protector Installation and Licensing Guide”.

Example: An ESX server is running two virtual machines, one Windows 2000 virtual machine and one Linux virtual machine. Oracle database is running on the Linux VM. In such case, the user can install Data Protector 5.50 Cell Manager on the Windows VM, and backup the Oracle data running on Linux VM.

Limitations

Following are the limitations of this solution:

- After creating or modifying the Data Protector backup specification, the user must update the provided configuration script in order to reflect the correct virtual machine's data in the configuration script as explained in section "Upgrading the script on the backed up client".
- Using the snapshot capabilities the entire virtual machine is backed up during the backup session and restored during the restore session.
- Individual files can not be restored if only a backup of entire virtual disk is available.
- During Hot mode backup the existing snapshots are also committed if there are any.

Troubleshooting

Following are typical troubleshooting scenarios and their solutions. For ESX server 3.0.2/3.5.0, you can look up into the log file created in the /tmp directory, for the preexec and postexec script failure. The naming notation for logs is same as that of Data protector debug logs and these logs will have "vmware_debug" keyword embedded in the file name.

Backup getting aborted with error message

Problem: During the Data Protector backup/restore session of VMware Virtual machine the following error is reported in the session report:

```
[Critical] From: VBDA@<hostname> "/vmfs/volumes/UU-ID/ VM/VM.vmx" Time:
dd-mm-yyyy   hh:mm:ss [81:52] /vmfs/volumes/UU-ID/ VM/VM.vmx Not a valid
mount point => aborting.
```

Solution: Using the "df" command check if the mentioned VMFS file system is mounted on the Service Console. If it's not listed in the "df" output then:

Execute `the DPvmware_setup` script with "–mount" option.

Output of "df" and "vdf" is different

Problem: If both df and vdf show the mount point as `/vmfs/volumes/<UU-id>` then the configuration is done but If the output of '`df`' and '`vdf`' is as shown below, wherein vdf shows the mount point `/vmfs/volumes/<UU-id>` and df doesn't show `/vmfs/volumes/<UU-id>`

```
[root@patamd17 home]# df
Filesystem          1K-blocks      Used           Available      Use%          Mounted on
/dev/cciss/c0d0p2   35270540       30049352       3429540        90%           /
/dev/cciss/c0d0p1   101089         32364          63506          34%           /boot
none                134156         0              134156         0%            /dev/shm
/dev/cciss/c0d0p6   2008108        56464          1849636        3%            /var/log

 [root@patamd17 home]# vdf
Filesystem                1K-blocks     Used          Available     Use%          Mounted on
```

```
/dev/cciss/c0d0p2         35270540      30049352      3429540       90%          /
/dev/cciss/c0d0p1         101089        32364         63506         34%          /boot
none                      134156        0             134156        0%           /dev/shm
/dev/cciss/c0d0p6         2008108       56464         1849636       3%           /var/log
/vmfs/volumes/4574f99c-
113aab61-e897-
0017a44bc283
                          128000000     0             128000000     0%           /vmfs
```

Solution: Execute the `DPvmware_setup` script with "–mount" option.

Warning during the snapshot mode backup

While taking a snapshot backup, the user may encounter a warning.

```
[Warning] From: VBDA@Hostname "/vmfs" Time: dd-mm-yyyy hh:mm:ss
[81:80] /vmfs/volumes/<UU-id>/VM/VM-flat.vmdk
Cannot preserve time attributes: ([16] Device or resource busy).
```

Solution: The file will be backed up normally. Therefore, the user can ignore the warning.

N.B:- Many utilities, including Linux commands supplied with ESX Server Console, have issues with vmfs because of file sizes and block sizes. E.g. one cannot copy files to non-vmfs volumes

Warning during the snapshot mode backup

When ESX VM is configured with a virtual disk in independent mode option the snapshot created can not be backed up.

```
[Warning] From: VBDA@Hostname "/vmfs" Time: dd-mm-yyyy hh:mm:ss
[81:80] /vmfs/volumes/<UU-id>/VM/VM-flat.vmdk
       Cannot open: ([16] Device or resource busy) => not backed up.
```

Solution: Verify if the disk option, make sure independent mode is not set!.

How to enable inet debugs on ESX

Solution:

1: Go to /etc/xinetd.d

2: Edit the file omni

```
server_args  = inet -log /usr/omni/log/inet.log -debug 1-200 inet.txt
```

3: reload services

```
/etc/init.d/xinetd reload
```

4: restart services

```
/etc/init.d/xinetd restart
```

How to troubleshoot the ESX snapshot with CLI command

The vmware-cmd command

```
# /usr/bin/vmware-cmd -help
Usage: /usr/bin/vmware-cmd <options> <vm-cfg-path> <vm-action> <arguments>
       /usr/bin/vmware-cmd -s <options> <server-action> <arguments>

  Options:
    Connection Options:
       -H <host>       specifies an alternative host (if set, -U and -P must also be set)
       -O <port>       specifies an alternative port
       -U <username>   specifies a user
       -P <password>   specifies a password
    General Options:
       -h More detailed help.
       -q Quiet. Minimal output
       -v Verbose.

  Server Operations:
    /usr/bin/vmware-cmd -l
    /usr/bin/vmware-cmd -s register <config_file_path>
    /usr/bin/vmware-cmd -s unregister <config_file_path>
    /usr/bin/vmware-cmd -s getresource <variable>
    /usr/bin/vmware-cmd -s setresource <variable> <value>

  VM Operations:
    /usr/bin/vmware-cmd <cfg> getconnectedusers
    /usr/bin/vmware-cmd <cfg> getstate
    /usr/bin/vmware-cmd <cfg> start <powerop_mode>
    /usr/bin/vmware-cmd <cfg> stop <powerop_mode>
    /usr/bin/vmware-cmd <cfg> reset <powerop_mode>
    /usr/bin/vmware-cmd <cfg> suspend <powerop_mode>
    /usr/bin/vmware-cmd <cfg> setconfig <variable> <value>
    /usr/bin/vmware-cmd <cfg> getconfig <variable>
    /usr/bin/vmware-cmd <cfg> setguestinfo <variable> <value>
    /usr/bin/vmware-cmd <cfg> getguestinfo <variable>
    /usr/bin/vmware-cmd <cfg> getproductinfo <prodinfo>
    /usr/bin/vmware-cmd <cfg> connectdevice <device_name>
    /usr/bin/vmware-cmd <cfg> disconnectdevice <device_name>
    /usr/bin/vmware-cmd <cfg> getconfigfile
    /usr/bin/vmware-cmd <cfg> getheartbeat
    /usr/bin/vmware-cmd <cfg> gettoolslastactive
    /usr/bin/vmware-cmd <cfg> getresource <variable>
    /usr/bin/vmware-cmd <cfg> setresource <variable> <value>
    /usr/bin/vmware-cmd <cfg> hassnapshot
    /usr/bin/vmware-cmd <cfg> createsnapshot <name> <description> <quiesce> <memory>
    /usr/bin/vmware-cmd <cfg> revertsnapshot
    /usr/bin/vmware-cmd <cfg> removesnapshots
    /usr/bin/vmware-cmd <cfg> answer
```

Here is easy way using the CLI command set:

Go to /vmfs and go for a test VMware virtual machine.

In this case I use g1 as test VM. This system is running!

```
# ll

total 53478784
-rw-------    1 root    root     1073741824 Mar  5 23:01 g1-7d3208ed.vswp
-rw-------    1 root    root     53687091200 Mar 19 13:47 g1-flat.vmdk
-rw-------    1 root    root         8684 Mar 5 23:01 g1.nvram
-rw-------    1 root    root          393 Mar 19 12:56 g1.vmdk
-rw-------    1 root    root          477 Mar 19 12:56 g1.vmsd
-rw-r--r--    1 root    root         1543 Mar 19 12:56 g1.vmx
-rw-------    1 root    root          257 Mar 6 00:03 g1.vmxf
-rw-r--r--    1 root    root        22264 Mar 5 23:00 vmware-1.log
-rw-r--r--    1 root    root       388718 Mar 19 12:56 vmware.log
```

The disk is the flat file **VM-flat.vmdk**

Copy the disk with the dd command

```
/vmfs/volumes/47cf162b-d7e92284-6170-001e0b91ab56/g1
```

```
# dd if=g1-flat.vmdk of=/dev/null bs=1024k count=10
dd: opening `g1-flat.vmdk': Device or resource busy
```

As you can see here we have a failure, which is correct since the disk is in use and not yet configured as snapshot.

Create a snapshot

```
A standard command to see all VM’s is:
```

```
# /usr/bin/vmware-cmd -l
/vmfs/volumes/47cf162b-d7e92284-6170-001e0b91ab56/g1/g1.vmx
/vmfs/volumes/47cf162b-d7e92284-6170-001e0b91ab56/g2/g2.vmx
/vmfs/volumes/47cf162b-d7e92284-6170-001e0b91ab56/g3/g3.vmx

#  /usr/bin/vmware-cmd
/vmfs/volumes/47cf162b-d7e92284-6170-001e0b91ab56/g1/g1.vmx createsnapshot g1
createsnapshot(g1) = 1


# ll
total 53496320
-rw-------    1 root    root    16881664 Mar 19 13:51 g1-000001-delta.vmdk
-rw-------    1 root    root         214 Mar 19 13:51 g1-000001.vmdk
-rw-------    1 root    root    1073741824 Mar  5 23:01 g1-7d3208ed.vswp
-rw-------    1 root    root    53687091200 Mar 19 13:51 g1-flat.vmdk
-rw-------    1 root    root        8684 Mar 5 23:01 g1.nvram
-rw-------    1 root    root       18544 Mar 19 13:51 g1-Snapshot33.vmsn
-rw-------    1 root    root         393 Mar 19 12:56 g1.vmdk
-rw-------    1 root    root         424 Mar 19 13:51 g1.vmsd
-rw-r--r--    1 root    root        1550 Mar 19 13:51 g1.vmx
-rw-------    1 root    root         257 Mar 6 00:03 g1.vmxf
-rw-r--r--    1 root    root       22264 Mar 5 23:00 vmware-1.log
-rw-r--r--    1 root    root      392611 Mar 19 13:52 vmware.log
```

```
The disk has a snapshot delta.vmdk
```

Copy the snapshot

```
#  dd if=g1-flat.vmdk of=/dev/null bs=1024k count=10
10+0 records in
10+0 records out
```

```
This is only a small test of 10 megabytes, the disk is 50Gbytes in this
case.
```

Remove the snapshot

```
# /usr/bin/vmware-cmd
/vmfs/volumes/47cf162b-d7e92284-6170-001e0b91ab56/g1/g1.vmx removesnapshots
removesnapshots() = 1


# ll
total 53478784
-rw-------    1 root    root    1073741824 Mar  5 23:01 g1-7d3208ed.vswp
-rw-------    1 root    root    53687091200 Mar 19 13:52 g1-flat.vmdk
-rw-------    1 root    root        8684 Mar 5 23:01 g1.nvram
-rw-------    1 root    root         393 Mar 19 13:52 g1.vmdk
-rw-------    1 root    root         478 Mar 19 13:52 g1.vmsd
-rw-r--r--    1 root    root        1543 Mar 19 13:52 g1.vmx
-rw-------    1 root    root         257 Mar 6 00:03 g1.vmxf
-rw-r--r--    1 root    root       22264 Mar 5 23:00 vmware-1.log
-rw-r--r--    1 root    root      410422 Mar 19 13:52 vmware.log
```

NOTE: if the snapshot fails always verify the DISK OPTIONS for the VM.
We do not support the INDEPENDENT MODE for the disk.

Remove the DP agents on ESX

In case the DP setup needs to be cleaned up, the DP software can be removed with rpm

Solution:

```
/bin/rpm  -e OB2-MA-A.06.00-1
/bin/rpm  -e OB2-DA-A.06.00-1
/bin/rpm  -e OB2-CORE-A.06.00-1
```

For more information

http://www.hp.com/go/dataprotector
http://www.vmware.com

4AA1-xxxxENW, April 2008