HP Data Protector 6.1 software
VMware Integration Installation Best Practice

Guidelines for installation of the HP Data Protector VMware Integration on ESX servers

Executive summary

This white paper provides information on how to plan and install the HP Data Protector VMware Integration in different ways.

Introduction

HP Data Protector software is a backup and disaster recovery application that provides reliable data protection and high accessibility for your fast-growing business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments. Data Protector can be used in environments ranging from a single system to thousands of systems on several sites. Due to the network component concept of Data Protector, elements of the backup infrastructure can be placed in the topology according to user requirements. The numerous backup options and alternatives to setting up a backup infrastructure allow the implementation of virtually any configuration you want.

HP Data Protector enables you to perform backup to a large number of backup devices simultaneously. It supports high-end devices in very large libraries. Various backup possibilities, such as local backup, network backup, online backup, disk image backup, synthetic backup, backup with object mirroring, and built-in support for parallel data streams allow you to tune your backups to best fit your requirements.

Since HP Data Protector 6.1, a fully automated integration for backing up VMware virtual machines is available. To enable the snapshot backup feature, you need to install the VMware Integration on the ESX server. This can be done in different ways, for example, if a network is already in place or if a Data Protector UNIX Installation Server is available.

This white paper discusses the different ways for installing the Data Protector package and shows the pros and cons of each method. You can choose the method which fits your requirements.

At the end of this white paper, a troubleshooting chapter lists error messages and necessary steps for fixing these problems.

A sample HP Data Protector Cell with VMware ESX server as Data Protector Client

Figure 1 shows a Data Protector Cell in a typical ESX environment. For simplicity, only two ESX servers are shown.

- For the Snapshot and Suspend backup method, install the DP VMware Integration on the ESX Server.
- For the VCB-Image and VCB-File backup method, install the DP VMware Integration on the VCB Proxy Server.
- For restoring from Snapshot/Suspend and VCB-Image backups, install the DP/VMware integration on the ESX server.
- For restoring from VCB-File- backups, install DP VMware integration on the destination system, which is usually the Virtual Machine from which the backup was performed.
- An installation on the VMware Virtual Center Server (vCenter Server) is optional.

Note: It is recommended to install the DP VMware Integration on the vCenter Server. Data Protector contacts the vCenter Server to get a list of all VMs and its hosting ESX servers. This allows the use of VMotion without any impact on already scheduled backups.

Figure 1: Overview

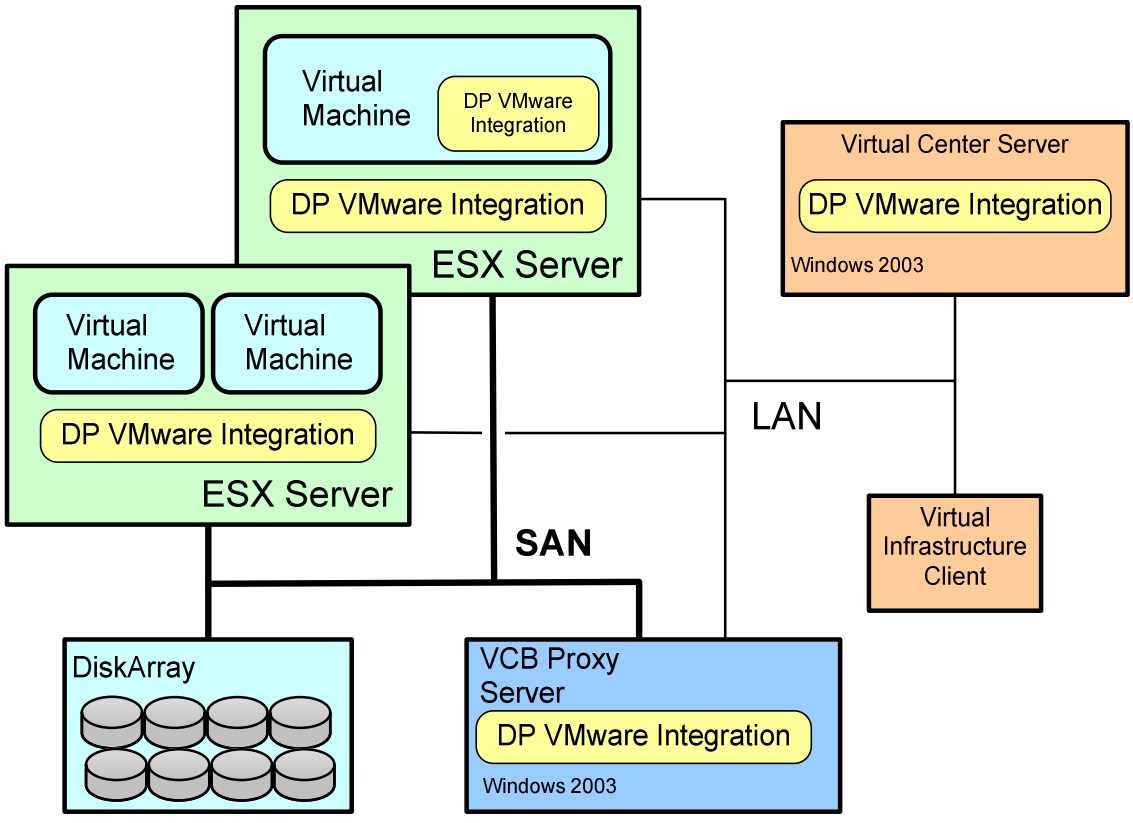


Table1 shows where the integration has to be installed for the different methods.

Table 1: Installation Targets for Data Protector VMware Integration

	Backup Method			
	Suspend	**Snapshot (on/ offline)**	**VCB Image**	**VCB file**
VMware Integration required for **backup**	on ESX Server optional: vCenter	on ESX Server optional: vCenter	on VCB Server and on ESX or vCenter	on VCB Server and on ESX or vCenter
VMware Integration required for **restore**	on ESX Server	on ESX Server	on ESX Server	on VCB Server or any Windows System

Different ways to install the HP Data Protector VMware Integration on an ESX Server

Table 2 shows the advantages and disadvantages of the different installation methods.

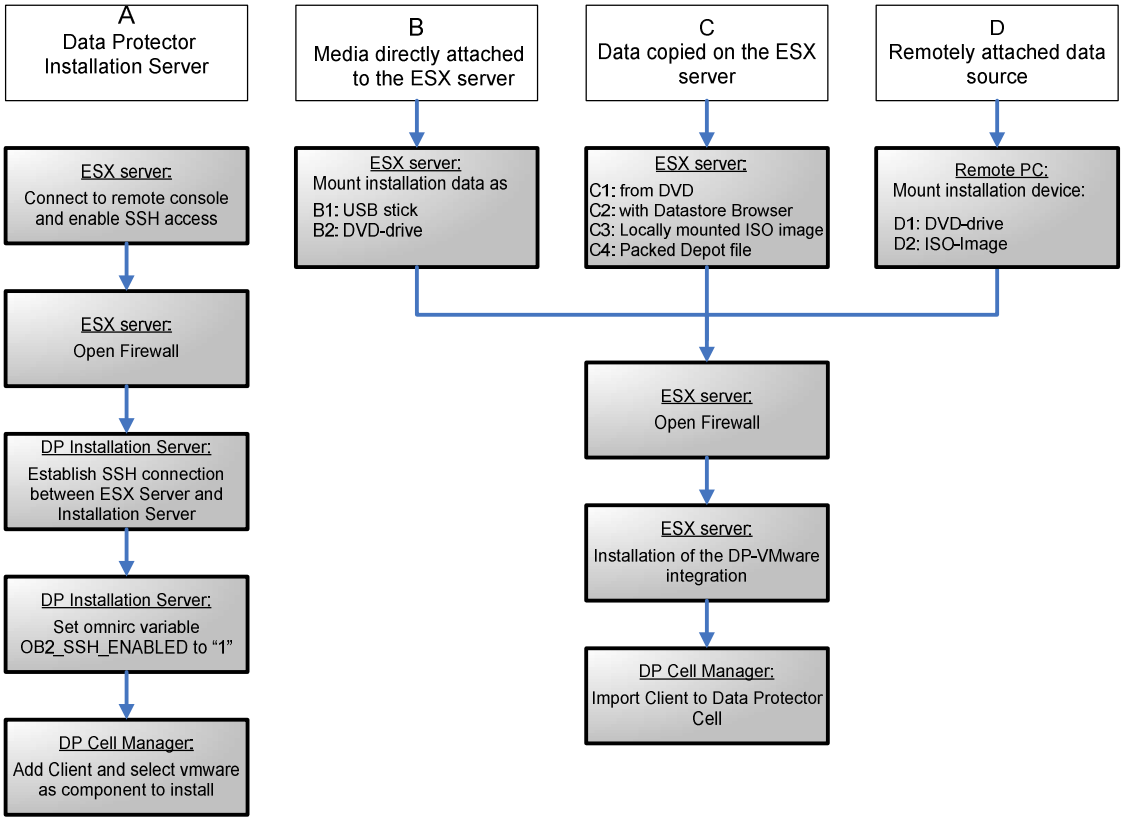
Table 2: Pros and cons of the different ways of installing the Data Protector VMware Integration

	Installation Method	Pros	Cons
A	Data Protector Installation Server	• No physical access to the ESX server necessary • Installation of multiple ESX servers in parallel • Easy maintenance (patching)	• DP UNIX Installation Server necessary • Network must be ready • Requires ssh connection
B	Media directly attached to the ESX server B1: USB stick B2: DVD-drive	• Can be done before the network has been configured • Does not require DP UNIX Installation Server • With an USB stick no local DVD drive is necessary	• Physical access to the ESX server is necesarry • No central patching possible without Installation Server
C	Data copied on the ESX server C1: from DVD C2: Datastore Browser C3: Locally mounted ISO image C4: Packed Depot file	• Does not require DP UNIX Installation Server • With an USB stick no local DVD drive is necessary	• Requires a lot of space on the ESX server • No central patching possible without Installation Server
D	Remotely attached D1: DVD-drive D2: ISO-File	• Does not require DP UNIX Installation Server • No local DVD drive needed • Enables remote installation	• Network must be ready • No central patching possible without Installation Server • Could be slow

Installation procedures flow

Figure 2 shows the required steps for the different installation methods:

Figure 2: Required steps for the different installation methods



Installation Method A – Data Protector Installation Server

Prepare the ESX Server to get access

1. You can access the ESX server either through the console or through remote access tools (such as Putty or ReflectionX). These remote access tools are based on the SSH protocol.

   By default SSH is blocked by the ESX server. To enable the login on the ESX server with SSH, see Appendix A: "Enable SSH-login on ESX Server".

2. The push-installation of the Data Protector-VMware integration requires a Data Protector UNIX Installation Server and an SSH connection between the Installation Server and the ESX server.
3. Create a public/private key pair:

   To create an SSH key pair on the Data Protector UNIX Installation Server, the command `ssh-keygen` has to be processed. Do not enter a passphrase.

   ```
   #ssh-keygen

       Generating a public/private rsa key pair.

       Please be patient... Key generation may take a few minutes
       Enter file in which to save the key (//.ssh/id_rsa):
       Created directory '//.ssh'.
       Enter passphrase (empty for no passphrase):
       Enter same passphrase again:
       Your identification has been saved in //.ssh/id_rsa.
       Your public key has been saved in //.ssh/id_rsa.pub.
       The key fingerprint is:
       33:15:17:5c:c0:83:52:76:7a:3b:13:ef:57:04:c9:6c root@server
   ```

   Explanations:

   The file `//.ssh/id_rsa` contains the private key. The default location was chosen, so it is stored in the ssh-directory of root user (`<$HOME>/.ssh`).

   `33:15:17:5c:c0:83:52:76:7a:3b:13:ef:57:04:c9:6c` is the fingerprint of the Data Protector Installation Server, server.domain.com.

4. Check the newly generated files:

   ```
   # cd /.ssh
   # ls -la
     -rw-------   1 root   sys    1679 Apr 26 14:12 id_rsa
     -rw-r--r--   1 root   sys     393 Apr 26 14:12 id_rsa.pub
   ```

5. To establish the SSH connection with the DP-client (ESX-server), append the public key to the file <$HOME>/.ssh/authorized_keys on the ESX server. This can be easily done as follows:

   Transfer the `id_rsa.pub` file to a temporary location on the ESX server:

   ```
   # scp id_rsa.pub root@esx.domain.com:.ssh/

       The authenticity of host 'esx.domain.com(16.xx.yy.zz)' can't be
       established.
       RSA key fingerprint is
              3d:d2:1b:5e:7e:56:7e:b3:4d:9c:74 :ff:0d:f4:64:b0.
       Are you sure you want to continue connecting (yes/no)? yes
       Warning: Permanently added 'esx.domain.com,16.xx.yy.zz' (RSA) to the
       list of known hosts.

       root@esx.domain.com's password:

         id_rsa.pub 100%  393  0.4KB/s  0.4KB/s  00:00  Max throughput:0.4KB/s
   ```

   Possible error messages:

   - ```
     @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
     @    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
     @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
     ```
     ```

See Troubleshooting "Man-in-the-middle attack" on page 17.

– *Error message:* `scp: .ssh/: Is a directory`

  The scp command fails because there is no .ssh directory on the ESX server.

  Solution:

  On the ESX server, login with root.

  Create a directory:

  ```
  # mkdir .ssh
  ```

  Apply the correct setting to the `.ssh` directory:

  ```
  # chmod 600 .ssh
  ```

6. Append the key manually:

   ```
   #cat id_rsa.pub >> authorized_keys
   ```

   (The file `authorized_keys` will be created if it is not already available.)

7. Make a simple test to check that the SSH connection is working. From the Data Protector Installation Server, ask the ESX server via the SSH connection for the date and time:

   ```
   # ssh esx.domain.com date
          Thu Apr 21 17:56:33 CET 2009
   ```

   Note: The remote system must not ask for a passphrase or the Data Protector installation will fail.

8. Firewall configuration.

   By default, the firewall from the ESX server blocks the port 5555. To open this port, perform the following command:

   ```
   # esxcfg-firewall –-openPort 5555,tcp,in,HP-DataProtector
   ```

   See Appendix A: "Firewall settings" for additional information.

9. Set the omnirc variable `OB2_SSH_ENABLED`.

   Before the installation can start, set the omnirc variable `OB2_SSH_ENABLED` on the Installation Server to "1".

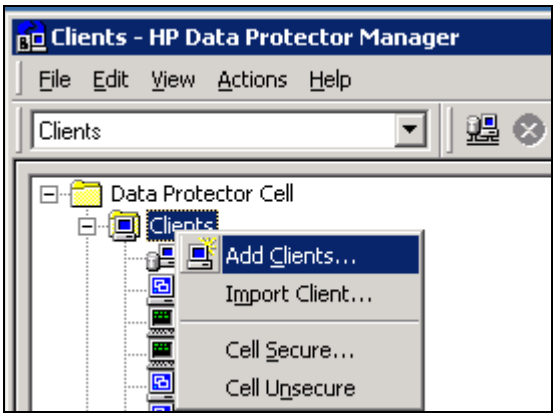
   Extract from the omnirc file:

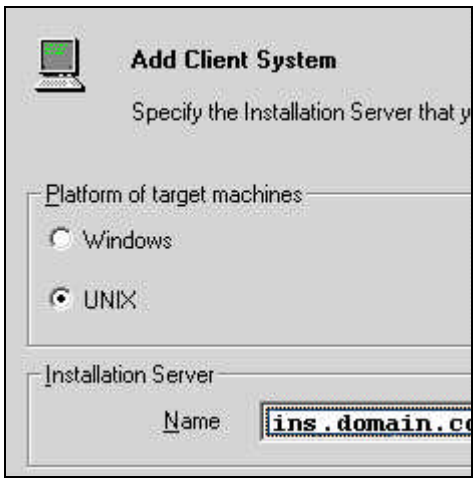
   ```
   #
   OB2_SSH_ENABLED=1
   #   Default: 0
   #   Allows SSH protocol to be used for remote installation of DP agents. This
   #   secures the remote connections while distributing the agents. Set this variable
   #   on Installation Server host. This is applicable only on UNIX platforms
   ```

   You can find the .omnirc file on HP-UX, Linux and Solaris at: `/opt/omni/.omnirc`. If there is no .omnirc file, copy the file `.omnirc.TMPL` to .omnirc.

10. Open the Data Protector GUI:

    Go to the Client context and right-click "Add client":





The platform of the target system is UNIX. When you have entered the name of the ESX server and selected the VMware Integration, the installation starts. After the installation the client is automatically added into the Data Protector Cell.

Installation Method B – Media directly attached to the ESX server

B1: Using a local DVD Drive

Prepare the ESX Server to get access

1. You can access the ESX server either through the console or through remote access tools (such as Putty or ReflectionX). These remote access tools are based on the SSH protocol.

   By default SSH is blocked by the ESX server. To enable the login on the ESX server with SSH, see Appendix A: "Enable SSH-login on ESX Server".

2. Firewall configuration.

   For Data Protector, the port 5555 needs to be open. By default, the firewall on the ESX server blocks the port. To open it, execute the following command:

   ```
   # esxcfg-firewall –-openPort 5555,tcp,in,HP-DataProtector
   ```

   See Appendix A: "Firewall settings" for more information.

3. Insert and mount the DVD: HP-UX B6960-15001.

   If the directory `/mnt/cdrom` does not exist, create it with the command:

   ```
   # mkdir /mnt/cdrom
   ```

   Then mount the drive:

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

   You can identify the DVD Drive by checking the directory listing of `/dev`:

   ```
   # ls -l /dev
   ```

4. Go to the Local Install directory on the DVD drive:

   ```
   # cd /mnt/cdrom/LOCAL_INSTALL
   ```

5. Start the installation:

   ```
   # /mnt/cdrom/LOCAL_INSTALL/ommnisetup.sh –install vmware
   ```

6. Check the installation:

   ```
   # rpm –qa | grep –i OB2
     OB2-CORE-A.06.10-1
     OB2-VMW-A.06.10-1
   ```

7. Umount the cdrom:

   ```
   # cd /
   # umount /mnt/cdrom
   ```

8. Import the ESX server as client to the Cell Manager:

   Open the Data Protector GUI, go to the context menu, right-click on clients, select **import client...**.

Note: If the port 5555 on the firewall is already open, you can combine the import step (8) with the installation step (5). Additionally the DA and the MA are installed:

```
# /mnt/cdrom/LOCAL_INSTALL/ommnisetup.sh –server cellmanager.domain.com
–install da,ma,vmware
```

where *cellmanager.domain.com* is the name of the Cell Manager.

B2: Using local USB stick

1. Copy the whole DVD onto an USB stick (can be done with a Windows PC).
2. Prepare the ESX Server to get access. See step1 of *B1: Using a local DVD drive.*
3. Firewall configuration. See step 2 of *B1: Using a local DVD drive.*
4. Insert the USB stick in an USB port fro*m the ESX server and wait a* couple of seconds.
5. Login on the ESX server and use the *fdisk* command to see the used USB-port(s). In the output below the local disk is also shown. One differentiator can be the size of the device. Here the USB stick has 16 GB and the disk 36.4 GB. In cases where many devices are listed, it may be difficult to identify the USB stick. In this case, perform the command "`fdisk –l`" *before* inserting the USB stick and the output of the command will be redirected in a file. Insert the USB stick and perform the command again. Using a command like `diff`, you can identify the USB stick.

```
# fdisk -l

   Disk /dev/sda: 16.0 GB, 16028794368 bytes
   254 heads, 63 sectors/track, 1956 cylinders
   Units = cylinders of 16002 * 512 = 8193024 bytes

   Device Boot       Start    End   Blocks     Id  System
   /dev/sda1           1      1955  15641929    c  Win95 FAT32 (LBA)

   Disk /dev/cciss/c0d0: 36.4 GB, 36414750720 bytes
   255 heads, 32 sectors/track, 8716 cylinders
   Units = cylinders of 8160 * 512 = 4177920 bytes

   Device Boot              Start       End    Blocks   Id  System
   /dev/cciss/c0d0p1   *         1        25    101984   83  Linux
   /dev/cciss/c0d0p2            26      1279   5116320   83  Linux
   /dev/cciss/c0d0p3          1280      8054  27642000   fb  Unknown
   /dev/cciss/c0d0p4          8055      8716   2700960    f  Win95 Ext'd (LBA)
   /dev/cciss/c0d0p5          8055      8190    554864   82  Linux swap
   /dev/cciss/c0d0p6          8191      8691   2044064   83  Linux
   /dev/cciss/c0d0p7          8692      8716    101984   fc  Unknown
```

6. Mount the USB device.

   Create a mount point if one is not already available:
   ```
   # mkdir /mnt/cdrom
   ```

   Now mount the USB stick:
   ```
   # mount -t auto  /dev/sda1 /mnt/usb
   ```

7. Once the USB device is mounted, follow the steps 5-8 from *B1: Using a local DVD drive.*.
8. Unmount the USB-stick:
   ```
   # cd /
   # umount /mnt/usb
   ```

Installation Method C – Data copied on the ESX Server

C1: With the DVD

1. Prepare the ESX Server to get access. See step1 of *B1: Using a local DVD drive*.
2. Firewall configuration. See step 2 of *B1: Using a local DVD drive*.
3. Mount the DVD. See step 3 of *B1: Using a local DVD drive*.
4. Copy the HP-UX and the `LOCAL INSTALL` directory on the ESX server

   ```
   # cp -r /dvdrom/platform_dir/DP_DEPOT directory
   # cp -r /dvdrom/platform_dir/LOCAL_INSTALL directory
   ```

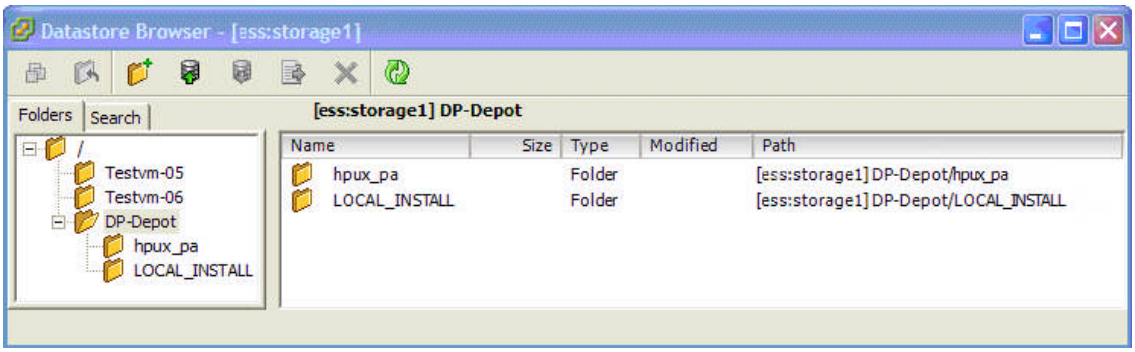
   For further details see the *HP Data Protector A.06.10 Installation and licensing guide*→ "Local installation of UNIX clients" → "Running the installation from the hard disk".

5. Proceed with the installation as described in steps 4-8 of *B1: Using a local DVD drive*.

C2: With the VMware Datastore Browser

With the VMware Infrastructure Client, every Datastore that belongs to the ESX server can be browsed. A feature of the Datastore Browser is that it allows exchange of data in both directions, between the system running the Infrastructure Client and the ESX server. You can use this to upload the Data Protector installation bits directly on the ESX server, without any UNIX command.

To install the DP VMware integration agent, it is enough to upload the hpux_pa depot and the `LOCAL_INSTALL` directory.



The directory where the data is stored is:

```
/vmfs/volumes/datastore directory
```

The procedure is identical to section C1: With the DVD, except for step 4. Note that the omnisetup.sh file may have a different location in this case, such as: </vmfs/volumes/<datastore>/LOCAL_INSTALL>.

C3: Locally mounted ISO image

Under ESX, an ISO-Image can be mounted like a CD-ROM. For this, you must place the ISO image on the ESX server.

You can copy the ISO image with the VMware Datastore browser (see *C2: Data copied on the ESX server with the VMware Datastore browser)* or with FTP.

To use FTP, open the firewall on the ESX server:

```
# esxcfg-firewall --allowOutgoing
```

then use ftp to fetch the ISO file from a remote system.

Close the firewall afterwards with:

```
# esxcfg-firewall --blockOutgoing
```

Or set the firewall back to default:

```
# esxcfg-firewall –r
```

1. Assuming that an ISO image `B6960-15003.iso` has been copied onto the ESX server in the directory `/vm/iso_depot/DP_6.10`, and a mount point such as */mnt/DP-ISO* has been created, to mount the ISO image use the command:

   ```
   # mount -o loop /vm/iso_depot/DP_6.10/B6960-15003.iso /mnt/DP-ISO
   ```

2. Proceed with the installation as described in steps 5-8 of *B1: Using a local DVD drive*

   Note: See Appendix A: "Firewall settings" for additional information about firewall configuration.

C4: Packed Depot file

To reduce the total amount of data, simply extract and compress the directories `hpux_pa` and `LOCAL_INSTALL` from the DVD.

1. Extract the resulting gzipped tarfile on the ESX server with the following command:
   ```
   # gunzip -c DP-Depot.tar.gz | tar xvf –
   ```
2. Proceed with the installation as described in steps 5-8 of *B1: Using a local DVD drive.*

Note: See Appendix A: "Firewall settings" for additional information about firewall configuration

Installation Method D — Remotely attached Data Source

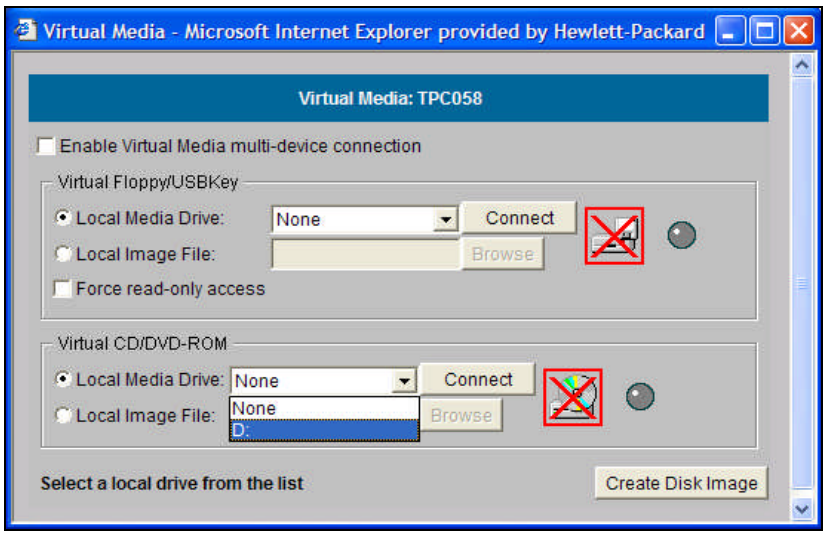
D1: Remote DVD

HP's iLO (integrated Lights Out) allows you to connecting a remote DVD-drive to the ESX server.

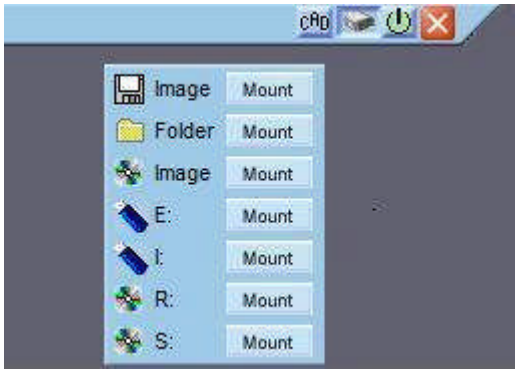
The PC or laptop from which the iLO is reached needs a DVD drive, which you can use as an installation drive for the Data Protector VMware Integration.

1. Insert the DVD in the local PC drive.
2. Connect with a web browser to the iLO from the ESX server.
   - With iLO:

     Under the tab "Virtual devices" click "Virtual Media" and select the local DVD drive.



   - With iLO2 you can mount a DVD directly using the "Integrated Remote Console". The following screen shows the top right corner of the Console window. Click on the drive symbol to open the selection menu.



3. On the console, check for drives under `/mnt`:
   ```
   # ll /mnt
   ```
4. Mount the DVD:
   ```
   # mount /dev/cdrom /mnt/cdrom1
   ```
5. Go to the `LOCAL_INSTALL` directory:
   ```
   # cd /mnt/cdrom1/LOCAL_INSTALL
   ```
6. Start the installation:
   ```
   # /mnt/cdrom1/LOCAL_INSTALL/omnisetup.sh –install vmware
   ```

7. Unmount the DVD:
```
# cd /
# umount /mnt/cdrom1
```
8. Check the installation. See step 6 of *B1: Using a local DVD drive.*
9. Firewall configuration. See step 2 of *B1: Using a local DVD drive.*
10. Import the ESX server as client to the Cell Manager. See step 8 of *B1: Using a local DVD drive.*

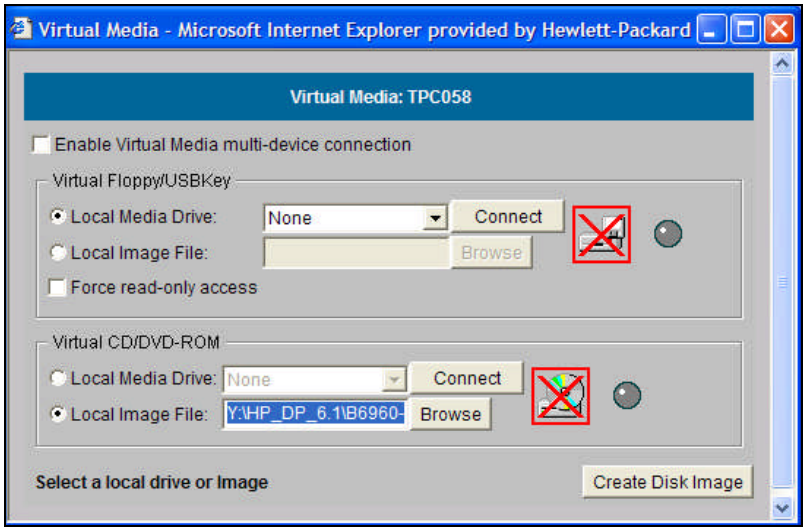
D2: Remote ISO-image

HP's iLO and iLO2 not only allow you to connect a DVD drive from the local PC, you can also mount a directory that holds an ISO image. This directory need not be a directory on the PC, it could be a mapped network drive. This means the installation runs directly from a foreign ISO-store onto the ESX server. There is no need to copy any data first. Note that the network can slow down the installation process.

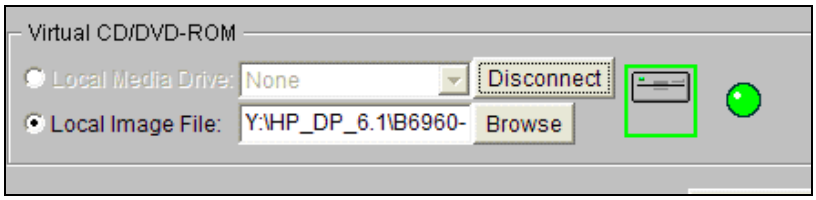
The procedure is similar to *D1: Remote DVD, b*ut instead of a local Media Drive, select a local ISO image file. There are two possible sources: an ISO image created from the DVD B6960-15001, and the ISO image `B6960-15003.iso` which you can download from the web. See *Appendix A: "*DVDs and downloadable bits".

- With iLO:

  Click "Connect".



  If the connection works properly, the drive logo becomes green.



  The mount and installations steps are similar to *D1: LOCAL DVD*

- With iLO2 using the "Integrated Remote Console" you can mount an ISO image directly from a directory. The following screen shows the top right corner of the Console window. Click on the drive symbol to open the selection menu. For example, click **Mount** next to a folder symbol to browse the local system and select an ISO image.

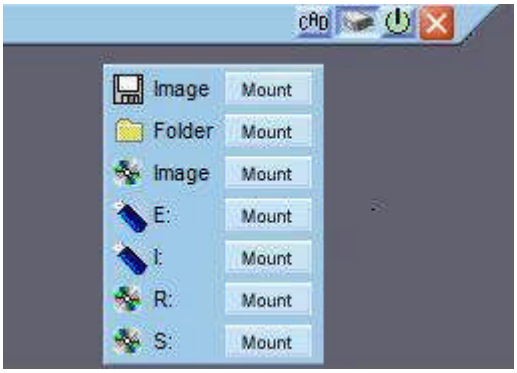


Image
Mount
Folder
Mount
Image
Mount
E:
Mount
I:
Mount
R:
Mount
S:
Mount

Troubleshooting

This section covers the following:

Problems

Problem: push installation

Push installation with the Data Protector Installation Server generates the error message:

```
[Critical] <esx.domain.com>  [110:24] Client esx.domain.com : client not responding.
[Critical] <esx.domain.com>  Error connecting to client esx.domain.com
   Skipping client!
```

Possible reason

The omnirc variable OB2_SSH_ENABLED is not set to "1".

Problem: error message: "No medium found"

During local installation, using a local DVD drive, the following error message occurs during the mount step of the DVD:

```
Mount: block device /dev/cdrom is write-protected, mounting read-only
Mount: No medium found
```

Action

To check for a DVD drive:

```
      # dmesg | grep –i dvd
  cdrom_read_toc: Model string: "HL-DT-STCD-RW/DVD DRIVE GCC-C10N
```

To check for a CD drive:

```
     # dmesg | grep –i cd
hda: CRN-8245B, ATAPI CD/DVD-ROM drive
hda: attached ide-cdrom driver
hda: ATAPI 24X CD-ROM drive, 128kB Cache
Uniform CD-ROM driver Revision: 3.12
```

The message text shows that this is not a DVD-drive.

Possible solutions

- Exchange the CD drive with a DVD-drive.
- Use a USB stick instead of a DVD.
- If ILO is available, mount the DVD remotely.
- Install remotely with the Data Protector Installation Server.

Problem: scp does not work or man-in-the-middle attack

Action

If an ESX server has been reinstalled, the system will have a new fingerprint. The scp command checks the fingerprints that are stored in the file /.ssh/known_hosts on the Installation Server. To delete the old entry, search for the host name and IP address in the known_host file. If the content is encrypted check the line given in the message below.

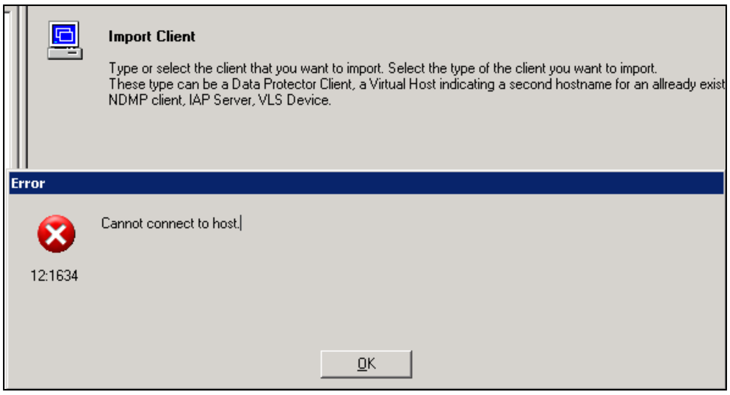
```
"Offending key in /.ssh/known_hosts:3"
```

```
# scp id_rsa.pub root@esx.domain.com:.ssh/
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
d0:3f:56:3f:9e:92:8c:20:fa:b9:02:ce:75:b9:bf:b6.
Please contact your system administrator.
Add correct host key in /.ssh/known_hosts to get rid of this message.
Offending key in /.ssh/known_hosts:3
RSA host key for esx.domain.com has changed and you have requested strict
checking.
Host key verification failed.
lost connection
```

It may be that there are two entries for one host in the `known_hosts` file, one with an IP address and one with the host name.

Problem: installation works but the import of the client failed



Possible reason

The firewall blocks the 5555 port.

Action

You can open the port with the following command executed on the ESX Server:

```
# esxcfg-firewall --openPort 5555,tcp,in,HP-DataProtector
```

Problem: util_vmware does not work correctly

Error message:

```
*RETVAL1602
[111] Connection refused
```

This error message occurs because the Cell Manager could not be reached.

Action

Check the firewall setting on the ESX server and the Cell Manager.

How to enable Inet debugs on ESX

1. On the ESX host go to `/etc/xinetd.d`:
   ```
   # cd /etc/xinetd.d
   ```
2. Edit the file `omni`:
   ```
   server_args = inet -log /usr/omni/log/inet.log -debug 1-200 inet.txt
   ```
3. Reload the services:
   ```
   # /etc/init.d/xinetd reload
   ```
4. Restart the services :
   ```
   # /etc/init.d/xinetd restart
   ```

Useful troubleshooting commands

Firewall problems

To isolate network problems, it could be helpful to switch off the whole firewall on the ESX server:

```
# esxcfg-firewall --AllowOutgoing
# esxcfg-firewall --AllowIncoming
```

After the tests, switch the firewall back on:

```
# esxcfg-firewall --BlockOutgoing
# esxcfg-firewall --–BlockIncoming
```

To check the ports:

```
# esxcfg-firewall –q
```

Date and time

Date and time should be synchronized on all systems. The time on the ESX server can be quickly adjusted with the date command:

```
# date
Tue Apr 21 11:16:51 CEST 2009
```

Use the same format to change the date:

```
# date --set="Wed Apr 22 11:18:00"
Wed Apr 22 11:18:00 CEST 2009
```

To enable the ntp service, go to:
http://kb.vmware.com/selfservice/viewContent.do?language=en_US&externalId=1339

Appendix A

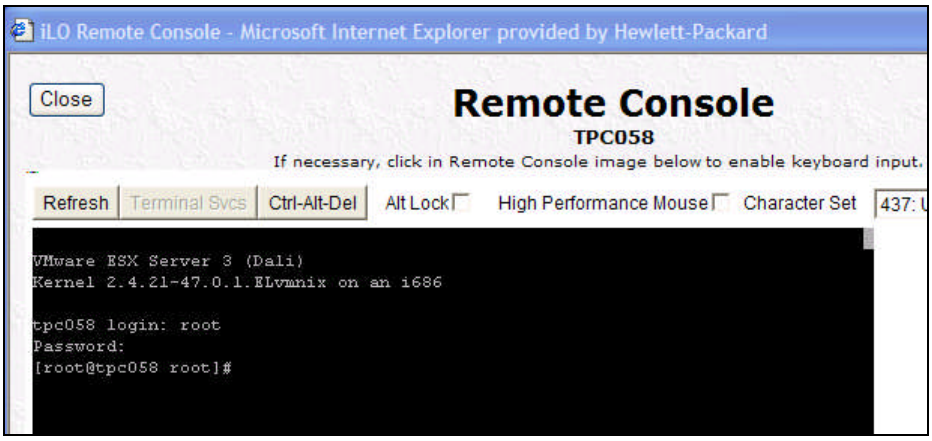
This section covers the following:

- Enabling SSH-login on an ESX Server, see below
- Firewall configuration, see page 20
- DVDs and downloadable binaries, see page 22
- For more information, see page 23

Enabling SSH-login on an ESX Server

1. Login via the console.

   To enable SSH login access, use the console. For example, with the help of the iLO Remote Console (part of the HP server):



   The password that you need to enter here was provided during the ESX installation.

2. Enable root login.

   In the file: `/etc/ssh/sshd_config`, set the parameter *PermitRootLogin* to *yes*.

   Note: Do not confuse this with the `ssh_config` file in the same directory.

3. Restart the SSH-daemon.

   To make the changes active, restart the ssh-deamon:

   ```
   # /etc/init.d/sshd restart  or  # service sshd restart
   ```

   Note: If you want to disable root login for SSH, change the file `sshd_config` back and restart the SSH daemon. However, this will block patching the ESX Server by a Data Protector Installation Server.

Firewall configuration

Data Protector uses by default only two dedicated ports: 5555 (Inet) and 5556 (Java GUI). All other ports used by Data Protector are dynamically allocated in the range of 1024 to 65535. In cases where firewalls become important, this range can be restricted to a smaller number of usable ports. The `esxcfg-firewall` command and two omnirc variables can be used to define a narrower range of ports.

It is possible to use the `esxccfg-firewall` command manually to open ports for an application. However, especially if many ESX servers have to be installed, it is preferable to create an xml file in the directory `/etc/vmware/firewall` that opens one or more ports or port ranges.

The following is an example configuration of an ESX server and a Cell Manager with open ports 5555 and 42000-42100.

Create a file, such as `DataProtector-ports`, and insert:

```
<ConfigRoot>
<service>
    <id>HP DataProtector</id>
    <rule id='0000'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <port type='dst'>5555</port>
      <flags>-m state --state NEW</flags>
    </rule>
    <rule id='0001'>
      <direction>outbound</direction>
      <protocol>tcp</protocol>
      <port type='dst'>5555</port>
      <flags>-m state --state NEW</flags>
    </rule>
    <rule id='0002'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <port type='dst'>
        <begin>42000</begin>
        <end>42100</end>
      </port>
      <flags>-m state --state NEW</flags>
    </rule>
    <rule id='0003'>
      <direction>outbound</direction>
      <protocol>tcp</protocol>
      <port type='dst'>
        <begin>42000</begin>
        <end>42100</end>
      </port>
      <flags>-m state --state NEW</flags>
    </rule>
  </service>
</ConfigRoot>
```

With the command

```
# esxcfg-firewall –e "HP DataProtector"
```

the file `DataProtector-ports.xml` is read and ESX opens the ports. "HP DataProtector" is the name given in line #3 as the service ID.

Show the configuration of the firewall:

```
# esxcfg-firewall –q
```

Check the configured ports for Data Protector on the VirtualInfrastructure Client:

Now configure Data Protector:

1. On the ESX server, set the omnirc variable OB2PORTRANGE:
   `OB2PORTRANGE=42000-42100`
2. Make the same changes on the Cell Manager
3. Restart the services on the Cell Manager with `omnisv -stop` and `omnisv -start`. This completes the configuration.

You can check the configuration of the ESX server and the ports directly from the command line on the ESX server. Foe example, to configure the ESX server in Data Protector with standard security:

```
#/opt/omni/lbin/util_vmware.exe -config -security 0 -user root -
password secret -port 443 \ -webroot /sdk
```

If the command runs successfully, a file is created on the Cell Manager under <Data_Protector_home>\config\server\Integ\Config\VMware\hostname%_OB2GLOBAL which contains the configuration and the encrypted login credential.

Note: The range of 42000–42100 with100 ports in the example above is quite large. This can be reduced to a smaller number. It is also not necessarily to start at 42000; it can be anywhere in the range 1024 to 65535. As well as the OB2PORTRANGE variable, there is OB2PORTRANGSPEC, which can be used to define dedicated port ranges for dedicated Data Protector agents.

For more information, see:

- For installation of the VMware: *HP Data Protector Integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server*
- For configuring omnirc variables: HP Data Protector online Help
- For open ports and port ranges on Data Protector:
  search the Data Protector online Help index "How to Limit a Port Range" and "About Firewall Support"
- For open port on ESX servers:
  http://pubs.vmware.com/vi35/server_config/wwhelp/wwhimpl/common/html/wwhelp.htm?context=server_config&file=sc_security_servcon.17.6.html

DVDs and downloadable binaries

DVD-set (contains 3 DVDs), product number: B6960MA

```
Windows          B6960-15000
HP-UX            B6960-15001
Solaris & Linux  B6960-15002
```

Downloadable binaries

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

→ Evaluations & Demos → Evaluation Software → HP Data Protector v6.1
Overview:

```
DVD, HP DP 6.1 for Windows          B6960-15000.tar.gz      1910.11MB
CD,  HP DP 6.1 Media Operations     B7129-15004.iso          491.92MB
ESD, HP DP 6.1 for HP-UX-PA         B6960-15003.tar.gz      1470.57MB
ESD, HP DP 6.1 for HP-UX-IA         B6960-15004.tar.gz      1515.38MB
ESD, HP DP 6.1 for Linux            B6960-15005.tar.gz      1426.89MB
ESD, HP DP 6.1 for Solaris          B6960-15006.tar.gz      1443.29MB
```

For more information

- On Data Protector: www.hp.com/go/dataprotector
- On installation: see the Data Protector online Help index: "setting up openssh"
  or see the *HP Data Protector Installation and licensing guide*, "Setting up OpenSSH"
- On SSH: see the official web page http://www.openssh.org available in multiple languages en, de, fr, ja, nl