Cisco TelePresence Conductor on Virtual Machine

Installation Guide

XC3.0

January 2015

Contents

Introduction

Cisco TelePresence Conductor (TelePresence Conductor) software supports flexible deployment options and is available as a virtualized application for VMware or similar virtual environments. This enables enterprises to run TelePresence Conductor on the 'company standard' Virtual Machine (VM) hardware platform for ease of management and deployment within an existing data center.

This deployment guide specifies:

- the VM platform requirements for TelePresence Conductor
- how to load the TelePresence Conductor .ova installation file
- how to install a VM
- how to troubleshoot the system, when there are issues

With a suitably specified VM platform, the TelePresence Conductor running on VMware will perform identically to the TelePresence Conductor running on its appliance hardware.

Using the VM .ova file for initial VM installation only

The VM TelePresence Conductor is licensed using information that is generated at the time of the .ova file installation. If the .ova was installed a second time, new licensing information would be created, and to use the new VM, new release and licence keys would need to be purchased. To upgrade a VM TelePresence Conductor, follow the procedure under Upgrading a VM TelePresence Conductor [p.15], using the .tar.gz version of the TelePresence Conductor software.

After installation we recommend that you take a snapshot of the VM TelePresence Conductor (see Taking and restoring snapshots [p.12]) so that it can be restored if the running VM gets damaged in any way. The VM snapshot retains the licensing information that was generated when the .ova file was installed, including any release and license keys that were applied.

Obtaining release keys and license keys

Licenses can be obtained after the VM TelePresence Conductor is installed, using the serial number of the VM TelePresence Conductor. The serial number is available from the **Option key** page and from the footer of the TelePresence Conductor web interface. See Ordering and entering release and option keys [p.11] for more information.

Installing a VM

The sections below list the recommended platform and specifications-based system requirements, and describe the VM installation process. The requirements outlined below refer to the minimum requirements for TelePresence Conductor version XC3.0. The minimum requirements for future TelePresence Conductor software releases may differ and you should refer to the release notes or administrator guide to ensure that pre-requisites are met.

Recommended platform

See http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_TelePresence_Conductor for the current list of supported UCS Tested Reference Configurations and specs-based supported platforms.

Ensure that:

- VT is enabled in the BIOS before installing VMware ESXi
- the VM host “Virtual Machine Startup/Shutdown” is configured to “Allow Virtual machines to start and stop automatically with the system”, and that the VM TelePresence Conductor has been moved to the Automatic startup section

Specifications-based system – minimum specification

If using a UCS Tested Reference Configuration or specifications-based system, the minimum requirements are:

- VM host operational and running ESXi 4.1, ESXi 5.0 (Update 1), ESXi 5.1 or ESXi5.5
- 6GB of RAM per VM TelePresence Conductor
- 132GB disk space per VM (for a 4GB virtual disk 1 and a 128GB virtual disk 2)
- 2 cores reserved per VM TelePresence Conductor; each core >= 2.8GHz processor (5600MHz for 2 vCPUs)
- vCenter or vSphere operational

Note: ESXi 5.0 is currently not supported; during testing a problem was observed on a host using ESXi 5.0 and an LSI MegaRAID card. We strongly recommend using ESXi 5.0 (Update 1), where this issue has been resolved.

Co-residency support

The TelePresence Conductor can co-reside with applications (any other VMs occupying same host) subject to the following conditions:

- no oversubscription of CPU: 1:1 allocation of vCPU to physical cores must be used
- no oversubscription of RAM: 1:1 allocation of vRAM to physical memory
- sharing disk storage subsystem is supported subject to correct performance (latency, bandwidth) characteristics

Installation process

This process guides you through installing the TelePresence Conductor VM using vSphere client.

Configuring the VM host

Ensure that the VM host is configured with a valid NTP server – the same NTP server that will be specified in TelePresence Conductor.

1. Select the host.
2. Go to the **Configuration** tab.
3. Select **Time configuration**.
4. Select **Properties**.
   If the date and time were red on the previous page, set the date and time manually to the current time.
5. Click **Options**.
6. Select **NTP Settings**.
7. Click **Add**.
8. Enter the IP address of the NTP server.
9. Click **OK**.
10. Select the **Restart NTP service to apply changes** check box.
11. Click **OK**.
12. Click **OK**.

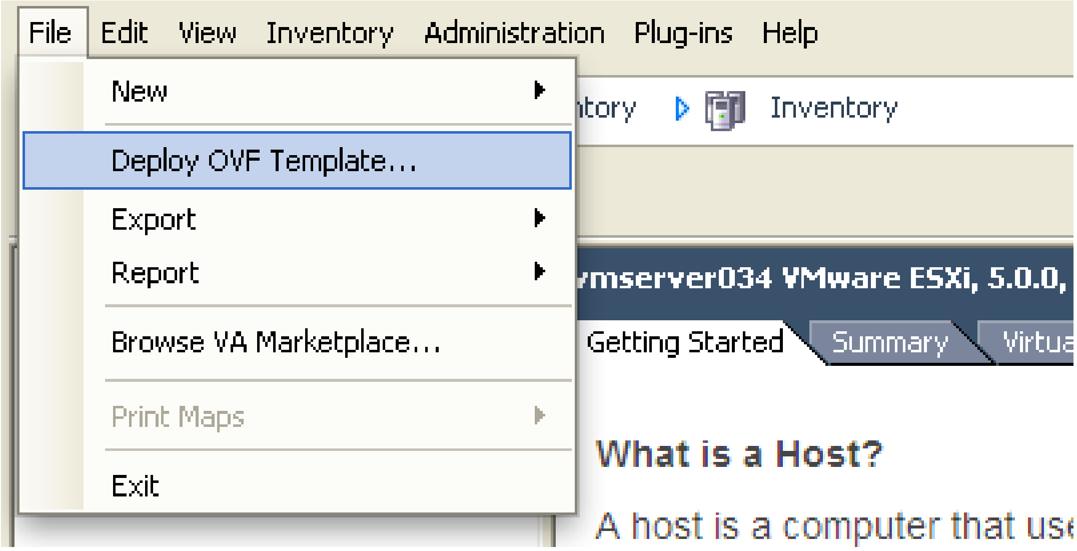
The following section describes how to deploy the ova to host using vSphere.

Deploying ova to host using vSphere client

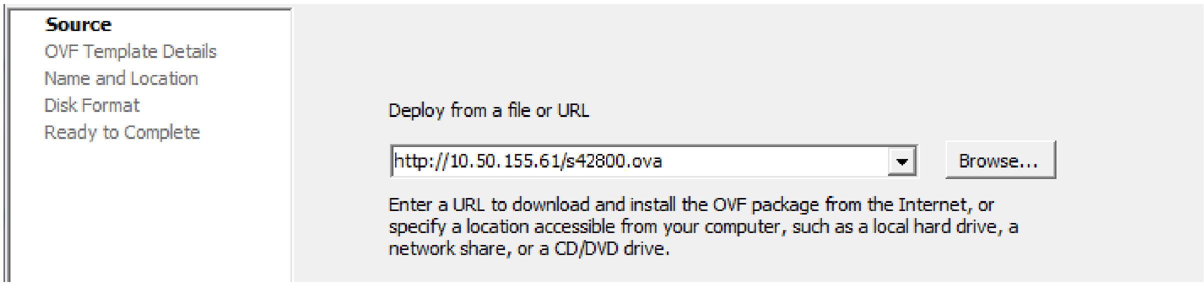
These instructions represent a typical installation. The Deploy OVF Template wizard dynamically changes to reflect host configuration.

1. If the .ova file is already preloaded onto the ESXi Host datastore (for example, in Cisco Business Edition 6000 deployments):
   a. Using a web browser, go to https://<VMwareHost>/folder supplying any required credentials (typically the same username and password as used to log into the vSphere client).
   b. Navigate through the index of datacenters to find the .ova file you want to deploy from the datastore.
   c. Right click on the .ova file and select **Copy Link Location**.
   (If the .ova file is not preloaded on the datastore, you can select and upload it in the following steps.)
2. Log in to the vSphere client to access the ESXi Host.

3. Select **File > Deploy OVF Template**.



4. On the **Source** page, identify where the .ova file is located, and then click **Next**.
   - If the .ova file is already preloaded onto the ESXi Host datastore, paste the URL you copied from step 1 above. You may have to re-enter username and password credentials so that the vSphere client can access the web server.
   - If the .ova file is not preloaded on the datastore, **Browse** to the location of the .ova file.

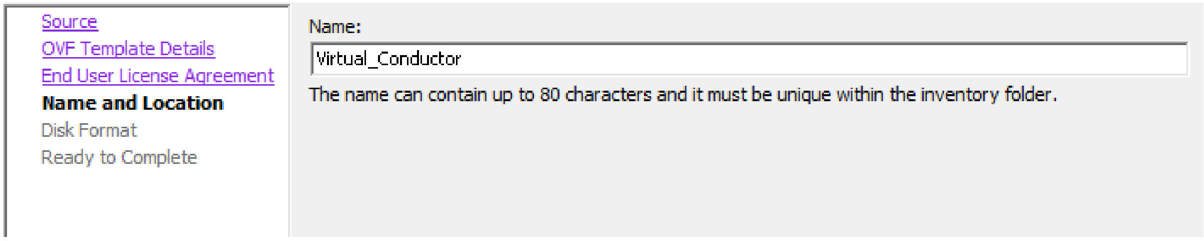


Deploy from a file or URL

http://10.50.155.61/s42800.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

5. On the **OVF Template Details** page, check that the Publisher certificate is valid and click **Next**.
6. On the **End User License Agreement** page:
   a. Read the EULA
   b. If you accept the EULA, click **Accept** then **Next**.
7. On the **Name and Location** page enter a **Name** for this TelePresence Conductor VM guest, for example "Virtual_Conductor" and click **Next**.

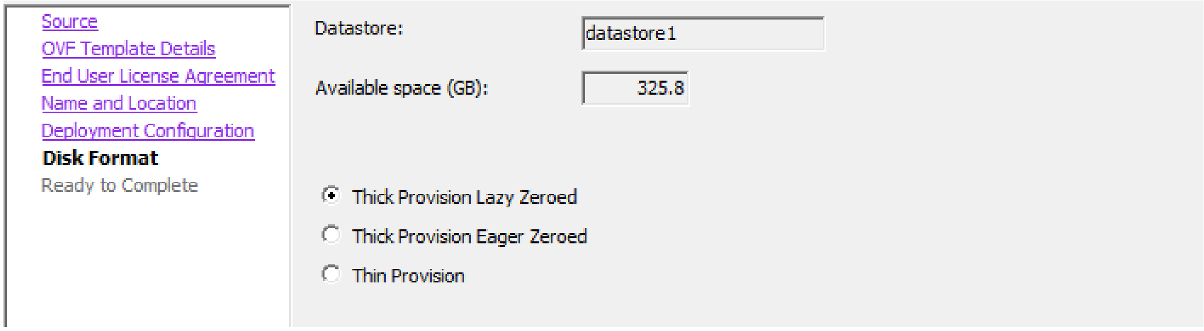


Name:

Virtual_Conductor

The name can contain up to 80 characters and it must be unique within the inventory folder.

8. On the **Disk Format** page, ensure that the default disk format of **Thick Provision Lazy Zeroed** is selected and then click **Next**.
   Thin Provision is not supported as VM performance may degrade during resizing of a partition.



Datastore: datastore1

Available space (GB): 325.8

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

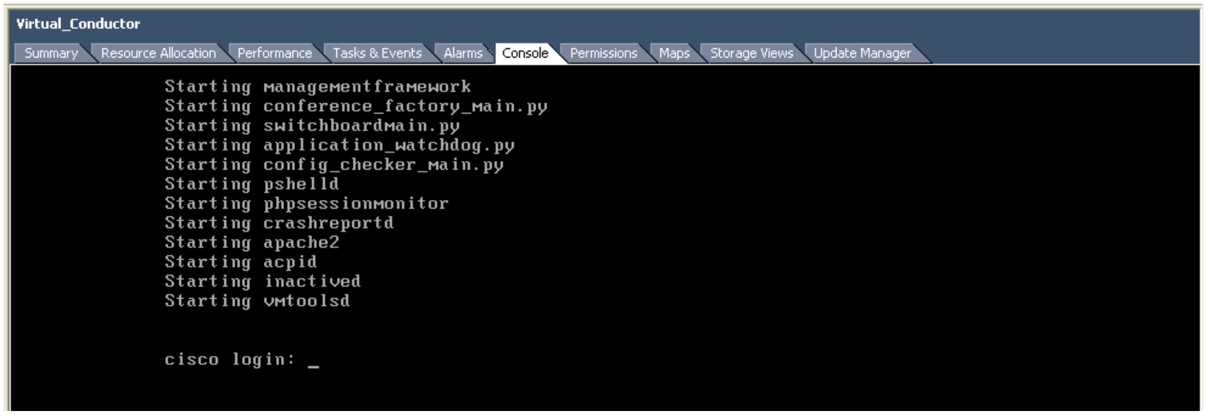
9. On the **Ready to Complete** page:
   a. Confirm the deployment settings.
   b. Select the **Power on after deployment** check box.
   c. Click **Finish**.
   The installation process will begin and a progress bar will be displayed.

The TelePresence Conductor ova is now deployed as a guest on the VM Host.

You now have to enter the network IP information for the TelePresence Conductor; see Configuring the VM guest (vSphere clients) [p.8].

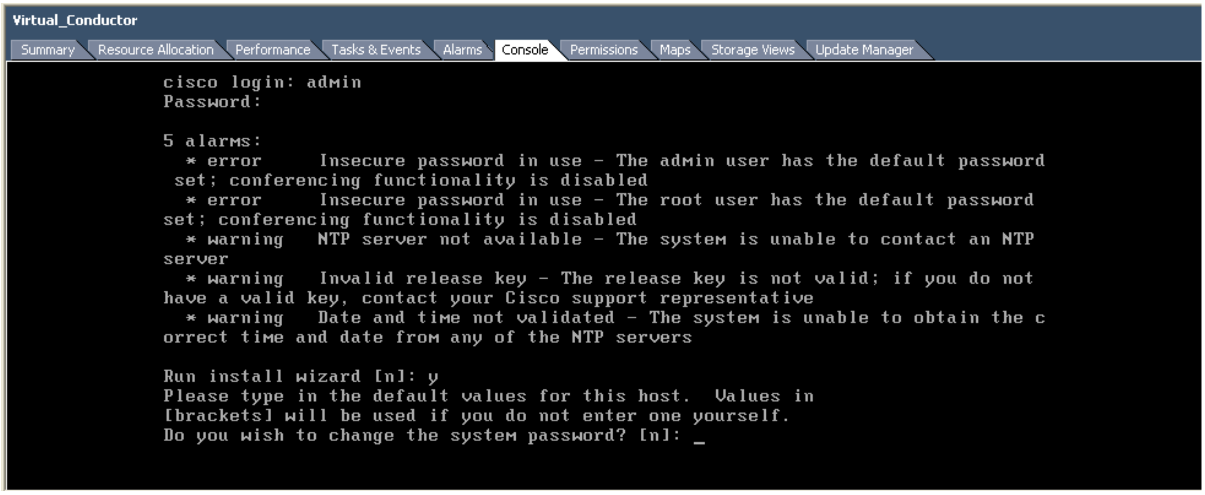
Configuring the VM guest (vSphere clients)

1. Select the VM guest and then select the **Console** tab.
   The VM guest will take some time to boot, create its second hard disk partition and then reboot to a login prompt.
2. If you do not see a login prompt, hit Enter.
   At the login prompt enter 'admin' for the username and 'TANDBERG' for the password.



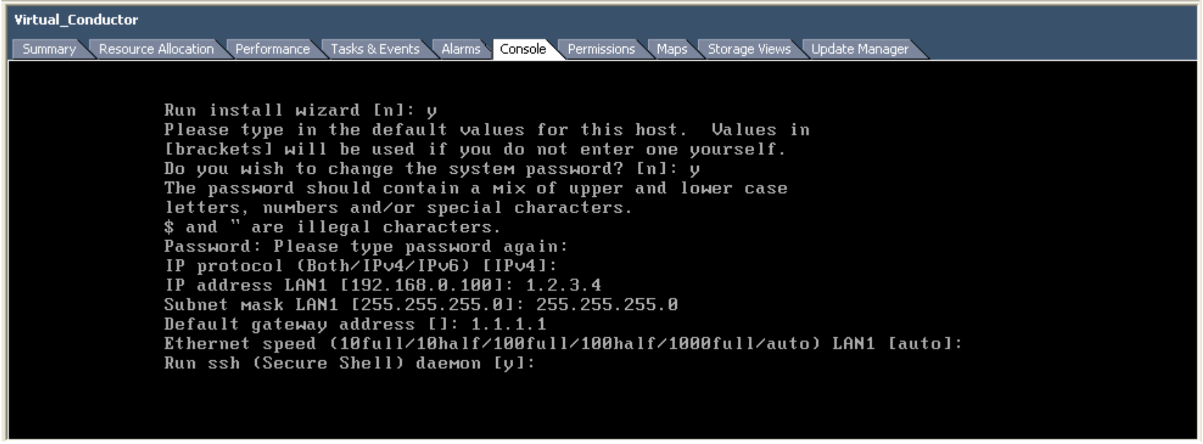
```
Starting managementframework
Starting conference_factory_main.py
Starting switchboardmain.py
Starting application_watchdog.py
Starting config_checker_main.py
Starting pshelld
Starting phpsessionmonitor
Starting crashreportd
Starting apache2
Starting acpid
Starting inactived
Starting vmtoolsd


cisco login: _
```

3. At the Install Wizard prompt type **`y`** and then press **`Enter`**.



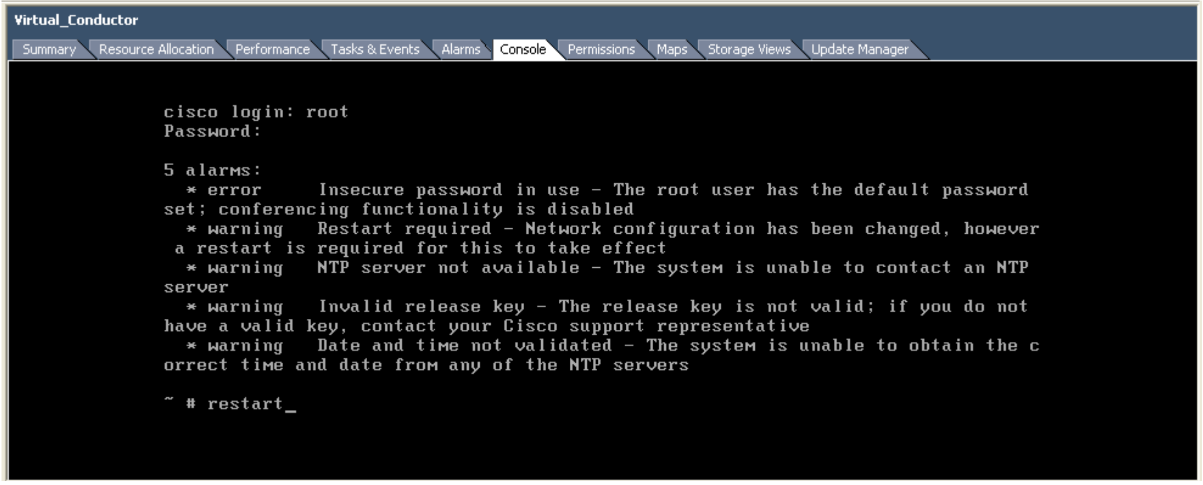
```
cisco login: admin
Password:

5 alarms:
  * error     Insecure password in use - The admin user has the default password
 set; conferencing functionality is disabled
  * error     Insecure password in use - The root user has the default password
set; conferencing functionality is disabled
  * warning   NTP server not available - The system is unable to contact an NTP
server
  * warning   Invalid release key - The release key is not valid; if you do not
have a valid key, contact your Cisco support representative
  * warning   Date and time not validated - The system is unable to obtain the c
orrect time and date from any of the NTP servers

Run install wizard [n]: y
Please type in the default values for this host.  Values in
[brackets] will be used if you do not enter one yourself.
Do you wish to change the system password? [n]: _
```

4. Follow the Install Wizard to enter the network IP information for the TelePresence Conductor. (Defaults can be entered by pressing **`Enter`** at the prompt.)



```
Run install wizard [n]: y
Please type in the default values for this host.  Values in
[brackets] will be used if you do not enter one yourself.
Do you wish to change the system password? [n]: y
The password should contain a mix of upper and lower case
letters, numbers and/or special characters.
$ and " are illegal characters.
Password: Please type password again:
IP protocol (Both/IPv4/IPv6) [IPv4]:
IP address LAN1 [192.168.0.100]: 1.2.3.4
Subnet mask LAN1 [255.255.255.0]: 255.255.255.0
Default gateway address []: 1.1.1.1
Ethernet speed (10full/10half/100full/100half/1000full/auto) LAN1 [auto]:
Run ssh (Secure Shell) daemon [y]:
```

5. When the wizard completes, the configuration is applied and the TelePresence Conductor logs you out.
6. Log into the TelePresence Conductor as root with a password of TANDBERG and then restart the VM guest by typing **`restart`**.



```
cisco login: root
Password:

5 alarms:
  * error     Insecure password in use - The root user has the default password
set; conferencing functionality is disabled
  * warning   Restart required - Network configuration has been changed, however
 a restart is required for this to take effect
  * warning   NTP server not available - The system is unable to contact an NTP
server
  * warning   Invalid release key - The release key is not valid; if you do not
have a valid key, contact your Cisco support representative
  * warning   Date and time not validated - The system is unable to obtain the c
orrect time and date from any of the NTP servers

~ # restart_
```

7. You should now be able to access the TelePresence Conductor via a web browser.

You can now order your release key; see Ordering and entering release and option keys [p.11].

Ordering and entering release and option keys

After the TelePresence Conductor ova has been deployed as a Guest on the VM Host you should be able to access the TelePresence Conductor via a web browser and order your release key.

1. Log in to the TelePresence Conductor via a web browser as admin with the default password of TANDBERG.
2. Get release key:
   a. Go to the **Option keys** page (**Maintenance > Option keys**).
   b. Copy the **Hardware serial number**.
   c. Use this serial number to order a release key for this VM TelePresence Conductor.
   For full details on obtaining your release keys, see Appendix 2: VM TelePresence Conductor activation process [p.21].

When the release key is available:

1. Log in to the TelePresence Conductor via a web browser as admin.
2. Enter the release and option keys:
   a. Go to the **Option keys** page (**Maintenance > Option keys**).
   b. Enter the release key provided in the **Release key** field.
   c. Click **Set release key**.
   d. For each option key provided:
      i. Enter the option key value in the **Add option key** field.
      ii. Click **Add option**.
3. Reboot the TelePresence Conductor to activate the licenses:
   a. Go to the **Restart options** page (**Maintenance > Restart options**).
   b. Click **Reboot**.
4. After the reboot, log in to the web interface and configure the TelePresence Conductor, including changing any default passwords, configuring DNS, NTP, conference configuration settings and so on as required.
   Follow the relevant Cisco TelePresence Conductor Deployment Guide to guide you through configuring this VM TelePresence Conductor ready for operation.
5. After the TelePresence Conductor has been configured it is good practice to backup the TelePresence Conductor configuration using the TelePresence Conductor backup facility, and also to take a VM snapshot (see Taking and restoring snapshots [p.12]).
   The snapshot is important as it can be used to restore a VM should it become damaged – the snapshot retains the existing license keys. If the VM is re-installed instead of being restored, new license keys would be required.

Taking and restoring snapshots

The VMware snapshot feature is especially useful in test labs where it is required to return to a known starting point. This is not a replacement for the TelePresence Conductor backup – the TelePresence Conductor backup should always be performed prior to the VMware snapshot being taken.

A VMware snapshot can be used to restore a VM should it become damaged (because the VMware snapshot retains the existing license keys).

- Ensure that the host has spare disk space on which to create and store the snapshot – each snapshot can take up to 132GB + 6GB.
- Only perform the snapshot when the VM TelePresence Conductor is idle – performing the snapshot will likely disturb the operation of the TelePresence Conductor.

If the VM is re-installed instead of being restored, the serial number will change and new license keys would be required. If you need to move TelePresence Conductor to a new host you must perform a host migration via vMotion.

Creating a VMware snapshot

We strongly recommended to perform a VMware snapshot only when the TelePresence Conductor is idle, in order to ensure reliability.

1. Select the relevant TelePresence Conductor VM Guest.
2. Right-click the TelePresence Conductor VM Guest and select **Snapshot > Take Snapshot**.
3. Enter name and description.
4. Ensure **Snapshot the virtual machine’s memory** is selected.
5. Click **OK**.
6. Wait for the “Create virtual machine snapshot” task to complete.

Restoring a VMware snapshot

1. Select the relevant TelePresence Conductor VM Guest.
2. Right-click the TelePresence Conductor VM Guest and select **Snapshot > Snapshot Manager**.
3. Select the required snapshot image.
4. Click **Goto**.
5. Click **Yes**.
6. Click **Close**.

Incremental VMware backups

If incremental backups are to be enabled, ensure that you follow the VMware Guides on 1st & 3rd Party Guest Backup Solutions.

Hardware references

Serial interface

A VM TelePresence Conductor has no physical serial interface; the serial interface is accessible through the console tab of the VM guest.

You can use CTRL+ALT to exit from the Console window (this is identified in the bottom right corner of the vSphere Client window).

Ethernet interfaces (NICs)

In VM TelePresence Conductor the LAN interfaces are Virtual NICs. Appropriate drivers are set up as VM TelePresence Conductor is installed; configuration of IP addresses is carried out through the standard TelePresence Conductor interface.

VM TelePresence Conductor allocates 3 virtual NICs:

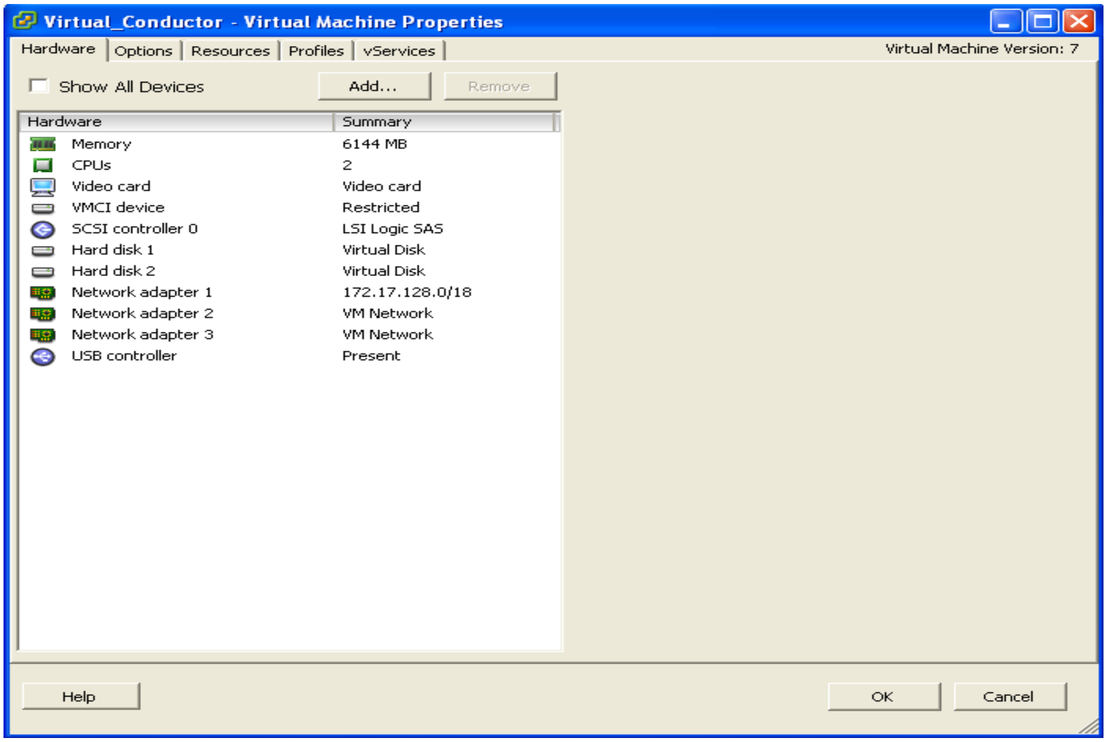
- the first is used for the standard LAN 1 interface
- the second and third are reserved for future use

Allocating a virtual NIC to a physical NIC interface

Virtual NICs can be assigned to physical interfaces as follows:

1. Ensure that the physical NIC on the VM host is connected and operational.
2. Set up or check that there are Virtual Switches (vNetwork Distributed Switches) for each physical NIC. (Select the host on which the VM TelePresence Conductor will run, select the **Configuration** tab and select **Networking**.)
3. Ensure that there is at least one Virtual Machine Port Group (with associated VLAN IDs) set up for each physical NIC.
   To add a new Virtual Machine Port Group:
   a. Click **Properties** on the appropriate Virtual Switch or vNetwork Distributed Switch.
   b. Follow the network wizard.
4. Note the name of a Virtual Machine Port Group connecting to the required NIC.

5. Select the VM guest; right click it and select **Edit settings…**

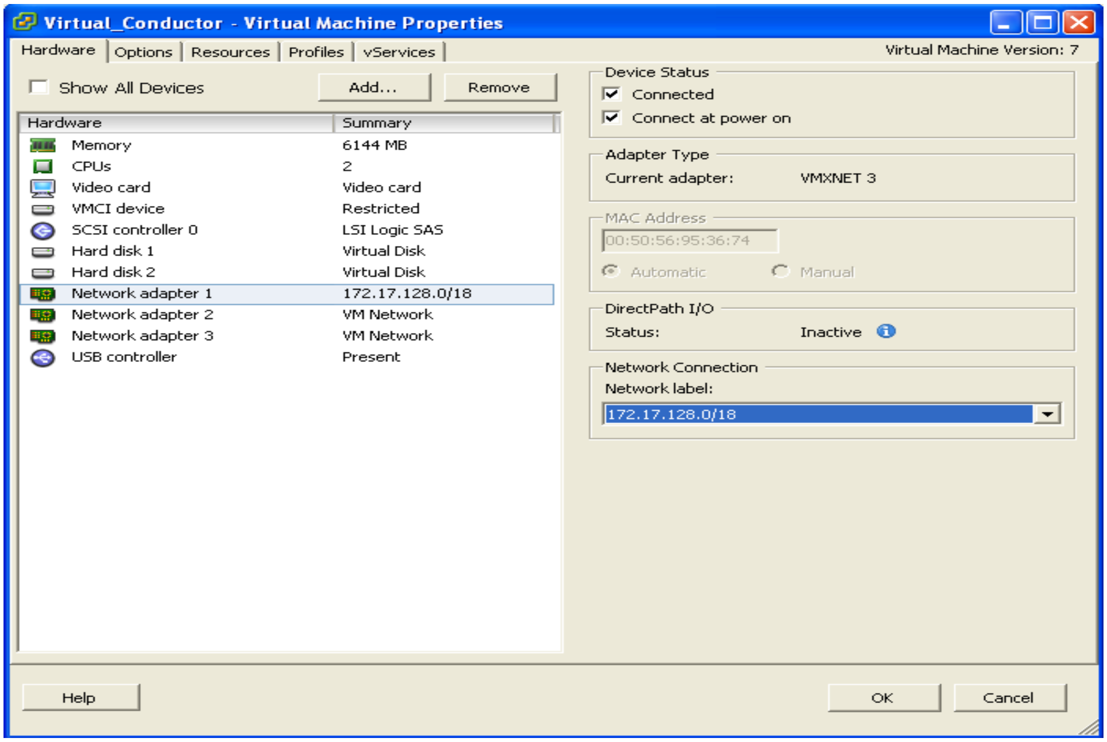


Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory	6144 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	172.17.128.0/18
Network adapter 2	VM Network
Network adapter 3	VM Network
USB controller	Present

6. Select the required network adaptor (Network adaptor 1 = LAN 1, Network adaptor 2 = LAN 2).



Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory	6144 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	172.17.128.0/18
Network adapter 2	VM Network
Network adapter 3	VM Network
USB controller	Present

Device Status

☑ Connected

☑ Connect at power on

Adapter Type

Current adapter: VMXNET 3

MAC Address

00:50:56:95:36:74

● Automatic ○ Manual

DirectPath I/O

Status: Inactive

Network Connection

Network label:

172.17.128.0/18

7. Select the appropriate Network label (Virtual Machine Port Group) to associate the TelePresence Conductor LAN interface with the required physical NIC.

8. After a few seconds the TelePresence Conductor will be able to communicate over the physical interface.

Additional information

Upgrading a VM TelePresence Conductor

When upgrading a VM TelePresence Conductor you must use a .tar.gz file (available from the software download site), not an .ova file:

1. To avoid any performance degradation we recommend that you upgrade the TelePresence Conductor while the system is inactive.
2. If the TelePresence Conductor is part of a cluster follow the relevant Cisco TelePresence Conductor Clustering deployment guide.
3. If the TelePresence Conductor is not part of a cluster:
   a. Log in to the TelePresence Conductor VM web interface as an administrator.
   b. Backup the TelePresence Conductor from the **Backup** page (**Maintenance > Backup and restore**).
   c. Upgrade the TelePresence Conductor from the **Upgrade** page (**Maintenance > Upgrade**).

Clustering for resilience and capacity

When clustering VM TelePresence Conductors it is strongly recommended to use at least two physical hardware hosts – clustered TelePresence Conductors are designed to support resilience and capacity.

To support hardware resilience, TelePresence Conductor peers must run on at least two different hardware platforms.

Each and every TelePresence Conductor peer in a cluster must be within a 15ms hop (30ms round trip delay) of each and every other TelePresence Conductor in or to be added to the cluster.

For more information on clustering TelePresence Conductors, see the relevant Cisco TelePresence Conductor Clustering Deployment Guide.

Migrating from a physical appliance to a VM

If you are migrating from a physical appliance to a VM TelePresence Conductor, the backup/restore process (**Maintenance > Backup and restore**) can be used to transfer configuration between the two installations. You will receive a warning message, but you will be allowed to continue.

Supported features

vMotion

vMotion has been tested and TelePresence Conductor will move (migrate) successfully. If you need to move TelePresence Conductor to a new host you must perform a host migration via vMotion.

We recommend that a vMotion move is carried out when there is low conference creation activity on the VM TelePresence Conductor.

SAN with Fibre interconnect

Use of a SAN with Fibre interconnect, rather than a NAS, is recommended in order to maximize the transfer speed.

Unsupported features

VMware fault tolerant mode

VMware fault tolerant mode is not supported (because the TelePresence Conductor uses multiple cores).

Licensing

VM TelePresence Conductors require licensing in the same way that the appliance TelePresence Conductor units require licensing.

If you copy the VM, the TelePresence Conductor serial number will change and the existing license keys will be invalidated. If you need to move TelePresence Conductor to a new host you must perform a host migration via vMotion.

Security hardening

Information on how to deploy and operate VMware products in a secure manner is available from the VMware Security Hardening Guides.

Appendix 1: Troubleshooting

This section contains information to help in troubleshooting system issues.

Checking VMware compatibility

If you are using third party hardware for hosting the VM TelePresence Conductor application, check the hardware compatibility. This can be done using the VMware compatibility guide tool available from http://www.vmware.com/resources/compatibility/search.php.

VMware checklist

1. Check the accessibility to the VM host server (by ping, physical console access, ssh remote access, KVM-over-IP console, and so on).
2. Check the network connectivity of the VMkernel (by executing the **`vmkping`** command using Tech Support Mode to verify network connectivity from the VMkernel NIC level).
3. If you are having problems connecting to the vSphere Client management console, execute the command **`/sbin/services.sh`** from an SSH session to restart the ESXi management agent.
4. Check the utilization of the VM host server (CPU utilization, memory utilization, disk access speed, storage access speed, network access status, power utilization, and so on).
   If any specific application causes high utilization, stop or restart this application to isolate the overall VM host performance level. Alternatively execute the command **`esxtop`** from Tech Support Mode to list all system processes running on the ESXi host application.
5. Check the ESXi server file log (hostd.logs) under the folder /var/log/vmware.
   This log contains common error logs such as iSCI naming error, authentication error, host convertibility error, and so on.
6. Verify that there is adequate disk space available on the physical volume that stores the database files, and free up disk space if necessary.
7. Validate the authentication to the vCenter Server database. The vCenter Server service may not be able to authenticate with the database if:
   a. There are permission issues with the database when importing from one instance to another.
   b. The password on the account you are using to authenticate to the database has changed but the password in the registry has not changed as well.
   c. The vCenter Server database user is not granted correct permissions.

Isolating a possible root cause

Potential issue area	What to look for
Storage	Look for the VM store application image stored either on the local drive, SAN or NFS. VMs often freeze or hang up if the application failed to access the storage. Possible error messages are: ■ vCenter Server does not start ■ vCenter Server is slow to respond ■ vCenter Server fails after an indefinite amount of time

Potential issue area	What to look for
Network	Any network failure or locking causes a connection failure between the VM and the virtual network. Also, if using NFS or iSCSI, storage may cause application failures because the application cannot access the file system.
DNS	DNS server failures or communication failures between DNS and the VM server may cause the VMware application or the VM TelePresence Conductor application to fail.
vCenter Server	If vCenter is not operating properly, even though the VM TelePresence Conductor application is still up and running, you may lose connection to the VM TelePresence Conductor application from the network.
Host application	Check any critical alarms on the VM application for events on the host or application level (check the event information from vSphere Client).

Possible issues

VM image fails to boot

If the VM image fails to boot, check the VT (Virtualization Technology) setting in BIOS. This needs to be enabled for hosting VMs. If it is not set, set it and re-install ESXi then load the .ova file.

TelePresence Conductor application fails to start

Look at the /tmp/hwfail file – its content will indicate any violations in the installation.

For example, TelePresence Conductor reserves 3 virtual NICs – these are required in the TelePresence Conductor, do not try deleting one or more of them otherwise hwfail will be created and the VM TelePresence Conductor will not run.

Configured NTP does not work

For NTP to work on TelePresence Conductor, the same NTP must also be configured on the VM host.

Guest console in vSphere 5 fails to run on some Microsoft platforms

When attempting to open a console screen from vSphere for the VM:

- Error message: “The VMRC console has disconnected...attempting to reconnect.”
- Screen remains black

The following operating systems are at risk:

- Windows 7 64 bit – reported on VMware forum (http://communities.vmware.com/thread/333026)
- Windows Server 2008 R2 (64-bit) – found by use

Raid controller synchronization

If the VMware system is synchronizing its RAID disks, disk performance is seriously degraded. It is strongly recommended that TelePresence Conductor is not installed or run on VM platforms where RAID disks are in a degraded or synchronizing state.

Analyzing the cause of VMware issues

If VMware is causing problems on the TelePresence Conductor host, you are initially recommended to collect logs from the host for analysis:

1. Using the vSphere client (or the vCenter Server managing this ESXi host) connect to the ESXi host on which the TelePresence Conductor is running.
2. Go to **File > Export > Export System logs**, choose the appropriate ESXi host and go with the default settings.

After you have downloaded the logs analyze them, or have them analyzed to determine the issue.

More information on exporting logs can be found at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=653.

Restoring default configuration (factory reset)

Very rarely, it may become necessary to run the "factory-reset" script on your system. This reinstalls the software image and resets the configuration to the functional minimum.

Note: Restoring default configuration causes the system to use its current default values, which may be different from the previously configured values, particularly if the system has been upgraded from an older version.

Prerequisite files

The **`factory-reset`** procedure described below rebuilds the system based on the most recent successfully-installed software image. The files that are used for this reinstallation are stored in the **/mnt/harddisk/factory-reset/** folder on the system. These files are:

- A text file containing just the 16-character Release Key, named **rk**
- A file containing the software image in tar.gz format, named **tandberg-image.tar.gz**

In some cases (most commonly a fresh VM installation that has not been upgraded), these files will not be present on the system. If so, these files must first be put in place using SCP as root.

Performing a reset to default configuration

The following procedure must be performed from the serial console. This is because the network settings will be rewritten, so any SSH session used to initiate the reset would be dropped and the output of the procedure would not be seen.

The process takes approximately 20 minutes.

1. Log in to the system as **root**.
2. Type **`factory-reset`**
3. Answer the questions as required:

The recommended responses will reset the system completely to a factory default state.

Prompt	Recommended response
Keep option keys [YES/NO]?	YES
Keep IP configuration [YES/NO]?	YES
Keep ssh keys [YES/NO]?	YES
Keep ssl certificates and keys [YES/NO]?	YES
Keep root and admin passwords [YES/NO]?	YES
Save log files [YES/NO]?	YES

4. Finally, confirm that you want to proceed.

Resetting your administrator password or root password

If you have forgotten the password for either an administrator account or the **root** account and you are using a VM (Virtual Machine) TelePresence Conductor, you can reset it using the following procedure:

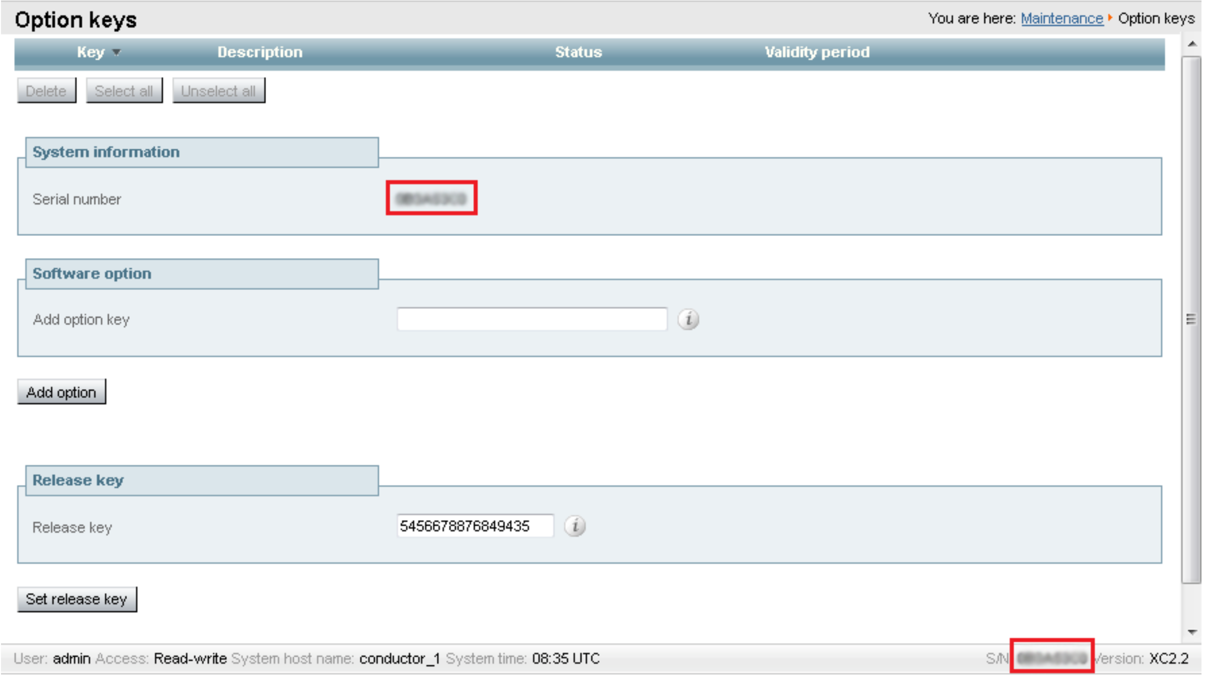
1. Open the vSphere client.
2. Click on the link **Launch Console**.
2. Reboot the TelePresence Conductor.
3. In the vSphere console log in with the username `pwrec`. No password is required.
4. When prompted, select the account (*root* or the username of the administrator account) whose password you want to change.
5. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a reboot. After that time you will have to reboot the system again to reset the password.

Appendix 2: VM TelePresence Conductor activation process

Follow this procedure to activate your Cisco TelePresence Conductor software.

1. Ensure you have downloaded and installed the virtual TelePresence Conductor software before attempting to register your Product Authorization Keys (PAKs) that you will have received via email. The TelePresence Conductor software can be downloaded from http://software.cisco.com/download/navigator.html.
2. After the VM TelePresence Conductor software is installed, retrieve the 8 character serial number from the **Option keys** page (**Maintenance > Option keys**) or from the bottom right hand corner of the TelePresence Conductor web interface.



Serial number [redacted]

Release key 5456678876849435

User: admin Access: Read-write System host name: conductor_1 System time: 08:35 UTC S/N [redacted] Version: XC2.2

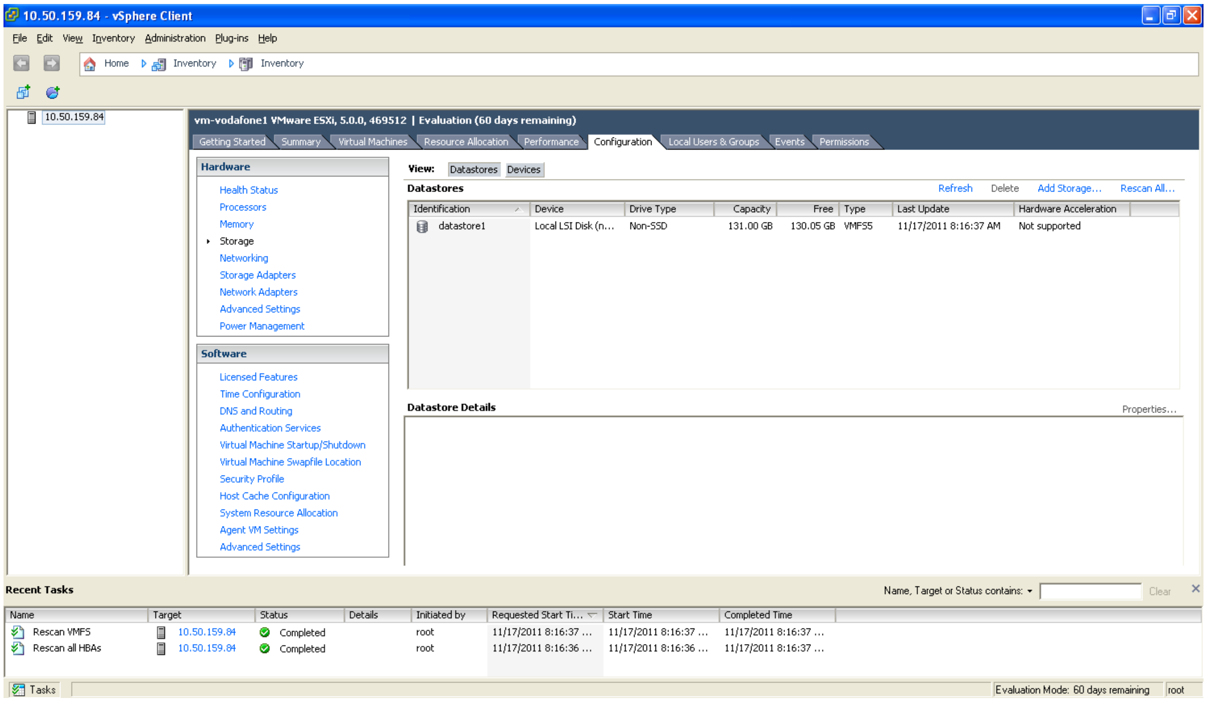
3. Register your software and feature PAKs at the customer licensing portal to retrieve your **Release** key and any relevant **Option** keys:
   a. Go to www.cisco.com/go/license and sign in.
   b. If necessary, click **Continue to Product License Registration**.
   c. Follow the onscreen instructions to register your software PAK (with a part number prefix of LIC-SW-CNDTR), utilizing the product serial number obtained from the previous step.
   d. Continue to register any applicable feature PAK.

   You will shortly receive 2 emails containing your Release and Option keys.
4. Enter your **Release key** and any **Option keys** on the **Option keys** page (**Maintenance > Option keys**) on the TelePresence Conductor web interface.
5. Restart the TelePresence Conductor (**Maintenance > Restart options**).
   Only one restart is required after the release key and option keys have been entered.

Appendix 3: Deploying multiple datastores

This process should be carried out during the initial build of the VM host, if the VM host has two or more RAID arrays of disk storage. This configuration enables vSphere / vCenter to know about all the datastores.

1. From vSphere or vCenter Inventory list select the relevant Host.
2. Select the **Configuration** tab.
3. Select **Storage**.

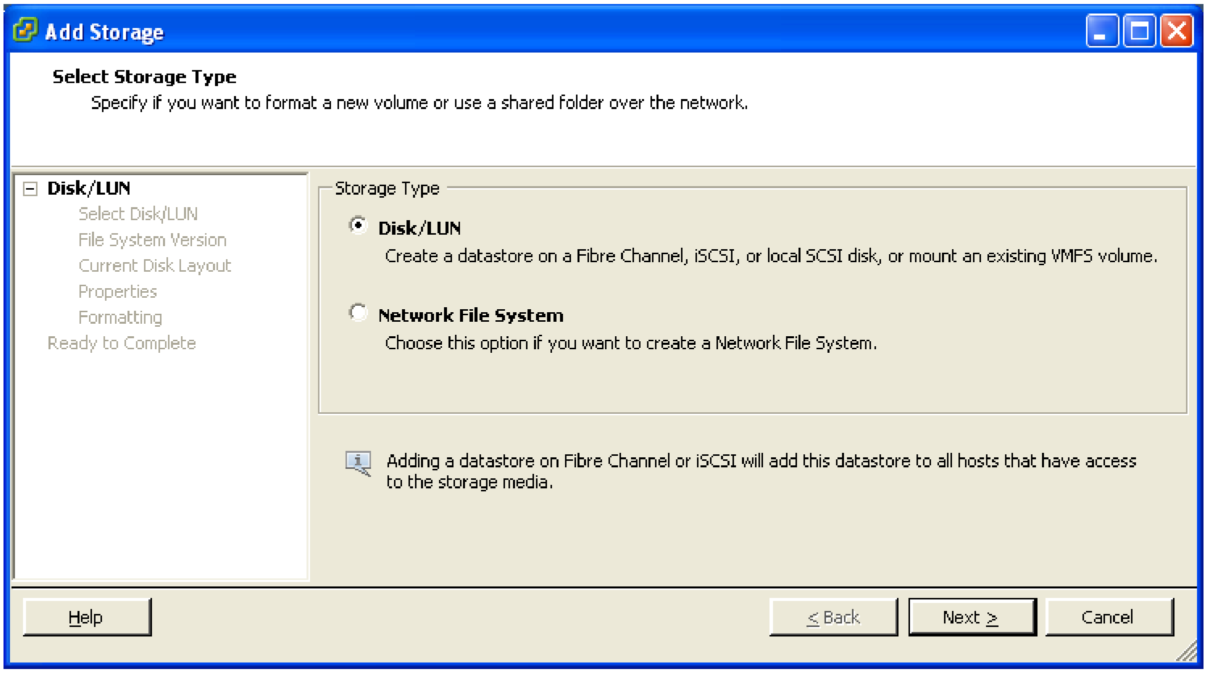


Identification	Device	Drive Type	Capacity	Free	Type	Last Update	Hardware Acceleration
datastore1	Local LSI Disk (n...	Non-SSD	131.00 GB	130.05 GB	VMFS5	11/17/2011 8:16:37 AM	Not supported

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Rescan VMFS	10.50.159.84	Completed		root	11/17/2011 8:16:37 ...	11/17/2011 8:16:37 ...	11/17/2011 8:16:37 ...
Rescan all HBAs	10.50.159.84	Completed		root	11/17/2011 8:16:36 ...	11/17/2011 8:16:36 ...	11/17/2011 8:16:37 ...

4. Select **Add Storage ...** (on the right hand side window).

5. Select **Disk/Lun** and click **Next**.



Select Storage Type

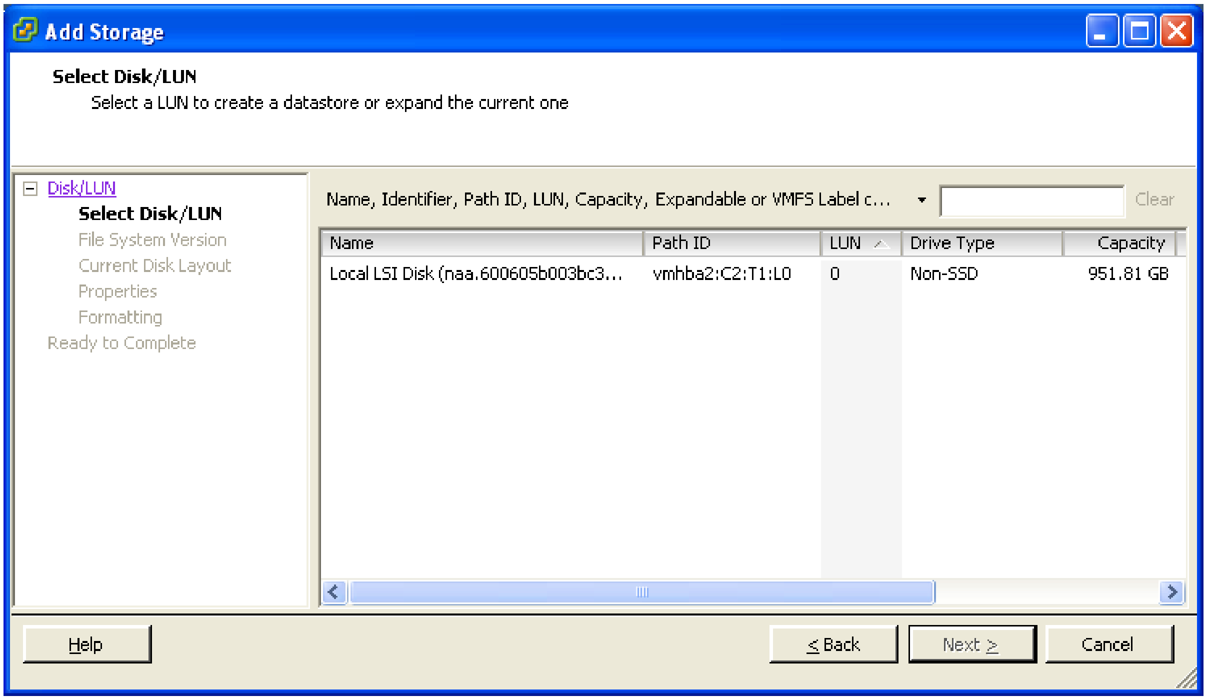
Specify if you want to format a new volume or use a shared folder over the network.

● **Disk/LUN**
Create a datastore on a Fibre Channel, iSCSI, or local SCSI disk, or mount an existing VMFS volume.

○ **Network File System**
Choose this option if you want to create a Network File System.

Adding a datastore on Fibre Channel or iSCSI will add this datastore to all hosts that have access to the storage media.

6. Under **Disk/LUN** select the required Disc/LUN from the list presented and click **Next**.

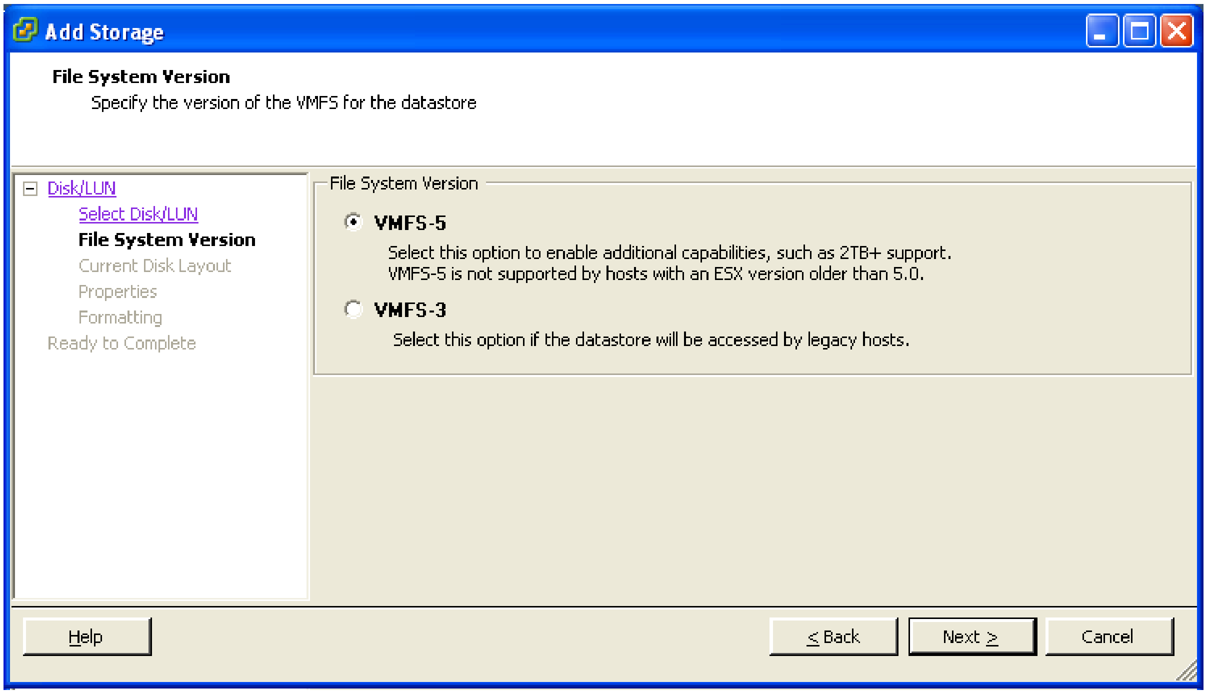


Select Disk/LUN

Select a LUN to create a datastore or expand the current one

Name	Path ID	LUN	Drive Type	Capacity
Local LSI Disk (naa.600605b003bc3...	vmhba2:C2:T1:L0	0	Non-SSD	951.81 GB

7. On the **File System Version** page select **VMFS-5** and then click **Next**.



File System Version

Specify the version of the VMFS for the datastore

File System Version

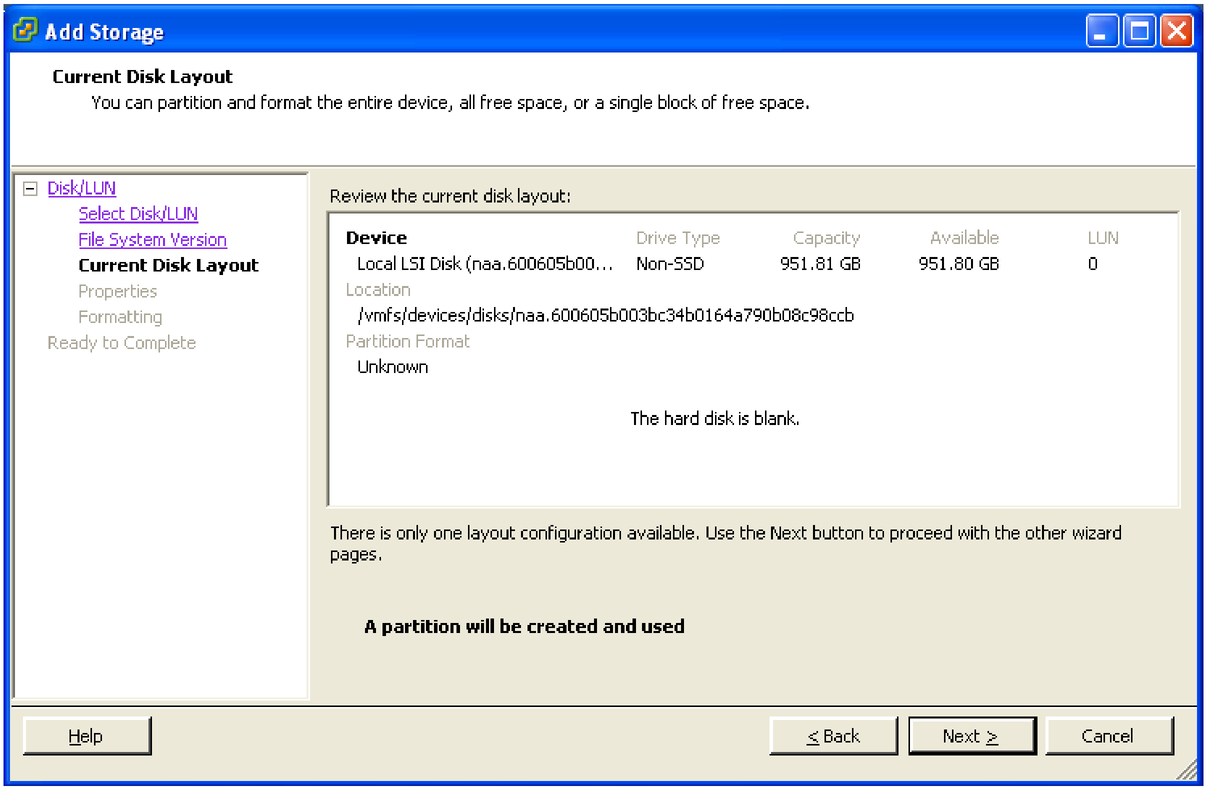
● **VMFS-5**

Select this option to enable additional capabilities, such as 2TB+ support.
VMFS-5 is not supported by hosts with an ESX version older than 5.0.

○ **VMFS-3**

Select this option if the datastore will be accessed by legacy hosts.

8. On the **Current Disk Layout** page verify the details and then click **Next**.



Current Disk Layout

You can partition and format the entire device, all free space, or a single block of free space.

Review the current disk layout:

Device	Drive Type	Capacity	Available	LUN
Local LSI Disk (naa.600605b00...	Non-SSD	951.81 GB	951.80 GB	0

Location

/vmfs/devices/disks/naa.600605b003bc34b0164a790b08c98ccb

Partition Format

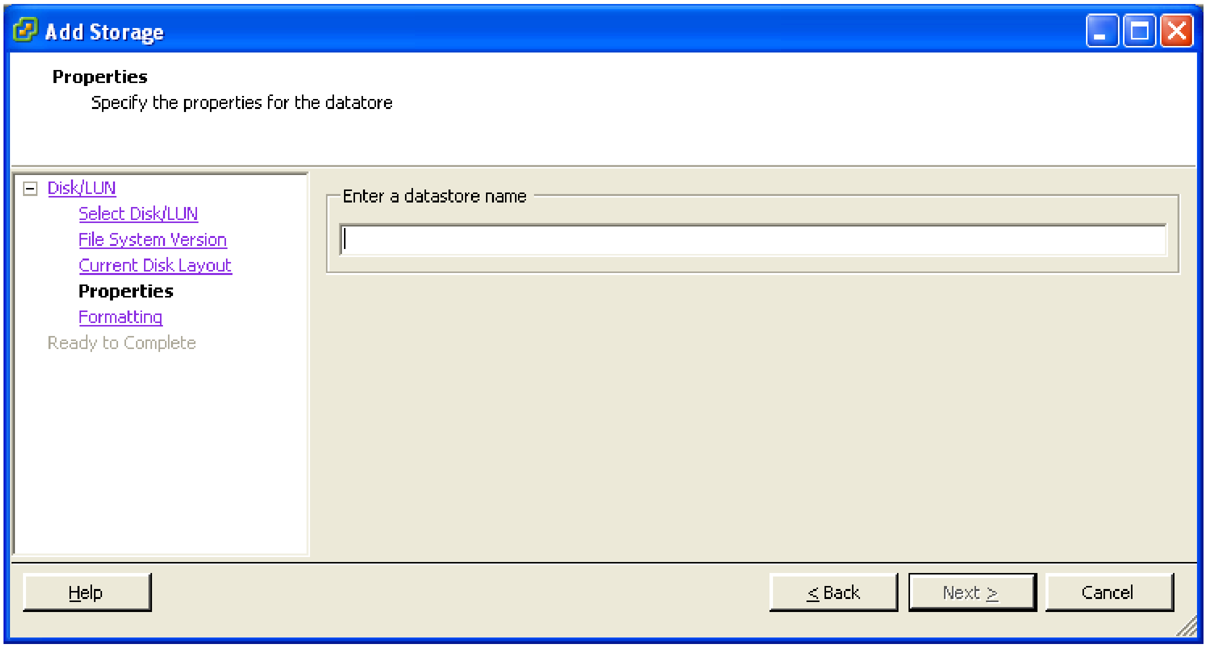
Unknown

The hard disk is blank.

There is only one layout configuration available. Use the Next button to proceed with the other wizard pages.

A partition will be created and used

9. On the **Properties** page enter a name for the new datastore and then click **Next**.

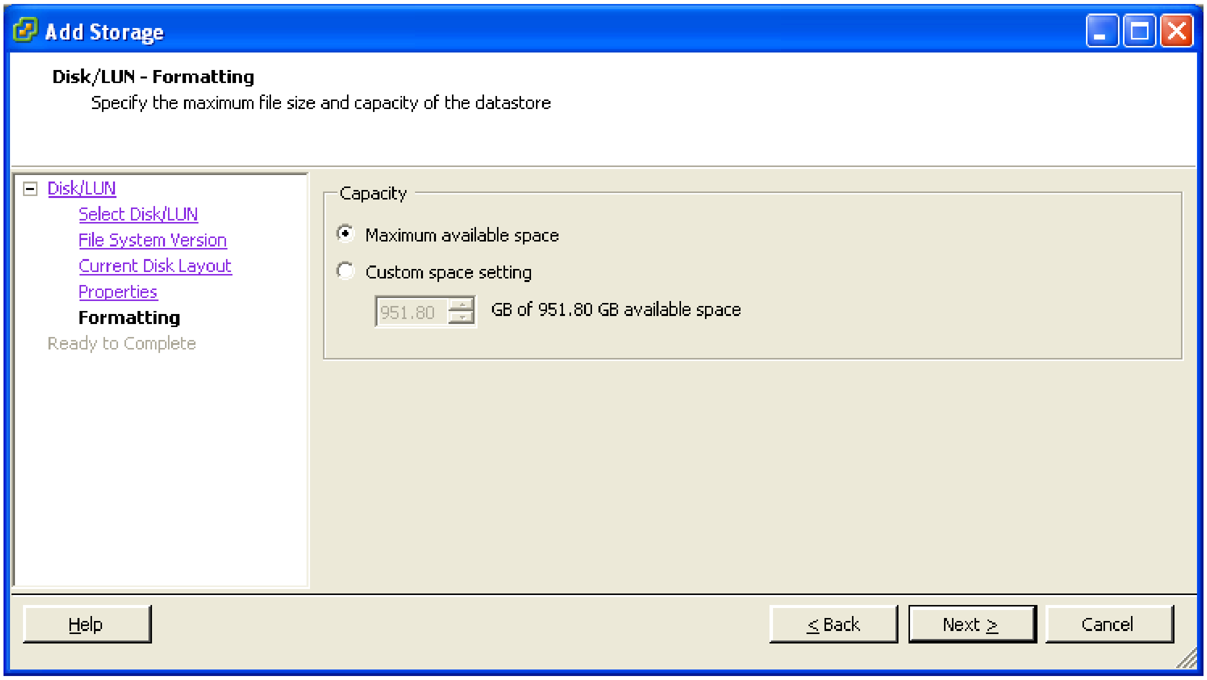


Properties

Specify the properties for the datatore

Enter a datastore name

10. On the **Formatting** page select **Maximum available space** and then click **Next**.



Disk/LUN - Formatting

Specify the maximum file size and capacity of the datastore

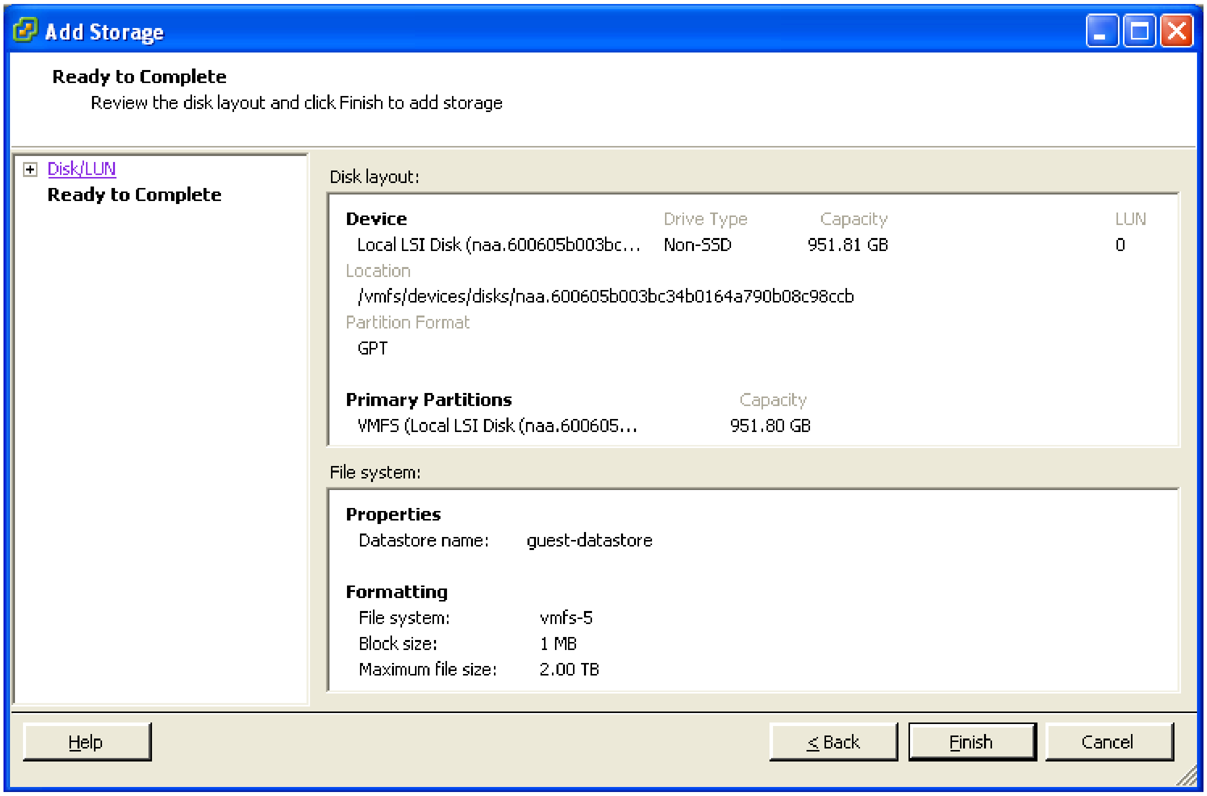
Capacity

● Maximum available space

○ Custom space setting

951.80 GB of 951.80 GB available space

11. On the **Ready to Complete** page verify the details and then click **Finish**.



Ready to Complete

Review the disk layout and click Finish to add storage

Disk layout:

Device	Drive Type	Capacity	LUN
Local LSI Disk (naa.600605b003bc...	Non-SSD	951.81 GB	0

Location

/vmfs/devices/disks/naa.600605b003bc34b0164a790b08c98ccb

Partition Format

GPT

Primary Partitions	Capacity
VMFS (Local LSI Disk (naa.600605...	951.80 GB

File system:

Properties

Datastore name: guest-datastore

Formatting

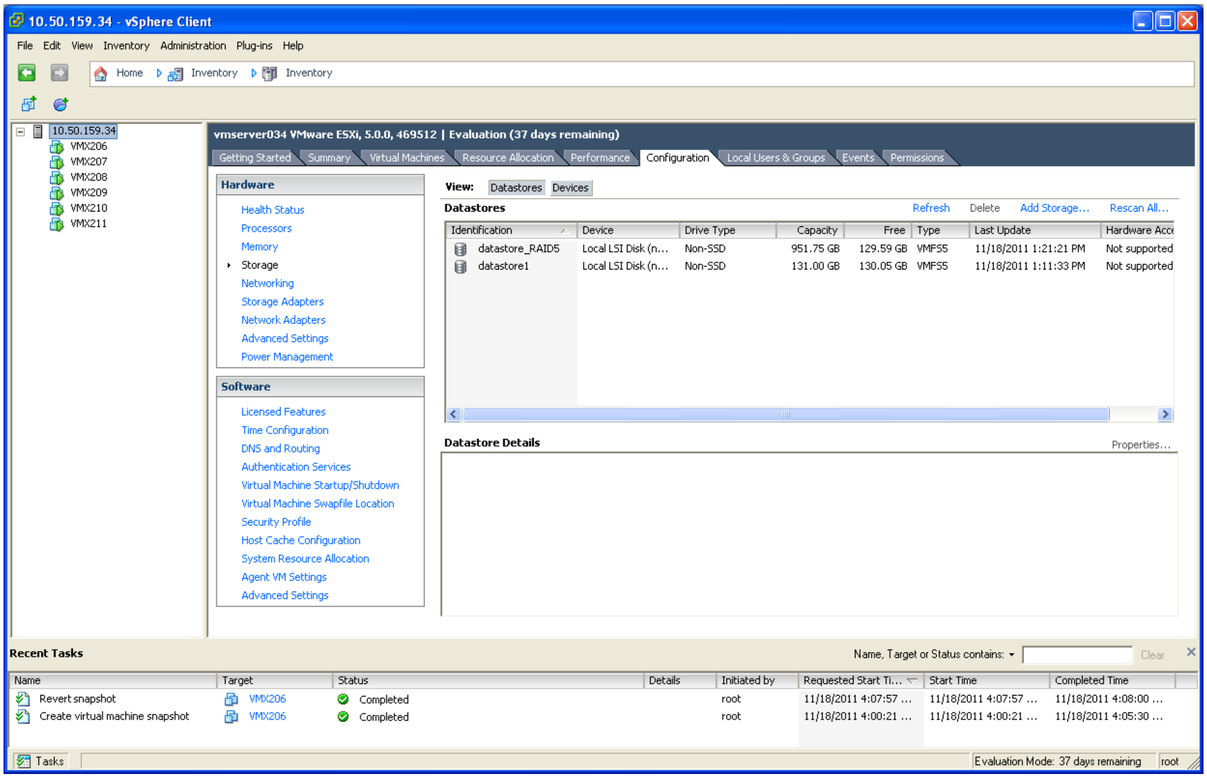
File system: vmfs-5

Block size: 1 MB

Maximum file size: 2.00 TB

12. Wait for the Create VMFS Datastore task to complete.

13. On completion, the new datastore will be listed under the **Storage** section.



vmserver034 VMware ESXi, 5.0.0, 469512 | Evaluation (37 days remaining)

Datastores

Identification	Device	Drive Type	Capacity	Free	Type	Last Update	Hardware Acce
datastore_RAID5	Local LSI Disk (n...	Non-SSD	951.75 GB	129.59 GB	VMFS5	11/18/2011 1:21:21 PM	Not supported
datastore1	Local LSI Disk (n...	Non-SSD	131.00 GB	130.05 GB	VMFS5	11/18/2011 1:11:33 PM	Not supported

Datastore Details

Recent Tasks

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Revert snapshot	VMX206	Completed		root	11/18/2011 4:07:57 ...	11/18/2011 4:07:57 ...	11/18/2011 4:08:00 ...
Create virtual machine snapshot	VMX206	Completed		root	11/18/2011 4:00:21 ...	11/18/2011 4:00:21 ...	11/18/2011 4:05:30 ...

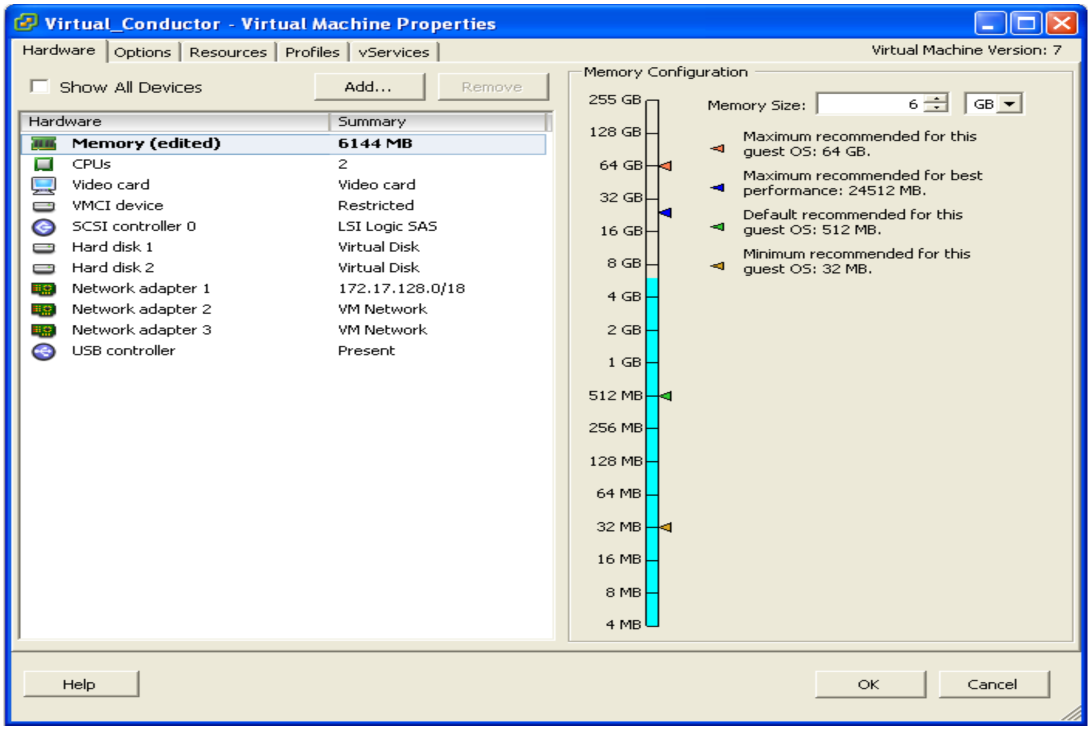
Evaluation Mode: 37 days remaining

root

Appendix 4: Ensuring that 6GB of memory is allocated for the VM TelePresence Conductor

If the wrong amount of memory has been allocated to the VM TelePresence Conductor, this can be corrected as follows:

1. Power off the guest:
   a. Select TelePresence Conductor VM Guest.
   b. Select the **Console** tab.
   c. Right-click TelePresence Conductor VM Guest and select **Power > Shut Down Guest**.
   d. Select to confirm shutdown.
   e. Wait for Initiate guest OS shutdown to complete.
   f. Wait for Console screen to go blank and the icon by TelePresence Conductor VM Guest to lose its green Power On indication.
2. When the guest is off, right-click the guest and select **Edit Settings**.
3. Select the **Hardware** tab.
4. Select **Memory**.
5. On the right side, ensure that Memory Size is set at 6GB – if not set it to 6GB and click **OK**.



Virtual Machine Version: 7

□ Show All Devices

Hardware	Summary
Memory (edited)	**6144 MB**
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	172.17.128.0/18
Network adapter 2	VM Network
Network adapter 3	VM Network
USB controller	Present

Memory Size: 6 GB

◄ Maximum recommended for this guest OS: 64 GB.

◄ Maximum recommended for best performance: 24512 MB.

◄ Default recommended for this guest OS: 512 MB.

◄ Minimum recommended for this guest OS: 32 MB.

6. Power on the guest.
   a. Select TelePresence Conductor VM Guest.
   b. Select the **Console** tab.
   c. Right-click on the TelePresence Conductor VM Guest and select **Power > Power On**.
   d. Wait for console to show the login: prompt.
7. Check that other configuration requirements (for example, number of CPUs, disk space allocation, version of ESXi) are correct.

Document revision history

The following table summarizes the changes that have been applied to this document.

Date	Description
January 2015	Republished for XC3.0 release.
September 2014	Republished for XC2.4 release.
April 2014	Republished for XC2.3 release.
October 2013	Republished for new product activation process.
August 2013	Republished for XC2.2 release.
August 2013	Re-added the minimum specifications and modified the minimum processor specifications.
May 2013	Added a link to Cisco docwiki for hardware requirements information. Clarified use of vMotion if a move is required. Restructured the "Additional information" section to contain details on upgrading, clustering and migrating from a physical appliance.
February 2013	Information on .ova file usage and VM New Product Hold release process added.
December 2012	Updated for XC2.0 release
September 2012	Initial release.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.