Cisco TelePresence VCS Virtual Machine

Deployment Guide

VCS X7.2

D14951.06

October 2013

Contents

Introduction

Cisco TelePresence Video Communication Server (VCS) is playing an increasingly important role in the deployment of video networks. Although the 1 U appliance provides a solid platform on which to run VCS, many companies now want to run VCS 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 VCS
- how to load the VCS .ova installation file
- how to install a VM
- how to troubleshoot the system, when there are issues

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

Why does the VM .ova file specify "use .ova for initial VM install only"?

The VM VCS 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 VCS, follow the procedure under Upgrading a VM VCS [p.16], using the .tar.gz version of the VCS software.

After installation we recommend that you take a snapshot of the VM VCS (see Snapshot and restore using VM snapshot [p.13]) 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.

How do I get release keys and license keys for my VM VCS?

Licenses can be obtained after the VM VCS is installed, using the serial number of the VM VCS. The serial number is available from the **Option key** page and from the footer of the VCS web interface.

For full details on obtaining your release and license keys, see Appendix 2 — VM Cisco TelePresence Video Communication Server activation process [p.22].

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 VCS version X7.2. The minimum requirements for future VCS software releases may differ and you should refer to the release notes or administrator guide to ensure that pre-requisites are met.

Requirements

Recommended platform

See http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_TelePresence_Video_Communications_Server 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 VCS has been moved to the Automatic startup section
- your UCS system is configured with RAID 5

Co-residency support

The VCS 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 (2 cores required per VM VCS)
- 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 VM; it assumes that you are using vSphere.

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 VCS.

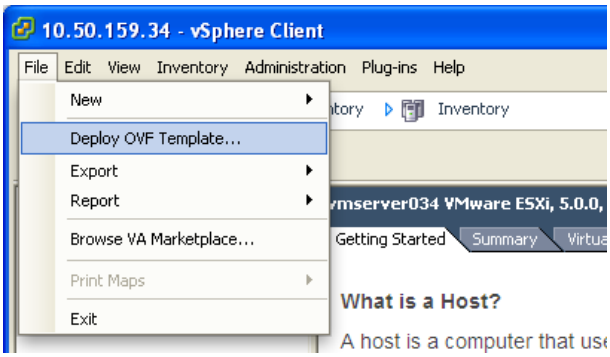
1. Select the host.
2. Go to the **Configuration** tab.
3. Select **Time configuration**.
4. Select **Properties**.
   If the date and time were red on the previous page, set the date and time manually to the current time.
5. Click **Options**.
6. Select **NTP Settings**.

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**.

Deploying OVA to host

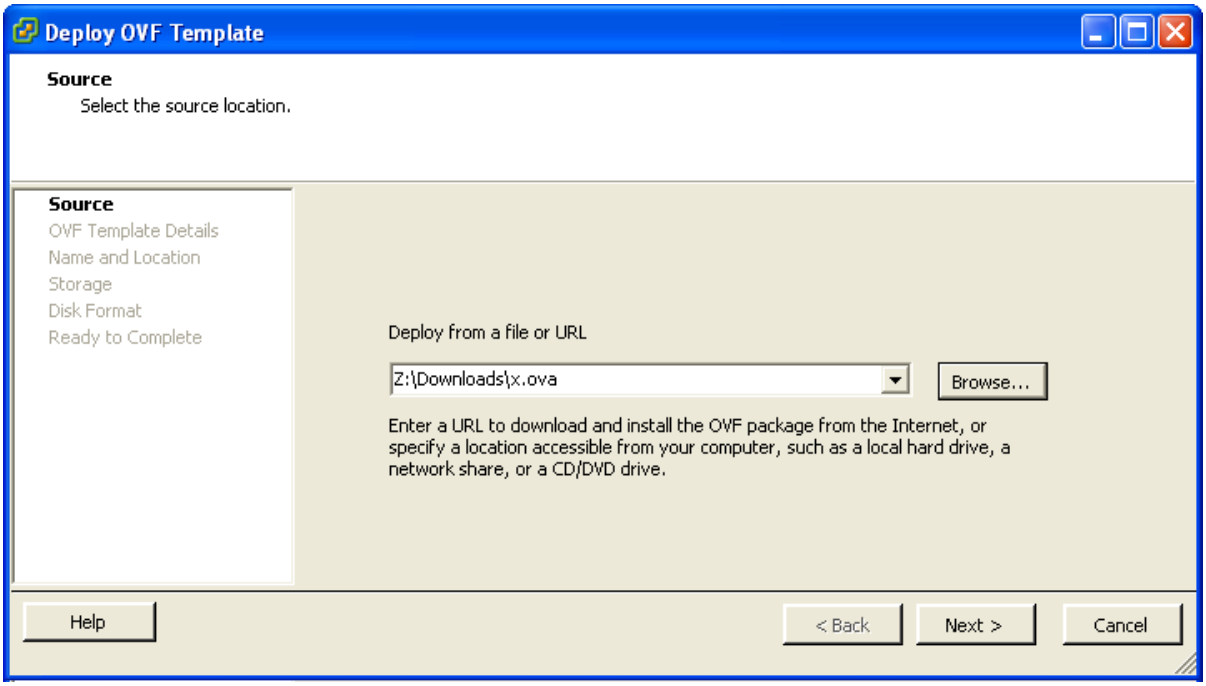
These instructions represent a typical installation. The Deploy OVF Template wizard dynamically changes to reflect host configuration.

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 (for example, s42700x7_2_0_BE6K.ova).
   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 vSphere to access the ESXi Host.
3. Select **File > Deploy OVF Template**.

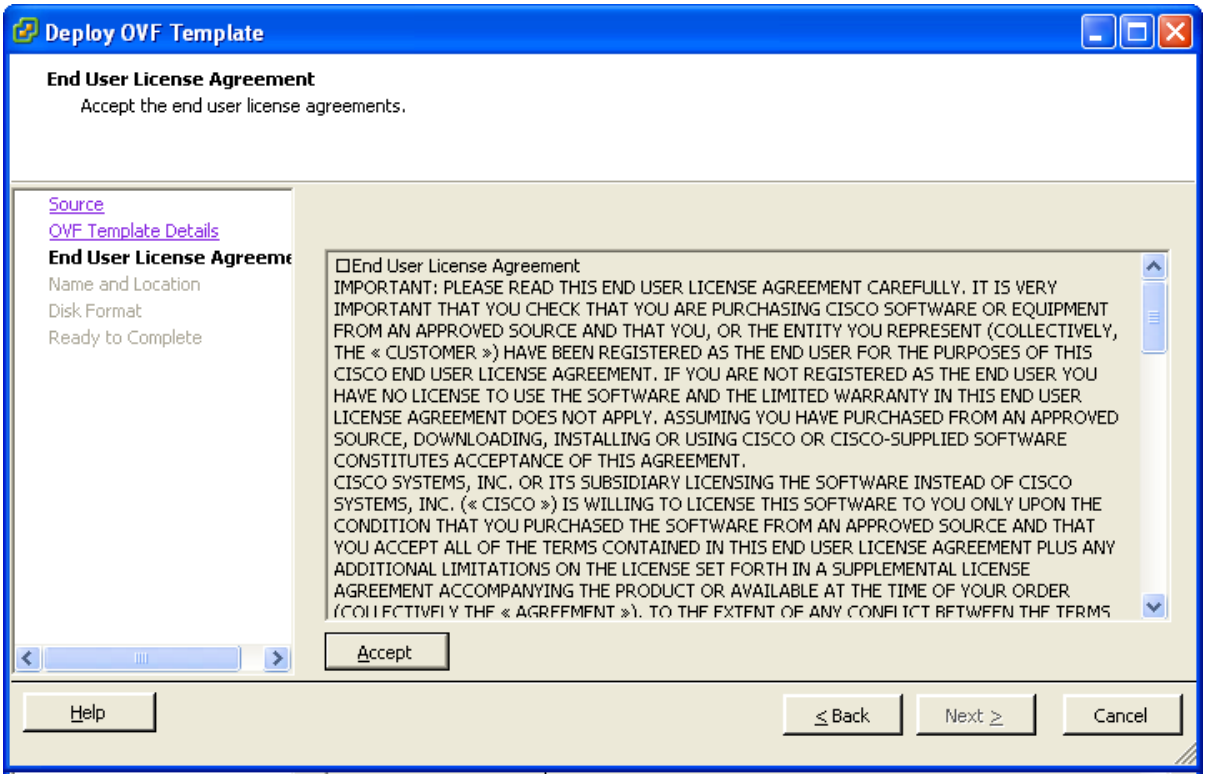


4. Select **Source** and then specify where the .ova file is located:
   - If the .ova file is already preloaded onto the ESXi Host datastore, paste the URL you copied from step 1 above.
   - If the .ova file is not preloaded on the datastore, **Browse** to the location of the .ova file.

5. Click **Next**.
   If the .ova file is already preloaded onto the datastore,you may have to re-enter username and password credentials so that vSphere client can access the web server.

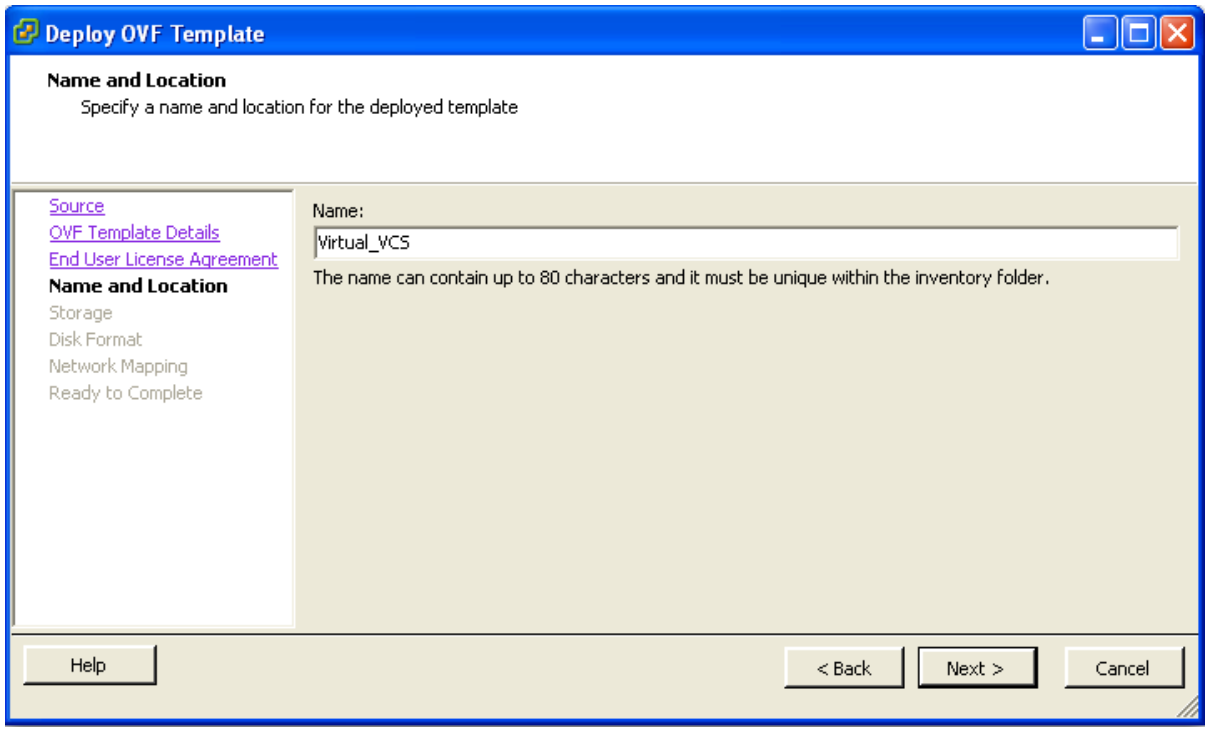


6. On the **OVF Template Details** page click **Next**.
7. On the **End User License Agreement** page read the EULA.

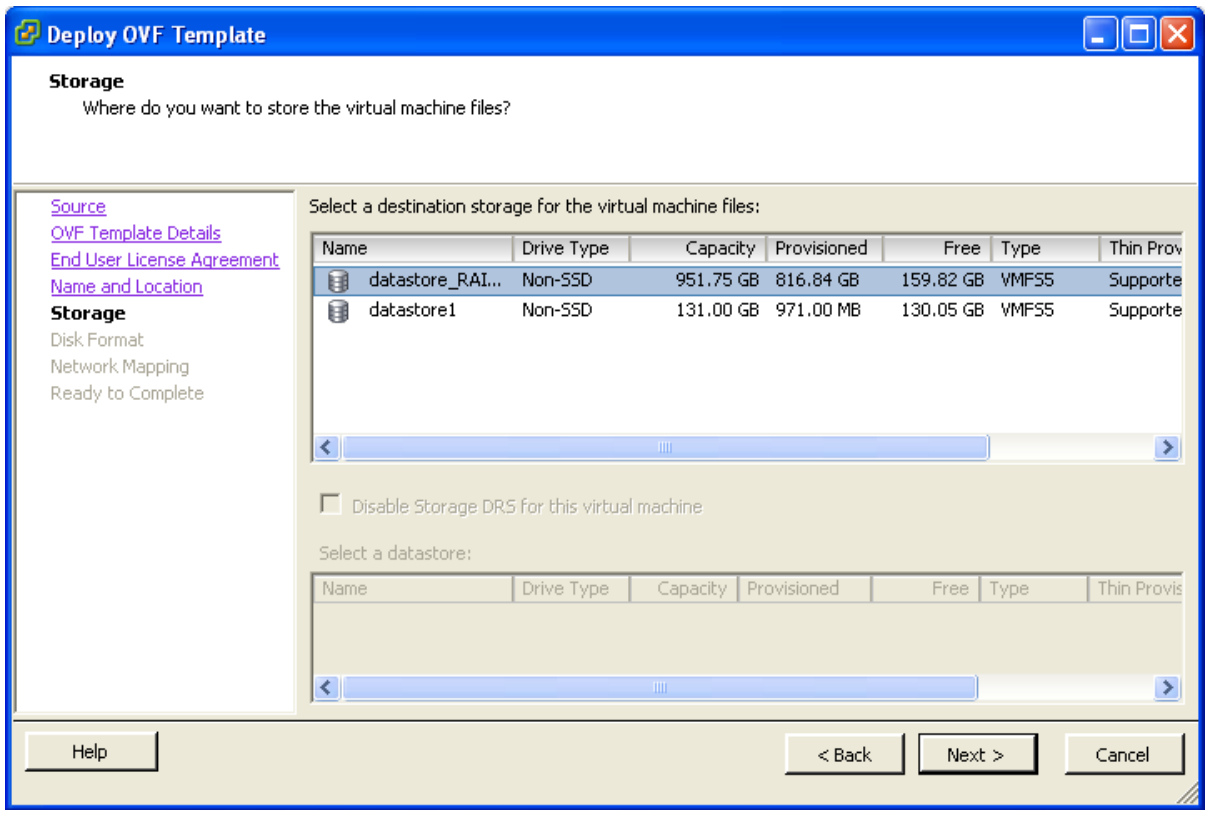


8. If you accept the EULA, click **Accept** then **Next**.

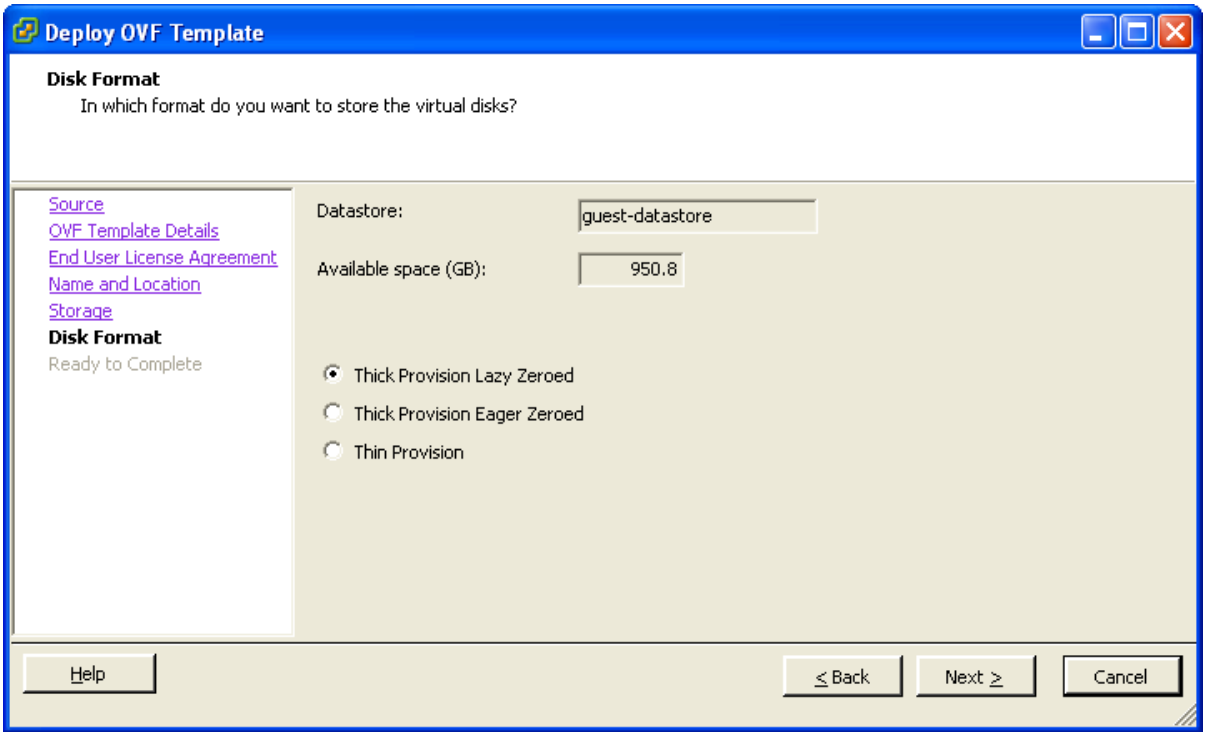
9. On the **Name and Location** page enter a **Name** for this VCS VM guest, for example "Virtual_VCS".



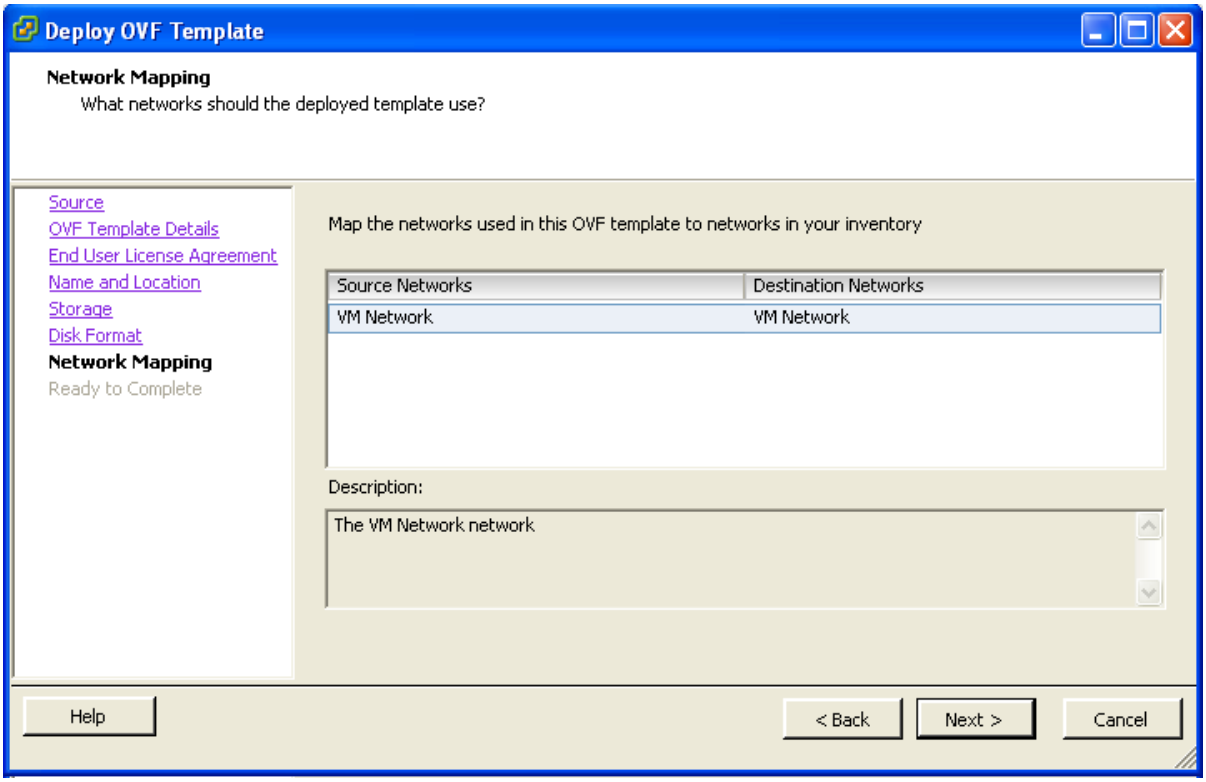
10. On the **Storage** page, select the datastore onto which the VCS VM Guest will be deployed and then click **Next**.



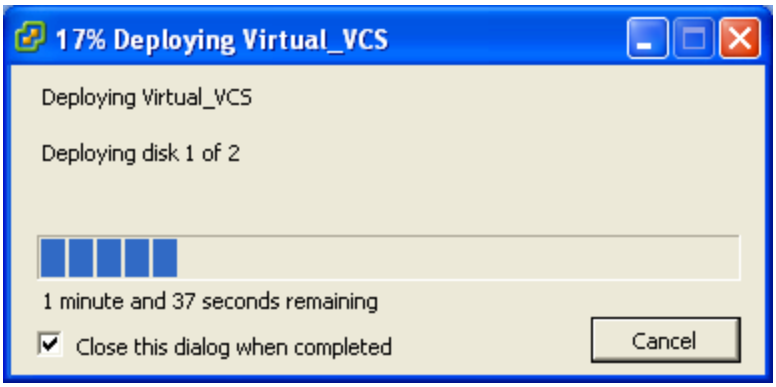
11. On the **Disk Format** page, ensure that the default disk format of **Thick Provision Lazy Zeroed** is selected and then click **Next**.
    Note that **Thin Provision** is not supported as VM performance may degrade during resizing of a partition.



12. If listed, configure **Network Mapping** and select the network mapping that applies to your infrastructure and then click **Next** (default is **VM Network**).



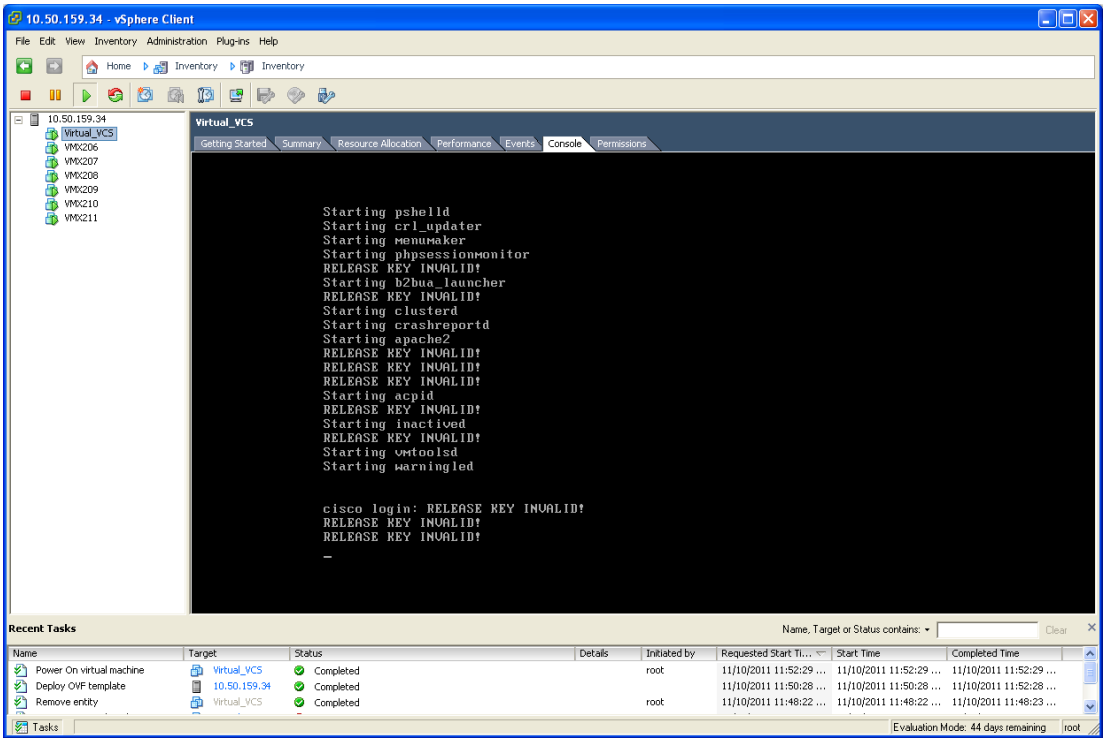
13. On the **Ready to Complete** page confirm Deployment Settings.
14. Select the **Power on after deployment** check box.
15. Click **Finish**.



The VCS OVA is now deployed as a Guest on the VM Host.

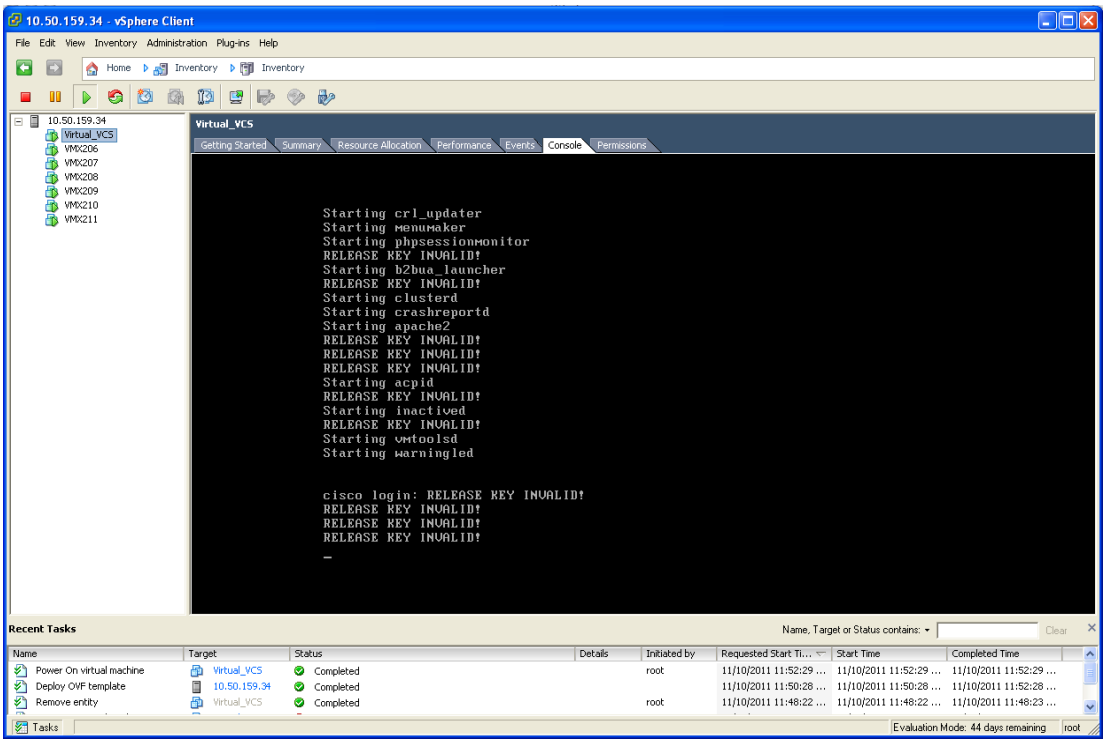
Configuring the VM guest

1. Either:
   - Select the VM guest and then select the 'Console' tab, or
   - Right-click on the VM guest and select 'Open Console'.

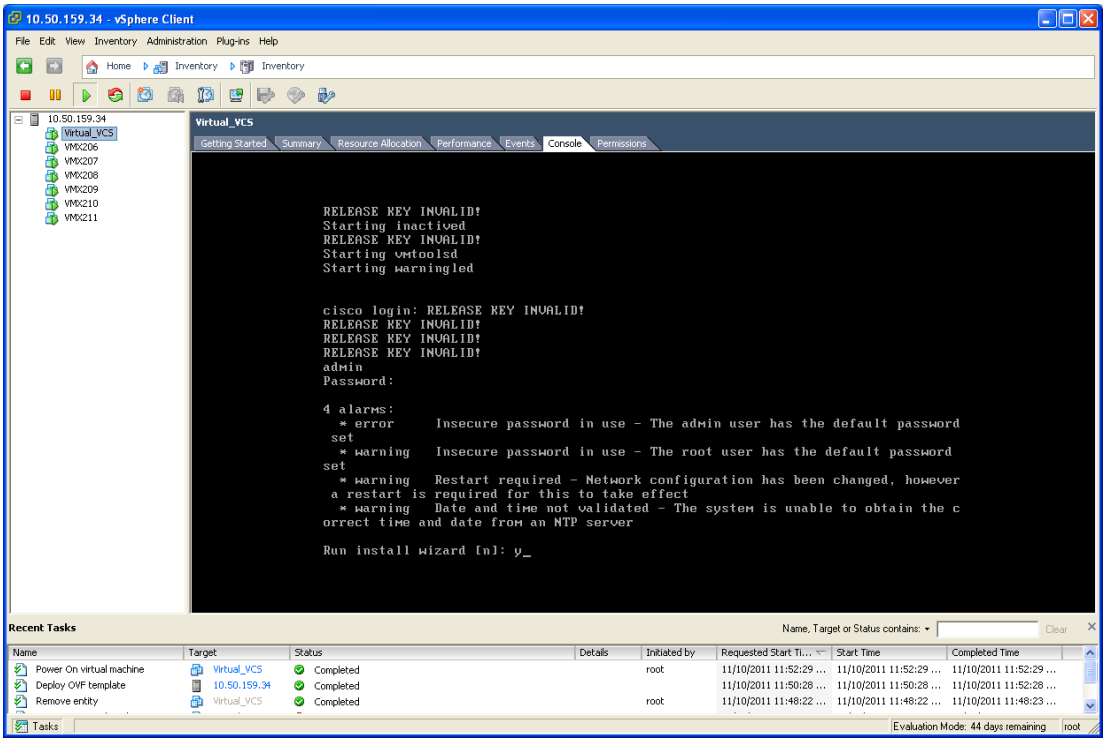


2. The VM guest will take some time to boot, create its second hard disk partition and then reboot to a login prompt.

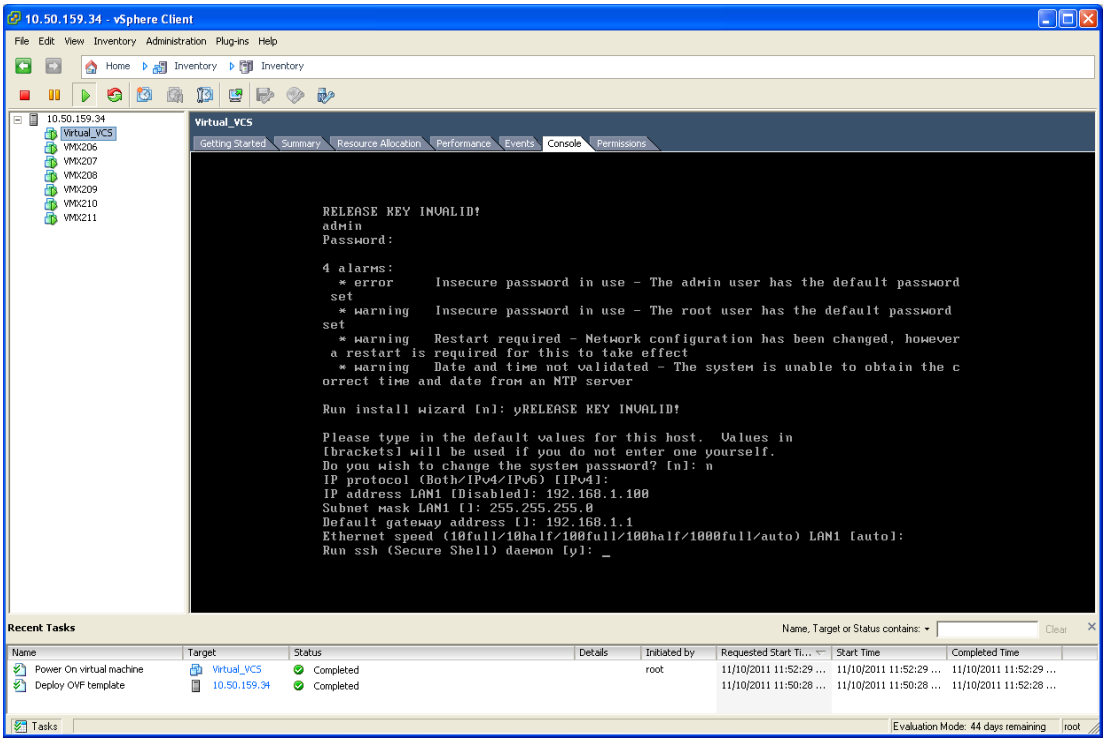
3. At the login prompt enter 'admin' for the username and 'TANDBERG' for the password.



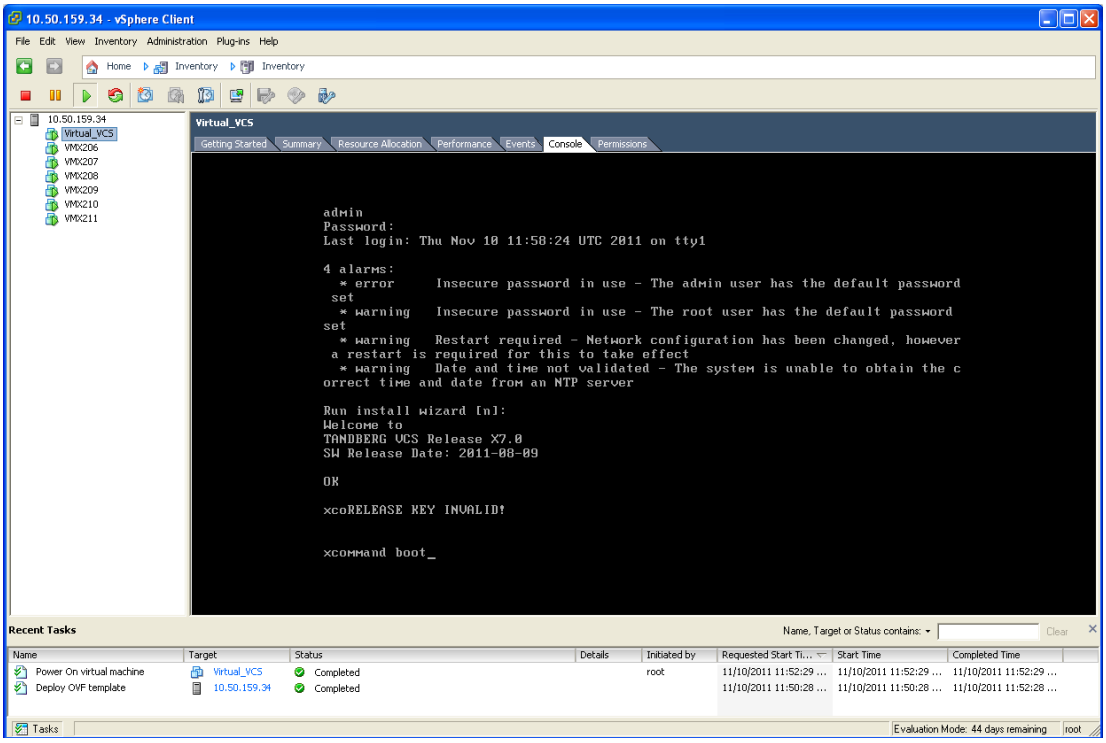
4. At the Install Wizard prompt type y and then press Enter.



5. Follow the Install Wizard to enter IP information. (Defaults can be entered by pressing Enter at the prompt.)



6. At the end, the configuration is applied and the VCS logs you out.
7. Log back into the VCS as admin and then type **`xcommand boot`** to reboot the VM guest.



8. You should now be able to access the VCS via a web browser.
9. Click Administrator Login and log in as admin.

10. Get release and option keys:
    a. Go to the **Option keys** page (**Maintenance > Option keys**).
    b. Copy the **Hardware serial number**.
    c. Use this serial number to order release and option keys for this VM VCS.
    For full details on obtaining your release and option keys, see Appendix 2 — VM Cisco TelePresence Video Communication Server activation process [p.22].

When the release and option keys are available:

1. Click **Administrator Login** and log in 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 VCS 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 VCS, including changing any default passwords, configuring DNS, NTP, zones, search rules and so on as required.
    Follow the *Cisco VCS Basic Configuration (Single VCS Control) Deployment Guide* or a similar deployment guide to guide you through configuring this VM VCS ready for operation.
5. After the VCS has been configured it is good practice to backup the VCS configuration using the VCS backup facility, and also to take a VM snapshot (see Snapshot and restore using VM snapshot [p.13]). 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.

Snapshot and restore using VM snapshot

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 VCS backup – the VCS 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 VCS has little activity going on – performing the snapshot will degrade the performance of the VM.

Note that 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 VCS to a new host you must perform a host migration via vMotion.

Creating a VMware snapshot

We strongly recommended to perform a VMware snapshot when there are no calls in progress to ensure reliability.

1. Select the relevant VCS VM Guest.
2. Right-click the VCS 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 VCS VM Guest.
2. Right-click the VCS 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 VCS has no physical serial interface; the serial interface is accessible through the console tab of the VM guest.

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

VM VCS allocates 3 virtual NICs:

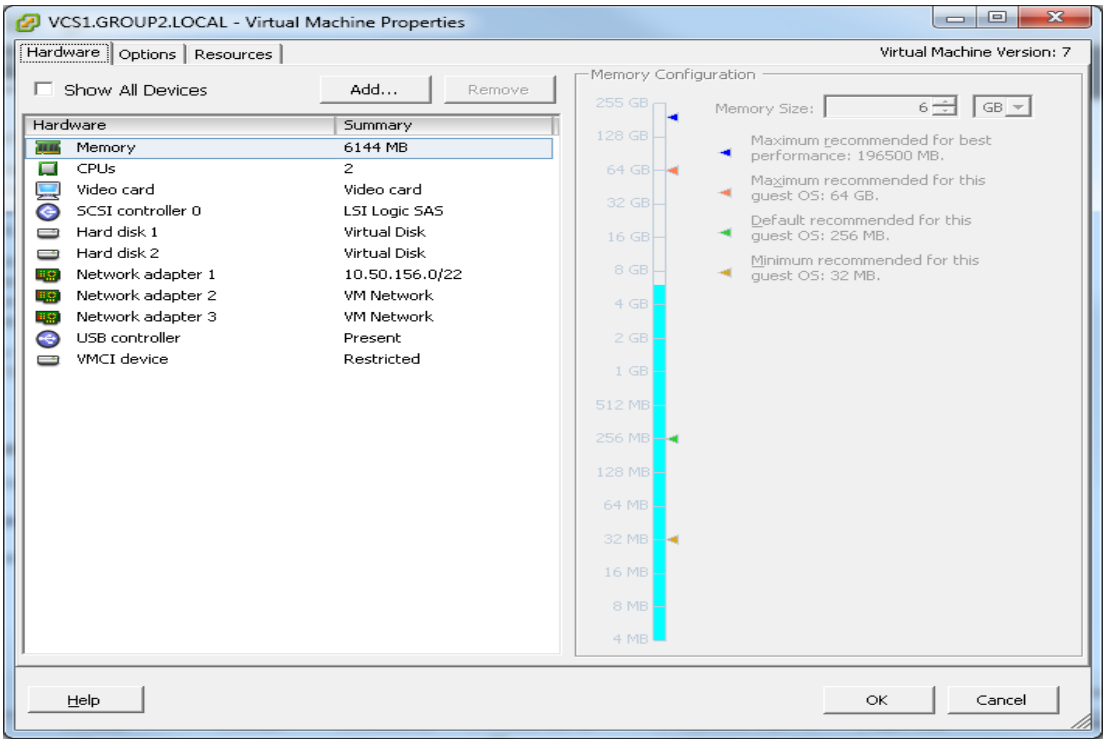
- the first is used for the standard LAN 1 interface
- the second is used if Dual Network interfaces is enabled (LAN 2)
- the third is reserved for future use

Allocating a virtual NIC to a physical NIC interface

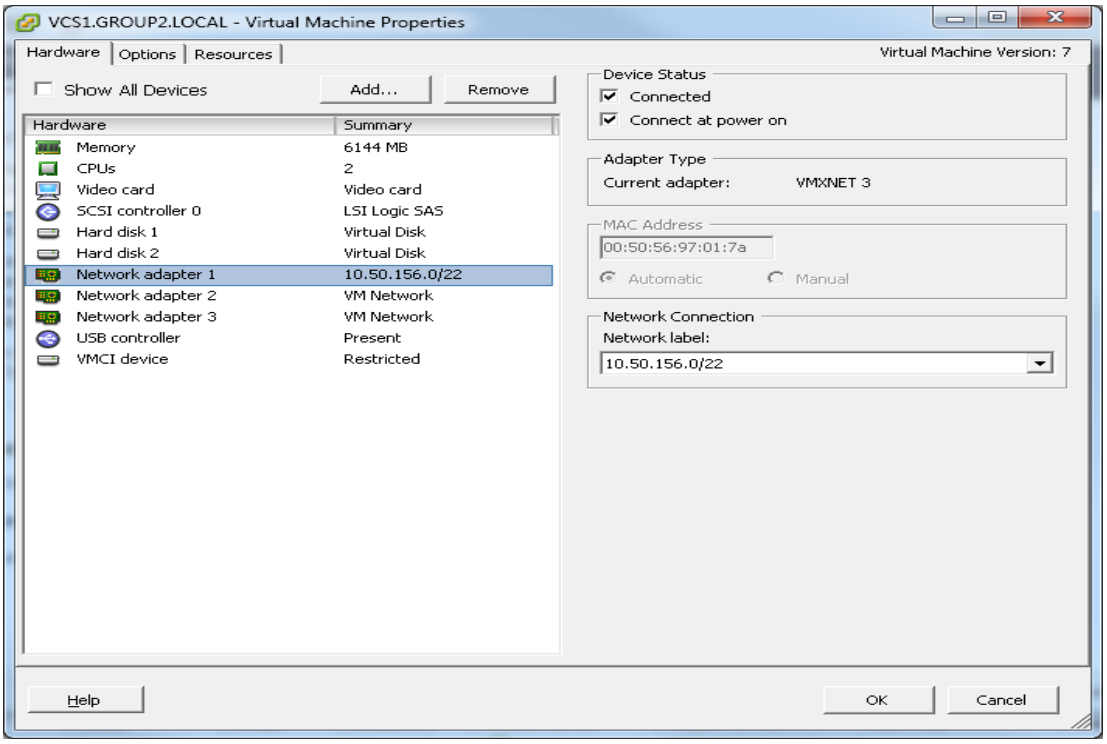
Virtual NICs can be assigned to physical interfaces as follows:

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 VCS 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…**



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



7. Select the appropriate Network label (Virtual Machine Port Group) to associate the VCS LAN interface with the required physical NIC.
8. After a few seconds the VCS will be able to communicate over the physical interface.

Additional information

Upgrading a VM VCS

You upgrade a VM VCS in the same manner as you would upgrade a non-VM VCS (using the .tar.gz file, not a .ova file):

1. If the VCS is part of a cluster or is using provisioning or FindMe, follow the relevant VCS Cluster deployment guide.
2. If the VCS is not part of a cluster and is not using provisioning or FindMe:
   a. Log in to the VCS VM web interface as an admin user.
   b. Backup the VCS from the **Backup** page (**Maintenance > Backup and restore**).
   c. Upgrade the VCS from the **Upgrade** page (**Maintenance > Upgrade**).

Clustering for resilience and capacity

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

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

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

For more information on clustering VCSs, see Cisco VCS Cluster Creation and Maintenance Deployment Guide.

Migrating from a physical appliance to a VM

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

Supported features

vMotion

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

There may be glitches (packet loss/jitter) in media for calls that are interworked by VCS as the VM is moved. We recommend that a vMotion move is carried out when there is low call activity on the VM VCS.

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 VCS uses dual cores).

Licensing

VM VCSs require licensing in the same way that the appliance VCS units require licensing.

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

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 VCS 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 volume that is storing the database files to ensure correct operation of the database.
   If there is not adequate space available on the physical volume that stores the database files, free up disk space.
   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
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 VCS application to fail.
vCenter Server	If vCenter is not operating properly, even though the VM VCS application is still up and running, you may lose connection to the VM VCS 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.

VCS application fails to start

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

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

Configured NTP does not work

For NTP to work on VCS, 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 VCS 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 a VCS 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 VCS 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 a VCS. This reinstalls the VCS software image and resets the configuration to the functional minimum.

Prerequisite files

The `factory-reset` procedure described below rebuilds the VCS 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. In such a case, to use this procedure, 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 or via a direct connection to the appliance with a keyboard and monitor. 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 VCS 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.

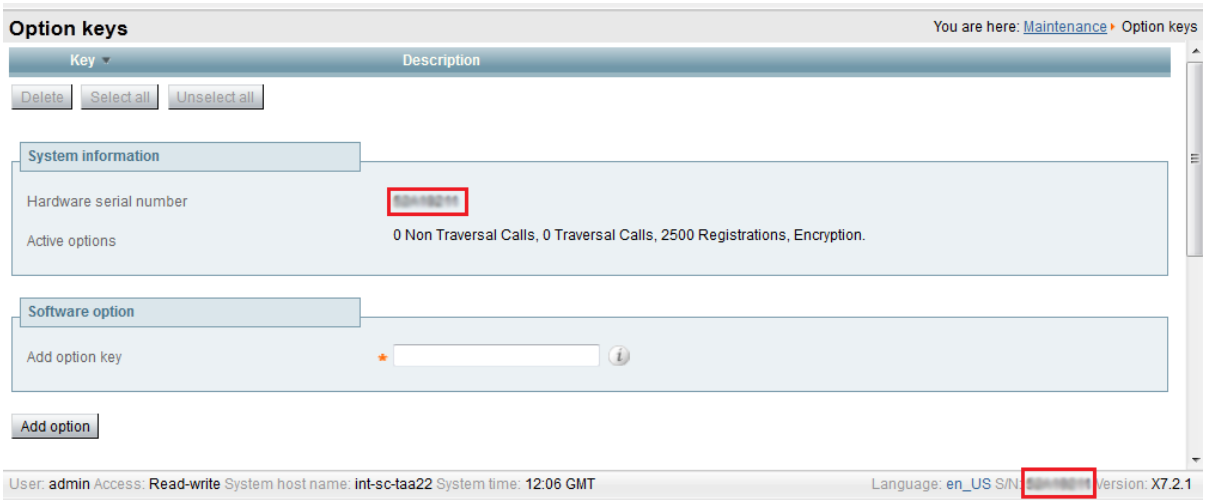
Prompt	Recommended response
Keep option keys [YES/NO]?	YES
Keep IP configuration [YES/NO]?	YES
Keep ssh keys [YES/NO]?	YES
Keep ssl certificates and keys [YES/NO]?	YES
Keep root and admin passwords [YES/NO]?	YES
Save log files [YES/NO]?	YES
Replace hard disk [YES/NO]?	NO

4. Finally, confirm that you want to proceed.

Appendix 2 — VM Cisco TelePresence Video Communication Server activation process

Follow this procedure to activate your Cisco TelePresence Video Communication Server software.

1. Ensure you have downloaded and installed the virtual VCS software before attempting to register your Product Authorization Keys (PAKs) that you will have received via email. The VCS software can be downloaded from http://software.cisco.com/download/navigator.html.
2. After the VM VCS 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 VCS web interface.



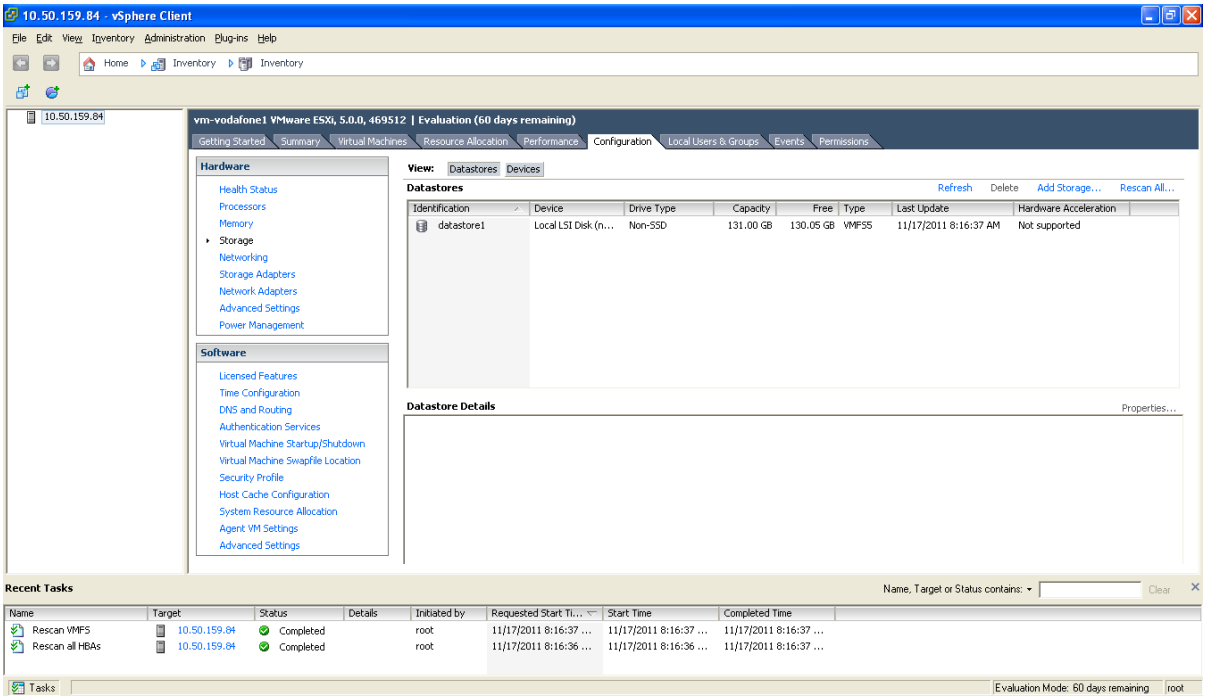
3. Register your software and feature PAKs at the customer licensing portal to retrieve your **Release** key and any relevant **Option** keys:
   a. Go to www.cisco.com/go/license and sign in.
   b. If necessary, click **Continue to Product License Registration**.
   c. Follow the onscreen instructions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

Appendix 3 — Deploying multiple datastores

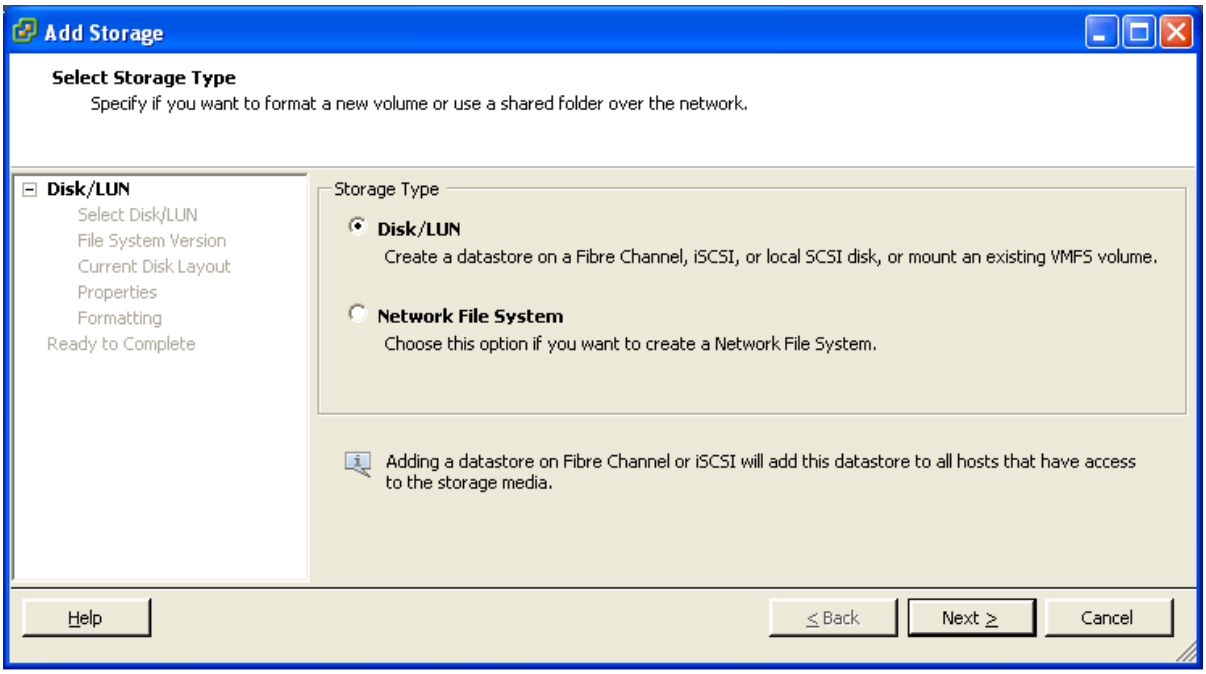
This process should be carried out during the initial build of the VM host, if the VM host has two or more RAID arrays of disk storage. This configuration enables vSphere / vCenter to know about all the datastores.

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

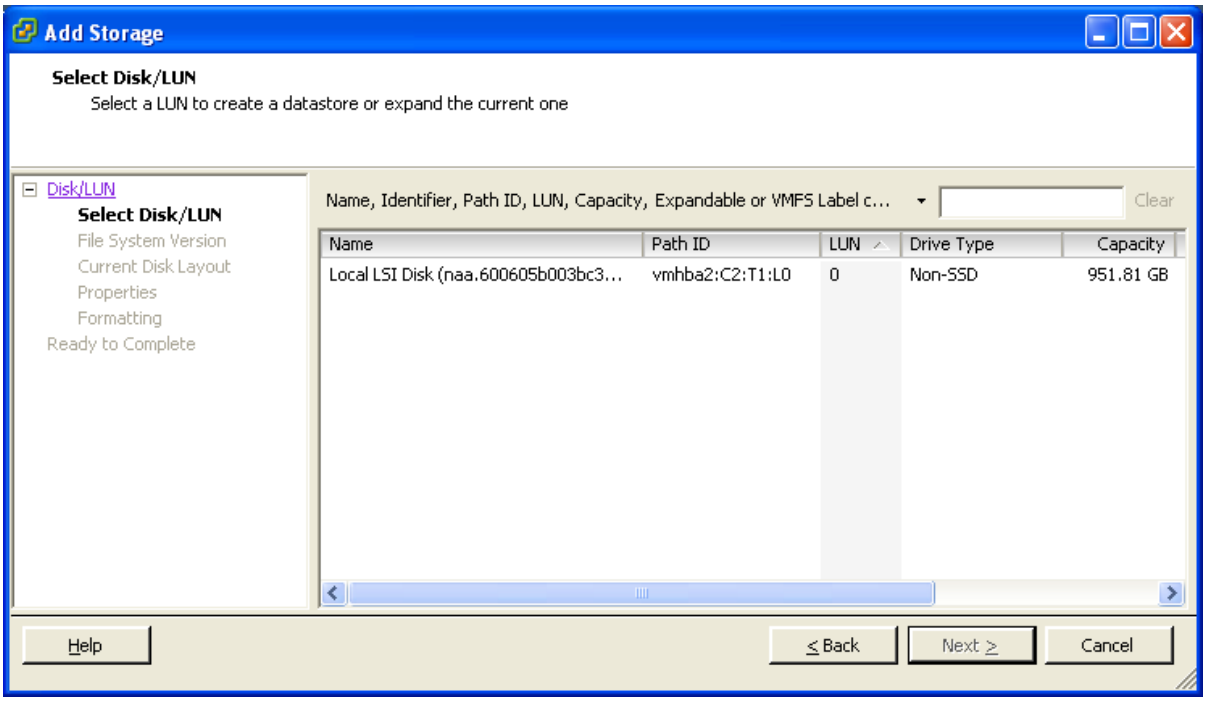


4. Select **Add Storage …** (on the right hand side window).

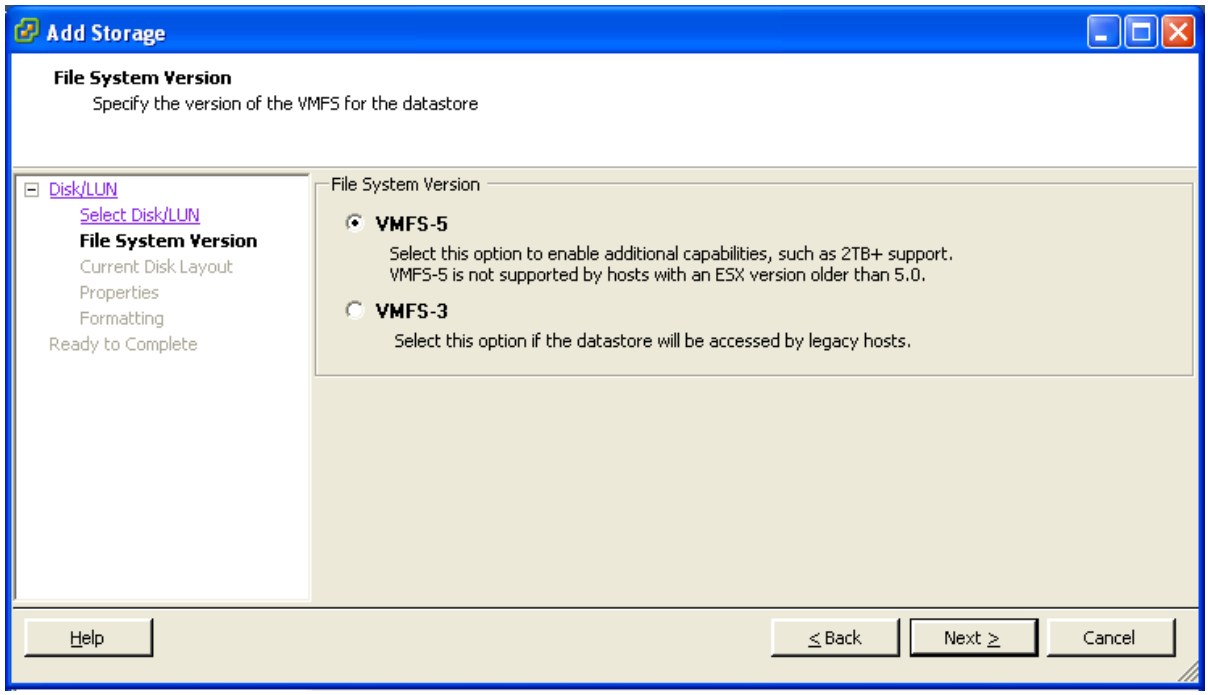
5. Select **Disk/Lun** and click **Next**.



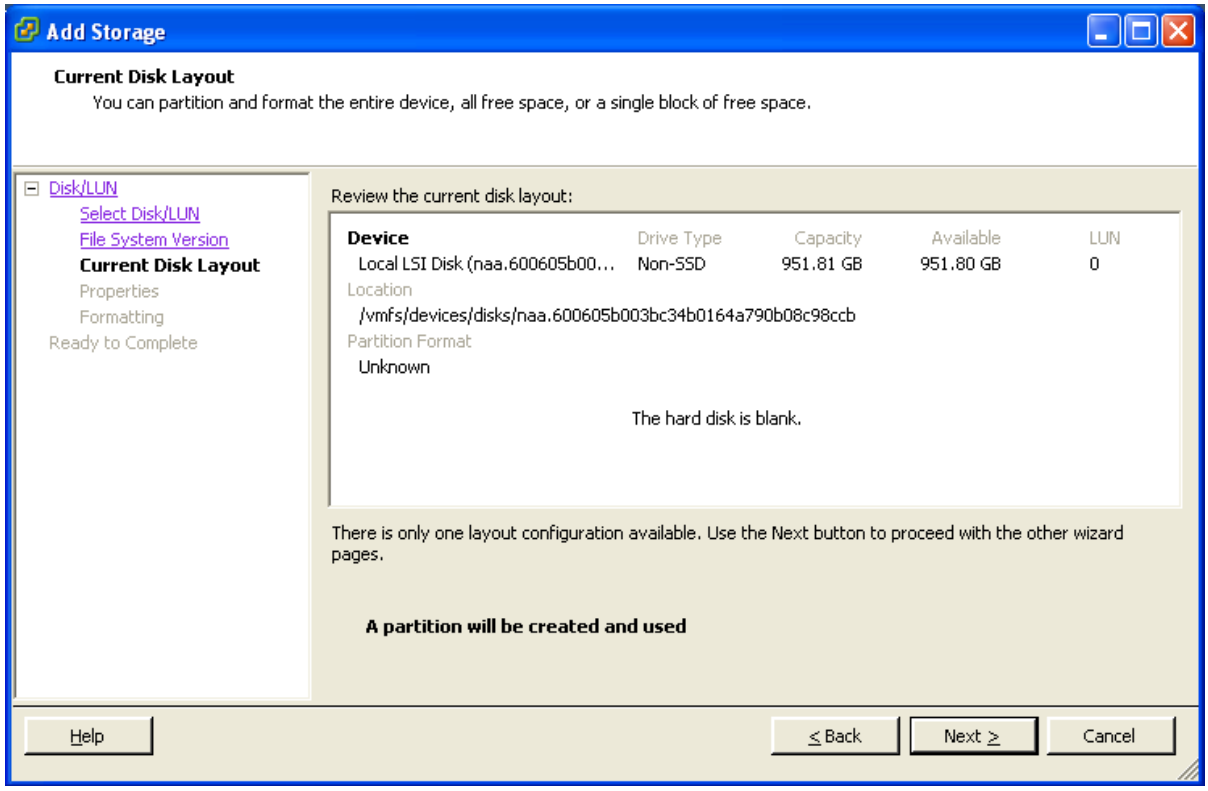
6. Under **Disk/LUN** select the required Disc/LUN from the list presented and click **Next**.



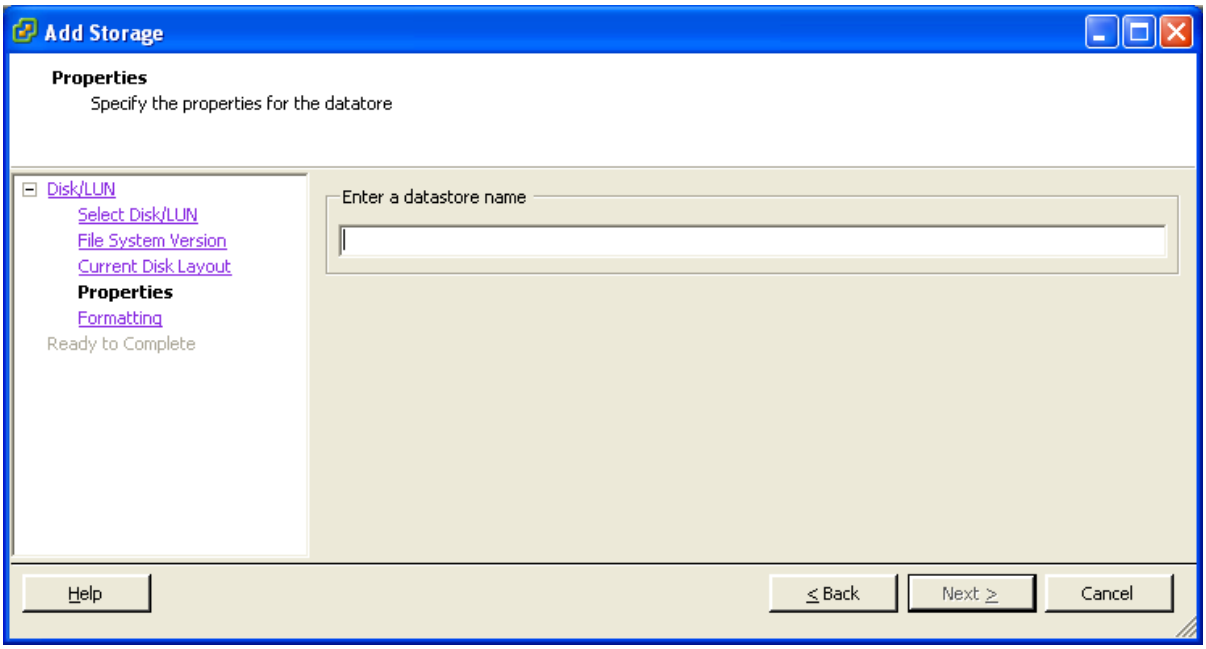
7. On the **File System Version** page select **VMFS-5** and then click **Next**.



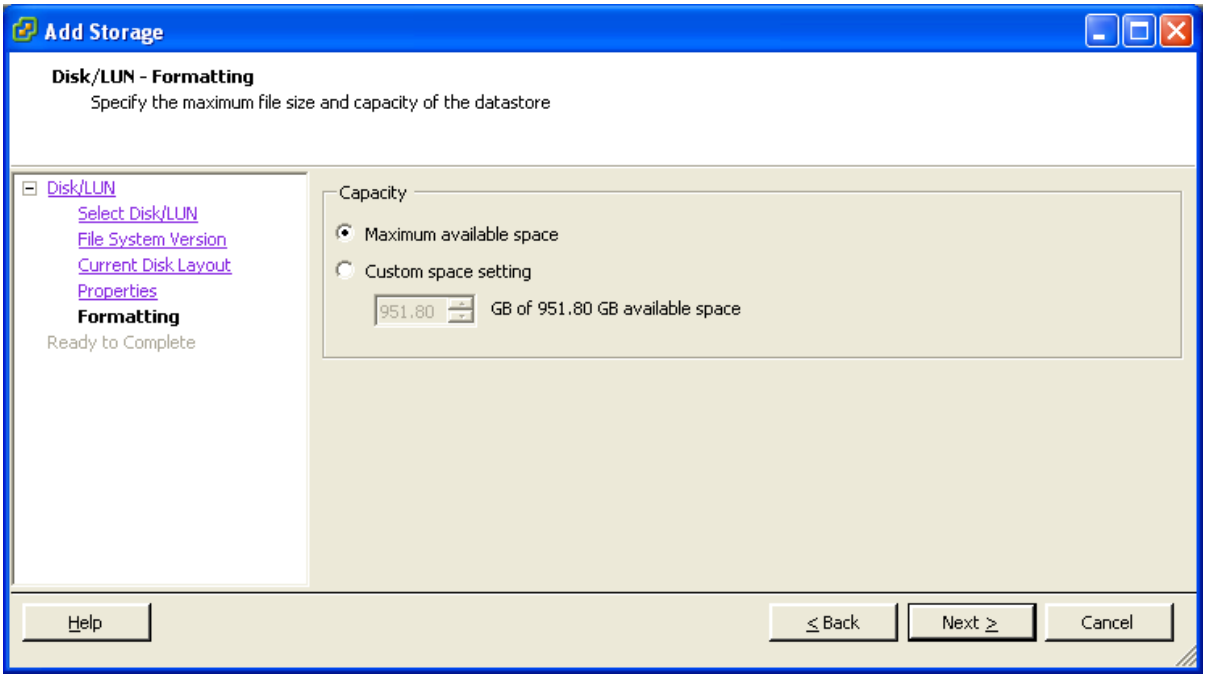
8. On the **Current Disk Layout** page verify the details and then click **Next**.



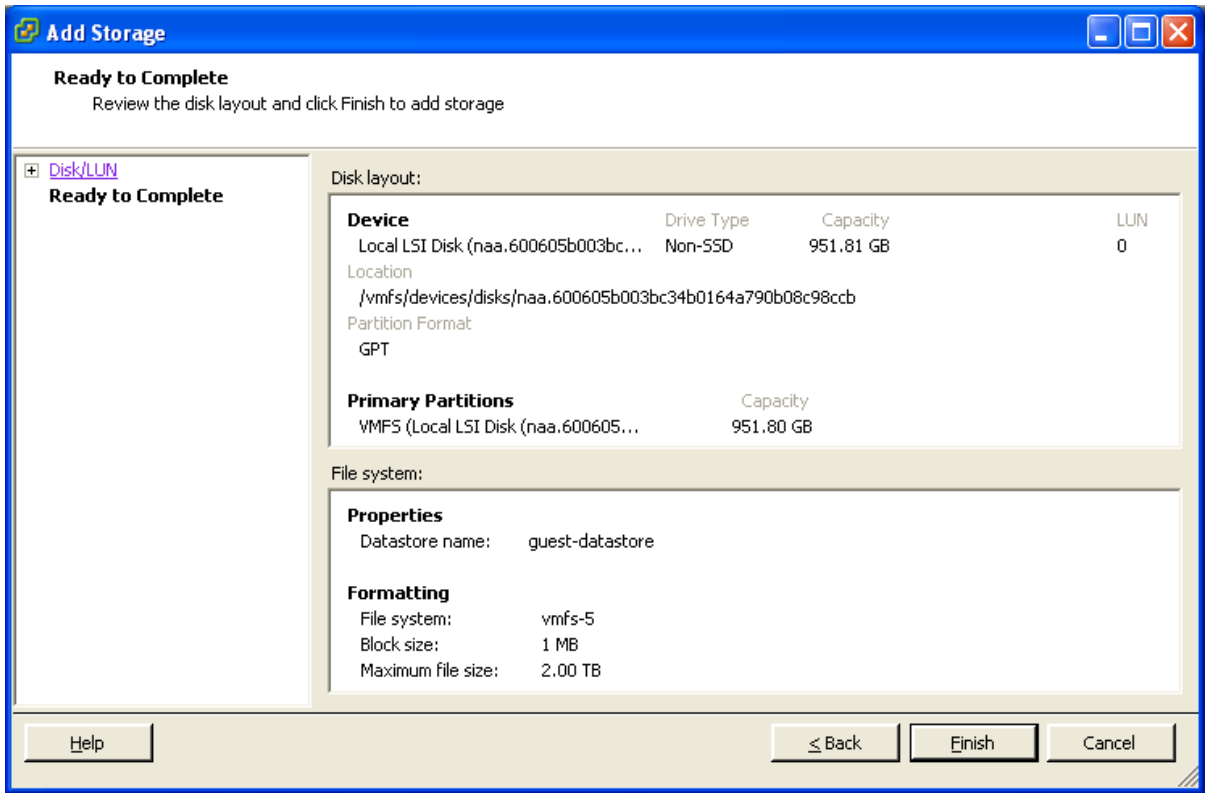
9. On the **Properties** page enter a name for the new datastore and then click **Next**.



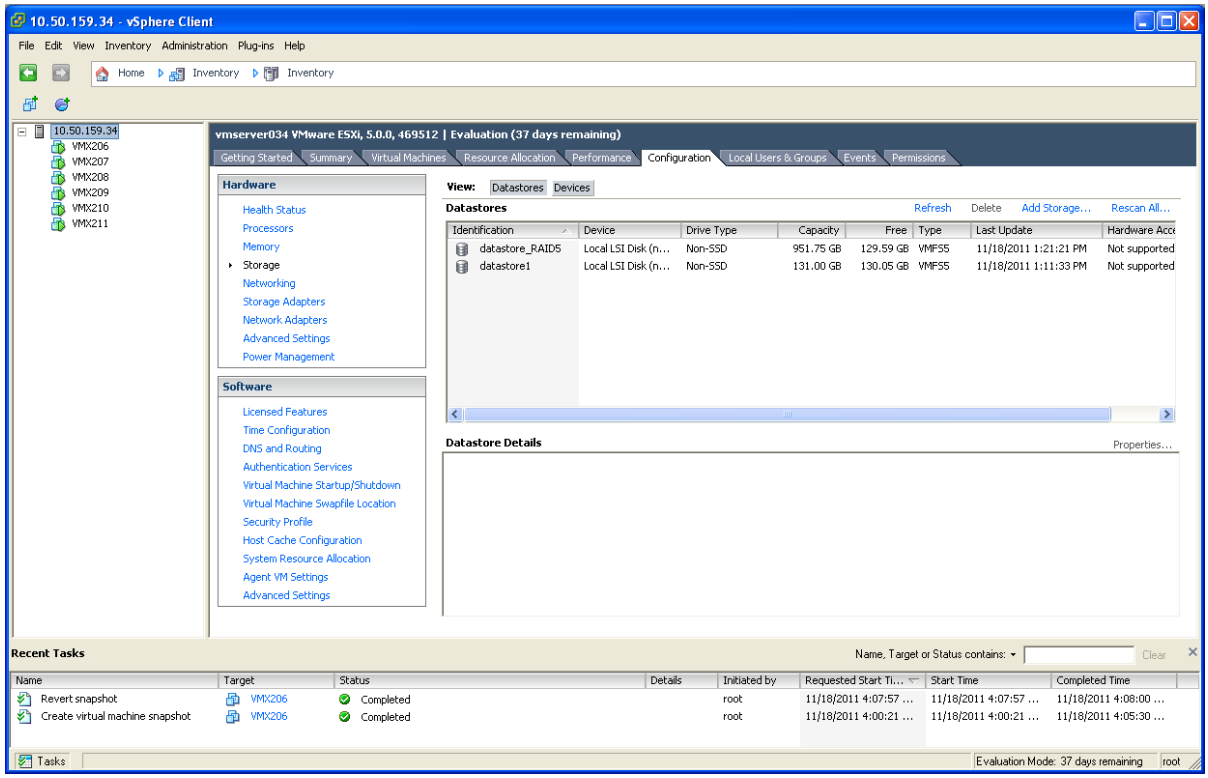
10. On the **Formatting** page select **Maximum available space** and then click **Next**.



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



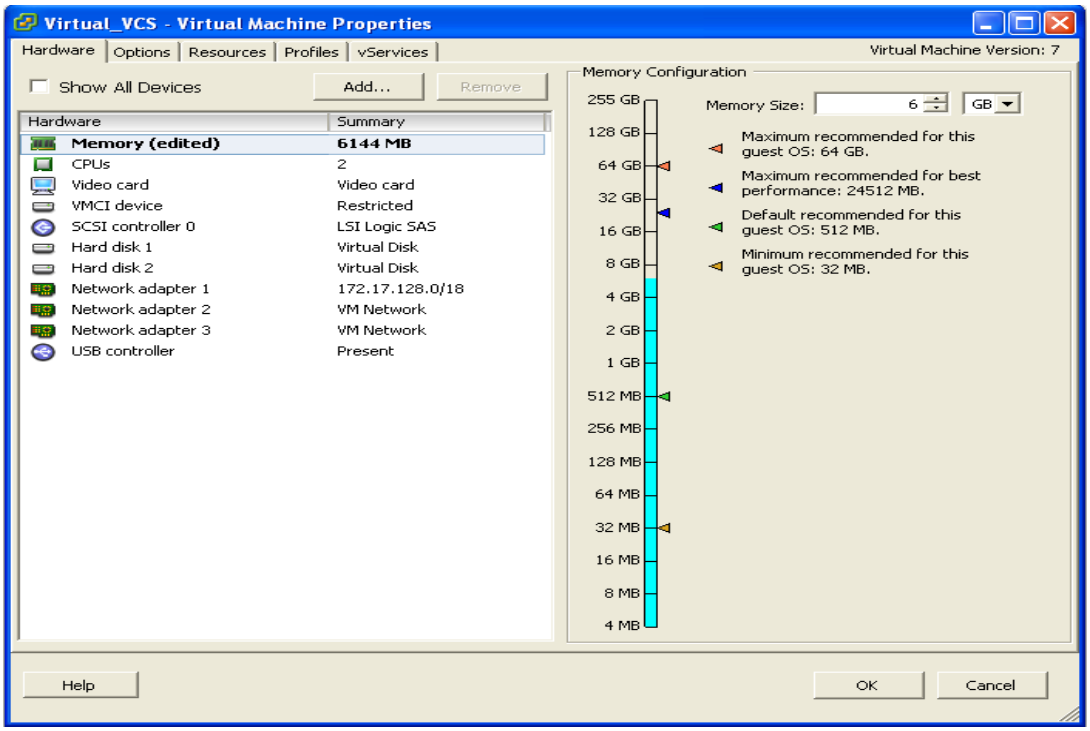
12. Wait for the Create VMFS Datastore task to complete.
13. On completion, the new datastore will be listed under the **Storage** section.



Appendix 4 — Ensuring that 6GB of memory is allocated for the VM VCS

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

1. Power off the guest:
   a. Select VCS VM Guest.
   b. Select the **Console** tab.
   c. Right-click VCS 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 VCS 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**.



6. Power on the guest.
   a. Select VCS VM Guest.
   b. Select the **Console** tab.
   c. Right-click on the VCS 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.

Revision	Date	Description
6	October 2013	Republished for new product activation process.
5	May 2013	Added a link to Cisco docwiki for hardware requirements information. Clarified use of vMotion if a move is required. Added instructions for deploying an .ova file that is already preloaded onto the ESXi Host datastore. Referred to the new Compliance Hold release process. Restructured the "Additional information" section to contain details on upgrading, clustering and migrating from a physical appliance.
4	February 2013	Information on .ova file usage and VM New Product Hold release process added.
3	November 2012	Restoring default configuration (factory reset) procedure updated.
2	July 2012	Troubleshooting section updated.
1	March 2012	Initial release.