

VMware Server 2.0 Tips and Tricks

Check for the latest version of this document at <http://communities.vmware.com/docs/DOC-9394>.

This is not an official VMware document – it was written by an enthusiast to assist other enthusiasts.

It does not replace VMware documentation which should still be consulted.

Before you install

1. The release notes detail various issues you may come across during installation so definitely read before installing - http://www.vmware.com/support/server2/doc/releasenotes_vmserver2.html
2. Similarly, reading the user guide is a necessity, particularly if you have not used virtualisation before - http://www.vmware.com/support/server2/doc/releasenotes_vmserver2.html
3. Server 2.0 is an application that sits on top of an existing operating system – either Windows or Linux. This is called the host. If you want a bare metal hypervisor, so will only run virtualisation; consider ESXi which is free also but be advised that the hardware compatibility list for ESXi is quite short.
4. You will need administrative rights to install it and subsequently for the initial logon to the management interface but you can then grant granular permissions to other users/groups.
5. Where are you going to store your Virtual Machines – since Server 2.0 does not use linked clone technology as found in Workstation then you will need up to the full size of your disk (e.g. 4GB+ for XP) per VM although the use of expanding disks means that the disk only takes the space it needs but will be slightly slower than a disk that is allocated to its full size when it is created.
6. Note that FAT32 file systems have a maximum single file size of 4GB so if your virtual disk (a .vmdk file or files) is going to be bigger than this you will need to select the option to split it into 2GB chunks.
7. VMware provides virtual hardware inside the VM – it does not map through your physical hardware on the host so PCI cards and the like will not be available in the guest. The same is obviously true of the host's graphics card.
8. USB devices on the host can be mapped through to the guest and Server 2.0 supports USB 2.0.
9. The host's serial and parallel ports and sound card can be mapped through to the guest although the sound card will be virtualised to a Creative SoundBlaster.
10. Server 2.0 stores VMs in datastores – a default datastore is created which is called “[standard]” and will map to the root of the folder you select during installation.
11. VMs can be run from external USB drives by defining a datastore for the mount point.
12. Remote datastores can also be added – NFS for Linux hosts and CIFS/SMB for Windows.

13. If you have a 64 bit host and want to run 64 bit guests, test that VMware can run 64 bit guests first with the checker tools found at the following URL since BIOS settings/limitations can mean a 64 bit processor is unable to run 64 bit VMs - http://www.vmware.com/download/server/drivers_tools.html
14. There is no “shared folders” or “drag’n’drop” feature to provide file transfer between host and guest as is found in Workstation – instead use regular SMB/CIFs between Windows host and Windows guest or Samba on Linux host/guest. Alternatively, use the rdesktop Linux RDP client with client mapped drives via the “-r disk:” option.
15. For Linux hosts, you do not need to have X or any window managers installed but obviously you will have to manage it remotely which is easy enough as long as you configure your firewall accordingly.
16. You can only have one VMware virtualisation product installed on the host at any one time. This also includes the VMware View client with offline desktop since it also includes a virtualisation engine.

Installation

1. If you get policy errors on Windows, try renaming the registry keys HKLM\Software\Policies and HKCU\Software\Policies. If you cannot rename them then you do not have sufficient privileges to install VMware anyway.
2. If you get early installation errors on Windows, run the package with the /l option and the name of a log file as an argument (e.g. “/l c:\server2install.log”) and then look in this log file for clues after the installation has failed.
3. If the Windows installation fails before a log file is generated as above, perform an administrative installation via the /a option which will just extract the files to a folder you specify. Then run the following command and take a look at the log file:

```
Msixec /i "admin_install_folder\VMware Server.msi" /l*vx  
c:\server2install.log
```
4. On Windows, ensure you have installed the Visual C++ Redistributable Package for your architecture.
5. The tar file for Linux includes some symbolic links so check that your extraction mechanism creates these links properly, particularly “vmware-install.pl”. If this file is zero length then you have an extraction issue as it is a symbolic link to “vmware-uninstall.pl”.
6. For Linux you will need kernel headers and compilers to link a new kernel.
7. Do not install on a Linux host that already has a virtualisation product installed such as KVM, Xen, VirtualBox, etc as it will almost certainly not work.
8. After installing on Linux, you will need to run “/usr/bin/vmware-config.pl” in order to build kernel modules and configure the settings such as networking.
9. If Server 2.0 processes do not automatically start on Linux and you have correctly hooked in the /etc/init.d/vmware* scripts then try setting “RUN_PARALLEL=no” in /etc/sysconfig/boot.

10. If autorun for CD/DVD and USB stop working after installation, try setting the registry value “NoDriveTypeAutoRun” in key “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer” to 251 decimal.
11. Some Linux hosts give a warning that an older version of gcc is being used than was used to compile the kernel but this appears to be benign.
12. Some Linux hosts fail to compile the vsock module which results in the VMCI functionality not being available. This is only required if you will be using third party products that use VMCI which is VMware mechanism for faster communications between guests.
13. Install the licence you received after registration, and can retrieve from the VMware web site, to prevent expiration of the software.

Management

1. Unlike Server 1.0, Server 2.0 does not include a native management client.
2. Use a web browser (Firefox and Internet Explorer are the two officially supported ones) to connect to <http://yourserver:8222> or <https://yourserver:8333> if you selected the default ports during installation/configuration.
3. You will get a self-signed certificate error when using https since obviously VMware cannot ship a certificate from a trusted root for the FQDN of your server.
4. If you manage from a Windows client then the VI (Virtual Infrastructure) client is also available which is what is used to manage ESX/ESXi and Virtual Center too. It is available at <https://yourserver:8333/client/VMware-viclient.exe>.
5. The VI Client cannot edit virtual hardware greater than version 4 – the web ui creates virtual machines by default at version 7.
6. The VI Client cannot add USB devices to VMs running at hardware versions greater than 4 – version 7 is required for USB 2.0 support.
7. Specify yourserver:8333 for the connection in the VI Client.
8. The credentials you specify to logon are admin credentials that you would use on the host even without VMware installed – VMware does not introduce any credentials/accounts itself.
9. The admin account you use must have a password defined for it or you will not be able to login.
10. There have been some issues with authentication on Linux hosts which have been due to PAM (Pluggable Authentication Modules) issues which require config changes.
11. The remote console is a locally installed application which will be installed when the console tab is first clicked onto.
12. For remote management through firewalls, VPNs or over SSH tunnels, port 902 is also used as well as 8222/8333. Note that during Linux configuration; you may have selected a different port from 902 as sometimes it can be statically detected as being in use.

13. Although there is a file “/usr/bin/vmware” on Linux hosts, this is just a shell script wrapper for your browser to connect it to <https://127.0.0.1:8333>
14. For Windows VMs, you can enable Remote Desktop connectivity to the guest as you would for a physical machine.

Creating VMs

1. Please take a look at the “Guest Operating System Installation Guide” - http://www.vmware.com/pdf/GuestOS_guide.pdf
2. You will need bootable media either physical CD/DVD or ISO images.
3. Check installation media is bootable outside of VMware.
4. Make sure you set the CD drive to be connected at boot.
5. Using ISOs is much faster than physical media and means you can keep a library of them on disk. There are free tools available for creating bootable ISOs from physical media.
6. VMs will PXE boot if required which is the default if no other bootable device is found.
7. The default BIOS boot order is removable devices, hard drives, CD then network.
8. To get into the BIOS, press “F2” as the VM powers up or set the option in the “Power” tab of the VM’s configuration to enter the BIOS on the next start-up.
9. Press “Esc” at power up to get a one time boot menu.
10. If you want more time at start-up to press keys, add a line similar to:

```
bios.bootDelay = "5000"
```

to the .vmx file for your VM where the delay units are milliseconds so the above is 5 seconds. This can be set directly in the VI Client.

11. Windows XP does not include drivers for the VMware SCSI controller so you need to use a driver from floppy and press F6 at the start of the boot. The driver is available here and remember to change the boot order so it does not try to boot off the floppy - http://www.vmware.com/download/server/drivers_tools.html.
12. The default is to use a SCSI controller although you can use IDE but that will limit compatibility with other VMware products, particularly ESX/ESXi.
13. To get an existing physical Windows computer into a VM, use VMware vCenter Converter which is an application you install on the physical machine and run from there. It does not communicate with Server 2.0 – you create a standalone VM and copy the files it produces to your datastore and add it from there - <http://www.vmware.com/download/converter>
14. If you use Converter to convert a non-ACPI machine then the VM produced will also not switch off when shutdown; it will prompt to press the (virtual) power button when shutdown.
15. Always install VMware Tools into the guests.

16. Cloning is just a matter of taking a copy of all the files that constitute a VM, when it is shutdown, to a new folder. In the Web UI, with the host selected in the left pane, there is an option "Add Virtual Machine to Inventory". On power up, you will be asked whether you moved or copied it so select the latter which regenerates new unique identifiers such as MAC address.
17. After booting a cloned VM, you must take the steps necessary for the guest OS to make it unique if it is to be networked on the same subnet as the machine it was copied from. Microsoft Sysprep or newsid should be used for Windows platforms.
18. If you need to make VMs that are compatible with other VMware products, it is best to create the VM initially this way. The Web UI VM creation wizard offers the following in the guest operating system selection tab which refers to the virtual hardware version:

	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Virtual Hardware	7	6	4
ESX Server			3.0+
Fusion		1.0+	1.0+
Server	2.0+	2.0+	1.0+
Workstation	6.5+	6.0+	5.0+

Note that for ESX/ESXi compatibility, you also need to have a pre-allocated disk that is not split into 2GB chunks and it must use a SCSI controller.

19. If moving VMs from Windows to Linux, check the paths in all configuration files (.vmx, .vmdk, etc) to ensure they exist and are not wrong due to bad case since Windows file systems are not case sensitive but Linux ones generally are. Also check the encoding/locale of .vmx and .vmdk files.

Networking

1. There are three type of networking available in Server 2.0 – bridged, host-only and NAT. Bridged gives the VM networking as if it were a physical machine connected to your LAN. NAT gives the VM an IP address on a unique subnet and will allow access to the LAN but will by default block all unsolicited incoming traffic. Host-only only allows VMs to communicate with other VMs on the same host-only network and to the host itself.
2. Networking on Windows hosts is configured by running vmnetcfg.exe as an administrator. On Linux, by running vmware-config.pl which requires all VMs to be suspended or shutdown.
3. No special adapter is created for the bridged network(s) but you will see VMnet* adapters for host-only and NAT networks on the host with IP addresses for their corresponding subnet.
4. For Windows hosts, the VMware Bridging Protocol should be bound to all NICs that will be used for bridging. On Linux, there should be vmnet-bridge processes running for each bridged NIC.

5. Multiple bridged NICs are configured by simply creating new VMnet* NICs for each physical NIC on the host. On Windows, automatic bridging must first be disabled and the change applied.
6. Make sure NICs are set to connect at power on and are connected if you want them to function normally.
7. With NAT networking, ports on the host can be forwarded to specific ports in specific VMs. Refer to chapter 11 of the user guide for details which differs between Windows and Linux.
8. A VM can have more than one NIC which can be of the same or different type.
9. VMware by default will provide DHCP to host-only and NAT networks but not bridged. This can be disabled if you want to provide your own DHCP services.
10. With multiple connected NICs on the host, on a Windows host you will probably want to leave automatic bridging enabled if the NICs are on the same subnet but disable automatic bridging, via `vmnetcfg.exe`, if they connect to different subnets and then create multiple VMnet* interfaces that map to the physical NICs via `vmnetcfg.exe`. On Linux hosts, run `vmware-config.pl` and create multiple bridged interfaces selecting a different name and physical adapter for each device.
11. If you need host-only networking where the host itself is not included, for Windows hosts just disable the relevant VMnet* adapter and on Linux remove the IP address from the VMnet* adapter.
12. The VMware networking does not provide packet shaping, e.g. bandwidth throttling, but there are virtual appliances that will do this if required.

Scripting

1. Use the “`vmrun`” command - http://www.vmware.com/pdf/vix160_vmrun_command.pdf
2. The `vmrun` command requires a username and password to be passed on the command line.
3. You can create roles on Server 2.0 which define privileges to perform specific tasks such as suspending VMs. These roles can then be assigned to users or groups, for all or specific VMs, and these users can then be locked down on the host to reduce what they are allowed to do – e.g. assign a shell of “`/bin/false`” on Linux and deny the ability to logon locally and through terminal services on Windows.
4. If the username or password contains special characters, such as spaces, then they must be quoted on the command line.
5. For example, to list the running VMs locally:

```
vmrun -T server -u username -p password -h https://127.0.0.1:8333/sdk list
```
6. When a VM path is passed, it is specified relative to, and including, the name of the datastore. For example “[standard] folder/vmname.vmx”.

7. The error “Insufficient permissions in host operating system” may also simply mean incorrect credentials were specified.
8. VMware configuration files (.vmx) may also be constructed programmatically since they are text files. If this is for an existing VM then it should be shutdown before changing the file.
9. On Linux hosts there is also the vmware-vim-cmd command but this is not officially documented.

Troubleshooting

1. Do you have sufficient privileges – retest using a different account with more privileges.
2. Check log files – “/var/log/vmware” on Linux hosts and either “c:\documents and settings\all users\application data\vmware\vmware server” or “c:\programdata\vmware\vmware server” on Windows.
3. If using the VMware communities:
 - a. Search for existing posts.
 - b. If you post, post as much detail as possible including the host and guest operating systems, hardware specification and screenshots of errors. Attach relevant .vmx files. If a networking issue, attach “ipconfig /all” or “ifconfig -a” from host and guest. If a disk issue, post the small, text, .vmdk file if there is one.
 - c. If someone asks you questions, please answer them (all).
 - d. Do not rant or swear – it achieves nothing other than make you look foolish.
 - e. Do not tag on to existing threads with a new problem as your post is likely to get overlooked.
 - f. Do not forget to award points for correct or helpful answers.
 - g. Remember that the people helping you are enthusiasts and are not paid to help you.
4. For Windows hosts, check event logs for relevant issues and /var/log/messages on Linux.
5. For Windows hosts, try using SysInternals/Microsoft Process Monitor to look for missing items, bad permissions, etc.
6. If a VM will not boot, try creating a new VM but configure it to use the existing disk from the problematic VM.
7. If a VM fails to power on and was not shut down properly, check for .lck files/folders and remove them if they exist as long as the VM definitely is not running.
8. Check for uniqueness – particularly IP and MAC addresses and, on Windows guests, SIDs.
9. On Linux hosts with USB connection issues, check the permissions on the USB devices in /dev.

Other tricks

1. If you have a VM that will not boot, add its disk to working VM, ideally running the same OS, where you can check the disk, make repairs and recover data.
2. A Linux Live disc or ISO image can also be used for recovery or a WinPE/BartPE image on Windows.
3. Server 2.0 includes VNC access to guests which does not require networking to be functional in the guest. Add lines like the following to your .vmx file:

```
RemoteDisplay.vnc.enabled = TRUE
RemoteDisplay.vnc.port = "5910"
RemoteDisplay.vnc.password = "somepassword"
RemoteDisplay.vnc.keymap = "uk"
```

And then use your preferred VNC client to connect to the above port using the IP address of the host, not the guest. For VNC access to multiple VMs, use different port numbers.

4. The utility `vmware-vidskmanager` can be used for various disk tasks such as defragmentation, creating new disks and converting virtual disks from one type to another.
5. To mount .vmdk files directly on the host, download the Virtual Disk Development Kit - <http://www.vmware.com/download/sdk/virtualdisk.html>
6. If you have template VMs, as in files that you copy to create a new VM, add this line to the .vmx to create new unique ids when the copy is powered on:

```
uuid.action = "create"
```
7. The files that you may find for each VM are documented in the VMware User Guide.
8. Backing up VMs can be achieved in a number of ways:
 - a. If the VM is not powered up then simply copy all of its files to another location.
 - b. If the VM is running, take a snapshot and then copy the base disk file(s) to another location (*.vmdk except *-00001*.vmdk). A new VM can then be constructed using this disk. Note that you can only have a single snapshot.
 - c. In a Windows VM, use a VSS (Volume Shadow copy Service) aware backup tool to create a backup that can then be restored using the same tool to a bare VM.
 - d. On a Windows host, use a VSS aware backup tool to backup the files that constitute the VM.
9. To give different VMs different priorities on Linux hosts, use the `renice` utility to change the nice values for the `vmware-vmx` processes. The more negative the value, the higher the priority.
10. If you want to copy a VM that has a snapshot but you do not want the copied VM to have a snapshot, e.g. to reduce disk space requirements¹, use an imaging tool to copy the existing VM to an empty disk allocated to your new VM.