VMware Server Tips & Tricks

Kevin Gehrke

Product Support Engineer

VMWORLD 2006

VMware Server Tips & Tricks

Agenda - Mixed Bag of Tips & Tricks

- Web based Management User Interface
- Tools shipped with VMware Server
- Connecting remotely to Virtual Machines
- Logging VMware Server Events on Windows
- Migrate Physical or Microsoft Virtual Machine to VMware Server
- Best practices for backing up Virtual Machines
- Running VMware Server Virtual Machines on other VMware products
- Securing Virtual Machines and the Host
- Tips when setting up Clustering
- Troubleshooting
- Online Resources
- Questions?

Web based Management User Interface

VMware Server provides the VMware Management Interface, a Web based management tool that allows you to:

- Control (power on, suspend, resume, reset and power off) the virtual machines on that host.
- Connect the VMware Server Console to a given virtual machine, for hands on management.
- View details about each virtual machine, including system summary, hardware information, any connected users and a log of recent events.
- Secure console and management interface sessions with SSL (administrator and root users only).
- Download the VMware Virtual Machine Console
- Control the start order and start/stop delay time of auto start virtual machines.

Web based Management User Interface

Setting the auto start order and the delay start / stop time of the virtual machines on boot and shutdown of the host

If the Management User Interface is not installed you can manually set these options in the global configuration file and .vmx file for the virtual machine.

Windows host = \Documents and Settings\All Users\Application Data\VMware\VMware Server\config.ini

Linux host = /etc/vmware/config

Set the delay start / stop time of the virtual machine

autoStart.defaultStartDelay = "300" ← **Start delay of 5 Min's**

autoStart.defaultStopDelay = "300" ← **Stop delay of 5 Min's**

Set the start and stop order of the virtual machines.

autostart = "poweron"

autostart.order = "10" ← **Set VM#1 to 10, VM#2 to 20....etc**

autostop.order = "10" ← **Set VM#1 to 10, VM#2 to 20....etc**

VMware Server Tools

Tips & Tricks using the command line utilities

- vmware-vdiskmanager
- vmrun
- vmware-cmd
- vmnet-sniffer (Linux) vnetsniffer (Windows)

VMware Server Tools

Using VMware Virtual Disk Manager

vmware-vdiskmanager

You can use the virtual disk manager for the following tasks:

Create virtual disks with a particular disk controller type, size, type of virtual disk (Pre-allocated, Growable, Split into 2Gb files)

Disk types:

0	: single growable virtual disk
1	: growable virtual disk split in 2Gb files
2	: preallocated virtual disk
3	: preallocated virtual disk split in 2Gb files

Example:

vmware-vdiskmanager.exe -c -s 8Gb -a lsilogic -t 2 myscsiDisk.vmdk

Switch the virtual disk type from preallocated to growable, or vice versa. When you change the disk type to growable, you reclaim some disk space. You can shrink the virtual disk to reclaim even more disk space.

Example:

vmware-vdiskmanager.exe -r sourceDisk.vmdk -t 0 destinationDisk.vmdk

VMware Server Tools

- **Expand the size of a virtual disk so it is larger than the size specified when you created it.**

  Example:

  vmware-vdiskmanager.exe -x 36Gb myDisk.vmdk

  (Must use disk management software to expand the guest partition)

  - Defragment virtual disks.

  Example

  vmware-vdiskmanager.exe -d myDisk.vmdk

  - Prepare and shrink virtual disks without powering on the virtual machine (Windows hosts only).

  Example

  vmware-vdiskmanager.exe -k myDisk.vmdk

VMware Server Tools

vmrun

Usage: vmrun [Authentication flags] COMMAND [PARAMETERS]

Authentication flags

-h <hostName>

-P <hostPort>

-u <userName>

-p <password>

VMware Server Tools

COMMAND	PARAMETERS	DESCRIPTION
list		List all running VMs
start	Path to vmx file	Start a VM
stop	Path to vmx file	Stop a VM
reset	Path to vmx file	Reset a VM
suspend	Path to vmx file	Suspend a VM
upgradevm	Path to vmx file	Upgrade VM file format, virtual hw
installtools	Path to vmx file	Install Tools in Guest OS
snapshot	Path to vmx file	Create a snapshot of a VM
deleteSnapshot	Path to vmx file	Remove a snapshot from a VM
revertToSnapshot	Path to vmx file	Set VM state to a snapshot

Example:

vmrun snapshot “/var/lib/vmware/Virtual Machines/Windows 2000/ w2k.vmx”

VMware Server Tools

Tips for using for the vmrun command:

- List all running virtual machines.
- In a development / QA environment automate taking snapshot before installing test application.
- Automate the snapshot of all virtual machines before applying Windows updates.
- Automate the revert to snapshot or deletion of a snapshot.

VMware Server Tools

These are only some of the options available for the vmware-cmd

- C:\Program Files\VMware\VMware Server\vmware-cmd <cfg> getstate
- C:\Program Files\VMware\VMware Server\vmware-cmd <cfg> start
- C:\Program Files\VMware\VMware Server\vmware-cmd <cfg> stop
- C:\Program Files\VMware\VMware Server\vmware-cmd <cfg> reset
- C:\Program Files\VMware\VMware Server\vmware-cmd <cfg> suspend

(Linux host) /usr/bin/vmware-cmd

Note: <cfg> is path to virtual machine .vmx file.

Use vmware-cmd in a batch file to suspend virtual machine to create a backup.

Example batch file:

call vmware-cmd “c:\virtual machines\winXPPro.vmx” suspend

VMware Server Tools

vmnet-sniffer (Linux) vnetsniffer.exe (Windows)

- A very simple packet sniffer to use to help troubleshoot network issues. Utilities like Ethereal® (New name Wireshark) can provide a more detailed network protocol analyze.

Windows host usage:

vnetsniffer.exe /e VMnet0

Linux host usage:

Vmnet-sniffer –e /dev/vmnet0

Connecting remotely to Virtual Machines

- **VMware Virtual Machine Console (Windows & Linux)**

VMware Server Windows client package. A zip package containing installer files for the following VMware Server Windows Client components:
- Windows VMware Server Console (.exe)
- COM scripting API for Windows (.exe)
- Perl scripting API for Windows (.exe)
- Programming API (.exe)

VMware Server Linux client package. A zip package containing installer files for the following VMware Server Linux Client components:
- Linux VMware Server Console (.tar and .rpm)
- Perl scripting API for Linux (.tar)
- Programming API (.tar)

Connecting remotely to Virtual Machines

- **Tips using Microsoft Remote Desktop**

Do not use the Microsoft Remote Desktop to connect to the host to launch the VMware Server console. This method can cause issue with mouse performance and/or display issues. If you have no other choice to connect to the host using RDP, use the remote login option in the VMware Server console.

It is best to only use Microsoft Remote Desktop to connect directly to Windows guests.

Connecting remotely to Virtual Machines

- **Configuring a Virtual Machine for Access by a VNC Client**

To connect to a virtual machine with a VNC client, you must modify the virtual machine's configuration file (.vmx) while the virtual machine is powered off.

Open the .vmx file in a text editor and add the following lines:

RemoteDisplay.vnc.enabled = TRUE

Setting this option to TRUE enables standard VNC support. This setting is valid only while the virtual machine is running. If the virtual machine is powered off, you cannot connect to it with a VNC client.

Connecting remotely to Virtual Machines

Configuring a Virtual Machine for Access by a VNC Client

RemoteDisplay.vnc.port = “5900”

- Specify the port the VNC client uses to connect to the virtual machine. 5900 is the default VNC port used for . If you want to connect to more than one virtual machine on the same host with a VNC client, you must specify a unique port number for each virtual machine. VMware suggests you use a port number in the range from 5900 to 5999.

Connecting remotely to Virtual Machines

Configuring a Virtual Machine for Access by a VNC Client

RemoteDisplay.vnc.password = “Top-Secret”

- VMware Server supports VNC 3.3 authentication, which is an eight character password. Use this password when you are prompted for authentication as you use the VNC client to connect to the virtual machine.

- Make these changes for each virtual machine to which you want to connect with a VNC client. Remember to specify a unique port number for each virtual machine if you intend to connect to more than one virtual machine on the host with a VNC client.

Connecting remotely to Virtual Machines

Configuring a Virtual Machine for Access by a VNC Client

- Only the 8-character password is encrypted with the standard VNC client. All VNC client traffic is sent unencrypted across the network. If security is a concern in your organization, VMware recommends using the VMware Virtual
- You cannot take or revert to snapshots.
- You cannot change the power state of the virtual machine; that is, you cannot power on, power off, suspend or resume. You can shut down the guest operating system, which may or may not power off the virtual machine (some operating systems do not power off their systems when shut down).
- You cannot copy and paste text between the host and guest operating system.
- You must install VMware Tools in the virtual machine before you connect with the VNC client. Otherwise, the mouse cannot work. (VNC clients do not support relative mice; VMware Tools contains an absolute mouse driver.)
- You cannot configure the virtual machine with the virtual machine settings editor, nor can you upgrade VMware Tools.

Logging VMware Server events of Windows

eventlog.win.message = “FALSE”

- This setting prevents the logging of all dialog box and message events that appear in VMware Server.

eventlog.win.register = “FALSE”

- This setting prevents the logging of power state change events and logging of when a virtual machine is added to or removed from the inventory.
- To modify what gets logged for a virtual machine, add either or both of the options to the virtual machines configuration (.vmx) file.
- To modify what gets logged for all virtual machines on a host, add either or both of the options to the VMware Server config.ini file, located by default in

C:\Documents and Settings\All Users\Application Data\VMware\VMware Server.

Turn logging on by using “TRUE”, turn off by using “FALSE”

Migrate Physical & Microsoft Virtual Machine to VMware Server

- Use VMware Coverter utility to migrate a physical machine to VMware Server.
- Technical white paper on other methods of P2V

  http://www.vmware.com/pdf/p2v_thirdpartyimage.pdf
- Use the VMware importer to migrate a Microsoft Virtual PC virtual machine or Microsoft Server virtual machine to VMware Server. You can use importer to make a full copy or linked clone virtual machine.

Best practices for backing up Virtual Machines

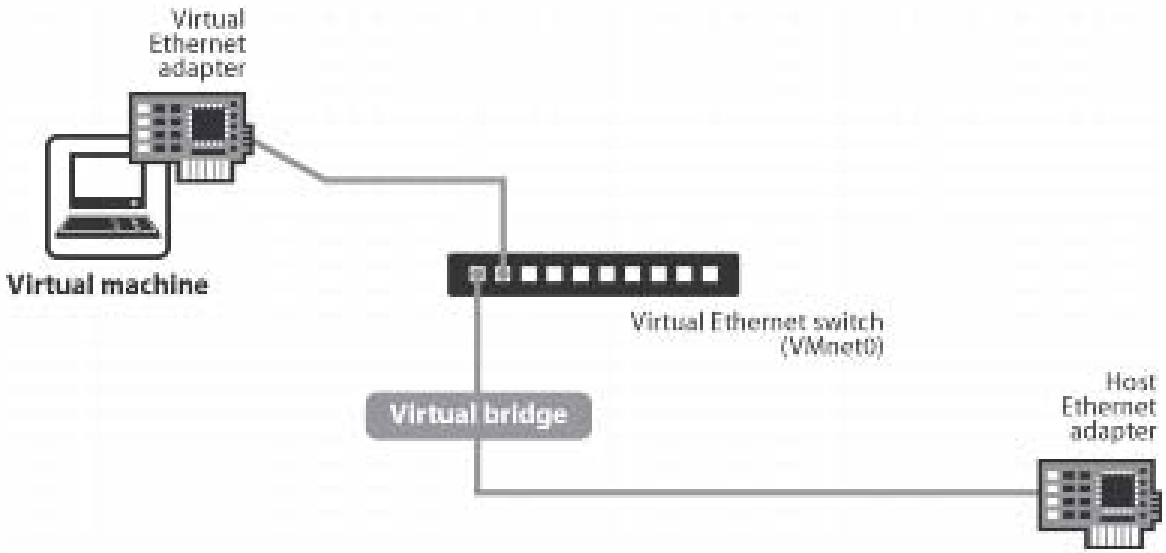
- A virtual machine directory should not be backed up on the VMware Server host if the virtual machine is powered on. You should either suspend or shut down the virtual machine before backing up its directory. Use the vmware-cmd or vmrun to suspend the virtual machine from a pre backup script and use vmware-cmd or vmrun to restart the virtual machine from a post backup script.
- If the virtual machine is running when you try to back it up, the virtual machine can hang and be unreachable.
- The best way to back up virtual machines that require constant uptime (24 hours a day, seven days a week) is to load a backup agent in each virtual machine. This agent should connect directly through your network to your backup servers. This method allows you to completely back up individual files on your virtual machines and recover files individually.
- Before implementing a backup method, test and document the method in advance to ensure a successful backup.

Running VMware Server Virtual Machines on other VMware products

- To migrate a virtual machine to ESX, the virtual machine must be configured to use a virtual SCSI disk. See knowledge base article 1881 for instructions on how to convert from virtual IDE to virtual SCSI disk.
- To migrate a VMware Server Virtual Machine to Workstation, you must be using VMware Workstation 5.x
- You can not migrate a VMware Server virtual machine to WS 4.x, GSX 3.x directly. You could ghost the virtual disk and restore it in a new WS 4.x or GSX 3.x virtual machine.

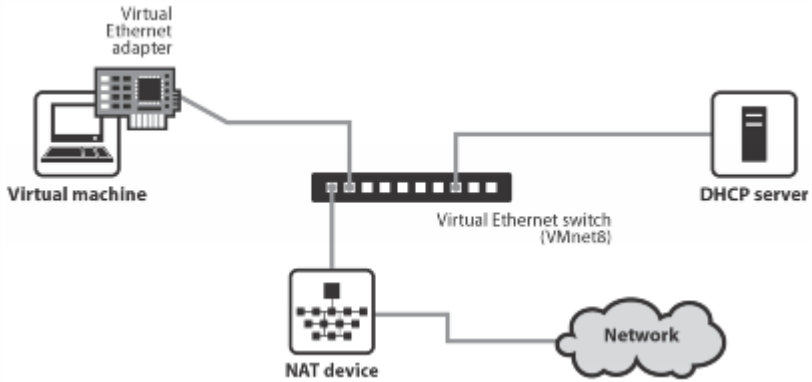
Securing Virtual Machines and the Host

- Typical Virtual Machine Bridged networking configuration



Securing Virtual Machines and the Host

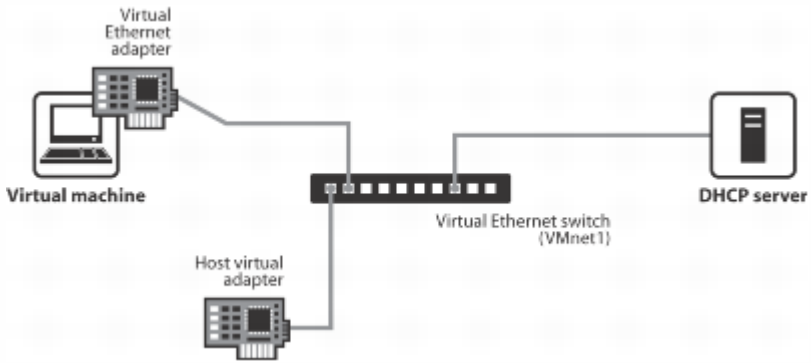
- Typical Virtual Machine NAT networking configuration



- By default the virtual switch vmnet8 provides a DHCP server
- The virtual switch vmnet8 provides NAT (Network Address Translation)

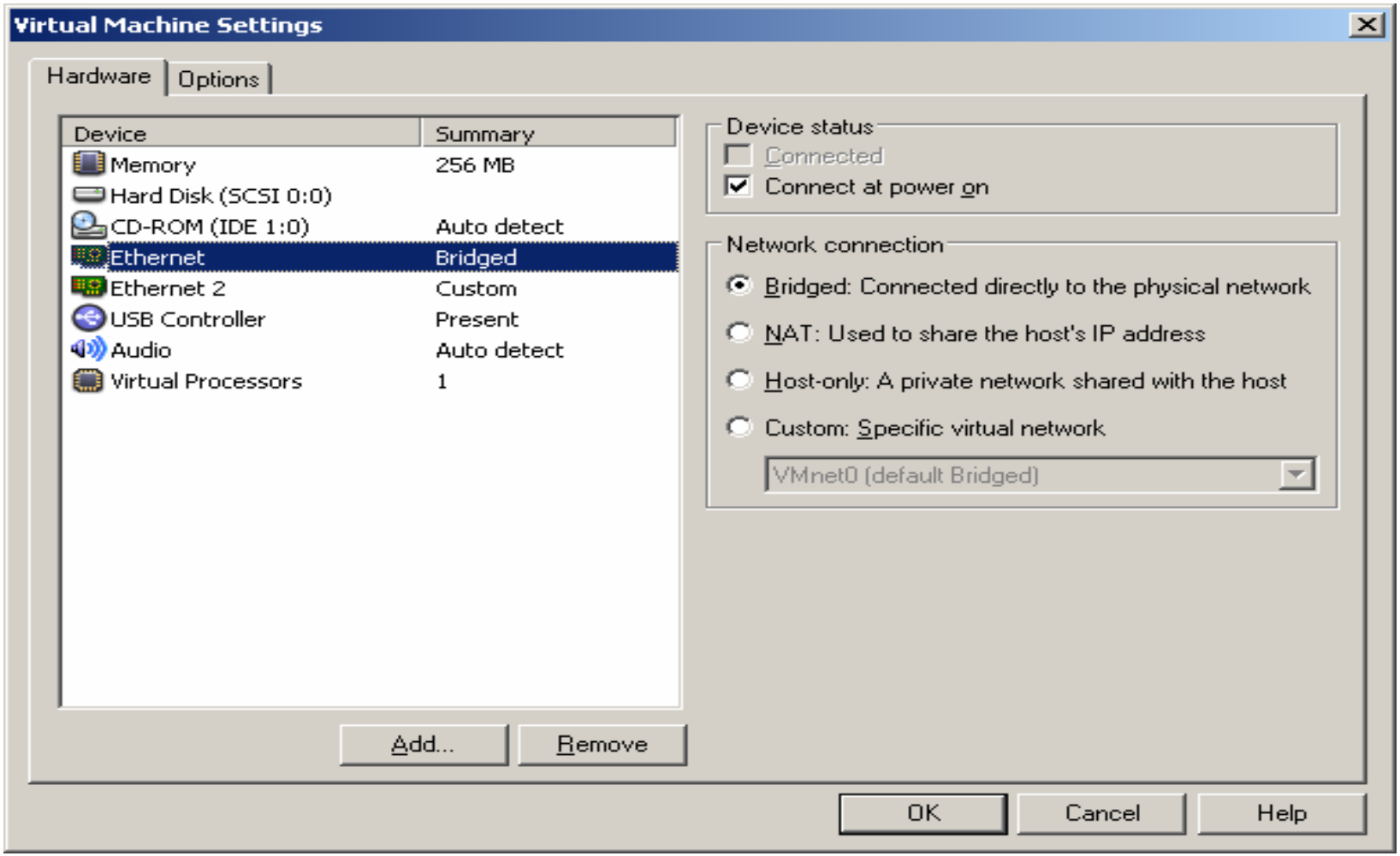
Securing Virtual Machines and the Host

- Typical Virtual Machine Host-Only networking configuration



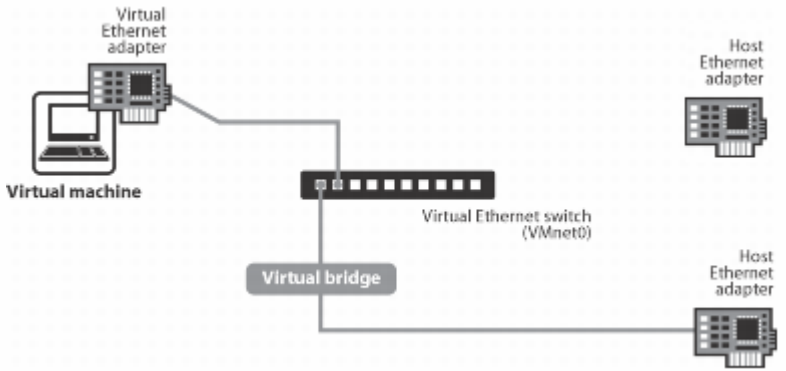
- By default the virtual switch vmet1 provides a DHCP server.

Securing Virtual Machines and the Host



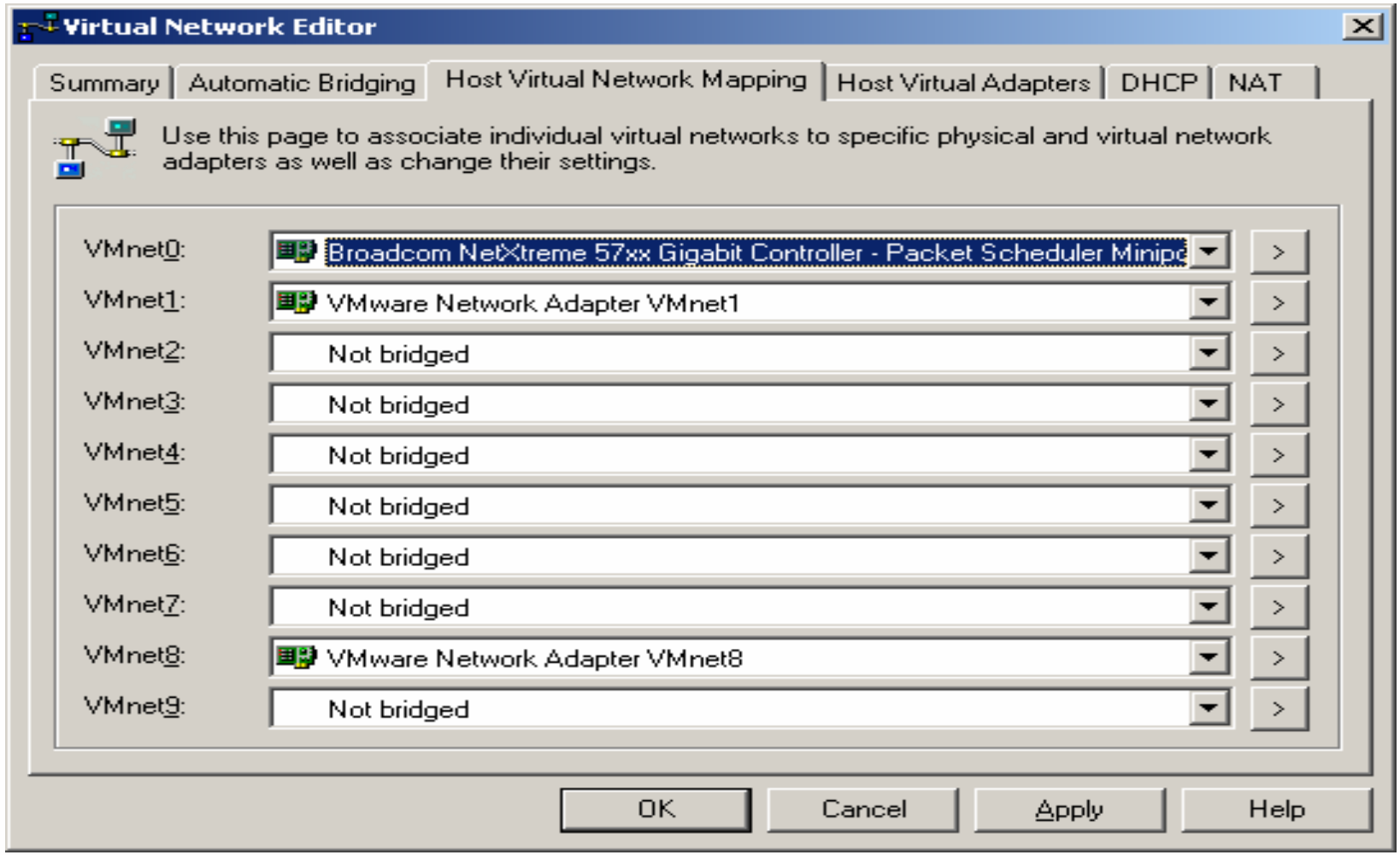
Securing Virtual Machines and the Host

- Dedicate a physical host network adapter for the virtual machines on a different subnet than the host.



- Set Linux physical network adapter dedicated to virtual machine to IP an address of 0.0.0.0
- Remove all network protocols, except VMware Bridged protocol from a Windows host network adapter dedicated to virtual machines.

Securing Virtual Machines and the Host



Securing Virtual Machines and the Host

Run the vmware-config.pl script to make network changes on the host

You have already setup networking.

Would you like to skip networking setup and keep your old settings as they are? (yes/no) [yes] no

Do you want networking for your virtual machines? (yes/no/help) [yes]

Would you prefer to modify your existing networking configuration using the wizard or the editor? (wizard/editor/help) [wizard] editor

The following virtual networks have been defined:

. vmnet0 is bridged to eth0
. vmnet1 is a host-only network on private subnet 172.16.222.0.
. vmnet8 is a NAT network on private subnet 192.168.158.0.

Securing Virtual Machines and the Host

Do you wish to make any changes to the current virtual networks settings? (yes/no) [no] yes

Which virtual network do you wish to configure? (0-99) 0

The network vmnet0 has been reserved for a bridged network. You may change it,
but it is highly recommended that you use it as a bridged network. Are you
sure you want to modify it? (yes/no) [no] yes

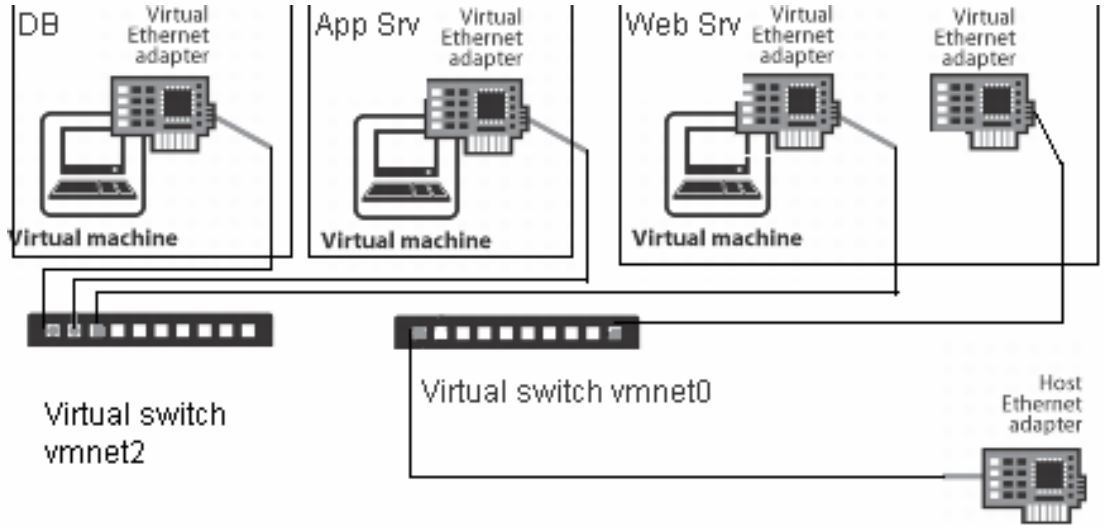
What type of virtual network do you wish to set vmnet0?
(bridged,hostonly,nat,none) [bridged] bridged

Configuring a bridged network for vmnet0.

Your computer has multiple ethernet network interfaces available: vmnet1,
vmnet8, eth0, eth1. Which one do you want to bridge to vmnet0? [eth0] eth1

Securing Virtual Machines and the Host

- Back-end traffic is constrained to the internal virtual switch. The Web server virtual is not a router, which protects the back-end server from hostile connections



Securing Virtual Machines and the Host

Changing the Port Number on a Windows Host or Client

To change the port number on the VMware Server for Windows host, add the following line to config.ini in C:\Documents and Settings\All Users\Application Data\VMware\VMware Server:

authd.port = <portNumber>

Where <portNumber> is the port number that all consoles connecting to virtual machines on this host must use.

Securing Virtual Machines and the Host

Changing the Port Number on a Windows Host or Client

To change the port number that is used by the console installed on a Windows client, you must create a file called config.ini and place it in C:\Documents and Settings\All Users\Application Data\VMware\VMware Virtual Machine Console. In this file, add the following line:

authd.client.port = <portNumber>

Where <portNumber> is the port number that all consoles on this machine connecting to virtual machines on the VMware Server host must use. The VMware Server host must have this port number set to the authd.port variable in its config.ini file (Windows host) or vmware-authd file (Linux host).

To change the port number for a specific user who is using the console installed on a Windows client, add the following line to the preferences.ini file located in C:\Documents and Settings\<user>\Application Data\VMware:

authd.client.port = <portNumber>

Where <portNumber> is the port number to use only when this user is logged on and using a console to connect to a virtual machine on the VMware Server host. The VMware Server host must have this port number set to the authd.port variable in its config.ini file (Windows host) or vmware-authd file (Linux host).

Securing Virtual Machines and the Host

Changing the Port Number on a Linux Host or Client

To change the port number on the VMware Server for Linux host, you first need to determine whether your host is configured to use xinetd or inetd. If your host is configured to use xinetd, look for the following line in /etc/xinetd.d/vmware-authd:

port = 902

Change the port number — 902 in this case — to the desired number.

If your host is configured to use inetd, look for the following line in /etc/inetd.conf:

902 ... vmware-authd

Change the port number — 902 in this case — to the desired number. All consoles connecting to virtual machines on this host must use this port number.

Securing Virtual Machines and the Host

Changing the Port Number on a Linux Host or Client

To change the port number that is used by the console installed on a Linux host or client, add the following line to either /etc/vmware-console/config or /usr/lib/vmware-console/config:

authd.client.port = <portNumber>

Where <portNumber> is the port number that all consoles on this machine connecting to virtual machines on the VMware Server host must use. The VMware Server host must have this port number set to the authd.port variable in its config.ini file (Windows host) or vmware-authd file (Linux host).

Note: If the port numbers specified in these files are different, the port number specified in /etc/vmware-console/config takes precedence.

To change the port number for a specific user who is using the console installed on a Linux host, add the following line to ~/.vmware/preferences:

authd.client.port = <portNumber>

Where <portNumber> is the port number to use only when this user is logged on and using a console to connect to a virtual machine on the VMware Server host.

Tips when setting up Clustering

Tips to remember clustering two or more virtual machines on the same VMware Server host.

- VMware recommends you set up any shared disks on the same SCSI bus, which is a different bus from the one the guest operating system uses. For example, if your guest operating system is on the scsi0 bus, you should set up disks to share on the next available bus, typically the scsi1 bus. (scsi1:0.filename = quorumdisk.vmdk)
- Configure shared disks as preallocated virtual disks.
- To enable SCSI reservation for devices on the scsi1 bus, add the following line to the virtual machine.s configuration file:

scsi1.sharedBus = "virtual“

- In addition to enabling SCSI reservation on the bus, you need to allow virtual machines to access the shared disk concurrently. Add the following line to the virtual machines configuration file:

disk.locking = "false"

Tips when setting up Clustering

When you use VMware Server virtual machines in a cluster, you must turn off disk caching for each virtual machine that is a member of the cluster. If you do not turn off data on the shared drive might become corrupted. To turn off disk caching open the configuration .vmx file of each virtual machine in a text editor and add the following line:

diskLib.dataCacheMaxSize = “0”

Troubleshooting

- VMware Server Console log file location
  - Windows host = C:\Documents and Settings\<username>\Local Settings\Temp\vmware-<username>\vmware-<username>-<pid>.log
  - Linux host = /tmp/vmware-<username>/ui-<pid>.log
  - PID = Process ID of vmware-vmx
- Management User Interface log file locations
  - Windows host = C:\Program Files\VMware\VMware Management Interface\mui.log
  - Linux host = /var/log/vmware-mui
- Virtual machine log file
  - The vmware.log file is located in the directory where the virtual machine was created.

Online Resources

- **Product Documentation**

http://www.vmware.com/support/pubs/

A documentation library for all VMware products reference materials in one searchable location.

- **Knowledge Base**

http://kb.vmware.com/

A database of searchable technical documents authored by VMware technical staff.

- **VMware Product Centers**

http://www.vmware.com/vmtn/resources/

Contains links to White papers, technical notes, compatibility guides and other technical information for all currently released VMware products

- **VMware Community Discussion Forums**

http://www.vmware.com/community/index.jspa

Questions

Presentation Download

Please remember to complete your
session evaluation form
and return it to the room monitors
as you exit the session

The presentation for this session can be downloaded at
http://www.vmware.com/vmtn/vmworld/sessions/

Enter the following to download (case-sensitive):

Username: cbv_rep
Password: cbvfor9v9r

VMWORLD 2006