Chapter 10

Troubleshooting Your Virtual Environment

When problems occur in your virtual environment, you need to know where to look for clues to the cause and what to do to resolve them. Often, just trying to figure out the exact cause is the most difficult part, because virtual servers are more complicated than physical servers and there are more potential causes of problems. Troubleshooting problems can often be frustrating, and you should take your time and not make any rash decisions that might worsen the problem. When you know where to look to find the cause of a problem, the process becomes a lot easier.

Troubleshooting ESX and ESXi Hosts

Some differences exist between ESX and ESXi hosts, so we cover them separately. ESX hosts are more complex than ESXi hosts due to the Service Console that they have, and therefore can be a bit more challenging to troubleshoot. There are also many more log files that can be viewed on an ESX host compared to an ESXi host, and therefore more things to check when you are troubleshooting an ESX host.

Troubleshooting ESX Hosts

There are many common problems that happen with ESX hosts. We cover some of them and resolutions and what log files to check, how to check the version of ESX components, and what resources you can use to help you troubleshoot your problem.

Log Files

Let's begin with the log files that you can use to troubleshoot your ESX host. There are numerous log files that you can look at depending on the nature of your problem. These log files are located on the ESX Service Console and can be viewed by opening the logs with a text editor, via SCP with a tool such as WinSCP, using the VI Client, or using the `tail` Linux command. Here is a summary on how to use the various methods for viewing log files:

- **Text editor.** Log on to the Service Console and use the built-in text editors to open a log file. You can use nano, which is a bit easier to use, or vi to open a log file. Type `nano` or `vi log` *`file path/name`* to open one (for example, `nano /var/log/vmware/hostd.log`).
- **SCP tool.** If you install an SCP tool such as WinSCP or FastSCP on your workstation, you can connect to an ESX host and browse through the file system using a GUI similar to Windows Explorer. Then just select the file you want to view and open it, which downloads it to your workstation for you to view.
- **`tail` command.** The Linux `tail` command enables you to view the last part of a text file. By default, without any options, it will show you the last ten lines of a file, but you can specify more lines or have it follow the file so that it continually reads the file and displays new additions to the file. To use this command, log on to the Service Console and type `tail` *`log file path/name`*. You can use the `-f` option to follow the file or the `-n #` command to specify the number of lines to display (for example, `tail /var/log/vmware/hostd.log -f` or `tail/var/log/vmware/hostd.log 50`).
- **VI Client.** If you connect to an ESX host with the VI Client, you can view the logs by clicking the Administration button at the top and then selecting the System Logs tab, as shown in Figure 10.1. Here you can select between the various log files, search for log entries, and control how many of the log entries display.

The following log files are available on an ESX host:

- **VMkernel, /var/log/vmkernel.** Records activities related to the VMs and ESX hosts. Rotated with a numeric extension. The current log has no extension, and the next newest one has a .1 extension
- **VMkernel Warnings, /var/log/vmkwarning.** Records activities with the VMs. It is a subset of the VMkernel log and uses the same rotation scheme.
- **VMkernel Summary, /var/log/vmksummary.** Used to determine uptime and availability statistics for ESX hosts; a human-readable summary can be found in /var/log/vmksummary.txt.
- **ESX Server host agent, /var/log/vmware/hostd.log.** Contains information about the agent that manages and configures the ESX host and its VMs. (Search the file date/time stamps to find the log file it is currently outputting to or open hostd.log, which is linked to the current log file.)

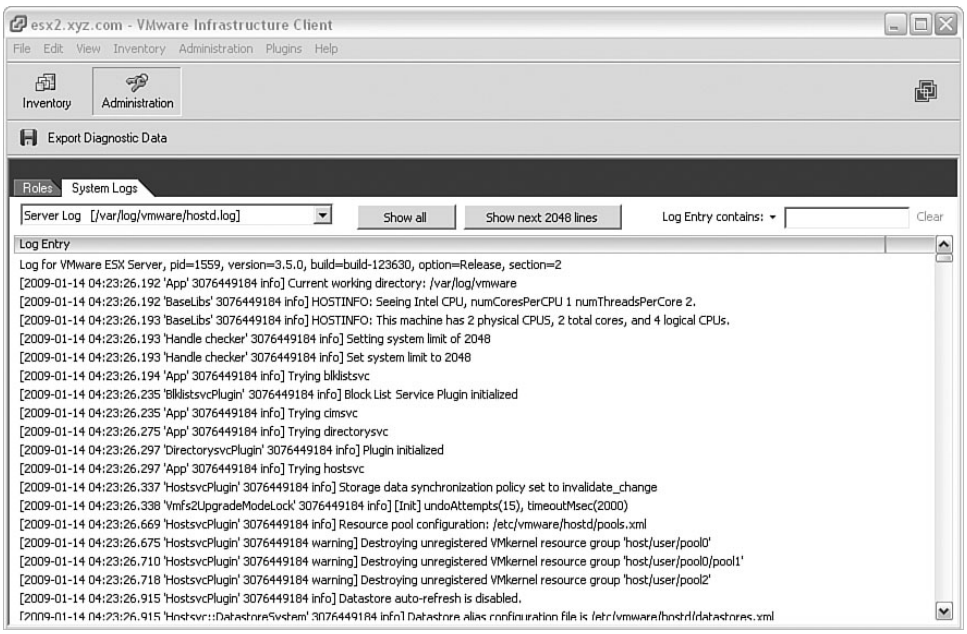

Figure 10.1 Using the VI Client to view ESX host log files

- **ESX Firewall, /var/log/vmware/esxcfg-firewall.log.** Logs all firewall rule events. Rotated with a numeric extension. The current log has no extension, and the next newest one has a .1 extension
- **ESX Boot, /var/log/vmware/esxcfg-boot.log.** Logs all ESX boot events. Rotated with a numeric extension. The current log has no extension, and the next newest one has a .1 extension.
- **ESX Update, /var/log/vmware/esxupdate.log.** Logs all updates done through the esxupdate tool.
- **Service Console, /var/log/messages.** Contains all general log messages used to troubleshoot VMs or an ESX host.
- **Web Access, /var/log/vmware/webAccess.** Records information about web-based access to an ESX host.
- **High Availability (HA), /var/log/vmware/aam.** Logs information related to the High Availability service. In ESX 3.0.x, these logs were in /opt/LGTOaam512/ instead.
- **Authentication, /var/log/secure.** Contains records of connections that require authentication, such as VMware daemons and actions initiated by the xinetd daemon.
- **Vpxa, /var/log/vmware/vpxa.log.** Contains information about the agent that communicates with vCenter Server. Search the file date/time stamps to find the log file it is currently outputting to or open vpxa.log file, which is linked to the current log file.

Which log you use will depend on the problem you are troubleshooting. In general, the VMkernel and hosted log files are the ones you will use for most problems. For other problems that lie in specific areas, you may check logs related to those areas (for example, checking the esxupdate.log for problems with Update Manager or the vpxa.log for problems with connections to vCenter Server). Viewing some of these log files, you might be overwhelmed by the number of entries and the somewhat cryptic entries in the log files. You might not understand everything in the log file, but you can look for obvious error messages that may relate to your problem. Log files contain a lot of information, and it can sometimes be difficult to sort out what is normal and what is not. If you open a support case with VMware, they will request the log files, and will be able to analyze them and tell you what they find.

In addition to the methods to view individual log files, you can use the `vm-support` command (it's actually a script) that you can run on the ESX Service Console that will bundle together all the log files, configuration files, and output from various commands into a single TGZ file. After the file has been created, you can copy it to your workstation and extract it using the Linux `tar` command or WinZip. There can be hundreds or thousands of little files that are extracted. These files are very useful to VMware support to help troubleshoot your problem.

You can run the `vm-support` command without any parameters, which will collect all the files and bundle them together, or you can specify parameters to collect specific information or do certain tasks. Here are some of the most commonly used parameters that can be used with `vm-support`:

- `-n` Causes no core files to be included in the tar file
- `-s` Takes performance snapshots in addition to other data
- `-S` Takes only performance snapshots
- `-x` Lists world IDs (wid) for running VMs
- `-X` *`wid`* Grabs debug info for a hung VM
- `-w` *`dir`* Sets working directory for output files
- `-h` Displays help for command usage and available options

To run `vm-support`, log on to the Service Console and type the command either by itself or with options. The script will run and perform all the data collection and create the tar file, as shown in Figure 10.2.

Just remember to delete these files from your ESX host when you have copied them off to avoid filing up your disk partitions.

The VI Client also has an option to export diagnostic data (`vm-support` output and more) to files on your local workstation, which you can open and review the various files inside or send to VMware support. If you connect to a vCenter Server, you can select multiple hosts simultaneously and include VI Client and vCenter Server logs and files in the output. When you use the VI Client and select hosts, it calls the `vm-support` script on the host and then copies the output file to your local PC. To do this, connect to a host or vCenter Server with

the VI Client, and then select File from the top menu, and then Export, and then the Export Diagnostic Data option. A window will appear, as shown in Figure 10.3, in which you can select what you want to include and a directory on your workstation to download the data to.

```
[root@esx2 root]# vm-support

VMware ESX Server Support Script 1.29

Preparing files: \
Waiting up to 300 seconds for background commands to complete:

Waiting for background commands: \
Creating tar archive ...


File: /root/esx-2009-01-22--08.20.24895.tgz
Please attach this file when submitting an incident report.
To file a support incident, go to http://www.vmware.com/support/sr/sr_login.jsp


To see the files collected, run: tar -tzf /root/esx-2009-01-22--08.20.24895.tgz

Done
[root@esx2 root]#
```

Figure 10.2 Running `vm-support` on an ESX host

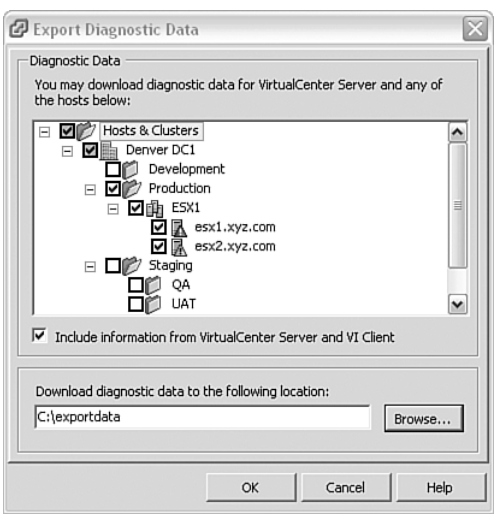

Figure 10.3 Exporting diagnostic data from hosts

When it begins, a task will appear in the Recent Tasks pane of the VI Client, and a new window will open showing the download progress of each bundle, as shown in Figure 10.4.

When it completes, it will create a new subdirectory in the directory that you specified with a date/time stamp and containing the TGZ file from the hosts, a zip file from the vCenter Server, and a VI Client subdirectory containing log files created by the local VI Client.

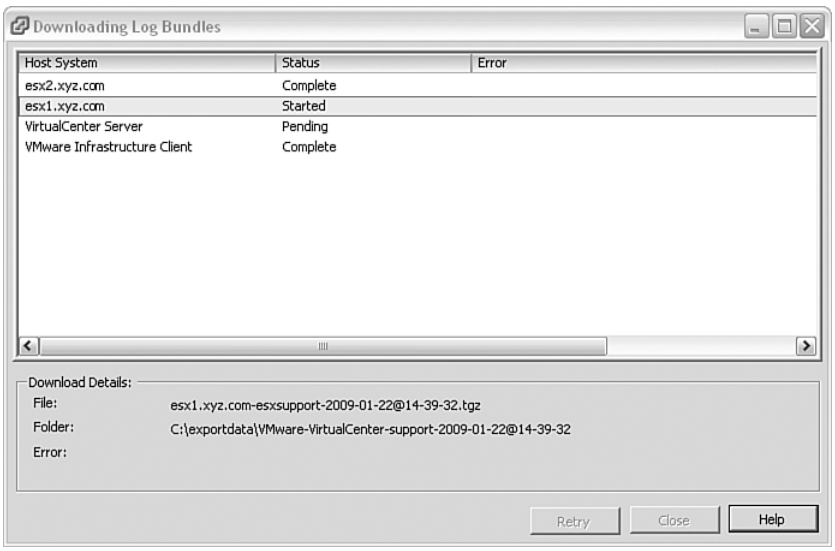

Figure 10.4 Log bundles are written to a workstation.

Determining Versions

Many times, you need to know the versions of the various components of an ESX host and what patches are applied because VMware support will need this information to help determine whether certain known issues affect your host. Listed here are some Service Console commands that you can use to determine this:

- `vmware -v` will display the ESX host version and build number.
- `/opt/vmware/vpxa/sbin/vpxa -v` will display the vCenter Server agent version and build number.
- `rpm -qa ¦ grep VMware-esx-tools` will display the version and build number of the VMware Tools installation bundle on the ESX host.
- `esxupdate -l query` will display all patches installed on the ESX host.

Sample output from some of these commands is shown in Figure 10.5.

```
[root@esx2 root]# vmware -v
VMware ESX Server 3.5.0 build-123630
[root@esx2 root]#
[root@esx2 root]# /opt/vmware/vpxa/sbin/vpxa -v
VMware VirtualCenter Agent Agent Daemon 2.5.0 build-119598
[root@esx2 root]#
[root@esx2 root]# rpm -qa | grep VMware-esx-tools
VMware-esx-tools-3.5.0-123630
```

Figure 10.5 Determining versions of an ESX host components

You can also obtain the ESX host and build number by selecting the host in the VI Client. Version numbers usually change only when major product upgrades are installed (for example, ESX 3.0, 3.5) and build numbers change frequently when any type of upgrade is applied, whether it is a patch, update, or major upgrade.

Common Problems and Resolutions

There are some problems that occur with ESX hosts that are fairly common, and we cover those here. Many times, you can take simple steps to correct them, but some require more in-depth troubleshooting and resolutions.

Purple Screen of Death

One occurrence that can happen on both ESX and ESXi hosts is called the purple screen of death (PSoD), which is VMware's version of Microsoft's infamous blue screen of death (BSoD) and the result of a host crashing and becoming inoperative. A PSoD, as shown in Figure 10.6, is definitely not something you want to see on your hosts.

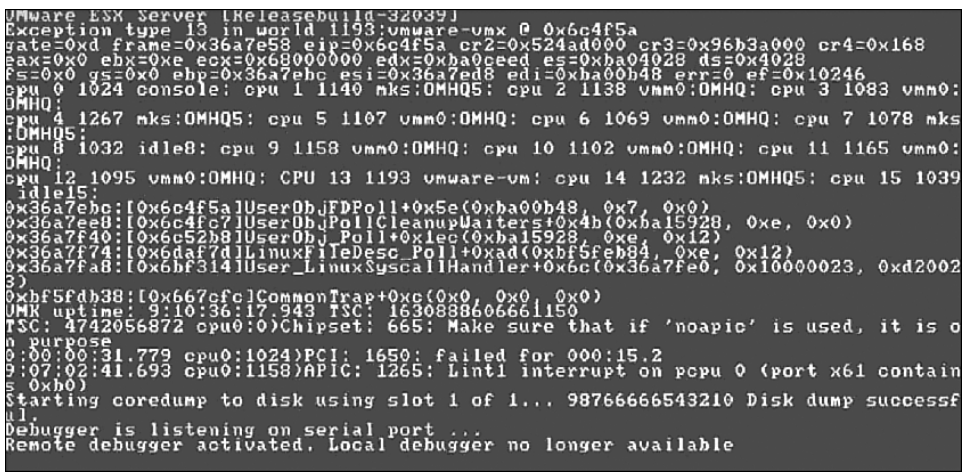

Figure 10.6 ESX host purple screen of death

When one occurs, it will completely halt the host and cause it to become unresponsive. The causes of PSoDs are typically hardware related (defective memory is the most common cause) or a bug in the ESX application. Your only recourse when it happens is to power off the host and power it back on. The information that displays on the screen is useful, however, and you should attempt to capture it by writing it down, using a camera phone to take a picture of it, or taking a screen capture from a remote management board if present. You might not be able to make much sense out of the information, but it will be very useful to VMware support. What is displayed consists of the ESX version and build number, the exception type, register dump, what was running on each CPU when the crash occurred, back-trace, server uptime, error messages, and memory core information.

When you reboot a host after experiencing a PSoD, a file beginning with the name vmkernel-zdump should be present in your host's /root directory. This file will be useful to VMware support, and you can also use it to help determine the cause by using the vmkdump utility to extract the VMkernel log file and look for any clues as to the cause of the PSoD. To use this command, type `vmkdump -l dump filename`. As previously mentioned, defective memory is a common cause of a PSoD. You can use the dump file to help identify the memory module that caused the problem so that it can be replaced.

If you suspect defective memory is the cause, you can test your host's memory by using a utility application that burns in memory. These utilities require you to shut down your host and boot from a CD to run the memory tests. One commonly used utility is Memtest86+, which does extensive memory testing, including checking the interaction of adjacent memory cells to ensure that writing to one cell does not overwrite an adjacent cell. You can download this utility at www.memtest.org/.

Did You Know?

ESX 3.0.x servers had a built-in memory test utility called Ramcheck that was removed in ESX 3.5. This nondisruptive utility could be run by typing the command `service ramcheck start` and would test unused memory in the background with little resource overhead. Ramcheck wrote its result output to the /var/log/vmware/ directory in files named ramcheck.log and ramcheck-err.log and would run until the host was restarted or it was stopped with the `service ramcheck stop` command.

It is a good idea to burn in and test your host's memory when you are first building it to avoid disruptions later. Most memory problems are not obvious and will not be detected by the simple memory test a server does as part of its POST boot procedure. You can download the free Memtest86+ utility as a small 2MB ISO file, which you can burn to a CD to boot from and let it run for at least 24 hours to run various memory tests on your host. The more RAM you have in the system, the longer it will take to complete one pass. A server with 32GB of RAM will generally take about one day to complete. Besides the system memory, Memtest86+ will also test your CPU's L1 and L2 cache memory. Memtest86+ will run indefinitely, and the pass counter will increment as all the tests are run.

Service Console Problems

You might sometimes experience a problem with your Service Console where it hangs and will not allow you to log on locally. The condition, which can be caused by hardware lockups or a deadlocked condition, will usually not affect the operation of the VMs running on the host. Rebooting is often the only recovery for this condition. Before doing this, however, you should shut down or VMotion the VMs to other hosts. You do this by whatever method works, such as using the VI Client, connecting to the Service Console remotely via SSH, or trying to use an alternative/emergency console, which can be accessed by pressing Alt-F2

through Alt-F6. When you move the VMs or shut them down, you can reboot the host with the `reboot` command. If all the console methods are unresponsive, you will need to cold boot the host instead.

Networking Problems

You may also experience a condition that causes you to lose all or part of your networking configuration or where a configuration change causes the Service Console to lose network connectivity. If this happens, you will not be able to connect to the host by any remote method, including the VI Client or SSH. Your only recourse will be to rebuild or fix the network configuration from the local Service Console using the `esxcfg-` command-line utilities. Here are some of the commands that you can use to configure networking from the ESX CLI:

- `esxcfg-nics` This command displays a list of physical network adapters along with information about the driver, PCI device, and link state of each NIC. You can also use this command to control a physical network adapter's speed and duplexing. Type `esxcfg-nics -l` to display NIC information and `esxcfg-nics -h` to display available options for this command. Here are some examples:
  - Set the speed and duplex of a NIC (vmnic2) to 100/Full:

    ```
    esxcfg-nics -s 100 -d full vmnic2
    ```

  - Set the speed and duplex of a NIC (vmnic2) to autonegotiate:

    ```
    esxcfg-nics -a vmnic2
    ```

- `esxcfg-vswif` Creates and updates Service Console network settings, including IP address and port group. Type `esxcfg-vswif -l` to display current settings and `esxcfg-vswif -h` to display all available options for changing settings. Here are some examples:
  - Change your Service Console (vswif0) IP and subnet mask:

    ```
    esxcfg-vswif -i 172.20.20.5 -n 255.255.255.0 vswif0
    ```

  - Add a Service Console (vswif0):

    ```
    esxcfg-vswif -a vswif0 -p "Service Console"
    ➥-i 172.20.20.40 -n 255.255.255.0
    ```

- `esxcfg-vswitch` Creates and updates VM (vSwitch) network settings, including uplink NICs, port groups, and VLAN IDs. Type `esxcfg-vswitch -l` to display current vSwitch configurations and `esxcfg-vswitch -h` to display all available options for changing settings. Here are some examples:
  - Add a physical NIC (vmnic2) to a vSwitch (vSwitch1):

    ```
    esxcfg-vswitch -L vmnic2 vswitch1
    ```

  - Remove a pNIC (vmnic3) from a vSwitch (vSwitch0):

    ```
    esxcfg-vswitch -U vmnic3 vswitch0
    ```

- Create a port group (VM Network3) on a vSwitch (vSwitch1):

```
esxcfg-vswitch -A "VM Network 3" vSwitch1
```

- Assign a VLAN ID (3) to a port group (VM Network 3) on a vSwitch (vSwitch1):

```
esxcfg-vswitch -v 3 -p "VM Network 3" vSwitch1
```

- `esxcfg-route` Sets or retrieves the default VMkernel gateway route. Type `esxcfg-route -l` to display current routes and `esxcfg-route -h` to display all available options for changing settings. Here are some examples:
  - Set the VMkernel default gateway route:

```
esxcfg-route 172.20.20.1
```

  - Add a route to the VMkernel:

```
esxcfg-route -a default 255.255.255.0 172.20.20.1
```

- `esxcfg-vmknic` Creates and updates VMkernel TCP/IP settings for VMotion, NAS, and iSCSI. Type `esxcfg-vmknic -l` to display VMkernel NICs and `esxcfg-vmknic -h` to display all available options for changing settings. Here is an example:
  - Add a VMkernel NIC and set the IP and subnet mask:

```
esxcfg-vmknic -a "VM Kernel" -i 172.20.20.19 -n 255.255.255.0
```

In addition, you can restart your Service Console network by using the command `service network restart`.

Other Problems

Sometimes just restarting some of the ESX services will resolve problems and not affect the VMs running on the host. Two services that can be restarted and often fix many problems are the hostd service and the vpxa service. The hostd service runs in the Service Console and is responsible for managing most of the operations on the ESX host. To restart the hostd service, log on to the Service Console and type `service mgmt-vmware restart`.

Watch Out!

Be aware that a bug has existed in many versions of ESX 3.x that causes VMs to reboot when restarting the hostd service. (See VMware knowledge base article 1003312 for more info.) This only happens if your host is configured to use automatic startups. This bug was fixed in a patch for 3.0.1 and in 3.0.2, but appeared again in ESX 3.5, and another patch was released to fix it. It's best to temporarily disable auto-startups before you run this command.

The vpxa service is the management agent that handles communication between the ESX host and its clients, including the vCenter Server and anyone who connects to the host using the VI Client. If you experience problems with vCenter Server showing a host as

disconnected, not showing current information, or any other strange problems involving vCenter Server and a host, restarting this service may resolve it. To restart the vpxa service, log on to the Service Console and type `service vmware-vpxa restart`. It is recommended to try to restart these two services when you are experiencing problems because this will often resolve many problems.

Troubleshooting ESXi Hosts

Troubleshooting ESXi hosts is a bit different because there is no Service Console. However, ESXi still has a console that you can use for troubleshooting purposes. In addition, ESXi has many of the same log files as an ESX host, but the methods to access them are a bit different.

Log Files

ESXi uses some of the same core log files as ESX, with a few differences. There are four main log files on an ESXi host: the hostd log, messages that combine the VMkernel and vmkwarnings log files (the vmksummary log file does not exist on ESXi hosts), the config log file, and the vpxa log file if the ESXi host is managed by a vCenter Server. You can access the log files in various ways, as follows:

- **Local console.** If you log on to the local ESXi console and select the View System Logs option, you will be able to choose from the log files to view, as shown in Figure 10.7. Option 4, which is the vpxa log, will display only if the host is managed by a vCenter Server.

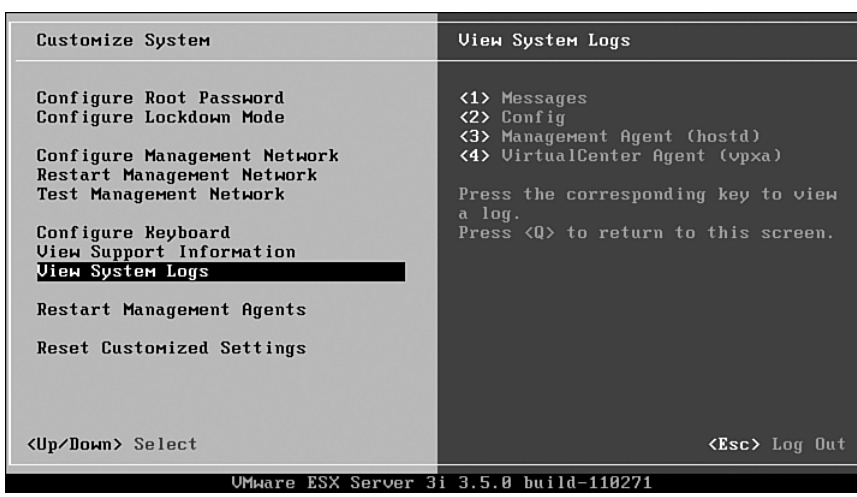

Figure 10.7 Viewing system logs of an ESXi host

- **VI Client.** Similar to that of an ESX host, if you connect to an ESXi host using the VI Client and select the Administration tab and then the System Logs tab, you can select between the various log files, search for log entries, and control how many of the log entries display.

Determining Versions

You can determine the version of the various components of an ESXi host using the following methods:

- **RCLI.** Type the command `vihostupdate --server` *`hostname or IP address`* `--username root -q` to display the ESXi version and build number and the versions of the installed packages, including the VI Client and VMware Tools, as shown in Figure 10.8.

```
C:\Program Files\VMware\VMware VI Remote CLI\bin>vihostupdate.pl -server esxi1.x
yz.com -username root -q
Enter password:
VMware ESX Server 3i 3.5.0 build-110271

Installed packages:
viclient        119801
tools           130755
firmware        110271
```

Figure 10.8 Determining versions of an ESXi host components

- **ESXi console.** The local ESXi console will display the version and build number on the main screen and at the bottom of every screen.

Just such as with ESX, if you select an ESXi host in the VI Client, it will also show you the version and build number of the ESXi host.

Accessing Tech Support Mode

Tech Support Mode is the name for a hidden console (Busybox shell) that can be accessed to troubleshoot and diagnose an ESXi host. This mode is enabled by default, but can also be disabled for security purposes using the Advanced Settings configuration. It is generally not recommended to use this console unless you know what you are doing and are advised by VMware support to use it to resolve a problem. However, if you want to access it, be aware of the following caveats:

- The console is not audited or logged, so any commands issued inside of it are not recorded.
- Some of the commands if used incorrectly can result in an unusable system.
- You can only log on to the console using the root account.

To access this mode, follow these steps:

1. At the local ESXi console, as shown in Figure 10.9, press Alt-F1. It does not matter whether you are at the main screen or in the Customize System screen.

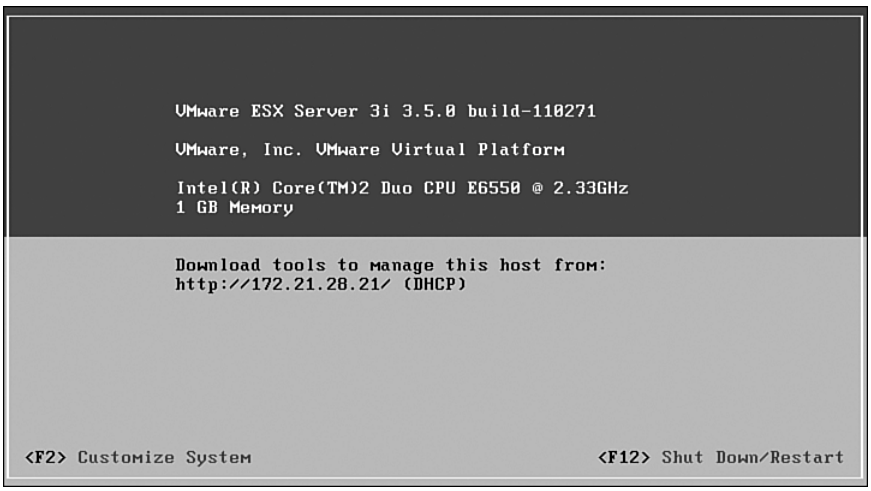

Figure 10.9 ESX console screen

2. This will display a screen that shows various system messages, as shown in Figure 10.10. You will not receive a prompt, and anything you type on this screen will not be displayed. Type the word `unsupported` to enter the Tech Support Mode.

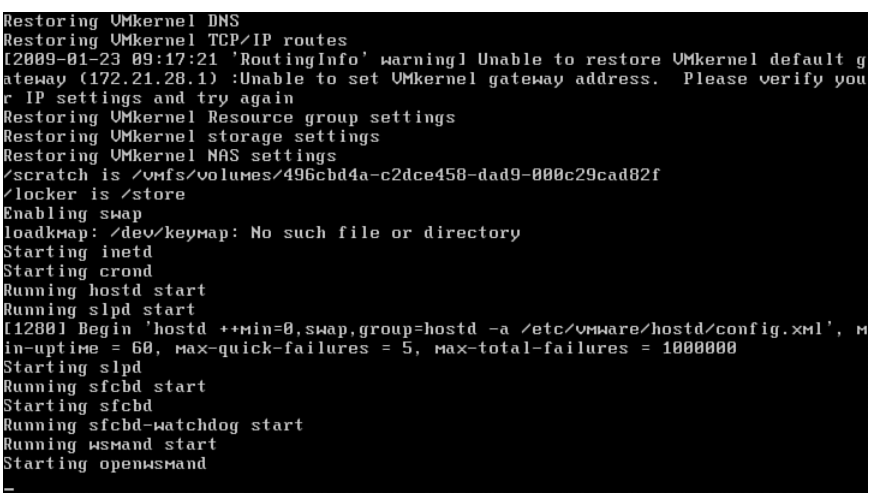

Figure 10.10 Hidden console screen displayed after you press Alt-F1

3. A warning message will display, and you will be prompted for the root password, as shown in Figure 10.11.

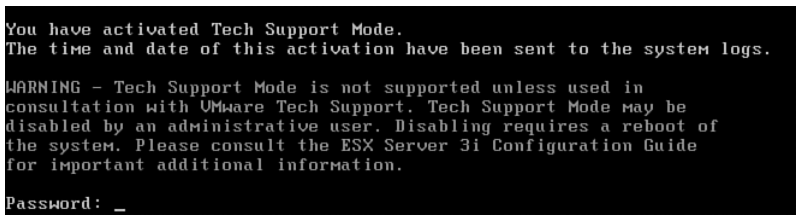

Figure 10.11 Logging on to Tech Support Mode

4. When you enter the root password, you will be at a prompt where you can enter commands, as shown in Figure 10.12.

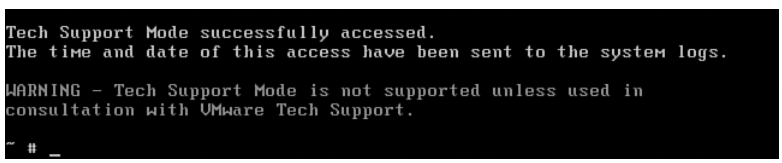

Figure 10.12 Prompt shown after you successfully log in to Tech Support Mode

5. A limited number of Linux commands work in the console. Commands such as `cd`, `ls`, `vi`, `reboot`, and `cp` will work, but others will not. In addition, you can use many of the `esxcfg` commands to view or change configurations, as shown in Figure 10.13, and use the esxtop application to view performance statistics. These commands are all located in the /sbin directory, and you can view a list of them all using the `ls` command.

When you have finished using the console, you can log off by typing the `exit` command. To get back to the regular ESXi console at any time, just press Alt-F2.

Common Problems and Resolutions

Some of the common problems with ESX also apply to ESXi. The PSoD screen, which will lock up a host, can also occur on an ESXi host, and dealing with it is similar to dealing with it in ESX. Rebuilding or correcting networking configurations is also similar in ESXi. You can configure the management network by using the configuration options in the local console (which are accessible by pressing F2). You can also use the hidden console to access the `esxcfg` commands to view and configure the rest of your networking. In addition, you can restart the vpxa management agents by selecting the option from the local console menu that is displayed by pressing F2. You can also view the VMkernel log from the local console at any time by pressing Alt-F12.

```
dcui                generateSLPReg.sh    vmkdump
decodeSel           groupadd             vmkerrcode
decodeSel.sh        groupdel             vmkfstools
dosfsck             hostd                vmkgdbd
dropbearmulti       hwclock              vmkiscsi-tool
esxcfg-advcfg       hwinfo               vmkiscsi-util
esxcfg-dhcp         init                 vmkiscsid
esxcfg-dumppart     lspci                vmkload_mod
esxcfg-hwiscsi      ntpd                 vmklogger
esxcfg-info         openwsmand           vmkperf
esxcfg-init-eesx    partedUtil           vmkping
esxcfg-locker       poweroff             vmksystemswap
esxcfg-loglevel     reboot               vmkvsitools
esxcfg-module       scantools            vsi_traverse
esxcfg-mpath        services.sh          vsish
esxcfg-nas          sfcbd                watchdog.sh
/sbin # esxcfg-vswitch -l
Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0       64          4           64                1500    vmnic0

  PortGroup Name      VLAN ID  Used Ports  Uplinks
  VM Network          0        0           vmnic0
  Management Network  0        1           vmnic0

/sbin # _
```

Figure 10.13 Command listing and running the `esxcfg-vswitch` command in Tech Support Mode

Troubleshooting vCenter Server

A vCenter Server that is down will not affect hosts or running VMs, but certain features will no longer work while it is unavailable. The HA feature will continue to work, but features such as DRS and VMotion that rely on vCenter Server will not. In addition, you lose centralized management of your hosts while it is down, which can make managing large environments difficult. Therefore, it is important to troubleshoot and resolve any problems with vCenter Server as quickly as possible.

Log Files

The primary log file used by vCenter Server is the vpxd-#.log file (the # sign represents a number), which is located in the %allusersprofile%\Application Data\VMware\VMware VirtualCenter\Logs directory on the vCenter Server 2.5. The %allusersprofile% variable on most systems is the C:\Document and Settings\All Users directory. On older VirtualCenter 2.0 servers, this file was located in the C:\Windows\Temp directory. New log files are automatically created when the logs grow to a certain size, and the number in their filename is incremented. You can see which one is currently being used by sorting by modified date or by checking the vpxd-index file, which lists the number of the log file currently in use.

In addition to viewing the files on the vCenter Server's file system, you can view them using the VI Client when you connect to a vCenter Server. Just click the Administration button and select the System Logs tab, and you can then choose from the various log files listed. If you select vpxd-, you will see the number of the one currently in use.

You can control the number of logs kept, the maximum size in bytes, and the amount of information written to the log by editing the vpxd.cfg file, which is in the %allusersprofile%\Application Data\VMware\VMware VirtualCenter directory on the vCenter Server. There is a section for <log>, as shown here, where you can configure this.

```
<log>
    <level>info</level>
    <maxFileSize>10485760</maxFileSize>
    <maxFileNum>10</maxFileNum>
</log>
```

Here you can change the logging level to either None, Error, Warning, Info, Verbose, or Trivia, with each level displaying more information. These levels can also be changed using the VI Client under Administration, VirtualCenter Management Server Configuration, and then choosing Logging Options. You can also change the maximum file size and number of logs. When you change these settings, you must restart the vCenter Server Windows service for them to take effect.

If you are experiencing database-related problems with vCenter Server, you can also enable database logging in the vpxd log by adding the following section beneath the </log> line in the vpxd.cfg file:

```
<trace>
    <db>
          <verbose>true</verbose>
    </db>
</trace>
```

In addition to the vCenter Server log, there are logs for some of the other components, including Update Manager, Capacity Planner, and Converter Enterprise. The logs are located in the \logs subdirectory under the various product directories, which are located in %allusersprofile%\Application Data\VMware\.

If you do increase your log levels or enable database logging to troubleshoot a problem, just remember to change them back to avoid quickly filling up your logs and causing increased utilization on your vCenter Server.

You can also generate diagnostic log bundles for your vCenter Server that you can use to send to VMware support, who will usually request them when you open a case with them. To do this, connect to your vCenter Server with the VI Client and select File, Export, and then Export Diagnostic Data. When the selection window is displayed, don't select any hosts if you want to include only vCenter Server in the output, and make sure the Include Information from VirtualCenter Server and VI Client is selected. Then enter a directory on your workstation to save it in, and it will create the bundle. The bundle will contain log files,

configuration files, dump files, and files that contain the output of various commands that are run as part of generating the bundle.

Common Problems and Resolutions

The most common problems with vCenter Server include database problems and communication problems between the vCenter Server and the hosts that it manages. When you learn to recognize the symptoms of these problems, resolving them is often fairly simple.

Database Problems

Many problems that the vCenter Server may experience are caused by issues with its database. These types of problems can be caused by different things, and in most cases you will want to work with your database administrators to resolve them. Common occurrences include the following:

- **Authentication problems.** If your vpxd.cfg log shows problems authenticating with the database server, first verify that you can successfully authenticate with the database server. Open the ODBC Administration Control Panel on the vCenter Server and select the ODBC connection for the database server and click the Test Connection button. Enter the database username and password that is used by the vCenter Server and determine whether it can authenticate. If it cannot, check with your database administrator to make sure they are correct or that the account is not locked or modified.
  If you do need to change the database username and password, you must run the vCenter Server installation again and choose to do a Repair; the wizard will ask you for a database username and password. Just be sure you select to use an existing database server and you choose to *not* reinitialize the database (which would wipe out your existing data). The reason that you need to run the installation again is that the database username and password is stored in encrypted form in the registry of the vCenter Server and can only be set when installing vCenter Server or by accessing the settings using the VI Client once the vCenter Server is running. See VMware knowledge base article 1003928 for more information about this.
- **Connectivity problems.** The vCenter Server relies on its database constantly, and losing connectivity to the database server even for short periods can cause it to stop running. The vpxd.cfg log will show any connectivity errors in it. Have your network administrators make sure there are no connectivity or latency problems between the vCenter Server and the database server. Also, check for mismatched NIC speed and duplex and make sure both the physical NIC and physical switch port are set identically (for example, 100/Full). In addition, if your vCenter Server or database server is running on VMs, check that they are getting sufficient resources and are not having bottleneck problems.

- **Tablespace problems.** For Oracle databases, the tablespace assigned to the database that is used by vCenter Server may be set to not auto-extend automatically once it reaches the maximum size that was configured when the database was created. Check with your database administrators and have them extend the tablespace if needed. See VMware knowledge base article 1003982 for more information about this.
- **Disk space problems.** A common problem when using a SQL Server database is the transaction logs filling up and subsequently the database server runs out of disk space. Have your database administrator check the recovery model that you are using. The default Full Recovery Model causes the transaction logs to grow very large. Consider switching to the Simple Recovery Model instead to greatly reduce the size of the transaction logs. You can also shrink the transaction log to reduce its size. See VMware knowledge base article 1003980 for more information about this. You may also want to purge some of the older task and event and performance data from the database; this data may be responsible for taking up most of the space in the database. Task and event data is not automatically purged and can grow quite large over time. You can also adjust the performance data-retention intervals to decrease the amount of data kept in the database. You can also manually purge old data from the database by using some SQL scripts that VMware provides. See VMware knowledge base article 1000125 for more information about this.

Host Problems

Sometimes a host will show as disconnected in vCenter Server or will not be displaying up-to-date information or statistics. This can also happen when upgrading a vCenter Server, which also updates the management agents on the hosts. If for some reason the management agent cannot be upgraded, the host will show disconnected in vCenter Server. Restarting the management agent or the hostd agent will usually resolve these types of problems. To restart both services, type `service mgmt-vmware restart` and `service vmware-vpxa restart` from the Service Console. See VMware knowledge base article 4478241 for more information about this. As mentioned earlier, restarting these services will often resolve many problems, so it is recommended to do this first before trying other options.

Troubleshooting Virtual Machines

VM problems can sometimes be challenging to troubleshoot compared to physical servers because more things can affect your VM in virtual environments. When a server becomes stuck in a physical environment, you can always unplug the power cord. This is a last resort, but in a virtual environment doing this to a host will also affect all the other VMs running on the host. At the same time, however, virtual environments have some benefits that can make troubleshooting easier, such as being able to quickly mount bootable ISO files and mounting a disk from a VM with a problem onto another VM so that it can be fixed.

Log Files

There is only one log file for VMs on a host, and it is located in the working directory on the VMFS volume for the VM. The current log file is always vmware.log, and older log files are incremented numerically (for example, vmware-5.log). You can access this log file using some of the same methods as you would for other ESX logs, including using text editors, SCP utilities, the `tail` command, and you can also use the datastore browser built in to the VI Client to access it. A lot of information is written to this log, and much of it will not be relevant to any problems you are experiencing, but you should look for any obvious error messages. In addition, check the VMkernel and hostd log files on the host that the VM is located on for any errors that may relate to the problem that your VM is experiencing.

Common Problems and Resolutions

Many common VM problems relate to the state of the VM and changing it from one state to another. Sometimes a VM will get stuck and you will not be able to easily power it off, or you may encounter difficulty powering a VM on. Other times, you might have problems with a VM not booting properly or with its virtual disk file.

Power-State Problems

These types of problems can include issues with either powering off or on a VM. Occasionally a VM will not power off when using the power controls in the VI Client. Fortunately when this happens, there are several ways to forcibly shut down the VM so that you do not have to reboot the host to fix the VM. Listed here are a few ways to kill a stuck VM that will not power off. These methods are all done using the ESX Service Console and are listed in the order of usage preference:

- **Method 1.** You can use the `vmware-cmd` command, which is the CLI equivalent to using the VI Client. Here's how:
  1. Log on to the Service Console.
  2. Type `vmware-cmd -l` to get a list of all VMs running on the host and the path to their configuration file, as shown in Figure 10.14. Note the path uses the UUID or long name of the datastore. You can optionally use the friendly name instead.

```
[root@esx2 root]# vmware-cmd -l
/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/green/green.vmx
/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/yellow/yellow.vmx
/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/orange/orange.vmx
/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/purple/purple.vmx
```

Figure 10.14 Running the `vmware-cmd` command to list running VMs

  3. You can first check the power state of the VM by typing `vmware-cmd` *`VM config file path and name`* `getstate`, as shown in Figure 10.15.

```
[root@esx2 root]# vmware-cmd /vmfs/volumes/esx2-local/purple/purple.vmx getstate
getstate() = on
[root@esx2 root]#
```

Figure 10.15 Running the `vmware-cmd` command to display the power state of a VM

4. To forcibly shut down a VM, type `vmware-cmd` *`VM config file path and name`* `stop hard`, as shown in Figure 10.16.

```
[root@esx2 root]# vmware-cmd /vmfs/volumes/esx2-local/purple/purple.vmx stop hard
stop(hard) = 1
[root@esx2 root]#
```

Figure 10.16 Running the `vmware-cmd` command to forcibly stop a VM

5. You can check the state again to determine whether it worked; if it did, the state should now be off, as shown in Figure 10.17.

```
[root@esx2 root]# vmware-cmd /vmfs/volumes/esx2-local/purple/purple.vmx getstate
getstate() = off
[root@esx2 root]#
```

Figure 10.17 Running the `vmware-cmd` command to confirm the VM has been powered off

- **Method 2.** You can use the `vm-support` command to shut down the VM by first finding the VM ID and then using the `vm-support` command to forcibly terminate it. This method does a lot more than shutting down the VM; it also produces debug information that you can use to troubleshoot an unresponsive VM.
  1. Log on to the Service Console.
  2. Type `vm-support -x` to list the VM IDs (VMID) of your running VMs. Optionally, you can also type `cat /proc/vmware/vm/*/names` to display VMIDs, as shown in Figure 10.18.
  3. To forcibly shut down the VM and generate core dumps and log files, type `vm-support -X` *`VMID`*. You will receive prompts asking whether you want to take a screen shot of the VM, which can be useful to determine whether there are any error messages, and you will also be prompted as to whether you want to send an NMI and an ABORT to the VM, which can aid in debugging, as shown in Figure 10.19. When the process completes, which can take five to ten minutes, a TGZ file will be created in the directory in which you ran the command that you can use for troubleshooting purposes. To avoid filling up your file system, when the file is created, switch to the /tmp directory when you run the command.

```
[root@esx2 root]# vm-support -x

VMware ESX Server Support Script 1.29


Available worlds to debug:

vmid=1080       orange
vmid=1085       green
vmid=1095       yellow
vmid=1100       purple
[root@esx2 root]#
[root@esx2 root]# cat /proc/vmware/vm/*/names
vmid=1080   pid=-1     cfgFile="/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/orange/orange.vm
x"  uuid="50 23 53 6b 63 f7 b5 76-ea 96 8a 31 59 81 94 d5"  displayName="orange"
vmid=1085   pid=-1     cfgFile="/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/green/green.vmx"
  uuid="50 23 bf f8 62 9b 6b 80-38 2c 4b 91 6a 6d 32 d1"  displayName="green"
vmid=1095   pid=-1     cfgFile="/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/yellow/yellow.vm
x"  uuid="50 23 b4 ab 4b 5e ad 14-f6 e4 05 39 b5 0c a2 4b"  displayName="yellow"
vmid=1100   pid=-1     cfgFile="/vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/purple/purple.vm
x"  uuid="50 23 47 07 0f be f0 b7-77 eb c4 56 40 ab 6f b9"  displayName="purple"
[root@esx2 root]#
```

Figure 10.18 Running `vm-support` and `cat` to obtain a list of running VMs and their VMIDs

```
[root@esx2 root]# vm-support -X 1095

VMware ESX Server Support Script 1.29

Preparing files: |

Can I include a screenshot of the VM 1095? [y/n]: n
Can I send an NMI (non-maskable interrupt) to the VM 1095? This might crash the VM, but could aid
in debugging [y/n]: y
Can I send an ABORT to the VM 1095? This will crash the VM, but could aid in debugging [y/n]: y
Preparing files: \
Grabbing data & core files for world 1095. This will take 5 - 10 minutes.


Taking performance snapshots.  This will take about 300 seconds.

Starting detailed scheduler stats.

Starting vscsiStats.
Snapping 7: 207  seconds left.
```

Figure 10.19 Running `vm-support` to forcibly stop a VM

4. You can check the state of the VM again either by using the `vmware-cmd` command or by typing `vm-support -x`, and you should not see the VMID for that VM listed anymore.

- **Method 3.** You can use the `kill` command by first finding the process identifier (PID) of the VM and then using the `kill` command to forcibly terminate it.
  1. Log on to the Service Console.
  2. Type `vmware-cmd -l` to get a list of all VMs running on the host and the path to their configuration file. Note the path uses the UUID or long name of the datastore. Optionally, you can use the friendly name instead.

3. You can first check the power state of the VM by typing `vmware-cmd` *`VM config file path and name`* `getstate`.
4. Type `ps auxfww ¦ grep` *`virtualmachinename`* to get the PID of the VM, as shown in Figure 10.20. You will have two entries returned. The longer entry that ends in the config filename of the VM is the correct one. The number in the second column of that entry is the PID of the VM.

```
[root@esx2 root]# ps auxfww | grep purple
root      1050  0.0  0.2  3700  676 pts/0    S    10:58   0:00          \_ grep purple
root     31253  0.0  0.3  2012  908 ?        S<   10:23   0:00 /usr/lib/vmware/bin/vmkload_app /us
r/lib/vmware/bin/vmware-vmx -ssched.group=host/user -# name=VMware ESX Server;version=3.5.0;licens
ename=VMware ESX Server;licenseversion=2.0 build-123630; -@ pipe=/tmp/vmhsdaemon-0/vmx1d7a697443d6
e5f0; /vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/purple/purple.vmx
[root@esx2 root]#
```

Figure 10.20 Running the `ps` command to get the PID of a running VM

5. Type `kill -9` *`PID`* to forcibly terminate the VM, as shown in Figure 10.21.

```
[root@esx2 root]# ps auxfww | grep purple
root      1372  0.0  0.2  3692  672 pts/0    S    11:03   0:00          \_ grep purple
root     31253  0.0  0.3  2012  908 ?        S<   10:23   0:00 /usr/lib/vmware/bin/vmkload_app /us
r/lib/vmware/bin/vmware-vmx -ssched.group=host/user -# name=VMware ESX Server;version=3.5.0;licens
ename=VMware ESX Server;licenseversion=2.0 build-123630; -@ pipe=/tmp/vmhsdaemon-0/vmx1d7a697443d6
e5f0; /vmfs/volumes/4979f8f9-a7e0850c-0dd0-000802edb060/purple/purple.vmx
[root@esx2 root]#
[root@esx2 root]# kill -9 31253
[root@esx2 root]#
```

Figure 10.21 Using the `kill` command to forcibly stop a VM

6. You can check the state again to determine whether it worked. If it did, the state should now be off.

Additional power problems may occur when attempting to power on a VM. If this happens, check that there are enough resources available for the VM to meet any reservations that the VM may have assigned to it. If a VM has a 2GB memory reservation and the host does not have 2GB of free physical RAM available, the VM will not be allowed to power on. Instead, you will need to remove the reservation, move the VM to another host with enough free memory, or shut down or move other VMs to free up memory on the host. In addition, ensure that you have enough free disk space for the VSWP file that is created when the VM is powered on and removed when it is powered off. The VSWP file needs enough disk space equal to the amount of memory assigned to the VM minus the VM's memory reservations. You can set a memory reservation equal to the amount of memory assigned to the VM, which will result in a 0-byte VSWP file being created, but you should always take care to leave sufficient disk space free on your VMFS volumes for logs, VSWP files, and snapshots.

Other Problems

Sometimes you might encounter problems with your VMs not booting properly because of configuration changes or operating system problems. Virtual environments make these types of problems relatively easy to fix. You can easily mount an ISO file to the VM's CD/DVD-ROM drive and boot from a live CD (for example, Ultimate Boot CD or Knoppix) to fix the problem. In addition, you can mount the VM's disk file onto another VM, where you can access the file system and fix any issues with it. Just add a new virtual disk to another working VM and choose an existing disk and browse to the problem VM's virtual disk. Then power on the working VM and you can access the problem VM's disk as an additional drive. When you have finished, remove (not delete) the problem VM's disk from the working VM and power on the problem VM to determine whether the problem has been resolved.

Summary

Troubleshooting can often be frustrating and challenging, and knowing where to look and what to do is the key to quickly finding and resolving problems. You shouldn't just look through log files when you are experiencing known problems, however. Often, many problems might not be that obvious, and the log files are a good place to look for signs of them happening. You should keep a list of all the log files handy so that you can quickly access them if needed and so not have to waste time when a problem is happening trying to remember their path and filenames. You might not know how to resolve or troubleshoot every problem you encounter, so be sure to rely on the resources available to you, including documentation, support forums, knowledge base, and VMware's technical support. Being properly prepared to handle problems when they occur is one of the best troubleshooting skills that you can have.

Additional Resources

Listed here are some additional resources that will help you troubleshoot and resolve problems with your virtual environment.

VMware Knowledge Base

VMware puts considerable time and effort into their online knowledge base (http://kb.vmware.com), as shown in Figure 10.22, and it is full of fantastic information.

The knowledge base contains a lot more than solutions to known problems and issues. It also contains many how-to and troubleshooting documents. I urge you to periodically browse through the knowledge base and sign up for the weekly update emails that list all the new entries to the knowledge base. The knowledge base should be the first place you start when troubleshooting any problems. You can search on the keywords of the symptom of your problem and narrow the results by choosing your product name.

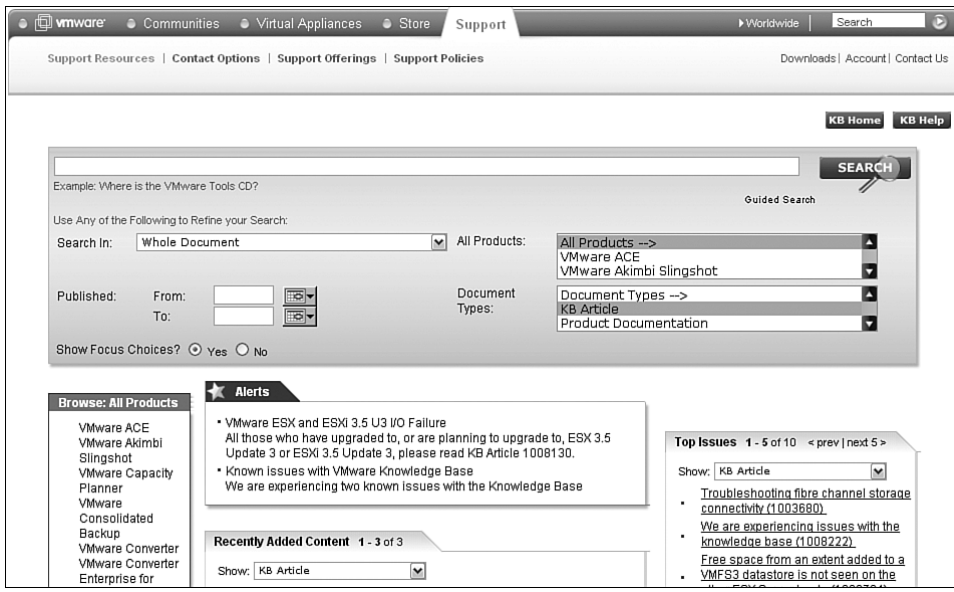

Figure 10.22 VMware's knowledge base website

VMTN Forums

VMware has one of the best technical support forums around: the VMTN support forums (VMware Technology Network, http://communities.vmware.com/community/vmtn), as shown in Figure 10.23.

The discussion forums are filled with other VMware users from all over the world who use their knowledge and experience to assist others with problems and questions. The level of participation in these forums is very high; it is not uncommon to get an answer to your question in minutes and usually by multiple people. The forums are unofficially known as VMware's tier 1 support. You can usually get your problem/question resolved in the forums faster than it would take you to call VMware. There are many VMware experts in these forums who help others just for the feeling of satisfaction that comes with helping someone else solve a problem.

A point system also exists that allows the author of a topic to reward helpful answers with points as a form of recognition. The forums tend to be very competitive, with users competing to collect points for posting responses to questions. Six points can be awarded by the person who asked the question for up to two helpful responses, and ten points can be awarded to one response that is deemed correct. The point system allows people to gain status levels as their points increase. There are nine status levels, ranging from Lurker (0–5 points) all the way up to the elite Guru level (20,000+ points). There are more than 500,000

forum members, with an average of about 20,000 new members being added each month. Figure 10.24 shows the multiple status levels that users can achieve in the forums.

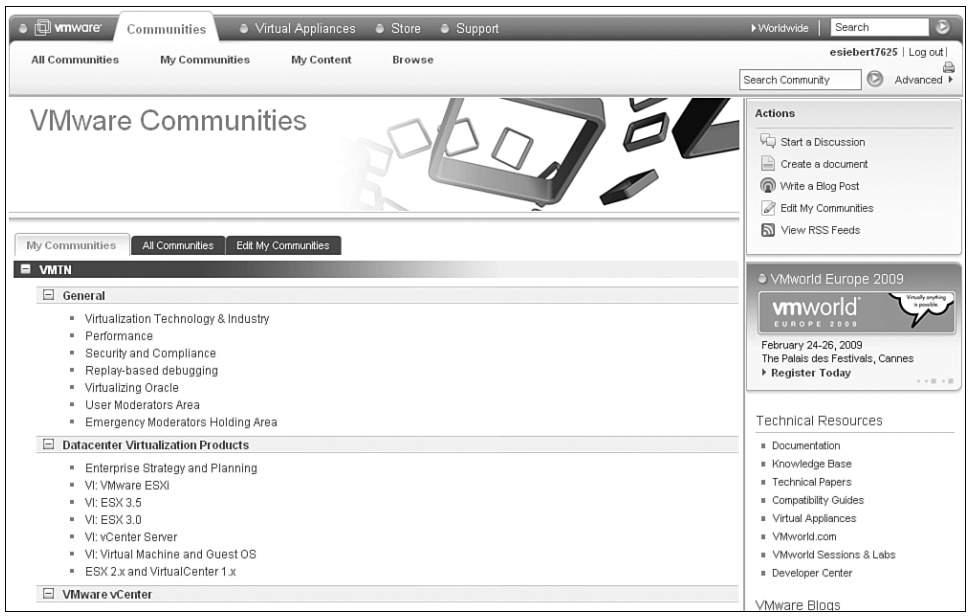

Figure 10.23 VMware's VMTN support forums

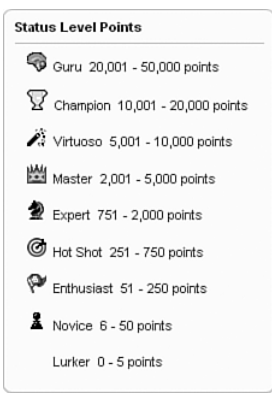

Figure 10.24 VMTN forum status levels

The forums are also a good place for users of all levels to discuss advanced subjects and share methods and experiences with each other. There is also a fair amount of participation from VMware employees who do their best to also lend a hand in the forums. I spent a lot of

times in the forums when I was trying to learn more about VMware. I've made countless friends there, and would like to mention some of the most active VMTN contributors who consistently go out of their way to help others in the forums. These are a very bright, experienced bunch of guys, and if you are fortunate enough to have one of them answer your question, be assured that you are in very capable hands:

- Dave Mishchenko (forum name Dave.Mishchenko)
- Ken Cline (forum name Ken.Cline)
- Oliver Reeh (forum name Oreeh)
- Steve Beaver (forum name Sbeaver)
- Jason Boche (forum name Jasonboche)
- Edward Haletky (forum name Texiwill)
- Tom Howarth (forum name Tom Howarth)

So don't be afraid to ask your questions in the forums, and be sure to search on anything that you need help with. Chances are your question may have been already asked and answered. If you use any VMware product, I highly recommend that you head on over to the forums and check them out, even if you do not have a question of your own. Reading through some of the posts from others is a great way to expand your own knowledge as you benefit from the experiences of others. I also find that helping others in the forums is a great way to help yourself, because teaching and helping others is a great way to help yourself learn, too.