Global Knowledge®

Expert Reference Series of White Papers

Seven Tips for Troubleshooting VMware vSphere 5

Seven Tips for Troubleshooting VMware vSphere 5

Steve Baca VCP, VCI, Global Knowledge Instructor

Introduction

This white paper discusses seven tips for working with vSphere 5. Some of the topics are: logging in via Command Line, dealing with connection problems using ssh to an ESXi host, and important log files and their locations. In addition, some of the tips are going to look at dealing with performance-related issues, such as networking and storage.

1. Logging in via Command Line
2. Performance Monitoring Tools
3. If You Suspect a Network Performance Issue
4. Metrics to Check for a Possible Storage Problem
5. Log Files to View in vSphere ESXi 4.x
6. Last-Level Cache (LLC) performance issue
7. Cannot Migrate a Virtual Machine (VM) Using VMotion

1. Logging in via Command Line

By default, the ESXi host does not have ssh enabled, and the method to enable ssh can change based on whether or not the host is ESX or ESXi, and the version of the ESX/ESXi host. There are occasions when you need to login via command line using ssh to troubleshoot problems. In addition, there are alternative methods to get to a command line prompt such as DCUI and TSM, depending on the version and type of host. The ability to manage the host at a command line prompt will allow you to use many different Unix based commands as well as commands introduced by VMware called **esxcli** commands. The ability to make changes to network, storage and other critical parts of the host, depending on the state of the host, might only be possible at a command line prompt.

ESXi 5

In vSphere 5, an administrator can manage the ESXi host from the command line using esxcli commands, such as **esxcli network vswitch standard**. The esxcli command set was first introduced in vSphere 4.0 and allows an administrator to manage many aspects of the ESXi host from the command line. The commands are available using the Direct Console User Interface (DCUI) to access the ESXi shell, using a remote application like putty to ssh into the host, or through the vSphere Command-Line Interface (vCLI).

The DCUI is similar to the BIOS of a computer and allows you to interact with the host through the console of the ESXi server to perform initial basic configuration and can also be used for troubleshooting using text-based menus. You can use the DCUI to enable local and remote access to the ESXi Shell.

A second method to access the command line is by utilizing an application such as putty to ssh into the ESXi host. In order for ssh to work you must enable the sshd service on the ESXi host.

A third method to run command line commands is thru vCLI. The vCLI provides a command-line interface for ESXi hosts. Multiple ESXi hosts can be managed from a central system with vCLI installed on it. The central system that VMware uses is a downloadable appliance called vMA. vMA enables administrators to run scripts that interact with ESXi hosts and VMware vCenter Server systems without having to authenticate each time. vMA is easy to download, install, and configure through the vSphere Client.

Direct Console User Interface (DCUI)

1. When the DCUI screen appears, press **F2 Customize the System** and login as root.
2. Scroll to T**roubleshooting Options** and press **Enter**.
3. Choose **Enable ESXi** shell and press **Enter**.
4. Press **Esc** until you return to the main DCUI screen.

To enable ssh from the vsphere Client

1. Select the host and click the **Configuration** tab.
2. Click **Security Profile** in the **Software** panel.
3. In the **Services** area, click **Properties**.
4. Select **ssh** and click **Options**.
5. Change the ssh options. To change the Startup policy across reboots, click **Start and stop with host** and reboot the host.
6. Click **OK**.

ESXi 4.1

First method from the Direct Console User Interface (DCUI)

1. Hit **Alt+F1**, if TSM is enabled, log in with root credentials, else
2. Once the DCUI screen appears, press **F2** and login as root to enable the TSM.
3. Navigate down the screen and choose **Troubleshooting Options**, and press **enter**.
4. **Troubleshooting Options** provides additional options for TSM in ESXi 4.1.

   <Enable/Disable> Local Tech Support – Access command line via Alt+F1 on the console.

   <Enable/Disable> Remote Tech Support (ssh) – ssh access on the console of the ESXi host.

   Modify Tech Support Timeout – Tech Support Mode will be disabled after a certain amount of time.

Second Method from the vSphere Client

1. From the vSphere Client, select the host and click **Configuration** tab.
2. Then choose **Security profile** and **Properties**.
3. Here you can enable **Local Tech Support** as well as **Remote Tech Support** (ssh). They are enabled if the Daemon is running, and disabled if the Daemon is **Stopped**.

   If you want to enable either mode, highlight the mode, then choose **Options.**
4. Now you can modify the Startup Policy or change the Service to **Start**, then click **OK**.

Access the local TSM (Local Tech Support):

At the main DCUI screen, press **Alt+F1**, login.

Access the remote TSM:

Use a utility, such as putty, to establish an ssh connection.

ESX 4.x and Earlier

If you are using an ESX 4.x or earlier host, then you will need to use a third-party tool like putty to ssh into the ESX box. Essentially, you are logging into the service console, which is running Red Hat Linux. The challenge comes with ESXi because ESXi does not have a service console, although it is possible to setup a virtual appliance called vMA to run the command line. However, we are going to take a more direct approach and use no service console and no ssh. Instead let's look at a method called **Tech Support Mode**, which is a hidden or unsupported method to gain command line access to the host. Essentially, you are enabling the ssh daemon directly on VMware's proprietary version of Unix where the hypervisor is running, enabling the root user to either log in directly on the console of the ESXi host, or log in remotely via ssh.

ESXi 3.5 or 4.0

1. To start, check the **techSupportMode** setting. To make sure this setting is correct, log into the vCenter Server, using the vSphere Client. Depending on version, this may not be necessary.
2. Select the **ESXi host** and choose the **Configuration** tab, then select **Advanced Settings** in the **Software** panel. In the left pane, click **VMkernel**.
3. Enable **VMkernel.Boot.techSupportMode** and click **OK**. Reboot the ESXi host if you need to enable technical support mode.
4. To use Tech Support Mode, log in to the ESXi host using the **Direct Console User Interface** (DCUI).
5. Press **Alt+F1** to display the console screen.
6. Enter by typing *unsupported* to start the Tech Support Mode process. Note that no text will appear on the console window.
7. Enter the password for the root user, and you should than see an ssh prompt.

2. Performance Monitoring Tools

There are a couple of built-in tools in vSphere that can be utilized to monitor performance and help in diagnosing problems, vSphere performance charts and esxtop.

The vSphere performance charts allow you to display useful information when you are connected either to the ESXi host directly or to the vCenter Server. However, the problem with the vSphere performance charts are that they do not have the granularity that esxtop does. The performance charts can provide a lot of useful information, even if they do not provide all of the counters that you will find with esxtop.

The host based tool esxtop provides for some inherent advantages over the vSphere performance charts and third-party tools when it comes to performance analysis. One big advantage is that esxtop incurs very little overhead on the ESXi host. Since, esxtop is lightweight and the footprint is small, it is an excellent tool to measure performance. If you have a situation where poor performance is affecting connectivity to the host, you can use resxtop (remote esxtop). Another advantage of using esxtop is you can export the data into a comma delimited file. This gives you the ability to export the data into a CSV file or a flat text file. And than the data can be viewed offline or placed back into a third-party utility such as esxplot, Windows Perfmon, or even a Microsoft Excel spreadsheet. For more information about esxtop and its counters: http://communities.vmware.com/docs/DOC-9279.

3. If You Suspect a Network Performance Issue, Check Some of the Following Metrics

If the droppedRx (receive) is greater than 0 for a host, look at the CPU utilization. The CPU plays an important part in moving the packets from the guest operating system on the VM to physical device driver. Check metrics such as CPU overhead and high CPU utilization, which can cause the VM to be too busy to take on new packets or delays in receiving the packets. A possible solution is to increase CPU reservations for the VM or check the application to see if it supports adding more vCPUs.

If the droppedTx (transmit) is **greater** than 0, this usually means congestion at the physical layer. When a VM is transmitting packets, the packets get queued in the buffer of the virtual switch port until the packets are transmitted on the physical nic. The buffering of packets on the virtual switch port waiting to transmit can even cause incoming packets to be dropped. To prevent the dropping of transmit packets, look for ways to increase the physical network capabilities. Adding more nics or adding 10 GB Ethernet could solve the problem by increasing the physical network capacity.

Another thing to look for on the network side is to make sure you have the correct network device driver installed on the VM. By default, if **VMware tools** is not installed or running, the Vlance network adapter will be used. Vlance is a 10Mbps NIC, which is great for older 32-bit guest operating systems but not so useful running in a 1 GB Ethernet network. Therefore, you want to make sure that VMware tools is installed and is enabled, and that the correct network adapter for the operating system is installed in the VM.

4. Metrics to Check for a Possible Storage Problem

It is always important to consider storage performance in your vSphere environment. **esxtop/resxtop**, which comes with ESXi 5, is an excellent tool to measure performance. Some of the more significant statistics are commands queued. To check these metrics, open a vSphere Management Assistant (vMA) console and start **resxtop**. Type **d** to enter the Storage Adapter screen. Type **f** to select the fields that you want to view. The fields to view should be **A** (adapter name), **F** (queue stats), and **K** (error stats).

An important factor that can affect storage performance is queuing. Queuing will happen if there are excessive I/O operations and the buffer is full, which means that the host is waiting for the storage to complete outstanding I/O requests. The **ACTV** metric is the number of I/O operations that are currently active, and QUED is the number of commands waiting to be processed. **QUED** is the key value: this number should be zero; otherwise, the host is bottlenecking. Commands will be aborted if the storage is overloaded.

There are other esxtop fields that can be utilized to indicate that there could be a storage problem. To identify disk-related performance problems look at throughput and latency.

Throughput fields in esxtop (READS/s + WRITES/s = I/O operations/second (IOPS):

READS/s – Number of disk reads per second

WRITES/s – Number of disk writes per second

Latency fields in esxtop:

DAVG – Average delay from the adapter to the target in ms, value greater than 10-15 milliseconds indicates that the storage might be slow or overutilized

KAVG – Average delay from the vmkernel to the adapter in ms, value greater than 4 milliseconds indicates the VMs are attempting to send more data to storage than the storage can handle

GAVG – Average delay for the guest, which will be DAVG + KAVG = GAVG

High DAVG numbers also could indicate that there is a problem beyond the adapter of the ESXi host. There could be an overloaded or bad zone, over-used storage processors, too few disks on the RAID configuration, or other issues beyond the host. Whatever the cause, the problem is that it is taking too long for the acknowledgments from the storage array to come back to the host.

High KAVG numbers could indicate a problem at the host level, such as not enough memory or a full command queue.

When storage becomes severely overloaded, commands will be aborted due to the storage system's inability to acknowledge commands. The esxtop counter **ABRTS/s** will give you the number of dropped requests on an overloaded storage.

5. Log Files to View in vSphere 5

vSphere 5 adds several enhancements to system message logging. All log messages are now generated by syslog, and messages can now be logged on either local and one or more remote log servers, or both. In addition, a given log server can log messages from more than one ESXi host. The log file contents are especially useful to VMware support, and can provide clues to help support troubleshoot performance issues. When you call VMware support you will be asked to use the vSphere client to provide the system logs by compressing the log files into one archived file. This is accomplished by selecting **Home** > **Administration** > **System Logs** and then choose **Export System Logs**.

Syslog is a standard for forwarding log messages in a TCP/IP network.

To view ESXi system logs, in the vSphere Client menu bar, select **View** > **Administration** > **System Logs**.

/var/log/auth.log	ESXi Shell authentication success and failure.
/var/log/dhclient.log	DHCP client service.
/var/log/esxupdate.log	ESXi patches and updates log.
/var/log/hostd.log	Host management service logs.
/var/log/shell.log	ESXi Shell usage, including enable/disable and every command entered.
/var/log/sysboot.log	VMkernel startup and module loading.
/var/log/syslog.log	Management service initialization, watchdogs, scheduled tasks, DCUI.
/var/log/usb.log	USB device arbitration events, such as discovery and pass-through to VMs.
/var/log/vob.log	VMkernel Observation events, similar to vob.component.event.
/var/log/vmkernel.log	Core VMkernel logs (devices, storagage/network device/driver events, and VM startup.
/var/log/vmkwarning.log	VMkernel Warning and Alert log messages.
/var/log/vmksummary.log	ESXi startup/shutdown, uptime, VMs running, and service resource consumption.

Logs from vCenter Server Components on ESXi 5

/var/log/vpxa.log	vCenter vpxa agent logs.
/var/log/fdm.log	High Availability logs, produced by the Fault Domain Manager (FDM) service.

6. Last-Level Cache (LLC) Performance Issue

The ESXi CPU scheduler, by default, tries to place the vCPUs of a Symmetric Multiprocessor (SMP) VM into as much Last-Level Cache (LLC) as possible.

VMware support has seen an increase in performance problems due to the new CPUs utilizing LLC cache. The idea is that LLC is a shared cache for multi-core cpus. Each core inside a CPU package has its own L1 and L2 cache that is dedicated to that particular core. But with the modern multi-core processor, one of the things that the CPU vendors are doing is building a last-level cache around all of these cores so it's a shared cache for all

of the CPUs. Now ESXi, by default, is going to place as many vCPUs of a SMP VM into as many of the L LLCs as possible. Therefore, ESXi is going to attempt to spread out the cycle, and find space to run the workload. But for some workloads it's inefficient to use mostly LLC. If the application is a database server or an application that relies upon heavy CPU resources, than the default behavior can affect performance. If you are running a very CPU-intensive workload, you might benefit from setting up a clone of the application VM. Then turn on the LLC setting below and test the cloned application to see if there is a performance increase. If the modification works, the CPU scheduler is going to attempt to consolidate the vSMP VM into one CPU package, thus one shared LLC pool. Therefore, the CPU scheduler will now attempt to run the VM on the same package more than it would otherwise.

Using the vSphere client:

1. Power off the VM.
2. Right click the VM and select **Edit Settings**.
3. Select the **Options** tab.
4. Under **Advanced**, click **General**, and on the right click the configuration **Parameters** button.
5. Click **Add Row**.
6. Add **sched.cpu.vsmpConsolidate** set to **true**.
7. Power on the VM.

From the command line interface:

1. Power off the VM.
2. Add the following line into the configuration file (.vmx) of the VM.
3. **sched.cpu.vsmpConsolidate = "true"**.
4. Power on the VM.

Any new details on this problem can be found at VMware's knowledge base website. VMware keeps the site up to date.

kb.vmware.com KB article #1017936

7. Cannot Migrate a VM Using VMotion

Check the ESX(i) hosts to make sure all of the requirements have been met. Then check to make sure that the CPU is compatible. CPU compatibility is important in VMware and, if this is a problem, you might have to enable EVC to allow the feature set of both host CPUs to match. This can solve minor incompatibility issues.

If the VM is running a 64-bit operating system, the problem might be that the source machine has Intel Virtualization Technology (VT) enabled in the BIOS, and the destination host does not have VT enabled in the BIOS. If this is the case, you will have to make a change in the BIOS so both hosts match.

Also, both hosts must have a VMkernel port on the same LAN. The IP address and subnet mask should match the network configuration for VMKernel gateway.

You could run from command line:

 # vmkping <Destination_IP _address> to test the VMkernel TCP/IP stack.

Any VLAN settings should match the VLAN configuration of the local LAN. VMkernel ports should have the check box VMotion enabled. There should be no router separating the hosts.

- Check the VMs to make sure all of the requirements have been met.
- Check that there are no local devices connected to the VM.
- Check CD-ROM mappings to any ISO file on local storage, Floppy, SCSI, USB, CPU affinity, .vswp files stored on local storage.
- Check that the VM has enough CPU and memory resources on the destination host.

Check to be sure that the VM fully powered on. To check the status of the VM, simply open the console in vSphere to make sure the VM is fully powered on.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, check out the following Global Knowledge courses:

VMware vSphere: Fast Track [V5]

VMware vSphere: Install, Configure, Manage [V5]

VMware vSphere: Optimize and Scale [V5]

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Steve Baca has been working in the Information Technology field for more than 15 years, after graduating from the University of Nebraska with a Bachelors degree in Computer Science and Mathematics. Steve has been doing technical training for VMware, Netapp, Sun Microsystems, and Symantec. In addition to teaching, Steve has done technical editing. He wrote the course for Sun Microsystems Network Troubleshooting, as well as several white papers.