ActualTech Media

# Solving the Five Most Common VMware Virtual Machine Issues

**By David Davis, vExpert**

Co-Founder, ActualTech Media

January, 2015

# Introduction

Based on the analysis of several million virtual machines by opvizor, it's likely that you have already experienced, or will soon experience, one or more of the most common virtual machine issues. Rather than struggling to solve these issues (and possibly cause downtime in the process) why not solve these issues before they ever happen? In this whitepaper, you will learn about the top five most common virtual machine issues, how they impact you, how to detect them, the benefits to solving them, and, ultimately, how to solve them.

# #1. VMware Tools Are Outdated or Not Installed

The most common issue with a vSphere virtual machine is that the VMware Tools are either not installed or are out of date. The VMware Tools are a suite of utilities intended to enhance the performance of the virtual machine's guest operating system and improve the ability to manage the virtual machine. With each new version of vSphere, VMware also updates VMware Tools and, with some version of vSphere, administrators must proactively update Tools in each virtual machine in order to experience the benefits of the new features provided by VMware. As shown in Figure 1, "VMware Tools is out of date on this virtual machine" is a message that is very common in VMware environments in which VMware Tools is not consistently updated.

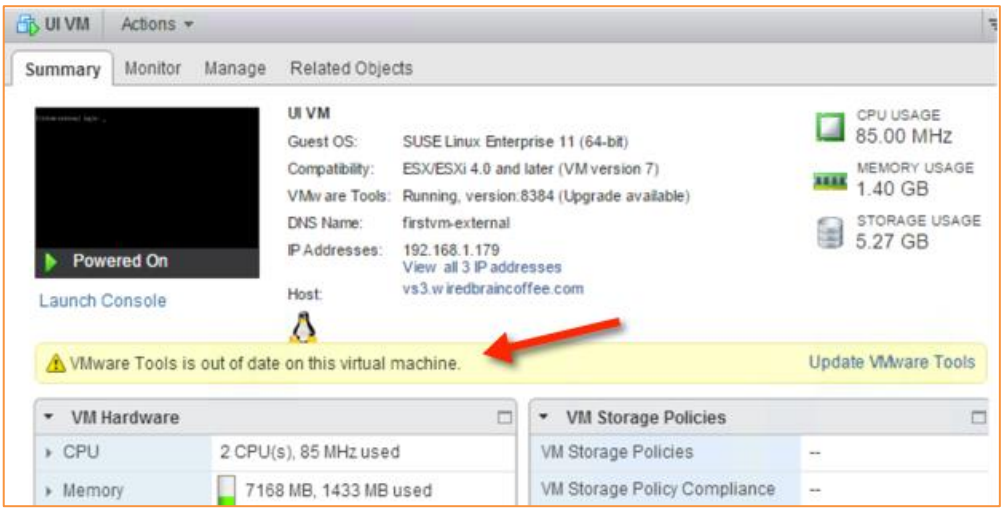


Figure 1: VMware Tools is out of date on this virtual machine

## Impact

Although the guest operating system can run without them, many VMware features are not available until you install VMware Tools. For example, if you do not have VMware Tools installed in your virtual machine, you cannot interact with the Guest OS to perform a graceful / clean shutdown or restart. This means you can only use the VM power options to perform a hard power off or power on of the virtual machine from the toolbar.

VMware Tools also improve the virtual machine's storage I/O, graphics performance, and allows the virtual machine to synchronize its clock with that of the host. Virtual machine performance is boosted with VMware Tools by enabling the use of *paravirtualized* devices such as the VMXNET3 network and paravirtualized SCSI devices. Paravirtualized devices require specialized device drivers, which are provided by VMware Tools.

Finally, reclamation of unused memory from each virtual machine won't be possible without the VMware Tools being installed, as memory ballooning and transparent page sharing won't be available. Memory ballooning is a technique by which a vSphere host, when it's running low on physical RAM, can reclaim RAM from guest virtual machines that may not be using the full complement of RAM currently assigned. Transparent page sharing is a method that allows virtual machines to share memory pages through what is essentially a memory deduplication process. The result of not being able to use such memory management techniques is that your virtual-machine-to-host consolidation ratio will be lower and your return on investment from the virtual infrastructure will be negatively impacted.

If you have the VMware Tools installed but they are out of date, you will lose some functionality depending on how out of date the VMware tools are.

## Ease of Detecting

Identifying that you have virtual machine with Tools that are out of date or not installed at all is easy to do. The virtual machine Summary tab in vCenter will show the status of the VMware Tools on that specific virtual machine.

To find out of the status of the VMware Tools across the entire vSphere infrastructure, go to the vCenter Inventory level, click on Related Objects, and then go to the Virtual Machine inventory. Here you will likely need to add the "VMware Tools Version Status" column to the report. To do this, right-click on the storage report column headers and click Show/Hide Columns, as shown in Figure 2. Next, click on the VMware Tools Version Status option to add it to the view, as shown in Figure 3. From there, you can sort and group all the VMware tools versions that are similar by clicking on the column header entitled VMware Tools Version Status, as shown in Figure 4.

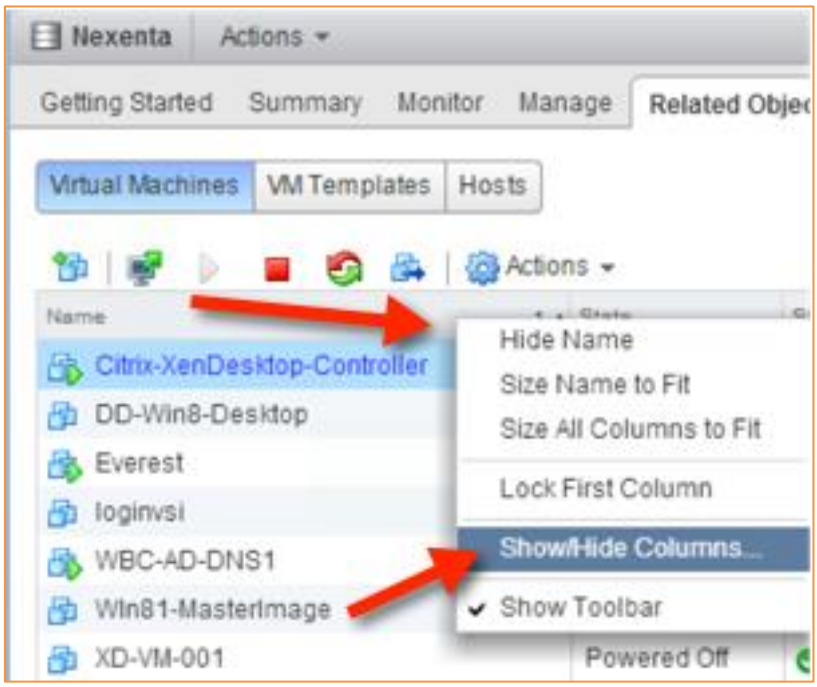


Figure 3 - Virtual Machine Tools Status

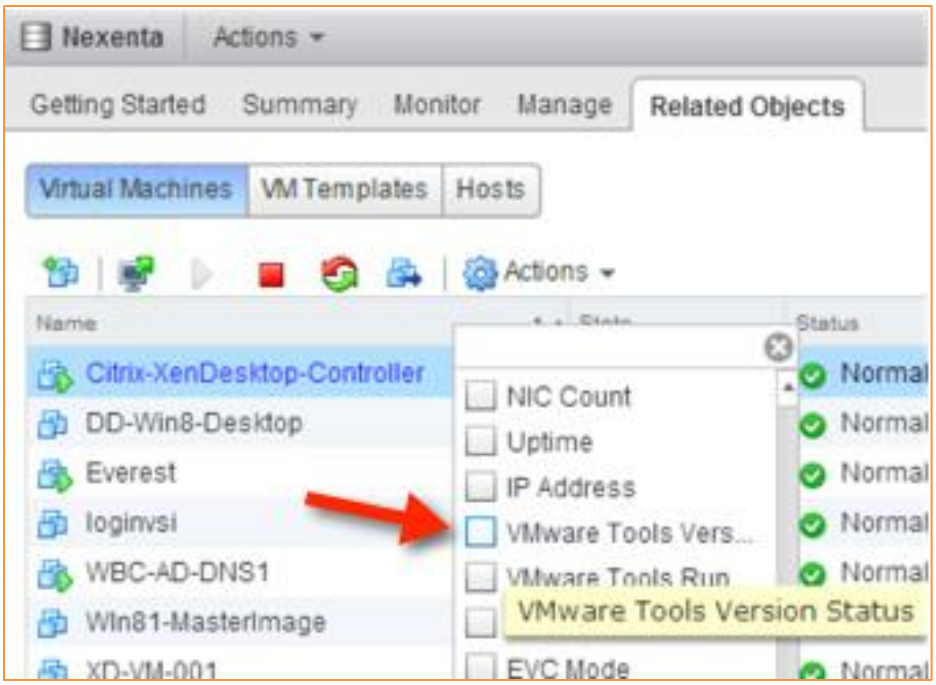


Figure 6 - Adding More Columns to the View

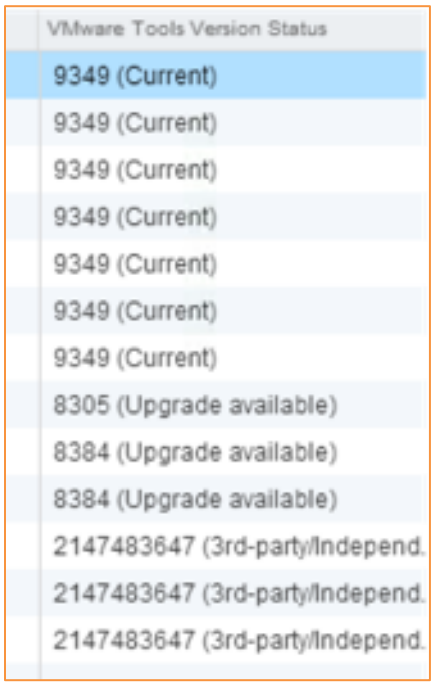


Figure 7 - Adding VMware Tools Version Status to the View

Additionally, you can run a PowerCLI script — which you can find at this link — to output the overall VMware Tools status.

## Benefits to Solving

The benefits to installing (or at least upgrading) the VMware Tools include:

- Gaining the ability to shut down or restart the guest OS from the vSphere client
- Improving guest OS performance
- Reducing resource utilization and improving VM to host consolidation ratio, which improves the ROI for the virtual infrastructure environment

## Ease of Solving

Installing or updating the VMware Tools is quickly accomplished through the vSphere Web Client. This installation or update may not even require a reboot of the virtual machine guest OS.

If VMware Tools need to be upgraded, you'll be prompted on the Summary tab of the virtual machine, as shown in Figure 5.

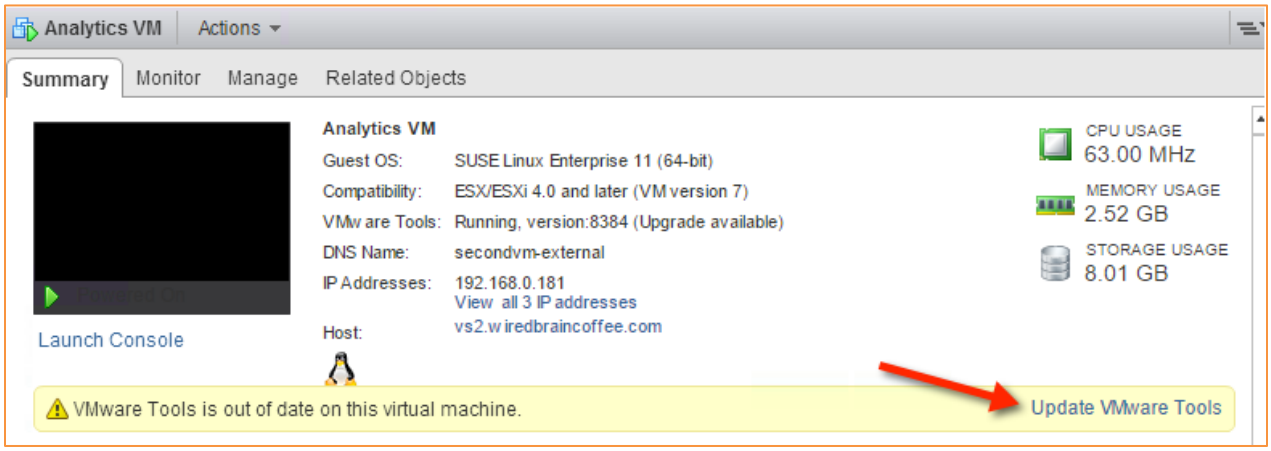


Figure 8: Prompted to update VMware Tools

Alternatively, you can right-click on the virtual machine go into All vCenter Actions, Guest OS, and click on Upgrade VMware Tools (shown in Figure 6), then follow the prompts inside the guest OS.

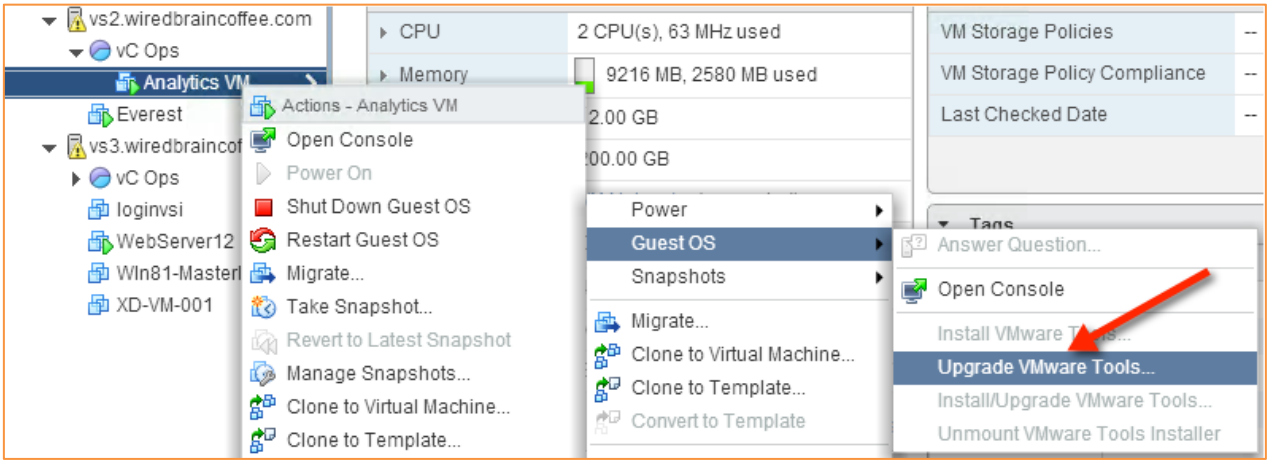


Figure 6: Upgrading VMware Tools

If you prefer to use the command line to accomplish your goal, the PowerCLI cmdlet is available via Update-Tools.

## How opvizor Helps

Rather than remembering to periodically search for virtual machines with older versions of VMware Tools, or on virtual machines that don't have any VMware Tools installed, opvizor continuously scans the environment for virtual machines that need their VMware Tools updated or installed (Figure 7). Not only does this save analysis time, it also ensures that you remain continuously aware of the status of your virtual machines, and that you can ensure that your virtual machines are always performing optimally.


Figure 7: opvizor identifying a VM with out-of-date VM tools

# #2. Old Virtual Machine Network Devices

Network performance in many vSphere virtual machines is typically less than what it otherwise could be as, in most cases, virtual network devices are not kept up-to-date as they should be. For example, if your virtual machine was created with a vSphere flexible NIC and you later upgrade the virtual machine hardware as new versions of vSphere are released, you could unknowingly end up with that virtual machine being subjected to using a virtual NIC that operates at a measly 10Mbps. No matter your situation, your network performance – which ultimately impacts application performance – could be greatly improved by using a new virtual network device and driver.

## Impact

By unknowingly using outdated virtual network devices, you could experience unexpected and unexplained poor application performance. This poor network performance is caused by

inefficiencies in the virtual network adaptor in use causing a higher number of IRQ requests than needed. This is especially problematic for virtual machines with applications that create high network load and packet generation such as virtual file servers, firewalls, and transaction processing servers. Not only will end users complain about poor performance and the inability to do their job, administrators may be confounded as to why the problem exists at all.

## Ease of Detecting

To detect old virtual network devices, you can manually verify the virtual network adaptor configuration on each virtual machine by clicking on the virtual machine settings and then expanding the virtual network adapter to verify the version (see Figure 8). VMware recommends the VMXNET3 virtual network adaptor type for optimal performance.

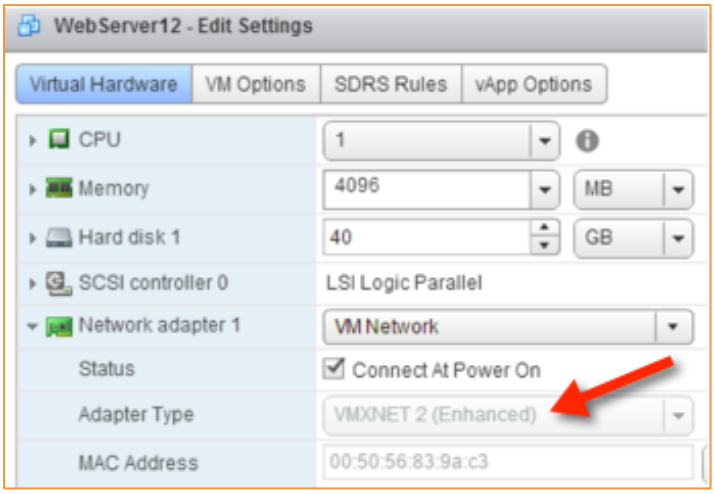


Figure 8: Viewing the Virtual Network adaptor type on a VM

If you have a large number of virtual machines this can become unwieldy. Instead, an automated tool that can detect these types of issues is needed in medium and large virtual environments.

## Benefits to Solving

By upgrading from an old virtual network device, such as a Vlance adaptor, to the latest VMXNET3 paravirtualized network drivers, network performance can be dramatically improved. This is because a Vlance adapter creates many more unnecessary IRQ requests compared to a VMXNET3 and a Vlance is not able to use any of the physical NIC features to offload and optimize network packets. Therefore older network virtual network devices can cause slowness for the VM they are attached to as well as negatively affect all other VMs due to the noisy neighbor syndrome.

## Ease of Solving

The easiest way to solve this issue is to use the following four-step process. (Note that the virtual machine must be rebooted to update the virtual network adaptor type.)

1) Upgrade the virtual machine hardware by:
    a. Shutting down the virtual machine.
    b. Right-clicking on the virtual machine.
    c. Going to "All vCenter Actions," to "Compatibility," and then clicking on "Upgrade VM Compatibility."
    d. Select the new VM compatibility mode to the latest compatibility mode which, as of today, is ESXi 5.5 and later, then click OK.
2) Add a new virtual network adaptor by:
    a. Clicking "edit settings" for the virtual machine.
    b. Clicking on "Select" next to New Device.
    c. Clicking on "Network."
    d. Clicking "Add" then setting the new virtual network device's network to match the current network of the out of date virtual network adaptor.
    e. Expanding the virtual network device.
    f. Setting the adaptor type to the latest version (which at this time is VMXNET 3).
3) Remove the old virtual network adaptor (which is still in settings) by clicking on the *X* next to the old adaptor, then clicking OK.
4) Power On the virtual machine and, once booted, reconfigure the new virtual network adaptor with the IP configuration of the old virtual network adaptor.

## How opvizor Helps

In order to prevent poor application performance as a result of outdated network adapters, opvizor is able to quickly identify the virtual machines that run such virtual network adaptors (Figure 9). With this information, you'll be able to update the virtual machines that are out of date and prevent application performance issues before they impact users. Additionally,

you'll be able to eliminate the finger pointing that all too commonly occurs when there is poor network performance in the virtual infrastructure.

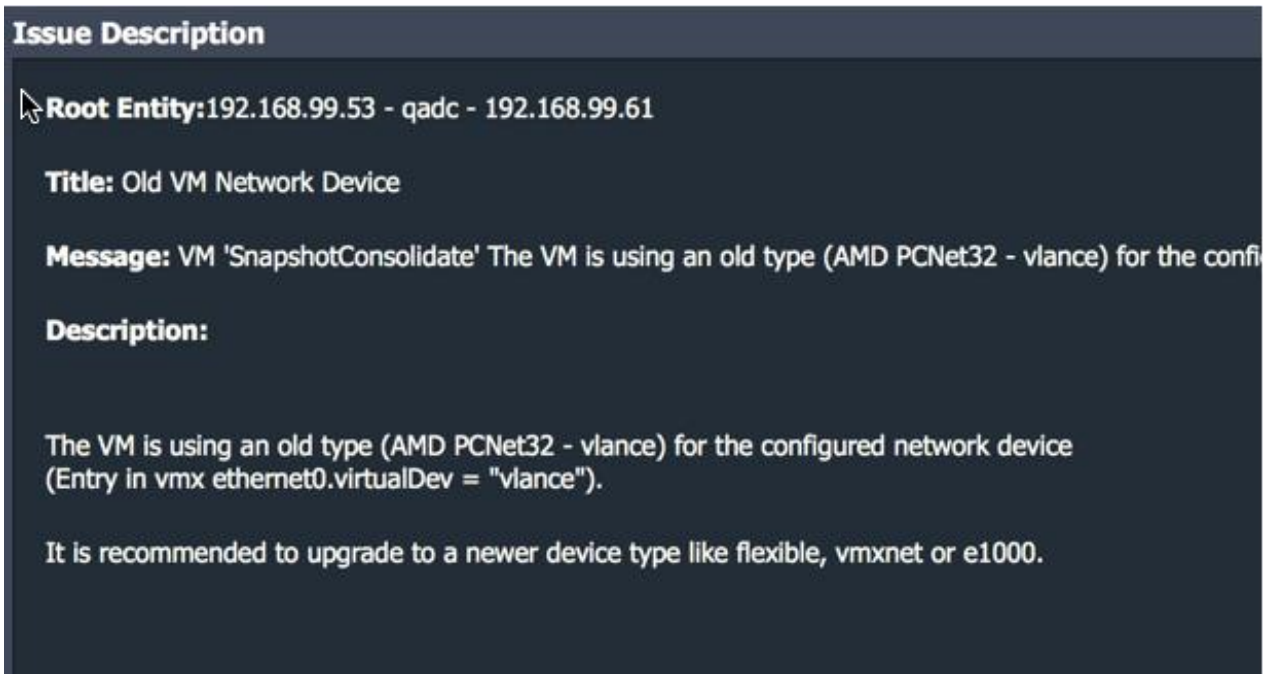


Figure 9 : opvizor identifying outdated network device

# #3. Virtual Machine Memory Limits

When a virtual machine is moved out of a resource pool that had a memory limit, the stand-alone virtual machine can, unknown to the administrator, maintain the memory limit to which it was subjected as a member of the resource pool. Additionally, some administrators configure memory limits thinking – erroneously – that memory limits should be configured to ensure that one virtual machine doesn't monopolize the memory on a single host.

## Impact

The impact of memory limits is such that virtual machines may not be able to access the memory they need precisely when they need it. If a guest OS cannot access the memory that it needs, any applications running inside the guest OS will perform poorly, may even become unresponsive, or completely fail. Additionally, memory ballooning and vmkernel swapping may occur in a virtual machine with a memory limit even though the vSphere host may have

plenty of memory available. As is the case in the physical world (when this memory to disk swapping process takes place), the system's overall performance is negatively impacted in a serious way since disk storage is almost never as fast as RAM.

## Ease of Detecting

To find memory limits, you can verify the memory configuration of each virtual machine, checking for memory limits and compare this against the actual memory assigned to a virtual machine. If you have a large number of virtual machines, this can be challenging and an automated tool that can detect memory limits is needed in medium and large virtual infrastructures.

## Benefits to Solving

By removing memory limits, vSphere's built-in memory optimization techniques can more adequately perform their role and virtual machine guest operating systems can receive the memory that they need to run applications. If the virtual machine's memory was limited when there was host memory available, the performance of the application in the guest OS will improve as the guest is then able to access adequate RAM.

## Ease of Solving

Removing memory limits is easily done by setting the limit back to zero. Unfortunately, *finding* memory limits can be more challenging than actually removing the limit. Without the right tools, determining whether you have any memory limits configured in your virtual infrastructure, you need to manually look through each virtual machine in your inventory by going into the settings of each virtual machine and verify whether a memory limit is configured, as shown in Figure 10. While it's not difficult, the process can be very time consuming, particularly if you have a great number of

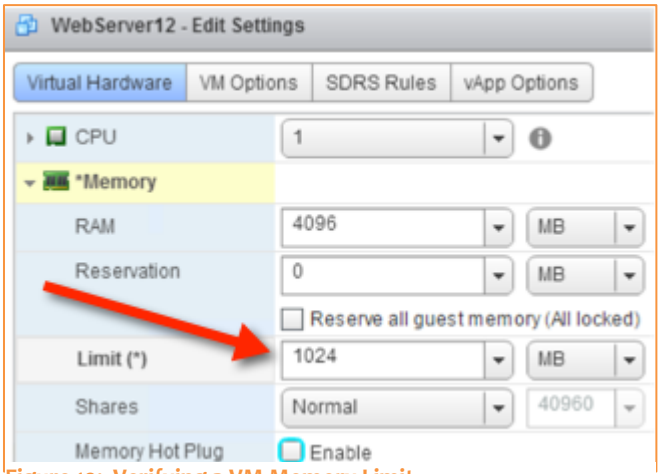

Figure 10: Verifying a VM Memory Limit

virtual machines. Alternatively, you can run a PowerCLI script, like this one, to identify VMs with memory limits.

## How opvizor Helps

opvizor helps to quickly and continually notify you of any virtual machines that have memory limits, and provides you with instructions on how to remove them, either from the GUI or using a PowerCLI script (Figure 11).

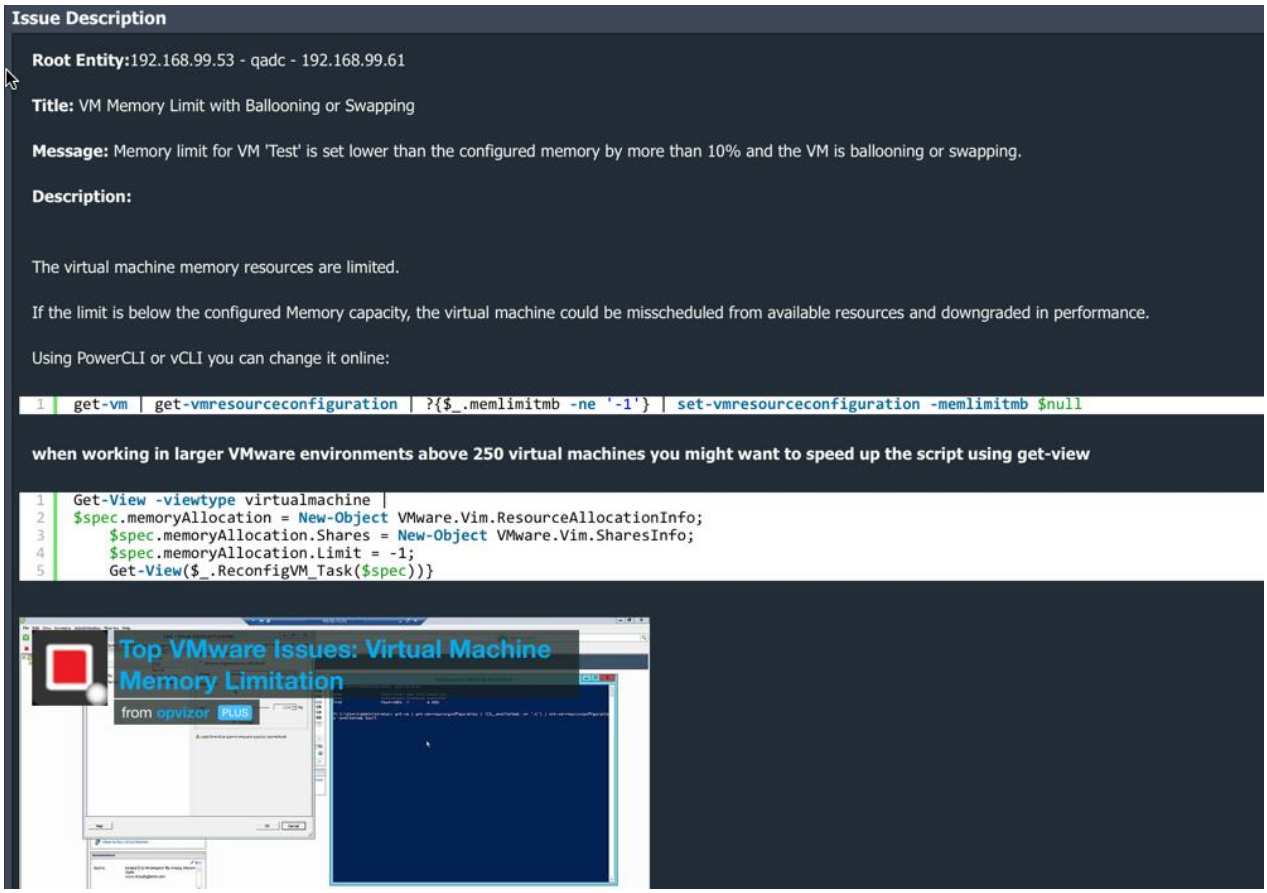


Figure 11: opvizor reporting a VM with a memory limit and how you can remediate

# #4. Virtual Machine Snapshot Age & Size

Virtual machine snapshots are one of the most useful features of VMware vSphere as they preserve the state of a virtual machine's virtual disk and, optionally, virtual memory before a critical event such as an application upgrade or configuration change. Snapshots are also

taken by most virtualization backup applications at the start of the backup and then removed at the end of the backup.  In fact, besides vMotion, snapshots were one of the original top reasons that organizations adopted virtualization technologies to begin with.

## Impact

What many vSphere administrators don't know is that the quantity and age of snapshots on a virtual machine are directly related to their performance impact on a virtual machine. This was especially true with older vSphere versions (prior to ESXi 4.1) because they locked the entire LUN where the virtual machine was stored using a SCSI-2 reservation while taking a snapshot or when booting virtual machines. With ESXi 5 and above, you have the option to configure VAAI (vSphere API for Array Integration) which only locks the individual virtual machine, and does so with hardware assisted locking, as long as your storage array supports VAAI. With VAAI in place, there is much less performance impact when snapshots are in use but that impact isn't completely eliminated.

Besides the performance impact, there is also the potential for vCenter to not be aware of snapshots due to an out-of-sync condition. In this case, it is possible that a virtual machine, which has snapshots and performs a large number of disk writes, could have a snapshot that fills the datastore and causes all virtual machines on that datastore to go down until space is freed.

Finally, there are situations where vSphere can report that snapshot files need to be consolidated. While the end result of this consolation is good, the actual consolidation process can mean that a virtual machine is paused (or at least runs very slow) for anywhere between a few minutes to more than 30 minutes.

## Ease of Detecting

While you could go into the Snapshot Manager for each virtual machine and see if that virtual machine has any snapshots, this is an exceedingly inefficient process, especially in larger organizations. Additionally, there are times that backup applications are unable to complete successfully and completely remove all the snapshots that have been created. As a result, it's easy to end up with unintended snapshots that you didn't even know existed. Additionally, it

is possible to have snapshot files consuming disk space that aren't even displayed in the snapshot manager!

One way of detecting snapshots is to use the storage reporting function, report on virtual machine files, and sort on the file type. It's here that you'll be able to see what snapshot data files are taking up space on each datastore. To access this report, go to the Storage Inventory in the vSphere Web Client, click on a datastore, click on Monitor, and then on Storage Reports. Finally, click on the File Type column heading to sort by file type and scroll down to the Snapshot Data files, if they exist (Figure 12).

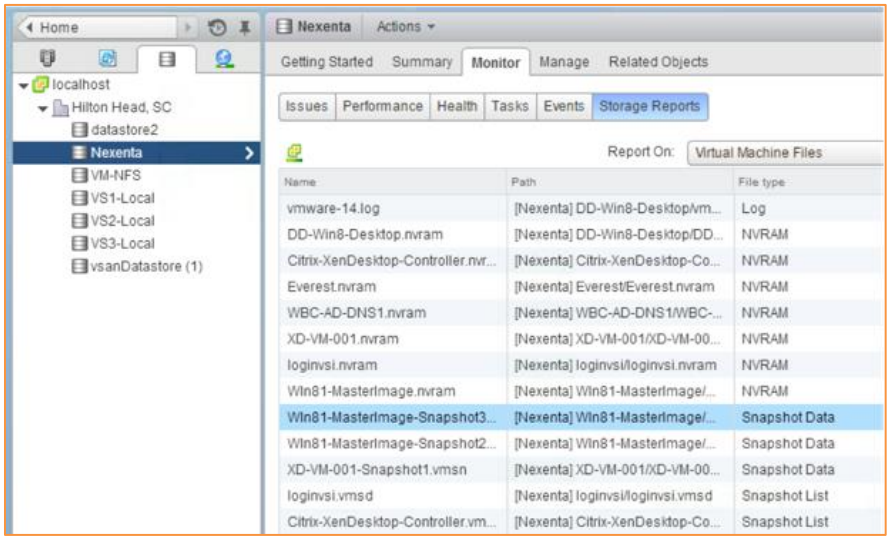


Figure 12: vSphere Storage Reports

Another way to identify snapshot files is to use PowerCLI, as shown in this article.

## Benefits to Solving

By removing snapshots for a virtual machine, guest OS and application performance can be improved, and you can reclaim the disk space that is currently consumed by unnecessary snapshot files. Additionally, you may be able to prevent outages causes if a datastore were to fill up or if a virtual machine had a large number of snapshots that needed consolidation.

## Ease of Solving

Simply removing a snapshot is easy but *finding* snapshots can be much more challenging. By having an automated tool that helps to identify and alert you to snapshots you may not have

known about can be invaluable. Note that the recommendation for snapshots is to have no snapshots older than one week and no snapshots over 5GB in size.

For more information about virtual machine backup best practices, see VMware KB 1025279.

## How opvizor Helps

As shown in Figure 13, opvizor allows you to very quickly identify snapshots that are large or have been aging for some time. Furthermore, invalid snapshots, the silent killer of any datastore, is also detected in minutes. Armed with this information, you'll be able to quickly remove these snapshots, if they aren't needed.

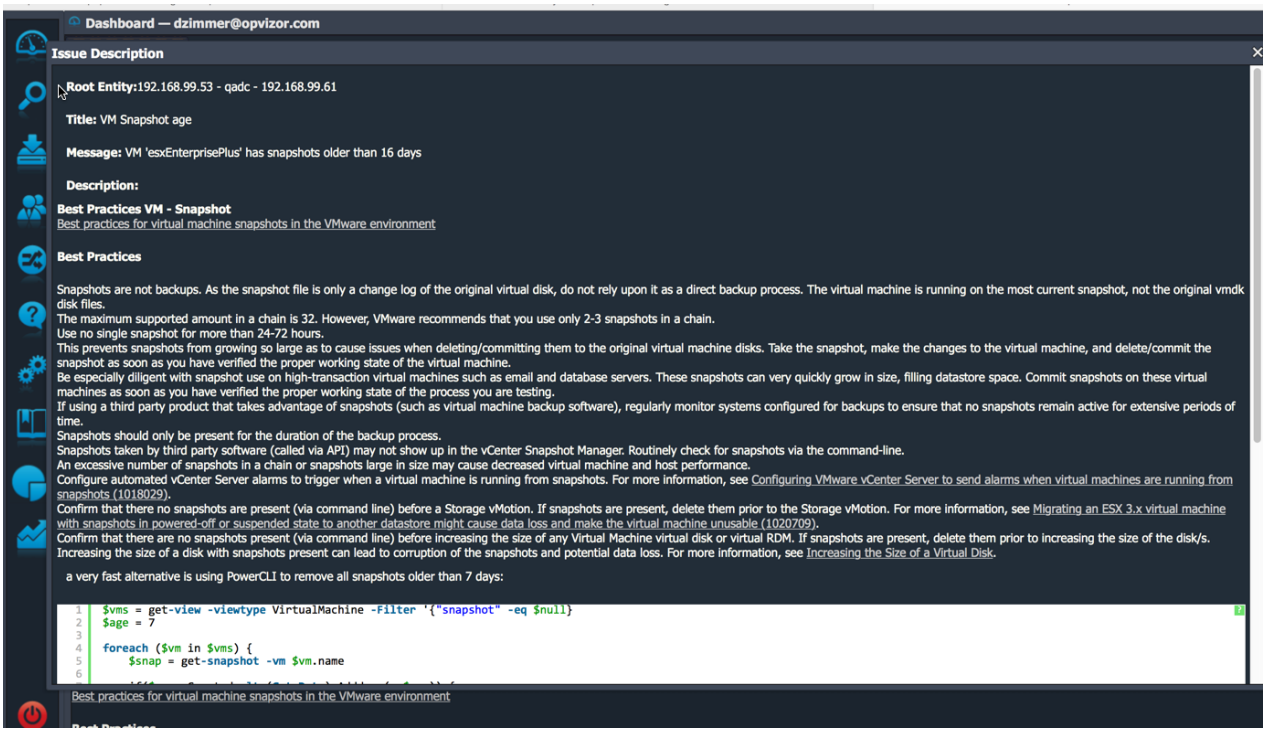

Figure 13: opvizor identifying large or aging snapshots

# #5. Virtual Machine Logging Limitation

The last of the five most common virtual machine issues is related to virtual machine logging. VMware vSphere offers a number of different log files that are stored in different places. Log files are used to provide more detailed information. Usually that detailed information is used

during the troubleshooting of a problem in the virtual infrastructure. One of those log file is the virtual machine log file, vmware.log.

By default, the vmware.log file is only rotated when a virtual machine is restarted and six old logs are retained. Because many virtual machines are likely stored in the same datastore, a malicious attacker could try to find ways to flood log files in order to fill the datastore and thus bring down all virtual machines running inside that datastore. To prevent a virtual machine log file from being maliciously flooded (which can lead to denial of service) you should limit the number and size of the log files ESXi generates.

## Impact

When configuring logging in a vSphere infrastructure, best practices should be used to ensure that you:

- Have log files that are useful for problem solving (to ensure that the logs haven't rotated out).
- Don't have log files that can be used to create a denial of service attack.

If your vSphere logging at the ESXi host level or at the vCenter server level are misconfigured, it's likely you won't always have the troubleshooting data that you need when unexpected issues happen. Worse yet, if your logging is misconfigured then you may be vulnerable to a denial-of-service attack that brings down the entire virtual infrastructure.

## Ease of Detecting

While there are numerous log configuration options that should be reviewed in the virtual infrastructure, you should first focus on the per-VM log file, vmware.log. By default these per-VM log files are stored with the virtual machine files in the VMFS datastore. In fact, if you go to each of your datastores in the vSphere Web Client storage reports section, you'll find all of the vmware.log files. However, the configuration for each of the individual virtual machines ultimately dictates the number and size of the vmware.log files. To determine your current VM logging configuration, you have to verify if any per-VM log configurations have been set inside each of your virtual machines' VMX files, a process which is explained below.

## Benefits to Solving

By standardizing on the best practices for virtual machine logging, you will ensure that you have the log files you need when troubleshooting as well as ensuring that your log files are never used for any kind of malicious attack.

## Ease of Solving

Because VMX configurations can only take effect at power on, that means that after you make these logging additions to your VMX file, you will have to reboot your virtual machines. To make the changes necessary, you will need to add these lines to the VMX file with the VM powered off:

- log.rotateSize = "1000000"
- log.keepOld = "3"
- Note: The log.rotateSize value is in bytes (such that 16384 would be 16MB) and the log.keepOld is the number of logs to keep.

These log tweaks will ensure that your log file doesn't grow forever and potentially fill the datastore where many other virtual machines are running.

Starting with vSphere 5.1 and above, the log.rotateSize setting is no longer available (but other log setting discussed here are). In those vSphere infrastructures, vSphere doesn't allow you to configure log rotation and, instead, uses a bandwidth/rate limit function. With the vSphere log-throttling feature in place with vSphere 5.1 and later, VMware says that vSphere logging is ready for even the most demanding use-case and virtual machines. However, monitoring log file sizes is still very important as you can still experience log files of several gigabytes if a virtual machine has not been powered off and back on in a long time.

This process can be automated using PowerCLI. For more information see this blog post.

You'll find VMware's best practices for log file configurations in VMware KB 8182749.

## How opvizor Helps

Instead of going through this process of log configuration verification across all virtual machines manually, opvizor can verify and reconfigure the logging for each of the virtual machines in your virtual infrastructure, as shown in Figure 14.

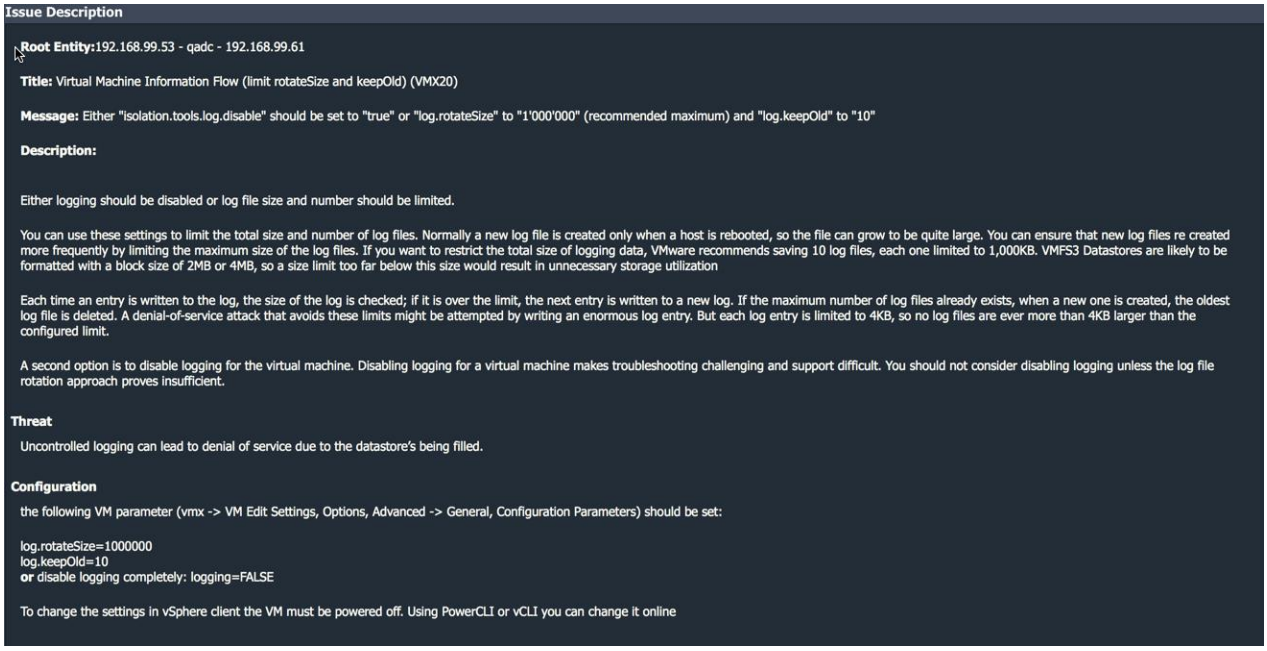


Figure 14: opvizor log configuration verification

# Summary

Virtual machine issues like the top five most common VM issues discussed here can wreak havoc on the virtual infrastructure and can cost companies millions. The opvizor virtualization management solution continues to monitor several million virtual machines and is continually updating its problem identification and remediation solutions. You can prevent these most common virtual machine issues with opvizor, but there are thousands of other potential issues possible. Smart virtualization admins are monitoring their virtual infrastructures with solutions like opvizor to prevent these types of issues in their infrastructure.

Learn more about opvizor at www.Opvizor.com

## About the Author

**David Davis** is a video training author at Pluralsight.com, the global leader in video training for IT pros. He holds several certifications including VCP5, VCAP-DCA, CCIE #9369, and has been awarded the VMware vExpert award 6 years running. Additionally, David has spoken at major conferences like VMworld and has authored hundreds of articles for websites and print publications, mostly around virtualization. David's personal blog is www.VirtualizationSoftware.com