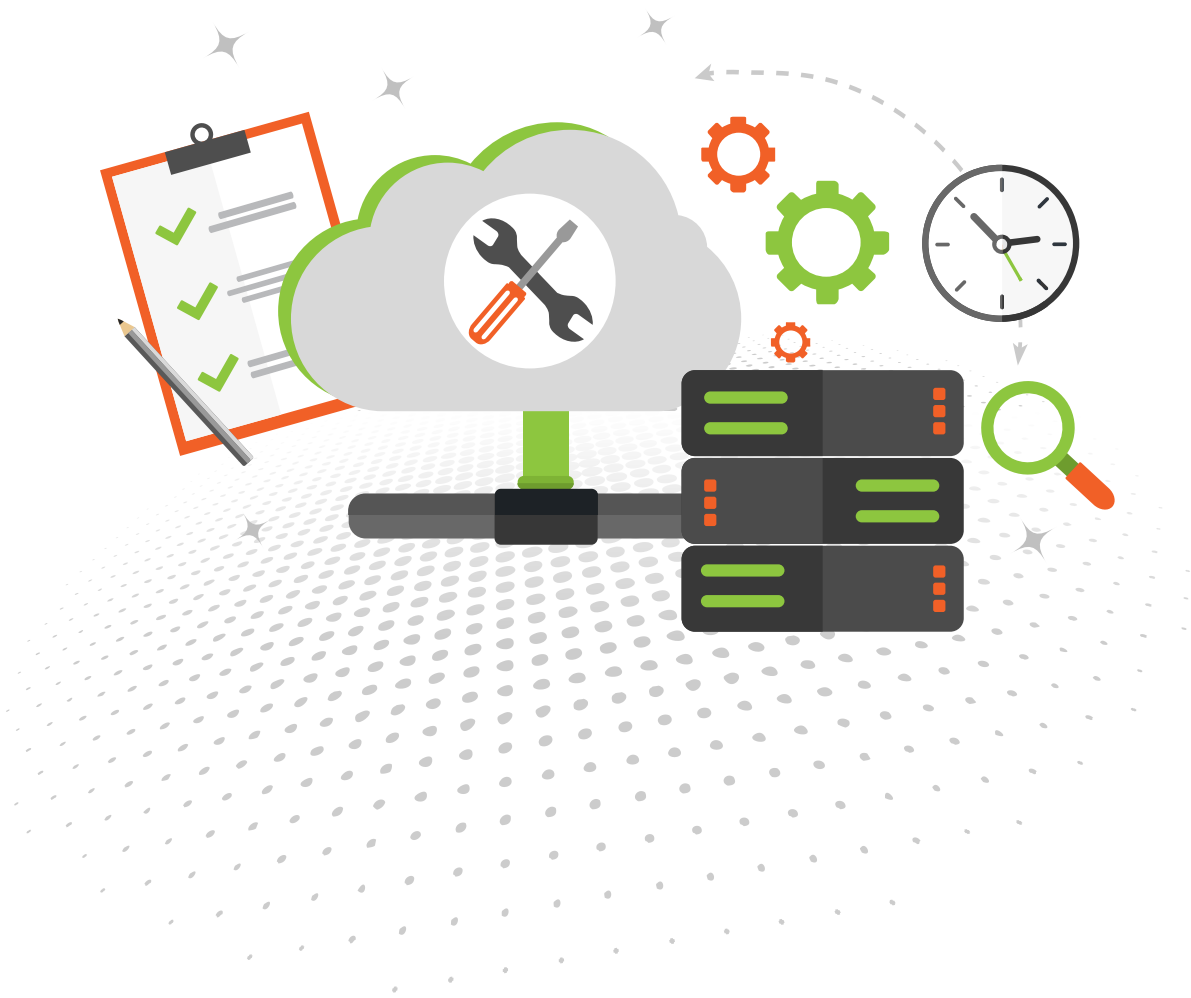


vSphere Troubleshooting Guide



ALTARO

CONTENTS

VSPHERE TROUBLESHOOTING INTRODUCTION	3
vSphere Troubleshooting Tools	4
VMware Command Line Tools	4
VMware Log Locations for Troubleshooting	6
The vSphere Syslog Collector	8
The VM Support Command	8
The vCenter Bash Cell	8
PART 1: VSPHERE INSTALLATION TROUBLESHOOTING	9
ESXi Host Troubleshooting	9
vCenter Troubleshooting	11
PART 2: VIRTUAL MACHINE TROUBLESHOOTING	13
Virtual Machine Troubleshooting Scenario #1 – Content ID Mismatch	13
Virtual Machine Troubleshooting Scenario #2 – Snapshot Issues	14
Virtual Machine Troubleshooting Scenario #3 – Virtual Machine Power On Issues	16
Virtual Machine Troubleshooting Scenario #4 – Orphaned Virtual Machines	17
PART 3: STORAGE TROUBLESHOOTING	19
Storage Troubleshooting Scenario #1 – Storage is not reachable from ESXi host	19
Storage Troubleshooting Scenario #2 – NFS Connectivity Issues	21
Storage Troubleshooting Scenario #3 – One or more paths to a LUN is lost	22
Storage Troubleshooting Scenario #4 – vSAN Troubleshooting	25
PART 4: NETWORK TROUBLESHOOTING	27
Network Troubleshooting Scenario #1 – No network connectivity to other systems	27
Network Troubleshooting Scenario #2 – ESXi hosts dropping from vCenter	28
Network Troubleshooting Scenario #3 – No Management Connectivity on ESXi Host	29
PART 5: VCENTER AND ESXI TROUBLESHOOTING	31
vCenter/ESXi Troubleshooting Scenario #1 – The vCenter Service fails to start	32
vCenter/ESXi Troubleshooting Scenario #2 – vCenter Database Health	32
vCenter/ESXi Troubleshooting Scenario #3 – An ESXi host hangs during boot or randomly	34
vCenter/ESXi Troubleshooting Scenario #4 – A VM is experiencing memory or CPU issues	34
PART 6: HA, DRS AND VMOTION TROUBLESHOOTING	37
HA, DRS and vMotion Troubleshooting Scenario #1 – HA does not turn on when enabled	37
HA, DRS and vMotion Troubleshooting Scenario #2 – Error messages about insufficient resources	38
HA, DRS and vMotion Troubleshooting Scenario #3 – vMotion fails or times out	39
HA, DRS and vMotion Troubleshooting Scenario #4 – DRS does not vMotion machines	39
CONCLUSION	40
ABOUT ALTARO	41
ABOUT RYAN BIRK	43
FOLLOW ALTARO	44

VSPHERE TROUBLESHOOTING INTRODUCTION

Before we begin, we need to start off with an introduction to a few things that will make life easier. We'll start with a troubleshooting methodology and how to gather logs. After that, we'll break this eBook into the following sections: Installation, Virtual Machines, Networking, Storage, vCenter/ESXi and Clustering.

ESXi and vSphere problems arise from many different places, but they generally fall into one of these categories:

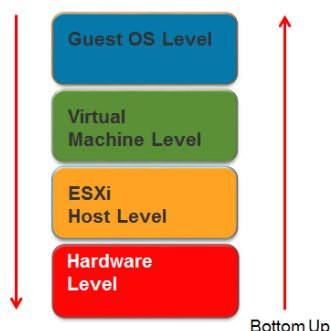
- Hardware issues
- Resource contention
- Network attacks
- Software bugs
- Configuration problems

A typical troubleshooting process contains several tasks:

1. Define the problem and gather information.
2. Identify what is causing the problem.
3. Fix the problem, implement a fix.

One of the first things you should try to do when experiencing a problem with a host, is try to reproduce the issue. If you can find a way to reproduce it, you have a great way to validate that the issue is resolved when you do fix it. It can be helpful as well to take a benchmark of your systems before they are implemented into a production environment. If you know HOW they should be running, it's easier to pinpoint a problem.

Top Down



You should decide if it's best to work from a "Top Down" or "Bottom Up" approach to determine the root cause. Guest OS Level issues typically cause a large amount of problems. Let's face it, some of the applications we use are not perfect. They get the job done but they utilize a lot of memory doing it.

In terms of virtual machine level issues, is it possible that you could have a limit or share value that's misconfigured?

At the ESXi Host Level, you could need additional resources. It's hard to believe sometimes, but you might need another host to help with load!

Once you have identified the root cause, you should assess the impact of the problem on your day to day operations. When and what type of fix should you implement? A short-term one or a long-term solution? Assess the impact of your solution on daily operations.

- Short-term solution: Implement a quick workaround.
- Long-term solution: Reconfiguration of a virtual machine or host.

VSPHERE TROUBLESHOOTING TOOLS

Before you can troubleshoot issues, you need to understand the various tools that are out there. In this section, we will discuss some of the tools that VMware provides and how to identify the log locations for additional troubleshooting.

VMWARE COMMAND LINE TOOLS

You can run command-line tools on an ESXi host in several ways:

- **The vSphere ESXi shell itself**, which includes:
 - esxcli commands (esxcli network, esxcli storage, esxcli vm, etc)
 - A set of esxcfg-* commands: The esxcfg commands are deprecated but you will likely still see some older documentation with them. The recommendation today is to use esxcli.
 - The host shell can be accessed a couple of different ways, either by using the local DCUI (Direct Console User Interface) or via SSH.

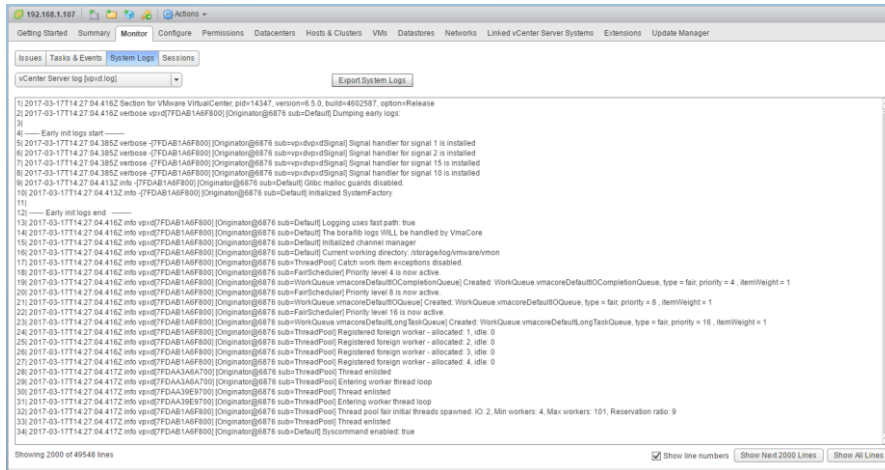
- Local access by using the Direct Console User Interface (DCUI):
 1. Enable the vSphere ESXi Shell service, either in the DCUI or vSphere Web Client. Typically, this is running by default.
 2. Access the ESXi Shell from the DCUI by pressing Alt-F1 after logging in.
 3. When finished, disable the ESXi Shell service when not using it.
- Remote access by using PuTTY or an SSH client.
 1. Enable the SSH service on your ESXi host, either in the DCUI or through the vSphere Web Client.
 2. Use PuTTY or your preferred SSH Client to access the ESXi host.
 3. Disable the SSH Service when finished.
- vSphere Management Assistant (This tool has been deprecated. 6.5 is final release):
 - A virtual appliance that includes components for running vSphere commands:
 - esxcli
 - vmware-cmd
 - vicfg-* commands
 - vi-fastpass authentication components for automated authentication to vCenter or ESXi hosts. This saves you from having to type your name and password with every command that is ran.
- VMware PowerCLI:
 - VMware PowerCLI provides an easy-to-use Windows PowerShell interface for command-line access to administration tasks or for creating executable scripts.

VMWARE LOG LOCATIONS FOR TROUBLESHOOTING

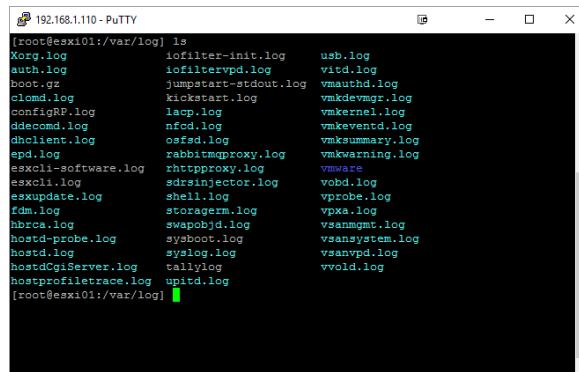
VMware stores logs for their products in various locations. It's important to know where to look when you're having problems quickly and efficiently.

- vCenter Log Locations:
 - Location for vCenter Server on Windows 2008/2012:
 - %ALLUSERSPROFILE%\VMWare\vCenterServer\logs
 - Location for VMware vCenter Server Appliance:
 - /var/log/vmware/
 - Includes logs for SSO, Inventory Service and the Web Client.
 - Useful ESXi Host Logs:
 - hostd.log: Host management service logs.
 - syslog.log: Service initialization, watchdogs, scheduled tasks, DCUI.
 - vmkernel.log: Core VMkernel logs. Storage and Networking device events.
 - vmkwarning.log: Warning and alert log messages.
 - vmksummary.log: ESXi host startup and shutdown, uptime details, resource consumption.
 - vCenter vpxd.log
 - This log file is the main vCenter Server log file. If you ever contact VMware for support, it is highly likely that they will ask you for this file. Don't confuse this with vpxa, that is the vCenter agent and runs on the ESXi hosts.
 - You can monitor and view the logs easily through the vSphere Web Client, under the Monitor tab (Figure 1), with an SSH session at /var/log (Figure 2) or in the DCUI under "View System Logs" under System Customization (Figure 3).

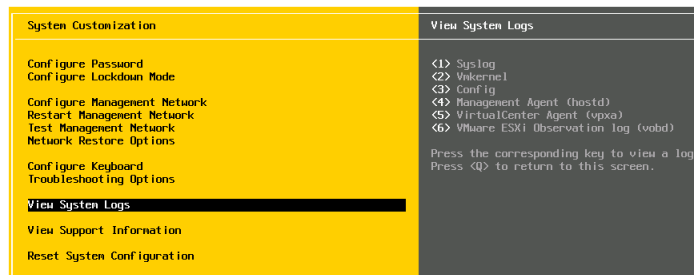
(Figure 1)



(Figure 2)



(Figure 3)



THE VSPHERE SYSLOG COLLECTOR

You can gather logs at the above locations or setup a single location for all of your ESXi hosts to point to. It uses port 514 for TCP and UDP, and port 1514 for SSL. The Syslog collector is installed on both the Windows based vCenter and the vCenter Appliance.

THE VM-SUPPORT COMMAND

In addition to the Syslog Collector, you can also gather logs with the vm-support command. It collects data from the ESXi hosts and compresses the following data:

- Log files
- System status
- Configuration files

The tool does not require any arguments and it create a zip file using the host name and time stamp.

THE VCENTER BASH SHELL

You can also use the vCenter Bash Shell from the vCenter Appliance console under troubleshooting options. From the Bash shell, you can verify the status of a service and start or restart services.



PART 1: VSPHERE INSTALLATION TROUBLESHOOTING

This section will cover some of the common issues with vSphere deployments. We will split this section into two sections. The first will cover ESXi host troubleshooting during installation, the second will cover vCenter deployments at installation.

ESXI HOST TROUBLESHOOTING

It's common to think that ESXi will just install on any hardware, but it's important to know a few details before you decide to get started. First, VMware only will support hardware that is officially supported on the [VMware Hardware Compatibility List](#).

Specific drivers are tested and chosen. If it's not on the list, don't expect support. VMware has a large partner eco-system and both hardware and software goes through rigorous testing and is signed off on for official support.

VMware also has various community driver support. What this means is that even though your hardware can work with ESXi, it's not running in a fully supported mode. This is a nice feature for users who build homelabs for practice.

Another important note to remember during installation is that not all of your drivers might install automatically. It's possible that your hardware could be newer and you might have to download a vSphere Installation Bundle, also called a VIB. A VIB is somewhat like a tarball or ZIP archive in that it is a collection of files packaged into a single archive to make software deployments easier.

A VIB is comprised of three parts:

- A file archive
- An XML descriptor file
- A signature file

The signature file is the electronic signature used to verify the level of trust. The trust level will be one of the four listed below:

- **VMwareCertified:** VIBs created and tested by VMware. VMware Certified VIBs undergo thorough testing by VMware.
- **VMwareAccepted:** VIBs created by a VMware partners that are approved by VMware. VMware relies on partners to perform the testing, but VMware verifies the results.
- **PartnerSupported:** VIBs created and tested by a trusted VMware partner. The partner performs all testing. VMware does not verify the results.
- **CommunitySupported:** VIBs created by individuals or partners outside of the VMware partner program. These VIBs do not undergo any VMware or trusted partner testing and are not supported by VMware or its partners.

If installation was successful and you have all the right VIBs and software configured, but other issues have come up, you should always check the `hostd.log` file first. The `hostd` management service is the main communication channel between ESXi hosts and VMkernel. If `hostd` fails, the ESXi host disconnects from vCenter and cannot be easily managed.

- Try restarting `hostd` by running `/etc/init.d/hostd restart`

Occasionally, an ESXi host will crash and display a purple diagnostic screen. A host can crash for several reasons. CPU exceptions, driver issues, machine check exceptions, hardware fault or a software bug.

To recover from a PSOD, you should try following these steps:

1. Take a screenshot of the screen.
2. Restart the host, get the VMs up and running on another host if possible. If using HA, this should happen on its own if configured properly.
3. Contact VMware support if you can't find any information online. Occasionally others have the same issue and the fix can be implemented easily through firmware or software updates.

Another possible issue is that the ESXi host simply hangs during the boot process. You never get a PSOD, it just sits there and the entire system becomes unresponsive. Typically hangs happen during a power cycle of a system during the boot process. It's caused by VMkernel being too busy or a possible hardware lockup.

To determine that the host has locked up:

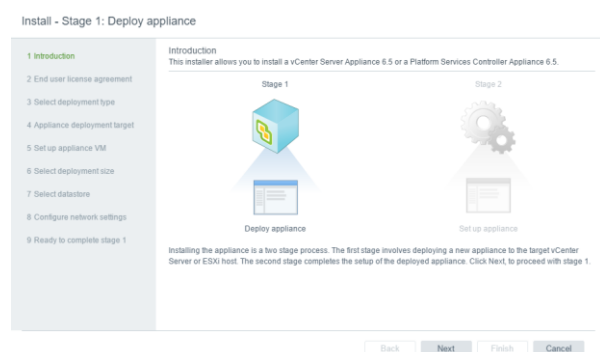
1. Ping the VMkernel (Management) network interface.
2. Try to login to the host with the vSphere Web Client or Embedded Host Client.
3. Monitor network traffic from the ESXi host.

If you can ping the host, that's a good sign. Next connect to the DCUI to display any messages on the screen. Press Alt-F12 at the host console to do that.

To recover from a host that has hung, try rebooting the ESXi host, review logs and gather performance statistics. If you determine it's a hardware issue, fix the hardware and if required reinstall or reconfigure ESXi. Lastly update the host with the most recent patches.

VCENTER TROUBLESHOOTING

When installing the vCSA, VMware has split the install into two different stages. Stage 1 is the appliance deployment. Stage 2 is the configuration of the appliance.



Stage 1 in most cases, is a very straightforward install. Stage 2 is where traditionally, users have had issues with deployments and it generally can be resolved with verifying your DNS settings and NTP.

Some deployments seem successful but upon login, the authentication fails if the NTP server on the ESXi host and the newly created appliance are not synced to the same source.

Occasionally you might run into issues replacing certificates with the Certificate Manager. It can hang at 0% and perform an automatic rollback error. This issue can be caused by using non-Base64 certificates. To resolve, manually publish the full chain to the certificate store using the vSphere 6.0 Certification Manager.

To launch the vSphere 6.x Certificate Manager, run this command using the command prompt:

- Windows vCenter Server:
`C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager`
- vCenter Server Appliance:
`/usr/lib/vmware-vmca/bin/certificate-manager`

1. You will then be prompted with the following options:

```
C:\Program Files\VMware\vCenter Server\vmcad>certificate-manager

*** Welcome to the vSphere 6.0 Certificate Manager ***
-- Select Operation --
1. Replace Machine SSL certificate with Custom Certificate
2. Replace UMCA Root certificate with Custom Signing Certificate and replace all Certificates
3. Replace Machine SSL certificate with UMCA Certificate
4. Regenerate a new UMCA Root Certificate and replace all certificates
5. Replace Solution user certificates with Custom Certificate
6. Replace Solution user certificates with UMCA certificates
7. Revert last performed operation by re-publishing old certificates
8. Reset all Certificates

Note : Use Ctrl-Z and hit Enter to exit.
Option[1 to 8]:
```

PART 2: VIRTUAL MACHINE TROUBLESHOOTING

Before we jump into troubleshooting virtual machines, let's review some of the typical virtual machine files you will run into.

TYPICAL VIRTUAL MACHINE FILES		
FILE	USAGE	DESCRIPTION
.vmx	<VM-Name>.vmx	Virtual machine configuration file
.vmxf	<VM-Name>.vmxf	Extended configuration file
.vmdk	<VM-Name>.vmdk	Virtual disk characteristics
-flat.vmdk	<VM-Name>-flat.vmdk	Virtual machine data disk
.nvram	<VM-Name>.nvram	Virtual machine BIOS or EFI configuration
.vmsd	<VM-Name>.vmsd	Virtual machine snapshot database file
.vmsn	<VM-Name>.vmsn	Virtual machine snapshot data file
.vswp	<VM-Name>.vswp	Virtual machine swap file
.vmss	<VM-Name>.vmss	Virtual machine suspend file
.log	vmware.log	Current virtual machine log file
-#.log	vmware-#.log	Older virtual machine log entries

VIRTUAL MACHINE TROUBLESHOOTING SCENARIO #1 – CONTENT ID MISMATCH

One of the most frustrating issues that comes up with VMs can be snapshots. In fact, our first few virtual machine troubleshooting scenarios will be focused on snapshots. Occasionally you will receive errors that return a content ID mismatch error like the one below.

Cannot open the disk '/vmfs/volumes/4a496b4g-eceda1-19-542b-000cfc0097g5/virtualmachine/virtualmachine-000002.vmdk' or one of the snapshot disks it depends on. Reason: The parent virtual disk has been modified since the child was created.

Content ID mismatch conditions are triggered by interruptions to major virtual machine migrations such as Storage vMotion or Migration, VMware software error, or user action.

The Content ID (CID) value of a virtual machine disk descriptor file aids in the goal of ensuring content in a parent virtual disk file, such as a flat or base disk, is retained in a consistent state. The child delta disks that derive from that base disk's snapshot contain all further writes and changes. These changes depend on the source disk to remain intact.

To resolve, open the latest vmware.log and locate the specific disk chain affected. You will see a line or warning that is similar to: "Content ID mismatch (parentCID ed06b3ce != 0cb205b1)"

```
# Disk DescriptorFile          # Disk DescriptorFile
version=1                      version=1
encoding="UTF-8"              encoding="UTF-8"
CID=0cb205b1                  CID=0cb205b1
parentCID=0cb205b1            parentCID=ed06b3ce
isNativeSnapshot="no"        isNativeSnapshot="no"
createType="vmfsSparse"       createType="vmfsSparse"
parentFileNameHint="          .vmdk" parentFileNameHint="          .vmdk"
```

In our case change the parentCID in the disk descriptor file from ed06b3ce to 0cb205b1. Then overwrite the existing vmdk file and power the machine back on.

VIRTUAL MACHINE TROUBLESHOOTING SCENARIO #2 – SNAPSHOT ISSUES

Taking a snapshot of a machine fails. The user cannot create or commit a snapshot to the VM. Typical errors will say something like:

- Cannot create a quiesced snapshot because the snapshot operation exceeded the time limit for holding off I/O in the frozen virtual machine.
- An error occurred while quiescing the virtual machine. The error code was: 4 The error was: Quiesce aborted.

Quiescing is done by two technologies.

- Microsoft Volume Shadow Copy Service
- VMware Tools Sync Driver

When taking snapshots be sure the following occur:

- VSS prerequisites are met. (See VMware KB 1007696)
- VMware Tools is running.
- The VSS provider is used.
- All the VSS writers are not showing errors.

When taking snapshots, be sure you do not reach 32 levels. If you have more than 32, you cannot create more snapshots. Generally, it's a recommended practice to keep as little of snapshots as possible on a virtual machine. They can be a performance hit and difficult to troubleshoot.

If a snapshot creation also fails, check that the user has permissions to take a snapshot. Then check that the disk is also supported. RDMs in physical mode, independent disks or VMs with bus-sharing are not supported.

Snapshots will grow based on delta files. You cannot create or commit a snapshot if a snapshot (delta) does not have a descriptor file.

Additional Snapshot Machine Files	
<vm name>-00000n-delta.vmdk	A delta vmdk is created whenever a snapshot is taken. The pre-snapshot vmdk in use is locked for writing. Any changes from there on are written to the vm's delta disk. This allows a vm to be restored to any state prior to a specific snapshot being taken.
<vm name>-00000n.vmdk	The descriptor file for the delta vmdk file.

If the -delta.vmdk has no descriptor file, you will need to create one before doing anything:

1. Copy the base disk descriptor file, use the name of the missing descriptor file.
 - The base descriptor file is the original top most .vmdk file.
2. Edit the new descriptor file. Change the format from a base disk to a snapshot delta disk descriptor.

Another possible issue that might arise when troubleshooting snapshots could be insufficient space on a datastore to commit all the snapshots. Be sure to check the Summary tab of your datastore or run the command “df -h” to determine if you have enough space. You’ll need to increase the size of a the datastore or move virtual machines to other datastores with enough space.

VIRTUAL MACHINE TROUBLESHOOTING SCENARIO #3 – VIRTUAL MACHINE POWER ON ISSUES

Typically when a virtual machine does not power on, it is recommended to start by creating a test virtual machine and power it on. Does the test VM power on successfully? If the test VM did not power on, check your ESXi host resources to make sure sufficient resources exist and that the host is responsive.

If the test VM does power on, that indicates it is likely isolated to that specific virtual machine. Each virtual machine has a vmware.log file in the virtual machine directory and contains detailed information. Before going through the logs, review the recent tasks and event sessions in vCenter as well as that can sometimes alert you to previous tasks that might contain an obvious fix.

Browse to the location of the VM and determine that all the virtual machine files are there. Look for vmx, vmdks, etc. Restore the file if you see anything missing.

A virtual machine will also not power on if one of the virtual machine’s files is locked.

Perform these steps to find a locked file:

1. Power on a virtual machine.
 - If the power-on fails, look for the affected file.
2. Determine whether the file can be locked.
 - touch filename
3. Determine which ESXi host has locked the file.
 - vmkfstools -D /vmfs/volumes/Shared/VM02/VM02-flat.vmdk

- Check the MAC address at the location (See below) in the output.
 - If you see all zeros for the owner that means the owner is the current ESXi server.
4. Login to the host that has the locked file and identify the process.
 - Run esxcli “vm process list” to display running VMs
 5. Kill the process that is locking the file.
 - Run esxcli “vm process kill” to kill the process.

```
Lock [type 10c00001 offset 196141056 v 120, hb offset 3256320
gen 9, mode 1, owner 4f9b001f-43a55858-7513-00237d37e25c mtime 97806 nHld 0 nOvf 0]
Addr <4, 459, 100>, gen 101, links 1, type reg, flags 0, uid 0, gid 0, mode 600
len 59055800320, nb 553 tbz 0, cow 0, newSinceEpoch 0, zla 3, bs 1048576
```

VIRTUAL MACHINE TROUBLESHOOTING SCENARIO #4 – ORPHANED VIRTUAL MACHINES

When a virtual machine is orphaned, you should begin by trying to determine if a vCenter reboot has occurred. Occasionally if you try to move a machine through a vMotion migration to another host and the vCenter is rebooted it can cause them to be orphaned. Virtual machines can become orphaned if a host failover is unsuccessful, or when the virtual machine is unregistered directly on the host. Some additional symptoms:

- Virtual Machines show as invalid or orphaned after a VMware High Availability (VMware HA) host failure occurs
- Virtual Machines show as invalid or orphaned after an ESX host comes out of maintenance mode
- Virtual Machines show as invalid or orphaned after a failed DRS migration
- Virtual Machines show as invalid or orphaned after a storage failure
- Virtual Machines show as invalid or orphaned after the connection is lost between the vCenter Server and the host where the virtual machine resides

To fix, follow the steps below:

1. Determine the datastore where the virtual machine configuration (.vmx) file is located.
2. Return to the virtual machine in the vSphere Web Client, right-click, and select:
 - a. **All Virtual Infrastructure Actions > Remove from Inventory.**
3. Click **Yes** to confirm the removal of the virtual machine.

Side Note: Remove from Inventory is far different than Delete from Disk. Remove from Inventory allows you to re-add the machine later. Delete from Disk destroys the data.

To register a virtual machine in vCenter Server:

1. Open the vSphere/VMware Infrastructure (VI) Client and log in with appropriate credentials.
2. If connecting to vCenter Server, click on the desired host.
3. Click the Configuration tab.
4. Click Storage.
5. Right-click on the appropriate datastore and click Browse Datastore.
6. Navigate to the folder named after the virtual machine, and locate the virtual machine.vmx file.
7. Right-click the .vmx file and click Add to inventory. The Add to Inventory wizard opens.
8. Continue to follow the wizard to add the virtual machine.

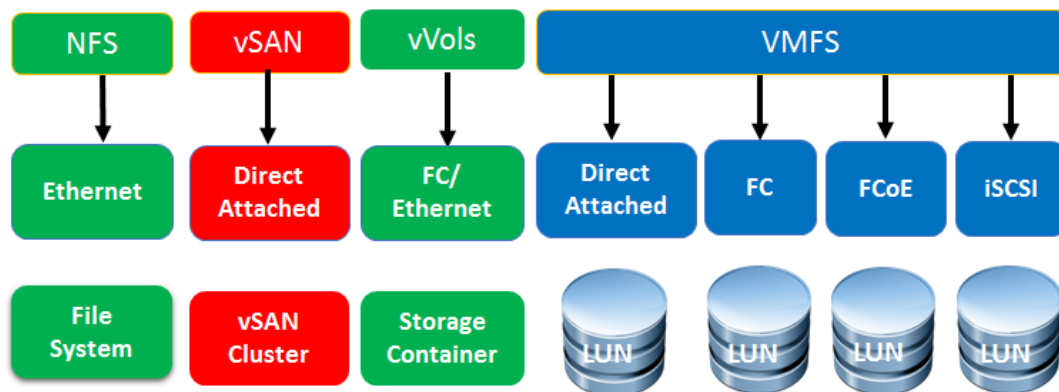
If you were looking to recreate and not just remove the virtual machine try the following:

1. Browse to the datastore and verify that the virtual machine files exist.
2. If the vmx configuration file was deleted or remove and the disk files are still there, attach the old disk files to a newly create machine.
3. If the disk files were deleted, restore from a backup.

PART 3: STORAGE TROUBLESHOOTING

If a virtual machine cannot access its virtual disks, the cause of the problem might be anywhere from the virtual machine to physical storage.

As you can see below, there are multiple types of storage, it's important to determine what type you're troubleshooting before starting. A "datastore" can be multiple things with different types of connectivity.



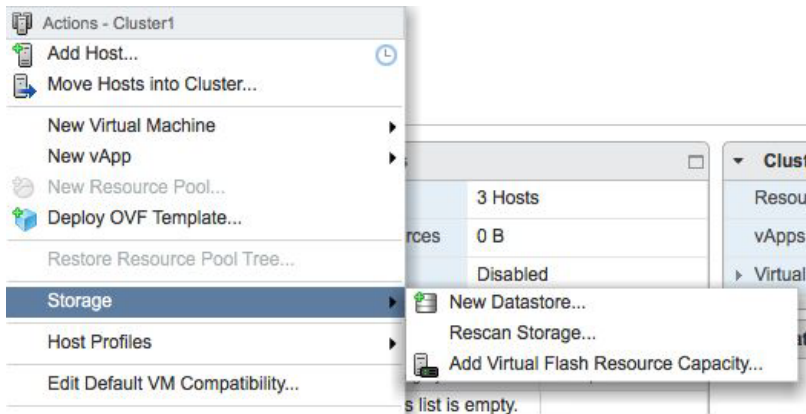
STORAGE TROUBLESHOOTING SCENARIO #1 – STORAGE IS NOT REACHABLE FROM ESXI HOST

This problem typically will be noticed when a datastore falls offline. The ESXi host itself appears fine but something has caused the datastore to fall offline.

Typically, the best method to start with would be:

- Verify that the ESXi host can see the LUN by running: “esxcli storage core path list” from the host.
- Check to see if a rescan of storage resolves it by running: “esxcli storage core adapter rescan -A vmhba##”

You can also rescan your storage adapters under your storage adapter section in the vSphere Web Client or rescan at the cluster level as show below:

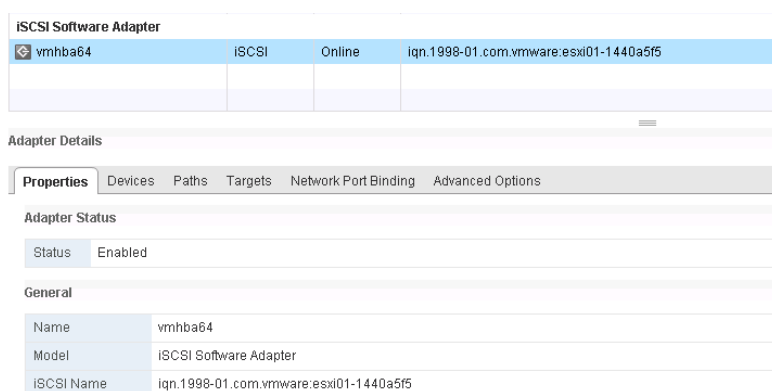


If the rescan does not resolve it, it is likely that something else is causing the issue. Have there been any other recent changes to the ESXi host?

Some other possible causes:

A firewall is blocking traffic	VMkernel interface is misconfigured
IP Storage is not properly configured	NFS storage is not configured properly
iSCSI port (3260) is unreachable	The actual storage device is online
Is LUN masking in place? Is the LUN still presented?	Check to see if the array is supported

Check your adapter settings. Are the network port bindings setup properly? Is the target name spelled properly? Is the initiator name correct? Are there any required CHAP settings needed? Do you see your storage devices under the devices tab?



If the storage device is online but functioning poorly, check your physical device latency metrics as well. High numbers (greater than 15 or 20 ms) represent a slow or overworked array. Your goal is to not oversubscribe your links. Try to isolate iSCSI and NFS.

Use the esxtop or resxtop command and press d:

```
12:07:31am up 5:22, 596 worlds, 2 VMs, 16 vCPUs; CPU load average: 0.12, 0.12, 0.09
ADAPTR  CMDS/s  READS/s  WRITES/s  MBREAD/s  MBWRTN/s  DAVG/cmd  KAVG/cmd  GAVG/cmd  QAVG/cmd
vmhba0   0.00    0.00     0.00     0.00     0.00     0.00     0.00     0.00     0.00
vmhba1  352.08  167.37  183.93    2.67     2.98     2.37     0.01     2.38     0.00
vmhba32   0.00    0.00     0.00     0.00     0.00     0.00     0.00     0.00     0.00
```

Column	Description
CMDS/s	This is the total amount of commands per second and includes IOPS (Input/Output Operations Per Second) and other SCSI commands such as SCSI reservations, locks, vendor string requests, unit attention commands etc. being sent to or coming from the device or virtual machine being monitored.
DAVG/cmd	This is the average response time in milliseconds per command being sent to the device.
KAVG/cmd	This is the amount of time the command spends in the VMkernel (2-3 ms here represent either an overworked array or an overworked host).
GANG/cmd	This is the response time as it is perceived by the guest operating system.

STORAGE TROUBLESHOOTING SCENARIO #2 – NFS CONNECTIVITY ISSUES

If you have virtual machines that are on NFS datastores, verify that the configuration is correct.

- Check NFS server name or IP address.
- Is the ESXi host mapped to the virtual switch?
- Does the VMkernel port have the right IP configuration?
- On the NFS server, are the ACLs correct? (read/write or read only).

VMware supports both NFS v3 and v4.1, but it's important to remember that they use different locking mechanisms:

- NFS v3 uses proprietary client-side cooperative locking.
- NFS v4.1 uses server-side locking.

Configure an NFS array to allow only one NFS protocol. Use either NFS v3 or NFS v4.1 to mount the same NFS share across all ESXi hosts. It is not a good idea to mix. Data corruption might occur if they try to access the same NFS share with different client versions.

NFS 4.1 also does not currently support Storage DRS, vSphere Storage I/O Control, Site Recovery Manager or Virtual Volumes.

STORAGE TROUBLESHOOTING SCENARIO #3 – ONE OR MORE PATHS TO A LUN IS LOST

If an ESXi host at one point had storage connectivity but the LUN is now dead, here are a few esxcli commands to run to use when troubleshooting this issue.

- esxcli storage core path list

```
[root@esxi02:~] esxcli storage core path list
iqn.1998-01.com.vmware:esxi02-2d0e7a5d-00023d000004, iqn.2000-01.com.synology:theboss.name,t,1-naa.6001405d392bd65d3e90d3b28d90aad8
UID: iqn.1998-01.com.vmware:esxi02-2d0e7a5d-00023d000004, iqn.2000-01.com.synology:theboss.name,t,1-naa.6001405d392bd65d3e90d3b28d90aad8
Runtime Name: vmhba64:CO:TO:LO
Device: naa.6001405d392bd65d3e90d3b28d90aad8
Device Display Name: SYNOLOGY iSCSI Disk (naa.6001405d392bd65d3e90d3b28d90aad8)
Adapter: vmhba64
Channel: 0
Target: 0
LUN: 0
Plugin: NMP
State: active
Transport: iscsi
Adapter Identifier: iqn.1998-01.com.vmware:esxi02-2d0e7a5d
Target Identifier: 00023d000004, iqn.2000-01.com.synology:theboss.name,t,1
Adapter Transport Details: iqn.1998-01.com.vmware:esxi02-2d0e7a5d
Target Transport Details: IQN=iqn.2000-01.com.synology:theboss.name Alias= Session=00023d000004 PortalTag=1
Maximum IO Size: 131072
```

- esxcli storage nmp device list

```
[root@esxi02:~] esxcli storage nmp device list
naa.6001405d392bd65d3e90d3b28d90aad8
Device Display Name: SYNOLOGY iSCSI Disk (naa.6001405d392bd65d3e90d3b28d90aad8)
Storage Array Type: VMW_SATP_ALUA
Storage Array Type Device Config: (implicit_support=on; explicit_support=off; explicit_allow=on; alua_follower=on; action_OnRetryErrors=off; (TPG_id=0,TPG_state=AO))
Path Selection Policy: VMW_PSP_MRU
Path Selection Policy Device Config: Current Path=vmhba64:CO:TO:LO
Path Selection Policy Device Custom Config:
Working Paths: vmhba64:CO:TO:LO
Is USB: false
```

A path to a storage/LUN device can be marked as Dead in these situations:

- The ESXi storage stack determines a path is Dead due to the TEST_UNIT_READY command failing on probing
- The ESXi storage stack marks paths as Dead after a permanent device loss (PDL)
- The ESXi storage stack receives a Host Status of 0x1 from an HBA driver

For iSCSI storage, verify that NIC teaming is not misconfigured. Next verify your path selection policy is setup properly.

Check for Permanent Device Loss or All Paths Down. There are two distinct states a device can be in when storage connectivity is lost; All Paths Down or Permanent Device Loss. For each of these states, the device is handled is different. All Paths Down (APD) is a condition where all paths to the storage device are lost or the storage device is removed. The state is caused because the change happened in an uncontrolled manner, and the VMkernel storage stack does not know how long the loss of access to the device will last. The APD is a condition that is treated as temporary (transient), since the storage device might come back online; or it could be permanent, which is referred to as a Permanent Device Loss (PDL).

Permanent Device Loss (PDL):

- A datastore is shown as unavailable in the Storage view
- A storage adapter indicates the Operational State of the device as Lost Communication
- A planned PDL occurs when there is an intent to remove a device presented to the ESXi host.
- An unplanned PDL occurs when the storage device is unexpectedly unrepresented from the storage array without the unmount and detach being ran on the ESXi host.

All Paths Down (APD):

- You are unable to connect directly to the ESXi host using the vSphere Client
- All paths to the device are marked as Dead
- The ESXi host shows as Disconnected in vCenter Server

It is also important to mention that you will need to check the SAN/NAS fabric as well to get further detailed information in the event of an APD.

The storage all paths down (APD) handling on the ESXi host is enabled by default. When it is enabled, the host continues to retry nonvirtual machine I/O commands to a storage device in the APD state for a limited time frame. When the time frame expires, the host stops the retry attempts and terminates any nonvirtual machine I/O. You can disable the APD handling feature on your host. If you disable the APD handling, the host will indefinitely continue to retry issued commands to reconnect to the APD device. If you disable it, it's possible that the host could exceed their internal I/O timeout and become unresponsive.

You might want to increase the value of the timeout if there are storage devices connected to your ESXi host which might take longer than 140 seconds to recover from a connection loss. You can enter a value between 20 and 99999 seconds for the Misc.APDTimeout value.



Name	Value	Description
Migrate.TcpTsoDeferTx	0	Use TCP tso defer optimization for transmit
Migrate.TryToUseDefaultHeap	1	Attempt use the default migration heap when beginning new migrations
Migrate.VASpaceReserveCount	128	Number of migrations to reserve virtual address space for at module l...
Migrate.VASpaceReserveSize	768	Megabytes of virtual address space to reserve per migration at modul...
Migrate.VMotionLatencySensitivity	1	Make vMotion helper worlds latency sensitive, avoid transmit delays.
Migrate.VMotionResolveSwapType	1	Attempt to resolve swap type during VMotion initialization
Migrate.VMotionStreamDisable	0	Pretend to not support streams
Migrate.VMotionStreamHelpers	0	Number of helpers to allocate for VMotion streams
Migrate.Vmknic	vmk1	vmknic for vMotion vmkernel VNIC
Misc.APDHandlingEnable	1	Enable Storage APD Handling.
Misc.APDTimeout	140	Number of seconds a device can be in APD before failing User World ...
Misc.BHTimeout	0	Time-out for bottom-half handlers in milliseconds
Misc.BHTimeBound	2000	Time bound on BH checking in us (microseconds).
Misc.BlueScreenTimeout	0	Time-out in seconds. Set to 0 for no time-out.

- Browse to the host in the vSphere Web Client
- Click the Manage tab, and click settings
- Under System, click Advanced System Settings
- Under Advanced System Settings select the Misc.APDHandlingEnable parameter and click the Edit icon
- Change the value to 0
- Edit the MiscAPDTimeout value if desired

STORAGE TROUBLESHOOTING SCENARIO #4 – VSAN WON'T TURN ON

Before you begin it is important to realize that vSAN is a software based storage product that is entirely dependent on the proper functioning underlying hardware components, like network, storage I/O controller and the individual storage devices. You always need to follow the vSAN Compatibility Guide for all deployments.

Many vSAN errors can be traced back to faulty VMkernel ports, mismatched MTU sizes, etc. It's far more than simple TCP/IP.

When enabling vSAN, you need to verify that each host has connectivity to all hosts in the cluster via a VMkernel port marked for vSAN. You will also need to verify that each host has flash based disks that will be dedicated as flash tier and another typically slower disk used for the capacity tier. Note that it is possible to run all flash for both cache and capacity tier.

Some of the tools you can use to troubleshoot vSAN are:

- vSphere Web Client
 - The primary tool to troubleshoot vSAN.
 - Provides overviews of individual virtual machine performance.
 - Can inspect underlying disk devices and how they are being used by vSAN.
- esxcli vsan
 - Get information and manage the vSAN cluster.
 - Clear vSAN network configuration.
 - Verify which VMkernel network adapters are used for vSAN communication.
 - List the vSAN storage configuration.

Ruby vSphere Console

- Fully implemented since vSphere 5.5
- Commands to apply licenses, check limits, check state, change auto claim mechanisms, etc.
- vSAN Observer
 - This tool is included within the Ruby vSphere Console.
 - Can be used for performance troubleshooting and examined from many different metrics like CPU, Memory or disks.
- Third Party Tools

PART 4: NETWORK TROUBLESHOOTING

In vSphere, networking problems can occur at many different levels. It is important to know which level to start with. Is it a virtual machine problem or a host problem? Did the issue arise when you migrated the machine to a new host?

- Virtual switch connectivity can be managed in two ways:
 - Standard switches
 - Distributed switches

You also must determine if it's a virtual machine or a host management issue.

NETWORK TROUBLESHOOTING SCENARIO #1 – NO NETWORK CONNECTIVITY TO OTHER ESXI HOSTS

One of the first things you need to do is a simple ping. Ping a system that is up and that you have tested and should be accessible to the ESXi host.

Starting at the ESXi host, verify these possible configuration problems:

- Does the ESXi host network configuration appear correct? IP, subnet mask, gateway?
- Is the uplink plugged in? Yes, that had to be said.
 - `esxcli network nic list`
- If using VLANs, does the VLAD ID of the port group look correct?
 - `esxcli network vswitch standard portgroup list`
- Check the trunk port configuration on the switch. Have there been any recent changes?
- Does the physical uplink adapter have all settings configured properly? (speed, duplex, etc.)
 - `vicfg-nics -d duplex -s speed vmnic#`

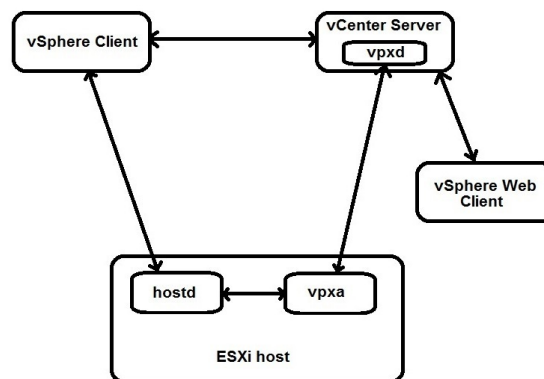
- If using NIC teaming, is it setup and configured properly?
- Are you using supported hardware? Any driver issues?
- If all of the above test ok, check that you don't have a physical adapter failure.

If you recently moved the VM to a new host, also verify that an equivalent port group exists on the host and that the network adapter is connected in the virtual machine settings. The firewall in the guest operating system might be blocking traffic. Ensure that the firewall does not block required ports.

NETWORK TROUBLESHOOTING SCENARIO #2 – ESXI HOSTS DROPPING FROM VCENTER

Occasionally an ESXi host is added to the vCenter Server inventory with no issues at all, but disconnects 60 seconds after the task completes.

Typically, this issue is because of lost heartbeat packets between vCenter (vpxd) and an ESXi host (vpxa).



The first thing you should check is that no firewall is in place blocking the vCenter communication ports. Then verify that network congestion is not occurring on the network. This issue is more prevalent with Windows based vCenter systems.

Adjust the Windows Firewall settings:

- If ports are not configured, disable Windows Firewall.
- If the firewall is configured with the proper ports, ensure that Windows Firewall is not blocking UDP port 902.

By default vpxa uses UDP port 902, but it is possible to change the ports to something else. Check the /etc/vmware/vpxa/vpxa.cfg file <ServerPort> setting.

```
~ # tail /etc/vmware/vpxa/vpxa.cfg
<hostIp>192.168.0.20</hostIp>
<hostKey>52402f1f-0caa-b281-cca7-fde7ed700a5e</hostKey>
<hostPort>443</hostPort>
<licenseExpiryNotificationThreshold>15</licenseExpiryNotificationThreshold>
<memoryCheckerTimeInSecs>30</memoryCheckerTimeInSecs>
<serverIp>192.168.0.10</serverIp>
<serverPort>902</serverPort>
</vpxa>
```

When it comes to network congestion, dropped heartbeats can happen as well. Some tools you can use to troubleshoot:

- You can use the resxtop utility or graphical views to analyze traffic.
- The pktcap-uw command is an enhanced packet capture and analysis tool.
 - pktcap is unidirectional and defaults to inbound direction only.
 - Direction of traffic is specified using --dir 0 for inbound and --dir 1 for outbound.
 - Two (or more) separate traces can be run in parallel but need to be merged later in Wireshark.
- Wireshark

NETWORK TROUBLESHOOTING SCENARIO #3 – NO MANAGEMENT CONNECTIVITY ON ESXI HOST

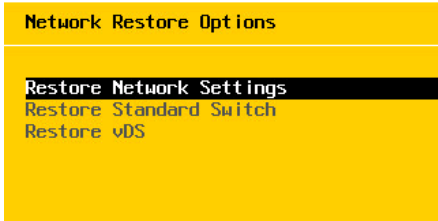
VMware Management networks are configured using VMkernel port groups. Typically, when a host loses connectivity to vCenter and was working prior, a recent change to that port group has caused the issue.

One feature VMware has, which helps in this case is the Rollback feature. Several different types of events can trigger a network rollback:

- Updating the speed or duplex of a physical NIC
- Updating teaming and failover for the management VMkernel adapter

- Updating DNS and routing settings on the ESXi host
- Changing the IP settings of a management VMkernel adapter

If any of the above are changed and it fails, the host rolls back to the last known good configuration.



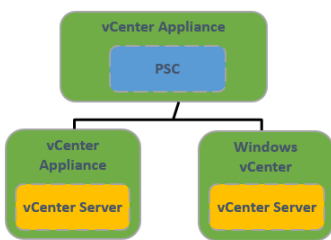
You can also restore the network configuration from the DCUI. Select “Network Restore Options” and you can select to restore either standard switches or distributed switches. The Restore Network Settings option deletes all the current network settings except for the

Management network if you’re looking to start with a new configuration.

PART 5: VCENTER AND ESXI TROUBLESHOOTING

Before we begin troubleshooting vCenter it is important to note that there are two major components to vCenter. First you have the Platform Services Controller. This component helps by scaling services across an organization and deals with identity management for various tools that interact with vSphere. It also includes vCenter Single Sign-On, the certificate store, certificate authority, the license service, directory service and lookup service. A Platform Services Controller can be connected to multiple vCenters.

vCenter Server includes the vCenter service, the web client service, inventory service, PostgreSQL, a syslog service, the dump collector and auto deploy.



Both components are required to run vCenter! Beginning with vSphere 6, vCenter Server for Windows and the vCenter Server Appliance can be used in the same deployment.

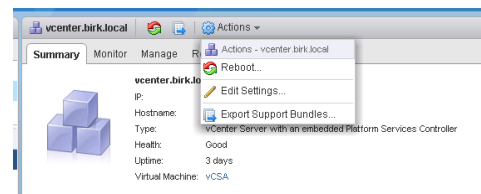
Side note: It is now recommended to use the vCenter Linux Appliance vs. vCenter on Windows.

Multiple Platform Services Controller instances can be used together when used with a load balancer.

One of the most important vCenter logs is vpxd.log. This is the main vCenter Server log, it contains all vSphere Client and web services connections, internal tasks and events, and communication with the vCenter Server Agent (vpxa) on managed ESXi/ESX hosts.

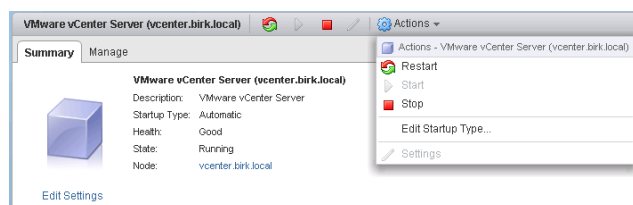
You may extract a support bundle from the vSphere Web Client as well.

- On the vSphere Web Client Home page, click **System Configuration**.
- Under System Configuration, click **Nodes**.
- Select a node from the list.
- Click the **Actions** menu and select **Export Support Bundle**.
- In the Export Support Bundle window, expand the trees to view the services running in the appliance and deselect the services for which you do not want to export log files.



VCENTER/ESXI TROUBLESHOOTING SCENARIO #1 – THE VCENTER SERVICE FAILS TO START

There are two different types of vCenters as mentioned, above. If you're using the Linux based appliance, check the vCenter Server service status from the vSphere Web Client. On a Windows based vCenter, run services.msc and check for error messages related to the service. In the image below, it is demonstrated using the vCenter appliance.



If the service still fails to start successfully:

- Check ODBC data source configuration.
- Use netstat and verify port 902, 443 or 80 are not being used by other services.

Occasionally the vCenter service will start but the Inventory Service is not functioning. You will generally notice this issue when creating storage profiles. VMware has also written scripts that will allow you to reset the inventory service database. See [KB 2146248](#) for more information and to download the script.

VCENTER/ESXI TROUBLESHOOTING SCENARIO #2 – VCENTER DATABASE HEALTH

The vCenter database is a critical component to vCenter. The database continues to grow because of the statistics collection and events tasks that it collects. If it is not healthy, the server will either not start or will start slower than normal.

Most of those these issues are related to a SQL Express installation where you may have a limited database file due to the edition limitation: SQL Express 2008 is limited to 1 CPU, 1 GB of RAM and 4 GB for database file, the SQL Express 2008 R2 version increase the maximum file to 10 GB and the SQL Express 2012 version also can use up to 4 cores. Generally this type of database should only be used in testing environments. Avoid using SQL Express for anything in a production environment!

Often, you will receive an error like this:

Could not allocate space for object 'dbo.VPX_EVENT':VPXI_EVENT_USERNAME' in database 'VCDB' because the 'PRIMARY' filegroup is full. Create disk space by deleting unneeded files, dropping objects in the filegroup, adding additional files to the filegroup, or setting autogrowth on for existing files in the filegroup.

If you are having problems with slow startups check the following items:

- If using SQL Server: Clean transaction logs.
- Verify disk space is available.
- Database authentication is setup properly.

If vCenter does not start, check the ODBC datasource configuration is correct. Verify that port 902, 80 or 443 is not being used by other processes. This happens more frequently when running vCenter on Windows.

If vCenter starts but is very slow to start up, you could also be experiencing database issues. Check that there happens to be disk space available, healthy transaction logs and that database authentication has not changed.

Follow these methods to resolve performance data growth issues:

- Ensure that statistic rollup jobs exist.
- Keep the vCenter statistic level at level 2 or lower and only increase when troubleshooting an existing issue.
- Ensure that statistic rollup jobs exist.

VMware has written a script and provided it in [KB 1025914](#). This script will truncate the event and tasks tables. Before running this script, be sure you take a full backup of the vCenter database.

VCENTER/ESXI TROUBLESHOOTING SCENARIO #3 – AN ESXI HOST HANGS DURING BOOT OR RANDOMLY

When an ESXi host hangs, it is typically either VMkernel being too busy, hardware failure or software failure.

To verify that an ESXi host is hanging, try the following tasks on the host:

- Ping the VMkernel network interface and check for response.
- If the host is hanging during boot, check what it's hanging on.
- Monitor network traffic and its virtual machine traffic. If you see virtual machine traffic, then your host is still functioning at a minimal level.

To verify that the host is hung, use the ESXi host's DCUI to check logs.

If the host is not responsive reboot the ESXi host first. Determine why the host locked up by reviewing the logs and looking for errors or performance anomalies. Reinstall ESXi and install the latest patches and updates.

VCENTER/ESXI TROUBLESHOOTING SCENARIO #4 – A VM IS EXPERIENCING MEMORY OR CPU ISSUES

ESXi hosts have several different levels of memory management techniques.

- Transparent Page Sharing
 - Allows pages with identical copies to be stored once.
- Balloon Driver (from VMware Tools)
 - Forces virtual machines to use their own internal page file, when host is in contention.
- Memory Compression
 - When memory contention is high, attempts to reclaim some memory performance.

- Memory Swapping
 - Uses swap space either specified at host level or with virtual machine files. Generally, performs poorly.

You can use esxtop or vCenter advanced performance charts to troubleshoot. First though, start with checking that hyperthreading is turned on. It can be overlooked.

We can navigate to screens displaying other resources by using different keystrokes. Although there are a multitude of available options, the following are the most commonly used when running esxtop.

c = cpu

m = memory

n = network

d = disk adapter

u = disk device

v = virtual machine disk activity

When troubleshooting memory performance:

MCTL This column is either YES or NO. If Yes it means that the balloon driver is installed. The Balloon driver is automatically installed with VMware tools and should be in every virtual machine.

MCTLSZ This column shows you how inflated the balloon is in the virtual machine. If it says 500MB, it translates to the balloon driver inside the guest operating system has “borrowed” 500MB from Windows/Linux etc. You would expect to see a value of 0 in this column.

SWCUR This section tells you how much memory the virtual machine has in the vswp file. If you see 500MB here, it means that 500MB is the swap file size. This does not necessarily mean bad performance however. To figure out if your virtual machine is suffering from swapping, you need to look at the next two counters.

SWR/s This value tells you the read activity to your swap file. If you see a number here, then your virtual machine is suffering from hypervisor swapping. Performance will likely be poor. You will probably be getting user complaints.

SWW/s This value tells you the write activity to your swap file. You want to see the number 0 (zero) here. Every number above 0 is BAD. Again, users will likely notice the performance issue at this point.

When troubleshooting CPU performance:

%USED This metric tells you how much time did the virtual machine spends executing CPU cycles on the physical CPU.

%RDY is one of the most important indicators when it comes to performance! Always start here. This defines how much time your virtual machine is waiting to execute CPU cycles but could not get access to the physical CPU. It tells you how much time you spend in line, patiently waiting for physical CPU.

%CSTP tells you how much time is spent waiting for a virtual machine with multiple vCPUs to catch up.

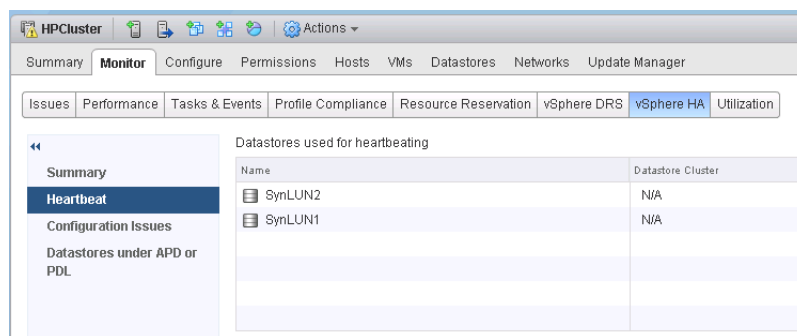
If you notice things are off, here a few things you can try to address these issues. First, start with resource pools, although if you are swapping and seeing significant performance problems, a resource pool is likely only going to be a temporary solution to fix the problem. You can, if acceptable, shut down other non-production machines to free up resources. Another option would be to add additional ESXi hosts.

PART 6: HA, DRS AND VMOTION TROUBLESHOOTING

HA, DRS AND VMOTION TROUBLESHOOTING SCENARIO #1 – HA DOES NOT TURN ON WHEN ENABLED

First check some possible causes. Start with the network connectivity between the ESXi host and the vCenter server. A proper VMkernel port group marked for Management is required. Are all hosts connected to vCenter?

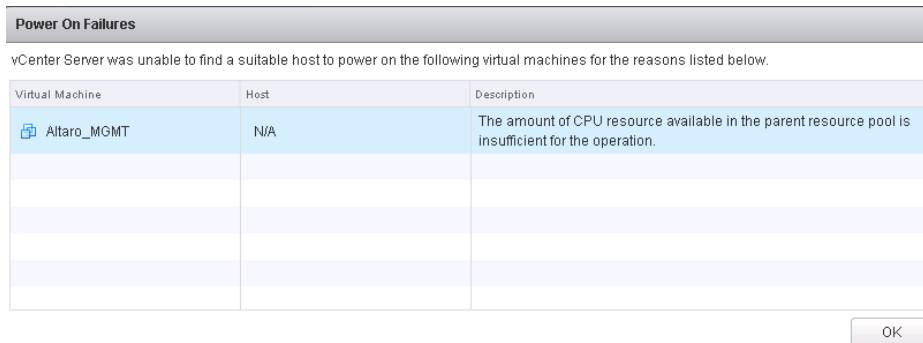
- All hosts in an ESXi HA enabled cluster require static IP addresses or if using DHCP, the IP addresses must stay persistent across reboots.
- Verify DNS name resolution works, this is more important in older versions of vSphere (4.x).
- You need at least two ESXi hosts.
- All hosts must be licensed for HA (Essentials Plus or higher).
- Are datastores required for network heartbeats connected to all the hosts? Two heartbeat datastores are recommended (see below).
- Even though HA will work with a single management VMkernel network, it is highly recommended to have two.



It is also possible that the FDM Agent cannot be installed on the ESXi host. Check the agent installation log at `/var/log/fdm-installer.log`.

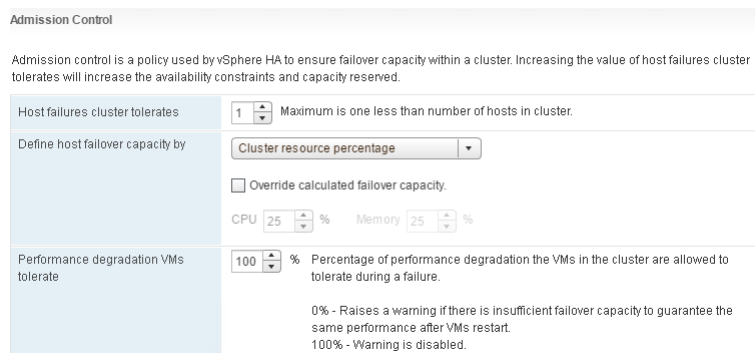
On the ESXi host, check to see if there are agent files (`clusterconfig`, `fdm.cfg`, `hostlist` and `vmmetadata`) in the `/etc/opt/vmware/fdm` directory.

HA, DRS AND VMOTION TROUBLESHOOTING SCENARIO #2 – ERROR MESSAGES ABOUT INSUFFICIENT RESOURCES



Typically, you will receive this error when powering on a machine in a HA cluster with insufficient resources. Check the following information:

- HA admission control policy is not configured correctly.
 - If using manually configured slot sizes, verify slot sizes.
 - The default admission control policy in vSphere 6.5 is now “Cluster resource percentage” which greatly reduces the number of slot related issues.



- The virtual machine does not have reservations set properly. Generally, they are set too high and the host cannot guarantee the reservation. Remember an ESXi host will only power on virtual machines if the reservations can be guaranteed.
- It is also possible that the cluster has no available physical resources. You will need to add more hosts to the cluster to ensure adequate performance.

HA, DRS AND VMOTION TROUBLESHOOTING SCENARIO #3 – VMOTION FAILS OR TIMES OUT

If vMotion was working and suddenly stops working first start by restarting your management agents by issuing the following commands:

- `/etc/init.d/hostd restart`
- `/etc/init.d/vpxa restart`

You can also restart the management agents in the DCUI on the host.

After restarting management agents, verify the following:

- Check VMkernel network connectivity. Are IP settings still valid?
- Check NTP settings, and verify all hosts are syncing to the same source.
- Verify VM reservation requirements are met at the target host.
- Verify that the `log.rotateSize` parameter in the virtual machine `.vmx` file is not set too low. The default is 0, which is unlimited.

HA, DRS AND VMOTION TROUBLESHOOTING SCENARIO #4 – DRS DOES NOT VMOTION MACHINES

When working in a cluster, it is important to make sure that all of your ESXi hosts are configured the same. They need access to the same virtual machine port groups, storage, vMotion network. If hosts are setup at different times this can be overlooked.

If the hosts are not equally balanced, and the cluster is set to fully automated mode, a vMotion should occur automatically.

If vMotions fail, check the following items:

Verify that the DRS automation level is not set to manual mode.

Test that vMotion is working manually.

This will verify that the vMotion network is properly configured.

If your virtual machine fails to migrate, check that it is not attached to any local resources that the other host does not have access to.

CONCLUSION

To wrap up, there is no perfect way to troubleshoot. The scenarios in this eBook are some of the more popular methods you will see as a VMware Administrator and should help get you in the right direction. Always start with the simple things and work from there!

ABOUT ALTARO

Altaro Software (www.altaro.com) is a fast growing developer of easy to use backup solutions used by over 30,000 customers to back up and restore both Hyper-V and VMware-based virtual machines, built specifically for Small and mid-market business with up to 50 host servers. Altaro take pride in their software and their high level of personal customer service and support, and it shows; Founded in 2009, Altaro already service over 30,000 satisfied customers worldwide and are a Gold Microsoft Partner for Application Development and Technology Alliance VMware Partner.

ABOUT ALTARO VM BACKUP

Altaro VM Backup is an easy to use backup software solution used by over 30,000 Small and mid-market business customers to back up and restore both Hyper-V and VMware-based virtual machines. Eliminate hassle and headaches with an easy-to-use interface, straightforward setup and a backup solution that gets the job done every time.

Altaro VM Backup is intuitive, feature-rich and you get outstanding support as part of the package. Demonstrating Altaro's dedication to Hyper-V, they were the first backup provider for Hyper-V to support Windows Server 2012 and 2012 R2 and also continues support Windows Server 2008 R2.

For more information on features and pricing, please visit:

<http://www.altaro.com/vm-backup>

Don't take our word for it – Take it for a spin!

DOWNLOAD YOUR FREE COPY OF ALTARO VM BACKUP

and enjoy unlimited functionality for 30 days. After your 30-day trial expires you can continue using the product for up to 2 VMs for free, forever. No catch!

Altaro VM Backup - Trusted by over 30,000 SMBs

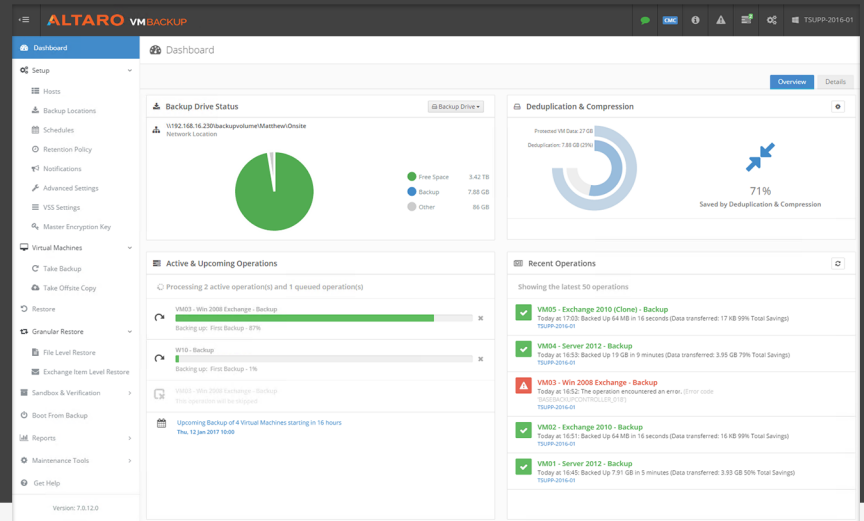
New v7! Altaro VM Backup for Hyper-V & VMware. Hassle-free and affordable VM backup software. Grab your free copy for 2 VMs now!

- ✓ Hassle-free and effective
- ✓ Unbeatable Value
- ✓ Outstanding Support

Free for 2 VMs, forever.

Back up unlimited VMs for 30 -days. After 30-days you get 2 VMs for free, forever. Download now!

Backup Now!

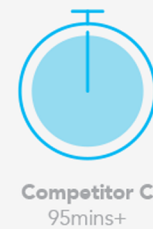


Up and running quickly, without the need for complex configurations!

With Altaro VM Backup, you can install and run your first virtual machine (VM) backup in less than 15 minutes. Get up and running quickly, without the need for complex configurations or software dependencies.

Altaro VM Backup is designed to give you the power you need, without the hassle and steep learning curve.

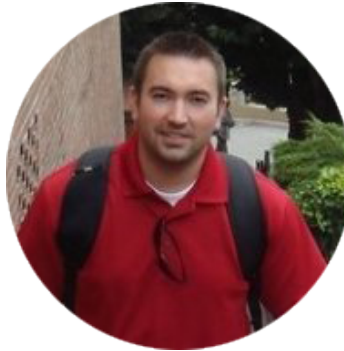
- **Easy to use, intuitive UI** - making it easy to implement a rock solid backup strategy
- **Managing and configuring backup/restore jobs across multiple hosts has never been simpler**
- **Full control & scalability** - Monitor and manage all your Hyper-V and VMware hosts from a single console



Virtual machine backup software packed with powerful features for Hyper-V and VMware.

[View Features](#)

ABOUT RYAN BIRK



Ryan has been working in Information Technology for many years and calls himself a “virtualization snob” these days. He has been a Virtualization Consultant, Engineer and Technical Instructor most recently. Since 2012, he has been a proud VMware vExpert and runs a blog at ryanbirk.com, which happens to focus on VMware home labs.

[@ryanbirk](#)

VMware vExpert 12-17

VMware Certified Instructor

FOLLOW ALTARO

Like our eBook? **There's more!**

Subscribe to our Hyper-V blog <http://www.altaro.com/hyper-v> and receive best practices, tips, free Hyper-V PowerShell scripts and more here: <http://www.altaro.com/hyper-v/sign-up>

Follow Altaro at:



SHARE THIS RESOURCE!

Liked the eBook? Share it now on:

