DST Systems, Inc.

ES VMware Performance, Best Practices, and Tasks for Supporting Teams

Documentation and Instructions v2015.04.30

VMware Virtualization Team –Jeff Walker
9/26/2014

Contents

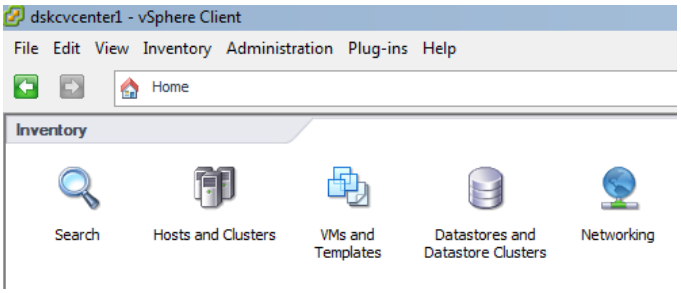
Enterprise Services Virtual Environment Overview

Accessing the Enterprise Services Production VMware Environment

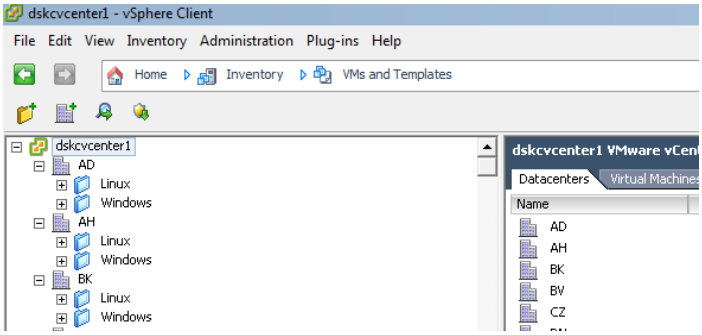
To access the Enterprise Services VMware Environment you will need permissions and the vSphere client. The vSphere client can be downloaded by navigating to https://dskcvcenter1 and clicking on the Download vSphere Client link. Install the software with the default settings. Once installed, launch the application and provide the name DSKCVCENTER1 in the IP address / Name box, and click on the box to Use Windows Sessions Credentials, or provide an account manually, then hit login. If prompted for certificates, select the box to install the certificates and hit Ignore. When you use the vSphere client you are connecting to a VMware vCenter Server.

Navigating the vSphere Client

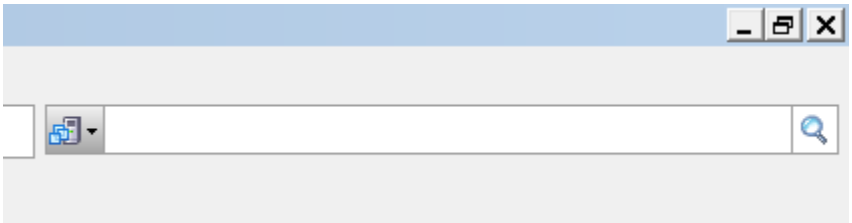
From the home screen of the vSphere client select the VMs and Templates icon. It is in the VMs and Templates view that most teams outside of the VMware team will operate:



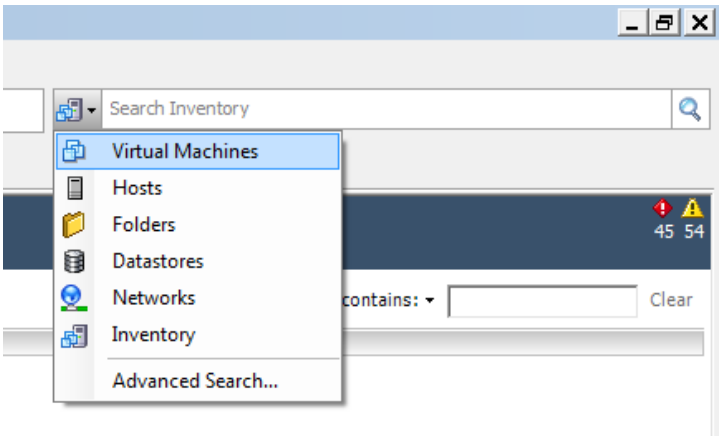
On the VMs and Template view, you will be presented with icons which represent each virtual Datacenter in inventory. Expand the Datacenter object you want to and you will see a Folder structure which organizes the Virtual Machines. Every Datacenter will have a Windows and Linux folders, their respective teams have access to their folders.



Become familiar with the search function in vCenter as it is very difficult to navigate the Virtual inventory manually because of the volume of objects. The search bar can be found in the top right corner of the vSphere client.



You can filter your search results by object type to speed up returns:



If you find yourself in a view in vCenter where you see no objects or "lack" permissions, you simply need to navigate back to the VMs and Templates view.

Permissions and AD Groups

It is important that you know which VMware AD groups you are a member of so that you can easy know what corresponding permissions are associated with your account. Outlined below are the current AD VMware groups associated with VMware and their permissions. If you are unsure which group you are in or believe you need additional permissions please contact a VMware Team member, in almost all cases additional permissions will require training on some degree from a VMware Team member. The mentioned AD groups are managed by the VMware team and a periodically audited.

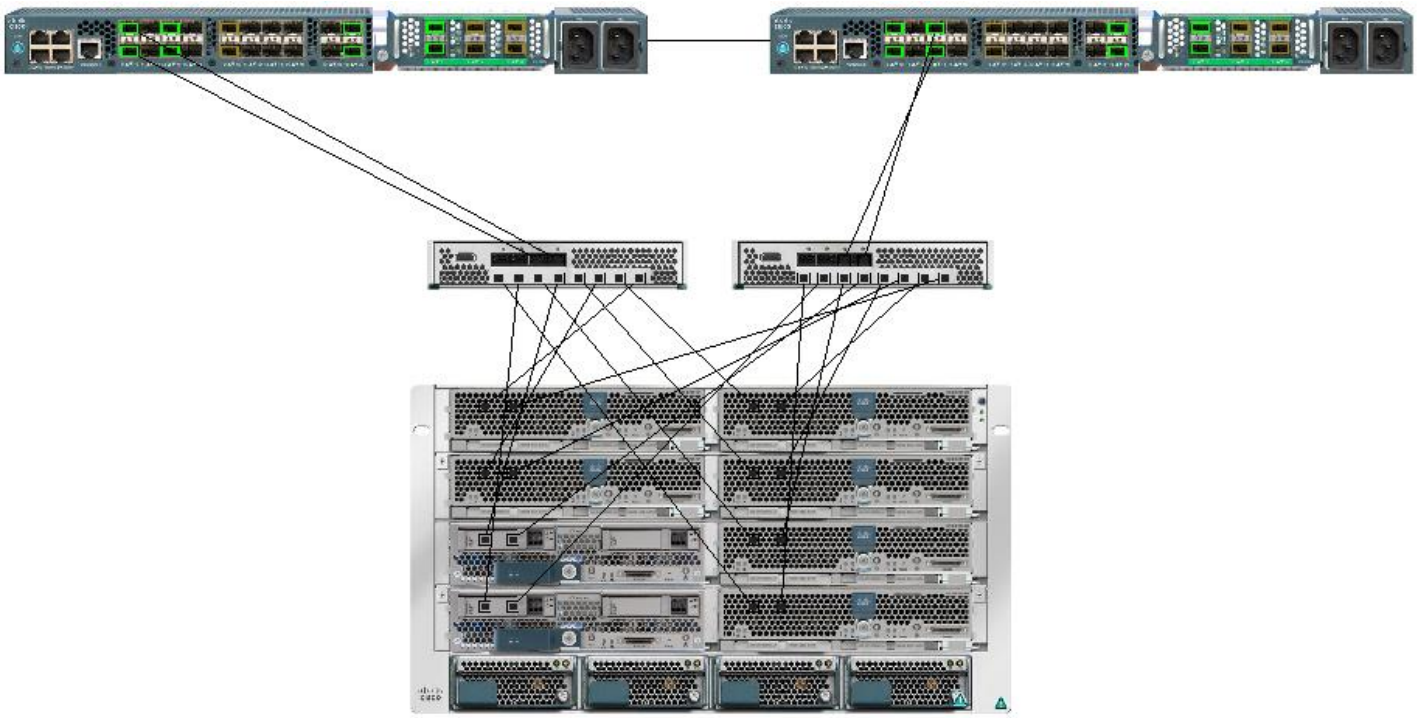
AD Group	VMware Role	Permissions
n/a	ES VM Console	Console Interaction, Power On/Off, Reset
G-ES VMware User (Linux, Windows)	ES VM User	All ES VM Console Permissions, Console Interaction, Assign Network, Scheduled Tasks, CD and Floppy Drive, Connect Hardware Devices, Move VM Folder, Create Remove and Revert To Snapshot, VMware Tools Install
G-ES VMware Modify (Linux, Windows)	ES VM Modify	All ES VM Console Permissions, All ES VM User Permissions, Allocate Datastore Space to VMs, Browse Datastores, Update Virtual Machine files on Datastores, View Storage Views, Change VM Resource, Extend Virtual Disk, Edit Memory, Modify Device Settings, Remove VM Disks, Upgrade Virtual Hardware, Edit and View VM Settings
G-ES VMware Template Admins (Linux, Windows)	ES VM Template Admin	All ES VM Console Permissions, All ES VM User Permissions, All ES VM Modify Permissions, Reconfigure Virtual machine, Assign Virtual machine to Resource Pool, Add New Disk, Remove Disk, Add or Remove Device, Change CPU Count, Change Resources, Create VM from Template, Create New VM, Clone Template, Deploy Template, Mark as Template, Mark as Virtual Machine, Read and Modify Customization Specifications.
G-ES VMware Dashboard	n/a	The VMware Team Dashboard outlines compliance standards we have established as a team and whether we are meeting or missing them. The dashboard also outlines our capacity needs for compute and storage resources. Link: \\ad.dstsystems.com\dskcdfs\data1\AHS\Virtualization Support\VMware\vSphere-Dashboard.html
DL-VMware vCenter RO (Read Only)	Read-Only	Read Only access allows all items in vCenter to be seen and reviewed but does not allow execution.

VMware Environment Underlying Infrastructure

The Enterprise Services VMware environment operates primarily on Cisco UCS server hardware and on Hitachi storage, only at the smaller remote sites do these primary platforms change. Currently 80% of our Virtual Machine workloads run on Cisco UCS and Hitachi storage.

VMware Server Platform

Cisco UCS is a completely redundant blade enclosure platform that in many ways is specifically tailored for virtualization workloads. Below is a high level diagram of UCS hardware architecture pulled straight from the UCS management software, called UCS Manager (UCSM):



A UCS environment is known as a UCS Domain or UCS Hardware Domain. A UCS domain is comprised of two Fabric Interconnects (FIs, seen and the top of the image) and at least one UCS Chassis (seen at the bottom of the image), the Chassis also includes two I/O Modules (IOMs), these IOMs are configured so that one IOM is associated to Fabric A and the second to Fabric B. This designation of Fabrics at both the FI and Chassis levels allow for an entire fabric to be lost, due to failure or upgrade, and operations still to continue. Although the FIs are seen as primary and subordinate, they operate as active/active for traffic. Three different resources are cabled to the FIs, and both FIs should be identical:

1. Upstream access (Network)
2. Chassis access (Server)
3. FCoE access (Storage)

UCS Manager (UCSM) operates from the primary Fabric Interconnect and provides the brain for the UCS environment. UCSM serves many purposes but, for the sake of this document, suffice it say that UCSM is utilized to create and apply hardware identities (Service Profiles) to blades in the connected Chassis.

While ESXi provides us a platform to virtualize individual guest server workloads, Cisco UCS provides us the platform to virtualize Server hardware identities. This virtualization of server hardware identities is based on a technology called Service Profiles. Service profiles contain all of the details and components that comprise a physical server, only they are kept in an XML file. A Service Profile contains all details relating to BIOs, HBA, NIC, CIMC, Firmware, Power Control, and UUID. A Service Profile Template can be created which allows for children profiles to be spun up and keep the base configuration of the parent, this allows for easy standardization

for all ESXi hosts. When a Service Profile is applied to a blade, that blade is then configured with BIOs settings, firmware is applied, and all HBAs and NICs are logically created on the blades Virtual Interface Card (VIC).

If utilizing boot from SAN, which is a standard within the VMware team, server identities can float from one blade to another if needed.

The Cisco UCS Domains and hardware are managed by the VMware team.

VMware Storage Platform

The storage platform for the VMware environment is provided to the VMware team as a consumable resource from the Open Systems Storage team. 80% of our Virtual Machine workloads run on Hitachi Storage, while some of the smaller sites use local storage, EMC, and 3PAR.

At a high level the Hitachi arrays are configured in pools, these pools include the following types of disk: 7K Near-line SAS, 10K SAS, and SSD. The Hitachi arrays are configured to perform dynamic tiering of workloads, which means that if certain blocks of storage or certain LUNs are hit heavy than others then those blocks or LUNs will be potentially migrated up to a higher Tier of storage disk. This makes it difficult for a VMware administrator to tell you directly what type of disk a certain VM is operating on, but in a general sense, if a workload needs more I/O it will be moved accordingly.

The Storage arrays are managed by the Open Systems Storage team.

Datacenters

In the Enterprise Services vCenter, each virtual Datacenter corresponds to a physical location/Datacenter. Datacenters in vCenter are logical representations and folder hierarchy of an actual Datacenter defined by a VMware Administrator. For description purposes below are the building codes and Long names for the Datacenters in vCenter. Some Datacenters contain multiple ESXi clusters for different environments, such as the WC Datacenter which houses clusters for Share Serve, HE1, HE2, HE3, HETD, etc…

Name	Description	State/Country	Clusters	Cluster Description
AD	AD-Adelaide	Canada	ADBRK	Cluster for Brokerage Solutions
			ADSSRV	Cluster environment for IFDS/BPS
AH	AH-Birmingham	AL, USA	AHSSRV	Shareserve Cluster
BK	BK-Bangkok	Thailand	BKSSRV	Shareserve Cluster
BV	BV-Boston	MA. USA	BVSSRV	Shareserve Cluster
CZ	CZ-Pune	India	CZSSRV	Shareserve Cluster
DN	DN-Denver	CO, USA	ALPSSSRV	Cluster for ALPs at their location
			ALPSSSRVDR	DR Cluster for ALPs at a Colo DC
ED	ED-El Dorado Hills	CA, USA	DOINTA	Cluster for DSTO primarily
HA	HA-Hartford	CT, USA	HASSRV	Shareserve Cluster
HB	HB-Harrisburg	PA, USA	DHSSRVHB	Shareserve Cluster
IC	IC-St Louis	MO, USA	DSHE1B	DR Cluster for WC HE1
			DSHE2	DR Cluster for WC HE2
			ICDRE	DR Cluster for WC Shareserve
			ICEXC	Exchange Cluster, logically Shareserve
			ICHE3	Production HE3 at STL
			ICHE3DR	DR Environment for WC HE3
			ICSSRV	Shareserve Environment
LB	SWBP-Kansas City	MO, USA	LBSSRV	Previously Literbuilding now Southwest Business Park
MA	MA-Markham	Canada	MABRK	Cluster for Brokerage Solutions
			MASSRV	Cluster environment for IFDS/BPS
MP	MP-Minneapolis	MN, USA	MPSSRV	Shareserve Cluster
PD	PD-Kansas City	MO, USA	DSINTB	Being retired
			PDAWD	Test cluster provided to BPS for JVM workloads

			PDBIMON	Failover nodes for BPS Bimon workloads
			PDEUEM	Cluster for network collecters and analyzers in PD
			PDSSRV	Shareserve Cluster
QC	QC-Hyderabad	India	QCSSRV	Shareserve Cluster
UK	UK-Surbiton	United Kingdom	SBSSRV	Shareserve Cluster Primarily for SS&C
WC	WC-Kansas City	MO, USA	DSHE1B	HE1 Environment, boots and operates off 3PAR
			DSHE1BB	HE1 Environment, boots and operates off HDS
			DSHE2	HE2 Environment
			DSHE3A	HE3 Environment
			DSHETD	Hosting Test Dev environment
			DSSSRVWC	CLM Staging environment for SSRV deployments
			WCBIMON	BIMON cluster for BPS, 1 active 1 passive host
			WCDB	Dedicated database Cluster, licensed at the ESXi level
			WCEUEM	Cluster for network collecters and analyzers in WC
			WCEXC	Exchange Cluster, logically Shareserve
			WCLSS	Shareserve Cluster, only Linux workloads
			WCWSS	Shareserve Cluster, only Windows workloads
WE	WE-Weymouth	MA, USA	WESSRV	Shareserve Cluster

ESXi Clusters

ESXi Clusters are groups of servers which run the VMware Hypervisor called ESXi. In a clustered configuration, ESXi hosts can provide High Availability by utilizing VMware High Availability (HA) and compute resource Load Balancing through VMware's Dynamic Resource Scheduler (DRS). At the time of this writing there can be a maximum of 32 ESXi hosts per Cluster, this will increase to 64 when the environment is upgraded to version 6.0. Clusters show as objects under Datacenters in the Hosts and Clusters view in the vSphere client, not all individuals will be able to see clusters.

Virtual Machines

What is a Virtual Machine?

A virtual machine is a software computer that like a physical computer runs an operating system and applications. The virtual machine is comprised of a set of specification and configuration files and is backed by a physical server running a Hypervisor.

A Virtual Machine is operated in similar ways to that of a physical machine, it can be powered on and off, have CD ISO images attached, custom BIOs settings configured, boot policies set, etc.

Virtual Machine Hypervisor Processes

A virtual machine is composed of several processes or userworlds that run in the VMkernel which is a part of the ESXi Hypervisor. Combined, the processes collectively make up a group. The following is a summary of process components of a Virtual Machine:

- Virtual Machine Executable (VMX) process - A process that runs in the VMkernel that is responsible for handling I/O to devices that are not critical to performance. The VMX is also responsible for communicating with user interfaces, snapshot managers, and remote console.
- Virtual Machine Monitor (VMM) process - A process that runs in the VMkernel that is responsible for virtualizing the guest OS instructions, and manages memory. The VMM passes storage and network I/O requests to the VMkernel, and passes all other requests to the VMX process. There is a VMM for each virtual CPU assigned to a virtual machine.
- Mouse Keyboard Screen (MKS) process - A process that is responsible for rendering the guest video and handling guest operating system user input.

Virtual Machine Configuration File Types

In conjunction with the processes of that run a Virtual Machine, a VM is backed by a set of files that contains the VM details, disk layouts, UUIDs, and custom settings. The following is a summary of files that create a Virtual Machine:

.vmx – Primary configuration file of a Virtual Machine, a VM exists only if it has an associated .vmx file. This file contains the VM UUID, mappings to all of the VM devices such as hard disks, PCI details and other information.

.nvram – Virtual Machine BIOs data and state.

.vswp – Virtual memory swap file, this file is auto generated everytime the VM is powered on. It is equal to the size of the Virtual Machine memory allocation. It is used only in times of great strain on the ESXi host.

.vmdk – Virtual Disk descriptor file, text file containing information and settings for the actual data disks.

*-flat.vmdk - Virtual Disk file that stores the data of the Virtual Machine's hard disks, must have an associated .vmdk file.

-00000.vmdk – Snapshot disk file, this disk associates with a new descriptor file but tracks changes made to the flat.vmdk parent file.

In the below screen capture you can see all of the files that make up the VM called brad-app-test01, these files are all stored on a VMware Datastore talked about later in this document:

```
/vmfs/volumes/534d82db-3efee6a7-a3d4-0024817bcfa2/brad-app-test01 # ls -l
-rw-------    1 root     root          7063416832 Sep 29 18:30 brad-app-test01-000001-delta.vmdk
-rw-------    1 root     root                360 Sep 22 16:30 brad-app-test01-000001.vmdk
-rw-r--r--    1 root     root                 65 Sep  4 19:26 brad-app-test01-2609f13a.hlog
-rw-------    1 root     root          1073741824 Sep 22 16:30 brad-app-test01-2609f13a.vswp
-rw-------    1 root     root              29478 Apr 29 19:15 brad-app-test01-Snapshot3.vmsn
-rw-------    1 root     root       107374182400 Apr 29 19:13 brad-app-test01-flat.vmdk
-rw-------    1 root     root              8684 Sep 29 18:24 brad-app-test01.nvram
-rw-------    1 root     root               553 Apr 29 19:16 brad-app-test01.vmdk
-rw-------    1 root     root               410 Sep 22 16:27 brad-app-test01.vmsd
-rwxr-xr-x    1 root     root              3936 Sep 22 16:30 brad-app-test01.vmx
-rw-r--r--    1 root     root               270 Sep 18 18:18 brad-app-test01.vmxf
-rw-r--r--    1 root     root             95876 Sep  5 18:36 vmware-58.log
-rw-r--r--    1 root     root             96459 Sep  5 18:49 vmware-59.log
-rw-r--r--    1 root     root             95877 Sep  5 18:55 vmware-60.log
-rw-r--r--    1 root     root             96460 Sep  5 19:34 vmware-61.log
-rw-r--r--    1 root     root             95870 Sep 18 18:14 vmware-62.log
-rw-r--r--    1 root     root             94092 Sep 22 16:27 vmware-63.log
-rw-r--r--    1 root     root            110082 Sep 26 18:09 vmware.log
-rw-------    1 root     root          51380224 Sep 22 16:30 vmx-brad-app-test01-638185786-1.vswp
```

https://www.vmware.com/support/ws55/doc/ws_learning_files_in_a_vm.html

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1002511

Virtual Machine Sizing

Unlike physical machines where it can be common practice to purchase resources for future possible load, Virtual Machines should be sized with the minimum amount of resources needed to successfully handle the entire load on the VM. With the ability to hot add Virtual Machine resources in a matter of seconds, Virtual Machines should be sized to handle current load and if needed have resources added as greater demand is placed on the VM. Keep in mind that hot add is limited to certain guest OS types and versions and therefore reboots may be necessary.

The tighter a VM can run, the better performance it will have, for example, having a VM that runs on average between 0%-60% CPU utilization and is able to spike higher but never plateaus at 100% is a healthy VM, the same example is applicable to memory utilization.

Currently at DST the average Virtual Machine Resource Allocations are as follows:

- Average VM vCPU Allocation: 2 (90% of VMs have 2 vCPUs or less)
- Average VM Memory Allocation: 5 GB
- Average VM Disk Allocation: 256 GB

CPU

CPU Virtualization

ESXi does not use emulation to provide processor time and resources to a VM. Emulation designates that all operations are ran in software; this is not the case with virtualization using ESXi. When an ESXi host has a CPU or CPUs which allow for chipset virtualization (like Intel-VT or AMD-V), called Hardware Assisted Virtulization, CPU processes coming from the Virtual Machines are passed by the hypervisor and ran directly on the system processors.

Because Virtual Machines have such in-depth access to the physical CPUs, you will notice that at the guest OS level, the Operating system recognizes not only that it has the assigned CPUs but also the make and model. Virtual Machines have the ability to use every feature of the chipset because of this direct access. This is unlike virtualized memory presented to a VM, because the hypervisor creates a virtual contiguous memory space for a VM, the DIMMs presented to the guest OS show a generalized make and model for the Memory DIMMs that the VM thinks are physical banks.

The ESXi CPU scheduler spreads load across all sockets by default. This improves performance by maximizing the aggregate amount of cache available to the running virtual CPUs. As a result, the virtual CPUs of a single SMP virtual machine are spread across multiple sockets (unless each socket is also a NUMA node, in which case the NUMA scheduler restricts all the virtual CPUs of the virtual machine to reside on the same socket.)

In some cases, such as when an SMP virtual machine exhibits significant data sharing between its virtual CPUs, this default behavior might be sub-optimal. For such workloads, it can be beneficial to schedule all of the virtual CPUs on the same socket, with a shared last-level cache, even when the ESXi host is under committed. By default, Virtual machines are preferentially scheduled on two different cores rather than on two logical processors on the same core.

CPU Sizing

Determinations on whether CPU and Memory resources should be altered on a Virtual Machine should only be made with the assistance of member of the Enterprise Services VMware team, which includes reviewing VM performance in comparison to Guest level performance statistics. Although many individuals will have access to alter VM resources this should only be done once a performance review has been completed with a qualified individual. After the review, any number of people can then be instructed to add or remove the decided upon resources. If you are not qualified to determine VM resources or if a request has come in from a business unit to add resources, do not perform resource change operations without having a proper performance review with the VMware Team and without being instructed to do so.

CPU sizing and allocation is crucial to the performance of a Virtual Machine. Performance can be impacted negatively when a VM is presented to few vCPUs and conversely when a VM is presented too many vCPUs. In VMware, a vCPU (1 Virtual CPU assigned to a VM) is equal to 1 undedicated physical core. When the VMware team determines ideal CPU density on an ESXi host, they are determining the vCPU to pCPU ratio which can then be compared against actual resource usage numbers. For tier 1 workloads, ideally density ratios should be around 1.5:1 vCPU to pCPU, in normal operating environments (like Share Serve) anywhere between 3:1 and 5:1 is considered good.

Regarding CPU performance stats, when looking at both the VMware performance charts and the OS performance charts the VMware performance charts with always be most accurate. The hypervisor schedules each CPU cycle on the physical cores and is therefore able to track performance and usage to a degree that the OS performance tools cannot. In ideal situations, the CPU performance charts on both the VMware side and OS side should display performance data that is very close to one another, if large discrepancies are found between the VMware performance charts and OS level charts (i.e. VMware shows 10% CPU usage and the

OS is spiked to 90-100%) please engage the VMware team, this will require some troubleshooting from our side, for instance an ESXi host could be experiencing issues and the VM may need to be relocated.

CPU Performance

VMware CPU Performance Counters

https://www.vmware.com/support/developer/vc-sdk/visdk41pubs/ApiReference/cpu_counters.html

CPU Usage (Percent)

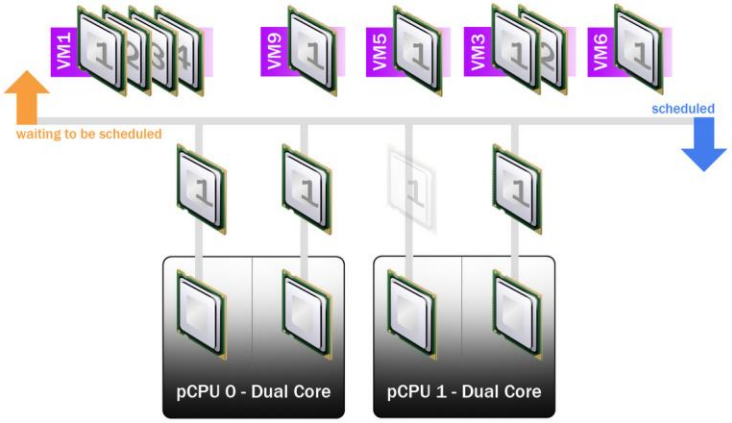
CPU usage by percent is an invaluable metric to reference. As simple as it sounds, it is the percent used of the allocated vCPUs. As mentioned earlier in this document, having a VM where the CPU runs on average between 0-60% and can spike higher but does not plateau is a healthy VM. If a VM is experiencing constant plateauing, then the VM should be evaluated for a vCPU increase, please contact a VMware Team member.

CPU Ready Time

CPU Ready time is a metric that tracks the amount of time in milliseconds that a VM's vCPUs needed to be scheduled on the physical CPUs but couldn't, therefore leaving the VM in a state where it is "Ready" for CPU cycles but instead finds itself not processing. CPU scheduling happens now (ESXi 5.0 and greater) differently than it did in previous versions, particularly in 3.x versions. The CPU scheduler in ESXi 3.x is now known as the "Strict Co-Scheduler", strict because in that version of the process and previous versions, all vCPUs of a VM must be scheduled on the physical hardware all at once or else it would wait for a time when all vCPUs could be scheduled at once, thus creating CPU ready time.

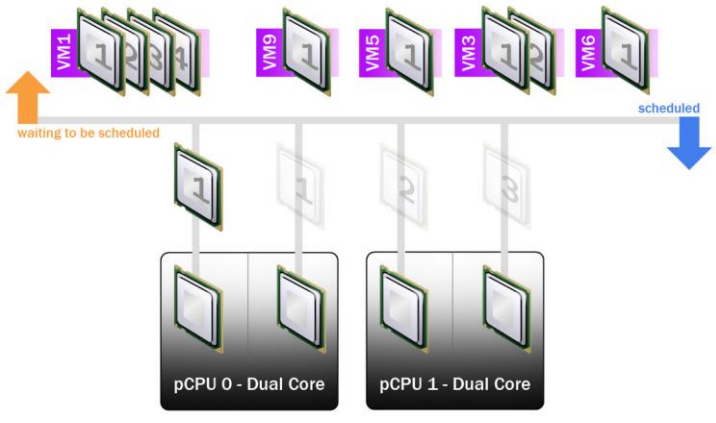
Below in Diagram 1, we can see that in the scheduled CPU requests, we have 1 available core that could be scheduled, represented by the lighter CPU icon. In the strict co-scheduler days, the only VMs that could be scheduled at that moment are VMs 5, 6, and 9. Because VM3 and VM1 have more than 1 vCPU, they accumulate CPU ready time being that they are in need of physical CPU resources but not all vCPUs can be scheduled simultaneously. In diagram 2, we have 3 available physical cores that can be scheduled; this means that any VM excluding VM1 could be scheduled; this scenario once again creates CPU ready time for VM1. In current versions of ESXi, a newer version of the co-scheduler has been implemented, known as the "Relaxed Co-Scheduler". The relaxed co-scheduler will always attempt first to schedule all vCPUs at once as this will produce the best performance for a VM, but it is no longer limited to scheduling all vCPUs or none. The relaxed co-scheduler can schedule individual vCPUs if it is determined that scheduling some is better than waiting for a time when all can be scheduled. Although this helps keeps VMs processing to some degree, a VM will still accumulate CPU ready time for the vCPUs that couldn't be scheduled. Effectively with the relaxed co-scheduler they are allowing a VM to process at a lower rate rather than not at all. The Relaxed co-scheduler increases performance but does not eliminate CPU Ready time especially in overly dense environments.

Diagram 1



1 Free pCPU

Diagram 2



3 Free pCPU

In situations like that illustrated by Diagram 2 some might wonder, "If all 4 VMs could be scheduled but the sum of the vCPUs for all 4 VMs is greater than what is physically available, which VMs would be scheduled?" The answer for Diagram 2 is that VM3 will get

scheduled and then between the three VMs with 1 vCPU it will be first come first served. VM3 will be scheduled first because it is considered more important being it has 2 vCPUs rather than 1 vCPU. By default, ESXi considers VMs with higher resource allocations as higher priority.

All virtual machines experience CPU ready time, the CPU ready time metric on a VM will never be zero on a powered on VM, unless the resources on the ESXi hosts can easily fulfill the resource requests for all VMs running on the host (i.e. a host with 2 sockets 12 cores running 10 virtual machines each with 1 vCPU). CPU ready time is a metric specific to VMware but metrics that are synonymous with it can be found in any virtualized shared resource environment:

- Hyper-V: CPU Wait Time Per Dispatch
- LPAR: CPU Ready Percent

Because all VMs have some degree of CPU Ready time it is important to bring awareness to the fact that there are safe zones for CPU Ready time, in these safe zones performance of the VM is not impacted.

It has been established that a CPU Ready time value of 2.5% is acceptable and no performance impact will be felt. Any amount above the acceptable threshold could result in negative performance on the Virtual Machine. The math to determine the percent CPU ready time value is this:

(<current Metric Value IN Milliseconds>/<interval collection IN Milliseconds>)*100

Because vCenter tracks metrics for different time periods at different intervals, it is important to know that the threshold for CPU Ready Time, as well as other metrics, can be different depending on the chart you are viewing in the vSphere Client. Below are the determined thresholds based on the different chat intervals.

Real-Time Chart:

- Updated every 20 seconds
- 500ms Threshold
- (500/20,000)*100=2.5%

Day Chart:

- Updated every 5 minutes (rolls up real-time stats)
- 7500ms Threshold
- (7500/((5*60)*1000))*100=2.5%

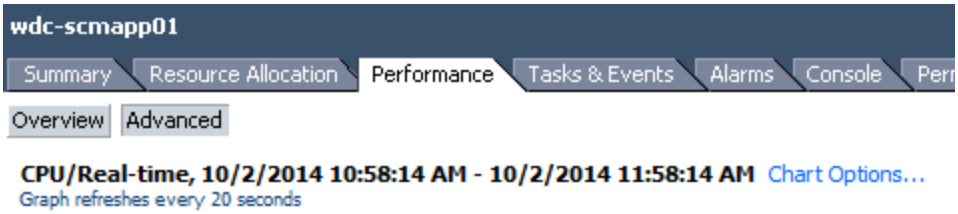
Week Chart:

- Updated every 30 minutes (rolls up 5 minute stats)
- 45000ms Threshold
- (45000/((30*60)*1000))*100=2.5%

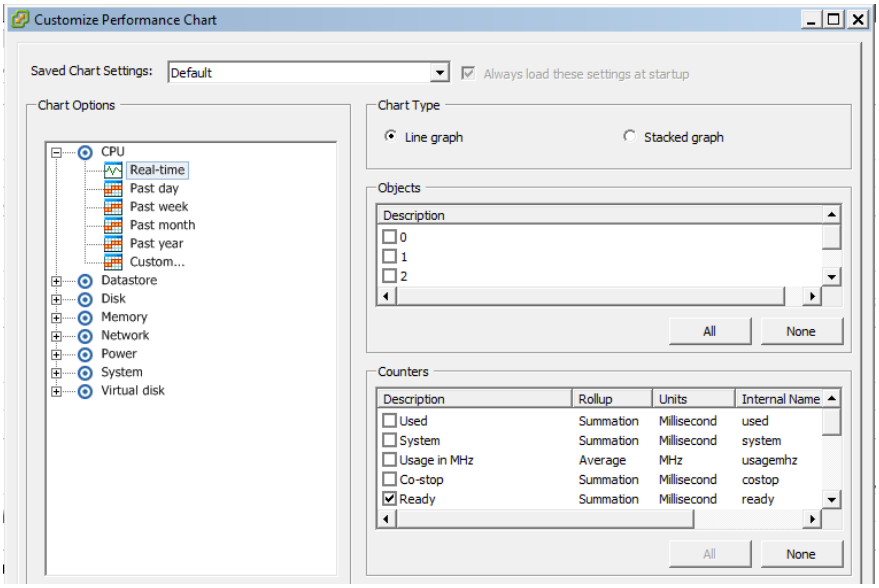
Keep in mind that periodic spikes above the threshold are acceptable. It becomes unacceptable when the average CPU Ready time is consistently over the threshold.

Accessing the CPU Ready Performance Charts for a VM

To access the performance charts to see CPU Ready Time, first go to the performance tab of a VM, then select Advanced.



Next click on Chart Options > Expand CPU > Select Real Time (or a different interval you wish) > Unselect the individual cores under Objects, leaving only the VM object selected > and select Usage (Percent) and Ready under Counters > Hit OK



This will display a chart where you can easily see CPU usage and CPU Ready time:

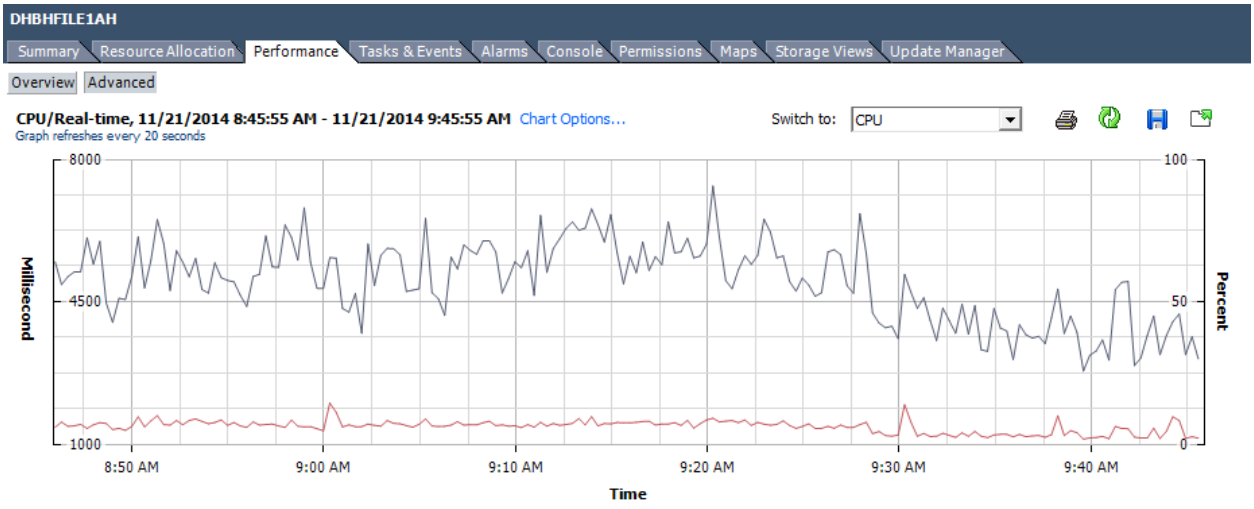
In the above screenshot, we can see that we are using the real-time performance chart, and we have an average of 170ms for CPU Ready Time which is below the 500ms / 2.5% threshold. (170/20000)*100=.85%.

CPU Ready Example

Determining if CPU Ready Time is occurring, if that the VM is negatively impacted, and if that the VM is oversized are not always as black and white as one would hope. If you are having difficulty coming to these conclusions please feel free to contact a VMware Team member for assistance in reviewing the performance charts. Below is an example of a real world scenario from vCenter to use as an example.

Example

Analysis: On the VMware Team Dashboard, DHBHFILE1AH was listed as the VM in vCenter suffering the worst from CPU Ready Time. With an average of nearly 5000ms of CPU Ready Time in the real time performance chart, this VM is experiencing 9 times the acceptable amount of Ready Time. Without even logging into the Guest OS we can know definitively that this VM is performing extremely horribly. DHBHFILE1AH has been allocated 4 vCPU with an average CPU usage across a week of only 7%. The ESXi host the VM is running on is only using 23% of its CPU resources. This would be a scenario that could be considered more black and white than normal.



Performance Chart Legend

Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
	DHBHFILE1AH	Ready	Summation	Millisecond	3090	7358	2790	4997.094
	DHBHFILE1AH	Usage	Average	Percent	1.89	14.3	1.56	5.949

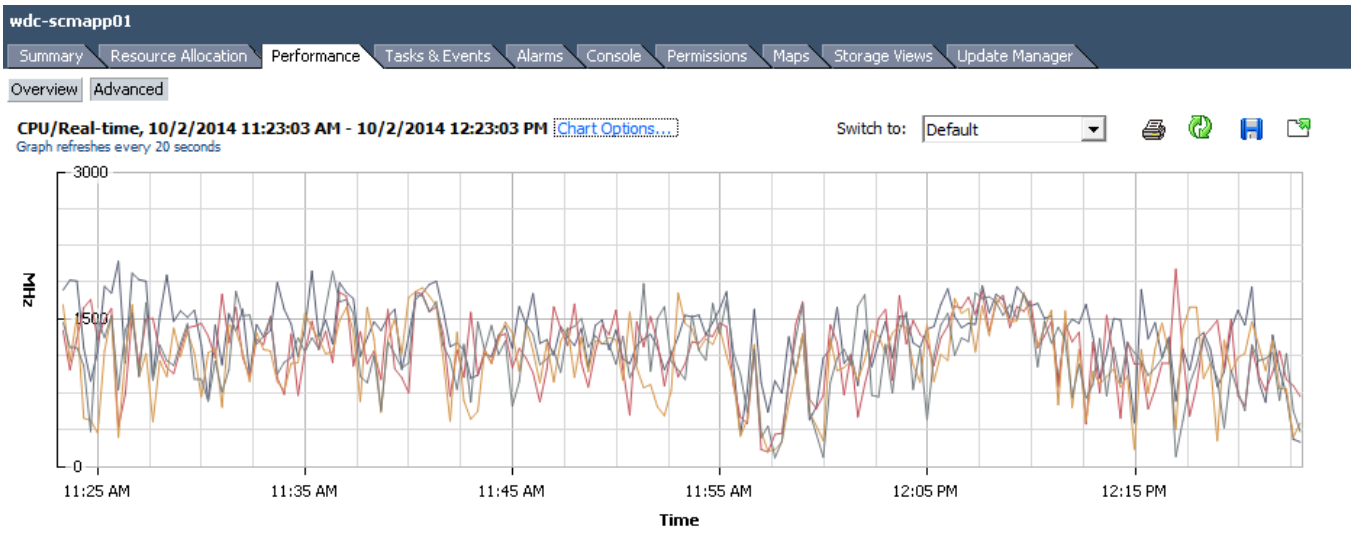
Conclusion: With the above few details we can paint an accurate picture of this situation. The ESXi host running this VM is taxed so little, the CPU usage on the VM is so low, and the CPU Ready Time is so high that we instantly know that this VM has been over allocated on vCPU resources. We also know that with a CPU Ready Time so high, this VM is making many requests for CPU that are not being serviced on the physical hardware.

A simple solution would be to drop the VM to 1 vCPU based on the usage in the above chart of an average of 6-7% and knowing that giving it a quarter of its vCPUs logically one would think it would still be able to service the 7% load, this solution would be incorrect. The utilization is so low on the VM because it cannot be serviced; therefore if the VM could be serviced by lowering the vCPU count, then ideally utilization would increase. To plan for utilization to increase and to account for current CPU Ready Time, a good recommendation for this VM would be to drop it 2 vCPUs and monitor for a weeks' time periodically, it may be possible that 1 vCPU would work but removing too many can be just a detrimental as having too many allocated. CPU utilization will increase while CPU Ready Time decreases.

Hyperthreaded Workloads and Multi Core Applications on CPU Performance Charts

Most current applications are hyperthread capable and/or able to use multiple cores to process data. It is asked quite often when performance is slow on a VM if the VM is using all of its vCPUs. We can easily determine that all vCPUs are being utilized by referencing the same performance chart options, but this time unselecting the VM object, and selecting each vCPU object, then select CPU Usage MHz and hit OK. This will display a chart where you are able to see the MHz usage of each vCPU, keep in mind,

there is no way to grant multiple vCPUs and disable certain ones for use in VMware, below you can see the utilization for each vCPU on a 4 vCPU VM:



Performance Chart Legend

Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
	0	Usage in MHz	Average	MHz	250	2096	250	1337.422
	1	Usage in MHz	Average	MHz	714	2016	149	1182.517
	2	Usage in MHz	Average	MHz	445	1824	156	1101.483
	3	Usage in MHz	Average	MHz	357	1993	89	1146.828

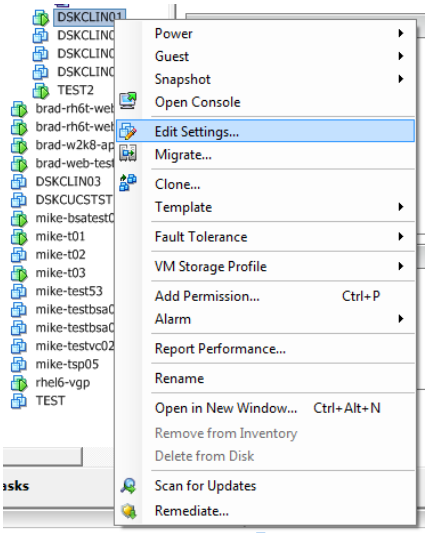
Adding vCPUs

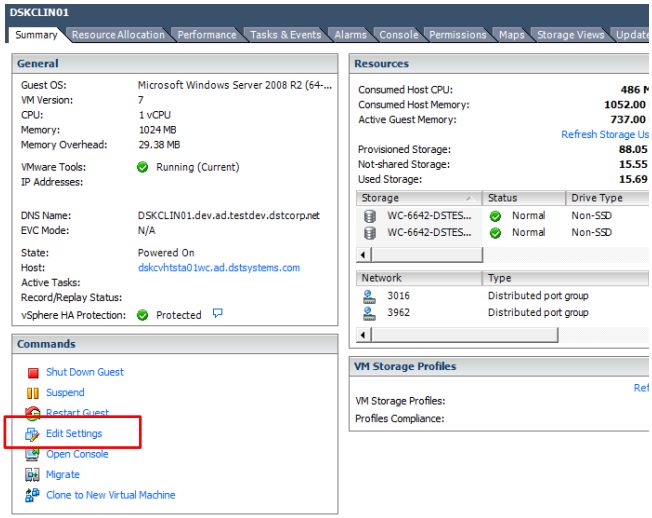
High Level Steps

1. If the CPU count will be over 4 vCPUs or you are doubling the CPU allocation, please review with a VMware Administrator.
2. Edit VM Settings
3. Select the CPU node on the Hardware Tab
4. Specify new socket count, if greyed out, the VM does not have hot add enabled.
5. Hit OK.
6. Verify Task completes in vCenter

Detailed Steps

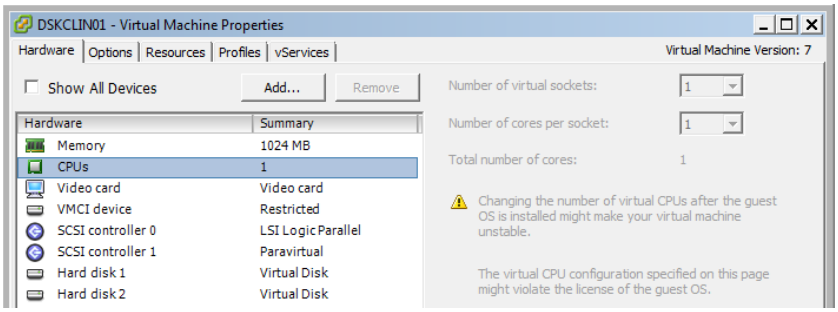
If it has been decided that additional vCPUs are to be added to a VM, this can be done by either right clicking the VM and selecting Edit Settings, or by selecting Edit Settings from the Summary tab of a VM.





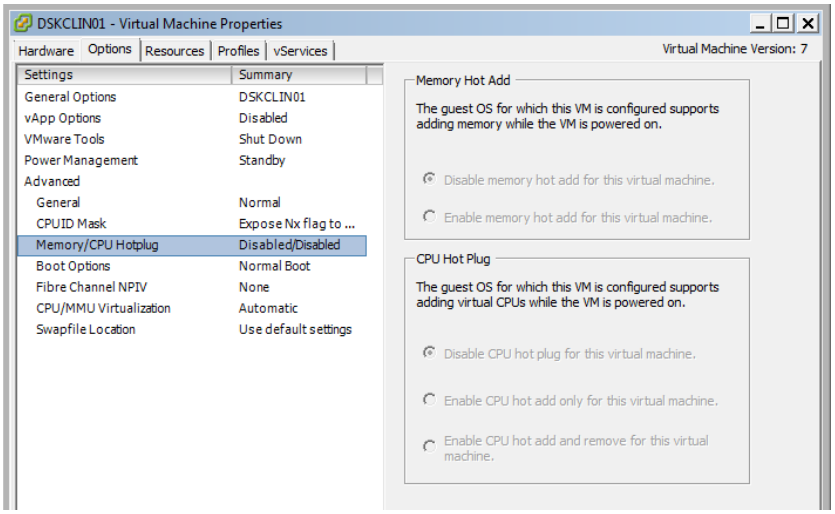
The Edit settings display box will appear, you will either be able to hot add the vCPU resources if that feature has been enabled, or you will need to Power Off the VM to add the vCPU resource if hot add is disabled.

If Hot Add is disabled, the ability to add additional CPU resources will be greyed out. Select the vCPU object in the list of hardware assets to determine if vCPUs can be hot added if the VM is powered on, if the VM is powered off, vCPUs can always be added:



To add vCPUs, select the CPUs object and increase the CPU count on the right side by either using the Up arrow or by typing a new value in the text box for Virtual Sockets. When adding vCPUs hot to a VM the only available option to change is the Virtual Sockets count, this is important to keep in mind. If you increase the socket count and the core count is unchangeable, this means that whatever the core count is will be applied to all sockets which in some circumstances can leave you with a vCPU core count that doesn't match the amount you were attempting to change to. For example if a VM has 1 Socket and 2 cores and 1vCPU needs to be added to total 3 vCPUs and adding sockets is the only option, increasing to 4 vCPUs instead of three will be the only option if the VM is powered on. If the cores to socket ratios ever creates this scenario, the VM will need to be powered down to add the appropriate number of vCPUs, in the example used above, changing the sockets to 3 and the cores to 1 when the VM is powered down is the only way to accomplish a 3 vCPU configuration.

To verify Hot Add is enabled for both CPU and Memory, you can navigate to the Options tab under the Edit Settings display and click on Memory/CPU Hotplug, this setting is stored in the VMX file, as are many of the other options under the Edit Settings display.



vCPU: Socket vs Core

When adding vCPUs to a VM be aware of your choice between adding additional sockets and the cores per socket setting. This choice is only presented in a Virtualized environment for licensing considerations. A good example is if the software being installed on a VM is licensed by sockets, we would then choose a core to socket ratio with less sockets and more cores.

Only when you begin to build VMs with larger vCPU allocations can performance potentially be affected by your cores per socket choices. The performance impact that may be felt has to do with how NUMA and Virtual NUMA are presented to the guest OS of a VM. See the below article for more details on that subject. At the time of this writing the UCS blades in use at DST have 2 sockets and between 8-12 cores each socket with only two NUMA nodes (1 per socket). NUMA considerations only need to be taken into account when a VM has greater than 1 NUMA node's allocation of cores and the VM will need to cross NUMA boundaries. Odd number vCPU allocations have no negative performance impact outside of NUMA considerations, vCPU alterations do not always need to occur in even numbers or by twos.

http://blogs.vmware.com/vsphere/2013/10/does-corespersocket-affect-performance.html

Limits on adding vCPUs before engaging the VMware Team

Please engage the VMware team when adding vCPUs will create a total of 4 vCPUs or greater on a VM. Always feel free to contact the VMware team to help analyze the performance charts and assist with determining if vCPUs are needed and a request should be fulfilled as is. Average VM vCPU Allocation at DST: 2 (90% of VMs have 2 vCPUs or less)

Memory

Memory Virtualization

When memory is virtualized, the hypervisor (ESXi) is able to present all VMs a contiguous physical memory space. Whether that memory is contiguous on the physical memory banks is not known to the VM, but the VM always believes it is so. This contiguous virtualized memory is important for Virtual machine integrity and also Virtual Machine security. By placing zero-based memory pages in a virtualized physical memory space to a VM, the host is also able to mark those claimed memory pages on the physical memory as allocated therefore denying access to the same memory pages in use to another VM.

The physical to virtual machine memory page mappings are maintained in a shadow page which is kept up-to-date by the VMM. This shadow page is used directly by the processors paging system.

Memory Allocation and Over Commitment

Determinations on whether CPU and Memory resources should be altered on a Virtual Machine should only be made with the assistance of member of the Enterprise Services VMware team, which includes reviewing VM performance in comparison to Guest level performance statistics. Although many individuals will have access to alter VM resources this should only be done once a performance review has been completed with a qualified individual. After the review, any number of people can then be instructed to add or remove the decided upon resources. If you are not qualified to determine VM resources or if a request has come in from a business unit to add resources, do not perform resource change operations without having a proper performance review with the VMware Team and without being instructed to do so.

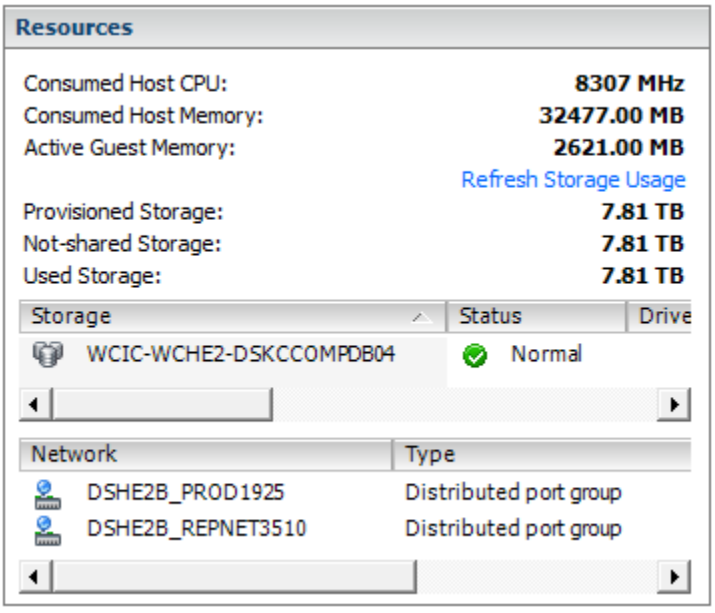
By default, memory allocated to a VM can be considered "Thin Provisioned" (to use a storage term). For example, a VM can be allocated 12GBs of memory but it will truly only use what is needed regardless of the allotment. This allows ESXi hosts to be over allocated on memory. When issues could arise is when hosts are too over allocated and when many VMs that normally don't use all of their memory need more of their allocated memory. Although not a likely scenario, this is a concern that needs to be considered. Ideally there is enough physical memory in a cluster so that there is no memory over commitment. At the time of this writing only 4 Clusters of 40 in the ES VMware environment have any memory over commitment with additional capacity in the works, the goal is to have no over commitment at all.

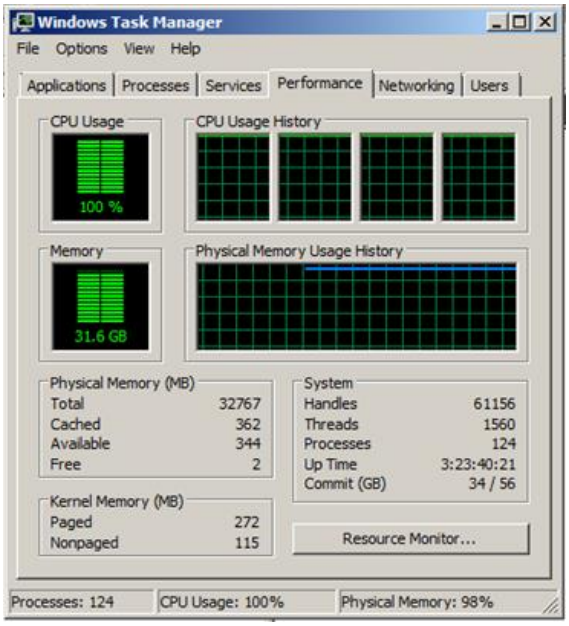
Memory Performance

VMware Memory Performance Counters

https://www.vmware.com/support/developer/vc-sdk/visdk41pubs/ApiReference/memory_counters.html

Example Memory Performance Stats





Active Memory

The amount of physical memory the Virtual Machine is using based on touched memory pages that the VMkernel has tracked. This is a measurement of only the pages of memory that are being requested and given back to the hypervisor actively. When applications are in use that manage their own memory (i.e. SQL Server, JVMs, Oracle, Etc.), the active memory metric should not be relied upon and instead the Consumed Host Memory metric should be used in conjunction with guest OS memory metrics. When applications manage their own memory they handle memory page releases and allocations internally therefore the hypervisor does not know truly how many pages are actively used therefore it must make a best estimate based on certain factors. Active memory is the hypervisors best estimate on how much memory of the memory allocated is actually being used by the Guest OS based on the pages of memory requested and released.

The screen captures under the example section above are of the Resource section on the Summary tab of a Virtual Machine and the Performance monitor in the guest OS of a VM running SQL Server. This VM is allocated 32GB of RAM and within the guest OS 30GBs are allocated to the SQL Server instance leaving 2 for the OS. Notice how different the memory usage is between the VM Active Memory metric of 2621MBs and the usage within the guest OS which is at 32GBs. This is a perfect example of when the Consumed Host Memory or Consumed Memory metrics should be used as they reflect that the ESXi host has allocated 32GBs of RAM to that VM which cannot be shared with other VM.

http://blogs.vmware.com/vsphere/2013/10/understanding-vsphere-active-memory.html

Consumed Memory

Consumed Memory is the amount of Host physical memory consumed by the virtual machine for guest memory. Consumed memory does not include overhead memory. It includes shared memory and memory that might be reserved. Using this metric is valuable in most all cases as it is more accurate in a wider breadth of use cases but it needs to be understood that if you calculated Consumed Memory for all VMs on a ESXi host there is potential that the total of that number could be greater than what is actually available on the ESXi host.

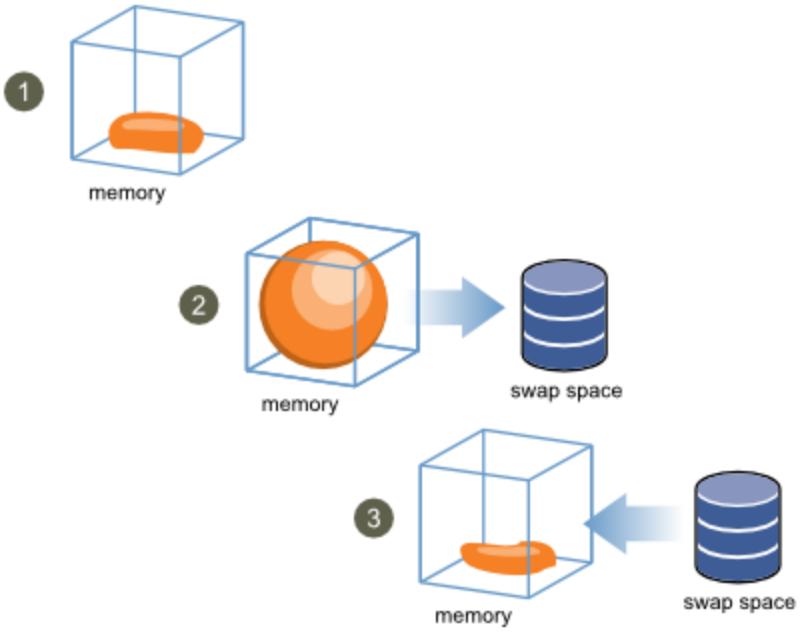
This is because the Consumed Memory includes in its calculations the amount of memory used regardless if the VM is participating in TPS and Reserved memory. A combination and analysis of the Active Memory, Consumed Memory, and Guest OS Memory metrics is the proper way to validate memory allocation and usage on a VM. Consumed Host Memory is the metric that would be used for chargeback purposes.

Balloon Driver

The memory balloon driver (vmmemctl) collaborates with the guest to reclaim memory pages that are considered least valuable by the guest operating system. The driver uses a proprietary ballooning technique that provides predictable performance that closely matches the behavior of a native system under similar memory constraints. The Balloon driver increases or decreases memory pressure on the guest operating system causing the guest to use its own native memory management algorithms to relieve system stress. When memory is tight, the guest operating system determines which pages to reclaim and, if necessary, swaps them to its own virtual disks.

The balloon driver is only available to VMs where VMware tools is installed, this functionality is one of the most crucial reasons to have VMware Tools installed on all guests. By increasing memory pressure by inflating the balloon driver within the guest OS, thus occupying more memory, the guest OS is forced to release the least important pages of memory to release stress. After inflation and Guest Release, the Balloon driver is deflated allowing the guest to then move swapped memory back into physical memory if needed. Inflation occurs for the duration of memory contention and stress within the guest OS.

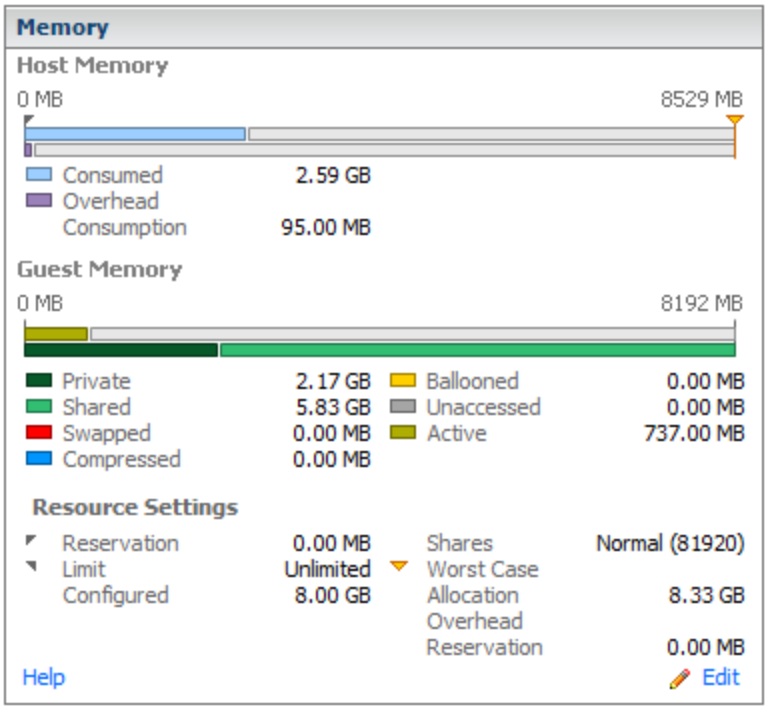
Memory Ballooning is available to assist with Guest OS memory stress and contention, ballooning is something that ideally never occurs, but when it does, it identifies one of two things; 1. Either the VM does not have enough memory allocated or 2. The ESXi host running the VM is being taxed. In either scenario if ballooning is occurring then VM performance is impacted negatively.



http://www.vmware.com/files/pdf/mem_mgmt_perf_vsphere5.pdf

Transparent Page Sharing

TPS is a memory reclamation technique used by ESXi that allows redundant copies of memory pages to be eliminated across any number of Virtual Machines. For example if there are 50 VMs with RHEL as the guest and they have same software packages installed, then the Hypervisor can recognize pages of memory that are identical, it will then create a hash mapping of those pages. At this point ESXi eliminates the redundant pages of non-changing memory and point all 50 VMs to those particular shared pages using the hash maps, thus allowing ESXi to reclaim those redundant pages and can use them to fill other needs. To see if a Virtual Machine is benefiting from TPS you can navigate the Resource Allocation tab for a VM and note the “Shared” metric under the Memory Section. Notice in the screen capture below that the VM is utilizing 5.83GBs of its memory from redundant TPS pages of memory. TPS can occur at any time but ESXi will look to this option as a means of relieving memory pressure on itself if it is low on resources also. A vulnerability was discovered in October 2014 where in very defined and staged circumstances a malicious individual could read the data held in the shared pages of memory between VMs, the circumstances are very unlikely. If a malicious attacker could perform the tasks to get into the system where they could execute this vulnerability, much bigger issues are at hand than reading memory pages for a VM. Because of this vulnerability TPS will be disabled by default in the next release of vSphere/ESXi, it was thought that for years that TPS could not be broken or exposed.



http://www.vmware.com/files/pdf/mem_mgmt_perf_vsphere5.pdf

Swapping

Memory Swapping is paging at the Hypervisor level. Just as guest memory paging is poor for performance swapping is also. Swapping additionally points to the fact that the ESXi host is not simply strained but is taking drastic steps to "stay alive".

Each VM that is powered on has a swap file which is equal to the size of the memory the VM is allocated, by default the swap file is stored in the same directory as the Virtual Machine files on a designated Datastore, see Virtual Machines File Types section for an example.

The Swap file is created at VM power on, this is important to know being that the more VMs stored on a Datastore the more swap space will be created. The swap file is only used during times of great contention for an ESXi host. If needed, the ESXi host will swap Virtual machine memory out of RAM and onto the Datastore via the swap file, a glorified paging system. Any swapping can be seen in the Memory section of the Resource Allocation tab for a Virtual machine and is extremely bad for performance.

http://www.vmware.com/files/pdf/mem_mgmt_perf_vsphere5.pdf

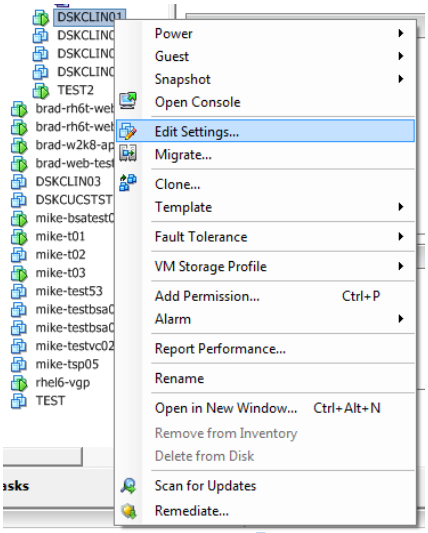
Adding Memory

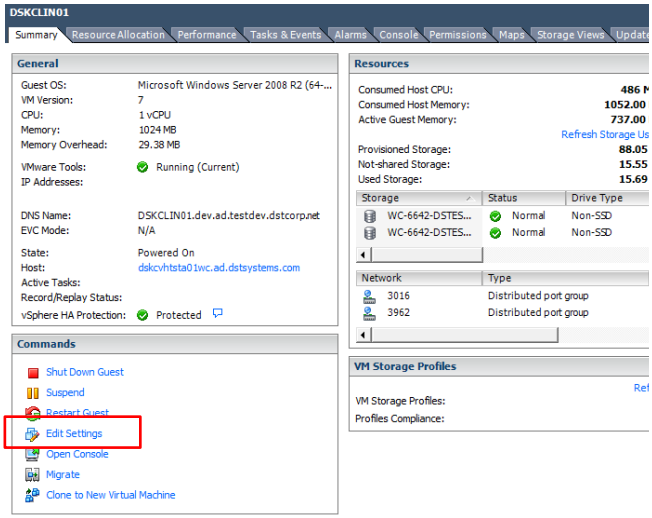
High Level Steps

1. If the memory will be over 10GB or you are doubling the memory allocation, please review with a VMware Administrator.
2. Edit VM Settings
3. Select the Memory node on the Hardware Tab
4. Specify new Memory amount, if greyed out, the VM does not have hot add enabled.
5. Hit OK.
6. Verify Task completes in vCenter

Detailed Steps

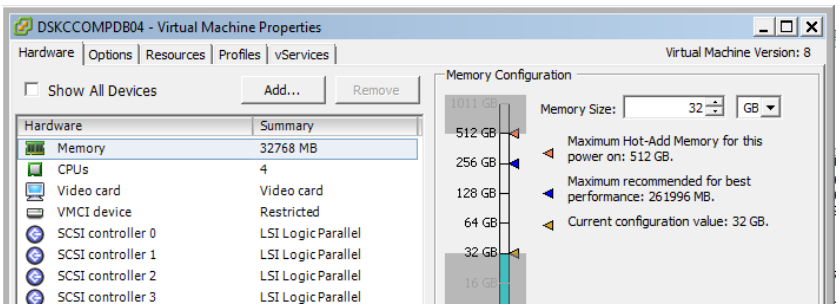
If it has been decided that additional Memory should be added to a VM, this can be done by either right clicking the VM and selecting Edit Settings, or by selecting Edit Settings from the Summary tab of a VM.





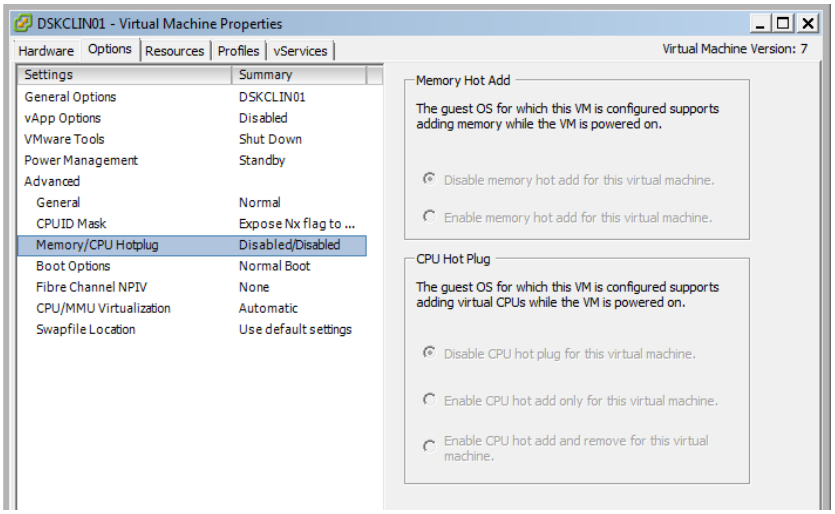
The Edit settings display box will appear, you will either be able to hot add the Memory if that feature has been enabled, or you will need to Power Off the VM to add the Memory if hot add is disabled.

If Hot Add is disabled, the ability to add additional Memory resources will be greyed out. To verify, select the Memory object in the list of hardware assets to determine if Memory can be hot added if the VM is powered on, if the VM is powered off, Memory can always be added:



To add Memory, select the memory object and increase the Memory Size on the right side by either using the Up arrow or by typing a new value in the text box.

To verify Hot add is enabled for both CPU and Memory, you can navigate to the Options tab under the Edit Settings display and click on Memory/CPU Hotplug, this setting is stored in the VMX file, as are many of the other options under the Edit Settings display.

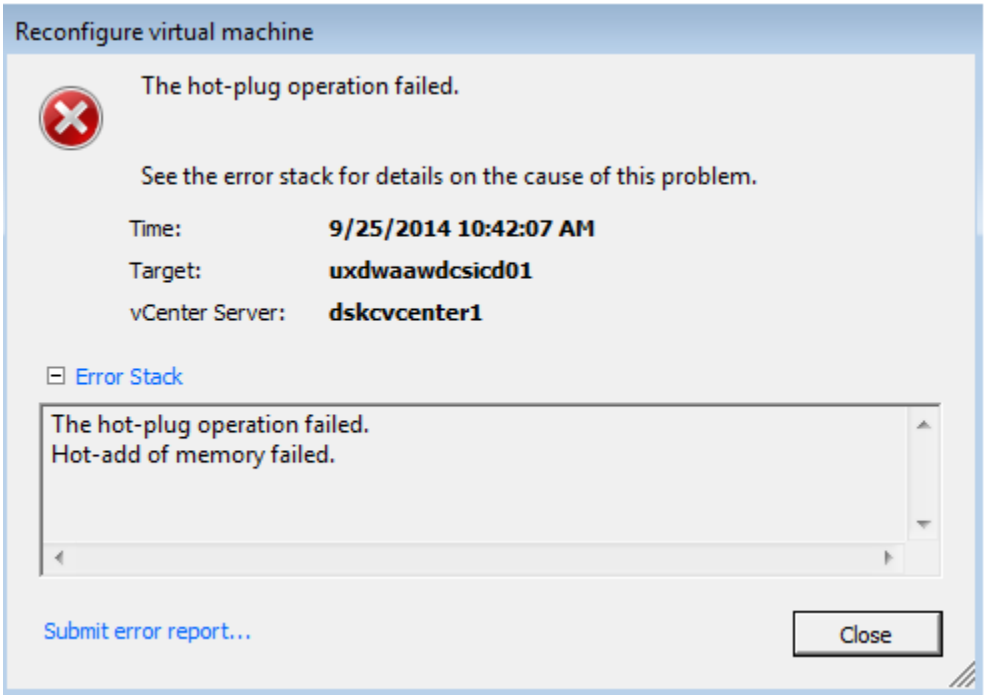


Limits on adding Memory before engaging the VMware Team

Please engage the VMware team when adding Memory will create a total of 10GBs or greater on a VM. Always feel free to contact the VMware team to help analyze the performance charts and assist with determining if Memory is needed and a request should be fulfilled as is. Average VM Memory Allocation at DST: 5GB.

Hot Add Failures

If the below message is ever received, contact a VMware admin as the VM most likely need to be relocated to a different ESXi host. The below error deals with FSR and Shadow Copy, when hot add is used to increase resources a shadow copy of the VM is created which must have allocated the exact amount of resources the parent VM has plus the additional capacity attempting to be added. When those resources cannot be allocated because of ESXi host over commitment, this error is displayed. Keep in mind the shadow copy tasks are all transparent to the user and happen in milliseconds. The VMware admin can move the VM to a new host with more free resources at which point the resources can be added to the VM.



Virtual Machine Shares

Shares specify the relative importance of a virtual machine (or resource pool). If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for said resources.

The relative priority represented by each share changes when a new virtual machine is powered on. This affects all virtual machines in the same resource pool. If all of the virtual machines have the same number of virtual CPUs, consider the following examples.

Shares can be assigned as Low, Medium or High which equates to a 1:2:4 ratio, it can also be read that a VM with shares set to medium is twice as “important” as a VM set to Low shares, and a VM with shares set to High is four times as important as a low share VM or twice as important as a Medium share VM.

For Example:

- Two CPU-bound virtual machines run on a host with 8GHz of aggregate CPU capacity. Their CPU shares are set to Normal and get 4GHz each.
- A third CPU-bound virtual machine is powered on. Its CPU shares value is set to High which means it should have twice as many shares as the machines set to Normal. The new virtual machine receives 4GHz and the two other machines get only 2GHz each.

Increasing or decreasing Shares should never be done by anyone outside of the VMware team as they are in limited use and are not a standard practice at DST, these situations must be evaluated by the VMware team. Virtual Machine Shares are periodically audited by the VMware team.

Virtual Machine Reservations

A reservation specifies the guaranteed minimum allocation of a resource for a virtual machine.

vCenter Server or ESXi allows you to power on a virtual machine only if there are enough unreserved resources to satisfy the reservation of the virtual machine. The server guarantees that amount even when the physical server is heavily loaded. The reservation is expressed in concrete units (megahertz or megabytes).

For example, assume you have 2GHz available and specify a reservation of 1GHz for VM1 and 1GHz for VM2. Now each virtual machine is guaranteed to get 1GHz if it needs it. However, if VM1 is using only 500MHz, VM2 can use 1.5GHz.

A server can allocate more than the reservation to a virtual machine, but never allocates more than the limit, even if there are unused resources on the system

When specifying the reservations for virtual machines, do not commit all resources (plan to leave at least 10% unreserved). As you move closer to fully reserving all capacity in the system, it becomes increasingly difficult to make changes to reservations and to the resource pool hierarchy without violating admission control. In a DRS-enabled cluster, reservations that fully commit the capacity of the cluster or of individual hosts in the cluster can prevent DRS from migrating virtual machines between hosts.

Unless there is resource contention on the ESXi hosts, reservations take no affect but setting a reservation removes the reserved amount of resources from the shared pool available to other VMs. If a VM with a reservation needs to be restarted on another ESXi host because an HA event was triggered and there are not enough ESXi host resources to meet the entire reservation then the VM will not be powered on when attempting to failover. This is an example of how inflexible reservations are.

When in a virtualization scenario and resources are being shared to virtual Machines by the hypervisor, there is the ability to over commit resources. Reservations are available to assist in guaranteeing resources to a VM when host resources have been over committed and VMs begin to contend for resources but without hypervisor level contention, reservations are mute.

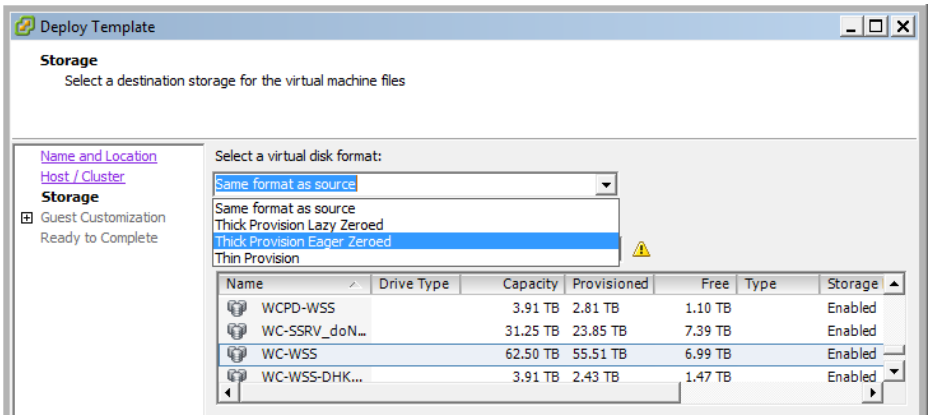
Reservations should never be set by anyone outside of the VMware team as they are in limited use and are not a standard practice at DST, these situations must be evaluated by the VMware team. Virtual Machine Reservations are periodically audited by the VMware team.

Disk Provision Types

Note: Disk formatting types can be changed at any time through the use of Storage vMotion, contact a VMware administrator if this needs to be done for any particular reason.

Note: When deploying a VM from a Template, or by cloning, the VM will be created with the same disk formatting as the source by default (Same format as source), this can be altered by specifying the desired formatting during VM deployment (discussed later in

this document), it is never a bad idea to be in the habit of always manually specifying the storage format for a VM you are deploying by any method.



Thin Provisioned

VMDK Format	Space Dedicated	Zeroed Out Blocks	Incremental Growth
Thin Provisioned	Reservation Only	As it Grows	1 VMFS Block at a time (1MB)

Thin provisioned disk are a method of defining a max size of a virtual disk or disks for a VM but the space is only actually consumed as storage is used from within the guest. If 1 hard disk 100GB in size is allocated to a Virtual Machine and the guest is installed which requires 20GBs, the VMDK (Virtual hard disk) is only occupying 20GB on the Datastore when the disks are thin provisioned. At the time of this writing the LUNs presented to the VMware team from the storage team are thin provisioned from the hardware side, therefore to not double thin provision our storage (by using both hardware thin provisioning and VMware software thin provisioning) the only area where Thin Provisioned VMDKs is the standard for disk provisioning is in HETD. Unless provisioning to HETD always choose to thick provision virtual disks. Creating Thin provisioned VMDKs is almost instantaneous. From VMware: *Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.*

Thick Provisioned Lazy Zeroed

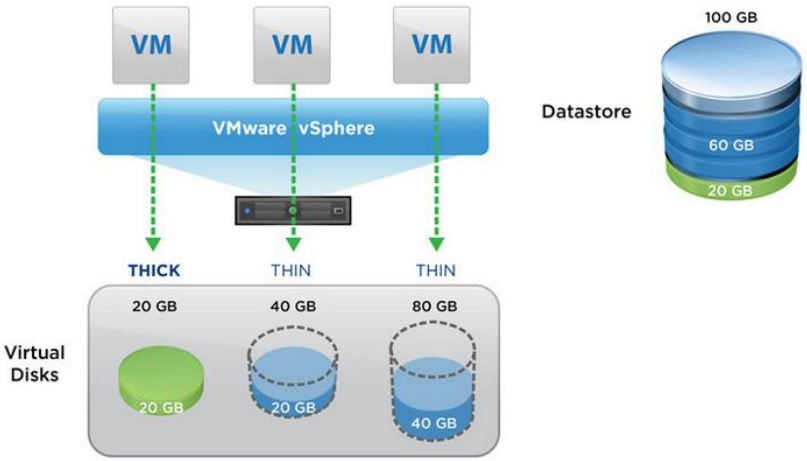
VMDK Format	Space Dedicated	Zeroed Out Blocks	Incremental Growth
Lazy Zeroed	Full Amount	As it Grows	No

Like Thin Provisioning, Lazy Zeroed disks do not write zeroes in the unused space of the virtual disk until the disk grows by usage within the guest OS. Unlike Thin provisioned disks, Lazy Zeroed disks create a marker on the physical Datastore and reserve the full amount of space that has been allocated to the VM. If 1 hard disk 100GB in size is allocated to a Virtual Machine and the guest is installed which requires 20GBs, the VMDK (Virtual hard disk) is still occupying 100GB on the Datastore when a disk is Lazy Zeroed but the Zeroes for the remainder of the disk are not written until growth. Creating Lazy Zeroed provisioned VMDKs is almost instantaneous. From VMware: *Lazy Zeroing creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. Using the default flat virtual disk format does not zero out or eliminate the possibility of recovering deleted files or restoring old data that might be present on this allocated space. You cannot convert a flat disk to a thin disk.*

Thick Provisioned Eager Zeroed

VMDK Format	Space Dedicated	Zeroed Out Blocks	Incremental Growth
Eager Zeroed	Zeroed Thick	At Creation Time	No

Unlike Thin provisioning in every way, Eager Zeroed disks both zeroes out the Virtual disk upon creation and also requires the allocated space in its entirety (like Lazy Zeroed) on the Datastore. If 1 hard disk 100GB in size is allocated to a Virtual Machine and the guest is installed which requires 20GBs, the VMDK (Virtual hard disk) is still occupying 100GB on the Datastore when a disk is Eager Zeroed. Best practice is to select this as the disk formatting option; this is also the DST default outside of HETD. Creating an Eager Zeroed VMDK is not instantaneous and can take between 10 minutes to multiple hours to create depending on the size as all blocks are zeroed out on the Virtual Disk. Most SANs, including the arrays in use at DST, can see Zeroes written to their LUNs and can reclaim them for use elsewhere until needed. By thick Provisioning using Eager Zeroed we are both protecting the VMware infrastructure by dedicating VM storage space from over committed and growth storms, we are also giving back to the physical SAN storage pool through hardware Zero page reclaim functionalities. From VMware: *Eager Zeroed is a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.*



References

About Virtual Disk Provisioning Policies

https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.storage.doc_50%2FGUID-4C0F4D73-82F2-4B81-8AA7-1DD752A8A5AC.html

Dynamic Storage Provisioning

http://www.vmware.com/files/pdf/VMware-DynamicStorageProv-WP-EN.pdf

Adding, Expanding, and Removing Virtual Disks

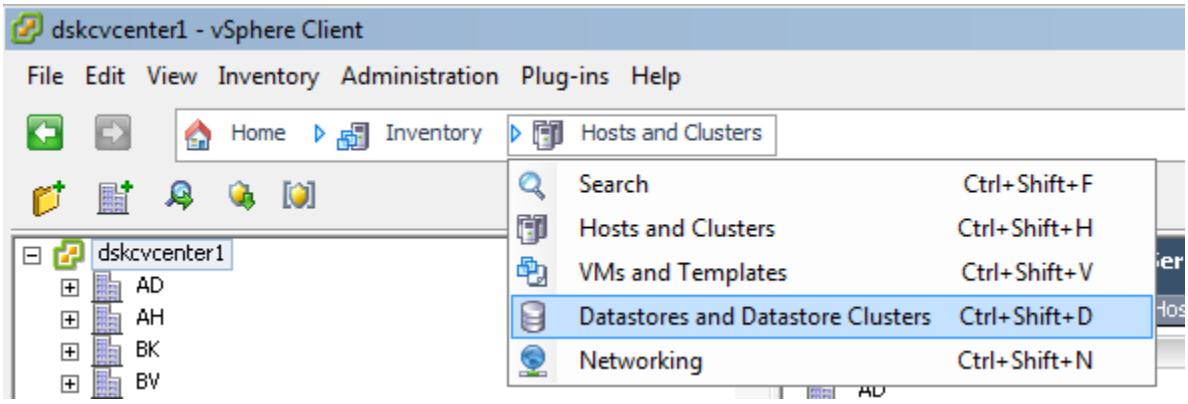
To understand and perform actions regarding Virtual Disks and their sizes it is important to understand how storage is presented to ESXi hosts and what a Datastore and Datastore Cluster are.

Datastores and Datastore Clusters

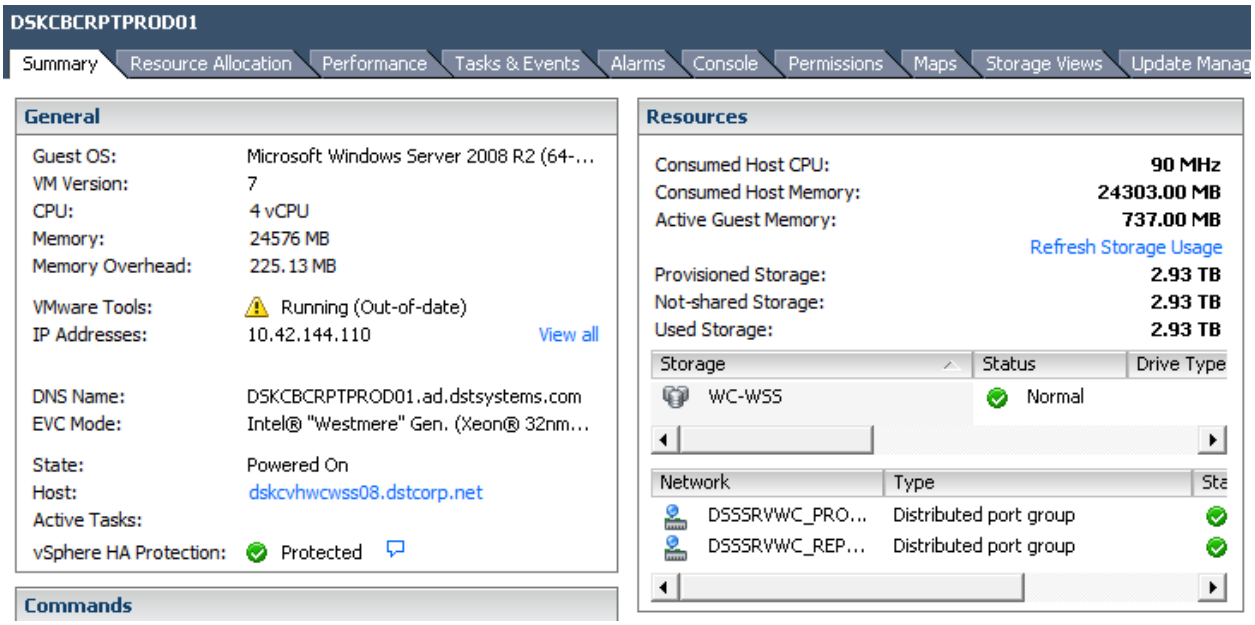
A Datastore in the DST ES VMware infrastructure is equal to 1 storage LUN presented to the ESXi hosts from a storage array. When the LUN is zoned and presented to the ESXi hosts the LUN is then brought into the environment and formatted with the VMware native file system called VMFS (Virtual Machine File System), VMFS is tuned to provide near physical performance for a shared storage Virtual Machine environment. At the moment the LUN is formatted with VMFS it is then known as a Datastore.

Just as ESXi compute hosts can be clustered together, Datastores can also be clustered together in groups known as Datastore Clusters. Unlike ESXi clusters which can be grouped together to provide fail over and HA, Datastore clusters are grouped together to even out Datastore storage usage and to protect against overly high disk latency using functionality called Storage I/O control.

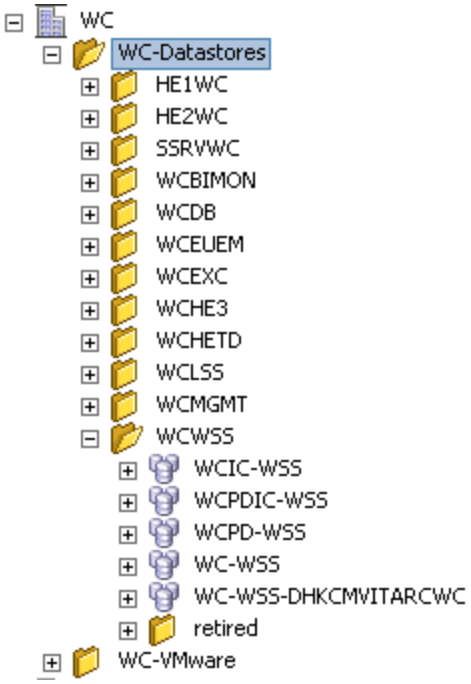
Datastores and Datastore Clusters can be viewed from many different areas, the main display for Datastores and Datastore Clusters is by using the navigation bar at the top of the vSphere client and selecting “Datastores and Datastore Clusters”. From this view you can see and navigate through all of the Datastores presented to each Datacenter in vCenter.



You can also see a Datastore and or Datastore Cluster from the Summary tab of a Virtual Machine (see screen capture below) under the Resources section, from this tab you can double click the Datastore or Cluster object for that VM which will navigate you to the Datastores and Datastore Clusters view for that selected object.



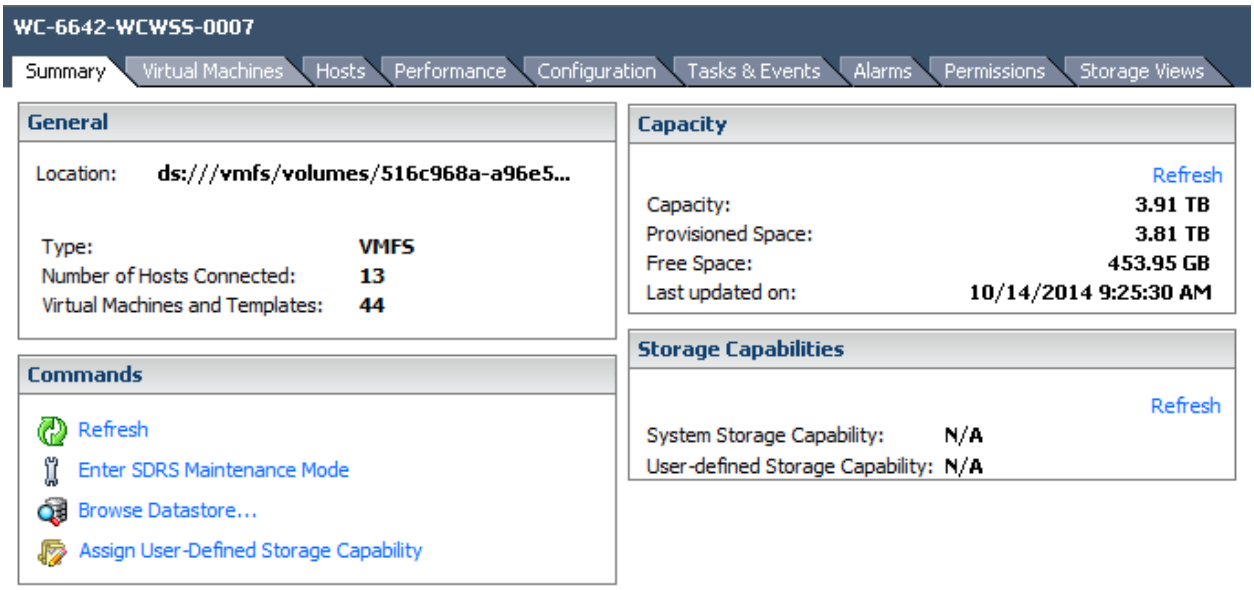
Once on the Datastores and Datastore Clusters screen, all Datastore nodes will be available to view. Simply expand a Datacenter object and drill down to which ever cluster folder you would like to view. For example, if someone wanted to view all Datastores and Clusters associated with the Windows Share Serve environment in Winchester you would navigate to the WC Datacenter object, expand out the WC-Datastores Folder then open the WCWSS folder. Under folder objects you will find either additional folders, Datastores, or Datastore Clusters, most likely either of the first two options. Under WCWSS you can see in the screen capture below that there are 5 Datastore Clusters, to see the associated Datastores for a Datastore Cluster simply expand out the Cluster object.



WC Windows Share Serve Datastore Clusters

Windows Share Serve non replicated Datastores

Selecting a Datastore or Datastore Cluster will allow to see a summary page with high level details about the object selected, just as is seen when selecting a VM object. Some items you will be able to see are Capacity, Used Space, Free Space, Number of Virtual Machines, etc.



Knowing the naming conventions of the Datastores and Datastore Clusters is crucial as use of certain Datastores and Clusters will determine if VMs are replicated and what hosts you can place a VM on. As seen in the screen shots above, Datastore Clusters follow the following standard naming format: SiteReplication-Environment-Dedication(optional), taking WCIC-WSS for example, we know that this Datastore Cluster is replicated between Winchester and BRC (WCIC) – and that it is presented to the Windows Share Serve Environment (WSS), this cluster is the general storage pool for all Windows VMs at WC in SSRV to be one site replicated to IC. Now for another example, let's look at the Cluster WC-WSS-DHKCMVITARCWC: We know that this is non replicated disk (WC, only one site listed), it is presented to Windows Share Serve (WSS) and that this Datastore Cluster is dedicated to one virtual machine (or

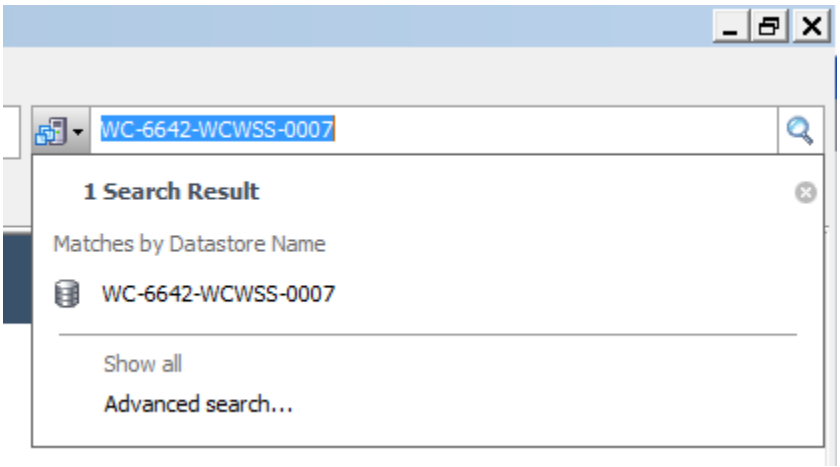
related virtual machines for certain applications or services) called DHKCMVITARCWC. Unless making changes or adding disk space to DHKCMVITARCWC, this Datastore cluster should not be used.

Individual Datastore naming conventions follow suit with Datastore Clusters but provide additional more detailed information. The Datastore naming scheme is as follows: SiteReplication-StorageArraySerialNumber-Environment-LUNLDEV. Using the Datastore/LUN WC-6642-WCWSS-0010 as an example, this Datastore is Non replicated at Winchester (WC), it is a LUN from the storage array 6642 (6642, useful information when working with the storage team), it is presented to the Windows Share Serve cluster at WC (WCWSS), and the LUNs LDEV is 0010 (useful also when working with storage team). Although this information is important to know, the OS teams will be dealing with Datastore Clusters as objects and less at the individual Datastore level unless verifying Datastore space for VM disk purposes.

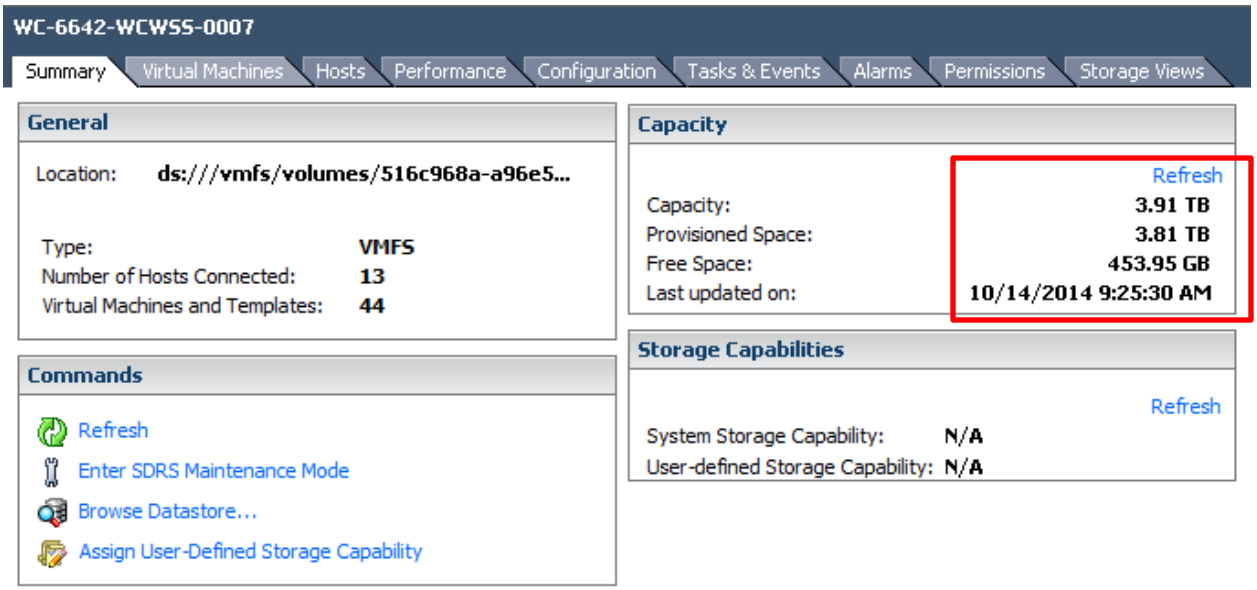
Validating Datastore Space

Validating Datastore space is crucial to running a safe environment. It is important that a VM has enough disk space to operate optimally but it is crucial that a Datastore be left with enough buffer space to account for any VM snapshots, emergency disk adds, or VM builds. When evaluating a Datastore for available space, do not drop the Free Space metric below 300GB on any Datastore. If the work you need to complete will do so and there is no other candidate Datastore to utilize, contact the VMware team for assistance as they have the ability to move VM storage around and potentially clear some free space.

To validate the Datastore space, identify the Datastore in question (this will be outlined below depending on if you are increasing a disk or adding a new disk), once you have the Datastore name, search for that Datastore using the vSphere clients search feature and navigate to that Datastores summary page.



Once on the Datastore's Summary Tab, you can easily identify the available Free Space on the Datastore by looking under the Capacity section. In the screen capture below, Datastore WC-6642-WCWSS-0007 has available free space of 453GB meaning that there is at a max 153GBs of usage space for a VM before the VMware team would need to be engaged.



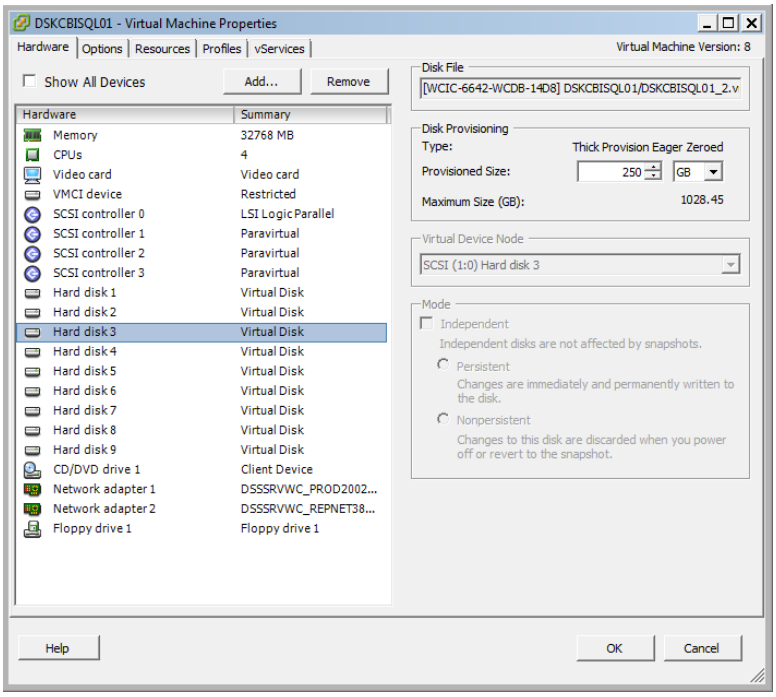
Expanding a Current Virtual Hard Disk

High Level Steps

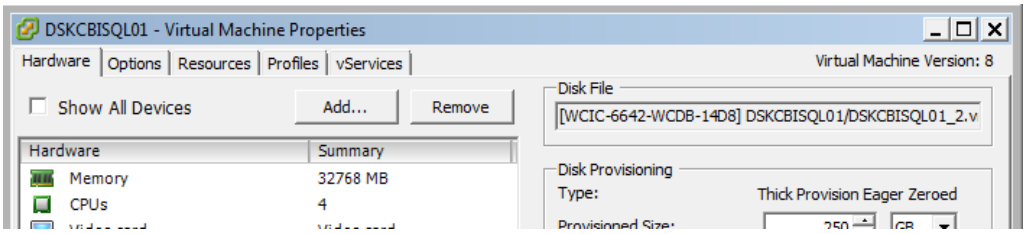
1. If expanding a disk will lower the available space of a Datastore to below 300GBs or the VM needs to be migrated to accommodate the additional space, please review with a VMware Administrator.
2. Edit VM Settings
3. Verify you have identified the correct Disk to expand, reference SCSI ID if needed.
4. Determine current Datastore the disk is on
5. Close VM Settings
6. Navigate to the determined Datastore and validate free space
7. If free space exists, navigate back to the VM Settings
8. Select again the appropriate disk
9. Increase the size on the right side
10. Hit OK
11. Verify Task completes in vCenter

Detailed Steps

To expand a current Virtual hard disk, navigate to the Virtual machine, select edit settings on that Virtual Machine and select the hard disk you wish to increase. Select the correct hard disk is many times very simple especially when dealing with VMs with only 1 to 3 hard disks of varying sizes. Trying to determine the correct hard disk to expand, on a Database VM with 10 disks, can be much more involved. If the disk you are attempting to increase is not unique in size and cannot easily be identified you will need to correlate the SCSI ID of the Hard disk from the VMware level to the OS level to verify you are expanding the correct disk. In the below screen capture you will notice how easy it is to identify the Hard disk SCSI ID, after selecting Hard disk 3, look to the right side of the Edit Settings display, verify the size the of the Hard disk matches the disk you are looking to expand and then look under the section in grey (if powered on) called “Virtual Device Node”. Hard disk 3 is on Virtual Device node 1:0, or SCSI controller 1 device 0.



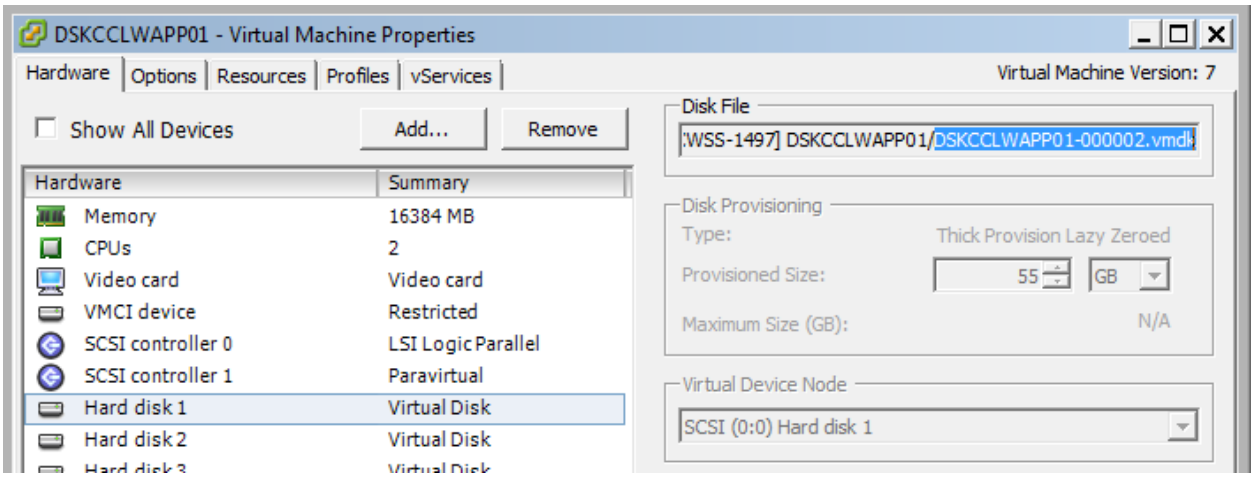
Verify within the guest that the SCSI Controller IDs match. At this point you have identified the Hard disk you wish to expand, either because you were able to simply identify the disk because so few disks are assigned to the VM or because you mapped the SCSI ID at the VM and Guest levels. Now that you know the Hard disk to expand you will then want to verify that enough space exists on the Datastore where the hard disk lives. To determine the Datastore of the particular Hard disk, because not every disk of a VM must live on the same Datastore, select the hard disk and refer to the Disk File section on the top right of the edit settings display. Referencing the screenshot above for example, Hard disk 3 for VM DSKCBISQL01 lives on Datastore WCIC-6642-WCDB-14D8 which was pulled from the beginning of the Hard disk file name in between the brackets: [**WCIC-6642-WCDB-14D8**] DSKCBISQL01/DSKCBISQL01_2.vmdk.



Now with the Datastore name, refer to the above section in this document “Validating Datastore Space” and follow the outlined steps. After validating the Datastore space and determining enough free space is available (or by contacting the VMware team to clear space if possible) the hard disk size can be increased by simply using either the up arrow or by typing in a new number in the Provisioned Size box and hitting OK. The task of applying the additional space will complete in differing amounts of time based on how much space is added, but almost all tasks for space that will be added by the OS teams will be completed within 5 -10 minutes at most. The length of time to add the additional space will also be dependent upon the Disk Provisioning state of a Hard disk, whether it is Thick Provisioned Eager Zeroed, Thick Provisioned Lazy Zeroed, or Thin Provisioned.

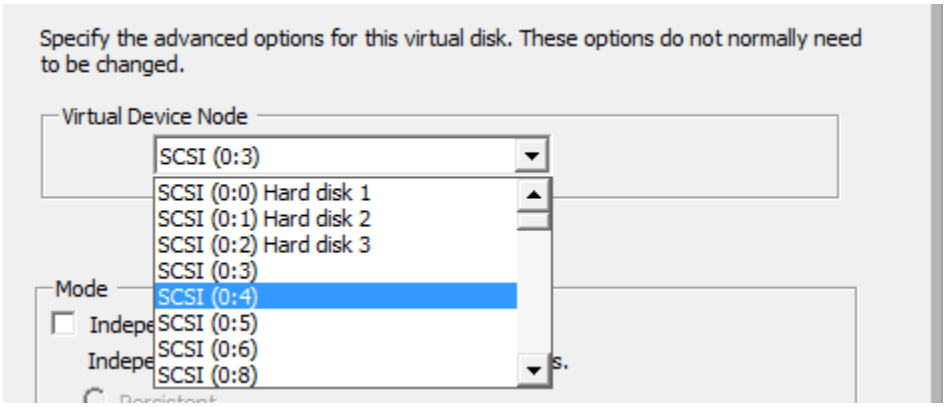
Expanding a Disk with a Snapshot

A Virtual Disk cannot be expanded when a snapshot exists. If the box to set a disk size is greyed out, most likely a snapshot exists on the VM. To identify if this is true, while the disk is selected look at the Disk File box in the top right corner of the Edit Settings menu. If you see a disk with many zeros on the tail end followed by an incremental number, the disk has a snapshot. Below is an example:



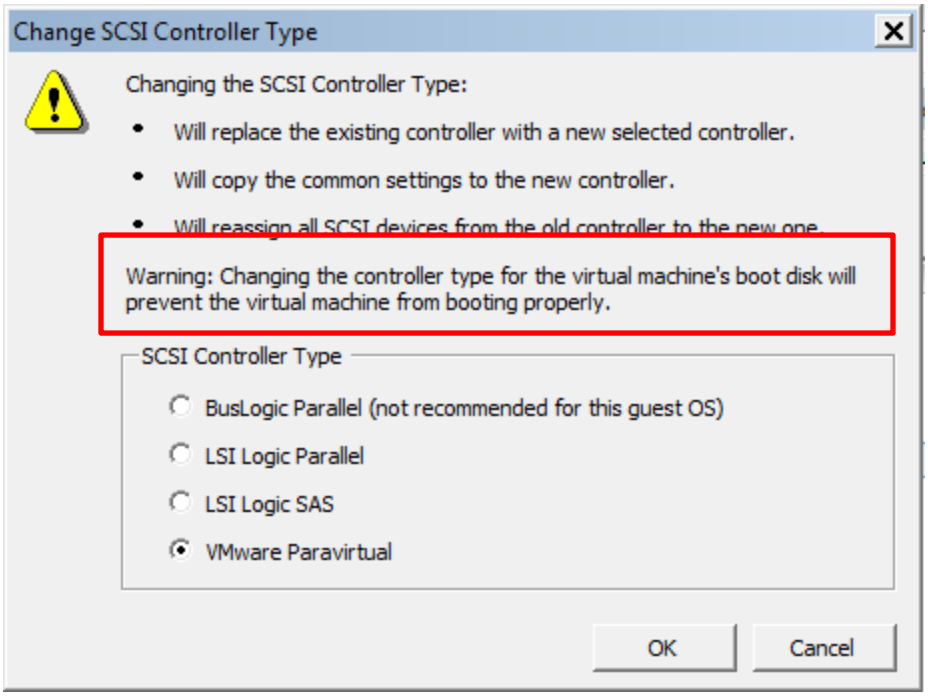
SCSI Controllers

Utilizing multiple SCSI controllers for a VM is a best practice as each controller will utilize its own device queue depth which in some circumstances can help improve VM I/O performance. A VM in vSphere 5.0 can have 4 Controllers and 15 devices (hard disks) per controller, it is best to add a controller as needed keeping in mind that most VMs in the environment have approximately 1-2 VMDKs. When a VM has 1-2 VMDKs it is acceptable to have them on 1 SCSI controller, when a third disk is added it is normal to add a second controller and place between 2-3 disks on that controller, and so on. Adding SCSI controllers can be done when a new VMDK is being added, when going through the wizard for adding a Hard disk (outlined later in this document), on the "Advanced Options" page, use the Virtual Device node drop down to select a SCSI node to place the Hard disk on. If a SCSI controller doesn't already exist for the node you are placing the Hard disk on, a controller will be added automatically and will be seen once returned to the Edit Settings screen after finishing the Add Hardware wizard. Already occupied SCSI Device nodes will show already assigned when selecting the Virtual Device node for a New Hard Disk:

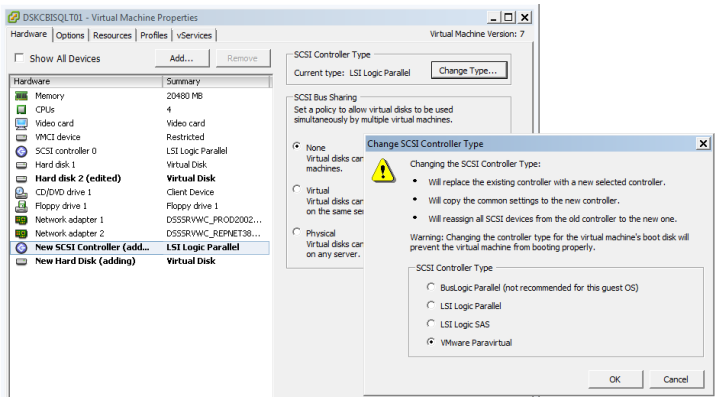


Although this can be helpful it can also be confusing in the scenario that you are adding more than 1 VMDK to a VM at a time. After the first VMDK is added if you immediately go back into the Add hardware wizard to add a second disk, when you locate the device node you want to place it on you will notice that the Device node you placed the first additional VMDK does show occupied although it is. When adding multiple VMDKs to a VM, keep track of the device nodes you have occupied so that the task doesn't fail when it tries to assign two different VMDKs to the same SCSI Device node.

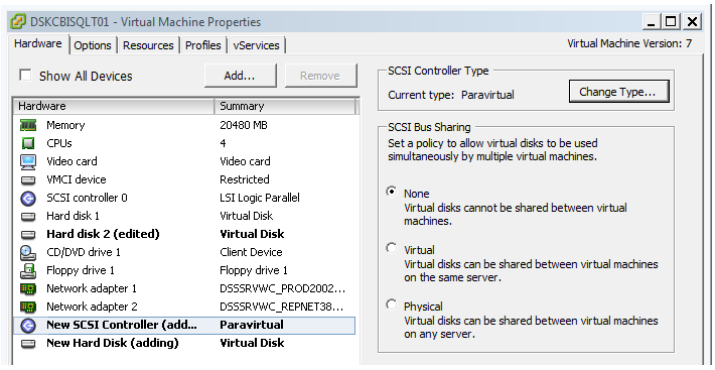
Never change the type of controller that the guest OS VMDK is using after the guest OS is installed, this will cause the VM to fail to start, see below screen shot.



When adding a new SCSI controller (which can also be added manually outside of adding a new disk by selecting an existing disk and changing its SCSI ID to a controller that does not exist), make sure you are selecting the VMware Paravirtual SCSI Controller always. This is a custom controller developed by VMware and has been shown to provide an increase in performance. No matter the method you added the SCSI controller, once you are returned to the Edit settings menu select the newly added controller and change its type by selecting Change Type in the upper right hand corner of the Edit settings menu (see Screen captures below), to Paravirtual as it is not the default.



1.Select the New SCSI Controller that has been added, select Change Type, Select VMware Paravirtual and hit OK



2. Verify the SCSI controller's type has been highlighted in bold indicating a change.

Contact a VMware Team member if you are having issues deciding how many controllers to use or which disks to place on which controllers and we can assist.

Adding a New Virtual Hard Disk

Just as expanding a Hard disk can be a simple process or a much more involved process so can the process of adding a new Virtual Disk. By default a when a new Hard disk is added to a VM the new disk is stored on the same Datastore as the VM, this is not always the desired location, we will cover both scenarios below.

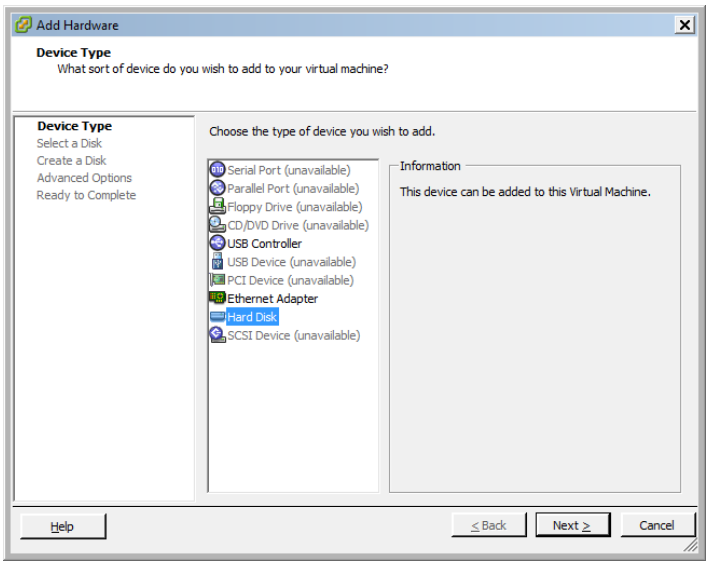
Adding a New Virtual Hard Disk Choosing Default Settings

To add a new Hard disk to a VM and place it on the same Datastore as the VM is currently located, simply navigate to the VM, select Edit Settings and click on Hard disk 1 of the VM, using the same method as outlined in "Expanding a Current Virtual Hard Disk", find

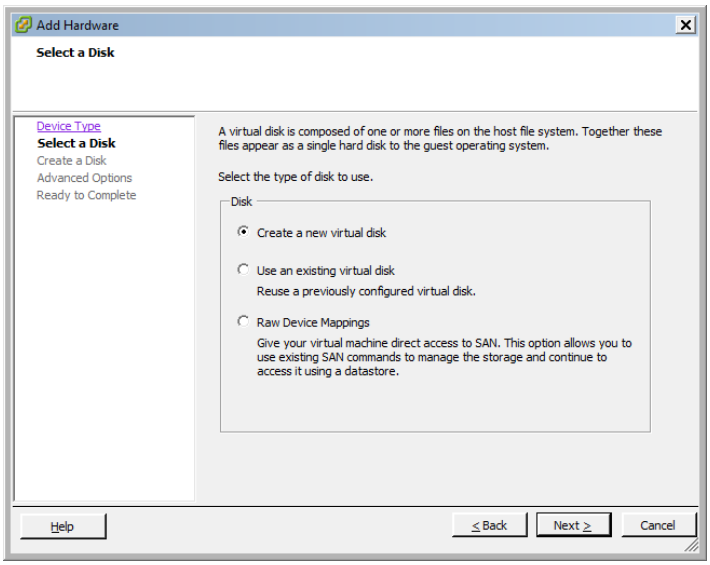
the Datastore name of the first Hard disk, then navigate to that Datastore in inventory and verify there is enough space to add the new Hard disk that is needed.

Hard disk 1 is located in the default VM directly 90% of the time which is why it is normally safe to choose it as the default location of the VM, if you are having a hard time verifying this, feel free to grab a VMware team member and we will be happy to take a look with you.

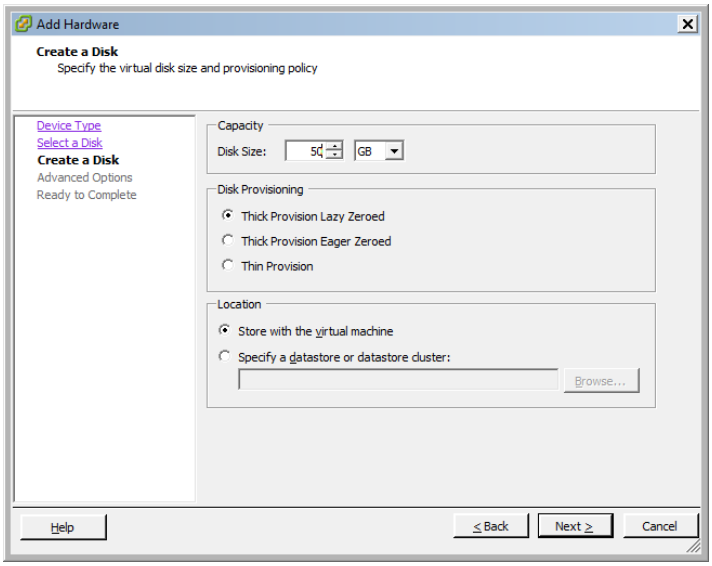
Once space is verified on the Datastore navigate back to the VM and open the Edit Settings display again, on the first screen for edit settings hit “Add...”, this will open a Menu to add a new device to a VM, all options will be available if the VM is powered off but only a select few will be available if the VM is powered on., on the next screen, on the next screen,



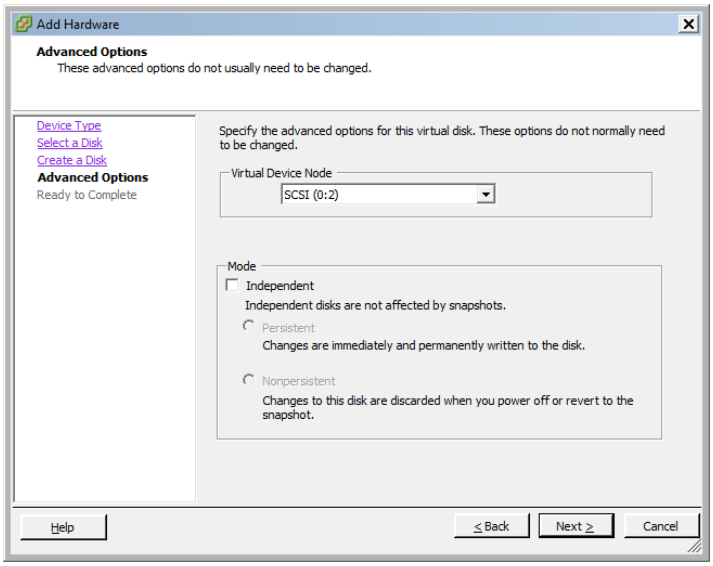
1. Select Hard Disk and hit Next



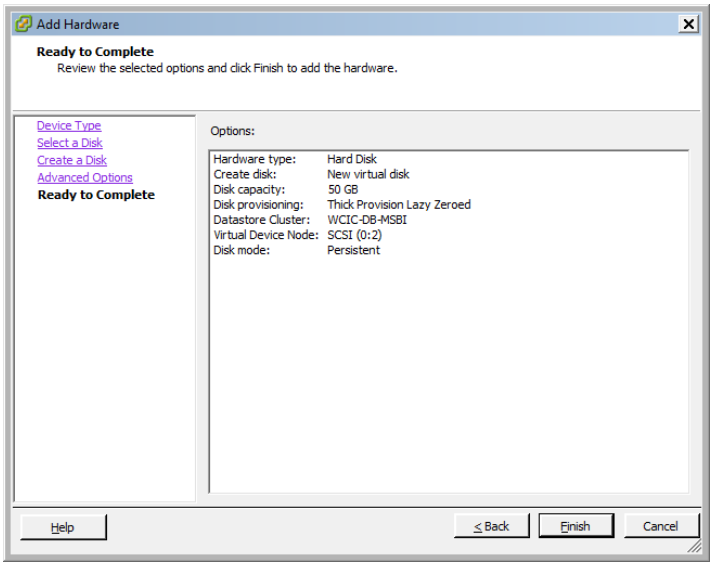
2. Select Create a New Virtual Hard Disk and hit Next



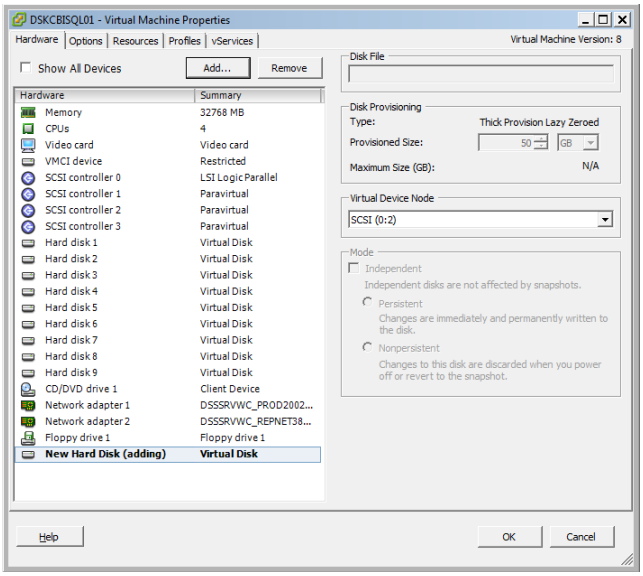
3. Specify the Hard disk size and select its Disk Provisioning type (reference the above section “Disk Provisioning Types”) also verify “Store with the virtual machine” for location is selected and hit next.



4. Determine if an additional SCSI controller should be created or determine if a different already existing SCSI controller should be used (See the above Section in this document, “SCSI Contollers”. By default the Virtual Device node selected will be the first node available. Hit next.



5. On the final screen review all of your choice and hit Finish which will close the Add Hardware display.



6. You will then see the edit settings display which will now show you the changes you are making, again if everything looks correct hit Ok and the tasks will kick off. The length of time to add the new disk will dependent upon the Disk Provisioning state of a Hard disk.

Adding a New Virtual Hard Disk by Specifying a Particular Datastore

Limits on adding Disk Space before engaging the VMware Team

Please engage the VMware team when adding Disk space will create a total of 250GBs or greater on a VM. Always feel free to contact the VMware team to help analyze disk usage and assist with determining if additional disk space is needed and a request should be fulfilled as is. Average VM Disk Allocation at DST: 250GB.

Removing a Virtual Hard Disk

The task of removing a Virtual Hard Disk should be done in conjunction with the VMware team because of the risk associated with doing so. If a disk needs to be removed from a VM, either only from a VM or deleted from disk, contact a member of the VMware Team.

Snapshots

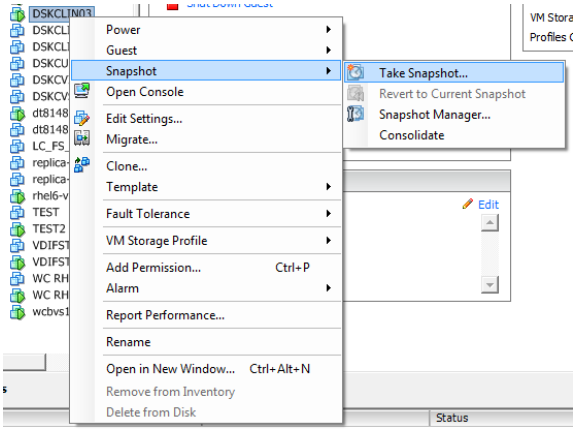
A snapshot is a marker that allows VM administrators to return to a certain point in time for a Virtual machine although changes may have been made to the system. Snapshots work by creating delta disks which become the primary target where changes are tracked, this is done in conjunction with locking the parent disk as read only. When a delta disk is in use, all changes made to blocks of data are stored in the delta files including changes to the same blocks repeated many times, this is important to know in regards to how snapshot delta disks can grow. A VM admin can create multiple snapshots but snapshot trees can become hard to manage, best practice is to live by the motto “One and Done”, meaning only use one snapshot at a time when and where possible. For every snapshot created there will be corresponding VM delta disk, managing multiple delta disks can also get tricky. The most crucial point to make about Snapshots is that a snapshot is NOT a backup and should never be treated as such. Snapshots should be used for testing patches, new software, software upgrades, and for a means of back out. Below is a list from VMware of import points and tips when dealing with snapshots:

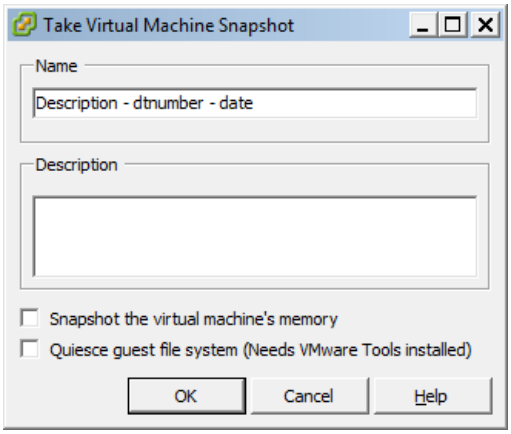
- Should be taken when testing something with unknown or potentially harmful effects.
- Is not meant to be a robust method of backup and recovery. If the files containing a virtual machine are lost, its snapshot files are also lost.

- Negatively impacts the performance of a virtual machine. This is based on how long it has been in place and how much the virtual machine and its guest operating system have changed since the time it was taken. It is not recommended to run production virtual machines off of snapshots on a permanent basis.
- Can take up as much disk space as the virtual machine itself. If multiple snapshots are possible, the amount of disk space used increases with the number of snapshots in place.
- Snapshots are not backups. A snapshot file is only a change log of the original virtual disk. Therefore, do not rely on it as a direct backup process. The virtual machine is running on the most current snapshot, not the original vmdk disk files.
- Snapshots are not complete copies of the original vmdk disk files. Taking a snapshot does not create a complete copy of the original vmdk disk file, rather it only copies the delta disks. The change log in the snapshot file combines with the original disk files to make up the current state of the virtual machine. If the base disks are deleted, the snapshot files are useless.
- Delta files can grow to the same size as the original base disk file, which is why the provisioned storage size of a virtual machine increases by an amount up to the original size of the virtual machine multiplied by the number of snapshots on the virtual machine.
- Use no single snapshot for more than 24-72 hours. Snapshots should not be maintained over long periods of time for application or Virtual Machine version control purposes.

Creating Snapshots

When a snapshot is needed, navigate to the VM in inventory and right click it, the context menu will open, navigate to Snapshot > Take Snapshot, the Take Virtual Machine Snapshot dialog box will appear:



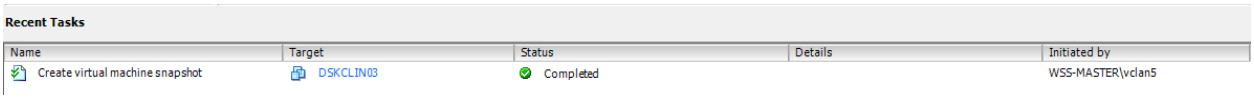


The name of the Virtual machine snapshot is the crucial portion of this menu, the description box is optional and normally not a lot of use is found for it. Please follow the snapshot naming format illustrated in the screenshot above, for example:

“Before OS Patching – dt12345 – 10-10-2014”

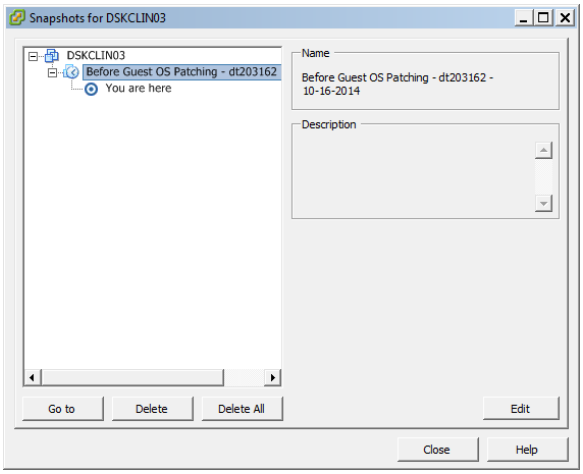
This allows everyone to know who the owner is and the date taken, two pieces of information not easily available from within vSphere standardly.

In almost all cases creating a snapshot without selecting the two optional boxes, “Snapshot the VMs memory” and “Quiescing the Guest file system”, will be the correct choice. In some circumstances Snapshotting the Virtual Machines Memory will be desirable but keep in mind that this instantly creates the snapshot that is the size of whatever data was in RAM in the guest (the .vmsn file), whereas creating a snapshot without the VMs memory will start a snapshot at 0 in size and only increase based on changes tracked. When a VM snapshot is created without Snapshotting the guest memory, if the VM admin reverts to the snapshot the VM will be in powered off state and will need to be powered on. When Snapshotting the VMs memory the VM admin can revert back to a live state with a running VM being that the data in RAM was captured and replaced when a revert occurs. When possible, use snapshots WITHOUT Guest Memory captured as they save on space and operate more reliably upon revert. After determining what options you would like selected, hit OK from with the Take Virtual Machine Snapshot dialog box and your snapshot will be created.



Managing, Navigating, and Removing Snapshots

To manage snapshots, navigate to the Snapshot Manager dialog box by navigating to the VM in inventory and right click it, the context menu will open, navigate to Snapshot > Snapshot Manager, from here you will be able to navigate to snapshot points in time, delete a snapshot, or delete all snapshots.



Go To a Snapshot

Choosing to navigate to and resume the state of a snapshot in your current snapshot tree does not delete any snapshots, only resumes the Virtual Machine to the state that you have chosen to "Go To". You can go to any snapshot in the snapshot tree to restore the virtual machine to the state of that snapshot. Virtual machines running certain kinds of workloads might take several minutes to resume responsiveness after reverting from a snapshot. Subsequent child snapshots from this point create a new branch of the snapshot tree. The delta disks for snapshots that you took after you restored the current snapshot are not removed and you can restore those snapshots at any time. Reverting to the most current snapshot (as seen when right clicking a VM > under Snapshot) will "Go To" the most recent snapshot, hence reverting the state of the VM to the most current snapshot that was taken.

Delete a Snapshot

Consolidates the snapshot data to the parent snapshot and removes the selected snapshot from the Snapshot Manager and virtual machine. Deleting a snapshot is better read as "Committing a Snapshot" as the operation is indeed Deleting the delta disk but it also applies all changes in the Delta disks to parent snapshot or in the case that the parent is the base image it removes the snapshot and commits all changes to the VM, this is irreversible.

Delete All Snapshots

Consolidates, read Commits, all of the immediate snapshots before the "You are here" current state to the base parent disk and removes all existing snapshots from the Snapshot Manager and virtual machine. In previous versions of ESXi when an administrator would delete all snapshots the snapshots, beginning with the most recent, would commit into the parent, and that task would repeat until eventually there would be one snapshot containing all changes that would be committed to the VM base disks.

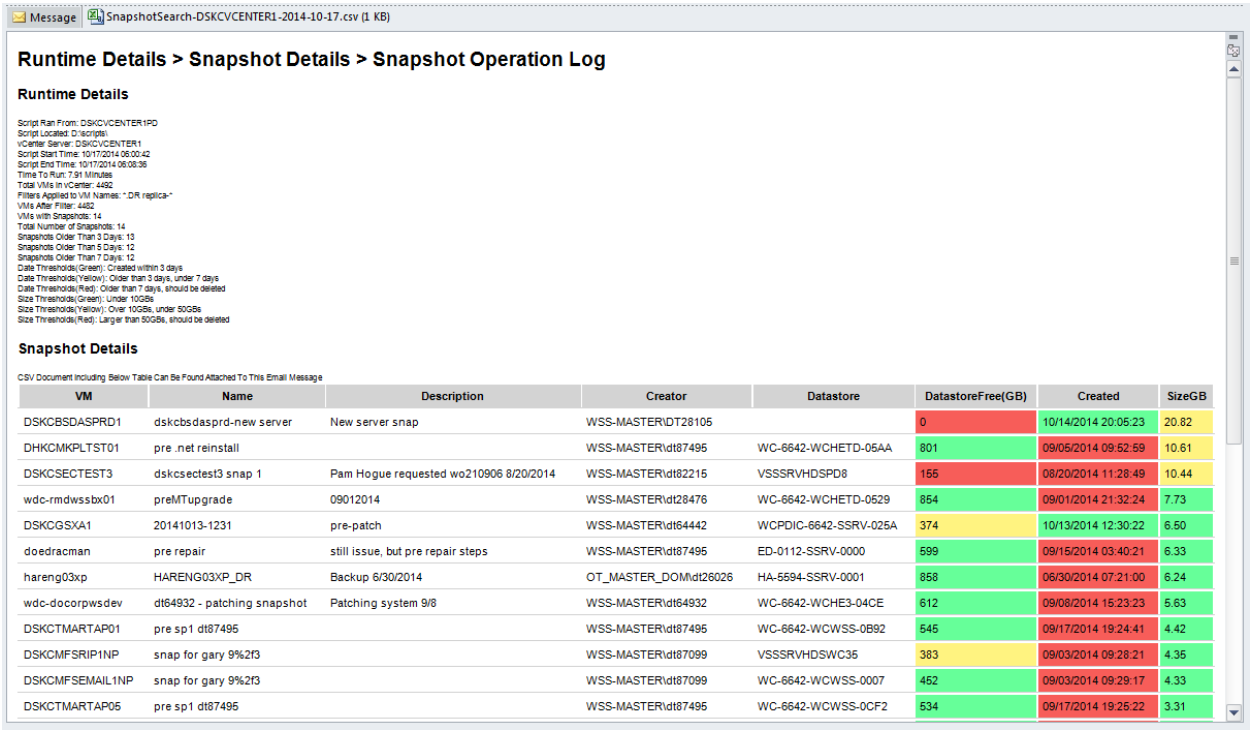
This method is the equivalent to having (x) amount of buckets of water lined up with a tub on one end, instead of pouring the water for each bucket into the tub directly, starting with the closest bucket, the bucket farthest away from the tub would be poured into the second farthest away bucket, then the second farthest away bucket would be poured into the 3 farthest away bucket, until eventually one bucket held all of the water from all buckets that would then be poured into the tub. This process was extremely slow, time consuming, and not transparent and has since changed. The Delete all functionality now starts with the oldest snapshot, commits that snap to the base disks then moves on to the next until it has cycled through all snapshots leaving none behind. When you Delete all, every change within a snapshot behind the "You are here" node will all be committed to the VM base image.

Life Span

Ideally snapshots will only exist during the time it takes to test a change and potentially a day beyond that for verification. Because snapshots are difficult to manage, particularly in an environment with 6000 VMs and especially because of how snapshots can grow to be extremely large, we ask that at a maximum you are keeping snapshots only for 1-3 days at most. There is a snapshot report sent out daily to the VMware team and weekly to the OS teams that outlines all of the snapshots in the environment, their sizes, and the space left on the Datastore they are on as one of the major concerns with snapshots is the potential it has to fill Datastores. The VMware team is reviewing the potential of automating the removal of snapshots that are past a certain date as we find that some individuals are not good stewards of snapshots they take. Keep in mind that there is a point where a snapshot that is x amount of days old is no longer even valid in the sense that if you rolled back, for example, to snapshot that is 5 days old you would need to ask yourself if this VM can handle loosing 5 days of data and how that truly would affect a client.

Sizes

The size of a Virtual machine snapshot is not easily located or presented in the vSphere client, although you can use the snapshot manager to view snapshots and navigate them, the snapshot manager does not tell you the date taken (unless specified by the user in the snapshot name) nor does it tell you the size of the snapshot. The simplest way to see the size of a snapshot you have taken is to review the Snapshot email sent out weekly from the VMware team, screen capture below:



Message SnapshotSearch-DSKCVCENTER1-2014-10-17.csv (1 KB)

Runtime Details > Snapshot Details > Snapshot Operation Log

Runtime Details

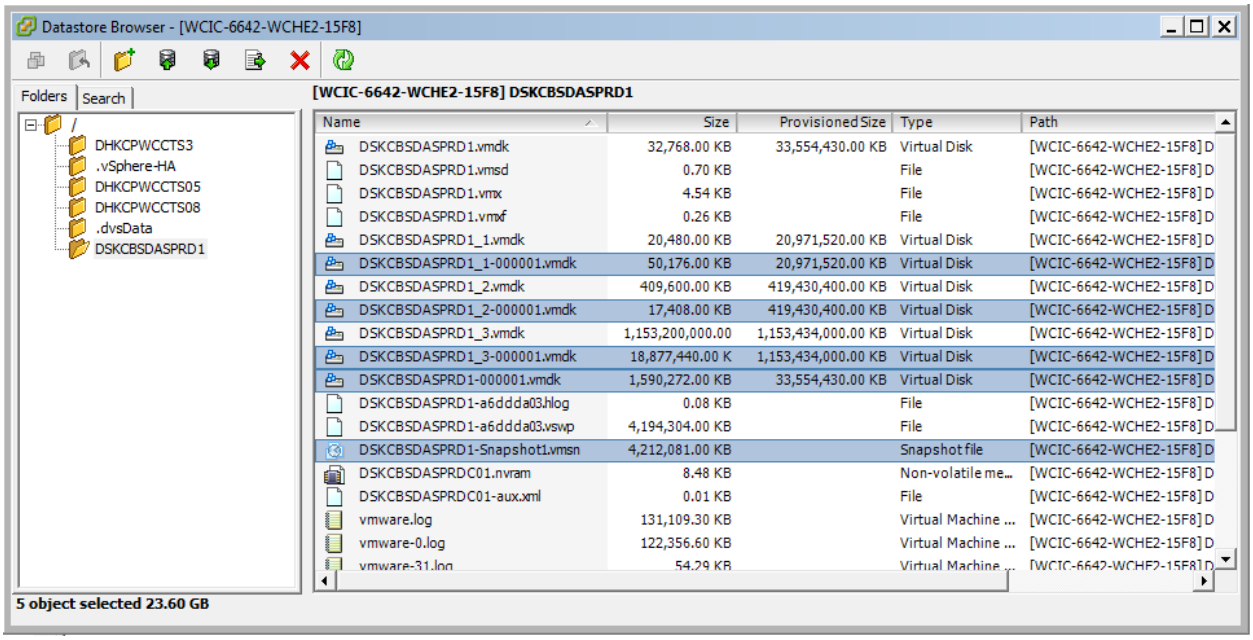
Script Ran From: DSKCVCENTER1PD
Script Located: D:\scripts\
vCenter Server: DSKCVCENTER1
Script Start Time: 10/17/2014 06:00:42
Script End Time: 10/17/2014 06:08:36
Time To Run: 7.91 Minutes
Total VMs in vCenter: 4492
Filters Applied to VM Names: *.DR replica-*
VMs After Filter: 4482
VMs with Snapshots: 14
Total Number of Snapshots: 14
Snapshots Older Than 3 Days: 13
Snapshots Older Than 5 Days: 12
Snapshots Older Than 7 Days: 12
Date Thresholds(Green): Created within 3 days
Date Thresholds(Yellow): Older than 3 days, under 7 days
Date Thresholds(Red): Older than 7 days, should be deleted
Size Thresholds(Green): Under 10GBs
Size Thresholds(Yellow): Over 10GBs, under 50GBs
Size Thresholds(Red): Larger than 50GBs, should be deleted

Snapshot Details

CSV Document Including Below Table Can Be Found Attached To This Email Message

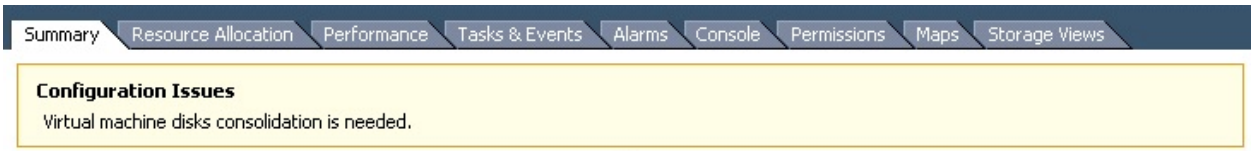
VM	Name	Description	Creator	Datastore	DatastoreFree(GB)	Created	SizeGB
DSKCBSDASPRD1	dskcbsdasprd-new server	New server snap	WSS-MASTER\DT28105		0	10/14/2014 20:05:23	20.82
DHKCMKPLTST01	pre .net reinstall		WSS-MASTER\dt87495	WC-6642-WCHETD-05AA	801	09/05/2014 09:52:59	10.61
DSKCSECTEST3	dskcsectest3 snap 1	Pam Hogue requested wo210906 8/20/2014	WSS-MASTER\dt82215	VSSSRVHDSPD8	165	08/20/2014 11:28:49	10.44
wdc-rmdwssbx01	preMTupgrade	09012014	WSS-MASTER\dt28476	WC-6642-WCHETD-0529	864	09/01/2014 21:32:24	7.73
DSKCGSXA1	20141013-1231	pre-patch	WSS-MASTER\dt64442	WCPDIC-6642-SSRV-025A	374	10/13/2014 12:30:22	6.50
doedracman	pre repair	still issue, but pre repair steps	WSS-MASTER\dt87495	ED-0112-SSRV-0000	599	09/15/2014 03:40:21	6.33
hareng03xp	HARENG03XP_DR	Backup 6/30/2014	OT_MASTER_DOM\dt26026	HA-5594-SSRV-0001	858	06/30/2014 07:21:00	6.24
wdc-docorpwsdev	dt64932 - patching snapshot	Patching system 9/8	WSS-MASTER\dt64932	WC-6642-WCHE3-04CE	612	09/08/2014 15:23:23	5.63
DSKCTMARTAP01	pre sp1 dt87495		WSS-MASTER\dt87495	WC-6642-WCWSS-0B92	545	09/17/2014 19:24:41	4.42
DSKCMFSRIP1NP	snap for gary 9%2f3		WSS-MASTER\dt87099	VSSSRVHDSWC35	383	09/03/2014 09:28:21	4.35
DSKCMFSEMAIL1NP	snap for gary 9%2f3		WSS-MASTER\dt87099	WC-6642-WCWSS-0007	452	09/03/2014 09:29:17	4.33
DSKCTMARTAP05	pre sp1 dt87495		WSS-MASTER\dt87495	WC-6642-WCWSS-0CF2	534	09/17/2014 19:25:22	3.31

Another way to determine the size of a snapshot is by navigating to the Datastore of the VM and adding together the snapshot file sizes from within the Directory of the VM. This will work 95% of the time granted all of the disks for the VM are in the same directory, or else you will be navigating to multiple Datastores and multiple directories to accomplish this. To calculate snapshot size for a VM by using the Datastore Browser, determine the Datastore of the VM (outlined earlier in this document), navigate to the Datastore, right click the Datastore and select Browse, the Browser will open, you then navigate to the VM's folder (Normally named the same thing as the VM name), then you add together the sizes of any snapshot delta disk (disks named *-000001.vmdk, the number will increment based on the number of snapshots) and the .vmsn file which will be created if you snapshotted the Guest memory also.



Disk Consolidation

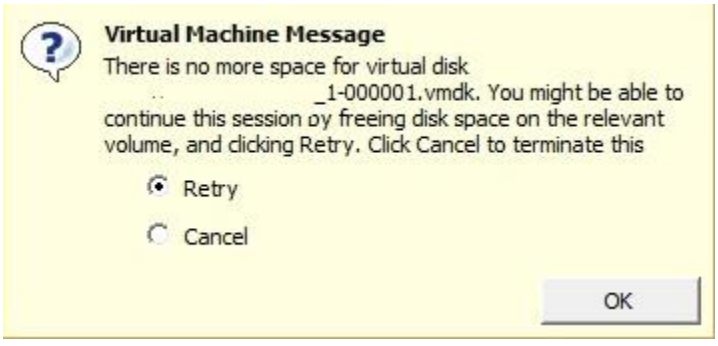
When you initiate a **Delete** or **DeleteAll** operation on snapshots, the snapshot is immediately deleted from Snapshot Manager, then the backing Virtual Machine Disk `.vmdk` files are consolidated on-disk. If the consolidation fails, some Virtual Disk files may remain on disk and/or be actively used on the Datastore, consuming storage capacity.



If a Virtual Machine requires disk consolidation because of a failed snapshot clean up, the process is simple but should be executed by a VMware admin. Consolidation goes through the same steps as removing a Snapshot which is to commit all delta changes stored in snapshot delta disks down to the base disks. If you see the above message on a Virtual Machines summary tab please engage a VMware admin to run consolidation which would be completed after hours. Disk consolidation should take place as soon as it is noticed as it can potentially be negatively impacting performance.

Filling Datastores

Although snapshots and Disk consolidations are not the only way a Datastore can be filled, it is however the most common. If a Datastore has been filled the below message will be seen on the Summary tab for all Virtual Machines on the affected Datastore.



When a Datastore has been filled the most likely scenario is that the VMs will be “Up” and “Running”, the VMs find themselves in a state where they will be responsive to pings but nothing else will be working as expected. Any operation on the VM that requires

disk writes will be failing. The most likely cause of this issue is that a snapshot was not managed and was allowed to run rampant. To remediate this situation, the VM with the snapshot will need to be powered off as to prevent the VM from continuing to attempt to write to disk, and then the snapshot will need to be removed. This needs to be accomplished by a VMware Admin as we need to watch at the hypervisor level that this process is occurring properly. This situation occurred early 2014 to a VM and Datastore at DST. The VM had approximately 8 snapshots on the VM which were approximately a year old. These snapshtos eventually filled the Datastore and the VM went down into the state of limbo, at this point the VMware team had to force kill the VM from the command line as power off operations were not working from the vSphere client, then the snapshot delete command was executed, the removal of the snapshots took approximately 12 hours to remove, which was 12 hours of downtime for that particular VM, luckily the VM had its own Datastore and it did not affect any other VMs.

References

Understanding Virtual Machine Snapshots
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

Working with Snapshots
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1009402

Deleting Snapshots in the vSphere Client
https://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.vsphere.vm_admin.doc_50/GUID-1DC05EAD-7EF1-4CE5-8BA0-307C1E9F9317.html

Go To a Snapshot in the vSphere Client
https://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.vsphere.vm_admin.doc_50/GUID-1D2B8CB5-35E7-47A5-82CC-3DEE1A343C64.html

Best Practices for Virtual Machine Snapshots in the VMware Environment
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1025279

Managing Snapshots
https://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.vsphere.vm_admin.doc_50/GUID-50BD0E64-75A6-4164-B0E3-A2FBCCE15F1A.html?resultof=%2522%2573%256e%2561%2570%2573%2568%256f%2574%2573%2522%2520%2522%2573%256e%2561%2570%2573%2568%256f%2574%2522%2520

VMware Snapshots
https://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.wssdk.pg.doc_50/PG_Ch11_VM_Manage.13.3.html?resultof=%2522%2573%256e%2561%2570%2573%2568%256f%2574%2573%2522%2520%2522%2573%256e%2561%2570%2573%2568%256f%2574%2522%2520

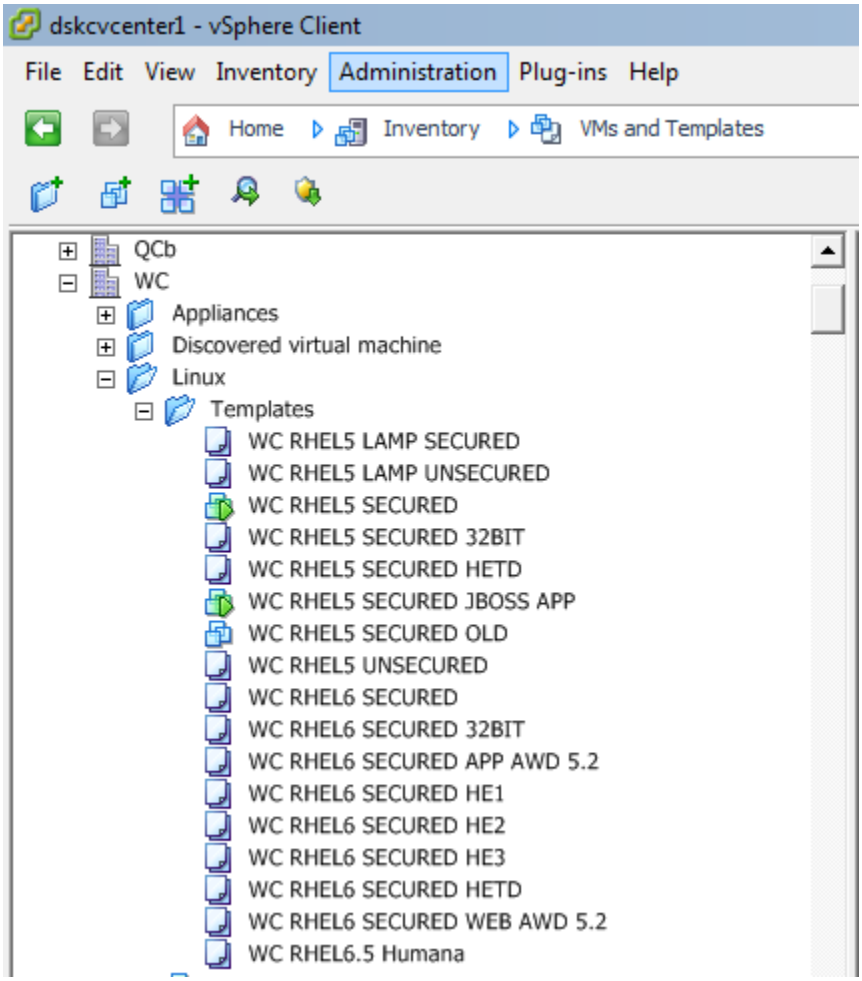
Snapshot File Types
https://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.vsphere.vm_admin.doc_50/GUID-38F4D574-ADE7-4B80-AEAB-7EC502A379F4.html

Templates

What is a Virtual Machine Template

A template is a simply a Virtual Machine that does not allow configuration changes which allows for Virtual machines to be deployed off of a consistent image. To edit a template, the template must be marked as a Virtual Machine to make any changes then marked back as a Template, the process of marking and unmarking is very quick. Templates can be viewed by navigating to the VMs and Templates View from within the vSphere client. Under each Linux and Windows folder for each Datacenter object there will be a Templates Folder. Although this logical folder separation exists, just placing a VM into the templates folder does not mean that the

VM is actually seen as a template, the folder is a spot to organize Templates but the folder can have any type of Virtual Machine placed into it. In the below screen capture you will see the Linux Template folder at the Winchester site:



A Template is designated by the Template Icon which looks like two pages stacked on one another. When a VM is marked as a template and this icon is seen although VM settings can be seen, they cannot be edited in this state. In the screen capture above, you will notice that a few VMs designated by name as Templates are actually in the Virtual Machine state and some are even Powered On, this most likely means that someone is making OS level changes and keeping their templates updated. This is a best practice to periodically Mark your templates as VMs and update the OS and apply any needed patches or any new VM level settings. This should be done in coordination with the cloud team as their product relies on the fact that Templates are actually marked as Templates.

Creating a Template

The actual process of taking a VM and marking it as a template is very simple, the process of actually building a VM which will become a Template is not necessarily difficult, but it is a process that takes some thought and verification as this Template could potentially be used to create hundreds of VMs.

Creating a Template starts with a VM, this VM will need the following:

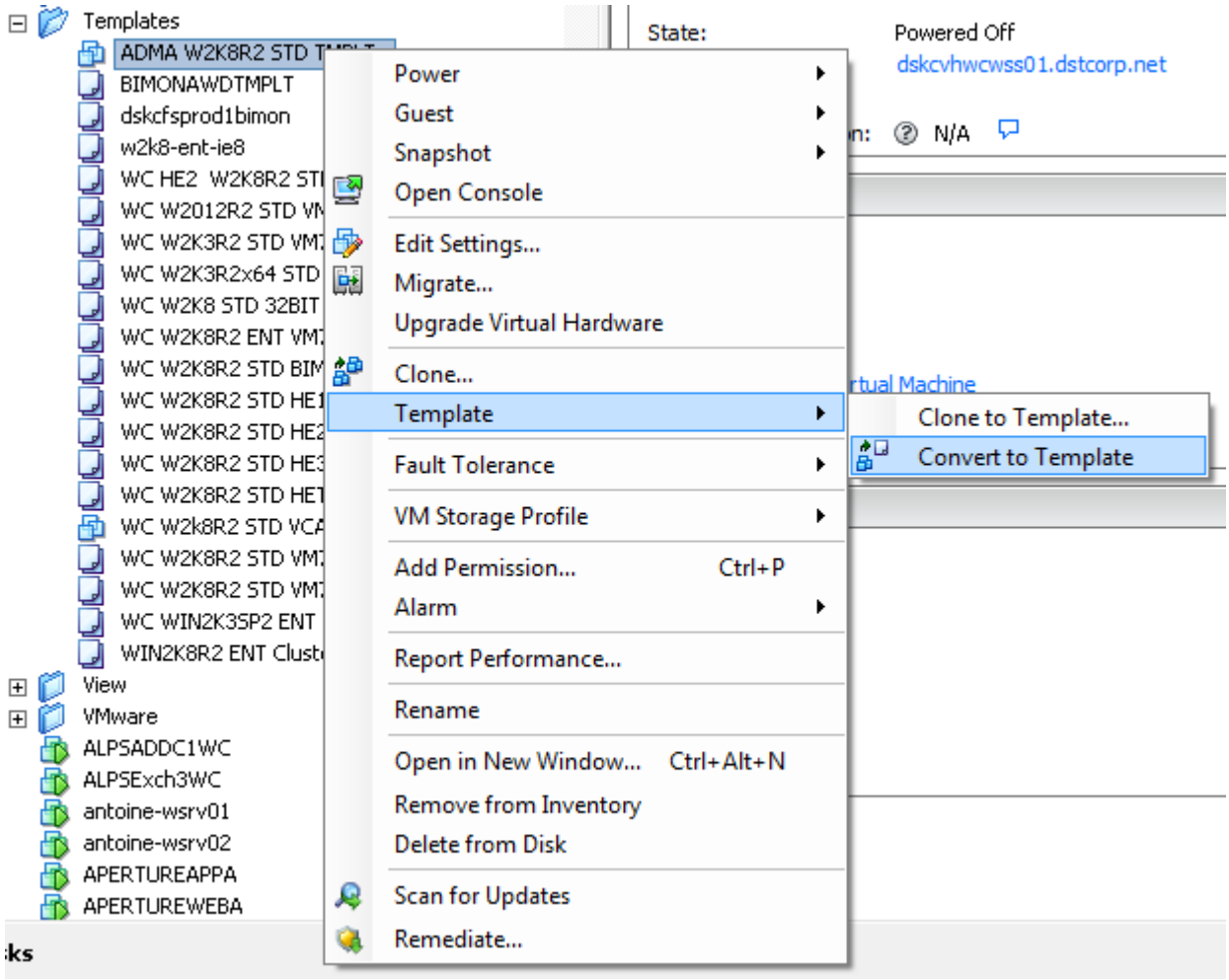
- Correct OS installed and patched on a correctly sized base VMDK (OS Drive)
- Correct number and Sizes of Data drives, for Windows an additional hard disk is provided for Data (D:) and for UNIX the normal is that it is provided 1 larger disk (around 100GBs)
- Correct OS Level Disk Partitioning Applied
- Correct Number of vCPUs Selected

- Correct Amount of Memory Selected
- Correct SCSI Controller Type Selected (VMware Paravirtual, select when building a new template from scratch, do not changed the controller type of OS VMDKs after the OS is installed)
- Verify Hot add is enabled for both Memory and vCPU
- If every VM deployed off of this template will have the same amount of NICs, the template creator can add the correct amount of NICs to the template.

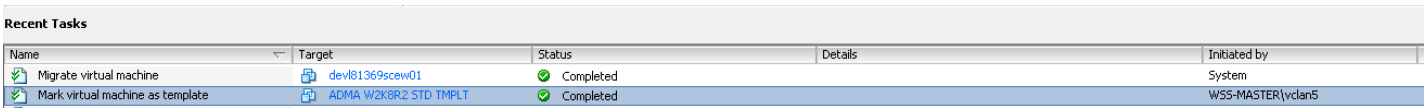
There are two methods for creating a Template: the first would be to take an existing VM and after applying all of the necessary settings and resources, mark that VM as a Template. The second method would be to create a brand new VM, a blank VM, from scratch, after which the OS must be installed and all configuration settings listed above applied then this new VM can be marked as a Template. Creating a new VM from scratch is outlined later in this document under the Deploying Virtual Machines section. Outlined below are the steps to mark a VM (regardless if it is new or existing) as a Template and how to mark a Template as a VM for editing or powering on purposes.

Marking a VM as a Template

To mark a VM as a Template to allow for VM deployment from said Template, navigate to the desired VM in inventory and right click the VM, then under Template select Convert to Template.

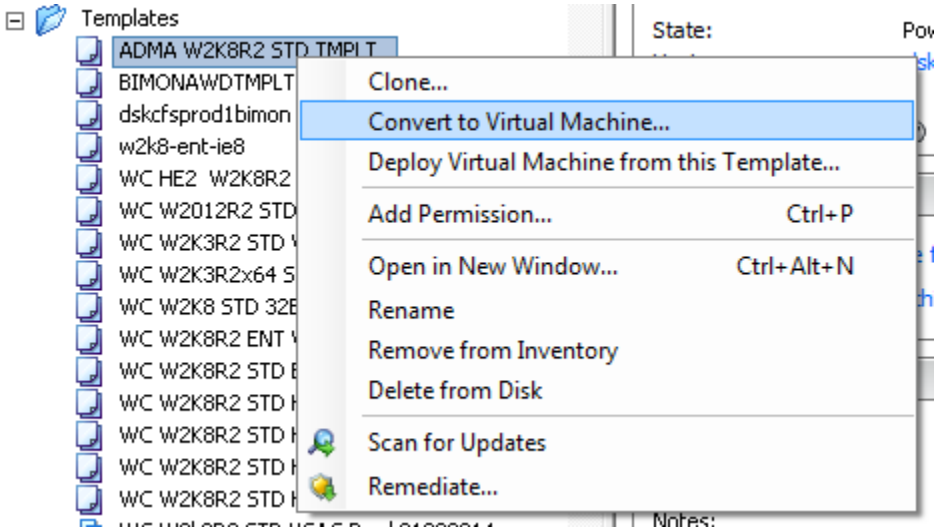


You will see the task kick off and finish within a few seconds:



Marking a Template as a VM to Make VM and Guest Changes

To mark a Template as a VM to allow for VM resource changes or power on operations to make guest level changes, navigate to the desired Template in inventory and right click the Template, then select Convert to Virtual Machine.



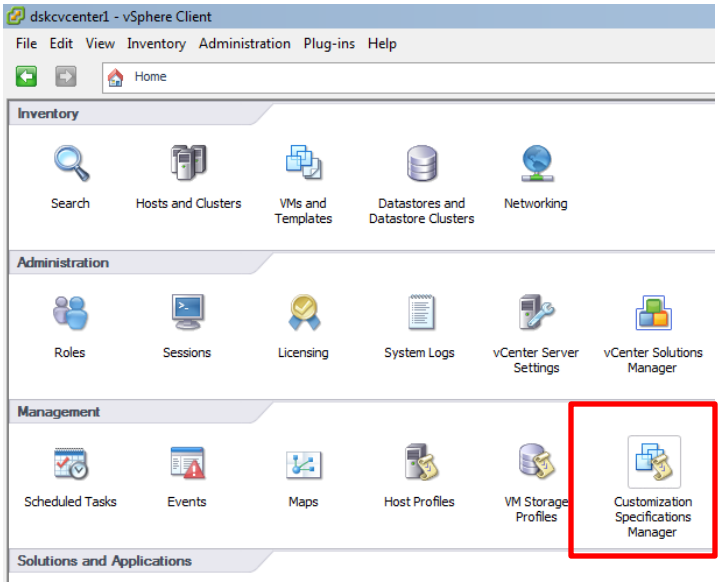
This will launch the Convert Template to Virtual Machine Wizard:

1. First in the wizard will be the Host / Cluster selection screen, select the Cluster where the Virtual Machine should reside, for example if the Template is a Windows VM then you would convert the Template to a VM and place it in the WCWSS cluster. Hit Next after determining the correct Cluster.
2. If the Specific Host selection screen appears, choose any host, DRS will move the VM if needed to a different host behind the scenes. Select any host and hit Next.
3. On the Resource Pool selection screen always select the Cluster object, such as WCWSS using the above example. All Clusters are seen as a top level Resource Pool. Select the Cluster and hit Next.
4. Review your selections and hit Finish. The Template icon will then change to a VM icon and you will then be able to edit the VM both at the VM level and guest.
5. After your changes are made, Mark the VM back as a Template and any new VM built from that Template will have your newly added changes.

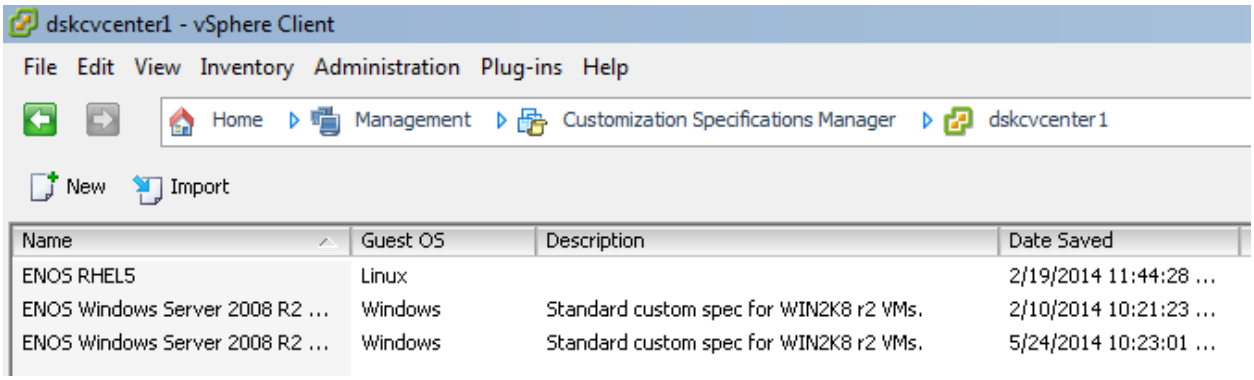
Customization Specifications

Customization Specifications are XML files that contain guest operating system settings for virtual machines. When you apply a specification to the guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names and OS level UUIDs.

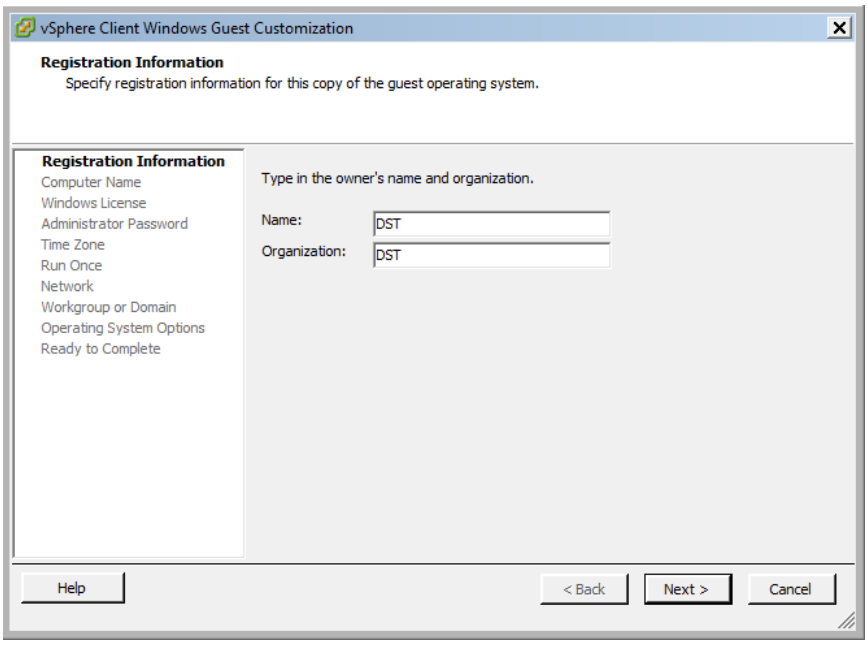
Customization Specifications are managed through the Customization Specifications Manager in vCenter, click on Home in the navigation bar at the top middle of the screen and select Customization Specifications Manager under the Management section.



You will be presented with a list of the currently created CS's, from here you can edit current CS's, create new ones by hitting the New button in the top left corner, or remove unused CS's.



A customization spec can do a lot of things for an admin, it can set local admin credentials, assign a OS license, set a computer name (always select Use the Virtual Machine Name), set Time Zone, configure Network adapters (if they exist on the Template you are using), join VMs to a domain, etc. In some areas for particular actions a password will need to be provided, these passwords are stored encrypted in the vCenter Database. See screen capture below of the menu of settings that can be set in the Wizard for CS's:



CS's are power tools that can drastically simplify the deployment of a new Virtual Server, if an existing CS won't work for your needs, please work with a VMware admin to create a new one as we want to keep CS manager clean of excess CS's, the fewer, the more simple to manager and the easier to keep consistent VM Server settings.

References

Creating and Managing Customization Specifications

https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-EB5F090E-723C-4470-B640-50B35D1EC016.html

Deploying Virtual Machines

Executing on Designs

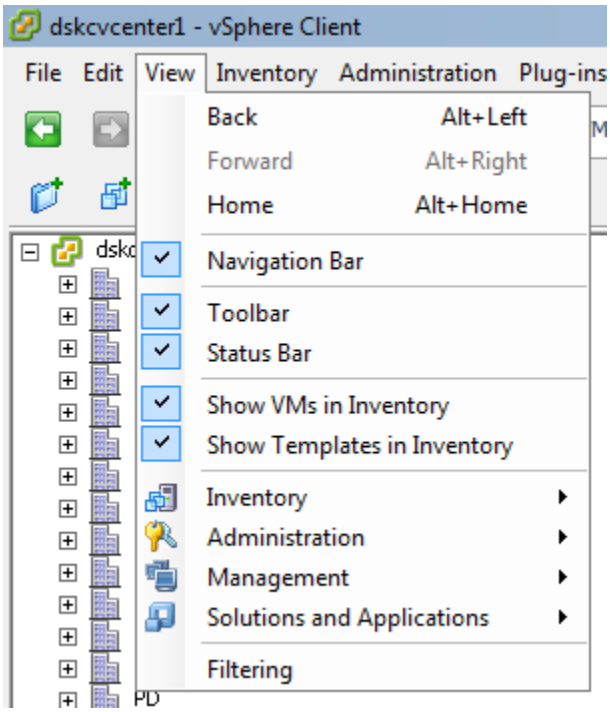
Which Teams?

Deploying Virtual Machines is not an inherently difficult process but it is a process that should include a lot of forethought. There are many items that require consideration when creating a new Virtual Machine, here are some questions to consider when deploying a VM:

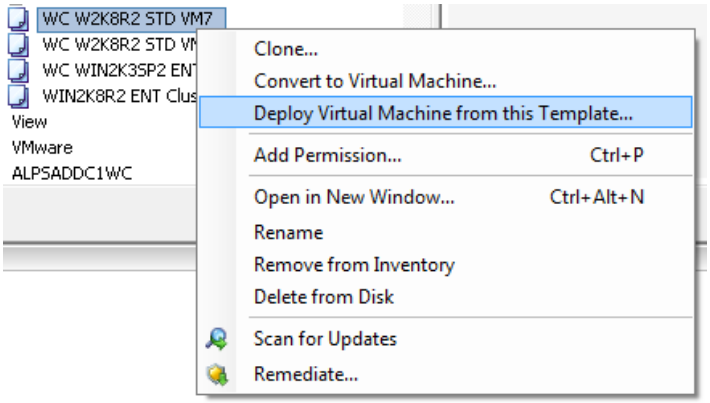
- Is the request for CPU resources for the VM(s) within the soft limitations set before I need to contact a VMware admin to review together?
- Is the request for Memory resources for the VM(s) within the soft limitations set before I need to contact a VMware admin to review together?
- Is the request for Storage resources for the VM(s) within the soft limitations set before I need to contact a VMware admin to review together?
- Is there enough space on the Datastore cluster, and Datastores to deploy the VM(s)?
- Is there an existing Template that I can use for deployment?
- Are there enough resources in the ESXi Cluster to accommodate the deployment of the requested VM(s)? (engage a VMware admin to answer this question, we would prefer you ask every time which could take less than 1 minute for the VMware team to analyze).
- Do the Portgroups (VLANs) exist that are needed for Prod and Repnet where applicable?

Deploying a VM from a Template

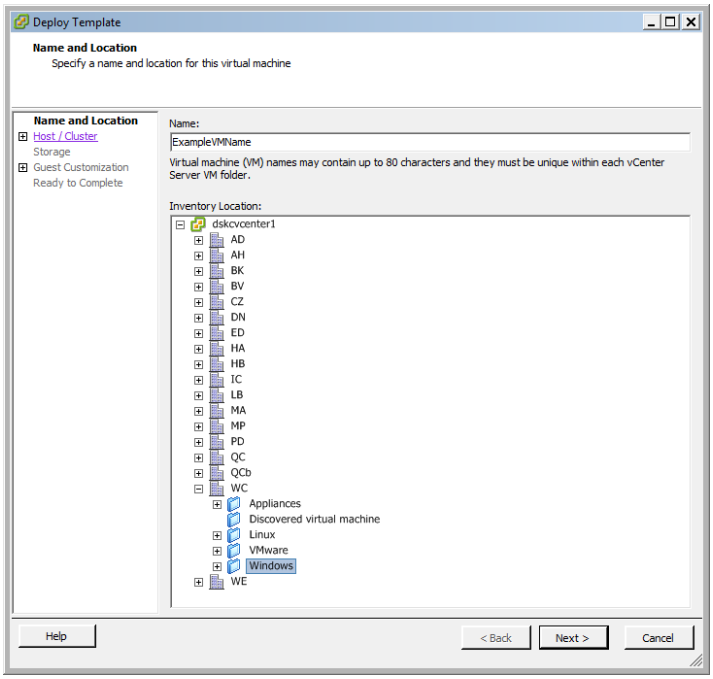
If CLM can be used to deploy a VM from the cloud, this should be the first option, secondary should be manual VM deployments as outlined in this section. To deploy a VM from an existing Template, Navigate to VMs and Templates view in the vSphere client navigate to the datacenter the VM will be deployed in. Expand the Datacenter object and either expand the Windows or Linux folder, in both folders resides a Templates folder. Expand the templates folder and determine the Template you wish to use, keep in mind that this view will display all Templates available in the Datacenter but there will be templates designated for certain environments like HE1,2, and 3. If you do not see the Templates in inventory you can verify viewing them is select by dropping down the View menu at the top and make sure “Show Templates in Inventory” is selected.



Once you have determined the Template to use, right click the Template and follow the below steps:

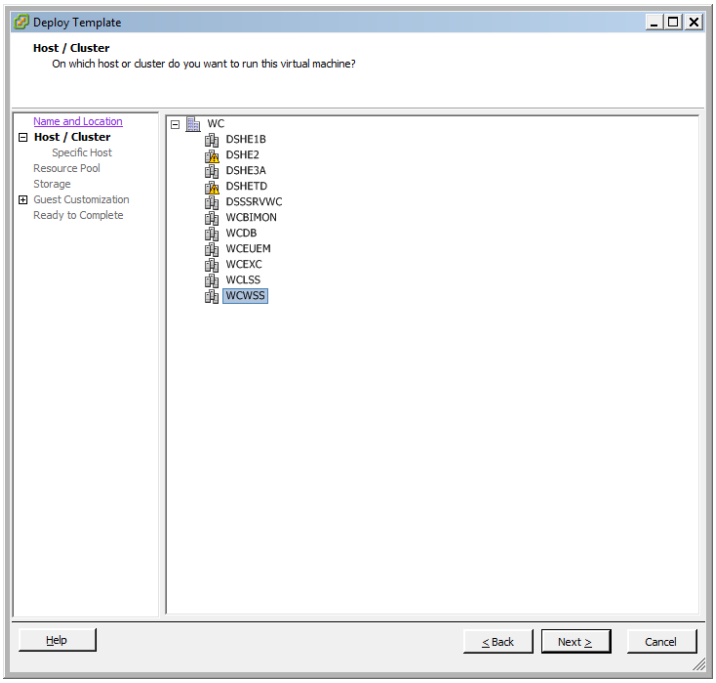


1. Select “Deploy Virtual Machine from this Template”, this will



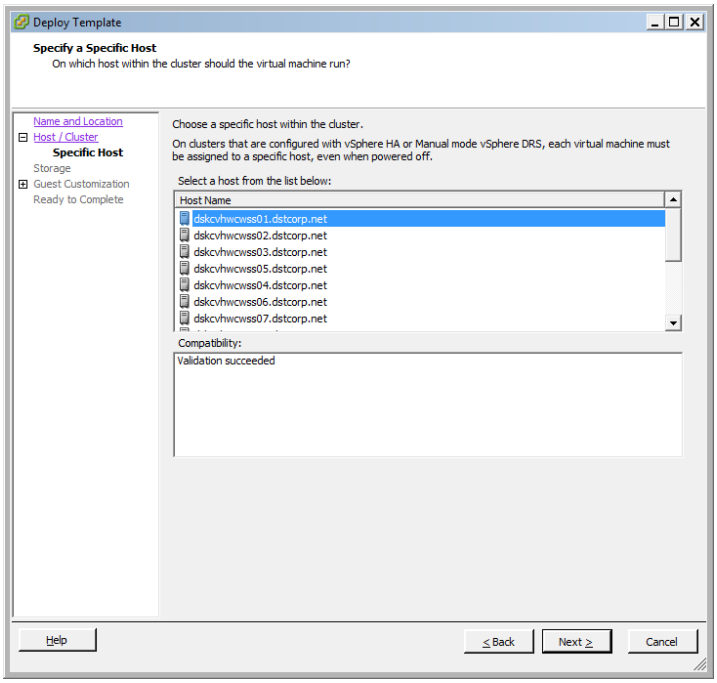
2. Provide the Name of the VM, this should match the Guest OS

launch the Deploy Template wizard.

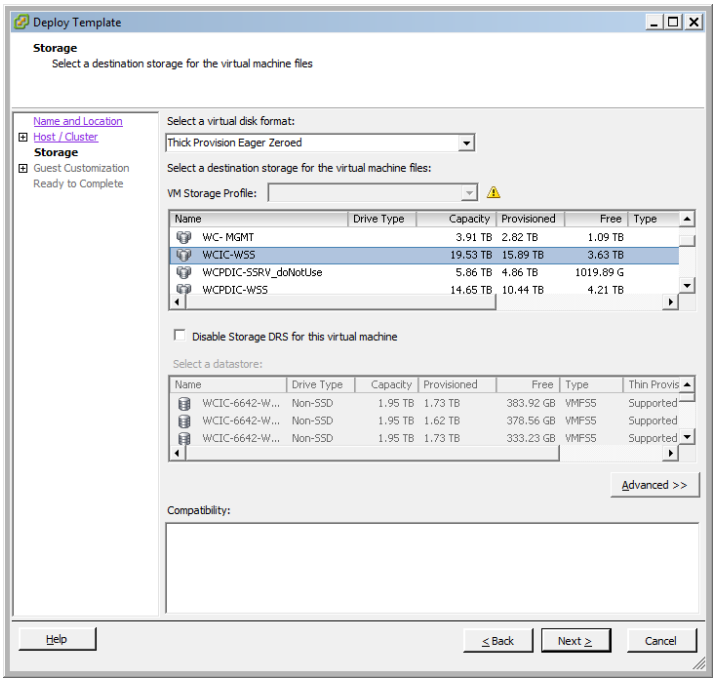


3. Select the ESXi Cluster to place the VM in. Hit Next.

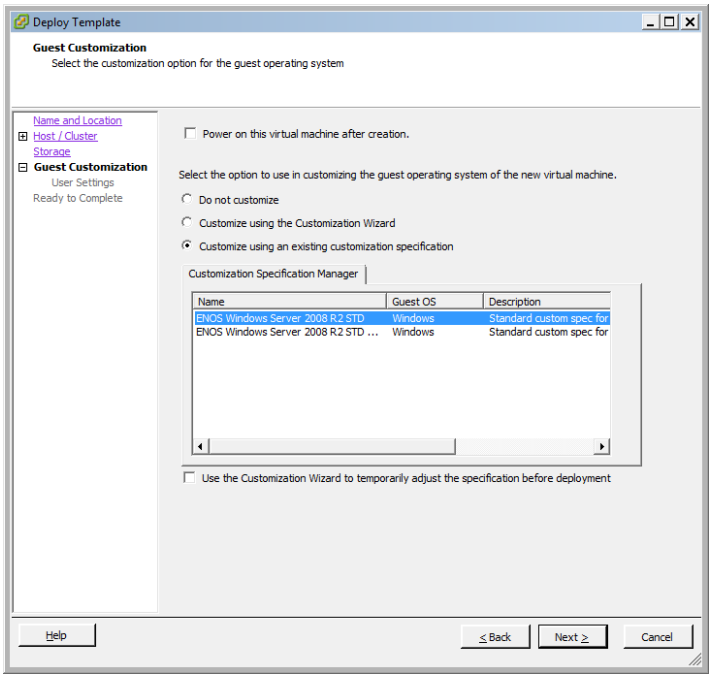
level server name in almost all circumstances. This prevents confusion when troubleshooting. Also select the Datacenter to place the VM under while also defining the Folder to place the VM in. Press Next.



4. If prompted to select a specific host in the cluster, choose any host and DRS will relocate the VM live if needed. Hit Next.

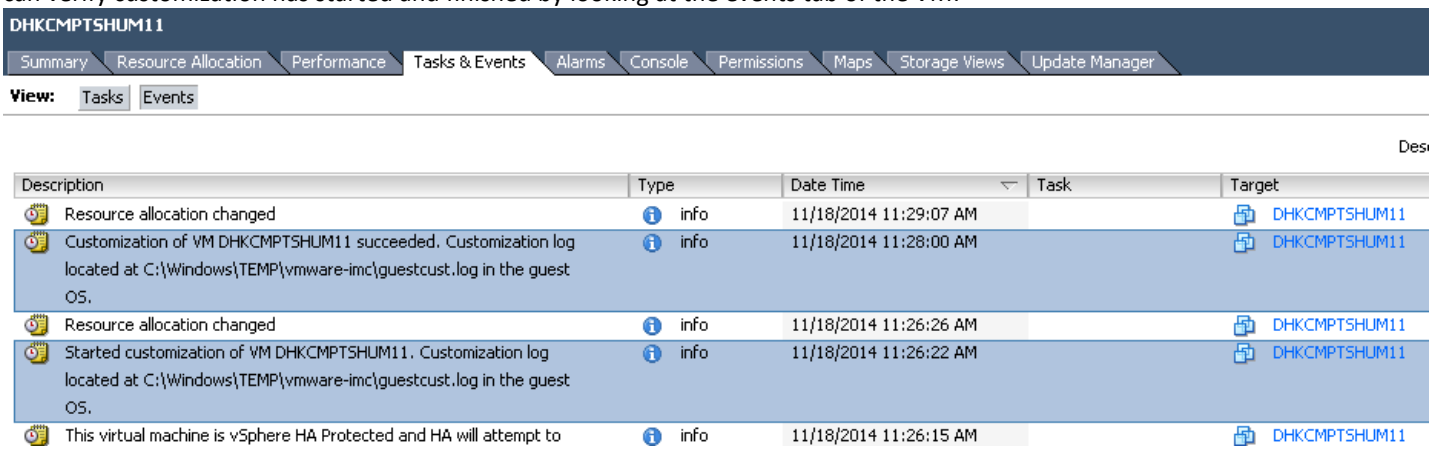


5. Select Thick Provisioned Eager Zeroed on the “Select a Virtual Disk Format:” menu, the select the Datastore Cluster to deploy the VM onto. At this stage you should only be confirming that the storage space is available because you should have already verified before starting deployment. Hit Next.



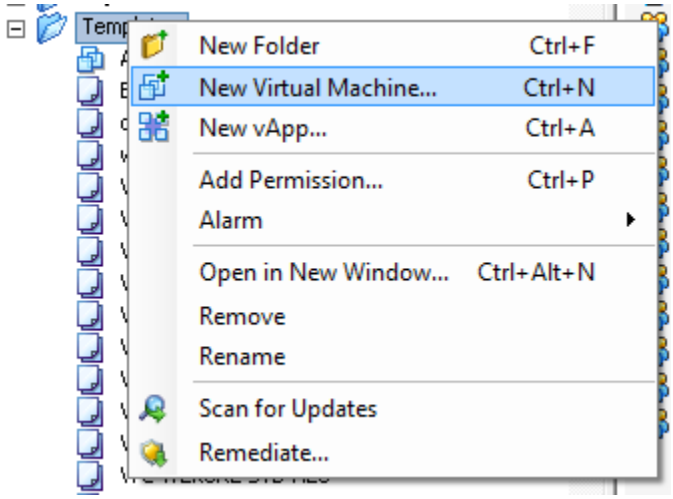
6. If an existing customization specification exists you can select the CS on this screen. You can also select Customize using the Customization Wizard which will be a onetime run of the CS wizard for this specific VM deployment. Select your option and Hit Next, do not select to Power on VM after completion. You will either be presented the CS wizard which you will follow the prompts for, or you will be presented the Ready to Complete screen. Review your build and hit Finish and the Deploy VM task will kick off.

7. After the VM has been deployed from Template, the following steps need to be taken before Power On and turn over. Add the required NICs using the VMXNET3 NIC driver (see later in the document, adding NICs), modify the CPU and Memory resources to the design, verify Hot Add is enabled on both Memory and CPU, and make sure you have added any additional nonstandard Hard disks.
8. If a customization specification was used during deployment, OS level configurations will take place after the VM is powered on for the first time. You should not perform any OS level configuration until the deployment customization has finished. During this customization the VM will be rebooted one or more times, initial deployment customization takes approximately 2-15 minutes. You can verify customization has started and finished by looking at the events tab of the VM:

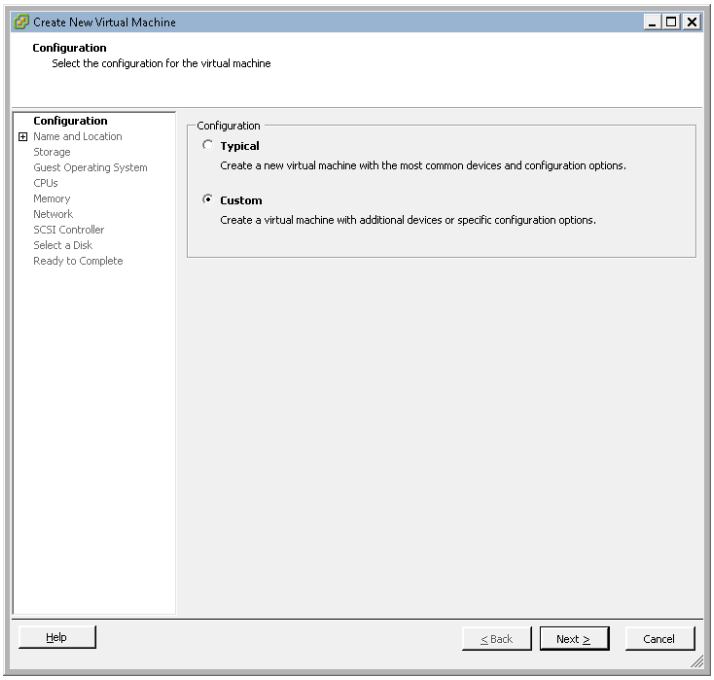


Deploying a Blank VM For New Template Creation

If CLM can be used to deploy a VM from the cloud, this should be the first option, secondary should be manual VM deployments as outlined in this section. IMPORTANT: Keep in mind that all new Template VMs must be vetted by the Cloud team if they will be used by CLM. Deploying a new VM for OS install is similar in some ways to deploying a VM from template, only with a few added steps. The OS teams look for consistency in their VM server builds, therefore the only reason a blank VM should be deployed outside of the VMware team is to produce a new VM that will be configured to be a new Template. A new VM build from scratch to become a Template is how this section will be viewed from. To create a new Template VM from scratch, Navigate to VMs and Templates view in the vSphere client, navigate to the datacenter the new Template VM will be deployed in, expand the Datacenter object and either expand the Windows or Linux folder, in both folders resides a Templates folder, then follow the below steps:

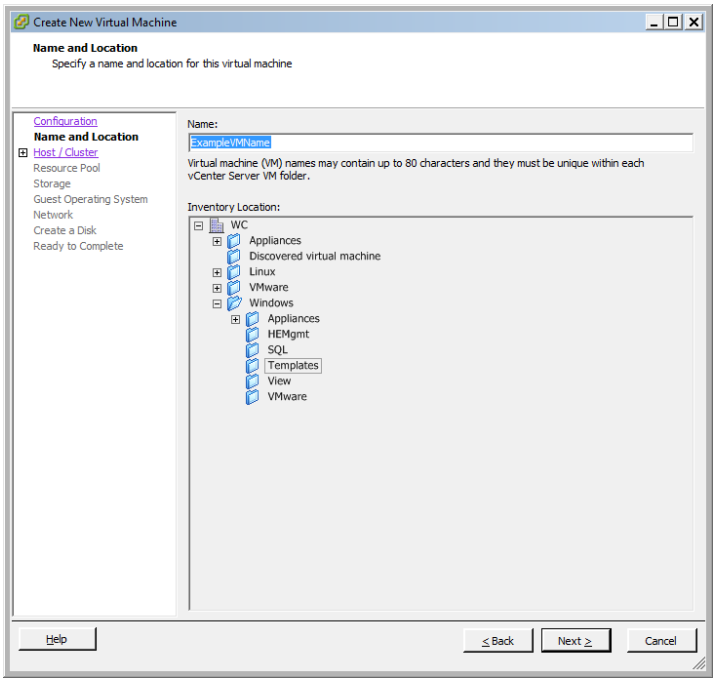


1. Right click the Template folder you have determined to be the location you wish to deploy the New Template VM, Select New

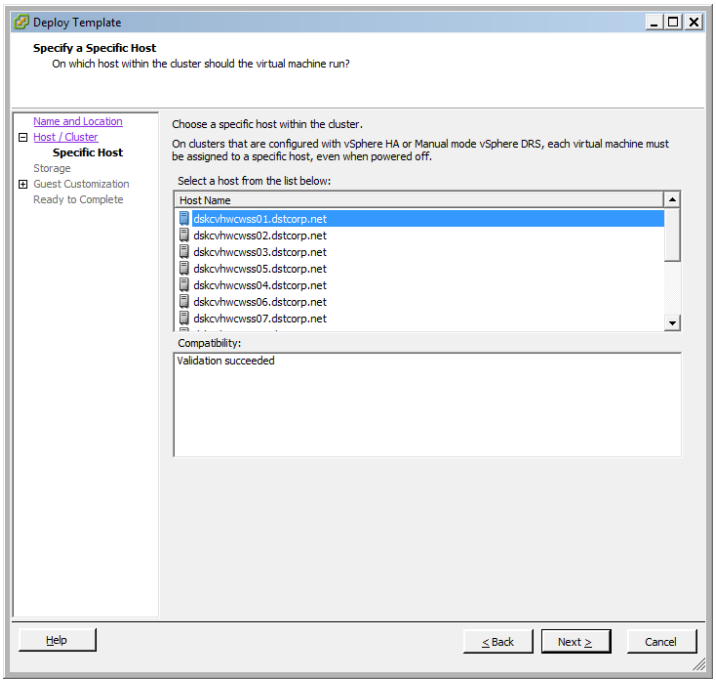


2. Begin to work through the wizard by choosing Custom configuration which will allow us to specify more advanced

Virtual Machine, this will launch the Create New Virtual machine Wizard.

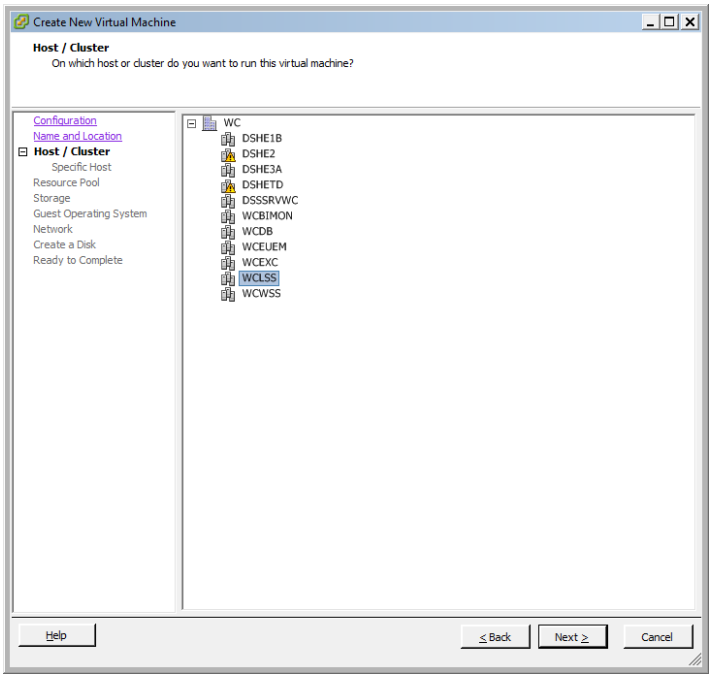


3. Specify a name for the new Template VM you are creating. Name usually include the site, the OS, the OS type, and environment it if is specific to a certain cluster. An example for a new Windows Server Template could be: WC W2012R2 ENT HE1. Hit Next.

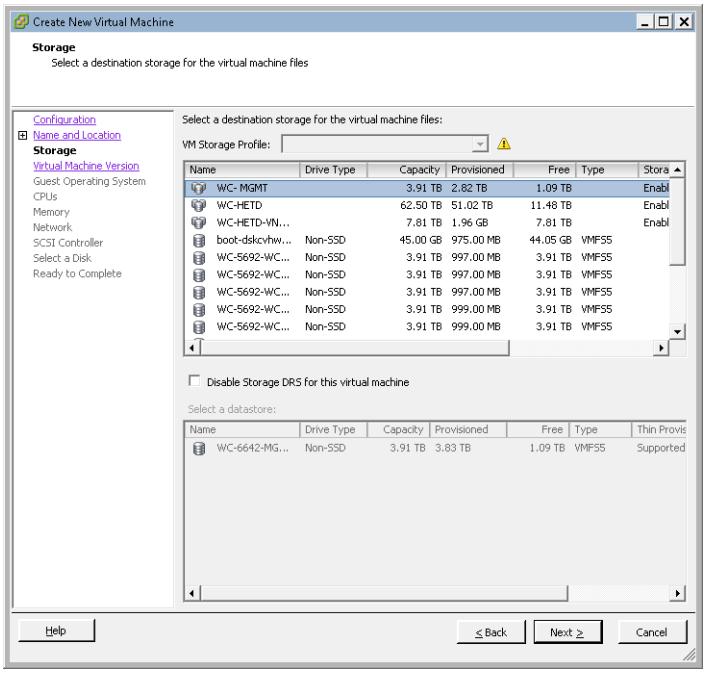


5. If prompted to select a specific host in the cluster, choose any host and DRS will relocate the VM live if needed. Hit Next.

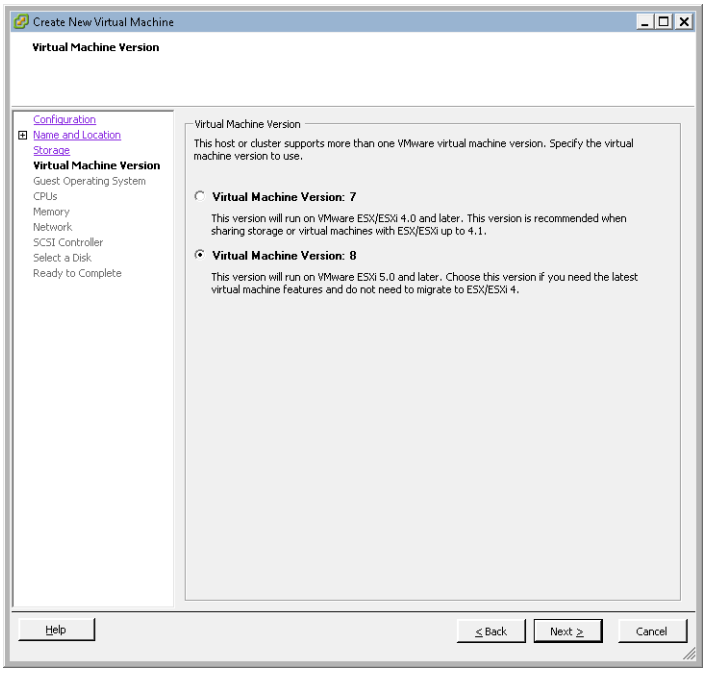
options that need to be included in a new Template build.



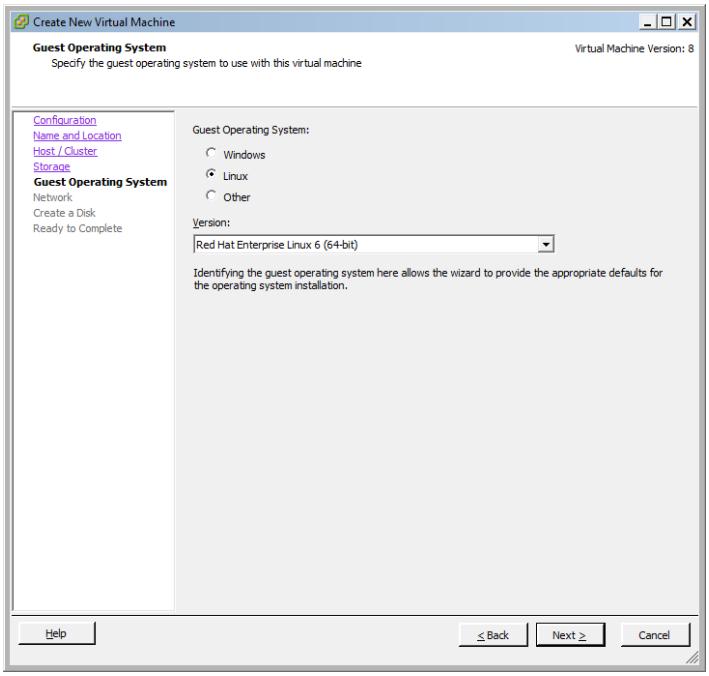
4. Select the ESXi Cluster to place the VM in. Hit Next.



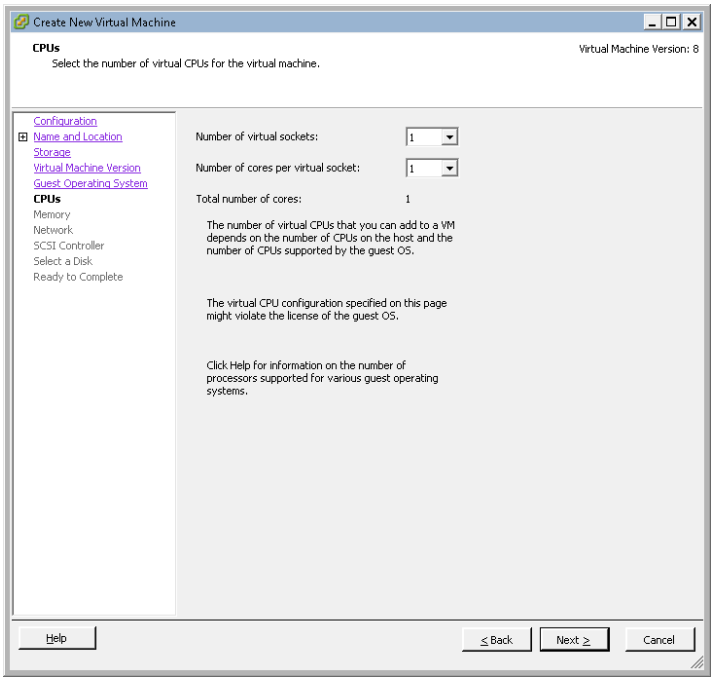
6. Specify WC-MGMT as the Datastore Cluster for the new Template VM. This Datastore Cluster spans all clusters allowing access to the Template across many environments if desired. Hit Next.



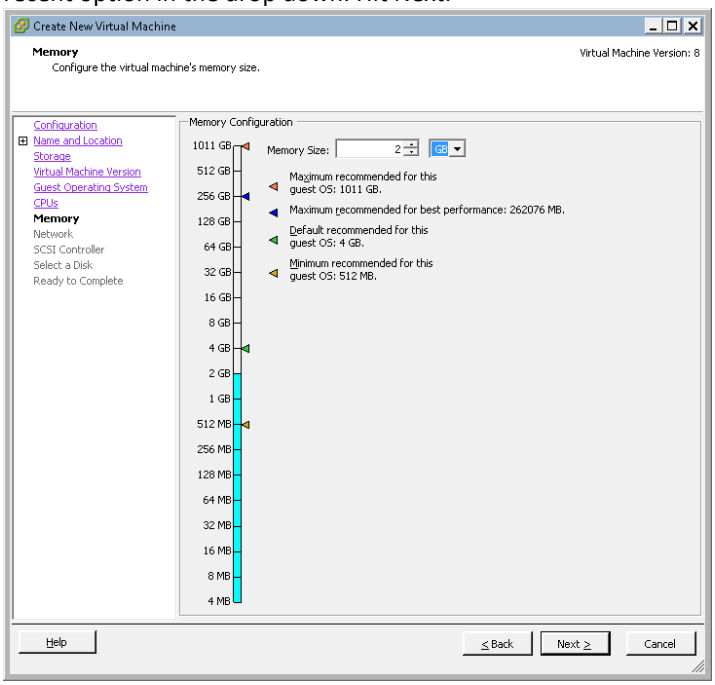
7. Select Virtual Machine Version 8 or greater where applicable. Hit Next.



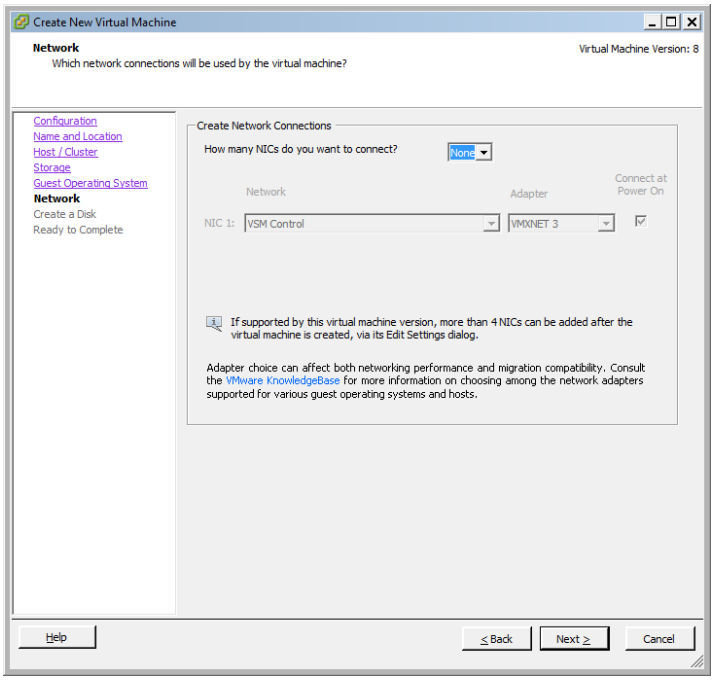
8. It is crucial you designate the correct OS version when deploying a new Template VM, some VM functionality may be unavailable if you choose the wrong OS. If you are deploying a new version of an OS and do not see it listed, select the most recent option in the drop down. Hit Next.



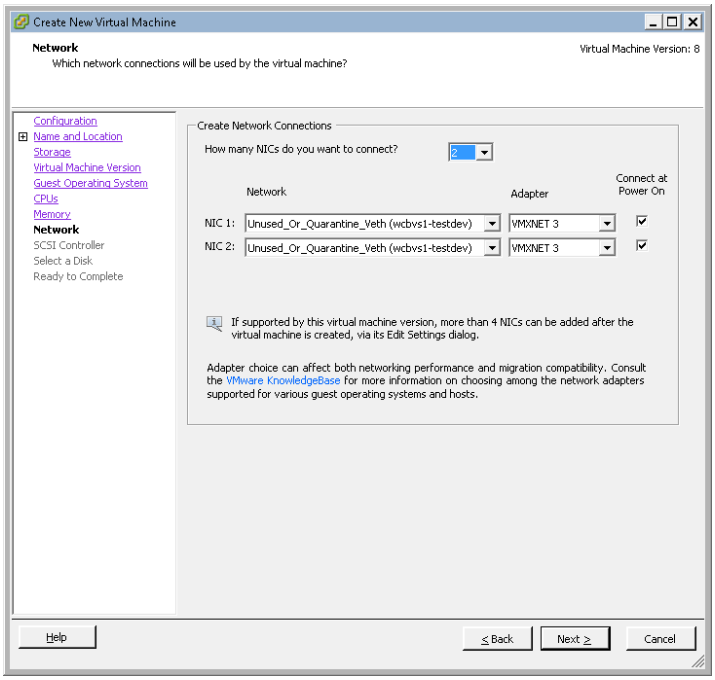
9. When building a Template VM, 1 Virtual socket with 1 Virtual core should always be the designated CPU allocation. When a VM is deployed from this Template in the future, the deployer can specify other resource settings. Make sure 1 is selected in eat box. Hit Next.



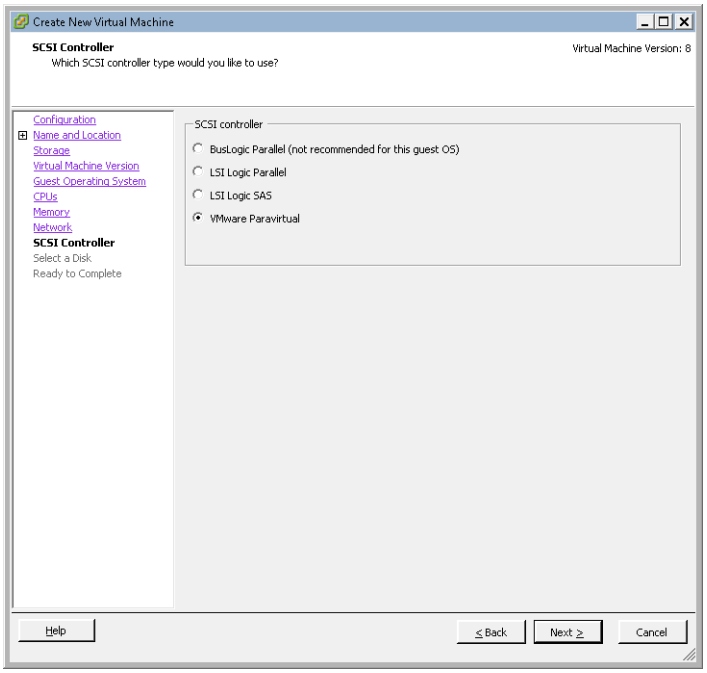
10. Choose 2 GB as the default Memory allocation for the new Template VM. When a VM is deployed from this Template in the future, the deployer can specify other resource settings. Hit Next.



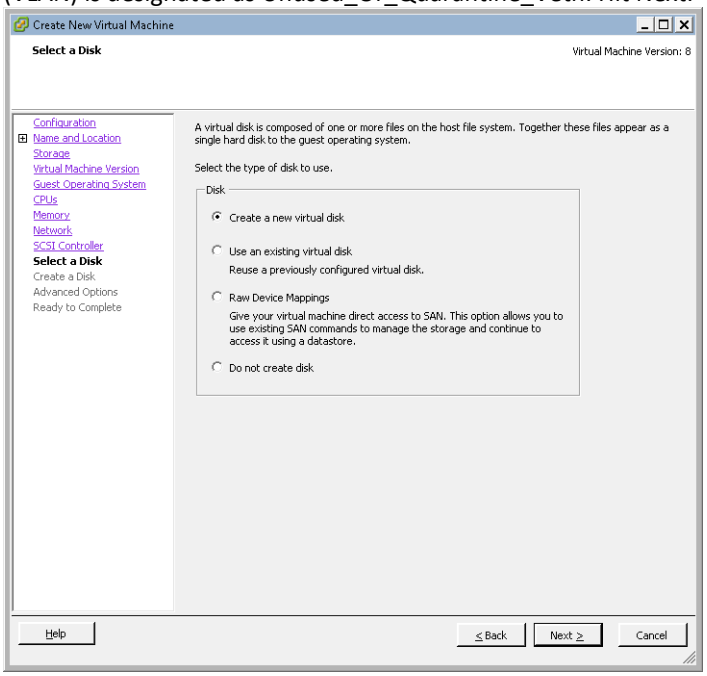
10-a. If you believe that VMs created from this new Template VM could use different amounts of network cards, select None on the new Template VM build. When a VM is deployed from this Template in the future, the deployer can specify other Network card amounts. Hit Next.



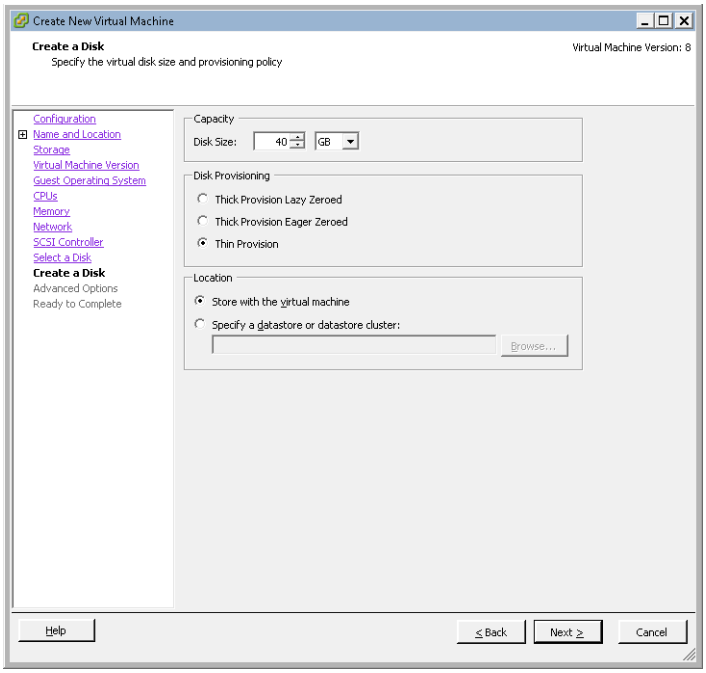
10-b. If all VMs that will be created from this Template will always need a set amount of NICs (i.e. 1 prod, 1 repnet) then you can specify the count on this screen. Make sure all NICs have the VMXNET3 adapter chosen and that their portgroup (VLAN) is designated as Unused_Or_Quarantine_Veth. Hit Next.



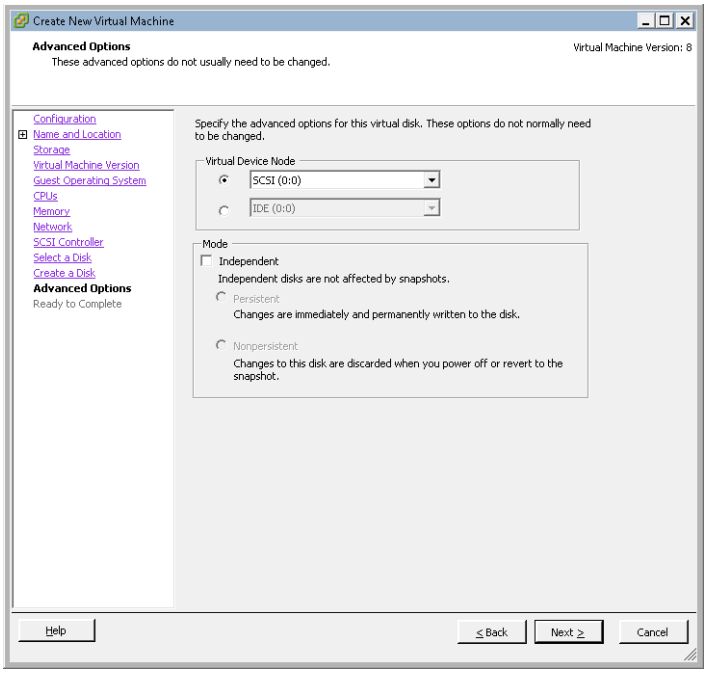
11. Always select to use the VMware Paravirtual SCSI Controller. Hit Next.



12. Select to Create a new virtual disk. This will be the Hard disk where the OS will be installed. Hit Next.



13. Because this is a Template, we want it to occupy as little space as it can, so in this circumstance select Thin Provisioning for the Disk format and specify the OS Hard disk's size. Leave selected "Store with the Virtual machine" under location. Hit Next.



14. Make no changes on the Advanced Options screen. Hit Next. Review your new Template VM Build settings on the Ready to Complete screen and hit Finish if all looks acceptable. The VM will be created at this point.

15. After the new Template VM is created a handful of things need to occur to prep the VM to be marked and used as a Template:

- Any additional Hard disks should be added (also thin provisioned) to the VM
- Temporary network access may need to be granted to the VM to download patches and software, put the NICs on the required VLANs but remember to set back to Unused before marking as a Template.
- Make sure Hot Add for Memory and CPU is enabled on the VM.
- An ISO with the OS software must be attached to the VM's CD drive and the OS must be installed
- VMware Tools MUST be installed after Guest OS is installed, very important.
- OS level: install any applications, format hard disks, create any needed partitions, if any temporary IPs were used for network access remove the IPs after customization.
- Power off VM.
- Mark VM as Template.

Deploying VMs/Appliances from OVAs or OVFs

Many vendors offer prepackaged Virtual Machines with preinstalled software and configurations often referred to as appliances. These appliances are packaged in an open virtualization format called OVA or OVFs. To deploy an OVA/Appliances please contact the VMware team for assistance.

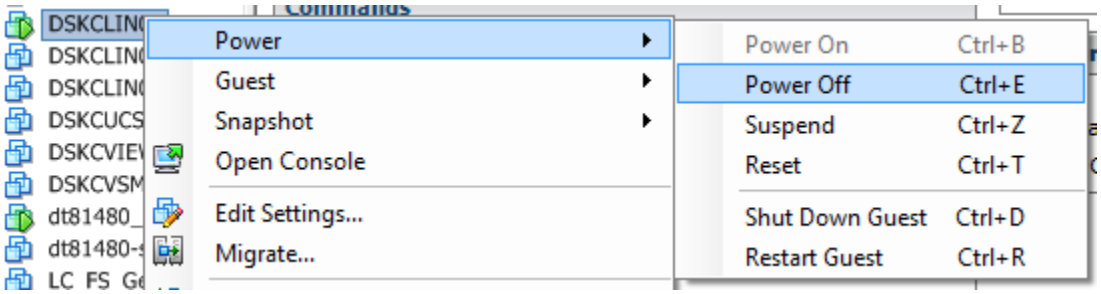
Limits on Deploying Virtual Machines before engaging the VMware Team

If you operate within the limits of acceptable VM resource limitations (CPU and memory), you have verified there is enough storage space and have verified that there are enough compute resources on the ESXi host clusters by working with a VMware admin, there are no limitations on the number of VMs that can be added by an individual if the guidelines outlined in this document are followed. Although this is the case, please notify a VMware admin when adding more than 5 VMs at once so that they can verify compute resources.

Virtual Machine Management, Maintenance, and Common Tasks

Power On and Off Operations

Virtual Machine Power operations are available in multiple areas in the vSphere Client. When a VM is Powered Off, the Power on operation can be seen on the Summary Tab of the VM under the Commands area. When a VM is Powered On, Shutdown Guest, and Restart Guest are available on the Summary Tab if VMware Tools are installed. You can also access the Power operations from the VMware Console if using a break out window console. The recommended way to handle power operations is to right click the desired VM and navigate to Power, this will present a menu with different options being selectable depending on the current VM Power state and if VMware Tools is installed:



Power On: Same as hitting the Power button on a Physical Server. The VM will boot.
Power Off: Equal to holding the Power button in until the Server turns off, also equal to Pulling the Power cable out. This is not the desired shutdown method as the guest will boot into recovery after hard power off.
Suspend: Do not use, disabled for all users including VMware admins.
Reset: Command is equal to holding the Power button in for hard power off and then powering on immediately.
Shut Down Guest: Runs a script through VMware tools to issue a soft system shutdown, this is the desired method if not shutting down from within the guest OS.
Restart Guest: Runs a script through VMware tools to issue a soft system reboot, this is the desired method if not rebooting from within the guest OS.

Renaming a Virtual Machine

VMware Tools

What is VMware Tools

VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. Without VMware Tools installed in your guest operating system, guest performance lacks important functionality. Installing VMware Tools eliminates or improves these issues:

- Low video resolution
- Inadequate color depth
- Incorrect display of network speed
- Restricted movement of the mouse
- Inability to copy and paste and drag-and-drop files
- Missing sound
- Provides the ability to take quiesced snapshots of the guest OS
- Synchronizes the time in the guest operating system with the time on the host
- Provides support for guest-bound calls created with the VMware VIX API
- Allows use of the VMware Balloon Driver
- Presents some Guest OS level visibility to the VMware Admins (IPs, DNS, Guest Disk Partitions)

- Guest OS Soft Shutdowns

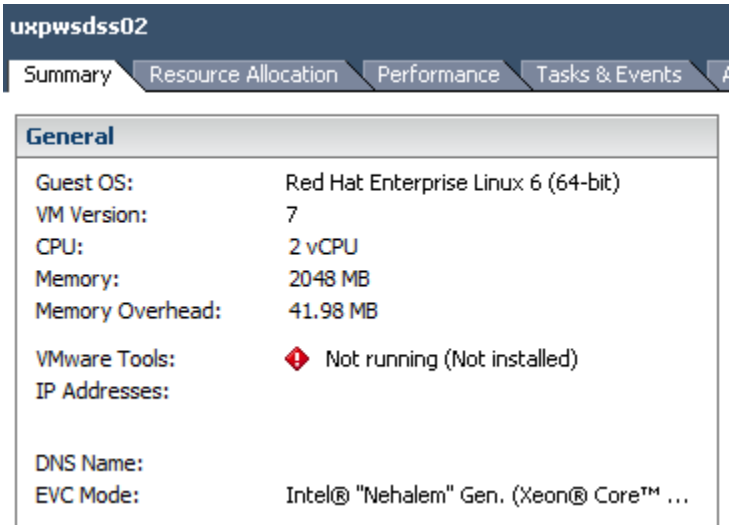
VMware Tools includes these components:

- VMware Tools service
- VMware device drivers
- VMware user process
- VMware Tools control panel

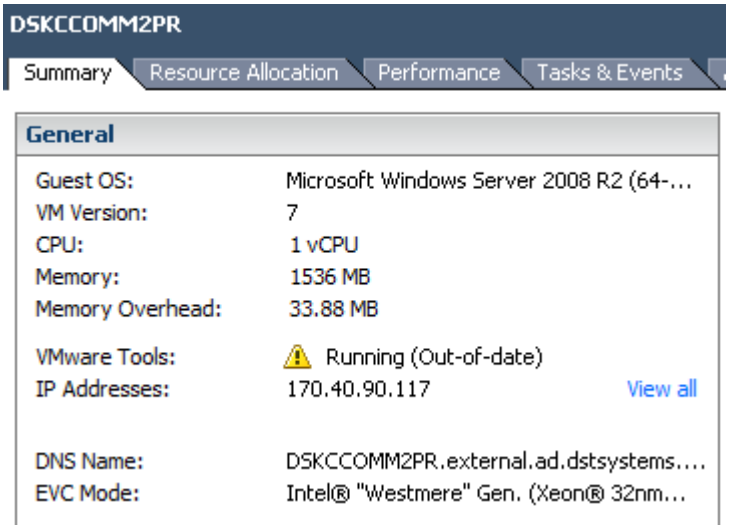
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340

Installing or Updating VMware Tools

VMware tools should be installed on every Virtual Machine in the ES VMware Environment, the VMware tools package install is managed by the Guest OS teams as it requires Guest level permissions which the VMware team does not have. You can see the status of VMware tools from the Summary tab for any Virtual Machine, below are two examples of a VM needing a VMware tools action to occur.

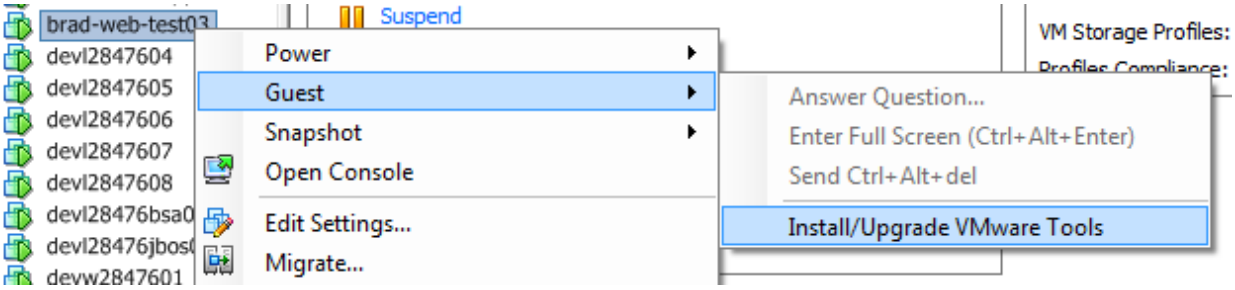


VMware Tools not installed, notice that vCenter is not aware of the IP addresses assigned nor the DNS name of the Guest. Needs VMware Tools Installed.



VMware Tools installed but needs update, notice that with VMware Tools vCenter is aware of the IP and DNS of the Guest. Needs VMware Tools Upgraded.

To install VMware tools you will mount the VMware Tools ISO Image to a VM and install it from that image in the guest OS. To mount the VMware Tools ISO right click the Virtual Machine of choice > go to Guest > then select Install/Upgrade VMware Tools. This will mount the ISO image to the Guest in the CD-ROM.

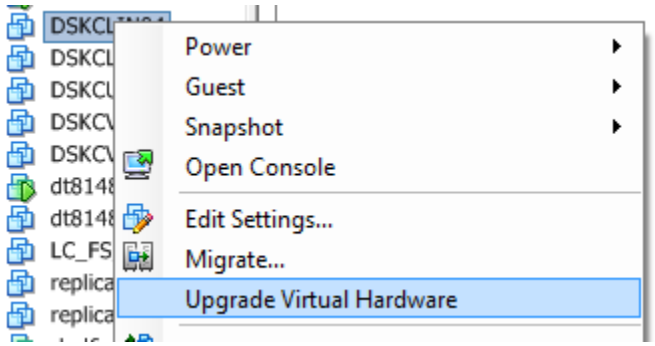


Install VMware Tools in Windows by double clicking the VMware Tools CD mounted and run through the installed. Install VMware Tools in UNIX by navigating to the mounted CD directory and run the following command: sudo ./vmware-install.pl –d, -d means to accept the defaults in the install. For both OS types taking the defaults is the desired install configuration. VMware Tools requires a reboot after install or upgrade which can be postponed if needed.

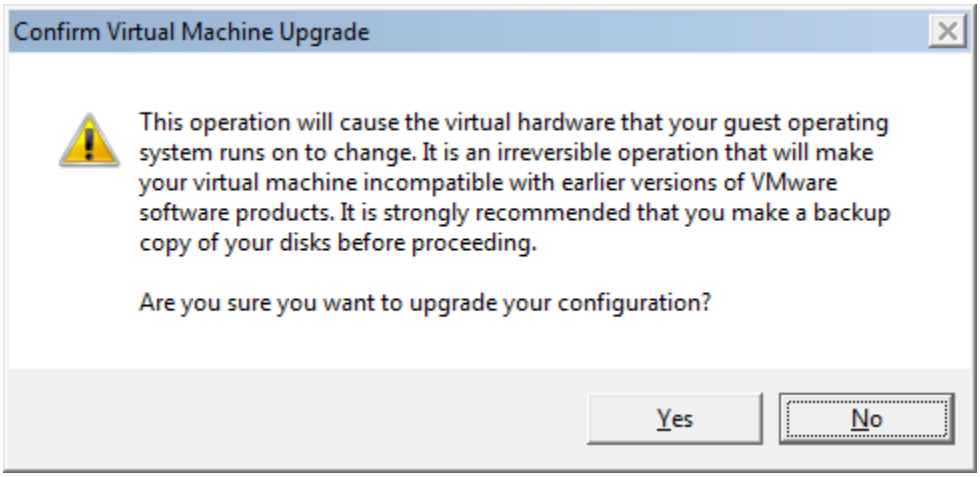
http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1014294

VM Hardware Versions

Virtual Machine hardware versions determine and set hardware settings for VMs, including maximums for devices such as max disk size and number of CPUs. The OS teams should upgrade VM hardware when possible as it requires the VM to Powered off. Upgrading VMware tools is extremely simple, when the VM is powered off right click the VM object and select Upgrade Virtual Hardware (this option only appears if an upgrade is possible).



Confirm the upgrade of the Virtual Hardware when prompted by hitting Yes. The VMs hardware will be upgraded to the highest possible based on the version of ESXi the host it is running on is at.

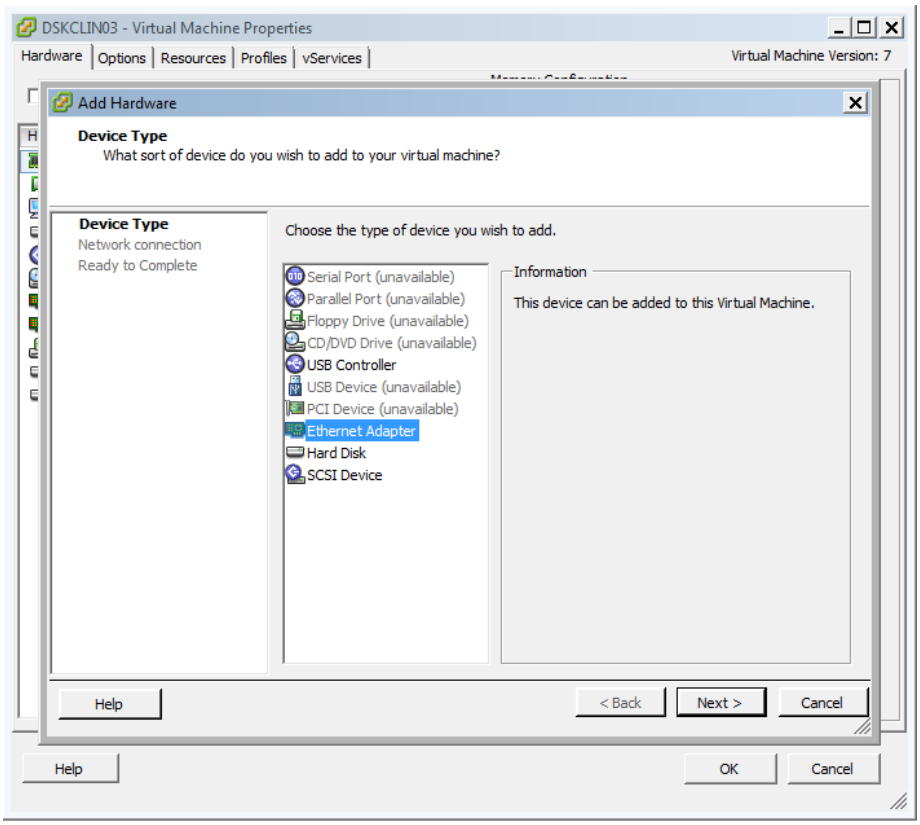


http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003746

Network Adapters

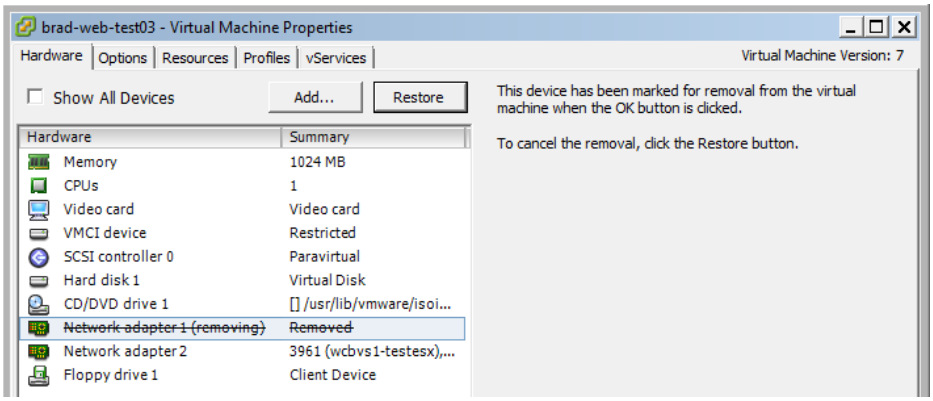
Adding a NIC

Adding a Virtual NIC to a VM can be done when the VM is powered on or off. Edit the VM settings > on the Hardware Tab select Add > highlight Ethernet Adapter and hit Next > Under type always Select VMXNET3, then select the desired VLAN under Network label and hit Next > Review change and Hit Finish > Once returned to the Edit settings screen Hit OK if you have added all of the NICs you wanted to.



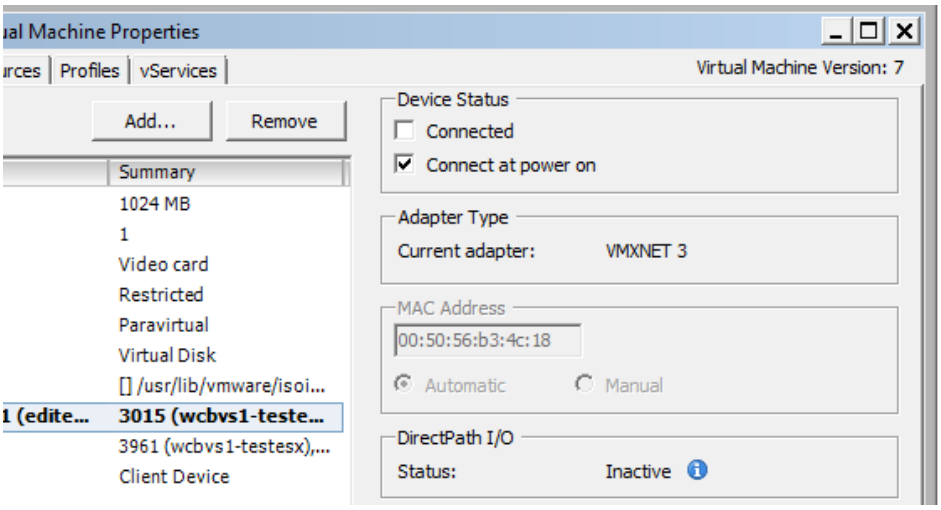
Removing a NIC

Removing a Virtual NIC from a VM can be done when the VM is powered on or off. To remove a NIC from a VM, Edit the settings of the Virtual Machine > Select the Network Adapter want to remove from the Hardware list > Select Remove > Hit Ok. The VM will be reconfigured and the NIC will be removed from the VM.



Connecting and Disconnecting a NIC

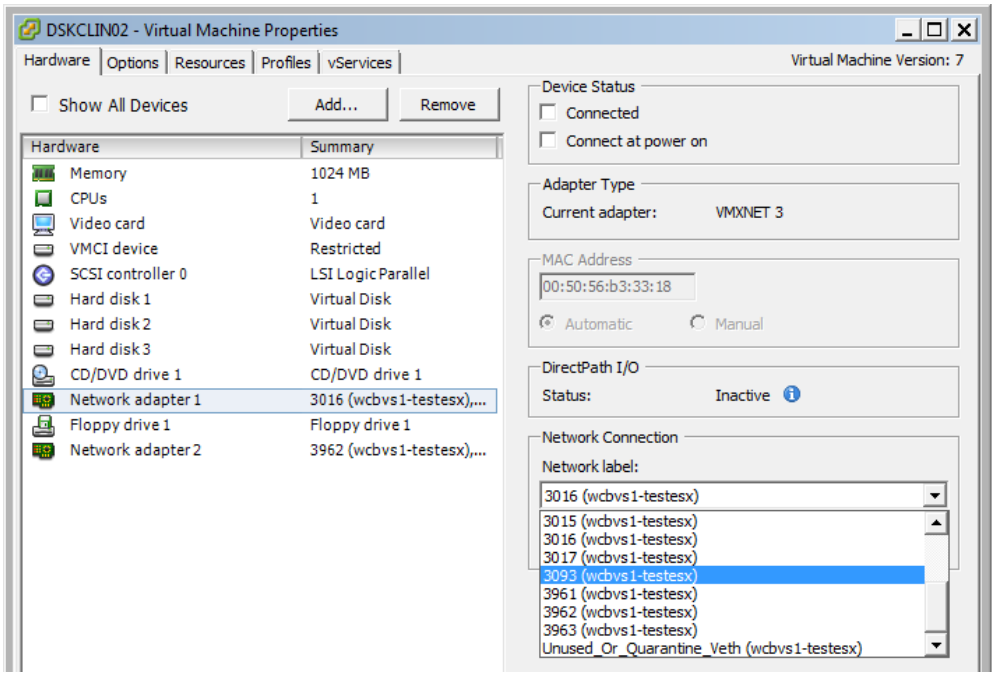
It can be necessary at times to disconnect a current attached NIC while keeping it attached to the VM or to reconnect a NIC on a VMware after it was disconnected. To disconnect or connect a NIC from a VM, Edit the settings of the Virtual Machine > Select the Network Adapter > Uncheck or check the Connected box in the top right corner of the screen.



It is also important to notice the Connect at Power On box, if you power on a Virtual machine and see no NICs, confirm that this box is checked, also confirm this box is connected when a new NIC has been added.

Assigning Portgroups (VLANs) to Virtual NICs

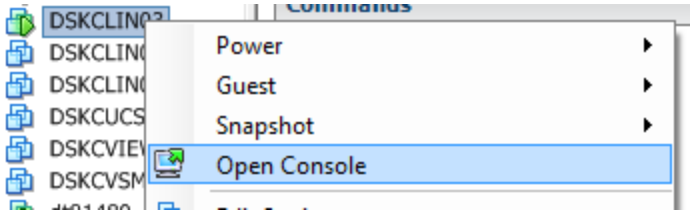
Assigning a Portgroup to a Virtual NIC is the equivalent of plugging a Network cable in from a physical server to a port on a switch which has been configured with the desired VLAN Tags. In the ES VMware environment a Portgroup is synonymous with a VLAN ID. To assign a Portgroup/VLAN to a VM's NICs edit the settings of the VM > Select the desired NIC > In the lower right corner use the drop down to select the Portgroup\VLAN you want to apply and hit Ok. The VLAN will be applied and network access can be tested.



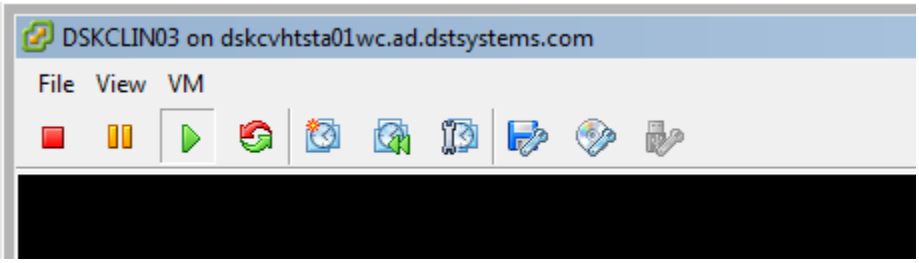
Troubleshooting Virtual Machine Connectivity

Using the VM Console

The VM Console is your "monitor connect to a physical server", before VMs are on the networking this is your only means of accessing your Virtual Machines. Connect to the console of a VM by right clicking the VM and selecting Open Console. This is the preferred method as it provides the user a breakout Console window where the console is not limited visible space like when you go to the Console Tab for a Virtual Machine which most times severly limits your view of the VM screen.



When using the break out VM console a menu of standard VM commands will be presented at the top of the Screen in the commands bar such as Power operations, snapshots, and attaching ISO images.



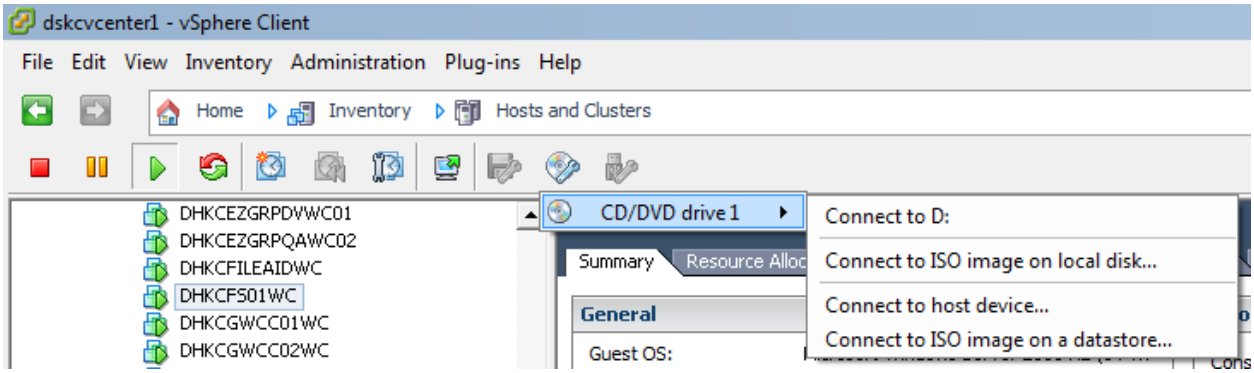
If you need to use the Ctrl+Alt+Del command, when the breakout VM console is in use you can instead use Ctrl+Alt+Ins which will execute the command only on the VM and not issue it on your workstation. Before VMware tools is installed on a VM, to have your mouse release from the VM console you need to press Ctrl+Alt.

Logging Out of the Console

There is not method for logging out of the VMware console in reality, but it is important that you log out of the Guest OS when done using a VM from console. Far too often the VMware admins find VMs unlocked because the user has simply closed the vSphere client or break out console for a VM which leaves the Server completely exposed to anyone with access to get onto the guest without logging into to it.

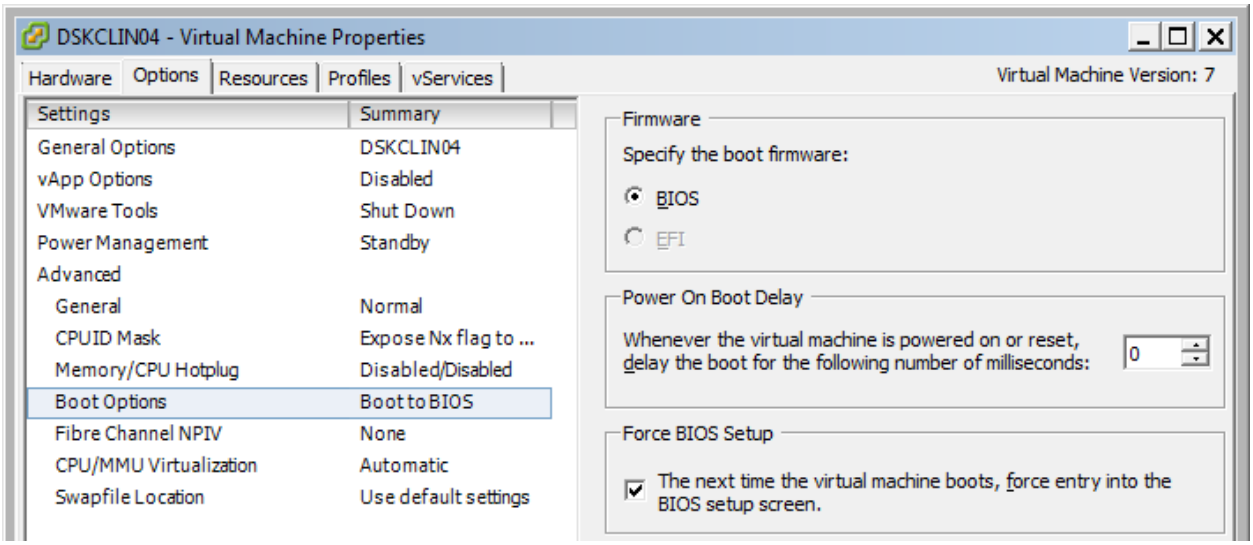
Attaching an ISO Image

There are cases where an ISO image may need to be connected to a Virtual Machine, mainly if a Guest OS is being installed on a New Template VM for the first time. In many circumstances, OS admins might use OS level tools to mount an ISO image from within the guest which is acceptable also. You can mount an ISO image from a few different areas in the vSphere client, you can select the desired VM in inventory and use the menu at the top to attach an ISO image by selecting the CD icon, the drive, then the method to attach. You can also use this same menu to attach an ISO when you have a break out VM console Window.



Select to select Connect to ISO image on local disk, this allows you to run an ISO image you have downloaded onto your workstation. This option is only available when a VM is powered on, in circumstances when installing the guest OS initially, power on the VM, Attach to ISO image, then reset the VM to have it launch from the ISO on boot.

If you have attach an ISO for initial guest OS install and reset the VM and it is not booting to the ISO you may need to set the boot order in the BIOs of the Virtual Machine just like you would on a physical server. POST occurs to quickly on a VM to hit the correct F key to launch the BIOs, instead, you can tell the VM to boot to BIOs, to do this select the desired VM and go to Edit Settings > Options Tab > Boot Options > Select Force BIOS Setup which will force the VM to go to BIOs on next boot.



Once in the BIOs, change the boot order as you would on any physical server, setting CD ROM as first boot priority.

Viewing Available VLANs

Changing Virtual Machine Names

OVFs and OVAs