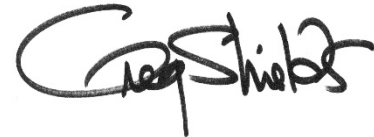


67 vSphere Tips & Tricks

Friday, November 18, 2016 12:10 PM

Notes to the Reader

- What you're currently holding are my notes for the TechMentor session noted above. As my notes, they're my own personal reminders about all the steps necessary to make our way through the demos. As I've been asked many times for these notes after this session, I provide them to you here as they are, warts and all. While I offer no support for them once the conference concludes, I wish you great success in building your own vSphere infrastructure!



The legal stuff...

THE CONTENT OF THESE NOTES IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT WITHOUT ANY WARRANTY. IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THIS CONTENT IS WITH YOU. SHOULD THEY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW THE AUTHOR WILL BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THIS CONTENT (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF THE AUTHOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Schedule

- 8:00am Workshop starts
- 10:00am 15 minute coffee break
- 12:00pm 1 hour lunch break
- 3:00pm 15 minute soda break
- 5:00pm Workshop ends

Preparation

vSphere Security Guide:

<https://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf>

Create and expose a LUN for later use as an RDM attached to VM1.

Login is administrator@vsphere.local, password is 123456Ab!

Create empty VM (for Auto Deploy) with these configs:

- VMware ESXi 6 OS
- 8GB RAM
- 1x4 vProc
- HD1, 250GB
- HD2, 1TB
- HD3, 512GB
- HD4, 256GB
- NIC1,2 - Bridged (vmnet0)
- NIC3,4,5,6 - vmnet1
- NIC7,8 - vmnet2

Introduction

#1 - Never trust a conference title that advertises 67 tips.

- Start by explaining that I've built a fully-functional and fully-production-ready vSphere infrastructure with which to work with.
- Mention that this *could* be a lab class as well, with a twist: That being that "the lab" in this case is actually your environment back at home. Consider remoting to it and following along. You'll see here that I won't be making all that many actual configuration changes, since this is an already-built environment, so for most of these demos you can follow along with your own hardware.
- Mention also that you'll be seeing a lot of old school ESXCLI commands. That's because this course was originally written as exam prep for the VCP exam, which focused a lot on ESXCLI. And, more importantly, the kinds of configs we're generally working with here are exposed via Get-EsxCli anyway, which is essentially a refactoring of ESXCLI. So, this'll help you understand the primitive commands that PowerCLI wraps around.

Security, Module 2

#2 - Grok vSphere Role-based Access Control

- SHOW ONE SLIDE
- **Global Permissions:** Global permissions are applied to a global root object that spans solutions. To assign permissions via global root allows to propagate them to the other products relying on SSO (vCO, vROPS, vCD..)
- **vCenter Server Permissions:** Hierarchical model. Permission gives you a certain number of privileges like in Microsoft's AD. You Select object > assign role to a group of users > to give them privileges on that object.
- **Group Membership in vSphere.local Groups:** The vsphere.local domain includes several predefined groups. Assign users from AD (if you're using AD) to one of those groups to be able to perform the corresponding actions. For some services that are not managed by vCenter Server directly, privileges are determined by membership to one of the vCenter Single Sign-On groups. For example, a user who is a member of the Administrator group can manage vCenter Single Sign-On. A user who is a member of the CAAadmins group can manage the VMware Certificate Authority, and a user who is in the LicenseService Administrators group can manage licenses.
- **ESXi Local Host Permissions:** If you are managing a standalone ESXi host that is not managed by a vCenter Server system, you can assign one of the predefined roles to users. There are only three default roles in ESXi host alone: No Access, Read-Only, and Administrator. These cannot be changed, but you can create custom roles.
- SHOW PERMISSIONS INHERITANCE - vSphere Security Guide, page 116
- SHOW APPROPRIATE PRIVILEGES FOR COMMON TASKS - Same document, page 127

Security, Module 3

#3 - Customize the ESXi Firewall

- ESX1 | Manage | Settings | Security profile > Firewall
- Check which services are active through the firewall
- esxcli network firewall ruleset list
- Open a firewall port for a specific service

- esxcli network firewall ruleset set -e true -r httpClient
- Create a custom firewall rule
 - cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak
 - chmod 644 /etc/vmware/firewall/service.xml
 - chmod +t /etc/vmware/firewall/service.xml
 - (Modifies access perms and toggles "sticky bit" flag)
 - vi /etc/vmware/firewall/service.xml
 - (Remember that "j" goes down a line and "G" goes to end of document)

```
<service id="0051">
<id>MyService</id>
<rule id='0000'>
  <direction>outbound</direction>
  <protocol>tcp</protocol>
  <porttype>dst</porttype>
  <port>10000</port>
</rule>
<enablei<d>true</enabled>
<required>>false</required>
</service>
```

```
cat /myfile
cat /myfile.xml >> /etc/vmware/firewall/service.xml
MAKE SURE TO REARRANGE closing XML brackets!!!
```

#4 - Enable Lockdown Mode (or Don't)

- This can be done in vSphere Client or ESXi DCUI.
- Hosts and Clusters | Host | Manage | Settings | System | Security Profile
- Disabled – Lockdown mode is disabled.
- Normal – Lockdown mode is enabled. The host can only be accessed from vCenter or from the console (DCUI).
- Strict – Lockdown mode is enabled. The DCUI service is stopped. The host cannot be accessed from the console (DCUI).
- NOTE -- Exception Users: New to lockdown mode in vSphere 6 is the implementation of Exception Users. Users added to the exception list do not lose their permissions or privileges when an ESXi host is placed into Lockdown Mode. Exception Users can only be added/configure via the vSphere Web client.

#5 - Restrict Access to the Managed Object Browser

- The Managed Object Browser, or MOB, is a Web-based server application available for all ESX/ESXi and vCenter Server systems. The MOB lets you examine the objects that exist on the server and navigate through the hierarchy of live objects by clicking on links. The MOB populates the browser with actual runtime information, for example, the names of properties.
- MOB is found at <http://vcenter.company.pri/mob>
- Disabled by default in vSphere 6
- Browse host | Manage tab | Settings | Advanced System Settings.
- Select the Config.HostAgent.plugins.solo.enableMob option and click Edit to enable or disable

the Managed Object Browser.

#6 - Download and Auto-Trust vCenter Server Certificates

- EXPLAIN THIS:
- vCenter Server comes equipped with its own certificate authority called VMCA
- You can install the root certificate of VMCA in your system or browser
- All vSphere components like vCenter, ESXi, solution users, etc can be issued certificates from VMCA if running in Default or Enterprise mode
- VMCA can be bypassed if you don't want to use it, however you'll need to do more steps to manage your certificates
- Regardless of which method, all certificates need to be installed into VECS (VMware Endpoint Certificate Store) with the exception of ESXi hosts.
- A Certificate Manager tool is provided to help you manage your 3rd party certificate installations
- VIEW CERTIFICATES: Administration -> System Configuration -> Nodes -> Node -> Manage -> Certificate Authority

ADD SELF-SIGNED CERT AS TRUSTED ROOT

- Navigate to <https://vcenter.company.pri/>
- Click on "Download trusted root CA certificates"
- Rename "download" to "download.zip"
- .0 file is root cert
- .r0 file is CRL
- Add .0 file to Chrome trusted root certification authorities

Security, Module 4

#7 - Harden SSO Authentication Policies

- FIRST, SHOW AUTHENTICATION METHODS:
 - Administration > Single Sign-On > Configuration > Identity Sources
- ATTEMPT TO CONFIGURE A NEW AUTH SOURCE:
 - Administration > Single Sign-On > Configuration > Identity Sources > "+" sign
 - Add AD as identity source.
- CONFIGURE POLICIES:
 - Administration > Single Sign-On > Configuration Policies | Password Policy, Lockout Policy, Token Policy

#8 - Respect When to Scale Out vCenter and its PSC (PSC and multi-site)

- SHOW SLIDE BUILD
- PSC Deployment Options – A two different type installation are allowed:
 - Embedded (in the same VM): The embedded PSC is meant to be used for standalone sites where vCenter server will be the only SSO integrated solution. In this case a replication to another PSC is not necessary.
 - External: External PSC shall be deployed in environments where there is more than one SSO enabled solution (vCenter Server, vRealize Automation, etc...) OR where replication to another PSC (another site) is necessary.

#9 - Regenerate Out-of-Box vSphere Certificates with Internal PKI

- Introduce the notion that some of us might have internal PKIs (or may be watching my other session on ADCS), or may have a subordinate PKI from a publicly-trusted PKI.
- In any of these cases, one super-easy solution is to just make vCenter a subordinate PKI. Doing so lets it automatically generate (and keep current) all the necessary certificates required by vSphere's services and components.
- I am doing a video here because this is a complex build that a) would take a long time doing here live, and b) must be done exactly correctly for all our later demos to work.
- **SHOW VIDEO #1 - "REPLACE VMCA CERTIFICATES"**
 - **Stop at roughly 14:15.**
- After video is done, show Administration -> System Configuration -> Nodes -> Node -> Manage -> Certificate Authority

Networking, Module 2

#10 - Migrate to vSphere Distributed Switches (if you can afford them)

- SHOW SLIDE BUILD

#11 - Aim Towards Full Network Redundancy; Aim Towards Network Convergence

- SHOW SLIDE BUILD
- Explore current configuration on VCENTER

Networking, Module 3

#12 - Understand the Impact of dvPortGroup Policies

- Common vSS and vDS Policies
 - Security
 - Traffic shaping
 - VLAN
 - Teaming and failover
 - Monitoring
 - Traffic filtering and marking
 - Miscellaneous
- Port Binding
 - Static binding (default, recommended)
 - When you connect a virtual machine to a port group configured with static binding, a port is immediately assigned and reserved for it, guaranteeing connectivity at all times. The port is disconnected only when the virtual machine is removed from the port group. You can connect a virtual machine to a static-binding port group only through vCenter Server.
 - Dynamic binding
 - In a port group configured with dynamic binding, a port is assigned to a virtual machine only when the virtual machine is powered on and its NIC is in a connected state. The port is disconnected when the virtual machine is powered off or the NIC of the virtual machine is disconnected. Virtual machines connected

to a port group configured with dynamic binding must be powered on and off through vCenter.

- Dynamic binding can be used in environments where you have more virtual machines than available ports, but do not plan to have a greater number of virtual machines active than you have available ports. For example, if you have 300 virtual machines and 100 ports, but never have more than 90 virtual machines active at one time, dynamic binding would be appropriate for your port group.
- Dynamic binding is deprecated from ESXi 5.0, but this option is still available in vSphere Client. It is strongly recommended to use Static Binding for better performance.
- Ephemeral binding
 - In a port group configured with ephemeral binding, a port is created and assigned to a virtual machine by the host when the virtual machine is powered on and its NIC is in a connected state. When the virtual machine powers off or the NIC of the virtual machine is disconnected, the port is deleted.
 - You can assign a virtual machine to a distributed port group with ephemeral port binding on ESX/ESXi and vCenter, giving you the flexibility to manage virtual machine connections through the host when vCenter is down. Although only ephemeral binding allows you to modify virtual machine network connections when vCenter is down, network traffic is unaffected by vCenter failure regardless of port binding type.
 - Ephemeral port groups must be used only for recovery purposes when you want to provision ports directly on host bypassing vCenter Server, not for any other case.
- Security Policies
 - Promiscuous mode (default: Reject) – If set to Accept then it allows the guest OS to receive all traffic observed on the connected vSwitch or PortGroup. Enabling essentially converts the switch into a hub, with all the associated inconveniences, packet collisions, performance degradation, and whatnot.
 - MENTION PORT MIRRORING (Single-click dvSwitch, then select Port Mirroring)
 - MAC address changes (default: Reject) – A host is able to accept requests to change the effective MAC address to a different address than the initial MAC address.
 - Classic use case: NLB Cluster in Unicast mode.
 - Forged transmits – A host does not compare source and effective MAC addresses transmitted from a virtual machine. By default it's Accept
 - Classic use case: NLB Cluster in Unicast mode.
 - Another use case: Nested virtualization.
 - CURIOSLY, AND I DIDN'T KNOW THIS (NOR HAVE I CONFIRMED IT)
 - MAC address changes and forged transmits are also used by Windows as a mechanism to protect against duplicate IP addresses on the network. If a Windows system detects an IP address conflict it will send out a forged transmit to reset the IP to the original MAC of the machine it think originally owned it and then take itself off the network. This protection mechanism for duplicate IP addresses won't work without these security settings allowed.
 - This may only be the case in older OSs.
- Traffic Filtering and Marking
 - Traffic Filtering policy engine allows for creation of ACLs, as well as to tag traffic and pass Quality of Service (QoS) or Differentiated Services Code Point (DSCP) values up to the physical network for prioritization.
 - ACL's allow you to create fine grain control of what traffic is allowed in or out of a VM, set of VM's or an entire port group. The feature is configured at the port group level

and allows for an unlimited number of rules. The rules are processed in the VMkernel, meaning no external appliance is needed which equates to no single point of failure and faster processing of rules and in some cases reduced network traffic since rule processing happens before the traffic leaves the ESXi host.

- Load Balancing and Failover Policies
 - SHOW SLIDE BUILD

#13 - Recognize the Locations where VLANs can be (mis)Configured

- Location #1: On the pNIC Uplink
- Location #2: On the dvPortGroup
- SHOW SLIDE BUILD

Storage, Module 2

- Start with a review of the storage configuration in the demo environment.

#14 - Understand Storage Naming Conventions

- SHOW SLIDE BUILD
- The EUI format takes the form eui.16 hex digits. The 16-hexadecimal digits are text representations of a 64-bit number of an IEEE EUI (extended unique identifier) format. The top 24 bits are a company ID that IEEE registers with a particular company. The lower 40 bits are assigned by the entity holding that company ID and must be unique.
- To display device names in vSphere CLI
- esxcli storage core device list

#15 - Respect the Differences Between Array and Virtual Disk Thin Provisioning

- SHOW SLIDE BUILD

#16 - Ain't Nuthin' Wrong with Renaming your iSCSI IQNs

- ESX1 | Storage | Storage Adapters | iSCSI Software Adapter | Properties | Edit

#17 - Understand (but don't) Disable vCenter Server Storage Filters

- SHOW SLIDE BUILD
- Administration | vCenter Server | Settings | Advanced Settings | Add filter key

Storage, Module 3

#18 - Differentiate Storage Multipathing Policies

- Storage | VMFSDatastore1 | Connectivity and Multipathing | ESX1 | Edit Multipathing
- SHOW SLIDE BUILD

#19 - Understand vSphere's Pluggable Storage Architecture

- All of these policies are encapsulated into this infrastructure we call the PSA.
- Notice here how there's this almost Plug-and-Play sense of automatically identifying new storage and "claiming" it with a certain multipathing policy. This entire process is handled through what is called the Pluggable Storage Architecture, and you need to know it if you plan to customize much past what you see here so far.
- SHOW 1ST HALF OF SLIDE BUILD
- PSA is a component of the vmKernel. It sits inside the vmKernel. It facilitates some out-of-box rules for auto-claiming storage and establishing load balancing policies, as well as defining APIs that 3rd parties can use to develop their own rules/policies.
 - NMP = Native Multipathing Plugin.
 - SATP = Storage Array Type Plugin. Handles failover for given storage arrays and to determine failover types for any particular LUN. VMware provides generic SATPs for different kinds of storage, as well as a Local SATP for local storage as well.
 - PSP = Path Selection Plugin. Handles the actual path selection for every given IOPS. Here within the PSP is where you'll find the MRU, Fixed, and RR policies.
 - MPP = Multi-Pathing Plugin. A framework for 3rd parties to code their own logic for how servers connect to storage and how that connection is balanced. You use the MPP only if your storage hardware specifically includes its own MPP.
- For every type of storage, you will choose (or it will be auto-chosen for you) an SATP and a PSP. The differences in SATP policies will depend on the kinds of feature sets your storage array will provide. The differences in PSPs have to do with the rules we discussed earlier.

#20 - Respect What Changes when you Change PSPs and SATPs

- Login to ESX1.
- `esxcli storage nmp satp list`
 - Shows the list of SATPs and their linked PSPs that're in the NMP.
 - DEFAULT_AA is for "active/active" storage, typically for iSCSI/FC.
 - DEFAULT_AP is for "active/passive" storage
 - LOCAL storage uses a fixed policy
 - Others relate to specific types of storage, like an HP EVA, an EMC Symmetrix, etc.
- `esxcli storage nmp psp list`
 - Shows the three policies in-box with the NMP.

#21 - Customize Storage Claim Rules

- **SHOW VIDEO #2 - "CUSTOMIZE STORAGE CLAIM RULES"**
- Mention that to change a PSP association with an SATP uses the command:
 - `esxcli storage nmp satp set -s VMW_SATP_INV -P VMW_PSP_RR`
 - `esxcli storage nmp satp list`
- Once the policy is changed, a further step is necessary to reclaim any existing devices against the new policy.
 - `esxcli storage nmp device list`
 - Locate the device NAA number for the MSFT iSCSI disk
 - `esxcli storage core claiming reclaim <naa.number>`

#22 - Extend the Windows Timeout for Delayed Write Operations

- HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > Disk > TimeoutValue = 60 (decimal)
- Do this in the VM.
- After you make this change, Windows waits at least 60 seconds for delayed disk operations to

- complete before generating errors.
- iSCSI takes a bit longer than FC to failover.
- NFS storage (or, really any non-block storage) takes even longer. Like "many seconds" longer.

#23 - Understand the Use Case and Behavior of Non-Optimized Storage Paths (e.g. ALUA)

- SHOW SLIDE BUILD

Storage, Module 4

#24 - Avoid the NFS3 Gotcha (include the "differentiate v3/v4.1 capabilities" slides)

- SHOW SLIDE BUILD
- In "mixed" environments, it is generally best to run NFS v3 everywhere.
- You should not mix NFS v3 with NFS v4.1 on the same volumes/datastores. This is because the two protocols versions use different locking mechanisms.
- Use LACP for port aggregation and link redundancy. LACP can combine multiple physical interfaces into a single logical interface; however, it is debatable whether this improves throughput/performance. Still limited to a single connection with NFS version 3. You will have several NFS workers when you run with multiple ESXi hosts, so they get balanced over the links. Many NFS-array vendors support this feature at the storage controller port level.

#25 - Avoid the "Upgraded VMFS5 Volume" Gotcha

- Properties of VMFS1Datastore | Show (greyed out) Upgrade to VMFS-5 right-click context menu link
- SHOW SLIDE BUILD

#26 - Know Your RDMs and their Sharing (includes bus sharing)

- We're talking about the use of RDMs for guest clustering here (with the bus sharing portion). This is equivalent to Shared VHDX/VHD Sets in Hyper-V
- SHOW 1ST HALF OF SLIDE BUILD
- Properties of VM1 | New RDM Hard Disk
- SHOW 2ND HALF OF SLIDE BUILD

Storage, Module 5

#27 - Configure Storage Policies Using Tags

- The whole point behind Storage Policies is that while you're the vCenter admin, you're not necessarily the person who is creating all the VMs for every consumer. Yes, you might in the beginning, but as you move to more automation, you as vCenter admin want to create an environment that allows others to create their own VMs (and, thus, each VM's disks) within a predetermined framework.
 - Properties of VM1 | Add New Hard Disk | VM Storage Policy
 - You as the vCenter admin can create a policy that dictates what kinds of disks some other administrator can create in your infrastructure.
- Storage Policies are a combination of vendor intelligence (VASA, vSphere APIs for Storage Awareness [VASA]) that is delivered by a Storage Provider and/or administrator-set "tags" on

storage.

- Storage Providers are like a Rosetta stone / universal translator for the storage "primitives" that any array supports.
- VMware provides an in-box VASA provider for VSAN.
- We begin by talking about creating a static tag on storage.
- Configure a tag on the iSCSI "VMFSDatastore" called "iSCSI Storage"
 - The user wouldn't necessarily know if this is iSCSI Storage or GOLD Storage or High Performance Storage, or whatever.
 - Discuss how tags are static and admin-handled.
- Home | VM Storage Policies | Create a Storage Policy | Name = "iSCSI Storage"
 - Go back to VM. Attempt to add a new hard disk and apply Storage Policy.

#28 - Configure Storage Policies Using VASA

- VSAN's VASA facilitates five different rules:
 - Number of disk stripes per object
 - (e.g. How disks get striped across nodes in a VSAN "cluster")
 - Flash read cache reservation (%)
 - (e.g. How much SSD space is guaranteed for the VM's use)
 - Number of failures to tolerate
 - Force provisioning
 - (e.g. provision a VM, even if it doesn't meet the capabilities)
 - Object space reservation (%)
 - (e.g. use thick provisioning instead of default thin provision)
- Home | VM Storage Policies | Create a Storage Policy | Name = "Thick-Provisioned Storage"
 - NOTE: We do this example because the default with VSAN is thin provisioned VMs
 - Configure object space reservation (%) to 100%.
- Home | VM Storage Policies | Create a Storage Policy | Name = "Reserved Flash Read Cache"
 - Configure Flash Read Cache (%) to 10%
- Finally, monitor for compliance:
 - Home | VM Storage Policies | <Choose a Policy> | Monitor
 - Properties of VM | VM Policies | Check VM Storage Policy Compliance

#29 - Use VSAN Fault Domains!

- SHOW SLIDE BUILD
- Hosts and clusters | Cluster | Manage | Settings | Virtual SAN | Fault Domains

#30 - Prepare for (but maybe don't [yet] use) VMware VVOLs

- SHOW VAAI SLIDE BUILD
- SHOW VASA SLIDE BUILD
- SHOW VVOL SLIDE BUILD
- VVOLs start with basically a bidirectional VASA capability, where VMs tell the underlying storage what performance, features, and capabilities they require. The storage array automatically creates VMDKs on itself to match those demands.
- Remember that VASA is intended to facilitate a mechanism to apply policies to storage. However, in its first iteration, the policies were applied by administrators and vSphere. With

VVOLs, the policies are transparently applied by the storage layer itself.

Resources, Module 2

#31/#32/#33 - Get Really (really, really) Familiar with Reservations, Shares, and Limits

- SHOW SLIDE BUILD

#34 - Avoid the Memory Reservations Gotcha

- SHOW SLIDE BUILD

#35 - Avoid the CPU Shares Gotcha

- SHOW SLIDE BUILD

#36 - Resource Pools are not Folders! Folders are not Resource Pools!

- SHOW SLIDE BUILD

#37 - Avoid the Resource Pool Gotcha

- SHOW SLIDE BUILD

#38 - Avoid the Flexible Reservations Gotcha

- SHOW SLIDE BUILD
- IMPORTANT NOTE: A Resource Pool with an expandable reservation can "borrow" from its parent only to satisfy a reservation, not to satisfy a request for resources in excess of those reservations. Without this checked, Admission Control will pop an error when you attempt to reserve more than is available (or power on a VM) when all resources are spoken for.

#39 - Implement a vFlash Resource Pool (or don't)

- If you're doing a lot of writes, vFlash doesn't help you very much because vFlash only accelerates disk reads.
- vFlash and VSAN are incompatible. The reason for this makes a lot of sense, as VSAN includes a read cache already.
- vFlash is designed for getting that same kind of acceleration you get with VSAN, but with remote storage.
- ESX1 > Manage > Settings > Virtual Flash Read Cache Resource Management > Add capacity
- Must then manually enable vFlash RC on each VM.
 - Properties of VM's hard disk
- VMware is moving forward with new Framework called VAIO. VMware VAIO stands for "vSphere APIs for IO Filtering". It's a new API framework technology present in vSphere 6.0 (6.0 U1 more precisely) allowing vendors to present capabilities for caching and replication to individual VMs. It's a framework, not feature. VAIO can be used not only caching but also for replication.
- VAIO would/is exposed via Storage Policies

#40 - (Don't) Implement a vFlash Host Swap Cache

- Used only when you're in a swap situation, and you should never get there anyway. If you ever get to swapping, you've done something wrong.
- This cache would only ever be addressed after **every other** possible pre-swap capability were exhausted first: Memory ballooning, page table sharing, etc.
- ESX1 > Manage > Settings > Virtual Flash Host Swap Cache Configuration

Resources, Module 3

#41 - Understand Why and Where to Implement Network I/O Control

- SHOW SLIDE BUILD
- NIOC is really designed around enforcing limits in converged scenarios, where many different types of traffic are passing through the same set of pNICs.
- Can set Reservations and Limits on system traffic. Can set only reservations on network resource pools.
- Network > Production-Dswitch > Edit Settings > Advanced
 - Show that NIOC is enabled by default
- Network > Production-Dswitch > Resource Allocation

Resources, Module 4

#42 - Understand Why and Where to Implement Storage I/O Control

- SHOW SLIDE BUILD
- Anytime you're running multiple VMs on the same storage frame, the activities of each individual VM can impact the total performance and behavior of all those surrounding that VM on the storage/in the LUN/on the volume. This is a problem because there hasn't traditionally been a really good way to surface alerts regarding this behavior to vSphere. The storage frame knows what's going on, but the VMs and vCenter doesn't.
- The further problem is that each different storage frame speaks a different language, and so trying to integrate this into vCenter is a difficult problem.
- SIOC attempts to do a best-effort attempt at detecting storage contention problems waaaaay deep down at the storage layer by gauging behaviors on VMs from the top looking down.
 - This is a bit like the Kepler program and it's finding of exosolar planets: We aren't observing the planets directly, but rather indirectly by how they interact with their host star.
 - Two measurements:
 - Latency, e.g. "How long does it take for a VM storage request to complete?"
 - This is something that's easy to measure. Just make a request and then see how long it takes to complete that request. Keep a running log of that timing and then alert when the time across any/all/configured VMs starts slowing down.
 - Peak throughput, e.g. "How much throughput do I get when I make a request?"
 - Accomplished through an "I/O Injector" that injects I/O into the connection as a known quantity with the goal of seeing how that known quantity behaves.
- Storage | VMFSDatastore1 | Settings | General | Datastore Capabilities | Edit
 - Some published starting values for manual settings:
 - 10ms for all SSD storage
 - 30ms for traditional spinning 10K/15K SAS disks
 - 50ms for traditional spinning 7200 SAS disks

- 30ms for auto-tiering solutions
 - YMMV! Must validate this against any config.
- Be aware that this configures a level playing field for all VMs. Need to adjust this for any VMs that need extra/less IOPS.
 - Properties of VM | Properties of Hard Disk | Shares or Limit IOPS

Availability, Module 2

#43 - Avoid Inadvertently Exploding Yourself with vSphere HA Admission Control

- First, show Admission Control Policies for HA
- SHOW (LONG) SLIDE BUILD

#44/#45 - Grok VM Component Protection and VM Monitoring Settings for HA

- Properties of Cluster1 | vSphere HA

#46 - Configure a Separate Network for HA Heartbeats

- SHOW SLIDE BUILD
- Show configurations in dvPortGroup networking

#47 - Configure Another vSphere HA Isolation Addresses

- Properties of Cluster1 | vSphere HA | Advanced Options
- das.isolationaddress0 = 192.168.0.10
 - Can have up to 10(?) addresses
- das.usedefaultisolationaddress = false

#48 - Avoid the Heartbeat Datastore Configuration Oops

- Properties of Cluster1 | vSphere HA | Datastore for Heartbeating
 - The oops is essentially: "Make sure all hosts have a path to the heartbeat datastore."

#49 - Respect the Complex Interplay Between HA, DRS, and DPM

- SHOW SLIDE BUILD

Availability, Module 3

#50 - (Really, Really, Really) Understand vSphere DRS Automation Levels

- SHOW SLIDE BUILD

#51 - Don't (or do) Configure vSphere DRS Affinity Rules

- SHOW SLIDE BUILD

#52 - Configure for Multiple-NIC vMotion

- SHOW ONE SLIDE
- CAUTION: Be aware that while NIOC can limit the outbound traffic coming out of a cluster, it has no bearing on the inbound traffic reaching the other side. If multi-NIC vMotion is setup between two different datacenters (long-distance), the raw throughput of data can

overwhelm the servers receiving traffic.

- NICs for multi-NIC vMotion are configured much the same way as iSCSI NICs.
 - Create multiple vmKernel interfaces and bind a separate IP to each.
 - Bind each interface to a single uplink WITH NO FAILOVER.

Deploy, Module 3

#53/#54/#55/#56 - Create, Customize, Attach, and Scan a vSphere Host Profile

- NOTE: A FULLY-COMPLIANT HOST PROFILE HAS BEEN CREATED AS A BACKUP.
- Create a Host Profile
 - Create a profile from ESX1
 - Show configurations that have been captured into Host Profile.
 - Remove all configurations.
 - Attach profile to ESX1
 - Check for Host Profile Compliance (this should work).
- A DESIGN (FLAW) PECULARITY: While VMware has designed Host Profiles to "check all the boxes" at first. This means that we care about all the settings being captured by a profile. Better idea to start small with just a few configurations and work your way up.
- Customize a Host Profile
 - This first example obviously doesn't get you very far, as networking, storage, and security settings are all generally things you want to control. In order to control them, we need to customize the profile by adding in what configs we're interested in.
 - Edit host profile settings and add some checkboxes
 - General System Settings | Console Configuration | DCUI Keyboard = US
 - Security and Services | Firewall | Firewall | Ruleset = Enable everything
 - Other settings are unique to each host. These are called "customizations".
 - Edit host profile settings again and enable Storage configuration | iSCSI Initiator Configuration.
 - Note that this now exposes customizations that need to be configured for each host.
 - iSCSI initiator Alias (must enter a unique value)
 - IQN
 - Disable the adapter
 - Do not complete the wizard. Step back to edit Host Profile.
 - Even others can be added if they're not already on the host, as in "Host Profiles can make the configuration for us".
 - General System Settings | Core Dump and Date and Time Configuration
 - For Date and Time | NTP, show that time settings can be hard-coded or configured as a "customization".
- Attach and Scan a Host Profile
 - Perform a compliance scan against the now purposely-invalid configuration.
 - Note that scan shows noncompliant.
 - Click "ESX1" to view the summary and noted failures.
 - Click to remediate the host.
- ****NOTE HERE****: Previous versions always required a host to enter maintenance mode in order to complete a remediation. Now, only fixes that require maintenance mode will force it.

VERY IMPORTANT!!!!!!!!!!!!!!!!!!!!!!

Remind also that vSphere Fat Client is very helpful (in this version) for troubleshooting why Host Profiles behave strangely -- which they often will, particularly if hosts aren't configured exactly the same as each other (vmk interfaces, vmnics, claim rules, etc.).
VERY IMPORTANT!!!!!!!!!!!!!!!!!!!!!!

#57 - Modify Network Configurations with a Host Profile

- Networking configuration | NetStack Instance | defaultTcpIpStack | DNS Configuration =
 - Change "host name" to "user specified host name to be..."
 - Enable the setting.
- SHOW THIS:
<https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.install.doc/GUID-C96915A0-FEED-48AC-9163-D94AAD43A3FB.html>
- Networking configuration | Host virtual NIC | Production-DSwitch | IP Address Settings =
 - Change "IPv4 address" to "user specified host name to be..."
 - Enable the setting.
- Click Next | Show how the hosts can now be customized.
- Show/discuss everything under "Network configuration" | Enable everything.
- Rerun the compliance verification.

#58 - Modify Storage Configurations with a Host Profile

- Storage configuration | VSAN Configuration = Select all
- Storage configuration | iSCSI Initiator Configuration = Select all
- Storage configuration | Pluggable Storage Architecture = Select all
- Native Multi-Pathing (NMP) | PSP and SATP Configuration for NMP devices = Select all
- Native Multi-Pathing (NMP) | Storage Array Type Plugin (SATP) Configuration | SATP default PSP configuration = Select all
- Native Multi-Pathing (NMP) | Storage Array Type Plugin (SATP) Configuration | SATP claimrule = (the "MyVendor/MyModel" one (the other LOCAL one seems to be the busted one))
- NOTE HERE: EVERY CHECKBOX (EXCEPT THE WEIRDO ONES THAT WON'T STAY CHECKED) SHOULD BE CHECKED IN THIS HOST PROFILE EXCEPT FOR:
 - Storage | NMP | SATP | SATP Claimrule
- Show how the claimrule we created on one host can now be remediated on the other hosts.

Deploy, Module 4

#59 - Grok the Architecture of Auto Deploy

- SHOW SLIDE BUILD
- SHOW DHCP console for DC | Scope Options
- SHOW "vSphere Auto Deploy Waiter" service on VCENTER
 - Note that this looks a little different if you're working with the VCSA where (I think) it is enabled by default.
- SHOW vSphere Web Client | vcenter.company.pri | Manage | Settings | Auto Deploy | Download TFTP
- Show WDS server
 - EXPLAIN: Remove F12 requirement at boot
 - TFTP file is uploaded to become boot file ([\\VCENTER\C\\$\RemoteInstall](#))
 - MENTION REGISTRY HACK
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WDSServer\Providers\WDSTFTP\ReadFilter | Add "*" to existing value at this key to open

- WDS to all inbound client requests.
- Attempt to boot VM | Watch this fail (We need to configure image profile).

#60 - Locate the VMware Online Software Depot (the not-GUI way)

- SHOW vSphere Fat Client | VMware Update Manager | Configuration | Download settings
- These settings show where to locate the Software Depot.
- Set Execution Policy to RemoteSigned.
- Launch PowerCLI (AS AN ADMINISTRATOR!)
- Connect-VIServer -Server vcenter.company.pri -Protocol https -User administrator@vsphere.local -Password 123456Ab!
- Add-EsxSoftwareDepot
<https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml>
- Get-EsxImageProfile
 - (WARNING: THIS WILL THROW AN ERROR. MUST BOUND THE RESULTS)
- Get-EsxImageProfile -Name "ESXi-6*"
- Get-EsxImageProfile -Name "ESXi-6*" | ft name
- Get-EsxImageProfile -Name "ESXi-6*" | sort name | ft name
 - ESXi-6.0.0-2494585-standard.zip is the final full package for v6.0

#61 - Create an ESXi Image Profile and Deployment Rule

SHOW ONE SLIDE

- Connect-VIServer -Server vcenter.company.pri -Protocol https -User administrator@vsphere.local -Password 123456Ab!
- Add-EsxSoftwareDepot
<https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml>
- Get-EsxImageProfile -Name "ESXi-6*" | ft name
- Export-EsxImageProfile -ImageProfile ESXi-6.0.0-2494585-standard -ExportToBundle -FilePath C:\ImageProfiles\ESXi-6.0.0-2494585-standard.zip
 - <<This takes a while. Should be done prior to start of session.>>
- Get-EsxSoftwareDepot | Remove-EsxSoftwareDepot
- Add-EsxSoftwareDepot C:\ImageProfiles\ESXi-6.0.0-2494585-standard.zip
- New-DeployRule -Name "Install" -item "ESXi-6.0.0-2494585-standard" -pattern "ipv4=192.168.0.130-192.168.0.180"
 - <<This takes a while. Should be done prior to start of session.>>
- Add-DeployRule -DeployRule Install
 - Show example machine ESX4 that has been created with the same configuration as the others.
 - Same network, same storage, etc.
- Boot the machine and see if it begins an installation.

#62 - Tune and Implement Host Profiles for Auto Deploy

- **IMPORTANT:** MUST MAKE A CHANGE to Host Profile we created in the last module.
 - Networking configuration | Host virtual NIC | <each dvSwitch> | Determine how MAC address for vmknics should be decided | SET TO "use the MAC address from which the system was PXE booted".
- Get-VMHostProfile
- \$img = Get-EsxImageProfile
- New-DeployRule -Name "Full Host Profile" -item \$img, "Full Host Profile", cluster1 -pattern "ipv4=192.168.0.130-192.168.0.180"

- Add-DeployRule -DeployRule "Full Host Profile"
- Get-DeployRule
- Get-DeployRuleSet -Active
- SHOW THE FOLLOWING, BUT DON'T NECESSARILY CONFIGURE
 - Configure DHCP Reservation for vmnic0
 - Configure DNS records for reserved address
 - Configure IQN name for iSCSI
 - iqn.1998-01.com.vmware:esx5-5555555
 - No need to worry about these. Just here for capture.
 - Storage - 192.168.1.140, 192.168.1.150
 - Storage2 - 192.168.1.141, 192.168.1.151
 - vMotion1 - 192.168.2.141, 192.168.2.151
 - vMotion2 - 192.168.2.142, 192.168.2.142
 - VSAN - 192.168.1.241, 192.168.1.242
- MENTION Stateful Install vs. Stateless Caching
 - Properties of Host Profile | Advanced | System Image Cache Configuration

#63 - Deploy an ESXi Host with Auto Deploy

- **SHOW VIDEO #3 - Deploy an ESXi Host with Auto Deploy**

#64 - Customize ESXi Images for Auto Deploy

- What we're doing here is updating the VIBs that correspond to the core of ESX itself, esx-base.
- Connect-VIServer -Server vcenter.company.pri -Protocol https -User administrator@vsphere.local -Password 123456Ab!
- Add-EsxSoftwareDepot C:\ImageProfiles\ESXi-6.0.0-2494585-standard.zip
- Get-EsxSoftwarePackage
- Get-EsxSoftwarePackage -Name esx-base
 - Note the version number (6.0.0-0.0.2494585)
- Get-EsxSoftwareDepot | Remove-EsxSoftwareDepot
- Add-EsxSoftwareDepot <https://hostupdate.vmware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml>
- Get-EsxImageProfile -Name "ESXi-6*"
- Get-EsxSoftwarePackage -Name esx-base
- Get-EsxSoftwarePackage -Name esx-base -Version "6*"
 - Note this much-newer version number (6.0.0-2.52.4600944)
- Get-EsxImageProfile -Name "ESXi-6*"
- Get-EsxImageProfile -Name ESXi-6.0.0-2494585-standard
- \$myprofile = Get-EsxImageProfile -Name ESXi-6.0.0-2494585-standard
- New-EsxImageProfile -CloneProfile \$myprofile -Name "Greg's Image Profile" -vendor "Pluralsight"
- Get-EsxSoftwareDepot
 - Note that the previous action didn't update the online depot. It created something local. Now, let's add in a more-recent copy of ESXi. Let's pick one that's relatively new, like this version 6.0.0-1.29.3568940. Some of the later versions have further dependencies that complicate our storyline here, so we'll do what's just simple.
- Add-EsxSoftwarePackage -ImageProfile "Greg's Image Profile" -SoftwarePackage "esx-base 6.0.0-1.29.3568940"
 - Yes, that's a space between "esx-base" and the version number.
- Export-EsxImageProfile -ImageProfile "Greg's Image Profile" -ExportToBundle -FilePath c:

\ImageProfiles\Updated.zip

- <<This takes a while. Should be done prior to start of session.>>
- Once downloaded, then you can take a look at the VIBs in that ZIP file by adding it as a depot and listing all the packages.
- Get-EsxSoftwareDepot | Remove-EsxSoftwareDepot
- Add-EsxSoftwareDepot C:\ImageProfiles\Updated.zip
- Get-EsxSoftwarePackage
- Can also do this with 3rd party drivers
- Add-EsxSoftwareDepot <http://vibsdepot.hp.com/index.xml>
- Get-EsxSoftwarePackage -Vendor Hewlett-Packard

Finale

#65 - Tip Your Waiters and Waitresses

#66 - Remember the Number 5 when Filling out Evaluations

#67 - Have a Great TechMentor!

IP Addresses

Management-DPortGroup (vmk0, vmnic0, vmnic1)

esx1 - 192.168.0.21

esx2 - 192.168.0.22

esx3 - 192.168.0.23

Storage-DPortGroup (vmk1, vmnic2, vmnic3)

esx1 - 192.168.1.110

esx2 - 192.168.1.120

esx3 - 192.168.1.130

Storage2-DPortGroup (vmk2, vmnic2, vmnic3)

esx1 - 192.168.1.111

esx2 - 192.168.1.121

esx3 - 192.168.1.131

vMotion1-DPortGroup (vmk3, vmnic6, vmnic7)

esx1 - 192.168.2.111

esx2 - 192.168.2.121

esx3 - 192.168.2.131

vMotion2-DPortGroup (vmk4, vmnic6, vmnic7)

esx1 - 192.168.2.112

esx2 - 192.168.2.122

esx3 - 192.168.2.132

VSAN-DPortGroup (vmk5, vmnic4, vmnic5)

esx1 - 192.168.1.211

esx2 - 192.168.1.221

esx3 - 192.168.1.231

Replication-DPortGroup (vmk6, vmnic0, vmnic1)

esx1 - 192.168.0.25

esx2 - 192.168.0.26

esx3 - 192.168.0.27

STORAGE1

192.168.0.12

192.168.1.200

esx55-1 192.168.0.55

esx55-2 192.168.0.56

esx55-3 192.168.0.57

esx7 192.168.0.17

ops1 192.168.0.13

vccnode 192.168.0.32

vccserver 192.168.0.31

vcenter2 192.168.0.15

vcsa 192.168.0.34

vcsa55 192.168.0.35

vdp 192.168.0.37

vrops-ui 192.168.0.39

vrops-an 192.168.0.40

vcenter55 192.168.0.41