Virtual Design Master

Challenge 1 – Security Design

Secure Earth Data center environment from services/goods black market

Submitted by-Harshvardhan Gupta

7/6/2016

Table of Contents

1. Executive Summary

1.1.1 Project Synopsis

While we're planning and doing implementation for our new Earth Datacenter, behind the scenes someone modified Shipping manifest to defeat us. This one person on Earth, who has survived the apocalypse deep in the bowls of the SuperNaps, and they have managed to rig up satellite capabilities. One of our brand new datacenter, the closest drop and go datacenter for Earth has been taken over. While it has not disappeared from any monitoring it is no longer in anyone's direct control. Now we need to take back control, find out the culprit and put some processes with security measures to protect our Data from prying eyes of black market.

1.1.2 Intended Viewers

This document is specifically written for technical people responsible for deploying Datacentre in Earth and Moon. Put stringent check and maintain logbook of all the activities without fail. "if you don't write it down, it didn't happen"

1.1.3 Project Vision

To protect our confidential data from black market's prying eyes at all times on Earth and Moon Data center. Put processes and controls in place to audit the environment periodically to detect/prevent any Intrusion in the data center.

1.1.4 Project Requirements

Reference	Description
R001	Make datacentre completely secure
R002	Enable auditing of events/logs etc. for correlating intrusion, if any.
R003	Harden Processes and put change control methods in place
R004	Log retention period must be 90 days or more for further analysis
R005	Avg. detection time must be low, as we're dealing with critical software

1.1.5 Project Constraints

Reference	Description
C001	Operations Staffs are very less on both Sites.
C002	Limited resources available to do IR/RCA
C003	No prior experience available with staff on securing/protecting assets.
C004	Principle vendor support is not available, only Break/fix KB's available offline

1.1.6 Project Assumptions

Reference	Description
A001	Staffs are able to run some predefined command line and compare it with previous runs. Able to read and follow SOP.
A002	Data center has manned security 24x7 with two factor authentication access (card/retina scan).
A003	Satellites communication link is encrypted and works in dual ring fashion as fibre optic does.
A004	VMware vSphere vSOM license with Enterprise Plus ESXi hosts is available and RSA product installed for 2FA.
A005	CCTV monitoring is in place to do surveillance nearby datacentre location.

A006	HCI/Blade comes with Kensington Lock for additional Physical protection
A007	McAfee IPS VM Appliance must be installed and configured for IPS
A008	Staff knows how to do tasks like assigning tokens and configuring “stuff”in AuthMan.

1.1.7 Project Risks

Reference	Description
I001	Due to heavy Security focus Cost of implementation will increase four times
I002	Deliverable date will get extended, due to additional checks & configuration items.
I003	Computer systems will be accessible to lesser number of privileged staffs.

2. Security Design

2.1.1 Conceptual Design

Datacenter equipment will be assembled in moon, installed and hardened by Server build group, then inspected by Security experts (Logs will be maintained at all times with Signature of Individual). Once everyone is satisfied with all the tests scanned Log book copy will be attached with the server for future need. As this equipment will be shipped to different location, it’s equipped with Advanced iLO (integrated Lights out) feature which emits Radio and GPS signals of its location (accuracy 10 miles radius). Signals are encoded with cipher and can be decoded by Moon Security staff only.

Russian Soyuz module will be used for transportation and Engineer accompanies with equipment for first installation on earth and giving crash course to earth staff for future installation in different locations.

3. Security Consideration

3.1.1 For External Network Connectivity

Satellite links are of paramount importance, as it’s only medium of communication between Earth and Moon. Satellite links are using encrypted communication and works in a Ring fashion; if one satellite is unavailable/compromised then second one takes over from where first left and connection state won’t get lost. Satellite communication must restrict other frequencies or bands apart from being used for datacenter communication.

3.1.2 For Shipment of Goods

For Shipping Goods from Moon center, we use Russian Soyuz Module (tested hundreds of times). Shipment follows standard based process with very stringent document checks (Coordinate details/weight/height etc). Based on this information fuel requirements are calculated to keep Opex (cryogenic fuel is costly) under control. Once shipment arrives at the destination, search party on earth finds the module, it recovers goods. If soyuz deviates from its itinerary then Engineer within module can start drifting soyuz by himself and reach at correct location.

3.1.3 For Datacenter Premises

Data center in both locations must be heavily guarded with CCTV camera surveillance; entry inside DC is protected with Security key card, passcode and Retina combination. Datacenter building management system has lot of Health checks (temperature/humidity/occupancy sensor etc.) any intrusion (unauthorized access) will either increase the temperature or trigger Occupancy sensor. Datacenter must have a log register for entries of work performed with engineer details and signature of the individual.

3.1.4 For Physical Hosts

All server/network equipment will be protected with Kensington lock method at all times. Kensington keys will be kept with Fire safety keys. Server hood latch panel must be locked (requires a coin to open). Advanced iLO must be soldered to Motherboard for extra protection. Remove information latch with default password for Advance iLO before shipping and email/pager alerts must be configured for watching activity.

3.1.5 For Internal Network Connectivity

Server must be connected with switch ports in a secure manner with documentation of each labelled cable running from server to switch port. Any changes must be documented under change control and entered into Datacenter log book. No idle Ethernet/fiber/infiniband cable must be left attached with switch. MAC Address filtering must be implemented and only allowed MAC address must traverse physical network. VLAN's must be pruned.

3.1.6 For Management VM's

Managements VM's must be hardened appliance with all the available patches applied. Patches must be applied to Dev->UAT->Prod as soon they are released. Mgmt VM's must be configured with two factor authentication only wherever possible.

3.1.7 For Humanity Link Suite

This software has paramount importance for humanities re-incarnation back on earth. Must be configured with two factor authentication and logon events must be monitored in real-time to detect the breach. Any failed logon attempt must generate an alarm. Logged-on users time stamp must be matched with their office door touch card access to verify his presence within premises. Database VM must be replicated to DR site and logs must be captured to centralized syslog server with 90 days retention period. OS Processes, service accounts and system files must be checked periodically for permission changes/ownership modification using CFG2HTML like tools. Must check OS for backdoors/buggy home call software using Wireshark like tools.

3.1.8 For Rest of the VM's

Rest of VM's must be isolated from Humanity link software suite using NSX Universal Distributed Firewall, OS Processes, service accounts and system files must be checked periodically for permission changes/ownership modification using CFG2HTML like tools. Must check OS for backdoors/buggy home call software using Wireshark like tools. Performance of VM's must be monitored carefully as they are running on shared infrastructure and might cause compute contention for VM's with paramount importance running on same host.

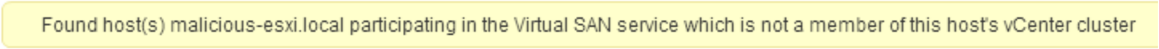
3.1.9 For protecting VSAN Network's

Virtual SAN traffic presents a large surface area to attacks. Virtual SAN has no authentication mechanism. It is expected behavior and well documented how you can join a VSAN Cluster and get access to the VSAN Datastore. There is no requirement that all ESXi hosts have to contribute hard drives to the VSAN Cluster. ESXi hosts without local drives can also be part of the VSAN Cluster and run Virtual Machines. The process is simple and does not require any authentication or vCenter assistance. Run the following command on any ESXi host with physical access to the VSAN Network:

```
~ # esxcli vsan cluster join -u [VSAN cluster UUID]
```

The host will join the VSAN Cluster and you have full access to the VSAN Datastore. As a default VSAN uses two multicast addresses, 224.1.2.3 (Master Group) and 224.2.3.4 (Agent Group). All hosts are sending one packet every second to one of the multicast addresses. UUID is exchanged in clear text and can be captured using any Network packet capture tool.

Detection- When an ESXi host that is not known to the vCenter joins the Virtual SAN, the following warning appears:



Found host(s) malicious-esxi.local participating in the Virtual SAN service which is not a member of this host's vCenter cluster

Create an alarm to trigger when following criteria met-

- Configure general settings
- Alarm name: Rogue Host Found in Virtual SAN Cluster.
- Monitor: Hosts
- Monitor for: specific event occuring on this object.
- Add a trigger for the event com.vmware.vc.vsan.RogueHostFoundEvent

Solution- This is intended VSAN behavior and the advice is to use an isolated non-routed VLAN.

4. Hardware implemented for Security

4.1.1 NTP Hardware servers

Our setup uses Hardware NTP server to manage the Time across the environment. They have 2xGalleon NTS-6000 Dual NTP hardware servers.

Ntp1.global.valkyrie.com

Ntp1.global.valkyrie.com is located in the Moon DC and it syncs time using MSF and GPS.

IP Address is 10.63.2.100

Public IP is 83.244.128.42 (need to confirm the public IP)

Time synchronisation status can be checked visually on the device unit itself and via the web interface.

Ntp2.global. valkyrie.com

Ntp2.global. valkyrie.com is located in the North Virginia DC and it syncs time using MSF and GPS.

IP Address is 172.20.65.22

Public IP is 64.215.157.133

Time synchronisation status can be checked visually on the device unit itself and via the web interface.
Both these Time Servers provide internal and external time to devices on external internal network. These Time devices are managed by Network team and password can be retrieved from Crypt-O.

5. Software implemented for Security

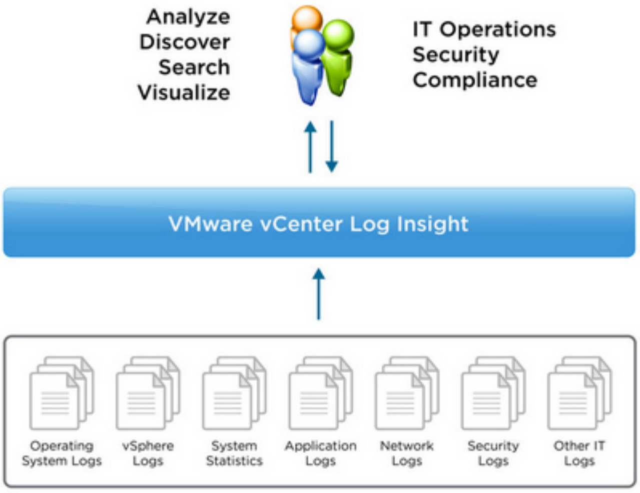
5.1.1 vRealize Log Insight

“Information is worthless until it’s correlated, analyzed and summarized” – Cuckoo’s Egg by Clifford stoll.

VMware vRealize Log Insight delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third party extensibility, providing deep operational visibility and faster troubleshooting. Sophisticated and scalable log analytics and log management organizes chaotic log data and gives you meaningful, actionable insights across multiple tiers of a hybrid cloud environments. All logs from

VM’s/ESXi hosts/VCSA/NSX etc. must be ingested into appliance and can be kept for as long as audit team requires it. This software also provide Splunk like data mining capabilities, with this we can correlate, analyze and summarize logs.

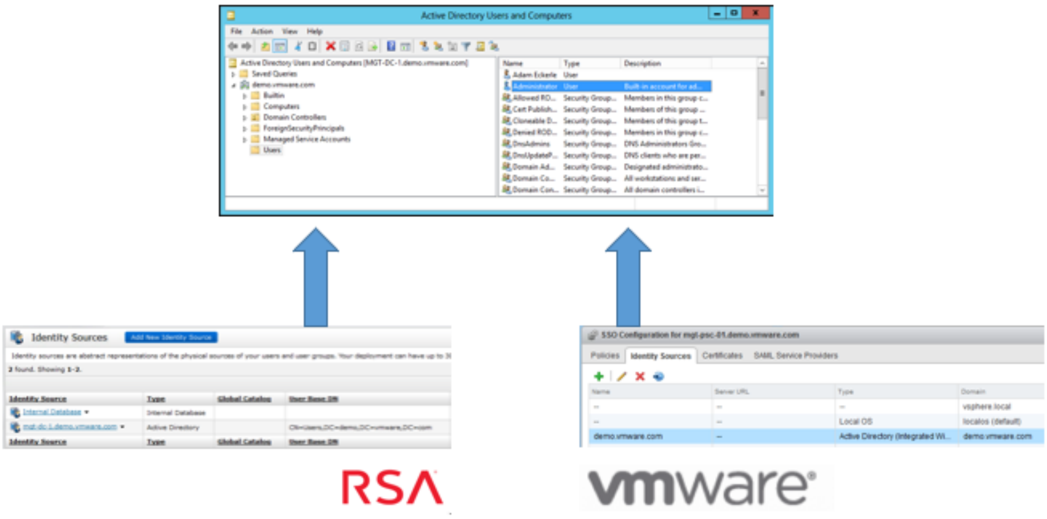
vRealize Log Insight is configured to accept only SSL connections, but the Log Insight Agents are configured to use non-SSL connection. so we need to configure the Log Insight Agents to send data through SSL cfapi protocol connection.



5.1.2 RSA Two Factor Authentication

Two factor authentication (2FA) has become ubiquitous nowadays. 2FA is “something you have”, like a hardware or software token and “something you know” which would be a secret PIN. vCenter supports two types of 2FA in 6.0 Update 2. SecurID and Smartcard. Admin staff has to carry RSA Key fob for inputting Secure Pin with their own predefined six- secret key e.g.51532298+key fob pin.

we’ll configure the Platform Services Controller (PSC) itself by uploading the sdconf.rec file and running the appropriate CLI commands to enable RSA SecurID. RSA Authentication Manager will also have Active Directory as an Identity Source. Active Directory will be the common Identity Source between VMware and RSA.


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [MGT-DC-1.demo.vmware.com]
Saved Queries
demo.vmware.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users

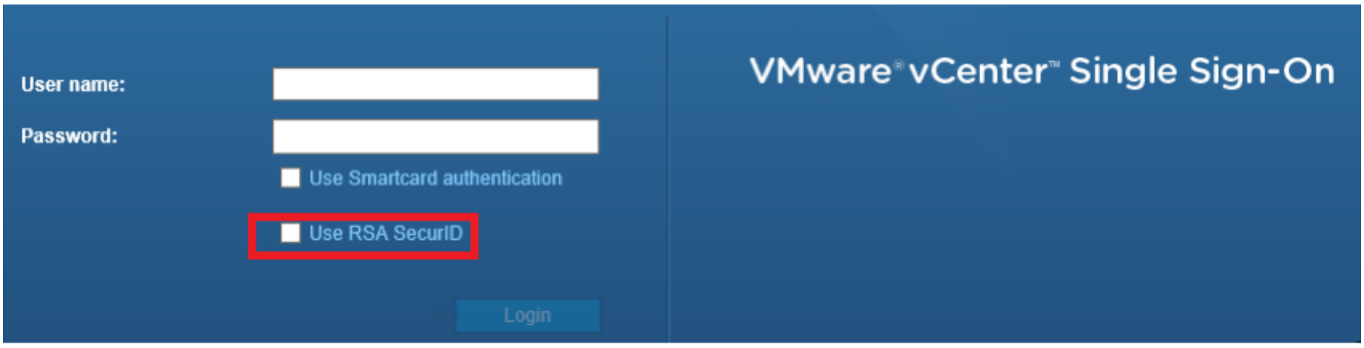
Name	Type	Description
Adam Eckerle	User	
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...

Identity sources are abstract representations of the physical sources of your users and user groups. Your deployment can have up to 3

2 found. Showing 1-2.

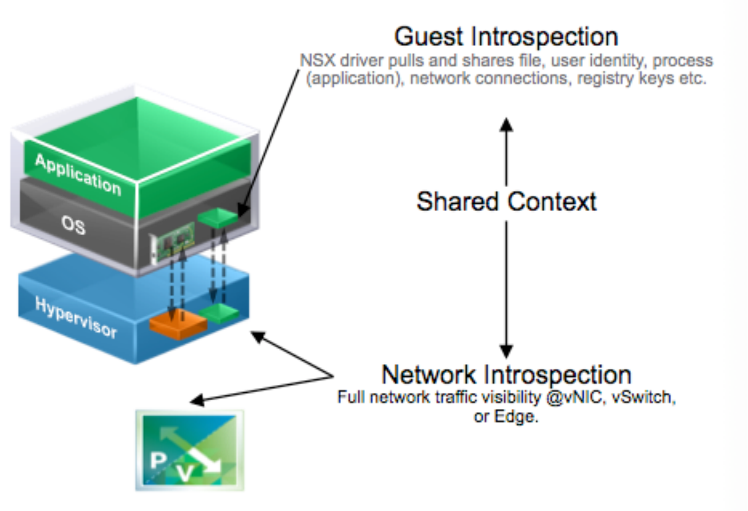
Identity Source	Type	Global Catalog	User Base DN
Internal Database	Internal Database		
mgt-dc-1.demo.vmware.com	Active Directory		CN=Users,DC=demo,DC=vmware,DC=com
Identity Source	Type	Global Catalog	User Base DN

Name	Server URL	Type	Domain
--	--	--	vsphere.local
--	--	Local OS	localos (default)
demo.vmware.com	--	Active Directory (Integrated Wi...	demo.vmware.com


VMware® vCenter™ Single Sign-On
User name:
Password:
□ Use Smartcard authentication
□ Use RSA SecurID
Login

5.1.3 McAfee AV with Guest Introspection

VMware NSX network virtualization platform to automate the distribution and enforcement of Intel Security's McAfee Network Security Platform (NSP), providing Intelligent Intrusion Prevention services (IPS) for the protection of east-west traffic within the data center. The new integrated solution includes the McAfee NSP IPS-VM100-VSS (a new IPS-VM Series model designed for interoperability with VMware NSX), McAfee Network Security Manager, Intel Security Controller and VMware NSX network virtualization platform.


Guest Introspection
NSX driver pulls and shares file, user identity, process (application), network connections, registry keys etc.
Shared Context
Network Introspection
Full network traffic visibility @vNIC, vSwitch, or Edge.
Application
OS
Hypervisor
P
V

5.1.4 VMware Fling – OS Hardening

This Fling provides Security Content Automation Protocol (SCAP) based assessment and remediation capabilities on any remote Linux machine running OpenSCAP. It can be used to assess compliance, provide Ansible-based remediation, and harden the target OS. With this app we can audit VMware estate for potential vulnerability and patch them using Ansible cookbooks, repeatable.

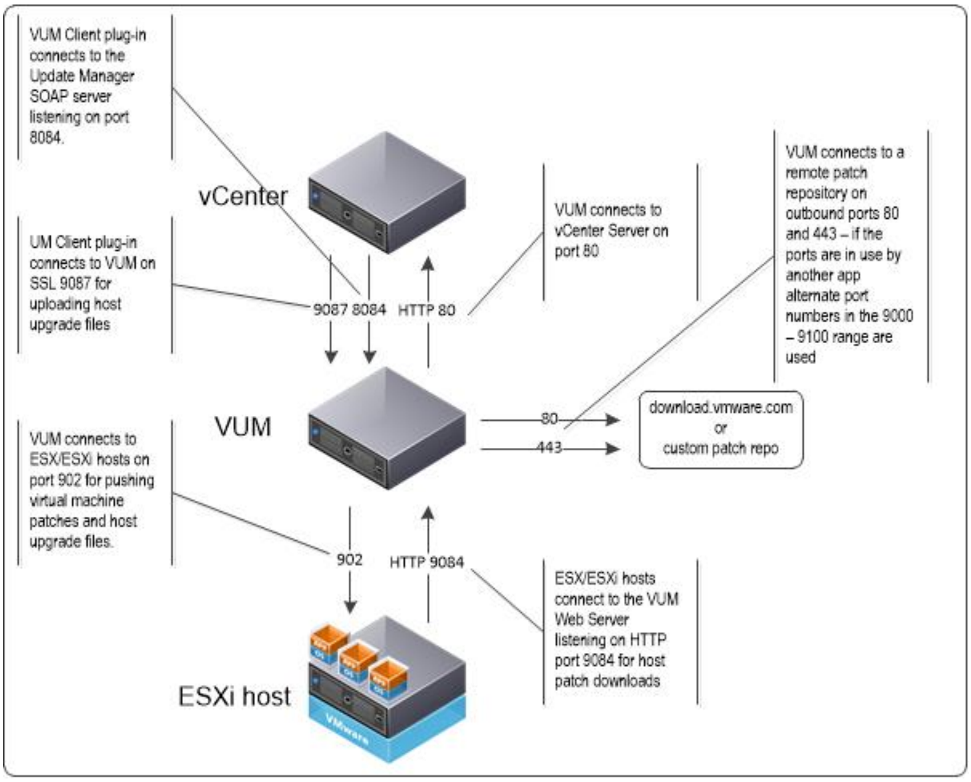
5.1.5 Crypt-O

This tool must be used for safe keeping of password being used in environment and for complex password generator. Password must be using below criteria-

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

5.1.6 Software Update Manager – WSUS/VUM/Redhat Satellite

Software update manager must be used with dynamic baselines for automatic remediation (on patch tuesday) of patches as-n-when they get released based on their criticality. Vmware update manager is available for patching VMware software (ESXi), WSUS for patching Windows VM’s and Redhat Satellite for patching Linux VM’s.



VUM Client plug-in connects to the Update Manager SOAP server listening on port 8084.

UM Client plug-in connects to VUM on SSL 9087 for uploading host upgrade files

VUM connects to ESX/ESXi hosts on port 902 for pushing virtual machine patches and host upgrade files.

VUM connects to vCenter Server on port 80

VUM connects to a remote patch repository on outbound ports 80 and 443 – if the ports are in use by another app alternate port numbers in the 9000 – 9100 range are used

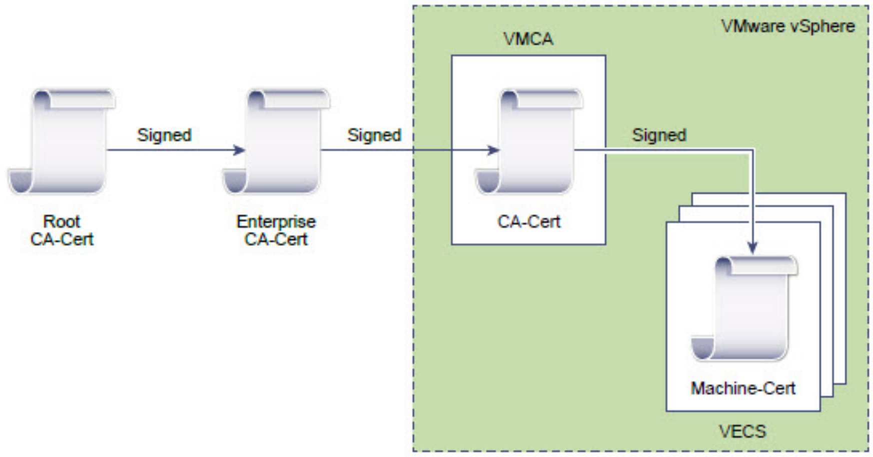
ESX/ESXi hosts connect to the VUM Web Server listening on HTTP port 9084 for host patch downloads

5.1.7 VMware Certificate Authority (VMCA)

This is a new exciting component in vSphere 6.0 that will radically change how many will issue and deploy SSL certificates in their vSphere environment. SSL certificates are used extensively to secure communications in a vSphere environment. This ensures data confidentiality and integrity. Any attempt to modify data in transit is detected, such as man-in-the-middle attacks.

The VMCA is a built-in certificate authority, which is included in the Platform Services Controller (PSC) service. This is a full blown CA, and can (if you wish) automatically issue certificates to all vCenter 6.0 components and ESXi 6.0 hosts in your environment. The VMCA is mostly command line driven, and does not have a fancy GUI like your Microsoft CA has. But once configured, it’s pretty much hands off operation.

In Subordinate VMCA mode it imports a root signing certificate from your trusted enterprise root CA. The VMCA then becomes an official subordinate CA to your enterprise root(s). All the certificates issued by the VMCA are trusted by your organization, even the web services exposed in browsers. As you deploy new vSphere components that are VMCA aware, they will get issued trusted SSL certificates. Since the VMCA now manages ESXi 6.0 host certificates, your ESXi hosts will also be issued trusted certificates without any manual intervention.



6. Automation implemented for Security

6.1.1 PS Pester Penetration testing

It’s always a good idea to enforce consistency for VMware environment as it leads to a predictable stack that better aligns architecture to reality. We’ll write a set of PowerShell scripts that would use a defined list of configuration state values to walk through vSphere environment and correct any deviations from what was declared to be normal. This will use raw PowerShell (and PowerCLI cmdlets) which results in no new install or configure and less overhead. These scripts allow a VMware environment to self-heal from modifications made by whomever. At this time, the jobs scripts defined are as follows and more can be configured:

- Remove VM limits and reservations (but it will purposefully error out on protected service VMs, such as NSX Edges)
- Remove ISO or connected CD-ROMs
- Set host DNS entries
- Set cluster DRS settings
- Set host NTP entries
- Configure the host SSH service
- Set host syslog setting

With slight modification to above scripts we can add Pester tests with some try/catch statement. If a test fails, the catch segment is invoked and remediates the identified config drift.

We've isolated each type of test into its own file to make collaboration and iterative work simple. Each test pulls from information from the Config.ps1 file to understand the desired state. It then reads the variables that it needs and applies them to the Pester tests.

Here’s an example from the DRS code.

```
#requires -Modules VMware.VimAutomation.Core
#requires -Version 1 -Modules Pester

Invoke-Expression -Command (Get-Item -Path 'Config.ps1')
[string]$drsmode = $global:config.cluster.drsmode
[int]$drslevel = $global:config.cluster.drslevel
```

The remaining bits of code check for the state of something (in this case, the DRS mode and DRS automation level) and then corrects any drift.

```
Describe -Name 'Cluster Configuration: DRS Settings' -Fixture {
    foreach ($cluster in (Get-Cluster))
    {
        It -name "$($cluster.name) Cluster DRS Mode" -test {
            $value = (Get-Cluster $cluster).DrsAutomationLevel
            try
            {
                $value | Should Be $drsmode
            }
            catch
            {
                Write-Warning -Message "Fixing $cluster - $_"
                Set-Cluster -Cluster $cluster -DrsAutomationLevel:$drsmode -
Confirm:$false
            }
        }
```

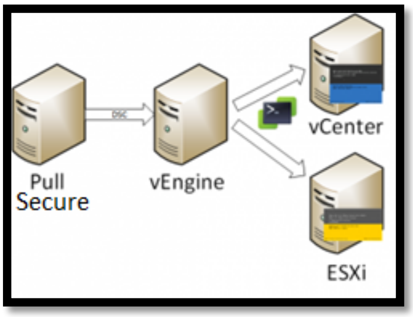
With this stuff we can make this autonomic and repeatable with lesser human intervention.

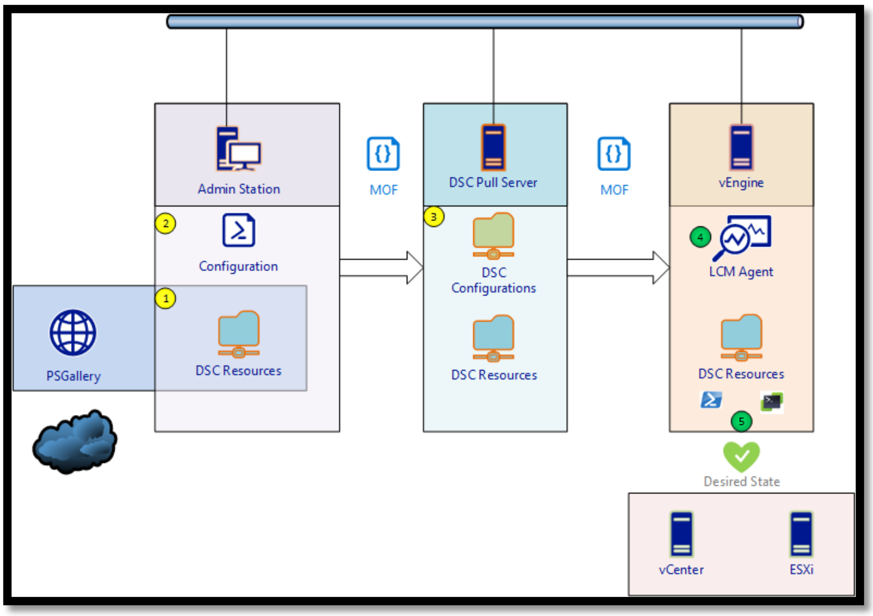
6.1.2 Power Shell DSC (Desired State Configuration)

DSC (Desired State Configuration) is a new management platform in Windows PowerShell that enables deploying and managing configuration data for software services and managing the environment in which these services run.

Following are some example scenarios where you can use built-in DSC resources to configure and manage a set of computers (also known as target nodes) in an automated way:

- Enabling or disabling server roles and features
- Managing registry settings
- Managing files and directories
- Starting, stopping, and managing processes and services
- Managing groups and user accounts
- Deploying new software
- Managing environment variables
- Running Windows PowerShell scripts
- Fixing a configuration that has drifted away from the desired state
- Discovering the actual configuration state on a given node





The LCM (Local Configuration Manager) is the DSC component that takes care of the “make it so” part. On regular intervals, or when you tell it to, it compares the Configuration, it has or has received, with the actual situation on the host.

If there are differences, and if the LCM was configured to correct this, the LCM will “correct” the drift. It will “Make it so!”

(1) The vSphere administrator makes sure he has the required DSC Resource modules on his workstation. This includes the vSphereDSC module. These modules can be retrieved from public or private repositories.

(2) The vSphere administrator creates a Configuration for his vSphere environment.

(3) The Configuration is pushed to the DSC Secure Pull Server. The Configuration is stored there as a MOF file.

(4) The LCM on the vEngine will query the Secure Pull Server at regular intervals to check if there is a new Configuration present. If there is, it will check if all the required resources for the new Configuration are present. If not, it will pull these DSC Resources from the Pull Server.

If there is no new Configuration, the LCM will use it’s local Current Configuration to “test” against the vSphere environment. If there is a drift, and if the LCM is configured to correct this, it will apply the Configuration on the vSphere environment.

Automation, in this case through DSC, will allow a continuous service availability, a continuous release cycle and continuous deployment.

Current Limitation - VDS configuration drifts can’t be programmed at the moment with VMware DSC module, so we have to stick with VDS config export/import feature available through Web Client.

6.1.3 vSphere host profiles and Auto deploy

VMware’s enterprise plus features i.e. host profiles and Auto deploy are two amazing utilities to automate host configuration stuff and manage host compliance.

Host profiles are used to help vSphere Auto Deploy provision physical ESXi hosts with configuration state information (virtual switches, driver settings, boot parameters, and so on).

Configuration state information cannot be stored directly on a host provisioned with Auto Deploy. Will create a reference host and configure it with the settings required. Then, create a host profile using this reference host. Auto Deploy can apply the host profile to these hosts so they are configured with these settings, or can apply the host profile using the client.

To apply a host profile to a host, the host must be placed into maintenance mode. The user is prompted to type answers for policies that are specified during host profile creation when the host profile is applied.

A host provisioned with Auto Deploy can be rebooted while the host profile is attached to the host. After rebooting, values stored in the answer file help the host provisioned with Auto Deploy to apply the profile. An answer file is created that contains a series of key value pairs for the user input options.

The answer file contains the user input policies for a host profile. The file is created when the profile is initially applied to a particular host.

After a host or cluster is configured with the reference host profile, a manual change, for example, can occur, making the configuration incorrect. Checking compliance on a regular basis ensures that the host or cluster continues to be correctly configured.

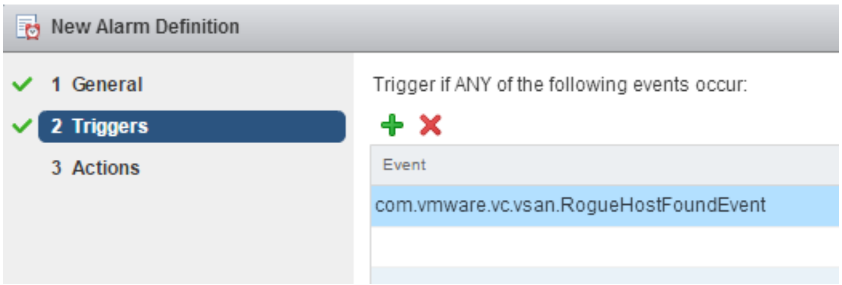
6.1.4 Alan Renouf's vCheck Scripts

We also run Famous vCheck scripts on daily basis to gather health check report for VMware Estate (vCSA/ESXi/VM/Network/Storage etc.) and send mail to admins on Moon Base.

This script picks on the key known issues and potential issues scripted as plugins for various technologies written as PowerShell scripts and reports it all in one place. This script is not to be confused with an Audit script.

6.1.5 vCenter event Alarms

Create alarms for event triggers and custom alarms can also be created for additional security measures. Visit URL for vCenter alerts database- http://www.virten.net/vmware/vcenter-events/



Trigger if ANY of the following events occur:

Event
com.vmware.vc.vsan.RogueHostFoundEvent

7. Log Files to audit for Intrusion Detection

7.1.1 ESXi Log Files

To collect diagnostic information we can create this log bundle with a special command line tool (vm-support), with the vSphere (Web-) Client or with the API. And extract this log bundle with Unix diagnostics scripts (VMware/HP GSS team have such scripts) for checking status of ESXi host and software. Log file rotation settings must be as per compliance policy and must be safely kept. ESXi's DCUI mode must be in lockdown mode (with selected USERs in access list, new feature in esxi 6.x). while checking logs on ESXi shell console keep in mind **UTC timing** is de facto.

There are couple of important files that are not included in support bundle purposefully, following files that contain sensitive information must be monitored at all times:

- /etc/vmware/vmkiscsid/vmkiscsid.db
- /etc/vmware/ssl/rui.crt
- /etc/vmware/ssl/rui.key
- /etc/vmware/ssl/rui.bak
- /etc/vmware/vmkiscsid/.#vmkiscsid.db
- /etc/vmware/ssl/.#rui.crt
- /etc/vmware/ssl/.#rui.key
- /etc/vmware/ssl/.#rui.bak
- /etc/ssh/ssh_host_dsa_key
- /etc/ssh/ssh_host_rsa_key
- /etc/shadow
- /etc/passwd
- /etc/vmware/vmware.lic

7.1.2 VCSA Log Files

Similarly you can create vCenter support log bundle via vSphere (Web-) Client for checking status of VCSA health and software. This support bundle can also be analyzed using Diagnostics scripts. Log file rotation settings must be as per compliance policy and must be safely kept.

- The vpxd.log: The main vCenter Server log, consisting of all vSphere Client and WebServices connections, internal tasks and events, and communication with the vCenter Server Agent (vpxa) on managed ESXi/ESX hosts.
- vpxd-profiler.log, profiler.log, and scoreboard.log: Profiled metrics for operations performed in vCenter Server. Used by the VPX Operational Dashboard (VOD) accessible at https://VCHostnameOrIPAddress/vod/index.html.
- vpxd-alert.log: Non-fatal information logged about the vpxd process.
- cim-diag.log and vws.log: Common Information Model monitoring information, including communication between vCenter Server and managed hosts' CIM interface.
- drmdump\: Actions proposed and taken by VMware Distributed Resource Scheduler (DRS), grouped by the DRS-enabled cluster managed by vCenter Server. These logs are compressed.
- ls.log: Health reports for the Licensing Services extension, connectivity logs to vCenter Server.
- vimtool.log: Dump of string used during the installation of vCenter Server with hashed information for DNS, username and output for JDBC creation.
- stats.log: Provides information about the historical performance data collection from the ESXi/ESX hosts
- sms.log: Health reports for the Storage Monitoring Service extension, connectivity logs to vCenter Server, the vCenter Server database and the xDB for vCenter Inventory Service.
- eam.log: Health reports for the ESX Agent Monitor extension, connectivity logs to vCenter Server.
- catalina.date.log and localhost.date.log: Connectivity information and status of the VMware Webmanagement Services.
- jointool.log: Health status of the VMwareVCMSDS service and individual ADAM database objects, internal tasks and events, and replication logs between linked-mode vCenter Servers.
- Additional log files:

    - manager.date.log
    - host-manager.date.log
- /etc/vmware/ssl/rui.crt
- /etc/vmware/ssl/rui.key
- /etc/vmware/ssl/rui.bak
- /etc/vmware/vmkiscsid/.#vmkiscsid.db
- /etc/vmware/ssl/.#rui.crt
- /etc/vmware/ssl/.#rui.key
- /etc/vmware/ssl/.#rui.bak
- /etc/ssh/ssh_host_dsa_key
- /etc/ssh/ssh_host_rsa_key
- /etc/shadow
- /etc/passwd

7.1.3 Windows Log Files

- Event log files. Log files that can be examined using Event Viewer. They include the following logs:
    - Application
    - System
    - Security
    - Directory service
    - File replication service
    - DNS server
    - Event logs created by other services or applications
- Other log files. Log files created by other services or applications such as the Windows Backup utility, antivirus programs, and third-party applications that cannot be viewed in Event Viewer. To examine the information in these log files, open the files with a text reader such as Notepad.

7.1.4 App/DB/Web Log Files

Common log files to watch on linux OS, services that are not being must be completely turned off using chkconfig command, remove/disable any system level service account if not being used, Use Linux OS hardening best practices. Disable public SNMP communities and use only protected/private snmp strings with encryption. SMTP relays must not be used for configuring alert mails.

- /var/log/messages : General message and system related stuff.
- /var/log/auth.log : Authenication logs.
- /var/log/kern.log : Kernel logs.
- /var/log/cron.log : Crond logs (cron job)
- /var/log/maillog : Mail server logs.
- /var/log/qmail/ : Qmail log directory (more files inside this directory)

8. Process implementation based on ITIL/ISMS

8.1.1 Password Rotation policy

Exception for VPXA user created on ESXi host once it’s attached to vCenter server, password can’t be changed manually.

Rest of the password fall under periodical password rotation policy (45 days), last 5 passwords can't be re-used. Complexity strength must be compliant to password policy (use crypt-o for password generation)

8.1.2 Password Expiry policy

Passwords that come with default must be changed before putting system in Production, default expiry of 90 days must be changed to 45 days with email alerts.

8.1.3 Document labeling policy

All documents must bear labels like- "CLASSIFIED", "EYES ONLY", "COMPARTMENTALIZED", "INTELLIGENCE", "SHRED AFTER READING", "NOFORN" and "TOP SECRET". Documents must be kept under lock and key at all times. Post-it shouldn't be left with remarks out in open (hide agile meeting notes, kan-ban notes).

8.1.4 Change control policy

All changes being made in the environment must fall under change control process and must go through stringent inspection by all team members and higher-ups.

8.1.5 Auditing policy

Monthly or quarterly audits must be put in place, where you can invite internal/external auditing personnel to perform routing auditing based on ISMS standards. Once All these processes are in-place will help in reducing average intrusion detection times and keep staff abreast on caveats (NCI's non-compliance) in their environments.

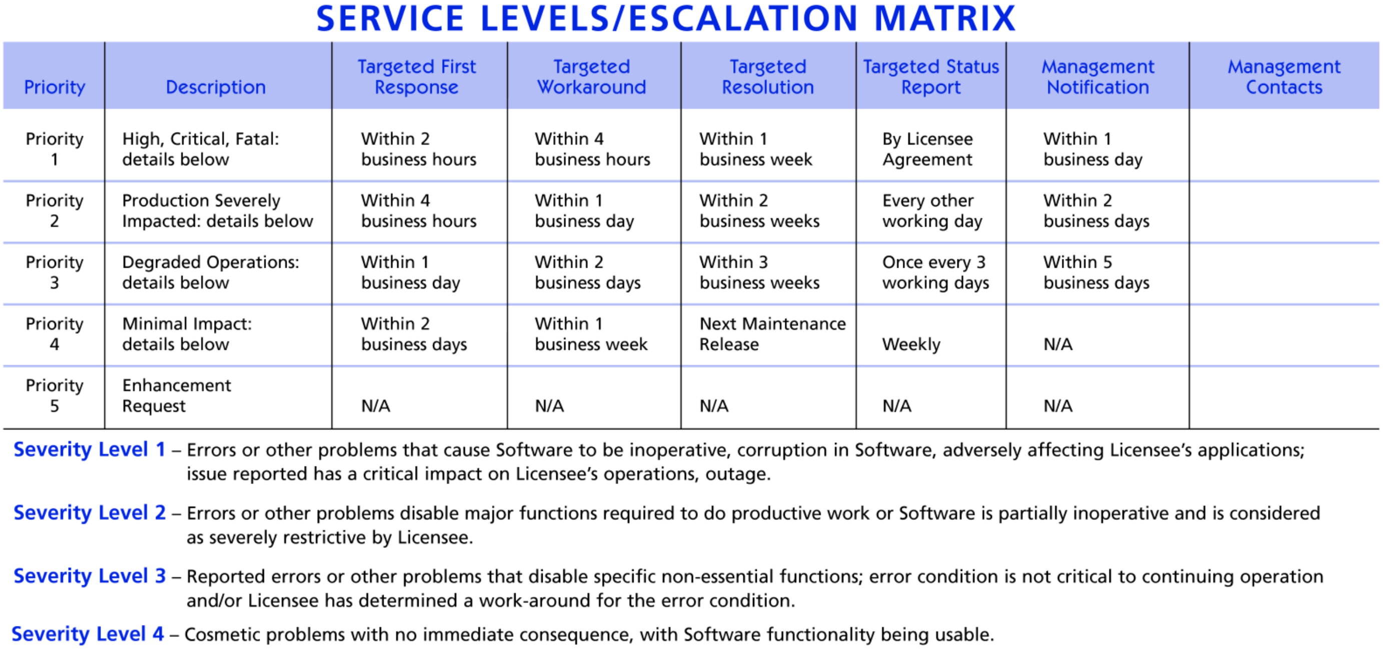
9. Emergency Response team /Escalation matrix

Process team must create an Outage evaluation based on business need, for identifying severity and impact of Incident and floating emergency message to C-Level executives.

9.1.1 ERT details phone numbers

Senior/Junior staff members must be designated with KRA/KPIs for working during Incident and gather all hands on deck in case of emergency. A toll free number must be floated at all sites with IT Equipment for emergency situation. PHS must be given to ERT members with monthly incentive to keep them motivated, team members must be rotated in shifts.

9.1.2 Escalation Matrix



SERVICE LEVELS/ESCALATION MATRIX

Priority	Description	Targeted First Response	Targeted Workaround	Targeted Resolution	Targeted Status Report	Management Notification	Management Contacts
Priority 1	High, Critical, Fatal: details below	Within 2 business hours	Within 4 business hours	Within 1 business week	By Licensee Agreement	Within 1 business day	
Priority 2	Production Severely Impacted: details below	Within 4 business hours	Within 1 business day	Within 2 business weeks	Every other working day	Within 2 business days	
Priority 3	Degraded Operations: details below	Within 1 business day	Within 2 business days	Within 3 business weeks	Once every 3 working days	Within 5 business days	
Priority 4	Minimal Impact: details below	Within 2 business days	Within 1 business week	Next Maintenance Release	Weekly	N/A	
Priority 5	Enhancement Request	N/A	N/A	N/A	N/A	N/A	

Severity Level 1 – Errors or other problems that cause Software to be inoperative, corruption in Software, adversely affecting Licensee's applications; issue reported has a critical impact on Licensee's operations, outage.

Severity Level 2 – Errors or other problems disable major functions required to do productive work or Software is partially inoperative and is considered as severely restrictive by Licensee.

Severity Level 3 – Reported errors or other problems that disable specific non-essential functions; error condition is not critical to continuing operation and/or Licensee has determined a work-around for the error condition.

Severity Level 4 – Cosmetic problems with no immediate consequence, with Software functionality being usable.

10. Network Ports to audit for Intrusion Detection

10.1.1 VMware vSphere Network Ports

Product	Port	Protocol	Source	Target	Purpose
Data Recovery	22024	TCP	Data Recovery vSphere Client Plug-in	Data Recovery Appliance	Data Recovery management
ESXi 6.x	22	TCP	vSphere client	ESXi 6.x	SSH Server
ESXi 6.x	80	TCP	vSphere client / vSphere Web client	ESXi 6.x	Redirect Web Browser to HTTPS Service (443)
ESXi 6.x	443	TCP	VI / vSphere client/ vSphere Web client	ESXi/ESX Host	VI / vSphere client to ESXi/ESX Host management connection
ESXi 6.x	902	TCP	vSphere Client	ESXi 6.x	vSphere Client access to virtual machine consoles (MKS)
vCenter 6.x	80	TCP	vSphere Client /vSphere Web Client	vCenter Server	vCenter Server requires port 80 for direct HTTP connections.
vCenter 6.x	443	TCP	vSphere Client /vSphere Web Client	vCenter Server	vCenter Server system uses to listen for connections from the vSphere Client.
vCenter 6.x	902	TCP/UDP	vSphere Client	ESXi 6.x	vSphere Client uses this ports to display virtual machine consoles.

vCenter 6.x	903	TCP	vSphere Client	ESX 3.5 and 4.x	Remote console traffic generated by user access to virtual machines. This applies to all ESXi/ESX versions.
vCenter 6.x	8080	TCP	vSphere client	vCenter Server	Web Services HTTP. Used for the VMware VirtualCenter Management Web Services.
vCenter 6.x	8443	TCP	vSphere client	vCenter Server	Web Services HTTPS. Used for the VMware VirtualCenter Management Web Services.
vCenter 6.x	9443	TCP	vSphere client	vCenter Server	vSphere Web Client Access
vCenter 6.x	10080	TCP	vSphere client	vCenter Server	vCenter Inventory Service HTTP
vCenter 6.x	10443	TCP	vSphere client	vCenter Server	vCenter Inventory Service HTTPS

Product	Port	Protocol	Source	Target	Purpose
ESXi 6.x	9	UDP	vCenter Server	Virtual Volumes	Used by the Virtual Volumes feature
ESXi 6.x	22	TCP	SSH Client	ESXi Host	Required for SSH access
ESXi 6.x	53	UDP	ESXi Host	DNS Server	DNS client
ESXi 6.x	68	UDP	DHCP Server	ESXi Host	DHCP client for IPv4
ESXi 6.x	80	TCP	Web Browser	ESXi Host	Welcome page, with download links for different interfaces
ESXi 6.x	161	UDP	SNMP Server	ESXi Host	Allows the host to connect to an SNMP server
ESXi 6.x	427	TCP/UDP	CIM Server	ESXi Host	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers
ESXi 6.x	443	TCP	vSphere Web Client	ESXi Host	Client connections
ESXi 6.x	546	TCP/UDP	DHCP Server	ESXi Host	DHCP client for IPv6
ESXi 6.x	547	TCP/UDP	ESXi Host	DHCP Server	DHCP client for IPv6
ESXi 6.x	902	TCP/UDP	VMware vCenter Agent	ESXi Host	vCenter Server agent

ESXi 6.x	2233	TCP	ESXi Host	Virtual SAN Transport	Used for RDT traffic (Unicast peer to peer communication) between Virtual SAN nodes.
ESXi 6.x	3260	TCP	ESXi Host	Software iSCSI Client	Supports software iSCSI
ESXi 6.x	5671	TCP	ESXi Host	rabbitmqproxy	A proxy running on the ESXi host that allows applications running inside virtual machines to communicate to the AMQP brokers running in the vCenter network domain. The virtual machine does not have to be on the network, that is, no NIC is required. The proxy connects to the brokers in the vCenter network domain. Therefore, the outgoing connection IP addresses should at least include the current brokers in use or future brokers. Brokers can be added if customer would like to scale up.
ESXi 6.x	598,88,889	TCP	CIM Server	ESXi Host	Server for CIM (Common Information Model)
ESXi 6.x	5989	TCP	CIM Secure Server	ESXi Host	Secure server for CIM
ESXi 6.x	6999	UDP	NSX Distributed Logical Router Service	ESXi Host	NSX Virtual Distributed Router service. The firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open.
ESXi 6.x	8000	TCP	ESXi Host	ESXi Host	vMotion

ESXi 6.x	8080	TCP	vsanvp	ESXi Host	VSAN VASA Vendor Provider. Used by the Storage Management Service (SMS) that is part of vCenter to access information about Virtual SAN storage profiles, capabilities, and compliance. If disabled, Virtual SAN Storage Profile Based Management (SPBM) does not work.
ESXi 6.x	8100820,08,300	TCP\UDP	Fault Tolerance	ESXi Host	Traffic between hosts for vSphere Fault Tolerance (FT).
ESXi 6.x	830,18,302	UDP	DVSSync	ESXi Host	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open.
ESXi 6.x	12345, 23451	UDP	ESXi Host	Virtual SAN Clustering Service	Cluster Monitoring, Membership, and Directory Service used by Virtual SAN.
ESXi 6.x	44046, 31031	TCP	ESXi Host	HBR	Used for ongoing replication traffic by vSphere Replication and VMware Site Recovery Manager.
ESXi Dump Collector	6500	UDP	ESXi	vCenter Server	Network coredump server
ESXi Dump Collector	8000	TCP	ESXi	vCenter Server	Network coredump web port
ESXi Syslog Collector	8001	TCP	ESXi	vCenter Server	Network syslog server

Update Manager	80	TCP	Update Manager Server	www.vmware.com and xml.shavlik.com	To obtain metadata for the updates, Update Manager must be able to connect to http://www.vmware.com and http://xml.shavlik.com
Update Manager	80	TCP	ESXi/ESX Host	Update Manager Host	ESXi/ESX Host to Update Manager Server. The reverse proxy forwards the request to port 9084
Update Manager	80	TCP	Update Manager Server	vCenter Server	Update Manager to vCenter Server communication
Update Manager	443	TCP	Update Manager Server	www.vmware.com and xml.shavlik.com	To obtain metadata for the updates, Update Manager must be able to connect to http://www.vmware.com and http://xml.shavlik.com
Update Manager	443	TCP	ESXi/ESX Host	Update Manager Server	ESXi/ESX Host to Update Manager Server . The reverse proxy forwards the request to port 9084
Update Manager	443	TCP	vCenter Server	Update Manager Server	vCenter Server to Update Manager Server. The reverse proxy forwards the request to port 8084
Update Manager	735	TCP	Update Manager Server	Virtual Machines	Update Managerlistenerport (rdevServer.exe) part of theRemote Device Server used for virtual machine patching.
Update Manager	902	TCP	Update Manager Server	ESXi/ESX Host	To push patches and updates from Update Manager to the ESXi/ESX Hosts to be updated
Update Manager	1433	TCP	Update Manager Server	Microsoft SQL Server	Update Manager to Microsoft SQL Server connectivity (for UM Database)

Update Manager	1521	TCP	Update Manager Server	Oracle Database Server	Update Manager to Oracle connectivity (for UM Database)
Update Manager	8084	TCP	Update Manager Server	Update Manager Client Plugin	SOAP between components of Update Manager Server and the vCenter Update Manager client plug-in. Configurable at install.
Update Manager	9084	TCP	ESXi/ESX host	Update Manager Server	ESXi/ESX hosts connect to the VUM (VMware Update Manager) webserver listening for updates. Configurable at install.
Update Manager	9087	TCP	Update Manager Server	Update Manager Client Plugin	Port used for uploading host update files. Configurable at install.
Update Manager	9000 to 9100	TCP	ESXi/ESX Host	Update Manager Server	This is the recommend port range from which to choose ports for Update Manager if ports 80 and 443 are already in use. Update Manager automatically opens these ports for ESX Host scanning and remediation.
vCenter Server 6.0	22	TCP/UDP	vCenter Server	SSH Client	System port for SSHD. This port is only used by the vCenter Server Appliance
vCenter Server 6.0	80	TCP	Client PC	vCenter Server	vCenter Server requires port80for direct HTTP connections. Port80redirects requests to HTTPS port 443. This redirection is useful if you accidentally usehttp://serverinstead ofhttps://server.
vCenter Server 6.0	88	TCP	vCenter Server	Active Directory Server	VMware key distribution center port

vCenter Server 6.0	389	TCP/UDP	vCenter Server	Linked vCenter Servers	This port must be open on the local and all remote instances of vCenter Server. This is the LDAP port number for the Directory Services for the vCenter Server group.
vCenter Server 6.0	443	TCP	vSphere Web Client	vCenter Server	The default port that the vCenter Server system uses to listen for connections from the vSphere Web Client. To enable the vCenter Server system to receive data from the vSphere Web Client, open port 443 in the firewall.
vCenter Server 6.0	514	UDP	Syslog Collector	Syslog Collector	vSphere Syslog Collector port for vCenter Server on Windows and vSphere Syslog Service port for vCenter Server Appliance
vCenter Server 6.0	636	TCP	Platform Service Controller	Management Nodes	For vCenter Server Enhanced Linked Mode, this is the SSL port of the local instance. If another service is running on this port, it might be preferable to remove it or change its port to a different port.
vCenter Server 6.0	902	TCP/UDP	vCenter Server	ESXi 6.0/5.x	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902to the vCenter Server system.

vCenter Server 6.0	10080	TCP	vCenter Server	Inventory Service	vCenter Server vCenter Inventory Service HTTP
vCenter Server 6.0	1514	TCP/UDP	Syslog Collector	Syslog Collector	vSphere Syslog Collector TLS port for vCenter Server on Windows and vSphere Syslog Service TLS port for vCenter Server Appliance
vCenter Server 6.0	2012	TCP	vCenter Server (Tomcat Server settings)	vCenter Single Sign-On	Control interface RPC for vCenter Single Sign-On(SSO).
vCenter Server 6.0	2014	TCP	vCenter Server (Tomcat Server settings)	vCenter Single Sign-On	RPC port for all VMCA (VMware Certificate Authority) APIs.
vCenter Server 6.0	2020	TCP/UDP	vCenter Server	vCenter Server	Authentication framework management
vCenter Server 6.0	6500	TCP/UDP	vCenter Server	ESXi host	ESXi Dump Collector port
vCenter Server 6.0	6501	TCP	Auto Deploy service	ESXi Host	Auto Deploy service
vCenter Server 6.0	6502	TCP	Auto Deploy Manager	vSphere Client	Auto Deploy management
vCenter Server 6.0	7444	TCP			Secure Token Service
vCenter Server 6.0	8009	TCP	vCenter Server	vCenter Server	AJP Port
vCenter Server 6.0	8089	TCP	vCenter Server	vCenter Server	SDK Tunneling Port
vCenter Server 6.0	9443	TCP	vSphere Web Client Server	vSphere Web Client	vSphere Web Client HTTPS
vCenter Server 6.0	11711	TCP	vCenter Single Sign-On	vCenter Single Sign-On	VMware Directory service (`vmdir`) LDAP
vCenter Server 6.0	11712	TCP	vCenter Single Sign-On	vCenter Single Sign-On	VMware Directory service (`vmdir`) LDAPS
vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	22	TCP	SSH Client	vRealize Log Insight (formerly known as vCenter Log Insight)	Secure Shell (SSH) access to the vRealize Log Insight (formerly known as vCenter Log Insight) virtual appliance
vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	25	TCP	vRealize Log Insight (formerly known as vCenter Log Insight)	SMTP Server	Email notifications from vRealize Log Insight (formerly known as vCenter Log Insight) to a configured mail server

vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	514	UDP	Syslog Client	vRealize Log Insight (formerly known as vCenter Log Insight)	Remote Syslog logging
vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	514	TCP	Syslog Client	vRealize Log Insight (formerly known as vCenter Log Insight)	Remote Syslog logging
vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	445	UDP	vRealize Log Insight (formerly known as vCenter Log Insight)	MS Directory Services Server	Connection to a Domain Controller for Active Directory Authentication
vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	80	TCP	HTTP Client	vRealize Log Insight (formerly known as vCenter Log Insight)	vRealize Log Insight (formerly known as vCenter Log Insight) Web Interface. Redirects to encrypted web interface
vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	443	TCP	HTTP Client	vRealize Log Insight (formerly known as vCenter Log Insight)	vRealize Log Insight (formerly known as vCenter Log Insight) Web Interface Encrypted
vRealize Log Insight (formerly known as vCenter Log Insight) 1.x	123	UDP	vRealize Log Insight (formerly known as vCenter Log Insight)	NTP Server	Time synchronization with NTP server

10.1.2 VMware NSX Network Ports

Client PC > NSX Manager 443/TCP (NSX Manager Administrative Interface)

Client PC > NSX Manager 80/TCP (NSX Manager VIB Access)

ESXi Host > ESXi Host 6999/UDP (ARP on VLAN LIFs)

ESXi Host > NSX Controller 1234/TCP (User World Agent Connection)

ESXi Host > NSX Manager 5671/TCP (AMQP)

ESXi Host > NSX Manager 8301, 8302/UDP (DVS Sync)

ESXi Host > vCenter Server 80/TCP (ESXi Host Preparation)

NSX Controller > NSX Controller 2878, 2888, 3888/TCP (Controller Cluster – State Sync)

NSX Controller > NSX Controller 30865/TCP (Controller Cluster -State Sync)

NSX Controller > NSX Controller 7777/TCP (Inter-Controller RPC Port)

NSX Controller > NTP Time Server 123/TCP (NTP client connection)

NSX Controller > NTP Time Server 123/UDP (NTP client connection)

NSX Manager > DNS Server 53/TCP (DNS client connection)

NSX Manager > DNS Server 53/UDP (DNS client connection)

NSX Manager > ESXi Host 443/TCP (Management and provisioning connection)

NSX Manager > ESXi Host 8301, 8302/UDP (DVS Sync)

NSX Manager > ESXi Host 902/TCP (Management and provisioning connection)

NSX Manager > NSX Controller 443/TCP (Controller to Manager Communication)

NSX Manager > NTP Time Server 123/TCP (NTP client connection)

NSX Manager > NTP Time Server 123/UDP (NTP client connection)

NSX Manager > Syslog Server 514/TCP (Syslog connection)

NSX Manager > Syslog Server 514/UDP (Syslog connection)

NSX Manager > vCenter Server 443/TCP (vSphere Web Access)

NSX Manager > vCenter Server 902/TCP (vSphere Web Access)

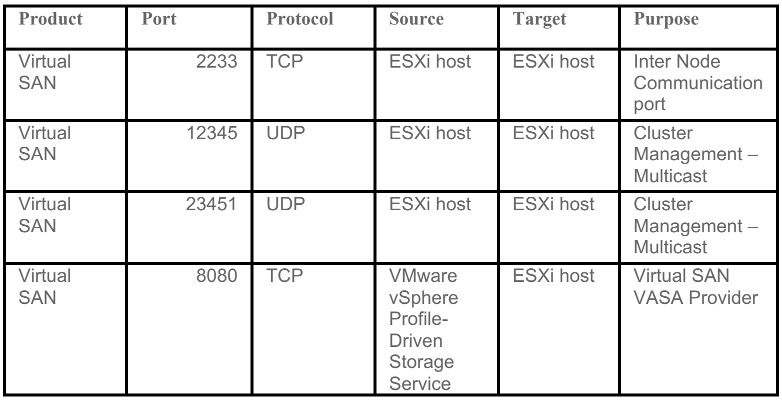
REST Client > NSX Manager 443/TCP (NSX Manager REST API)

vCenter Server > ESXi Host 80/TCP (ESXi Host Preparation)

vCenter Server > NSX Manager 80/TCP (Host Preparation)

VTEP > VTEP 4789/UDP (Transport network encapsulation between VTEPs.)

10.1.3 VMware vSAN Network Ports



Product	Port	Protocol	Source	Target	Purpose
Virtual SAN	2233	TCP	ESXi host	ESXi host	Inter Node Communication port
Virtual SAN	12345	UDP	ESXi host	ESXi host	Cluster Management – Multicast
Virtual SAN	23451	UDP	ESXi host	ESXi host	Cluster Management – Multicast
Virtual SAN	8080	TCP	VMware vSphere Profile-Driven Storage Service	ESXi host	Virtual SAN VASA Provider

11. References

1. **The Cuckoo's Egg novel By Clifford Stoll**
2. **Trojan horse novel By Mark Russinovich**
3. **IT Architect: Foundation in the Art of Infrastructure Design By J.Y. Arrasjid, M. Gabryjelski & C. McCain**
4. **http://www.virten.net/2015/10/whats-inside-an-esxi-vm-support-bundle/**

5. http://www.virten.net/2016/06/nsx-6-2-3-with-free-log-insight-entitlement-released/
6. http://www.virten.net/2016/05/vmware-nsx-6-component-communication-diagram/
7. http://www.virten.net/2015/11/how-to-create-custom-vcenter-alarms/
8. http://www.virten.net/2015/11/why-you-should-secure-your-virtual-san-network/
9. http://wahlnetwork.com/2016/06/16/remediating-vsphere-configuration-drift-powershell-pester-tests/
10. http://www.lucd.info/2016/06/07/vspheredsc-principles-operation/
11. http://www.lucd.info/2016/06/06/vspheredsc-vmwdatacenter/
12. http://www.lucd.info/2016/06/05/vspheredsc-vmwfolder/
13. http://www.lucd.info/2016/06/04/vspheredsc-intro/
14. http://www.virten.net/vmware/vcenter-events/
15. https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2131180
16. https://en.wikipedia.org/wiki/Kensington_Security_Slot
17. http://blogs.vmware.com/vsphere/2016/04/two-factor-authentication-for-vsphere-rsa-securid.html
18. https://blogs.vmware.com/vsphere/2016/04/two-factor-authentication-for-vsphere-rsa-securid-part-2.html
19. https://labs.vmware.com/flings/vmware-gold-vapp-stig-assessment-and-remediation-tool-start