IMPLEMENTATION METHODOLOGY

VMware Desktop Virtualization Health Check Services Health Check Report

for

MSPB

Prepared by

(b) (6)

VMware Professional Services

(b) (6)

Version History

Date	Ver.	Author	Description	Reviewers
9/1/2015	.1	(b) (6)	Draft	
9/3/2015	.5	(b) (6)	Add Content	
9/4/2015	1.0	(b) (6)	Organize Findings	
9/6/2015	1.5	(b) (6)	Added Recommendations	
9/8/2015	2.0	(b) (6)	Organized Recommendations	
9/9/2015	2.5	(b) (6)	Checked Formatting sent to (b) (6) for review	(b) (6)

VMware, Inc
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

1. Executive Summary

MSPB engaged VMware Professional Services to conduct a health check of their VMware View™ environment. This engagement included a health check of MSPB's current VMware vSphere® configuration, operations, and usage. If there are issues with the underlying vSphere implementation, the impact on the View environment could be severe.

2. Health Check Background

2.1 Scope

This document applies to the vSphere and Horizon View environments in the Washington DC office. All of the server systems are hosted in house and managed by internal personnel. This engagement is limited to the documentation and data gathered within the VMware Health Analyzer and the logs collected from each VMware component. The vSphere environment exists on Nutanix Hardware.

Infrastructure and VDI – Nutanix 3450

ComVault environment – Nutanix 6250

2.2 Health Check Participants

The following personnel were active participants during the course of the health check.

- (b) (6) - VMware
- (b) (6) – VMware
- (b) (6)
- (b) (6)
- (b) (6)
- (b) (6)

2.3 Summary of Activities

The following activities were conducted during the course of this project.

- Assessed and summarized the MSPB VMware vSphere environment health and architecture, focusing on technical and organizational aspects.
- Interviewed participants to determine priority issues and concerns.
- Collected View component information.
- Inventoried all hosted virtual desktops.
- Inventoried all linked clone pools, individually assigned virtual machines, and corresponding user entitlements.
- Researched MSPB's issues and concerns with View performance.
- Conducted basic knowledge transfer on following topics:
  - View operations best practices
  - Pool management best practices
  - View storage best practices

- Hosted desktop image build process
- PCOIP sizing considerations
- PCOIP protocol tuning

2.4 Next Steps

Review this report and consider the recommended action items. Consider follow-up consulting engagement and/or health check. If required, the VMware Professional Services Organization or one of the VMware partner organizations can help MSPB implement the recommended actions.

3. Findings and Recommendations

The assessment results are presented in a prioritized format. Table 1 summarizes the priority categories of the assessment.

Table 1. Priority Categories

Priority	Definition
P1	Items that require immediate attention and the corresponding actions to address each item.
P2	Items of potential concern. The items are either non-critical, or require further investigation.
P3	Deviation from best practices, but addressing these might not be an immediate priority.

3.1 Summary of vSphere Findings

The following table contains a summary of the results of the vSphere Health Check that was performed during this project.

3.1.1 Compute

Item	Comments
Observation 1	Remote syslog logging is configured but not enabled for 10 host(s).
Priority	P1
Recommendation	Use persistent and remote syslog logging to improve manageability.
Justification	Remote logging both persistently on each host and to a central host (syslog server) can greatly improve administration and management. By making files available when needed and gathering files on a central server, you can easily monitor all hosts and perform event correlation, aggregate analysis, and make root cause analysis easier for troubleshooting. Also, gathering the log files on a remote system allows you to retain more historical information for postmortem analysis of compromised systems. To collect syslog information, all the systems must have synchronized time and the correct firewall ports open between hosts so that events can be correlated. Also, log messages are not encrypted when sent to the remote host, so the network for the service console should be isolated from other networks. With vSphere 6.0, the vSphere Syslog Collector (Windows) or the VMware Syslog Service (Appliance) are installed by default and thus can be used to provide this function once configured. **References:** *Configure Syslog on ESXi Hosts* section of the *vSphere Installation and Setup* Guide http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-installation-setup-guide.pdf *ESXi tab in the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	Comments
Observation 2	ESXi shell has been enabled or configured to start automatically on 7 host(s). SSH access has been enabled or configured to start automatically on 10 host(s).

Priority	P1
Recommendation	Configure VMware vSphere ESXi Shell and SSH access per manageability requirements.
Justification	The vSphere ESXi Shell and ESXi host SSH access can provide essential host access that can be used when standard remote management or CLI tools do not function. Access to the vSphere ESXi Shell and SSH is primarily intended for use in break-fix scenarios and can be enabled from either the graphical user interface, or from the Direct Console User Interface (DCUI). When enabled, a warning is shown on the host, so that you are aware when vSphere ESXi Shell or SSH access to a host has been enabled. For security reasons, VMware recommends disabling these options until required by an administrator to decrease the attack surface of the ESXi host. **References:** *Using ESXi Shell in ESXi 5.x* and 6.0 (2004746) http://kb.vmware.com/kb/2004746 *ESXi tab in the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	Comments
Observation 3	2 cluster(s) have host HBA(s) configured inconsistently across ESX hosts. 1 cluster(s) have host NIC(s) configured inconsistently across ESX hosts.
Priority	P1
Recommendation	Place host devices in a consistent order and location.
Justification	Putting host devices in a consistent bus or slot for a particular type (vendor/model) facilitates automated installation and configuration, and makes administration and troubleshooting easier. Place storage adapters and network adapters on separate buses to reduce bus contention and improve performance. This does not apply for converged network adapters (CNA) with network and storage traffic. **References:** vSphere Installation and Setup Guide: http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-installation-setup-guide.pdf

Item	Comments
Observation 4	2 cluster(s) have host advanced parameter settings configured

	inconsistently across ESX hosts.
Priority	P2
Recommendation	Avoid unnecessary changes to advanced parameter settings.
Justification	Advanced parameters can cause unexpected behavior on ESXi hosts, if not configured correctly. It is best to avoid using them unless absolutely necessary. If they are used, it is best to perform a check to determine whether advanced parameters are consistently configured across ESXi hosts in a cluster. **References:** *Configuring Advanced options for ESXi (1038578)* *http://kb.vmware.com/kb/1038578* *vSphere Availability* guide *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-availability-guide.pdf*

3.1.1 Datacenter

Item	Comments
Observation 1	Strict Admission Control for 2 VMware HA enabled cluster(s) is not enabled.
Priority	P1
Recommendation	Size with HA host failure considerations.
Justification	VMware vCenter Server uses admission control to verify that sufficient resources are available in a cluster to provide failover protection and to protect virtual machine resource reservations. There are three different admission control policies: • The number of host failures that the cluster tolerates policy - In this case, HA calculates the slot size for the cluster. The slot size is generally based on the worst case CPU and memory reservation of any given virtual machine in the cluster but it can be configured differently as specified in the cluster configuration. This calculation can result in a conservative admission control policy, but is fully automated and allows virtual machines to be restarted in the event of a host failure. • The percentage of reserved cluster resources reserved policy - In this case, HA does not use the slot size calculation and uses a percentage of CPU and Memory resources for recovery from host failure. If the percentage reserved is low, virtual machines might not being protected due to insufficient resources. • Use Failover hosts - In this case, a host(s) are reserved as

	failover hosts. Sufficient capacity must be available on these stand-by hosts to ensure that recovery is possible in the event that a failure occurs. Selecting the number-of-host failures for HA admission control policy is recommended unless there are virtual machines with large reservations that result in a very conservative HA admission control policy. VMware recommends that all hosts in a cluster have similar CPU and memory configurations to have a balanced cluster and optimal HA resource calculations. **References:** VMware HA Admission Control section in *vSphere Availability* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-availability-guide.pdf*

Item	Comments
Observation 2	2 cluster(s) contain VM(s) and/or template(s) with mixed hardware versions.
Priority	P2
Recommendation	Maintain compatible virtual hardware versions for virtual machines.
Justification	Although not a recommended practice, clusters can have compatible but different versions of ESXi. This is known as Mixed Mode. Although this configuration allows you to create virtual machines with different virtual hardware, it also has these disadvantages: • New hardware virtual machines cannot be powered-on on older version hosts. • vSphere vMotion migrations are not possible between new and older hosts if the hardware level of the VM is not supported. • Limitations on deployment and creation of virtual machines per host. **References:** Virtual Machine Compatibility section of the *vSphere Virtual Machine Administration* Guide http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-virtual-machine-admin-guide.pdf

Item	Comments
Observation 3	10 virtual object(s) do not appear to follow a standard naming convention.

Priority	P2
Recommendation	Use a consistent naming convention for all virtual data center objects.
Justification	Using defined, documented, and consistent naming conventions provides order to the VMware virtual infrastructure and helps administrators readily and correctly identify its objects such as virtual machines, datacenters, clusters, resource pools, ESX hosts, vCenter folders, virtual switch port groups/dvport groups, uplink groups, datastores, templates, snapshots, and vApps. Define and use a consistent naming convention for datastores used in the VMware virtual infrastructure. Some attributes to incorporate in the naming convention are: • Type of storage (FC, NFS, and iSCSI) • Array vendor or type • Location • Business unit or function • Performance characteristics (RAID level) • Availability characteristics (replicated and non-replicated) • Hostname tag for local datastores Naming standards also help to streamline the troubleshooting and support process.

Item	**Comments**
Observation 4	5 user session(s) have been idle for at least 1 hour.
Priority	P2
Recommendation	Disconnect vSphere Clients from the vCenter Server when they are no longer needed.
Justification	vCenter Server must keep all client sessions current with inventory changes. When this process is used for connected but unused sessions attached to the vCenter Server, the vCenter Server system's CPU usage and user interface speed can be affected. To improve the performance of vCenter Server, disconnect vSphere Client sessions from the vCenter Server when they are no longer needed. This issue is true only for the vSphere Client. This behavior does not occur with the VMware vSphere Web Client. **References:** *Performance Best Practices for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

3.1.2 Network

Item	Comments
Observation 1	3 cluster(s) have inconsistently configured standard switches across ESX hosts. 1 cluster(s) have inconsistently configured distributed switches across ESX hosts.
Priority	P1
Recommendation	Configure networking consistently across all hosts in a cluster.
Justification	Minimize differences in the network configuration across all hosts in a cluster. Consistent networking configuration across all hosts in a cluster eases administration and troubleshooting. Also, because services such as vMotion require port groups to be consistently named, it is important to have a consistent configuration so that DRS and vSphere vMotion capabilities are not disrupted. A consistent naming convention for virtual switches, port groups, and uplink groups should also be used in the environment to prevent confusion when configuring virtual machines. VMware vSphere Distributed Switch™ can be used here to reduce administration time and promote consistency across the virtual data center. This is because changes to the distributed virtual port group are consistently and automatically applied to all hosts that are connected to the distributed switch. **References:** *vSphere Networking Guide* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf* *Security Hardening Guide* (vNetwork tab) http://www.vmware.com/security/hardening-guides.html

Item	Comments
Observation 2	1 host(s) has VMKernel port groups with no NIC redundancy.
Priority	P1
Recommendation	Verify that there is redundancy in networking paths and components to avoid single points of failure.
Justification	To avoid service disruption, make sure that the networking configuration is fault resilient to accommodate networking path and component failures. For example, provide at least two paths to each network. To do this configure all port groups and distributed virtual port

	groups with at least two uplink paths using different vmnics. NIC teaming can be used with at least two active NICs, to provide redundancy along with an increase in the available bandwidth for the network. Standby NICs can also be used, but are often seen as wasted resources, because they do not pass traffic unless a failure occurs. Set failover policy with the appropriate active and standby NICs for failover. Connect each physical adapter to different physical switches for an additional level of redundancy. In addition, upstream physical network components should also have the necessary redundancy to accommodate physical component failures. **References:** *vSphere Networking Guide* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf

Item	Comments
Observation 3	2 cluster(s) have portgroups configured inconsistently (either name or active NIC total speeds) across ESX hosts. 1 cluster(s) have distributed portgroups configured inconsistently (either name or active NIC total speeds) across ESX hosts.
Priority	P1
Recommendation	Minimize differences in the number of active NICs across hosts within a cluster.
Justification	Variance in the number of active NICs across hosts within a cluster can lead to inconsistent network performance when virtual machines are migrated to other hosts within a cluster. Hosts that have fewer NIC ports than others might experience network bottlenecks, but this might not be obvious if you assume that all hosts have the same number of active NIC ports available.

Item	Comments
Observation 4	18 standard portgroup(s) have NICs with mixed speed settings.
Priority	P1
Recommendation	Avoid mixing NICs with different speeds and duplex settings on the same uplink for a port group/dvport group.
Justification	Having a port group/dvportgroup mapped to multiple vmnics at different speeds is not recommended because, depending on the traffic load balancing algorithm, the network speed of the traffic can be arbitrarily and randomly determined and the result can be undesirable.

	For example, suppose there are several virtual machines all connected to a single vSwitch with two outbound adapters, one at 100-Mbps and one at 1-Gbps. Some virtual machines would have better performance than others depending on how their traffic is routed. A best practice is to verify that the speed is predictable and deliberately chosen.

Item	Comments
Observation 5	Network I/O Control is not enabled for 1 distributed virtual switch(es) that use 10 Gbps uplinks.
Priority	P1
Recommendation	Use Network I/O Control (NetIOC) to prioritize traffic.
Justification	All network traffic can benefit from NetIOC traffic prioritization during contention scenarios. 10-Gb Ethernet particularly can benefit from it as it provides high bandwidth for ESXi systems. If this bandwidth is not managed properly, an individual host can quickly saturate upstream network systems. VMware recommends enabling NetIOC to prioritize the correct network traffic across your data center. **References:** *Performance Evaluation of Network I/O Control in vSphere 6.0* *https://www.vmware.com/resources/techresources/10454*

Item	Comments
Observation 6	1 host(s) has VMKernel port groups with no NIC redundancy.
Priority	P1
Recommendation	Set up network redundancy for VMKernel network ports.
Justification	VMKernel network ports are the basis for many of the tasks that are performed on an ESXi host. Redundancy should be configured for each of the vmkernel ports, including: • Management Networks • iSCSI/NFS Storage networks • vMotion Networks • Fault Tolerance Logging Networks • Virtual SAN Networks Redundancy can most easily be accomplished by having multiple vmnics attached to the vSwitch. **References:** *vSphere Networking Guide*

	http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf

Item	Comments
Observation 7	4 DV Port Groups for Distributed Virtual Switches do not use Load-Based Teaming.
Priority	P1
Recommendation	Use Load-Based Teaming to balance virtual machine network traffic across multiple uplinks.
Justification	If link aggregation is not employed, Load-Based Teaming is the best option for spreading virtual machine traffic across multiple links. No additional physical network configuration is required when compared to the default, "Route based on originating virtual port ID." **References:** *Performance Evaluation of Network I/O Control in VMware vSphere 6* *https://www.vmware.com/resources/techresources/10454*

Item	Comments
Observation 8	10 host(s) have standard port groups which use a network that is not dedicated to a single type of traffic.
Priority	P1
Recommendation	Configure networks so that there is separation of traffic (physical or logical using VLANs).
Justification	Separate the following traffic where appropriate: • Management • IP storage • vMotion • Fault Tolerance Logging • Virtual machine • Virtual SAN • Provisioning • vSphere Replication Traffic separation improves performance, prevents bottlenecks, and increases security. Use physical separation or logical separation using VLANs as appropriate. Configure the physical switch ports as trunk ports for VLANs. **References:**

	Performance Best Practices for VMware vSphere 6.0 http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

Item	Comments
Observation 9	Outgoing traffic shaping is not enabled on 1 distributed virtual switches. Incoming traffic shaping is not enabled on 1 distributed virtual switches.
Priority	P1
Recommendation	Use DV Port Groups to apply policies to traffic flow types and to provide Rx bandwidth controls through the use of Traffic Shaping.
Justification	Configure each of the traffic flow types with a dedicated DV Port Group. For example, you might want to enable Traffic Shaping for the egress traffic on the DV Port Group used for vSphere vMotion. This can help in situations where multiple vMotion operation initiated on different vSphere hosts converge to the same destination vSphere server. **References:** *Performance Evaluation of Network I/O Control in VMware vSphere 6* *https://www.vmware.com/resources/techresources/10454*

Item	Comments
Observation 10	9 ESX host(s) have one or more port groups with physical NICs that share the same PCI bus.
Priority	P2
Recommendation	Distribute vmnics for a port group across different PCI buses for greater redundancy.
Justification	Distributing vmnics for a port group across different PCI buses provides protection from failures related to a particular PCI bus. Team vmnics from different PCI buses to improve fault resiliency from component failures.

Item	Comments
Observation 11	1 host(s) have physical NICs with misconfigured link speeds.
Priority	P3
Recommendation	Configure NICs, physical switch speed, and duplex settings consistently. Set to autonegotiation for 1-Gb NICs.
Justification	Incorrect network speed and duplex settings can impact performance. The network adapter (vmnic) and physical switch settings must be checked and set correctly. If your physical switch is configured for a specific speed and duplex setting, you must force the network driver to

	use the same speed and duplex setting. For Gigabit links, network settings should be set to auto-negotiate and not forced. You can set network adapter speed and duplex settings from the vSphere Client, but a reboot is required for changes to take effect. **References:** Solutions for Poor Network Performance section of *vSphere Monitoring and Performance vSphere 6.0* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-monitoring-performance-guide.pdf*

3.1.3 Security

Item	Comments
Observation 1	3 default users/group(s) are being used for vCenter user roles/permissions.
Priority	P1
Recommendation	Use vCenter Server roles, groups, and permissions to provide appropriate access and authorization to the virtual infrastructure. Avoid using Windows built-in groups such as the Administrators group.
Justification	By default, the administrator access is defined as a part of the Platform Services Controller installation. The configured user or group who has full administrative control of vCenter Server (and the virtual infrastructure). This can allow other system administrators who are not virtual infrastructure administrators access the infrastructure, if a dedicated group or user is not created. **References:** vSphere Users and Permissions section of the *vSphere Security Guide for vSphere 6.0* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf

Item	Comments
Observation 2	Tech Support Mode (TSM) timeout is not enabled for 10 host(s).
Priority	P1
Recommendation	Enable the ESXi Shell timeout feature and configure it per customer security requirements.
Justification	In ESXi, the ESXi Shell timeout feature automatically logs out unused ESXi Shell sessions to prevent unauthorized access.

	Set a timeout that does not disrupt the standard VMware administrator workflow. Setting appropriate timeout also avoids indefinite idle connection and unwanted privileged host access. **References:** ESXi tab in the *VMware Security Hardening Guides* http://www.vmware.com/security/hardening-guides.html

Item	Comments
Observation 3	Default firewall settings have been modified from default for 10 ESX host(s).
Priority	P1
Recommendation	Configure firewall rules and ports according to best practices.
Justification	The default firewall rules are configured to provide adequate security while allowing communication with the appropriate VMware virtual infrastructure components. Unless required to enable communication for VMware virtual infrastructure services, avoid changing firewall rules because this can introduce additional security issues. VMware recommends that you leave the default security firewall settings in place. These settings block all incoming and outgoing traffic that is not associated with enabled service. If you enable a service and open ports for it, document the changes, including the purpose for opening each port. Consistently make the changes on all the appropriate ESXi hosts and avoid changing the default ports unless necessary. **References:** VM and ESXi tabs in the *VMware Security Hardening Guides.* *http://www.vmware.com/security/hardening-guides.html* *TCP and UDP Ports required to access vCenter Server, ESX hosts, and other network components (1012382)* http://kb.vmware.com/kb/1012382 TCP and UDP Ports section in the *vSphere Security Guide* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf

Item	Comments
Observation 4	(b) (7)(E) [redacted].
Priority	P2
Recommendation	(b) (7)(E) [redacted]

Justification	(b) (7)(E) [redacted]
	(b) (7)(E) [redacted]
	(b) (7)(E) [redacted]

References:

	VM Tab of the *VMware Security Hardening Guides* http://www.vmware.com/security/hardening-guides.html

Item	Comments
Observation 5	10 host(s) have one or more port groups that allow forged transmits. 10 host(s) have one or more port groups that allow MAC address changes.
Priority	P2
Recommendation	Change port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes to Reject unless required.
Justification	VMware recommends that port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes be set to Reject for improved security. When the MAC address changes option is set to Reject, ESXi does not honor requests to change the effective MAC address to a different address than the initial MAC address. This setting protects the host against MAC impersonation. To protect against MAC impersonation, you can set the **Forged transmits** option to **Reject**. If you do, the host compares the source MAC address being transmitted by the guest operating system with the effective MAC address for its virtual machine adapter to see if they match. When the addresses do not match, the ESXi host drops the packet. Promiscuous mode eliminates any reception filtering that the virtual machine adapter performs so that the guest operating system receives all traffic observed on the wire. By default, the virtual machine adapter cannot operate in promiscuous mode. **References:** Securing ESXi Configurations section in the *vSphere Security Guide for vSphere 6.0* http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf *vNetwork Tab of the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	Comments
Observation 6	277 VM(s) have not configured RemoteDisplay.maxConnections value.
Priority	P2
Recommendation	Limit sharing console connections if there are security concerns.

Justification	By default, more than one user at a time can connect to remote console sessions. When multiple sessions are activated, each terminal window gets a notification about the new session. If an administrator in the virtual machine logs in using a VMware remote console during their session, a non-administrator in the virtual machine might connect to the console and observe the administrator's actions. Also, this can result in an administrator losing console access to a virtual machine. For example, if a jump box is being used for an open console session, and the administrator loses connection to that box, then the console session remains open. Allowing two console sessions permits debugging by way of a shared session. For highest security, only one remote console session at a time should be allowed. **References:** *VM Tab of the VMware Security Hardening Guides* *http://www.vmware.com/security/hardening-guides.html*

Item	Comments
Observation 7	9 host(s) have host bus adapters without bidirectional CHAP authentication setup.
Priority	P2
Recommendation	Enable bidirectional CHAP authentication for iSCSI traffic so that CHAP authentication secrets are unique.
Justification	vSphere allows for the use of bidirectional authentication of both the iSCSI target and host. By not authenticating both iSCSI target and host, there is a potential for a man-in-the-middle attack where an attacker can impersonate either side of the connection to steal data. Bidirectional authentication can mitigate this risk. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation. VMware recommends that the mutual authentication secret for each host be different. Set the secret different for each client authenticating to the server so that if a single host is compromised, an attacker cannot create another arbitrary host and authenticate to the storage device. With a single shared secret, compromise of one host can allow an attacker to authenticate to the storage device. **References:** ESXi tab of the *VMware vSphere Security Hardening Guides* http://www.vmware.com/security/hardening-guides.html

3.1.4 Storage

Item	Comments
Observation 1	10 host(s) have standard port groups that use a network that is not dedicated to a single type of storage(NFS or iSCSI) traffic.

Priority	P1
Recommendation	Configure NFS and iSCSI storage traffic for performance and security.
Justification	Storage traffic is potentially the most important of all for Virtual Machine performance. When configuring the network for storage traffic it should be: • low latency and have adequate bandwidth • Use dedicated pNICs • Use a dedicated IP storage network • Use isolated networks that are placed on different subnets **References:** *vSphere Storage Guide for vSphere 6.0* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-storage-guide.pdf*

Item	**Comments**
Observation 2	18 datastore(s) do(es) not have Storage I/O Control enabled.
Priority	P2
Recommendation	Use Storage I/O Control (SIOC) to prioritize high importance virtual machine traffic.
Justification	SIOC engages only if the storage system hosting a virtual machine becomes congested, as measured by increased latency. If congestion occurs, SIOC enforces disk I/O fairness among virtual machines, even across different hosts, respecting disk shares per virtual machine. Without SIOC, disk shares enforce fairness only among virtual machines on the same host. SIOC does not function correctly unless all datastores that share the same spindles on the array have the same congestion threshold. **References:** Storage I/O Resource Allocation section in *Performance Best Practices for VMware vSphere* 6.0 http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

Item	**Comments**
Observation 3	2 datastore(s) have both VMs and Templates.
Priority	P2
Recommendation	Allocate space on shared datastores for templates and media/ISOs separately from datastores for virtual machines.

Justification	To improve performance, separate virtual machine files from other files such as templates and ISO files that have higher I/O characteristics. As best practice, dedicate separate shared datastores/LUNs for virtual machine templates and to separate ISO/FLP files from the virtual machines. As of vSphere 6.0, VMware recommends using the Content Library for Media and template storage. Media files can be placed either locally on each host or in a shared datastore. To avoid storing unnecessary copies, place media files on shared storage.

3.1.5 Virtual Machines

Item	Comments
Observation 1	11 VM(s) do not meet some of the VMotion requirements (either floppy/cd-rom found, VM in internal network, network or datastore not visible to all ESX in cluster). VMotion traffic for 10 host(s) is on less than 1 GB network.
Priority	P1
Recommendation	Verify that virtual machines meet the requirements for vSphere vMotion.
Justification	To facilitate vSphere vMotion operations of virtual machines between hosts the following requirements must be met: • The source and destination hosts must use shared storage and the disks of all virtual machines must be available on both source and target hosts, or storage will be migrated. This comes with a cost in performance, resource utilization (storage and network) while migration occurs. • The port group names must be the same on the source and destination hosts or the networking will also need to be migrated. This could impact connectivity if incorrect network is chosen. • vSphere vMotion requires a 1-Gbps network interface. However, using a 10-Gbps network interface or multiple 1-Gbps network interfaces will result in significant improvements in vSphere vMotion performance. • CPU compatibility - source and destination hosts must have compatible CPUs [relaxed for Enhanced vMotion Compatibility(EVC)]. • No devices are attached that prevent vSphere vMotion (CDROM, floppy, serial/parallel devices) are attached. Prior to bringing an ESXi host into production, testing vMotion is recommended..

	References: VMware vMotion Best Practices in the VMware vMotion section of *Performance Best Practices guide for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf *vSphere Networking Guide for vSphere 6.0* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-networking-guide.pdf*

Item	Comments
Observation 2	15 VM(s) have snapshot(s).
Priority	P1
Recommendation	Limit use of snapshots, and when using snapshots limit them to short-term use.
Justification	Snapshots allow point-in-time state captures, which allow virtual machines to have their states reverted to a snapshot for testing and recovery. However, multiple snapshots result in more disk usage. Although SCSI contention was significantly improved in VMFS5, VMware recommends limiting use of snapshots, and when used, limiting them to short-term use.

Item	Comments
Observation 3	1 VM(s) do not have VMware Tools installed. 9 VM(s) have VMware Tools installed that are not up to date. 1 VM(s) do not have VMware Tools running.
Priority	P1
Recommendation	Verify that VMware Tools is installed, running, and up to date for running virtual machines.
Justification	Install VMware Tools (including open-vm-tools where applicable) in all guests that have supported VMware Tools available. **Note :** *open-vm-tools* is the open source implementation of VMware Tools and consists of a suite of virtualization utilities that improves the functionality, administration, and management of virtual machines within a VMware environment. The primary purpose for open-vm-tools is to enable operating system vendors and/or communities and virtual appliance vendors to bundle VMware Tools into their product releases. For compatibility and optimal performance, upgrade VMware Tools for older virtual machines to the latest versions supported by their ESXi hosts. For security purposes, disable the tools `autoinstall` option by setting

	the parameter `isolation.tools.autoInstall.disable` to True.

Item	Comments
Observation 4	11 VM(s) has(ve) unnecessary virtual device(s) that is/are either connected or start connected.
Priority	P2
Recommendation	Allocate only as much virtual hardware as required for each virtual machine. Disable any unused or unnecessary or unauthorized virtual hardware devices.
Justification	Provisioning a virtual machine with more resources than it requires can reduce the performance of that virtual machine and virtual machines that share the same host. For example, configuring more vCPUs than required for an application that is single threaded can reduce overall performance. Also, configuring more memory than required can impact the other virtual machines on the same host. In addition to disabling unnecessary virtual devices within the virtual machine, verify that no device is connected to a virtual machine if it is not needed there. For example, serial and parallel ports are rarely used for virtual machines in a data center environment, and CD/DVD drives are usually connected only temporarily during software installation. Disabling any unused or unnecessary virtual hardware devices improves performance (because it can reduce device polling), improves security, and reduces the probability of these devices preventing vSphere vMotion from succeeding. Disabling or disconnecting unauthorized devices enhances the security levels of the virtual machines and their hosts. Virtual machine performance can also be improved by configuring the virtual machines to use ISO images instead of physical drives. Physical drives can be avoided entirely by disabling optical drives in the virtual machines when the devices are not needed. **References:** Best Practices for Virtual Machine and Host Security sections of the *vSphere Security Guide for vSphere 6.0* *http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-security-guide.pdf*

Item	Comments
Observation 5	61 VMs are not using latest virtual hardware profile.
Priority	P2
Recommendation	Use the latest virtual hardware version to take advantage of additional capabilities.

Justification	ESXi 6.0 introduces virtual hardware version 11. By creating virtual machines using this hardware version, or upgrading existing virtual machines to this version, additional capabilities become available. This hardware version is not compatible with versions of ESXi prior to 6.0. If a cluster of ESXi hosts contains some hosts running pre-6.0 versions of ESXi, the virtual machines running on virtual hardware version 10 are constrained to run only on the ESXi 6.0 hosts. This could limit vSphere vMotion choices for vSphere DRS or DPM. **References:** *vSphere Virtual Machine Administration* Guide for vSphere 6.0 http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-60-virtual-machine-admin-guide.pdf

Item	Comments
Observation 6	2 VM(s) are not using VMXNET3 even though their configuration and guest OS support it.
Priority	P2
Recommendation	Use the latest version of VMXNET that is supported by the guest operating system.
Justification	For best performance, use the VMXNET3 paravirtualized network adapter for operating systems where it is supported. This requires that the virtual machine use at least virtual hardware version 7 and that VMware Tools be installed in the guest operating system. If VMXNET3 is not supported by the guest OS, use Enhanced VMXNET (VMXNET2). If Enhanced VMXNET is not supported in the guest operating system, then use the flexible device type, which automatically converts each AMD PCnet32 device (vlance) network device to a VMXNET device when VMware Tools is installed. Refer to information in the Knowledge Base article and product documentation for supported guest operating systems for the particular adapter. **References:** *Choosing a network adapter for your virtual machine* (1001805) http://kb.vmware.com/kb/1001805 Guest Operating System Networking Considerations section in *Performance Best Practices for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

Item	Comments

Observation 7	10 VM(s) have an installed OS that differs from the configured type.
Priority	P3
Recommendation	Select the correct guest operating system type in the virtual machine configuration to match the guest operating system.
Justification	Selecting the guest operating system type determines the following: • Optimal monitor mode to use • Default optimal devices for the guest OS (such as SCSI controller and network adapter) • The optimal default resource configuration for CPU/RAM • Appropriate VMware Tools to be installed in the guest OS Verify that the guest OS type matches the operating system installed in the virtual machine to maintain the performance and manageability of the virtual machine. You can change the guest OS type only when the virtual machine is powered off.

Item	Comments
Observation 8	
Priority	P3
Recommendation	Use reservations and limits selectively on virtual machines.
Justification	Setting reservations and limits on virtual machines increases the management overhead of the VMware virtual infrastructure, so selectively set these only on virtual machines that need it. For reservations do not set them too high because doing so can limit the number of virtual machines that you can power on in a resource pool, cluster, or host. Setting reservations can also affect the slot size calculation for HA clusters, which can affect the admission control policy of an HA cluster (for admission control policy of number of host failures). For limits, do not set them too low because doing so can affect the amount of CPU or memory resources available to the virtual machines, which can affect the overall performance. **References:** General Resource Management section in *Performance Best Practices for VMware vSphere 6.0* http://www.vmware.com/files/pdf/techpaper/VMware-PerfBest-Practices-vSphere6-0.pdf

3.2 Findings and Recommendations for View

The following table contains summary of the results of the View Health Check that was performed during this project. Details of these items are in the following sections of this document.

Table 2: Summary of View Health Check Findings and Recommendations

Priority	Component	Recommended Action Item
P1	Desktop Operating System	Verify that all guest OS installations were performed using a clean install.
P1	Desktop Operating System	Verify that the guest operating system was created using the VMware optimization guides. Determine which optimizations were applied and verify.
P1	Infrastructure	Verify that the Horizon View environment is configured to collect event information in a Horizon View events database.
P1	View Administrator	Verify that no Horizon View services or servers are down or have been down.
P1	View Connection Server	Verify that the Horizon View connection servers are configured with a system disk of at least 70 GB.
P1	vSphere Storage	Verify that the network is configured for jumbo frames on NFS/iSCSI connections.
P1	vSphere Storage	Verify that virtual desktops are distributed evenly across datastores.
P2	ESX/ESXi hosts	Verify that there are no unusually high disk I/O latencies or IOPS (CMDS/s, GAVG).
P3	vCenter	Verify that vCenter servers supporting the Horizon View environment are dedicated only to supporting Horizon View. Use separate vCenter servers for supporting the virtualized server environment.

3.3 Priority 1 Recommendations

Item	Comments
Observation 1	Master image has optimization potential
Priority	P1
Infrastructure Qualities	Configuration.
Recommendation	Verify that all guest OS installations were performed using a clean install.
Justification	While it is common for enterprises to take an existing physical desktop

	image and convert it to be virtualized, this generally results in slower performance to both the desktop and the virtual infrastructure. Creating a clean virtual machine and installing from scratch, with the proper optimizations in place and only the required applications, provides a much better performing virtual machine and subsequently better performing host and environment. **References** Windows XP Deployment Guide http://www.vmware.com/files/pdf/XP_guide_vdi.pdf VMware View Optimization Guide for Windows 7 http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf

Item	Comments
Observation 2	Master image has optimization potential
Priority	P1
Infrastructure Qualities	Performance, configuration.
Recommendation	Verify that the guest operating system was created using the VMware optimization guides. Determine which optimizations were applied and verify.
Justification	This is critical for a smooth-running desktop operating system. Customizations improve performance considerably. **References** *VMware View Optimization Guide for Windows 7* http://www.vmware.com/files/pdf/VMware-View-OptimizationGuideWindows7-EN.pdf *VMware OS Optimization Tool* http://labs.vmware.com/flings/vmware-os-optimization-tool

Item	Comments
Observation 3	No event database has been running in Horizon View environment to collect View events. This observation was collected when the event database was offline. The Database periodically goes on and offline. Recommend detaching and reattaching using FQDN of database server.
Priority	P1
Infrastructure Qualities	Availability, manageability, configuration.
Recommendation	Verify that the Horizon View environment is configured to collect event information in a Horizon View events database.

Justification	This allows for segregated management of the server and isolation of components supporting Horizon View. **References** *VMware Horizon with View Installation (6.x)* https://pubs.vmware.com/horizon-view-60/topic/com.vmware.ICbase/PDF/horizon-view-60-installation.pdf *VMware Horizon View Installation (5.x)* http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-installation.pdf

Item	Comments
Observation 4	4 View service(s) or server(s) is/are down.
Priority	P1
Infrastructure Qualities	Availability, configuration.
Recommendation	Verify that no Horizon View services or servers are down or have been down. Two connection servers are offline (intentional) and the events database connection periodically shows as an error.
Justification	These events can indicate problems in the environment.

Item	Comments
Observation 5	2 Connection server(s) are configured with system disk size less than the recommended size.
Priority	P1
Infrastructure Qualities	Availability, manageability, configuration.
Recommendation	Verify that the Horizon View connection servers are configured with a system disk of at least 70 GB.
Justification	The system disk should be 70GB or greater if you are configuring Horizon View. **References** *VMware Horizon with View Architecture Planning (6.x)* https://pubs.vmware.com/horizon-view-60/topic/com.vmware.ICbase/PDF/horizon-view-60-architecture-planning.pdf *VMware Horizon View Architecture Planning (5.x)* http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-architecture-planning.pdf

Item	Comments
Observation 6	10 NFS/ISCSI connections have been found to have management ports not configured for jumbo frames.
Priority	P1
Infrastructure Qualities	Performance, scalability, configuration.
Recommendation	Verify that the network is configured for jumbo frames on NFS/iSCSI connections.
Justification	Use of jumbo frames enhances storage performance. **References** *Performance Best Practices for VMware vSphere (5.5)* http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf *Performance Best Practices for VMware vSphere (5.1)* http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf *Performance Best Practices for VMware vSphere (5.0)* http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf

Item	Comments
Observation 7	Desktops on 2 datastore(s) are not distributed evenly.
Priority	P1
Infrastructure Qualities	Manageability, performance, scalability, configuration.
Recommendation	Verify that virtual desktops are distributed evenly across datastores.
Justification	This reduces storage contention and balances I/O loads. This helps to avoid SCSI reservation locking, for example. An even distribution of desktops spreads the I/O load so you do not have a single datastore handling most of the total I/O or causing unnecessary storage I/O contention. This goes together with the practice of rebalancing. In some situations, there may be different datastores for those very different desktop pool workloads, but even then you should balance the desktop distribution.

3.4 Priority 2 Recommendations

Item	Comments
Observation 1	Monitor VM statistics to ensure appropriate sizing.

Priority	P2
Infrastructure Qualities	Performance.
Recommendation	Verify that there are no unusually high disk I/O latencies or IOPS (CMDS/s, GAVG).
Justification	Many Horizon View implementations are impacted by poor storage design or performance. These issues can be identified on ESX hosts running virtual desktop workloads using ESXTOP. **References** Interpreting esxtop 4.1 Statistics http://communities.vmware.com/docs/DOC-11812

3.5 Priority 3 Recommendations

Item	Comments
Observation 1	1 vCenter(s) is/are not exclusively used for Horizon View environment.
Priority	P3
Infrastructure Qualities	Manageability, performance, scalability, configuration.
Recommendation	Verify that vCenter servers supporting the Horizon View environment are dedicated only to supporting Horizon View. Use separate vCenter servers for supporting the virtualized server environment. This is a small environment. It is best practice to have two vCenter servers, one managing the server systems and another managing only the desktop systems.
Justification	This allows for segregated management and provides room for growth as desktop deployments increase in the future. **References** *VMware Horizon with View Installation (6.x)* https://pubs.vmware.com/horizon-view-60/topic/com.vmware.ICbase/PDF/horizon-view-60-installation.pdf *VMware Horizon View Installation (5.x)* http://pubs.vmware.com/view-52/topic/com.vmware.ICbase/PDF/horizon-view-52-installation.pdf

5. VMware View Environment

The MSPB VMware View infrastructure must support up to 300 virtual desktops. There are currently 225 users configured.

This section provides the inventory of VMware View infrastructure collected during this engagement. It is important for MSPB to consider the recommendations given earlier in this document. The recommendations will assist MSPB in optimizing the existing implementation and enable the environment to scale with an acceptable and stable level of performance.

5.1 VMware View Inventory

5.1.1 View Connection Servers

5.1.1.1. Platform Specifications

- System: VMware Virtual Machine
- CPU: 4 vCPU
- RAM: 10 GB
- Disk: 140,0,120 GB

5.1.1.2. View Connection Server Virtual Machines

[redacted]

- Role: [redacted]
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

[redacted]

- Role: [redacted]
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

[redacted]

- Role: [redacted]
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E)

- Role: (b) (7)(E)
- NICs: 1 vNIC
- VMware Tools: guestToolsCurrent
- Virtual Devices: CD/DVD ,1 Floppy
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E)

- Role: (b) (7)(E)
- NICs: 1 vNIC
- VMware Tools:
- Virtual Devices: N/A
- Version: - 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

(b) (7)(E)

- Role: (b) (7)(E)
- NICs: 1 vNIC
- VMware Tools:
- Virtual Devices: N/A
- Version: 6.0.1-2088845
- OS: Microsoft Windows Server 2008 R2 (64-bit)

5.1.2 Hosted View Desktop Environment

vCenter Server Clusters

- (b) (7)(E)
  - ESX Versions: VMware ESXi - 5.5.0
- (b) (7)(E)
  - ESX Versions: VMware ESXi - 5.5.0
- (b) (7)(E)
  - ESX Versions: VMware ESXi – 5.5.0

5.1.3 View Desktop Pools

The configuration of these desktop pools is detailed in the following sections.

TEST

Type	Automated Desktop Pool
Desktop persistence	Floating
Desktop source	vCenter (linked clone)
Display state	Enabled
Number of desktop sources	6
vCenter Server	(b) (7)(E)
Tags	
When virtual machine is not in use	alwaysOn
Automatic logoff after disconnect	After
Allow user resets	No
Allow multisessions per user	No
Default display protocol	PC-over-IP
Allow user protocol override	Yes
Adobe Flash quality	noControl
Adobe Flash throttling	Disabled
Advanced Parameters	PCoIP # of monitors: 4 PCoIP Resolution: 1920x1200

MSPB

Type	Automated Desktop Pool
Desktop persistence	Floating
Desktop source	vCenter (linked clone)
Display state	Enabled

Number of desktop sources	200
vCenter Server	(b) (7)(E)
Tags	
When virtual machine is not in use	alwaysOn
Automatic logoff after disconnect	After
Allow user resets	No
Allow multisessions per user	No
Default display protocol	PC-over-IP
Allow user protocol override	Yes
Adobe Flash quality	noControl
Adobe Flash throttling	Disabled
Advanced Parameters	PCoIP # of monitors: 4 PCoIP Resolution: 2560x1600

5.1.4 Virtual Desktop Master Images

A virtual machine master is a copy, or *golden image*, of a virtual machine that can be used to create and provision new virtual machines. Typically, a master image includes an installed guest operating system and a set of applications.

It is a best practice to deploy a desktop pool manually or automated from a standardized desktop source, or template. Provisioning virtual machines in a desktop pool configures all virtual machines with the same settings, loaded operating system, applications and patches.

In addition, consider multiple desktop templates based on pool, department, or function. This is so that specific optimizations can be made to particular department virtual desktops without adversely affecting another desktop pool, while maintaining an efficient virtual desktop environment.

Conforming to these best practices reduces the complexities of troubleshooting, desktop pool deployments, recomposing, or recovering processes.

5.1.4.1. Desktop Master Build Process

The current desktop build process adheres to VMware best practices. MSPB uses the VMware Optimization Tool to maximize the performance on the linked clone desktops. It is recommended to continue to use the Optimization Tool and create additional master images dedicated to different use cases with isolated applications specific to users needs.

5.1.4.2. Master Desktop Virtual Machine Specifications

The following is a detailed report for the master image. All of the items identified with a yellow box are available optimizations that MSPB may benefit from configuring on the master image.

Analysis Report

Date: 9/1/2015 12:39:19 PM **Template**: Windows7 (built-in)

System Information

Operating System	Microsoft Windows 7 Enterprise	**System Name**	(b) (7)(E)
Version	Microsoft Windows NT 6.1.7601 Service Pack 1	**User Name**	(b) (7)(E)
Processor	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz	**Windows Directory**	C:\Windows
System Type	32-bit	**System Directory**	C:\Windows\system32
Physical Memory (RAM)	3.00 GB	**Locale**	United States

Details:

	Steps	Description	Expected Result	Actual Result
Apply HKCU Settings to Registry				
	Load HKCU for editing	Open HKey Users (Default User Profile) for Editing		
	Action Center Icon - Disable	The Action Center Icon notifies the user of the firewall, anti virus, security related things, etc. that may be configured differently than expected. Disabling this service can be useful to avoid end user confusion.	1	
	Default power setting	Set Start button > Power to log off as the default.	1	
	Default Screen Saver	Set the default screen saver to "Blank" - any graphics screensaver will put extra load on the virtual infrastructure.	%windir%\system32\scrnsave.scr	
	Lower Terminal Server Client send interval	Lower Terminal Server Client send interval	1	
	Reduce Menu Show Delay	Delay Show the Reduce Menu	120	

	Steps	Description	Expected Result	Actual Result
	RSS Feeds - Disable	Perform this task to disable RSS feed capability and potentially improve performance and reduce requirements for disk space growth related to this service.	0	
	Screen Save Secure	Secures the VM in case a user walks away	1	
	Screen Saver Timeout	Timeout set to 10 mins	600	
	Set Default Wallpaper	Set wallpaper to a "non existing" file to disable the end users ability to set a wallpaper.		
	Temporary Internet Files to Non Persistent	Purge cache for IE on every close of IE. Non persistence	0	
	Visual Effects	Set Windows Visual Effects to Optimized for best performance.	3	
	Unload HKCU for editing	Very Important Step! Need to close the ntuser.dat file to save changes.		
Apply HKLM Settings				
	Application Event Log Max Size	Set max size on Event Log to 1 MB	1048576	1048576
	Application Event Log Retention	Set no retention	0	0
	Background Layout Service - Disable	Disable Background Layout Service	0	0

	Steps	Description	Expected Result	Actual Result
	CIFS Change Notifications - Disable	Disable CIFS Change Notifications	1	1
	Crash Control - Automatically Reboot - Enable	Enable Automatically Reboot for the Crash Control	1	1
	Crash Control - Sending alert - Disable	Disable sending alert for the Crash Control	0	0
	Crash Control - Writing event to the system log - Disable	Disable writing event to the system log for the Crash Control	0	0
	Creation of Crash Dump - Disable	Removes the creation of a Crash Dump file	0	0
	Customer experience improvement program - Disable	Disable customer experience improvement program	0	0
	Disk Timeout Value	How long the OS will wait for a disk write or read to take place on the SAN without throwing an error	200	200
	Do not buffer UDP packets less than 1500 Bytes	Improves high bandwidth video performance	1500	1500
	Enable Remote Desktop	Enables RDP	0	0
	Hide Fast User Switching	Hide Fast User Switching	1	1
	Hide Hard Error Messages	Hide Hard Error Messages	0	0

	Steps	Description	Expected Result	Actual Result
	IE Wizard - Disable	Removes the customization wizard upon first launch of Internet Explorer	1	1
	Image Revision	Image Revision	1.0	1.0
	Image Virtual	Registry Entry to identify if virtual machine	Yes	Yes
	Increase Service Startup Timeout	Allows up to 120 seconds before timing out waiting for a service	120000	120000
	IPv6 - Disable	Disable IPv6	255	255
	Machine Account Password Changes - Disable	Disable Machine Account Password Changes	0	0
	Network Location	Creates a blank key that disables the "Choose default network location" prompt.		
	Remote Desktop Authentication	Sets default authentication level.	0	
	Screen Saver at Logon/Welcome Screen - Disable	Making modifications to .DEFAULT	0	0
	Security Event Log Max Size	Set max size on Event Log to 1 MB	1048576	
	Security Event Log Retention	Sets no retention	0	
	Set Wallpaper to blank at Logon/Welcome Screen	Making modifications to .DEFAULT		

	Steps	Description	Expected Result	Actual Result
	Storing Recycle Bin Files - Disable	Deleting files will delete immediately instead of storing in the recycle bin. Same behavior as non persistent VM	1	1
	Superfetch (Registry) - Disable	Set Superfetch to boot files only.	0	0
	System Event Log Max Size	Set max size on Event Log to 1 MB	1048576	1048576
	System Event Log Retention	Set no retention	0	0
	System Restore - Disable	Disable System Restore. System Restore provides rollback capability that should not be leveraged in a VDI environment. Space and reliability are factors.	1	1
	TCP/IP Task Offload - Disable	Disable TCP/IP Task Offload	1	1
	UAC - Disable	Disables User Access Control. Use Group Policy to configure more granularly	0	0
	Windows Sideshow - Disable	Disable Windows Sideshow	1	1
	Windows Update - Disable	Disable Automatic Update - important for non persistent VMs	1	0
Disable Features				
	Boot GUI	Disable the graphic for the Windows 7 boot	N.A	N.A

	Steps	Description	Expected Result	Actual Result
	Delete Restore Points for System Restore	Removes all restore points if they exist	N.A	N.A
	Firewall (All Profiles)	Netsh to disable firewall on all profiles.	N.A	N.A
	Hibernation for Power Config	Disable Hibernation for Power Config	N.A	N.A
	Last Access Timestamp	Disable Last Access Timestamp	N.A	N.A
	Stop Superfetch Service	Stop Superfetch Service	N.A	N.A
	System Restore	Powershell command to immediately disable system restore	N.A	N.A
Disable Scheduled Tasks				
	Application Experience - AitAgent	Disable Application Experience - AitAgent	DISABLED	Disabled
	Application Experience - Program Data Updator	Disable Application Experience - Program Data Updator	DISABLED	Enabled
	CEIP Consolidator	Disable Customer Experience Improvement Program (CEIP) scheduled task	DISABLED	Disabled
	CEIP Kernel	Disable Customer Experience Improvement Program (CEIP) scheduled task	DISABLED	Disabled
	CEIP Usb	Disable Customer Experience Improvement Program (CEIP)	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
		scheduled task		
	Defrag Schedule	Disable Defrag Schedule	DISABLED	Disabled
	Registry Idle Backup Task	Disable Registry Idle Backup Task	DISABLED	Disabled
	System Restore Schedule	Disable System Restore Schedule	DISABLED	Disabled
	Windows Defender Idle Task	Disable Windows Defender Idle Task	DISABLED	
	Windows Defender Schedule	Disable Windows Defender Schedule	DISABLED	Disabled
	WinSAT	Measures performance of Windows 7 and provides an index number. Causes performance impact on VMs.	DISABLED	Disabled
Disable Services				
	Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is disabled, Windows Update and MSN Explorer cannot automatically download programs and other information.	DISABLED	Manual
	Bitlocker Drive Encryption Service	Bitlocker service for drive encryption. Not recommended to encrypt VDI virtual machines.	DISABLED	Disabled
	Block Level Backup Engine Service	Used by Windows Backup	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
	BranchCache	Used for caching files on server in a branch office.	DISABLED	Disabled
	Change Group Policy Client start mode to manual	Responsible for applying settings configured by administrator for the computer and users through the Group Policy component.	MANUAL	Auto
	Computer Browser	Used for browsing computers on the same network.	DISABLED	Disabled
	Desktop Window Manager Session Manager	Used for Aero - disable if Aero is not desired. (VMware product compatibility: Do not disable if View 5.3 package will be installed.)	DISABLED	Auto
	Diagnostic Policy Service	Disable Diagnostic Policy Service	DISABLED	Disabled
	Diagnostic Service Host	Problem detection and troubleshooting resolution.	DISABLED	Disabled
	Diagnostic System Host	Problem detection and troubleshooting resolution.	DISABLED	Disabled
	Disk Defragmenter Service	Defrag can create unnecessary overhead on a virtual machine - the scheduled defrag has been set to disable below as well as disabling this service.	DISABLED	Disabled
	Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
		Services - Discovery (WS-D) protocol.		
	Function Discovery Resource Publication	Publishes his computer and resources attached to this computer so they can be discovered over the network.	DISABLED	Disabled
	HomeGroup Listener	Used for Homegroup services - N/A for VDI	DISABLED	Unknown
	HomeGroup Provider	Used for Homegroup services - N/A for VDI	DISABLED	Disabled
	Interactive Services Detection	Displays a dialog box when a service tries to send a message to the console.	DISABLED	Disabled
	IP Helper	Disable if IPv6 is not a factor in VDI	DISABLED	Disabled
	Media Center Extender	Allows Media Center Extenders to locate and connect to the computer.	DISABLED	
	Microsoft iSCSI Initiator Service	Not leveraged in a VDI	DISABLED	Disabled
	Microsoft Software Shadow Copy Provider	Leveraged by Windows Backup and System Restore.	DISABLED	Disabled
	Offline Files	Disable Offline Files	DISABLED	Disabled
	Reports and Solutions Control Panel Support	Provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports and Solutions control panel.	DISABLED	Disabled
	Secure Socket Tunneling	VPN tunneling service. Not likely leveraged in a	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
	Protocol Service	VDI environment.		
	Security Center	Remove the task tray regarding security center warnings	DISABLED	Disabled
	SSDP Discovery	Disable SSDP Discovery	DISABLED	Disabled
	Superfetch	Service is leveraged to optimize loading of applications over time. In a non persistent or commodity based VDI environment this service may impact performance. Depends on use and organization.	DISABLED	Disabled
	Tablet Services	Disable if you are not using Tablet PC functionality	DISABLED	Disabled
	Themes	Disable if you want to run "Classic" GUI	DISABLED	Disabled
	Universal PnP Host Service	Dependent on the SSDP Service.	DISABLED	Disabled
	Volume Shadow Copy Service	Used for System Restore and Backup Operations. (VMware product compatibility: Do not disable if Persona Management is in use.)	DISABLED	Disabled
	Windows Backup	Windows Backup service used by System Restore and Windows Backups.	DISABLED	Disabled
	Windows Defender Service	Windows Defender can be optionally disabled in a VDI environment especially for non persistent VMs where data will be purged. A scheduled task has also been marked to disable	DISABLED	Disabled

	Steps	Description	Expected Result	Actual Result
		below.		
	Windows Error Reporting Service	Error reporting services leveraged by Applications when they crash to send reports to Microsoft. If using DER within VDI consider alternate configuration.	DISABLED	Disabled
	Windows Firewall	Recommended to customize instead of disable the firewall.	DISABLED	Auto
	Windows Media Center Network Sharing Service	Used by Media Center	DISABLED	Disabled
	Windows Media Center Receiver Service	Media Center Service Related	DISABLED	
	Windows Media Center Scheduler Service	Media Center Service Related	DISABLED	
	Windows Search	If you do a lot of searching on a VM, do not disable this service.	DISABLED	Disabled
	Windows Update	If this is a non persistent VM, Windows Update should be handled differently via standard image maintenance practices.	DISABLED	Disabled
	WLAN AutoConfig	Wireless LAN Configuration - N/A for VDI environments.	DISABLED	Disabled
	WWAN AutoConfig	Service related to Mobile Broadband Devices	DISABLED	Disabled
Disable Visual Effects				

	Steps	Description	Expected Result	Actual Result
	Aero Peek	Disable Desktop Window Manager Aero Peek Visual Effect	0	1
	Animate Min/Max Windows	Disable Animate Min/Max Windows Visual Effect	0	1
	ComboBox Animation	Disable ComboBox Animation Visual Effect	0	1
	Control Animations	Disable Control Animations Visual Effect	0	1
	Cursor Shadow	Disable Cursor Shadow Visual Effect	0	1
	Desktop Window Manager	Disable Desktop Window Manager Visual Effect	0	1
	Drag Full Windows	Disable Drag Full Windows Visual Effect	0	1
	Drop Shadow	Disable Drop Shadow Visual Effect	0	1
	Font Smoothing	Disable Font Smoothing Visual Effect	0	1
	ListBox Smooth Scrolling	Disable ListBox SmoothScrolling Visual Effect	0	1
	Listview Alpha Select	Disable Listview Alpha Select Visual Effect	0	1
	Listview Shadow	Disable Listview Shadow Visual Effect	0	1
	Menu Animation	Disable Menu Animation Visual Effect	0	1
	Save Thumbnail	Disable Save Thumbnail Visual Effect	0	0

	Steps	Description	Expected Result	Actual Result
	Selection Fade	Disable Selection Fade Visual Effect	0	1
	Taskbar Animations	Disable Taskbar Animations Visual Effect	0	1
	Thumbnails Or Icon	Disable ThumbnailsOrIcon Visual Effect	0	1
	Tooltip Animation	Disable Tooltip Animation Visual Effect	0	1
	Transparent Glass	Disable Transparent Glass Visual Effect	0	1
VMware Components				
	VMware Tools	VMware Tools		
	VMware View Agent	VMware View Agent.		Registry key not found.
	VMware View Agent Debug - Disable	VMware	False	False
	VMware View Agent Trace - Disable	VMware	False	False

5.2 End User Persona

End user profile management is achieved using Liquidware Labs Profile Unity. It is recommended to engage Liquidware Labs in order to gather all necessary configurations to optimize the login process and deliver the best experience to the end users.

6. Recommendations

6.1 vSphere Recommendations

- Review above observations and make configuration enhancements based on business need
- Use resource pools for workload grouping
- Enable syslog collecting of ESXi environment (Configured, not enabled)

- Move vSphere Database to a dedicated SQL server (presently co-installed on the vSphere server)
- Set a max memory allocation for SQL server
- Increase size of Microsoft Event Log and collect a regular bundle for future analysis
- Discussed the importance of monitoring and root cause identification
- Leverage out of box monitoring and alerting in vSphere and View for regular review

6.2 Horizon View Recommendations

- Continue using the VMware OS Optimization tool for virtual desktops
- GPOs for PCoIP optimization (build to lossless, max image size, copy/paste and resolution for desktops, etc.)
- Using multiple datastores in more than one array for redundancy of View desktops
- Using connection server tags to provide explicit paths to users desktops
- Deploying cloud pod architecture for Horizon View redundancy and potential disaster recovery
- Providing connection server redundancy (load balancing) for high availability desktops
- Investigate the View Administrators Toolbox (located in labs.vmware.com/flings) for the ability to use more Horizon View metrics
- Discussions around some issues they have been experiencing within their View desktop environment
    - Cursor disappearing in View sessions (registry key, *kb.vmware.com/kb/2081495*)
    - KMS activation for Office (Use Office customization tool and check box activate with KMS and provide KMS server FQDN)
    - Typing lag on office applications in View sessions (Group Policy setting for View Agent)
    - Allowing larger screen resolutions (Group Policy setting for View Agent)
    - Printing issues (garbled text) when printing from a View session (usually caused by firmware/driver mismatch or older version of VMware tools. Will need to investigate as to which component is causing the issue)
    - Unlocking multiple desktops while using Horizon View client (Will need to investigate pass thru options)

6.3 Operational Recommendations

- Use the Liquidware Labs Stratusphere product (already own licensing and Profile Unity) to maintain higher visibility within the Virtual Machines and applications and the resources they consume.
- Use the Nutanix dashboard that was included in the host and storage solution for identifying metrics from physical components.
- Discussed vRealize Operations Manager and its ability to add value for maintaining a proactive environment.
- Develop regular habits to check dashboards and messages generated by infrastructure

6.4 Additional Recommendations

- Recommend advanced training on products for support personnel
- Enlisting a VMware resource while planning and preparing for product upgrades
- Annual Health Checks for the environment

Appendix A: References

Item	URL
Documentation	http://www.vmware.com/support/pubs
VMTN Technology information	http://www.vmware.com/vcommunity/technology
VMTN Knowledge Base	http://kb.vmware.com
Discussion forums	http://www.vmware.com/community
User groups	http://www.vmware.com/vcommunity/usergroups.html
Online support	http://www.vmware.com/support
Telephone support	http://www.vmware.com/support/phone_support.html
Education services	http://mylearn.vmware.com/mgrreg/index.cfm
Certification	http://mylearn.vmware.com/portals/certification/
Technical papers	http://www.vmware.com/vmtn/resources