|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | |  | | --- | | http://www.itone.com.br/front_desktop/foto/servicos-1.png | |  | |
| ISE | IT-ONE SERVIÇOS ESPECIALIZADOS HEALTH CHECK  **by THIAGO NERES** | |  |
| JURONG RECOMENDAÇÕES HEALTH CHECK | | 18 | 08 | 17  v1.0 |
|  | | |
|  | C:\Users\thiago.neres\AppData\Local\Microsoft\Windows\INetCache\Content.Word\EJA.JPG | |

COLETA DE RECOMENDAÇOES DO PROJETO

GERAÇÃO DE LOGS DO AMBIENTE

Os procedimentos de coleta aqui descritos, visam documentar a situação atual do ambiente antes que os procedimentos de adequação sejam executados. As informações obtidas ajudarão na construção do Plano de Arquitetura quando o projeto estiver na fase de PLANEJAMENTO.

vmware vsphere 5.5

RECOMENDAÇÕES HEALTH CHECK VMWARE 5.5

### **Recomendações técnicas**

Recomendações técnicas consolidadas

|  |  |  |
| --- | --- | --- |
| Priority | Component | Recommended Action Item |
| P1 | Compute | Configure firewall rules and ports according to best practices. |
| P1 | Compute | Enable Tech Support Mode timeout feature ESXi Shell timeout feature and configure it per customer security and manageability requirements. |
| P1 | Compute | Use persistent and remote syslog logging to improve manageability. |
| P1 | Datacenter | Set up redundancy for the management port (either using a separate vmnic or a separate uplink) and an alternate isolation response gateway address (if appropriate) for more reliability in HA isolation detection. |
| P1 | Datacenter | Tasks and Events Retention Policy set in the environment. |
| P1 | Network | If jumbo frames are enabled, verify that jumbo frame support is enabled on all intermediate devices and that there is no MTU mismatch. |
| P1 | Network | Verify that there is redundancy in networking paths and components to avoid single points of failure. For example, provide at least two paths to each network. |
| P1 | Storage | NFS and iSCSI storage traffic should be separated physically (for performance) and logically (for security). |
| P1 | Virtual Machines | Use NTP, Windows Time Service, or another timekeeping utility suitable for the operating system. |
| P1 | Virtual Machines | Verify that VMware Tools is installed, running, and up to date for running virtual machines. |
| P2 | Datacenter | Use a consistent naming convention for all virtual datacenter objects. |
| P2 | Datacenter | Use automatic mode for vSphere DRS, if possible, for optimal load balancing. |
| P2 | Datacenter | Use vCenter Server roles, groups, and permissions to provide appropriate access and authorization to the VMware virtual infrastructure. Avoid using Windows built-in groups (Administrators). |
| P2 | Network | Distribute vmnics for a port group across different PCI buses for greater redundancy. |
| P2 | Storage | Use Storage I/O Control (SIOC) to prioritize high importance virtual machine traffic. |
| P2 | Storage | Minimize differences in the number of storage paths. |
| P2 | Storage | Size datastores appropriately. |
| P2 | Storage | Allocate space on shared datastores for templates and media/ISOs separately from datastores for virtual machines. |
| P2 | Virtual Machines | Use the latest version of VMXNET that is supported by the guest operating system. |

### **Health Check Recommendations**

1. **COMPUTE**

|  |  |
| --- | --- |
| Item | Comments |
| Observation 1 | Default firewall settings have been modified from default for 7 ESX host(s). |
| Priority | P1 |
| Infrastructure Qualities |  |
| 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 *VMware Hardening Guide.* <https://communities.vmware.com/docs/DOC-22981>  <http://communities.vmware.com/docs/DOC-19605>  *TCP and UDP Ports required to access vCenter Server, ESX hosts, and other network components* <http://kb.vmware.com/kb/1012382>  TCP and UDP Ports section in *vSphere Security Guide* <http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-security-guide.pdf>  <http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-security-guide.pdf>  <http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-security-guide.pdf>  About the ESXi 5.0 firewall<http://kb.vmware.com/kb/2005284> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 2 | Tech Support Mode (TSM) timeout is not enabled for 7 host(s). |
| Priority | P1 |
| Infrastructure Qualities |  |
| Recommendation | Enable Tech Support Mode timeout feature ESXi Shell timeout feature and configure it per customer security and manageability 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:**  *Security Hardening Guide (ESXi tab)* <https://www.vmware.com/support/support-resources/hardening-guides.html> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 3 | Remote syslog logging is configured but not enabled for 7 host(s). NTP Server is not running in 2 host(s). |
| Priority | P1 |
| Infrastructure Qualities |  |
| 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.  **References:**  *Security Hardening Guide (ESXi tab)* <https://www.vmware.com/support/support-resources/hardening-guides.html>  VM and ESXi tabs in *VMware Hardening Guide.* <https://communities.vmware.com/docs/DOC-22981>  <http://communities.vmware.com/docs/DOC-19605> |

1. **NETWORK**

|  |  |
| --- | --- |
| Item | Comments |
| Observation 1 | Jumbo frames are configured inconsistently between virtual switches and their VNICs on 4 host(s). |
| Priority | P1 |
| Infrastructure Qualities |  |
| Recommendation | If jumbo frames are enabled, verify that jumbo frame support is enabled on all intermediate devices and that there is no MTU mismatch. |
| Justification | If using jumbo frames, make sure that MTU size is set to 9000 both in the guest and the virtual switch configuration. All devices throughout the configuration including the physical NICs at both ends and all intermediate hops, routers, and switches must support jumbo frames and must be configured appropriately. Cisco Discovery Protocol can be used to help determine this information without having to go to the physical hardware.  **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 2 | 7 host(s) do(es) not have optimum NIC teaming. |
| Priority | P1 |
| Infrastructure Qualities |  |
| Recommendation | Verify that there is redundancy in networking paths and components to avoid single points of failure. For example, provide at least two paths to each network. |
| Justification | To avoid service disruption, make sure that the networking configuration is fault resilient to accommodate networking path and component failures.  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.  Upstream physical network components should also have the necessary redundancy to accommodate physical component failures.  **References:**  Security Hardening Guide (vNetwork tab) <https://www.vmware.com/support/support-resources/hardening-guides.html> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 3 | 7 ESX host(s) have one or more port groups with physical NICs that share the same PCI bus. |
| Priority | P2 |
| Infrastructure Qualities |  |
| 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.  **References:**  Security Hardening Guide (vNetwork tab)  <https://www.vmware.com/support/support-resources/hardening-guides.html> |

1. **STORAGE**

|  |  |
| --- | --- |
| Item | Comments |
| Observation 1 | 7 host(s) have standard port groups which use a network that is not dedicated to a single type of storage(NFS or iSCSI) traffic. |
| Priority | P1 |
| Infrastructure Qualities |  |
| Recommendation | NFS and iSCSI storage traffic should be separated physically (for performance) and logically (for security). |
| Justification | Verify that paths are low latency and have adequate bandwidth. Use dedicated pNICs and consider dedicated switches. Consider non-routable IP addresses. Using a dedicated IP storage network removes contention with other network traffic. This decreases latency and improves performance. Security is also enhanced with a dedicated IP storage network. VMware recommends that isolated networks be placed on different subnets to avoid bandwidth issues.  **References:**  Security Hardening Guide (vNetwork tab) <https://www.vmware.com/support/support-resources/hardening-guides.html> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 2 | 21 datastore(s) do(es) not have Storage I/O Control enabled. |
| Priority | P2 |
| Infrastructure Qualities |  |
| 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 <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf> <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf> <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 3 | 1 cluster(s) contain hosts with inconsistent path configurations to one or more datastores. |
| Priority | P2 |
| Infrastructure Qualities |  |
| Recommendation | Minimize differences in the number of storage paths. |
| Justification | Consistent paths to storage improve availability, performance, and manageability. Some hosts might require additional paths (for example, zones for backup devices), but hosts should never have fewer than the recommended number of paths.  For LUNs that will be shared among multiple hosts, verify that LUN IDs are consistent across all hosts. For example, LUN 5 should be mapped to host 1, host 2, and host 3 as LUN 5.  **References:**  Setting LUN Allocations section in vSphere Storage  <http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-storage-guide.pdf><http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-storage-guide.pdf><http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-storage-guide.pdf> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 4 | 5 datastore(s) have limited free space available. |
| Priority | P2 |
| Infrastructure Qualities |  |
| Recommendation | Size datastores appropriately. |
| Justification | Use consistent LUN sizes and create one datastore per LUN. When choosing a LUN size, consider the time it takes to restore a LUN if a disk fails. There are restrictions on the maximum LUN size in vSphere — see Configuration Maximums.  **References:**  Configuration Maximums (VMware vSphere 5.5)<https://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf>  Configuration Maximums (VMware vSphere 5.1)<https://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf>  Configuration Maximums(VMware vSphere 5.0) <https://www.vmware.com/pdf/vsphere5/r50/vsphere-50-configuration-maximums.pdf> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 5 | 2 datastore(s) have both VMs and Templates. |
| Priority | P2 |
| Infrastructure Qualities |  |
| 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. A best practice is to dedicate separate shared datastores/LUNs for virtual machine templates, and to separate ISO/FLP files from the virtual machines themselves.  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. |

1. **DATACENTER**

|  |  |
| --- | --- |
| Item | Comments |
| Observation 1 | Strict Admission Control for 1 VMware HA enabled cluster(s) is not enabled. 5 ESX host(s) do(es) not have VMKernel port groups with a dedicated active NIC. |
| Priority | P1 |
| Infrastructure Qualities |  |
| Recommendation | Set up redundancy for the management port (either using a separate vmnic or a separate uplink) and an alternate isolation response gateway address (if appropriate) for more reliability in HA isolation detection. |
| Justification | Management redundancy can be accomplished by having multiple vmnics attached to the vSwitch, or by having multiple management ports. Depending on how the configuration is set up, you can also specify an additional isolation response address for the secondary management network. This allows HA detecting isolations on two separate networks, thereby making isolation detections more reliable.  Review the advanced settings you can use to optimize the vSphere HA clusters in your environment. Because these attributes affect the functioning of vSphere HA, change them with caution.  **References:**  Best Practices for VMware HA Clusters section in vSphere Availability Guide <http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-availability-guide.pdf>  <http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-availability-guide.pdf>  <http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-availability-guide.pdf> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 2 | 2 retention policies are not enabled or set. |
| Priority | P1 |
| Infrastructure Qualities |  |
| Recommendation | Tasks and Events Retention Policy set in the environment. |
| Justification | Verify that Task and Events Retention levels are set as conservatively as possible while meeting the customer’s data retention requirements. Every time a task or event that is executed through vCenter, it is stored in the database. For example, a task is created when a user powers on or off on a virtual machine, or an event where something occurs such as vCPU usage for a VM changing to red.  Tasks and event data is stored indefinitely in the vCenter database. This can cause substantial growth of the database in large environments.  vCenter Server has a Database Retention Policy setting that allows you to specify after how long vCenter Server tasks and events should be deleted. This correlates to a database rollup job that purges the data from the database after the selected period of time.  In comparison to statistical data, these tables consume a relevantly small amount of database space. However, it is good practice to consider this option for further reduce the consumed space in the database.  VMware recommends that the Task and Events Retention policies be turned on and configured to the appropriate settings per the customer business requirements. This policy controls the length of time that the tasks and events are retained in the database. There is no way to recover from removed data other than restoration from a backup.  **References:**  Configure Database Settings in the vSphere Web Client <http://pubs.vmware.com/vsphere-55/topic/com.vmware.vsphere.vcenterhost.doc/GUID-84DE30DD-E1C4-4E6D-899D-4756FE77CB15.html> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 3 | 7 virtual object(s) do not appear to follow a standard naming convention. |
| Priority | P2 |
| Infrastructure Qualities |  |
| Recommendation | Use a consistent naming convention for all virtual datacenter 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, iSCSI). * Array vendor or type. * Location. * Business unit or function. * Performance characteristics (RAID level). * Availability characteristics (replicated, non-replicated). * Hostname tag for local datastores.   Naming standards also help to streamline the troubleshooting and support process. |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 4 | 2 DRS cluster(s) with homogeneous ESX host configurations is/are not set to Fully Automatic. |
| Priority | P2 |
| Infrastructure Qualities |  |
| Recommendation | Use automatic mode for vSphere DRS, if possible, for optimal load balancing. |
| Justification | vSphere DRS continuously (every five minutes) monitors the distribution and usage of CPU and memory resources for all hosts and virtual machines in a cluster. Based on the specified attributes and current demand, vSphere DRS performs (or recommends) virtual machine migrations accordingly, thereby maintaining proper load balancing.  Use the automatic mode for vSphere DRS to maintain continuous and proper load balancing.  Set the appropriate migration threshold between Conservative to Aggressive (starting with a level 2 or 3), and adjust as necessary.  Set the migration threshold to more aggressive levels if the following conditions are satisfied:   * The hosts in the cluster are relatively homogeneous. * The virtual machine's resource utilization does not vary too much over time and there are few constraints on where a virtual machine can be placed.   Set the migration threshold to more conservative levels if hosts in the cluster are heterogeneous, or if virtual machine resource utilization varies greatly over time and there are constraints on where virtual machines can be placed.  **References:**  DRS Cluster Requirements section in vSphere Resource Management<http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-resource-management-guide.pdf>  <http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-resource-management-guide.pdf><http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-resource-management-guide.pdf>  Calculating the priority level of a VMware DRS migration recommendation<http://kb.vmware.com/kb/1007485> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 5 | 1 default users/group(s) are being used for vCenter user roles/permissions. |
| Priority | P2 |
| Infrastructure Qualities |  |
| Recommendation | Use vCenter Server roles, groups, and permissions to provide appropriate access and authorization to the VMware virtual infrastructure. Avoid using Windows built-in groups (Administrators). |
| Justification | By default, the administrator access is defined as a part of the Single Sign-On (SSO) installation. The configured user or group who has full administrative control of vCenter Server (and the VMware virtual infrastructure). This can allow other system administrators who are not VMware virtual infrastructure administrators access the infrastructure, if a dedicated group or user is not created.  In addition, to improve host security, VMware made several improvements to the ESXi Shell in vSphere 5.1 and later. There is no longer a dependency on a shared root account. Local users assigned administrative privileges automatically get full shell access. With full shell access, local users no longer have to su to root to run privileged commands. Administrative privileges can be removed from the default root account, effectively eliminating a popular target for anyone who might attempt to gain unauthorized access to a vSphere host.  **References:**  vSphere Users and Permissions section in vSphere Security Guide[http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-security-guide.pdf](http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-security-guide.pdf%20)[http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-security-guide.pdf](http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-security-guide.pdf%20)[http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-security-guide.pdf](http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-security-guide.pdf%20)  <http://www.vmware.com/files/pdf/techpaper/Whats-New-VMware-vSphere-51-Platform-Technical-Whitepaper.pdf><http://www.vmware.com/files/pdf/techpaper/Whats-New-VMware-vSphere-50-Platform-Technical-Whitepaper.pdf> |

1. **VIRTUAL MACHINES**

|  |  |
| --- | --- |
| Item | Comments |
| Observation 1 | 2 ESX host(s) do not have NTP Server running. |
| Priority | P1 |
| Infrastructure Qualities |  |
| Recommendation | Use NTP, Windows Time Service, or another timekeeping utility suitable for the operating system. |
| Justification | Time synchronization is important for many reasons, including easier correlation of information for troubleshooting and preventing erratic behavior of time-sensitive applications.  For ESXi hosts:  Configure each ESXi host to synchronize time with an NTP (Network Time Protocol) server.  For virtual machines:  The VMware Tools™ time-synchronization option is a suitable choice. (Versions prior to ESXi 5.0 were not designed for the same level of accuracy and do not adjust the guest time when it is ahead of the host time.) We recommend that within any particular virtual machine you use either the VMware Tools time-synchronization option or another timekeeping utility, but not both.  **References:**  Host Clock Synchronization section in Timekeeping in VMware Virtual Machines<http://www.vmware.com/vmtn/resources/238>  Timekeeping best practices for Linux Guests <http://kb.vmware.com/kb/1006427>  Timekeeping best practices for Windows <http://kb.vmware.com/kb/1318>  "Guest Operating System General Considerations" section in Performance Best Practices for VMware vSphere<http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf> <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf> <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 2 | 1 VM(s) do not have VMware Tools installed. 3 VM(s) have VMware Tools installed that are not up to date. |
| Priority | P1 |
| Infrastructure Qualities |  |
| 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.   1. 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.   VMware Tools optimize the guests to make them run better inside virtual machines by providing the following:   * Optimized virtual NIC and storage drivers. * Efficient memory management using the balloon driver. * Driver to assist with file system quiescing to facilitate backups. * Improved keyboard, video, and mouse operation. * Graceful shutdown of virtual machines. * Perfmon integration of virtual machine performance data (for vSphere).   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.  **References:**  Security Hardening Guide (VM tab)<https://www.vmware.com/support/support-resources/hardening-guides.html> |

|  |  |
| --- | --- |
| Item | Comments |
| Observation 3 | 33 VM(s) are not using VMXNET3 even though their configuration and guest OS support it. |
| Priority | P2 |
| Infrastructure Qualities |  |
| 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 for which it is supported. This requires that the virtual machine use 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). Both VMXNET3 and Enhanced VMXNET support jumbo frames.  If Enhanced VMXNET is not supported in the guest operating system, then use the Flexible device type, which automatically converts each vlance network device to a VMXNET device when VMware Tools is installed.  Refer to the Knowledge Base in the references and the product documentation for supported guest operating systems for the particular adapter.  **References:**  Choosing a network adapter for your virtual machine <http://kb.vmware.com/kb/1001805>  Guest Operating System Networking Considerations section in Performance Best Practices for VMware vSphere <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf> <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf> <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf> |