



IMPLEMENTATION
METHODOLOGY

VMware vSphere™ Health Check Report

for

AEROCIVIL

Prepared by

Blanca Ramirez

V2S COLOMBIA

blanca.ramirez@v2s.us

Version Historial

Fecha	Ver.	Autor	Descripcion	Revisor
15-12-2023	1.0	Blanca Ramirez	Borrador (vCenter Principal Solamente)	

© 2023 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contenido

Version Historial.....	2
Contenido	3
1. Resumen Ejecutivo	4
2. Antecedentes de Health Check.....	4
2.1 Alcance	4
2.2 Supuestos	5
2.3 Limitaciones	5
2.4 Metodologia.....	5
3. Hallazgos y Recomendaciones	7
3.1 Recomendaciones Tecnicas vCenter 172.16.63.37	7
4. Health Check Evaluzion y Recomendaciones	19
4.1 Exitoso	19
4.2 Fallas.....	98
Apéndice A: Participantes en el chequeo.....	127
Apéndice B: Inventario auditado	128
Apéndice C: Buenas prácticas para la evaluación del chequeo médico.....	133
Appendix D: Referencias	140

1. Resumen Ejecutivo

AEROCIVIL contrató los servicios profesionales de V2S COLOMBIA para llevar a cabo una comprobación del estado de vSphere. Este compromiso incluía una evaluación de la implementación actual de vSphere de AEROCIVIL en términos de configuración, operaciones y uso. Una parte clave de este servicio incluyó talleres con el personal de TI de AEROCIVIL para revisar las mejores prácticas en siete capas de la pila tecnológica de VMware. El objetivo de este informe es documentar el descubrimiento, el análisis y las recomendaciones de la comprobación de la salud de vSphere. Health Check.

El entorno vSphere es un componente crítico de las operaciones de TI de AEROCIVIL, tiene complejas interacciones técnicas y operativas con múltiples tecnologías, departamentos y personas. AEROCIVIL ha llegado a un punto en el que le gustaría analizar el entorno existente para conocer el estado de salud, configuración y capacidad de la infraestructura vSphere.

El entorno AEROCIVIL vSphere proporciona servicios a los diferentes departamentos que conforman la entidad. En su configuración actual, esta infraestructura funciona en un estado óptimo. La comprobación de estado se está realizando para analizar el entorno en busca de cualquier desviación de las prácticas recomendadas que pueda afectar al entorno vSphere.

Muchos de los retos descritos a continuación pueden abordarse para lograr un impacto positivo significativo en la infraestructura. Como parte del chequeo, se analizan las recomendaciones técnicas y se ofrecen recomendaciones.

Esto permite aplicar configuraciones coherentes al entorno en sistemas similares y realizar pequeños ajustes para mejorar la disponibilidad, la capacidad de gestión, el rendimiento, la fiabilidad y la seguridad del entorno vSphere..

Algunas de estas recomendaciones pueden aplicarse rápidamente, mientras que otras requerirán planificación adicional y apoyo ejecutivo. Los servicios profesionales de V2S COLOMBIA pueden proporcionar asistencia en cada una de las áreas de recomendación.

2. Antecedentes de Health Check

En esta sección se describen los pormenores del chequeo, incluidos el ámbito de aplicación, los motores de negocio y la metodología empleada.

2.1 Alcance

Este compromiso se aplica al ámbito que se muestra en la siguiente tabla. En la recopilación de datos se incluye el ambiente vSphere Principal de la AEROCIVIL.

Table 1: Alcance Reporte Health Check 172.16.63.37

VMware vCenter 7.0.3 - 172.16.63.37	Name	Count
	Data Center	1
	Cluster	1
	ESX server	2
	Virtual Machine	140
	Datastore	11

2.2 Supuestos

Este documento se basa en una serie de supuestos que se explican en la Tabla 2.

Table 2: Supuestos Health Check

#	Description
A101	La infraestructura virtual actual se basa en la arquitectura y el diseño de hace 1 año o mas.
A102	Se espera un crecimiento escalable del entorno vSphere de la AEROCIVIL.
A103	Los componentes de red y almacenamiento más allá de los conectados directamente a los hosts ESX están fuera del alcance.
A104	Acceso y derechos de consultor suficientes para realizar el chequeo.

2.3 Limitaciones

Además de las hipótesis, también hay una serie de limitaciones que se enumeran en la Tabla 3.

Table 3: Limitaciones Health Check Report

#	Description
C101	Limitado al centro de datos principal de la AEROCIVIL; ubicado en el CNA (Calle 26 # 112-09 primer piso Dirección de Infraestructura y Soporte de TI).
C102	No todas las partes interesadas en la virtualización estaban representadas en este compromiso. (por ejemplo, los usuarios finales y el equipo de alojamiento de Windows).

2.4 Metodología

El servicio vSphere Health Check para AEROCIVIL tiene los siguientes objetivos principales:

- Evaluar y resumir el entorno vSphere en términos de su estado y arquitectura actuales, centrándose en los aspectos técnicos y organizativos.
- Proporcionar recomendaciones claras para mejorar la disponibilidad, el rendimiento, la gestionabilidad, la recuperabilidad y la escalabilidad del entorno.
- Servir de referencia a AEROCIVIL para revisar las mejores prácticas y comunicar los problemas actuales de infraestructura entre las partes interesadas..

Para lograr estos objetivos, V2S COLOMBIA abordó este compromiso de dos maneras. El primer conjunto de actividades es una auditoría técnica de la infraestructura. Esto se realizó utilizando VMware HealthAnalyzer, así como a través de observaciones y medidas tomadas de los componentes de la infraestructura. Las configuraciones capturadas con HealthAnalyzer incluían ajustes detallados y puntuales de los componentes de vSphere.

La segunda serie de actividades consistió en aclarar con los miembros del equipo administrador de infraestructura de la AEROCIVIL el cumplimiento de buenas practicas a nivel de configuración y seguridad sobre el ambiente vSphere. Esta reunion se centro en cuestiones, preocupaciones y configuraciones de la infraestructura virtual.

Tras estas actividades de descubrimiento, se procedió al análisis detallado de los datos. Los datos incluían parámetros de configuración sin procesar, métricas de rendimiento y notas de observación. El análisis se basó en la comparación de los datos de AEROCIVIL con las mejores prácticas del sector para la infraestructura vSphere en las áreas técnicas de:

- **ESXi Host** – Configuración del hipervisor ESX(i) y del hardware host
- **vCenter Server** – vCenter, supervisión, copias de seguridad y otras tecnologías de apoyo a las operaciones
- **Licenciamiento** – Configuración de licencias y otros detalles
- **Redes** – Configuración de la infraestructura de red virtual y física
- **Seguridad** – Configuración de seguridad en el entorno
- **Almacenamiento** – Arquitectura y configuración del almacenamiento compartido
- **Maquinas Virtuales** – Cargas de trabajo virtuales, requisitos de las aplicaciones
- **vSAN** – Ajustes relacionados con vSAN cuando se utiliza como plataforma de almacenamiento. Para el caso de la AEROCIVIL esta área no aplica teniendo en cuenta que no se cuenta actualmente con este tipo de solución sobre la infraestructura vSphere.

Basándose en el análisis, a continuación se hace una evaluación de la infraestructura. Las conclusiones y recomendaciones resumidas se presentan en la siguiente sección de este documento. Los resultados detallados de la evaluación se presentan en un formato priorizado. La Tabla 4 resume las distintas categorías prioritarias de la evaluación.

Table 3: Report Card Priority Categories

Grade	Definition
P1	Motivos específicos de preocupación que requieren atención inmediata, con las acciones correspondientes para abordar cada motivo de preocupación.
P2	Elementos potencialmente preocupantes. Los puntos no son críticos o requieren más investigación.
P3	Se han observado desviaciones de las mejores prácticas, pero abordarlas puede no ser una prioridad inmediata.
OK	Los puntos se ajustan a las directrices de buenas prácticas. No se ha observado ningún elemento preocupante.
Not Applicable	Elementos no aplicables
No Data	Los artículos no tienen asignada una calificación
None	No se han podido recopilar datos para evaluar estos puntos.

Para cada área de evaluación, se midieron puntos de control específicos de la infraestructura y se compararon con las directrices de mejores prácticas de VMware.

3. Hallazgos y Recomendaciones

Esta sección describe las recomendaciones y conclusiones para el entorno. Las mejores prácticas descritas se han extraído de muchos años de experiencia de los consultores de V2S.

Aunque no todas las mejores prácticas pueden aplicarse a todos los entornos, el equipo administrador de vSphere y otros están limitados en su visibilidad y control sobre los diversos componentes que soportan la infraestructura. La colaboración técnica es esencial, entre equipos para tener éxito. Por ejemplo, el equipo de servidores puede depender del equipo de almacenamiento y redes para coordinar configuraciones y solucionar problemas.

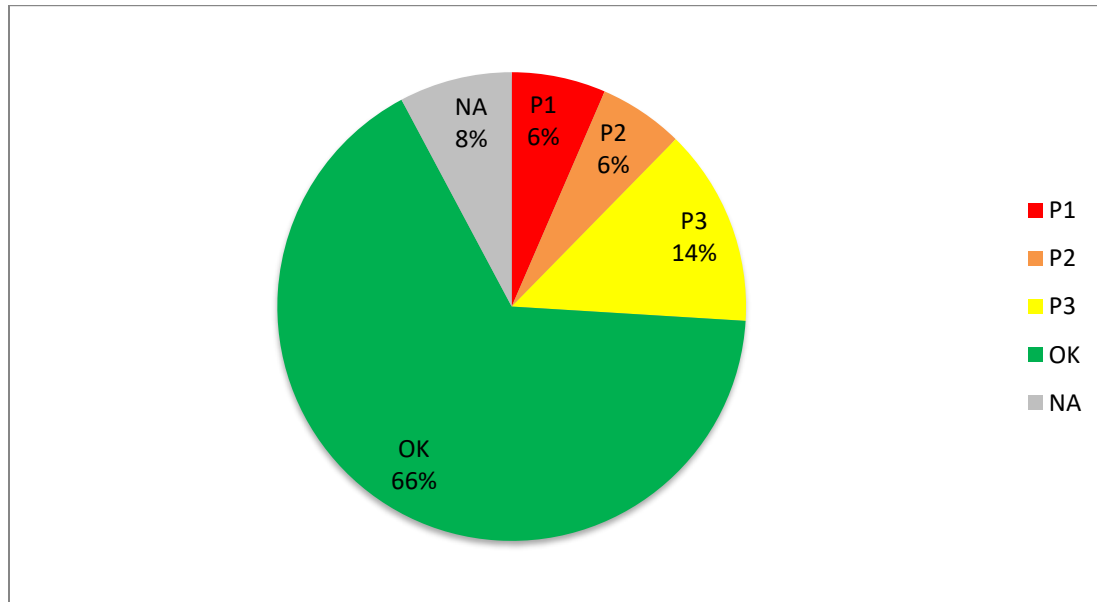
Cualquier número de cuestiones arquitectónicas puede afectar al entorno, incluidas las decisiones sobre la capacidad del servidor (cantidad de RAM, núcleos de CPU, etc.), el diseño de la red o la storage y los requisitos normativos de la empresa.

La siguiente sección describe las recomendaciones de alto nivel identificadas en esta evaluación.

3.1 Recomendaciones Técnicas vCenter 172.16.63.37

El desglose destaca la evaluación de la Infraestructura vSphere del Centros de Datos de la AEROCIVIL. Los resúmenes de la evaluación se basan en las mejores prácticas de VMware HealthAnalyzer. La siguiente figura muestra el resumen para todas las recomendaciones.

Figure 1. Recomendaciones técnicas desglosadas por prioridad



Como ilustra el gráfico, AEROCIVIL obtuvo una puntuación aproximada del 66% en las áreas evaluadas según las mejores prácticas de VMware. Sin embargo, el gráfico muestra que hay margen de mejora..

Nota Las revisiones típicas de Health Checks oscilan entre 10% y 50% en las áreas OK.

La siguiente tabla enumera las recomendaciones de alto nivel

vCenter	Prioridad	Componente	Identificación de mejores prácticas	Elementos de acción recomendado
---------	-----------	------------	-------------------------------------	---------------------------------

172.16.63.37	P1	ESXi Host	ESXI-009	Use persistent and remote syslog logging to improve manageability.
172.16.63.37	P1	ESXi Host	ESXI-008	Place host devices in a consistent order and location.
172.16.63.37	P1	Network	NE-002	Configure networking consistently across all hosts in a cluster.
172.16.63.37	P1	Network	NE-001	Deploy networking in compliance with all configuration maximums as documented in the most current vSphere Configuration Maximums document.
172.16.63.37	P1	Network	NE-007	Configure networks so that there is separation of traffic (physical or logical using VLANs).
172.16.63.37	P1	Network	NE-024	Use Distributed Virtual Port Groups to apply policies to traffic flow types and to provide Rx (receive) bandwidth controls through the use of Traffic Shaping.
172.16.63.37	P1	Storage	ST-013	Configure NFS and iSCSI storage traffic for performance and security.
172.16.63.37	P1	Virtual Machines	VM-019	Limit use of snapshots, and when using snapshots limit them to short-term use.
172.16.63.37	P1	Virtual Machines	VM-016	Verify that VMware Tools is installed, running, and up to date for running virtual machines.
172.16.63.37	P1	vCenter Server	VC-026	vSphere HA feature, VM Component Protection (VMCP) should be enabled and configured appropriately to provide enhanced protection from failures.
172.16.63.37	P2	ESXi Host	ESXI-005	Avoid unnecessary changes to advanced parameter settings.
172.16.63.37	P2	Network	NE-006	Distribute vmnics for a port group across different PCI buses for greater redundancy.
172.16.63.37	P2	Security	SEC-021	Limit sharing console connections if there are security concerns.
172.16.63.37	P2	Storage	ST-011	Allocate space on shared datastores for templates and media/ISOs separately from datastores for virtual machines.

172.16.63.37	P2	Storage	ST-020	Use Storage I/O Control (SIOC) to prioritize high importance traffic, such as virtual machine traffic.
172.16.63.37	P2	Virtual Machines	VM-018	Consider the implications and use the latest virtual hardware version to take advantage of additional capabilities, when appropriate.
172.16.63.37	P2	Virtual Machines	VM-017	Allocate only as much virtual hardware as required for each virtual machine. Disable any unused or unnecessary or unauthorized virtual hardware devices.
172.16.63.37	P2	Virtual Machines	VM-003	Verify that virtual machines meet the requirements for vSphere vMotion.
172.16.63.37	P2	Virtual Machines	VM-005	Use the latest version of VMXNET that is supported by the guest operating system.
172.16.63.37	P3	ESXi Host	ESXI-021	Check the active Swap in rate of virtual machines to verify that it is not greater than 0 at any point in the measurement period.
172.16.63.37	P3	ESXi Host	ESXI-010	Disconnect or disable unused or unnecessary physical hardware devices (COM and LPT ports, USB and storage controllers, CD/DVD/floppy drives, and NICs).
172.16.63.37	P3	ESXi Host	ESXI-002	Verify that all hardware in the system is on the VMware Compatibility Guide for ESXi.
172.16.63.37	P3	ESXi Host	ESXI-022	Use Host Profiles to ensure a consistent configuration across ESXi hosts.
172.16.63.37	P3	Network	NE-017	Configure NICs, physical switch speed, and duplex settings consistently.
172.16.63.37	P3	Network	NE-005	If the physical switches that support PortFast (or equivalent), enable it on the physical switches that connect to the host.
172.16.63.37	P3	Security	SEC-014	Use vCenter Server roles, groups, and permissions to provide appropriate access and authorization to the virtual infrastructure. Avoid using AD built-in groups such as the Domain Admins group.
172.16.63.37	P3	Security	SEC-023	VMware Certificate Authority should be configured as a subordinate CA in the environment for additional security.

172.16.63.37	P3	Security	SEC-015	Use Active Directory for local user authentication to ESXi Hosts.
172.16.63.37	P3	Storage	ST-010	Verify that Physical Device Read/Write Latency average is less than approximately 10 ms and peak is less than approximately 20 ms for all virtual disks.
172.16.63.37	P3	Storage	ST-019	Consider scheduling vSphere Storage vMotion operations during times of low storage activity, when available storage bandwidth is highest and when the workload in the virtual machine being moved is least active.
172.16.63.37	P3	Storage	ST-022	Optimize storage utilization through the datastore cluster and VMware vSphere Storage DRS features.
172.16.63.37	P3	Virtual Machines	VM-002	Use the correct virtual SCSI hardware for the operating system.
172.16.63.37	P3	Virtual Machines	VM-006	Select the correct guest operating system type in the virtual machine configuration to match the guest operating system.
172.16.63.37	P3	Virtual Machines	VM-024	Validate the schedule for recurring activities such as virus scans and backups is set appropriately to business policy.
172.16.63.37	P3	Virtual Machines	VM-014	Use reservations and limits selectively on virtual machines.
172.16.63.37	P3	Virtual Machines	VM-007	Disable screen savers and window animations.
172.16.63.37	P3	Virtual Machines	VM-009	Use as few vCPUs as possible to avoid over allocation of resources.
172.16.63.37	P3	Virtual Machines	VM-012	Allocate optimal memory to virtual machines, enough to minimize guest OS swapping, but not so much that unused memory is wasted.
172.16.63.37	P3	Virtual Machines	VM-011	Check vCPU for saturation or sustained high utilization.
172.16.63.37	P3	vCenter Server	VC-021	Configure HA Isolation addresses as appropriate for the configuration.
172.16.63.37	OK	ESXi Host	ESXI-013	Check virtual machines to verify that CPU ready is less than 2000 ms.

172.16.63.37	OK	ESXi Host	ESXI-018	Confirm that non-uniform memory access (NUMA) is enabled for NUMA-capable systems.
172.16.63.37	OK	ESXi Host	ESXI-023	Check that the appropriate Power Management Settings are configured for the ESXi Host which meet the power consumption versus performance characteristics desired.
172.16.63.37	OK	ESXi Host	ESXI-006	Maintain a similar version of ESXi within a cluster.
172.16.63.37	OK	ESXi Host	ESXI-020	Review ESXi hosts for driver and firmware consistency between hosts in a cluster.
172.16.63.37	OK	ESXi Host	ESXI-017	Enable Turbo Mode in the BIOS if your processors support it.
172.16.63.37	OK	ESXi Host	ESXI-014	Confirm that hardware assisted virtualization features are enabled if the CPUs support them.
172.16.63.37	OK	ESXi Host	ESXI-015	Confirm that you are running the latest version of the BIOS available for your ESXi servers.
172.16.63.37	OK	ESXi Host	ESXI-016	Verify that the BIOS is set to enable all CPU sockets, and enable all cores in each socket.
172.16.63.37	OK	ESXi Host	ESXI-004	Check CPU compatibility for VMware vSphere vMotion and VMware vSphere Fault Tolerance.
172.16.63.37	OK	ESXi Host	ESXI-011	Manage CPU oversubscription. Verify that the total CPU resources needed by virtual machines do not exceed the CPU capacity of the host.
172.16.63.37	OK	ESXi Host	ESXI-019	Consider enabling hyperthreading if applicable and if the CPU and BIOS support it.
172.16.63.37	OK	ESXi Host	ESXI-012	Monitor the ESXi hosts to verify that the CPU is not saturated or running with a sustained high CPU load.
172.16.63.37	OK	ESXi Host	ESXI-007	Avoid using third-party agents on the ESXi host.
172.16.63.37	OK	ESXi Host	ESXI-001	Deploy VMware ESXi in compliance with all configuration maximums as documented in

				the most current VMware vSphere Configuration Maximums document.
172.16.63.37	OK	ESXi Host	ESXI-003	Verify that hardware meets the optimal configuration supported by ESXi.
172.16.63.37	OK	Licensing	LIC-003	Evaluation licenses should not be used in the environment.
172.16.63.37	OK	Licensing	LIC-001	Verify that adequate licenses are available for vCenter Server instances.
172.16.63.37	OK	Licensing	LIC-002	Verify that adequate CPU licenses are available for ESXi hosts.
172.16.63.37	OK	Network	NE-014	Minimize differences in the number of active NICs across hosts within a cluster.
172.16.63.37	OK	Network	NE-008	If beacon probing is used verify that there are at least three NICs.
172.16.63.37	OK	Network	NE-009	Use at least one 1 GbE adapter for workloads that have a small number of memory operations. Use at least one 10 GbE adapter if you migrate workloads that have many memory operations.
172.16.63.37	OK	Network	NE-010	Use static IP addresses for the management ESXi host management interface.
172.16.63.37	OK	Network	NE-003	Verify that there is redundancy in networking paths and components to avoid single points of failure.
172.16.63.37	OK	Network	NE-019	Adjust load balancing settings from the default virtual port ID only if necessary.
172.16.63.37	OK	Network	NE-018	Avoid mixing NICs with different speeds and duplex settings on the same uplink for a port group/dvport group.
172.16.63.37	OK	Network	NE-023	If Fault Tolerance is used, set Network I/O Control Fault Tolerance resource pool shares to High.
172.16.63.37	OK	Network	NE-020	Verify that the network topology does not contain link oversubscription resulting in dropped packets.
172.16.63.37	OK	Network	NE-022	Use shares instead of limits when using NIOC for bandwidth allocation. Do not

				impose limits unless addressing physical network capacity requirements.
172.16.63.37	OK	Network	NE-013	Limit the number of installed NIC ports to recommended maximums.
172.16.63.37	OK	Network	NE-021	Use Network I/O Control (NetIOC) to prioritize traffic.
172.16.63.37	OK	Network	NE-004	Set up network redundancy for VMKernel network ports where required.
172.16.63.37	OK	Network	NE-011	Make sure that vSphere FT logging traffic is on at least a segregated 10-Gbps network.
172.16.63.37	OK	Network	NE-015	Check for dropped packets on vmnic objects.
172.16.63.37	OK	Network	NE-026	Verify latency between vCenter Server and other network components.
172.16.63.37	OK	Network	NE-012	Single port 10-GbE network adapters should use PCIe x8 (or higher) or PCI-X 266. Dual port 10-GbE should use PCIe x16 or higher.
172.16.63.37	OK	Security	SEC-005	Set the vCenter Single Sign-On default domain to the identity source which is most frequently used.
172.16.63.37	OK	Security	SEC-011	Configure VMware vSphere ESXi Shell and SSH access per manageability requirements.
172.16.63.37	OK	Security	SEC-012	Enable the ESXi Shell timeout feature and configure it per customer security requirements.
172.16.63.37	OK	Security	SEC-020	Verify that VMware isolation settings have not been disabled.
172.16.63.37	OK	Security	SEC-009	Limit remote access to all hosts by administrative users such as root.
172.16.63.37	OK	Security	SEC-008	Set the base domain name for users and groups accordingly in Single Sign-On when using LDAP or OpenLDAP identity sources.
172.16.63.37	OK	Security	SEC-002	Confirm that time is synchronized on the SSO Server and on any server that connects to the SSO server.

172.16.63.37	OK	Security	SEC-006	Set the Single Sign-On password and lockout policies per customer security requirements.
172.16.63.37	OK	Security	SEC-019	Validate that copy/paste between the guest operating system and the remote console is disabled.
172.16.63.37	OK	Security	SEC-003	Record the Single Sign-On administrator password in a safe place.
172.16.63.37	OK	Security	SEC-001	Confirm integrated Windows authentication is configured when using Active Directory identity sources.
172.16.63.37	OK	Security	SEC-018	Configure Management network Traffic on an isolated network.
172.16.63.37	OK	Security	SEC-016	Change port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes to Reject unless required.
172.16.63.37	OK	Security	SEC-004	Avoid using local operating system users with vCenter Single Sign-On.
172.16.63.37	OK	Security	SEC-013	Keep current with the latest VMware product versions and patches.
172.16.63.37	OK	Security	SEC-007	Add only the necessary identity sources to the vCenter Single Sign-On configuration.
172.16.63.37	OK	Security	SEC-024	Configure Encrypted vSphere vMotion if the organization policy requires it.
172.16.63.37	OK	Security	SEC-010	Configure firewall rules and ports according to best practices.
172.16.63.37	OK	Storage	ST-018	Prior to performing a VMware vSphere Storage vMotion operation, verify that there is sufficient bandwidth between the ESXi host running the virtual machine and both source and destination storage.
172.16.63.37	OK	Storage	ST-025	Validate and optimize Non-Volatile Memory Express (NVMe) device performance.
172.16.63.37	OK	Storage	ST-007	Manage the differences in the number of storage paths between hosts including maximum paths per host.
172.16.63.37	OK	Storage	ST-014	Align VMFS partitions.

172.16.63.37	OK	Storage	ST-023	When booting from SAN, verify that the datastore is masked and zoned to that particular ESXi host and not shared with other hosts.
172.16.63.37	OK	Storage	ST-006	Use the appropriate policy based on the array being used (MRU, Fixed, Round Robin, and so on).
172.16.63.37	OK	Storage	ST-005	Minimize differences in datastores visible across hosts within the same cluster or vSphere vMotion scope.
172.16.63.37	OK	Storage	ST-015	Verify the queue depth of the HBA and the max outstanding disk requests per virtual machine parameter according to storage vendor best practices.
172.16.63.37	OK	Storage	ST-021	To maximize the fairness benefit from SIOC, avoid introducing non-SIOC-aware load on the storage.
172.16.63.37	OK	Storage	ST-008	Verify that there is redundancy in storage paths and components to avoid single points of failure.
172.16.63.37	OK	Storage	ST-004	Zone Fibre Channel LUNs properly to the appropriate devices for vSphere vMotion compatibility, security, and shared services.
172.16.63.37	OK	Storage	ST-001	Consult with the storage vendor for recommendations for use with the storage device in the environment.
172.16.63.37	OK	Storage	ST-027	Check for consistent VAAI settings on ESXi Hosts in a cluster.
172.16.63.37	OK	Storage	ST-016	Spread I/O loads over the available paths to the storage (across multiple HBAs and storage processors).
172.16.63.37	OK	Storage	ST-026	Check ESXi Hosts for storage plugin version and consistency.
172.16.63.37	OK	Storage	ST-024	Keep the IP storage network physically separate from other traffic.
172.16.63.37	OK	Storage	ST-012	Size datastores appropriately for the environment.
172.16.63.37	OK	Storage	ST-002	Deploy storage in compliance with all configuration maximums as documented in

				the most current vSphere Configuration Maximums document.
172.16.63.37	OK	Storage	ST-003	Use shared storage for virtual machines instead of local storage.
172.16.63.37	OK	Storage	ST-009	Check that storage LUNs are not overloaded by verifying that the Command Aborts for all datastores is 0.
172.16.63.37	OK	Storage	ST-017	Choose placement of data disks and swap files on LUNs appropriately for virtual machines.
172.16.63.37	OK	Virtual Machines	VM-021	Consider setting the memory reservation value for performance-sensitive Java-based virtual machines (JVMs) to the operating system required memory plus the total JVM heap size.
172.16.63.37	OK	Virtual Machines	VM-013	Configure the guest operating system with sufficient swap space.
172.16.63.37	OK	Virtual Machines	VM-001	Use NTP, Windows Time Service, or another timekeeping utility for all ESXi Hosts and virtual machines.
172.16.63.37	OK	Virtual Machines	VM-020	Consider using a 64-bit guest operating system to improve performance, if applicable.
172.16.63.37	OK	Virtual Machines	VM-008	Verify that the file system partitions within the guest operating system are aligned.
172.16.63.37	OK	Virtual Machines	VM-022	Validate that there are no orphaned or invalid virtual machines in the inventory.
172.16.63.37	OK	Virtual Machines	VM-004	Do not specify CPU affinity rules unless needed.
172.16.63.37	OK	Virtual Machines	VM-010	Use the default monitor mode chosen by the Virtual Machine Monitor unless it is necessary to change it.
172.16.63.37	OK	vCenter Server	VC-018	Configure the vCenter Server statistics to a level appropriate for use. VMware recommends level 1 or 2.
172.16.63.37	OK	vCenter Server	VC-015	Verify that the hosts on which the primary and secondary FT-enabled virtual machines run are relatively closely matched (CPU make, model, frequency, and version/build/patches).

172.16.63.37	OK	vCenter Server	VC-025	vSphere HA should be enabled on all clusters.
172.16.63.37	OK	vCenter Server	VC-003	Use a consistent naming convention for all virtual data center objects.
172.16.63.37	OK	vCenter Server	VC-004	Maintain compatible and homogeneous (CPU, memory, and storage when using vSAN) hosts within a cluster to support the required functionality for vSphere vMotion, vSphere DRS, VMware vSphere Distributed Power Management, vSphere HA, and vSphere FT.
172.16.63.37	OK	vCenter Server	VC-010	Verify that DNS is configured for forward, reverse, short, and long lookups.
172.16.63.37	OK	vCenter Server	VC-013	Distribute vSphere FT VMs to multiple hosts, if the feature is in use.
172.16.63.37	OK	vCenter Server	VC-023	Validate storage requirements are met for the vCenter Server Appliance Database.
172.16.63.37	OK	vCenter Server	VC-005	Verify that the number of hosts in a cluster is within limits for the required functionality (HA, vSphere DRS, and vSphere DPM).
172.16.63.37	OK	vCenter Server	VC-017	Avoid making resource pools and virtual machines siblings in a hierarchy to avoid unexpected performance.
172.16.63.37	OK	vCenter Server	VC-009	Verify that hardware meets the optimal configuration required by vCenter Server and add-ons.
172.16.63.37	OK	vCenter Server	VC-020	Tasks and Events Retention Policy set in the environment.
172.16.63.37	OK	vCenter Server	VC-008	Use reservations and limits selectively on clusters and resource pools that require them. Do not set reservations too high or limits too low.
172.16.63.37	OK	vCenter Server	VC-024	Follow vPostgress best practices when maintaining the vCenter Server Database.
172.16.63.37	OK	vCenter Server	VC-022	Validate that the supported scale for vCenter Server configuration is not exceeded.
172.16.63.37	OK	vCenter Server	VC-001	Deploy vCenter Server in compliance with all configuration maximums as documented

				in the most current vSphere Configuration Maximums document.
172.16.63.37	OK	vCenter Server	VC-011	Use automatic mode for vSphere DRS, if possible, for optimal load balancing.
172.16.63.37	OK	vCenter Server	VC-007	Size VMware HA admission control policy considering the allowed host failures and available resources.
172.16.63.37	OK	vCenter Server	VC-002	Deploy vCenter Server appliance using an embedded platform services controller.
172.16.63.37	NA	Licensing	LIC-004	Validate that proper licenses are installed for VMware vSAN clusters (if applicable).
172.16.63.37	NA	Network	NE-016	If jumbo frames are enabled, verify that jumbo frame support is enabled end-to-end on all intermediate devices so that there is no MTU mismatch.
172.16.63.37	NA	Network	NE-025	Configure network appropriately when VMware vSphere Auto Deploy is used.
172.16.63.37	NA	Security	SEC-022	For additional security for NFS v4.1 shares, configure Kerberos authentication.
172.16.63.37	NA	Security	SEC-017	Enable bidirectional CHAP authentication for iSCSI traffic so that CHAP authentication secrets are unique.
172.16.63.37	NA	Virtual Machines	VM-015	Use paravirtualized SCSI (PVSCSI) with a supported guest OS where additional performance is needed.
172.16.63.37	NA	Virtual Machines	VM-023	If virtual machine encryption is used, validate that the ESXi host processors support AES-NI, for improved performance.
172.16.63.37	NA	vCenter Server	VC-006	Verify that vSphere HA settings allow sufficient capacity for vSphere DPM to power down hosts.
172.16.63.37	NA	vCenter Server	VC-019	vSphere Auto Deploy HA configuration practices.
172.16.63.37	NA	vCenter Server	VC-016	Verify that power management settings (BIOS, ESX) that cause CPU scaling are consistent on hosts running primary and secondary FT-enabled virtual machines.

172.16.63.37	NA	vCenter Server	VC-012	Consider enabling vSphere DPM for clusters in which virtual machine demand varies greatly over time.
172.16.63.37	NA	vCenter Server	VC-014	Verify that the number of vSphere FT-enabled virtual machines does not saturate the vSphere FT logging network.

4. Health Check Evaluacion y Recomendaciones

4.1 Exitoso

4.1.1 172.16.63.37

4.1.1.1. ESXi Host

Item	Comments
Best Practice ID	ESXI-001
Recommendation	Deploy VMware ESXi in compliance with all configuration maximums as documented in the most current VMware vSphere Configuration Maximums document.
Observation	All VMware ESXi Hosts are compliant with the vSphere version Maximums
Priority	OK
Infrastructure Qualities	ESXi Hosts, Configuration Maximums, Scalability
Justification	<p>VMware software is designed to function within specified operating parameters. If the software is implemented out of compliance with recommended specifications, unpredictable results can occur.</p> <p>References:</p> <p><i>Configuration Maximums vSphere 7.0</i> https://configmax.vmware.com/quest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0</p> <p>Procedure:</p> <p>Review the configuration maximums guide as well as the health check analyzer output for any configuration maximums that may be out of accepted limits.</p>
Item	Comments
Best Practice ID	ESXI-003

Recommendation	Verify that hardware meets the optimal configuration supported by ESXi.
Observation	The ESXi that make up the cluster comply with the optimal hardware configurations.
Priority	OK
Infrastructure Qualities	ESXi Hosts, Availability, Recoverability, Manageability, Scalability, Performance
Justification	<p>Hosts running VMware ESXi® require specific hardware and system resources. Check the product installation guide to verify that the CPU, memory, network adapters, storage adapters, RAID controllers, and disk drives meet the requirements supported by ESXi for proper production use.</p> <p>References:</p> <p>System Requirements section in the <i>vSphere Installation and Setup guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-E170469F-9C33-4950-8672-9825501557AE.html</p> <p>Procedure:</p> <p>Review the system requirements for ESXi to validate that it meets the requirements listed for vSphere 7.0.</p>

Item	Comments
Best Practice ID	ESXI-004
Recommendation	Check CPU compatibility for VMware vSphere vMotion and VMware vSphere Fault Tolerance.
Observation	Processor family is compatible with VMware vSphere vMotion and VMware vSphere Fault Tolerance.
Priority	OK
Infrastructure Qualities	ESXi Hosts, Availability, Recoverability
Justification	<p>VMware vSphere® vMotion® and VMware vSphere Fault Tolerance have specific CPU requirements. Reviewing the compatibility during planning helps to achieve the best availability through host clusters and primary/failover host pairings.</p> <p>Use the CPUID tool provided by VMware to check for vMotion compatibility and Enhanced vMotion Compatibility (EVC).</p> <p>Note: For vSphere 6.5 and beyond, vSphere FT has the same requirements as vSphere vMotion due to the changes made to support vSphere FT SMP CPU virtual machines.</p>

References:

Enhanced vMotion Compatibility (EVC) processor support (1003212)
<http://kb.vmware.com/kb/1003212/>

VMware Compatibility Guide (Select the Feature in the feature matrix)
<https://www.vmware.com/resources/compatibility/search.php?deviceCategory=cpu>

Procedure:

Validate that the CPUs are supported for the features required for the environment from the VMware Compatibility list.

Item	Comments
Best Practice ID	ESXI-006
Recommendation	Maintain a similar version of ESXi within a cluster.
Observation	VMware ESXi members of vSphere clusters are vSphere version compliant on VMware ESXi 7.0
Priority	OK
Infrastructure Qualities	ESXi Hosts, Availability, Manageability, Performance
Justification	Having consistent and uniform versions or version families of ESXi within a cluster allows for easier management and helps to make troubleshooting easier by minimizing the number of variables.

Maintaining a compatible version family of ESXi servers allows the use of features like vSphere vMotion, VMware vSphere Distributed Resource Scheduler, and vSphere FT.

Note: It is acceptable to have non uniform versions temporarily when in the middle of an upgrade cycle for a cluster of hosts.

References:

Performance Best Practices for vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Upgrade or create separate clusters for non uniform host versions.

Item	Comments
Best Practice ID	ESXI-007
Recommendation	Avoid using third-party agents on the ESXi host.

Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Manageability
Justification	<p>Using agents on the ESXi host might impact availability, performance, and security of the ESXi host. Any agent used consumes additional resources and as a result can cause unexpected failures.</p> <p>ESXi hosts do not support conventional agents, only CIM based plug-ins. Check with your software vendor for an appropriate version of the software that can be deployed and use the VMware vSphere API for management access into the system.</p> <p>If required, only install agents that are listed in the <i>CIM Providers VMware Compatibility Guide</i>.</p> <p>Common agents include hardware vendor (HP, IBM, DELL, and so on) CIM agents that enable monitoring of specific hardware components on the system. If a CIM agent becomes unstable, try disabling it as a part of troubleshooting issues.</p> <p>References:</p> <p><i>CIM Providers VMware Compatibility Guide</i> https://www.vmware.com/resources/compatibility/search.php?deviceCategory=cim</p> <p>How to disable the CIM agent on the ESX/ESXi host (1025757) https://kb.vmware.com/kb/1025757</p> <p><i>VMware Security Hardening Guides</i> http://www.vmware.com/security/hardening-guides.html</p> <p>Procedure:</p> <p>Review the configuration for any third party CIM agents which are installed, and if they are not needed remove them.</p>
Item	Comments
Best Practice ID	ESXI-011
Recommendation	Manage CPU oversubscription. Verify that the total CPU resources needed by virtual machines do not exceed the CPU capacity of the host.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Performance
Justification	When configuring virtual machines, the total CPU resources needed by the virtual machines running on the ESXi host should not exceed the

capacity of the host. If the host CPU is overloaded, the performance of the individual virtual machines can degrade.

For vSphere DRS clusters, take into account the cluster level resources and oversubscription. For VMware vSphere High Availability clusters, the host failure configuration must be taken into account.

References:

Performance Best Practices for VMware vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Review the amount of CPU being used, as well as the configured CPU capacity. If there is overcommitment, caution should be taken to ensure that there will not be performance degradation in the case that all VMs become active.

Item	Comments
Best Practice ID	ESXI-012
Recommendation	Monitor the ESXi hosts to verify that the CPU is not saturated or running with a sustained high CPU load.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Manageability, Performance
Justification	<p>Monitor CPU usage of the ESXi host.</p> <p>If the load average is greater than or equal to the number of processors, the CPU is overloaded. Monitor the CPU usage percentage. If the CPU average for the ESXi host is above 75%, or if there are peaks in the graph above 90%, it is possible that there is host CPU saturation. High CPU usage does not necessarily indicate a performance problem.</p> <p>References:</p> <p><i>Performance Monitoring Utilities resxtop and esxtop</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-A31249BF-B5DC-455B-AFC7-7D0BBD6E37B6.html</p> <p>Procedure:</p> <p>Review the performance graphs, and esxtop information to validate the load on the ESXi hosts and address as appropriate.</p>
Item	Comments
Best Practice ID	ESXI-013

Recommendation	Check virtual machines to verify that CPU ready is less than 2000 ms.
Observation	
Priority	OK
Infrastructure Qualities	Performance, Virtual Machine

Justification If CPU ready is greater than 2000 ms for any vCPU object, it could be an indication of host CPU saturation which might require one or more of the following approaches to resolve the issue:

- Reduce the number of virtual machines running on the host.
- Increase the available CPU resources by adding the host to a vSphere DRS cluster.
- Increase the efficiency with which virtual machines use CPU resources.
- Use resource controls to direct available resources to critical virtual machines

References:

vSphere Monitoring

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-5F8147A1-6416-4D29-BA3D-E4CED3966016.html>

Procedure:

To search for potential problems, use the vSphere Client and select the host, then the **Virtual Machines** tab. Sort by the **Host CPU MHz** column to determine the virtual machine with the highest CPU usage. Then look at the **Ready** metric from the CPU category of the **Advanced** performance charts.

The documentation link in the references, has several solutions to common issues which can cause high CPU Usage.

Item	Comments
Best Practice ID	ESXI-014
Recommendation	Confirm that hardware assisted virtualization features are enabled if the CPUs support them.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Performance

Justification

Many recent processors from Intel and AMD include hardware features to assist ESXi with virtualization and other features. For the best performance, confirm that the ESXi hosts use the latest processors that support hardware assisted virtualization features such as:

- Hardware-Assisted CPU Virtualization (Intel VT-x and AMD-V)
- Hardware-Assisted MMU Virtualization (Intel EPT and AMD RVI)
- Hardware-Assisted I/O MMU Virtualization (Intel VT-d and AMD-Vi)
- Intel AES-NI Support if using virtual machine encryption

References:

Performance Best Practices for VMware vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Navigate to a host hardware interface (a reboot may be required) to validate the features are enabled.

Item	Comments
Best Practice ID	ESXI-015
Recommendation	Confirm that you are running the latest version of the BIOS available for your ESXi servers.
Observation	The BIOS version is compatible with ESXi Hypervisor version 7.0.
Priority	OK
Infrastructure Qualities	ESXi Hosts, HCL, Manageability, Performance

Justification

ESX Host	Data Center	Cluster	Hypervisor	Hypervisor Version	Server Vendor	Server Model	BIOS Version	B
esxi02.aerocivil.gov.co	Aerocivil	Aerocivil	VMware ESXi	7.0.3	HP	ProLiant DL580 Gen9	U17	TI
esxi01.aerocivil.gov.co	Aerocivil	Aerocivil	VMware ESXi	7.0.3	HP	ProLiant DL580 Gen9	U17	TI

Keep current with the latest BIOS updates available for your server to take advantage of bug fixes and enhancements made in recent releases.

Document your BIOS settings and configuration prior to upgrading the BIOS. After updating the BIOS, you should confirm that BIOS settings are still correct.

References:

Hardware BIOS Settings section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Varies by hardware vendor, follow their procedures to check and update the BIOS in servers as appropriate, and as supported by the VMware compatibility guide.

Item	Comments
Best Practice ID	ESXI-016
Recommendation	Verify that the BIOS is set to enable all CPU sockets, and enable all cores in each socket.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Performance

Justification

ESX Host	Data Center	Cluster	Hypervisor	Hypervisor Version	Server Vendor	Server Model	BIOS Version	B
esxi02.aerocivil.gov.co	Aerocivil	Aerocivil	VMware ESXi	7.0.3	HP	ProLiant DL580 Gen9	U17	TI
esxi01.aerocivil.gov.co	Aerocivil	Aerocivil	VMware ESXi	7.0.3	HP	ProLiant DL580 Gen9	U17	TI

Verify that the BIOS is set to enable all sockets and all cores in each socket. This allows the computing resources available on the system to be fully utilized.

References:

Hardware BIOS Settings section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Varies by hardware vendor, however typically this is done from the BIOS of the server.

Item	Comments
Best Practice ID	ESXI-017
Recommendation	Enable Turbo Mode in the BIOS if your processors support it.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Performance
Justification	<p>If your processor supports <i>Turbo Mode</i>, enable it in the BIOS to improve performance. The user interface might not display the change in CPU speed because it is calculated at boot time, so it might not reflect the gain from the Turbo Mode.</p> <p>References:</p>

Hardware BIOS Settings section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Varies by hardware vendor, but typically this is performed from within the BIOS.

Item	Comments
Best Practice ID	ESXI-018
Recommendation	Confirm that non-uniform memory access (NUMA) is enabled for NUMA-capable systems.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Scalability, Performance
Justification	<p>Some NUMA-capable systems provide an option to disable NUMA by enabling node interleaving.</p> <p>If node interleaving is disabled, ESXi detects the system as NUMA and applies NUMA optimizations. If node interleaving (also known as interleaved memory) is enabled, ESXi does not detect the system as NUMA.</p> <p>NUMA systems are advanced server platforms with more than one system bus. They can harness large numbers of processors in a single system image with superior price to performance ratios. NUMA links several small, cost-effective nodes using a high-performance connection. Each node contains processors and memory, much like a small SMP system. However, an advanced memory controller allows a node to use memory on all other nodes, creating a single system image. When a processor accesses memory that does not lie within its own node (remote memory), the data must be transferred over the NUMA connection, which is slower than accessing local memory. Therefore, using it properly increases the performance dramatically.</p> <p>ESXi 6.0 and above has virtual NUMA (vNUMA), which exposes the ESXi host's NUMA topology to the guest operating systems. Virtual NUMA topology is available to hardware version 8 virtual machines and above and is enabled by default when the number of virtual CPUs is greater than 8, allowing for a significant increase in performance.</p> <p>References:</p> <p>Using NUMA systems with ESXi - <i>vSphere Resource Management Guide</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-7E0C6311-5B27-408E-8F51-E4F1FC997283.html</p>

Performance Best Practices for vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Varies by hardware type. Typically this is performed from the BIOS.

Item	Comments
Best Practice ID	ESXI-019
Recommendation	Consider enabling hyperthreading if applicable and if the CPU and BIOS support it.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Performance

Justification

ESX Host	Data Center	Cluster	Server Vendor	Server Model	HT Available	HT Configured	HT Active	CPU Model	CPU MHz	CPU Packed
esxi02.aerocivil.gov.co	Aerocivil	Aerocivil	HP	ProLiant DL580 Gen9	true	true	true	Intel(R) Xeon 2195	4	4
esxi01.aerocivil.gov.co	Aerocivil	Aerocivil	HP	ProLiant DL580 Gen9	true	true	true	Intel(R) Xeon 2195	4	4

Hyperthreading can improve performance by taking advantage of additional CPU interrupt controllers and registers. In rare cases, enabling hyperthreading can hamper performance, so monitor the performance metrics after changing this setting.

If hyperthreading is used, confirm that it is enabled both in the BIOS and in the configuration for the ESXi host in VMware vCenter Server®. Be aware that you should not include the hyperthreaded CPU in calculations for performance however, because it equates only to 25 percent of a full CPU in terms of performance.

References:

Hardware BIOS Settings section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Varies by hardware type, but typically this is performed from the server BIOS.

Item	Comments
Best Practice ID	ESXI-020
Recommendation	Review ESXi hosts for driver and firmware consistency between hosts in a cluster.
Observation	

Priority	OK
Infrastructure Qualities	ESXi Hosts, Manageability, Performance
Justification	<p>ESXi hosts have drivers, firmware and other software installed that may be different depending on whether the VMware ESXi ISO was used, a vendor ISO was used, the time that the host was assembled, or if manual installation was performed for a device</p> <p>Ensuring that all hosts in a cluster of a specific hardware type have consistent drivers and firmware, including version of VIBs is incredibly important to ensure stability of the environment.</p> <p>Many concerns in the past have come from third party drivers and VIBs such as:</p> <ul style="list-style-type: none"> • Cisco enic (renamed to <code>enic</code>™ in 6.5+) • Cisco Fnics • EMC Power Path <p>If different driver levels are found on ESXi hosts in the same cluster then this could pose a problem and should be resolved</p> <p>In addition to this, verify that the driver and firmware version is supported in the VMware Compatibility List. Sometimes older/newer drivers or firmware are used which has known bugs, or is not supported.</p> <p>Procedure:</p> <p>Connect to the ESXi host and run:</p> <pre>esxcli software vib list</pre> <p>This lists installed software, once listed for each host compare it to ensure software and driver levels are the same.</p>
Item	Comments
Best Practice ID	ESXI-023
Recommendation	Check that the appropriate Power Management Settings are configured for the ESXi Host which meet the power consumption versus performance characteristics desired.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts

Justification

VMware ESXi includes a full range of host power management capabilities in the software that can save power when a host is not fully utilized. Configure the ESXi host to allow for flexibility in using (or not using) the power management features offered in the hardware. Consider the following:

- Set the power management in the BIOS to "OS Controlled Mode" or equivalent, so that ESXi can Control the power saving features.
- Consider the performance implications of C1E hardware managed state and application performance. These states reduce power consumption, however can reduce performance in multi threaded workloads that are sensitive to I/O Latency such as financial platforms or media and entertainment.
- C-States deeper than C1/C1E (Usually C3 or C6) are managed by software and enable further power savings. To take advantage of the savings you should enable all C-States, thereby allowing ESXi Hosts power management to control their use.
- When Turbo Boost is enabled, C1E and deep halt states can sometimes increase the performance of lightly threaded workloads.
- Select the best power policy for the workload at hand. Typically the **Balanced** policy will not impact CPU intensive or memory intensive workloads, however **High Performance** may be better suited to the environment.

Note that the C-State implementation between hardware vendors is different, varying results can be noticed. Proper testing and benchmarking should be performed to ensure ideal performance of systems.

References:

vSphere Performance Best Practices 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

For host settings, the procedure varies based on hardware selection, but typically power settings are configured in the BIOS.

For ESXi Specific settings navigate to **Hardware > Configure > Power Management**.

4.1.1.2. Licensing

Item	Comments
Best Practice ID	LIC-001
Recommendation	Verify that adequate licenses are available for vCenter Server instances.

Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Licensing, Manageability
Justification	<p>Having the proper number of available licenses is a requirement for using the features and functions of vCenter Server. Each vCenter Server instance uses a single license.</p> <p>This recommendation validates whether or not there are adequate licenses available for vCenter Server in the environment.</p> <p>If there are more vCenter Server instances than available licenses, a P1 Recommendation will be made. Otherwise, a P2 will be made if the license counts are approaching a fully utilized state. The recommendation can be ignored if there are no plans to add additional vCenter Server instances to the environment and, therefore, license usage is at capacity.</p> <p>References:</p> <p><i>Licensing ESXi 7.x and vCenter Server 7.x (2107538)</i> http://kb.vmware.com/kb/2107538</p> <p>Procedure:</p> <p>Licensing information can be reviewed from Administration > Licenses in the vSphere Client.</p>

Item	Comments
Best Practice ID	LIC-002
Recommendation	Verify that adequate CPU licenses are available for ESXi hosts.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Licensing, Manageability
Justification	<p>Having the proper number of available licenses is a requirement for using the features and functions of ESXi Hosts. Each ESXi host uses a license per CPU socket, and therefore several licenses might be required per host, depending on the number of CPUs in the host.</p> <p>This recommendation validates whether or not there are adequate licenses available for ESXi Hosts in the environment.</p> <p>If there are more ESXi hosts than available licenses, a P1 Recommendation will be made. Otherwise, a P2 will be made if the license counts are approaching a fully utilized state. The recommendation can be ignored if there are no plans to add additional</p>

ESXi hosts to the environment and, therefore, license usage is at capacity.

References:

Licensing ESXi 7.x and vCenter Server 7.x (2107538)
<http://kb.vmware.com/kb/2107538>

Procedure:

Licensing information can be reviewed from **Administration > Licenses** in the vSphere Client.

Item	Comments
Best Practice ID	LIC-003
Recommendation	Evaluation licenses should not be used in the environment.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, vCenter Server, Licensing, Manageability
Justification	<p>By default, if no license is configured, vCenter Server instances and ESXi hosts have a 60-day fully-featured evaluation license that can be used.</p> <p>After this period of time, the license expires, and will not allow for operations to continue until a valid license is entered.</p> <p>This recommendation triggers a P1 warning if there are any hosts or vCenter Server instances that do not have a license configured and are in evaluation mode.</p> <p>References:</p> <p><i>Licensing ESXi 7.x and vCenter Server 7.x (2107538)</i> http://kb.vmware.com/kb/2107538</p> <p>Procedure:</p> <p>Licensing information can be reviewed from Administration > Licenses in the vSphere Client.</p>
Item	Comments
Best Practice ID	LIC-004
Recommendation	Validate that proper licenses are installed for VMware vSAN clusters (if applicable).
Observation	
Priority	NA

Infrastructure Qualities	Licensing, Manageability, vSAN
Justification	<p>Having the proper licenses configured and available is a requirement for using the features and functions of VMware vSAN.</p> <p>This recommendation validates vSAN licensing in the environment, and that no evaluation license is being used on the cluster.</p> <p>References:</p> <p><i>Licensing for Clusters with Enabled vSAN</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-31AADB51-799C-40C2-882C-8D71B31C4BB9.html</p> <p>Procedure:</p> <p>Licensing information can be reviewed from Administration > Licenses in the vSphere Client.</p>

4.1.1.3. Network

Item	Comments
Best Practice ID	NE-003
Recommendation	Verify that there is redundancy in networking paths and components to avoid single points of failure.
Observation	
Priority	OK
Infrastructure Qualities	Network, Recoverability, Manageability
Justification	<p>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.</p> <p>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.</p> <p>In addition, upstream physical network components should also have the necessary redundancy to accommodate physical component failures.</p> <p>Note: Internal only virtual switches should be ignored as there is no redundancy needed for these. In addition, systems such as Cisco UCS</p>

or others with converged networking, should be verified to have proper redundancy configured for the ports.

References:

vSphere Networking Guide

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-B57FBE96-21EA-401C-BAA6-BDE88108E4BB.html>

Procedure:

Review the networking configuration to ensure that there is proper redundancy for the hosts.

Item	Comments
Best Practice ID	NE-004
Recommendation	Set up network redundancy for VMKernel network ports where required.
Observation	
Priority	OK
Infrastructure Qualities	Network, Recoverability
Justification	<p>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:</p> <ul style="list-style-type: none"> • Management Networks • iSCSI/NFS Storage networks • vSphere vMotion Networks • Fault Tolerance Logging Networks • vSAN Networks <p>Redundancy can most easily be accomplished by having multiple vmnics attached to the virtual switch.</p> <p>Note: Although this is recommended for resiliency, it might not be required. For example, in some blade environments where each NIC is connected to a separate physical switch, or systems such as Cisco UCS, the benefits of doing this are diminished.</p> <p>References:</p> <p><i>vSphere Networking Guide</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-B57FBE96-21EA-401C-BAA6-BDE88108E4BB.html</p> <p>Procedure:</p> <p>Review the VMKernel ports to validate whether they are protected by redundant switches. In the case of iSCSI port binding, multiple iSCSI VMKernel ports should exist.</p>

Item	Comments
Best Practice ID	NE-008
Recommendation	If beacon probing is used verify that there are at least three NICs.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Recoverability, Manageability
Justification	<p>Beacon probing can be used to improve network failure detection by sending out beacon probes on all NICs in a team to determine failures in the switch closest to the ESXi hosts where a failure does not cause a link down event for the host.</p> <p>At least three NICs are needed to reliably detect failures using beacon probing. If at least two NICs still have good connectivity and are receiving each other's beacons, the system can reliably determine which failed NIC to take out of service. For fewer than three NICs, beacon probing is non-deterministic.</p> <p>References:</p> <p><i>vSphere Networking Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-4D97C749-1FFD-403D-B2AE-0CD0F1C70E2B.html</p> <p><i>What is beacon probing? (1005577)</i> http://kb.vmware.com/kb/1005577</p> <p>Procedure:</p> <p>Validate the configuration of the virtual switch to see if beacon probing is used. If yes, then validate the number of NICs used.</p>
Item	Comments
Best Practice ID	NE-009
Recommendation	Use at least one 1 GbE adapter for workloads that have a small number of memory operations. Use at least one 10 GbE adapter if you migrate workloads that have many memory operations.
Observation	
Priority	OK
Infrastructure Qualities	Network, Performance
Justification	VMware requires vSphere vMotion traffic to be on a 1-Gbps network at a minimum. VMware recommends that the vSphere vMotion network is on a separate, isolated, network segment.

Also, for increased performance consider using either a 10-Gb vSphere vMotion network, or multiple physical NICs. Using either one of these configurations for vSphere vMotion will result in significant improvements in vSphere vMotion performance. This is most evident when using large or a large number of virtual machines.

References:

Networking Best Practices for vSphere vMotion section of the *vCenter Server Host and Management Guide* for vSphere 7.0

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-7DAD15D4-7F41-4913-9F16-567289E22977.html>

Procedure:

Review the NIC attached to the vMotion network to ensure it uses the appropriate speeds required.

Item	Comments
Best Practice ID	NE-010
Recommendation	Use static IP addresses for the management ESXi host management interface.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Manageability
Justification	<p>Static IP addresses are recommended for management interfaces to ease administration, automation, management, and integration. If the management IP address changes, it can result in connection losses with other vSphere components that rely on communication through the management interface.</p> <p>Static IP addresses can be optionally assigned using DHCP with statically reserved addresses.</p> <p>Procedure:</p> <p>Review the management network configuration to see if it uses a static IP.</p>

Item	Comments
Best Practice ID	NE-011
Recommendation	Make sure that vSphere FT logging traffic is on at least a segregated 10-Gbps network.
Observation	
Priority	OK

Infrastructure Qualities	Network, Performance
Justification	<p>With the addition of vSMP Fault Tolerance, additional bandwidth is required for vSphere Fault Tolerance. VMware requires that vSphere FT traffic be on at least a 10-Gbps network.</p> <p>VMware also recommends that vSphere FT traffic be kept separate from other traffic through the use of dedicated NICs (or Network I/O Control)</p> <p>References:</p> <p><i>vSphere Availability Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-2A87B967-5BBB-4394-B1E6-EE87D50A2A86.html</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p> <p>Review the Fault Tolerance configuration to ensure a 10Gbps network is attached.</p>
Item	Comments
Best Practice ID	NE-012
Recommendation	Single port 10-GbE network adapters should use PCIe x8 (or higher) or PCI-X 266. Dual port 10-GbE should use PCIe x16 or higher.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Performance
Justification	<p>Single-port 10-Gigabit Ethernet network adapters should use PCIe x8 (or higher) or PCI-X 266, and dual-port 10-Gigabit Ethernet network adapters should use PCIe x16 (or higher). This is so that the required throughput is available for maximum performance.</p> <p>It is also preferable not to have a "bridge chip" (for example, PCI-X to PCIe or PCIe to PCI-X) in the path to the actual Ethernet device (including any embedded bridge chip on the device itself) because these chips can reduce performance.</p> <p>Ideally, 40Gb/s Ethernet network adapters should use PCI Gen3 x8/x16 slots (or higher).</p> <p>References:</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/</p>

[techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf](https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf)

Procedure:

Validate the hardware configuration of the host to ensure proper placement of NICs for top performance.

Item	Comments
Best Practice ID	NE-013
Recommendation	Limit the number of installed NIC ports to recommended maximums.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Configuration Maximums, Scalability
Justification	<p>This ensures that the configuration will be supported and no issues will occur as a result. When using a large number of NICs on an ESXi host, verify that the system has adequate memory and an appropriate number of CPUs. Thoroughly qualify all such configurations prior to deployment.</p> <p>References:</p> <p><i>Networking Maximums section of the Configuration Maximums for vSphere 7.0 guide</i></p> <p>https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p> <p>Review the network configuration and validate no maximums are exceeded.</p>

Item	Comments
Best Practice ID	NE-014
Recommendation	Minimize differences in the number of active NICs across hosts within a cluster.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Manageability, Performance
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.

References:

Performance Best Practices for vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Review the network configuration to ensure that there is no dramatic difference between hosts in a cluster.

Item	Comments
Best Practice ID	NE-015
Recommendation	Check for dropped packets on vmnic objects.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Performance
Justification	<p>Check the network performance for all vmnic objects for hosts using the performance information in vCenter Server. If the dropped transmit or dropped receive packets for one or more vmnics is greater than 0, then packets are being dropped.</p> <p>The solutions to the problem of dropped receive packets are all related to ways of improving the ability of the guest OS to quickly retrieve packets from the virtual NIC. Solutions include:</p> <ul style="list-style-type: none"> • Increase CPU resources provided to the virtual machine. • Increase the efficiency with which the virtual machine uses CPU resources. • Tune the network stack in the guest OS. • Add additional virtual NICs to the virtual machine and spread the network load across them. <p>If the traffic from the virtual machines sharing the virtual switch exceeds the physical capabilities of the uplink NICs or the networking infrastructure, the virtual switch buffers can fill and transmit packets can be dropped. To prevent transmit packets from being dropped, perform one of the following:</p> <ul style="list-style-type: none"> • Add additional uplink capacity to the virtual switch. • Move some virtual machines with high network demand to a different virtual switch. • Enhance the networking infrastructure.

- Reduce network traffic.

References:

Solutions for Poor Network Performance section of *vSphere Monitoring and Performance vSphere 7.0*

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-C4EA86FD-95CB-4DE7-A9E3-63F6BFC1A268.html>

Procedure:

Review the network statistics for the ESXi Hosts network interfaces for packet loss.

Item	Comments
Best Practice ID	NE-016
Recommendation	If jumbo frames are enabled, verify that jumbo frame support is enabled end-to-end on all intermediate devices so that there is no MTU mismatch.
Observation	
Priority	NA
Infrastructure Qualities	Network, Scalability, Performance
Justification	<p>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.</p> <p>Note: The configuration of Jumbo frames is one of customer choice and comfort. The performance gains are often not worth the cost and effort to configure them end-to-end in the environment. Misconfigurations can also cause more significant performance loss than the gains would provide. Guidance therefore is to configure them if the environment is already using them, not to convert the environment to use them.</p> <p>References:</p> <p><i>vSphere Networking Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-5823F07F-8B02-49C3-8FC0-DC220B0284C8.html</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p>

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and select **Properties**.
3. Click **Edit**.
4. Click **Advanced** and set the MTU property to a value greater than 1500 bytes. You cannot set the MTU size to a value greater than 9000 bytes.
5. Click **OK**.

Item	Comments
Best Practice ID	NE-018
Recommendation	Avoid mixing NICs with different speeds and duplex settings on the same uplink for a port group/dvport group.
Observation	
Priority	OK
Infrastructure Qualities	Network, Performance
Justification	<p>Having a port group/dvport group 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.</p> <p>For example, suppose there are several virtual machines all connected to a single virtual switch with two outbound adapters, one at 1-Gbps and one at 10-Gbps. Some virtual machines would have better performance than others depending on how their traffic is routed.</p> <p>A best practice is to verify that the speed is predictable and deliberately chosen.</p> <p>Procedure:</p> <p>Review the NIC configuration and adjust settings as appropriate</p>

Item	Comments
Best Practice ID	NE-019
Recommendation	Adjust load balancing settings from the default virtual port ID only if necessary.
Observation	
Priority	OK
Infrastructure Qualities	Network, Recoverability, Performance

Justification

A virtual switch has optional NIC teaming settings to set policies on traffic across multiple physical adapters. These settings can be defined at the virtual switch level or overridden at the individual port groups/port level.

The default load balancing policy is to route outbound network traffic based on the originating virtual port ID. ESXi chooses an uplink based on the virtual port where the traffic entered the virtual switch. Incoming traffic is controlled by the Load Balancing policy on the physical switch.

Alternative load balancing policies (routing based on IP hash, routing based on MAC address, routing based on physical NIC load) are available. They incur additional overhead but can offer better load balancing. IP hash should be used only if the link conforms to 802.3ad and has at least two NICs.

If using Network I/O Control (NETIOC), on a vSphere Distributed Switch, the Load-Based Teaming policy is recommended.

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:

Load Balancing and Failover Policy section of *vSphere Networking*
<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-4D97C749-1FFD-403D-B2AE-0CD0F1C70E2B.html>

Procedure:

Review the Load balancing configuration for the port group and validate that it is configured appropriately.

Item	Comments
Best Practice ID	NE-020
Recommendation	Verify that the network topology does not contain link oversubscription resulting in dropped packets.
Observation	
Priority	OK
Infrastructure Qualities	Network, Scalability, Performance
Justification	<p>Verify that the network topology does not contain Ethernet bottlenecks where multiple links are routed through fewer links, potentially resulting in oversubscription and dropped network packets. Oversubscription is possible if a number of links transmitting near capacity are switched to a smaller number of links.</p> <p>References:</p>

Performance Best Practices for VMware vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Review the physical network with the network team to validate that adequate bandwidth is available.

Item	Comments
Best Practice ID	NE-021
Recommendation	Use Network I/O Control (NetIOC) to prioritize traffic.
Observation	
Priority	OK
Infrastructure Qualities	Network, Performance
Justification	<p>All network traffic can benefit from NetIOC traffic prioritization during contention scenarios.</p> <p>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.</p> <p>Note: In converged systems where a limited number of NICs are available, Network I/O Control is highly recommended.</p> <p>References:</p> <p><i>Network I/O Control section of the vSphere Networking guide</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-ADEA0213-C969-43E4-B1F4-66D4A916EBDF.html</p> <p>Procedure:</p> <p>Review the distributed switch Network I/O Control configuration.</p>

Item	Comments
Best Practice ID	NE-022
Recommendation	Use shares instead of limits when using NIOC for bandwidth allocation. Do not impose limits unless addressing physical network capacity requirements.
Observation	
Priority	OK

Infrastructure Qualities	Network, Performance
Justification	<p>NIOC revolves around resource pools similar for CPU and memory. The vSphere administrator is given the control to ensure predictable network performance when multiple traffic types contend for the same physical network resources (NIOC is supported only with the vSphere Distributed Switch)</p> <p>NIOC shares “ Allows flexible networking capacity partitioning to help users deal when flows compete for the same resources.</p> <p>NIOC limits “ Enforce traffic bandwidth limit on the overall VDS set of dvUplinks.</p> <p>Shares provides flexibility and better utilization of bandwidth. Shares can be used to decide what percentage of physical bandwidth is allocated for a particular traffic type (For example, management, vSphere vMotion, NFS, and iSCSI).</p> <p>If a limit is configured for a traffic type, it cannot utilize the unused bandwidth of a NIC and go over unassigned limits.</p> <p>Note: Limits override shares</p> <p>As a best practice, VMware recommends not using the limits parameter, unless the customer really wants to control the traffic type. Use limits only to conserve physical network resources.</p> <p>References:</p> <p><i>Network I/O Control section of the vSphere Network Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-ADEA0213-C969-43E4-B1F4-66D4A916EBDF.html</p> <p>Procedure:</p> <p>Review the configuration for shares and limits and ensure that the appropriate configuration is in place to ensure optimal performance.</p>
Item	Comments
Best Practice ID	NE-023
Recommendation	If Fault Tolerance is used, set Network I/O Control Fault Tolerance resource pool shares to High.
Observation	
Priority	OK
Infrastructure Qualities	Network, Performance
Justification	<p>Fault tolerance is a latency-sensitive traffic flow. VMware recommends setting the NetIOC resource pool shares for Fault Tolerance traffic to a reasonably high relative value. If you are not using custom shares, a setting of High is appropriate.</p>

References:

Network I/O Control Section of the vSphere Networking Guide

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-ADEA0213-C969-43E4-B1F4-66D4A916EBDF.html>

Procedure:

Navigate to the Network I/O Control Configuration and review the Share configuration for Fault Tolerance Traffic.

Item	Comments
Best Practice ID	NE-025
Recommendation	Configure network appropriately when VMware vSphere Auto Deploy is used.
Observation	
Priority	NA
Infrastructure Qualities	Network, Manageability
Justification	<p>If VMware vSphere Auto Deploy is used, prevent networking problems by following vSphere Auto Deploy networking best practices:</p> <ul style="list-style-type: none"> IP Address allocation - Using DHCP reservations is highly recommended for address allocation. Fixed IP addresses are supported by the host customization mechanism, but providing input for each host is cumbersome and not recommended. VLAN considerations - Using Auto Deploy in environments that do not use VLANs is highly recommended. If you intend to use Auto Deploy in an environment that uses VLANs, confirm that the hosts you want to provision can reach the DHCP server. How hosts are assigned to a VLAN depends on the setup at your site. The VLAN ID might be assigned by the switch or by the router, or you might be able to set the VLAN ID in the host BIOS or through the host profile. Contact your network administrator to determine the steps for allowing hosts to reach the DHCP server.

References:

Auto Deploy Networking Best Practices section of the vSphere Installation and Setup Guide for vSphere 7.0

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-980D9E38-633E-4557-9144-AC422FA239C5.html>

Item	Comments
------	----------

Best Practice ID	NE-026
Recommendation	Verify latency between vCenter Server and other network components.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Network, Availability, Manageability
Justification	<p>Network latency can cause performance and availability problems within an environment. Verify that there is not significant latency (generally above 150 ms but this varies based on the component) on the network.</p> <p>The number of hops between the components of a data center can also increase latency. In particular, validate the connectivity between vCenter Server and ESXi hosts, between ESXi hosts, and from client to vCenter.</p> <p>References:</p> <p>Performance Best Practices for vSphere 7.0 https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p> <p>Review the latency metrics for the network to validate the appropriate configuration.</p>

4.1.1.4. Security

Item	Comments
Best Practice ID	SEC-001
Recommendation	Confirm integrated Windows authentication is configured when using Active Directory identity sources.
Observation	The vCenter server is integrated with the aerocivil.gov.co domain.
Priority	OK
Infrastructure Qualities	vCenter Server, Security
Justification	vCenter Single Sign-On can be configured to authenticate off of several different types of identity sources. When connecting to Microsoft Active Directory, SSO should be configured using Integrated Windows Authentication rather than LDAP binds. This allows the Single Sign-On server to connect to the Active Directory using native Active Directory API calls. It does this by using the credentials of an SPN user or the computer account of the computer on which SSO is installed.

This resolves many problems that occur with LDAP binds, including most commonly, a failure to properly authenticate using domain trusts.

References:

vSphere Authentication with vCenter Single Sign-On
<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.authentication.doc/GUID-B98DF9C2-FE7D-483F-9521-C17C138B59D8.html>

Procedure:

Navigate to **Administration > Single Sign-On > Configuration**, and validate the identity source.

Item	Comments
Best Practice ID	SEC-002
Recommendation	Confirm that time is synchronized on the SSO Server and on any server that connects to the SSO server.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Security
Justification	<p>Before you install vCenter Server verify that all machines on the vSphere network have their clocks synchronized, including any other vCenter Server instances and the ESXi servers.</p> <p>If the clocks on vCenter Server network machines are not synchronized, Kerberos and SSL certificates, which are time-sensitive, might not be recognized as valid in communications between network machines. Unsynchronized clocks can result in authentication problems, which can cause the vSphere Client to fail or prevent the VMware vCenter Server Appliance's vpxd service from starting.</p> <p>References:</p> <p>Synchronizing Clocks on the vSphere Network section of the <i>vSphere Installation and Setup Guide</i> for vSphere 7.0 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-9FD3A5E3-6C2D-4161-9270-4BF57FADCE6D.html</p> <p>Procedure:</p> <p>Validate that the time is correctly set on all components in the environment.</p>

Item	Comments
Best Practice ID	SEC-003
Recommendation	Record the Single Sign-On administrator password in a safe place.

Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Security
Justification	<p>When installing vCenter Server for first time, the administrator password for the Single Sign-On domain is configured. By default this account is the administrator@vsphere.local account. Be sure to record the password for future use, as it is the only account that has access to the virtual infrastructure until additional security is configured.</p> <p>References:</p> <p>Required information for installing or upgrading vCenter Single Sign-On section of the <i>vSphere Installation and Setup Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-077C7523-E0EA-4922-8D48-C026916323C4.html</p>
Item	Comments
Best Practice ID	SEC-004
Recommendation	Avoid using local operating system users with vCenter Single Sign-On.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Security
Justification	<p>With vCenter Single Sign-On, local operating system users become less important than the users in a directory service, such as Active Directory. As a result, it is not always possible, or even desirable, to keep local operating system users as authenticated users.</p> <p>VMware recommends that all users be part of a directory services instance. This allows for ease of administration because all accounts are stored in a central location.</p> <p>References:</p>
Item	Comments
Best Practice ID	SEC-005
Recommendation	Set the vCenter Single Sign-On default domain to the identity source which is most frequently used.
Observation	The vCenter servers SSO user is not used frequently. All users accessing the vCenter server environment do so with their Aerocivilian domain account.

Priority	OK
Infrastructure Qualities	vCenter Server, Security
Justification	<p>When a user logs in to a vCenter Server system from the vSphere Client, the login behavior depends on whether the user is in the default domain.</p> <ul style="list-style-type: none"> • Users who are in the default domain can log in with their user name and password. • Users who are in a domain that has been added to vCenter Single Sign-On as an identity source, but not the default domain, can log in to vCenter Server. However, they must specify the domain in one of the following ways: <ul style="list-style-type: none"> ○ Including a domain name prefix. For example, MYDOMAIN\user1 ○ Including the domain. For example, user1@mydomain.com • Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. <p>Only a single default domain can be set. If your user is not in the default domain, you must qualify it as mentioned previously.</p> <p>References:</p> <p><i>vSphere Installation and Setup Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.authentication.doc/GUID-11E651EF-4503-43BC-91F1-15502D586DE2.html</p> <p>Procedure:</p> <p>To set the Default Domain:</p> <ol style="list-style-type: none"> 1. Log in with the vSphere Client to the vCenter Server connected to the Platform Services Controller. 2. Specify the user name and password for <code>administrator@vsphere.local</code> or another member of the vCenter Single Sign-On Administrators group. If you specified a different domain during installation, log in as <code>administrator@mydomain</code>. 3. From the Home menu, select Administration. 4. Under Single Sign On, click Configuration. 5. Click Identity Sources, select an identity source, and click Set as Default. In the domain display, the default domain shows (default) in the Domain column.
Item	Comments
Best Practice ID	SEC-006
Recommendation	Set the Single Sign-On password and lockout policies per customer security requirements.

Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Security
Justification	<p>The vCenter Single Sign-On password and lockout policies are a set of rules and restrictions on the format, expiration, and conditions under which the account is locked. The policies apply only to users in the vCenter Single Sign-On domain (vsphere.local).</p> <p>The policies should be set according to the security policy that is required by the company.</p> <p>References:</p> <p>Edit the vCenter Single Sign-On Password Policy section of the <i>vSphere Security Guide</i> for vSphere 7.0 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.authentication.doc/GUID-43527B09-63BB-44A6-91D3-E3A470904698.html</p> <p>Procedure:</p> <p>To edit the password policy:</p> <ol style="list-style-type: none"> 1. Log in with the vSphere Client to the vCenter Server connected to the Platform Services Controller. 2. Specify the user name and password for <code>administrator@vsphere.local</code> or another member of the vCenter Single Sign-On Administrators group. 3. If you specified a different domain during installation, log in as <code>administrator@mydomain</code>. 4. From the Home menu, select Administration. 5. Under Single Sign On, click Configuration. 6. Click Policies, select Password Policy, and click Edit. 7. Edit the password policy and click Ok.
Item	Comments
Best Practice ID	SEC-007
Recommendation	Add only the necessary identity sources to the vCenter Single Sign-On configuration.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Security, Performance
Justification	To minimize search overhead and improve security, verify that only the necessary identity source servers are added to the vCenter Single Sign-On configuration.

You can browse and manage the identity sources attached to the vCenter Single Sign-On server using the configuration user interface in the vSphere Client.

References:

VMware Single Sign-On Server Performance section of *Performance Best Practices for vSphere 7.0 guide*.
<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Navigate to the **Administration > Single Sign-On > Configuration** interface and select Identity Sources. Verify that only the required sources are listed.

Item	Comments
Best Practice ID	SEC-008
Recommendation	Set the base domain name for users and groups accordingly in Single Sign-On when using LDAP or OpenLDAP identity sources.
Observation	LDAP: Aerocivil.gov.co
Priority	OK
Infrastructure Qualities	vCenter Server, Security, Manageability
Justification	<p>When using LDAP or OpenLDAP identity sources, assign a base domain name for users and for groups to the common portion of the domain name. This step significantly increases the performance of browsing and searching for users in large identity sources.</p> <p>References:</p> <p>VMware Single Sign-On Server Performance section of <i>Performance Best Practices for vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p> <p>Edit the identity source and you can see whether the Base DSN is chosen appropriately.</p>

Item	Comments
Best Practice ID	SEC-009
Recommendation	Limit remote access to all hosts by administrative users such as root.
Observation	

Priority	OK
Infrastructure Qualities	ESXi Hosts, Security, Manageability
Justification	<p>Manage the vSphere infrastructure using the vSphere Client connected to vCenter Server using a named administrative account with the appropriate level of access, rather than the default superuser <i>root</i> or <i>administrator</i> account. Using named user accounts provides auditability and traceability for changes in the environment.</p> <p>This can be accomplished by either:</p> <ul style="list-style-type: none"> • Enabling Active Directory authentication, allowing users to log in with their Active Directory accounts. • Creating separate non-root user accounts on the ESXi host directly. <p>In addition, for some administrative and bulk operations the vCLI, VMware vRealize Orchestrator or VMware PowerCLI can be used to programmatically access the environment.</p> <p>References:</p> <p><i>VMware Security Hardening Guide</i> http://www.vmware.com/security/hardening-guides.html</p>

Item	Comments
Best Practice ID	SEC-010
Recommendation	Configure firewall rules and ports according to best practices.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Security, Manageability
Justification	<p>The default firewall rules are configured to provide adequate security while allowing communication with the appropriate VMware virtual infrastructure components.</p> <p>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.</p> <p>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. For example, NTP, Syslog, and vSphere HA services require additional ports opened when using these features.</p>

References:

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 in the ESXi Prerequisites list

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-171B99EA-15B3-4CC5-8B9A-577D8336FAA0.html>

Item	Comments
Best Practice ID	SEC-011
Recommendation	Configure VMware vSphere ESXi Shell and SSH access per manageability requirements.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Security, Manageability
Justification	<p>The VMware 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).</p> <p>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.</p> <p>For security reasons, VMware recommends disabling these options until required by an administrator to decrease the attack surface of the ESXi host.</p> <p>References:</p> <p>Using ESXi Shell in ESXi 5.x, 6.x and 7.x (2004746) http://kb.vmware.com/kb/2004746</p> <p>VMware Security Hardening Guide http://www.vmware.com/security/hardening-guides.html</p>
Item	Comments
Best Practice ID	SEC-012
Recommendation	Enable the ESXi Shell timeout feature and configure it per customer security requirements.

Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Security
Justification	<p>In ESXi, the ESXi Shell timeout feature automatically logs out unused ESXi Shell sessions to prevent unauthorized access.</p> <p>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.</p> <p>References:</p> <p><i>VMware Security Hardening Guide</i> http://www.vmware.com/security/hardening-guides.html</p> <p>Procedure:</p> <p>Navigate to the ESXi Direct Console User Interface (DCUI), login, and select Troubleshooting Options > Modify ESXi Shell and SSH Timeouts.</p>
Item	Comments
Best Practice ID	SEC-013
Recommendation	Keep current with the latest VMware product versions and patches.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, vCenter Server, Security, Manageability
Justification	<p>Upgrade each ESXi host and vCenter Server with the latest available versions and patches to take advantage of bug fixes and enhancements. If problems are encountered, VMware Support is best positioned to assist with and troubleshoot current software versions.</p> <p>In addition, with vSphere vMotion properly configured, some loads can be temporarily shifted between ESXi hosts to facilitate ESXi host upgrades without impacting virtual machine availability.</p> <p>Note: When upgrading, verify that the hardware is supported for use with the newer version of ESXi.</p> <p>References:</p> <p><i>VMware Security Hardening Guide</i> http://www.vmware.com/security/hardening-guides.html</p> <p>Procedure:</p> <p>Review versions of vSphere, and use Update Manager to Update the hosts to the latest versions.</p>

Item	Comments
Best Practice ID	SEC-016
Recommendation	Change port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes to Reject unless required.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Network, Security
Justification	<p>VMware recommends that port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes be set to Reject for improved security.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>References:</p> <p>Securing ESXi Configurations section in the <i>vSphere Security Guide for vSphere 7.0</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-3507432E-AFEA-4B6B-B404-17A020575358.html</p> <p>VMware Security Hardening Guide http://www.vmware.com/security/hardening-guides.html</p> <p>Procedure:</p> <p>Review the port security settings to ensure that they are appropriately set for highest levels of security.</p>
Item	Comments
Best Practice ID	SEC-017

Recommendation	Enable bidirectional CHAP authentication for iSCSI traffic so that CHAP authentication secrets are unique.
Observation	
Priority	NA
Infrastructure Qualities	Storage, Security
Justification	<p>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.</p> <p>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.</p> <p>References:</p> <p><i>VMware vSphere Security Hardening Guide</i> http://www.vmware.com/security/hardening-guides.html</p>

Item	Comments
Best Practice ID	SEC-018
Recommendation	Configure Management network Traffic on an isolated network.
Observation	
Priority	OK
Infrastructure Qualities	Network, Security, Manageability
Justification	<p>VMware recommends having vSphere Management traffic on a restricted network and strictly control its access. To avoid bandwidth issues, configure the isolated networks on different subnets.</p> <p>While using VLANs to isolate the networks, it is recommended having different subnets so that routing tables are set up correctly.</p> <p>References:</p> <p><i>VMware Security Hardening Guide</i> http://www.vmware.com/security/hardening-guides.html</p>
Item	Comments
Best Practice ID	SEC-019

Recommendation	Validate that copy/paste between the guest operating system and the remote console is disabled.
Observation	
Priority	OK
Infrastructure Qualities	Security, Virtual Machine
Justification	<p>When VMware Tools runs in a virtual machine, the functionality exists to be able to copy and paste between the guest operating system and the computer where the remote console is running. As soon as the console window gains focus, non-privileged users and processes running in the virtual machine can access the clipboard of the virtual machine console. If a user copies sensitive information to the clipboard before using the console, the user, perhaps unknowingly, exposes sensitive data to the virtual machine.</p>

This functionality is disabled by default with vSphere 6.5 and beyond as the platform is secure by default. Validate that the values are still disabled. It is recommended that copy and paste for the guest operating system is disabled. Note that if no parameter exists it is disabled as indicated below. Validate that the setting is not set to false, meaning it is enabled.

Note: This does not disable copy and paste for the users when they access the virtual machine through other means such as Terminal Services. This disables copy and paste only from the virtual machine console, for example, when using the console from the vSphere Web Client and the vSphere Client.

Configuration Settings to Disable Copy and Paste

```
isolation.tools.copy.disable - true
```

```
isolation.tools.paste.disable - true
```

References:

VMware Security Hardening Guide
<http://www.vmware.com/security/hardening-guides.html>

Item	Comments
Best Practice ID	SEC-020
Recommendation	Verify that VMware isolation settings have not been disabled.
Observation	
Priority	OK

Infrastructure Qualities	Security, Virtual Machine
Justification	<p>VMware virtual machines are designed to work on both vSphere and hosted virtualization platforms (such as VMware Workstation®, and VMware Fusion®), some VMX parameters do not apply when running on vSphere.</p> <p>Although the functionality governed by these parameters is not exposed on ESXi, explicitly disabling them reduces the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus might help prevent successful attacks.</p> <p>As of vSphere 6.5 and beyond, the platform has been made secure by default. Thus, unless explicitly configured these settings are already enabled. Validate that none of these settings are set to False on the VMs.</p> <hr/> <pre>isolation.tools.ghi.autologon.disable - True</pre> <hr/> <pre>isolation.bios.bbs.disable - True</pre> <hr/> <pre>isolation.tools.getCreds.disable - True</pre> <hr/> <pre>isolation.tools.ghi.launchmenu.change - True</pre> <hr/> <pre>isolation.tools.memSchedFakeSampleStats.disable - True</pre> <hr/> <pre>isolation.tools.ghi.protocolhandler.info.disable - True</pre> <hr/> <pre>isolation.ghi.host.shellAction.disable - True</pre> <hr/> <pre>isolation.tools.dispTopoRequest.disable - True</pre> <hr/> <pre>isolation.tools.trashFolderState.disable - True</pre> <hr/> <pre>isolation.tools.ghi.trayicon.disable - True</pre> <hr/> <pre>isolation.tools.unity.disable - True</pre> <hr/> <pre>isolation.tools.unityInterlockOperation.disable - True</pre> <hr/> <pre>isolation.tools.unity.push.update.disable - True</pre> <hr/> <pre>isolation.tools.unity.taskbar.disable - True</pre> <hr/>

isolation.tools.unityActive.disable - True

isolation.tools.unity.windowContents.disable - True

isolation.tools.vmxDnDVersionGet.disable - True

isolation.tools.guestDnDVersionSet.disable - True

References:

VMware Security Hardening Guide

<http://www.vmware.com/security/hardening-guides.html>

Item	Comments
Best Practice ID	SEC-022
Recommendation	For additional security for NFS v4.1 shares, configure Kerberos authentication.
Observation	
Priority	NA
Infrastructure Qualities	Storage, Security

Justification

With NFS version 4.1, ESXi supports Kerberos authentication mechanism for additional security. Kerberos is an authentication service that allows for the NFS 4.1 client installed on ESXi to prove its identity to an NFS server before mounting an NFS share. Kerberos uses cryptography to work across an insecure network connection. The vSphere implementation of Kerberos for NFS 4.1 supports only identity verification for the client and server. It does not provide data integrity or confidentiality services.

References:

vSphere Storage Guide for vSphere 7.0

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-987194A1-E4F8-470D-B28F-3B4DB9B4CCB4.html>

Item	Comments
Best Practice ID	SEC-024
Recommendation	Configure Encrypted vSphere vMotion if the organization policy requires it.
Observation	

Priority	OK
Infrastructure Qualities	vCenter Server, Network, Security, Virtual Machine
Justification	<p>vSphere 6.7 and above allow for encrypted vSphere vMotion. This feature encrypts vSphere vMotion traffic when both the source and destination hosts are capable of supporting encrypted vSphere vMotion (that is, when both hosts are running ESXi 6.5 and beyond). If a virtual machine running on ESXi 6.5 or above is migrated to a host running an earlier VMware ESXi version, vSphere vMotion traffic is not encrypted.</p> <p>Encryption performance is significantly higher on hosts that support AES-NI (Intel's Advanced Encryption Standard New Instruction Set). Without AES-NI, encrypted vSphere vMotion operations might have unacceptable performance. Encrypted virtual machines are always moved with encrypted vSphere vMotion. For virtual machines that are not encrypted, vSphere vMotion encryption can be changed from Opportunistic (the default) to Disabled or Required (right-click the virtual machine, select Edit Settings, select VM Options, click Encryption, select an option from the Encrypted vMotion drop-down menu).</p> <p>References:</p> <p>Performance Best Practices for vSphere 7.0</p> <p>https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>

4.1.1.5. Storage

Item	Comments
Best Practice ID	ST-001
Recommendation	Consult with the storage vendor for recommendations for use with the storage device in the environment.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Configuration Maximums, HCL, Manageability, Scalability
Justification	<p>VMware Global Services has seen that the majority of storage problems are due to a misconfiguration of the underlying storage in the environment.</p> <p>These problems are generally avoided by ensuring that the environment is set up for best practices and considerations as put forward by the storage vendor. For example, configuring path policies and performing array software/firmware and performance tuning.</p>

In addition consult the vendor about technologies such as VMware vStorage APIs for Array Integration (VAAI) for best performance of an array. Many times a firmware upgrade of the array will be required but will provide significant gains in performance.

References:

vSphere Storage Guide for vSphere 7.0

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html>

Configuration Maximums for vSphere

<https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0>

Item	Comments
Best Practice ID	ST-002
Recommendation	Deploy storage in compliance with all configuration maximums as documented in the most current vSphere Configuration Maximums document.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Configuration Maximums, Manageability, Scalability
Justification	<p>VMware software functions within specified operating parameters. When the software is implemented out of compliance with recommended parameters, unpredictable results can occur.</p> <p>References:</p> <p><i>Configuration Maximums for vSphere 7.0</i></p> <p>https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0</p> <p>Fibre Channel SAN Concepts and iSCSI SAN Concepts section of the <i>vSphere Storage Guide</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p>
Item	Comments
Best Practice ID	ST-003
Recommendation	Use shared storage for virtual machines instead of local storage.
Observation	
Priority	OK

Infrastructure Qualities	Storage, Recoverability, Manageability, Scalability, Performance
Justification	<p>Shared storage provides availability, scalability, manageability, and performance benefits. Many vSphere advanced features, such as vSphere vMotion, vSphere DRS, and HA require shared storage. There are many available options that are supported such as Fibre Channel, iSCSI, NFS, or vSAN.</p> <p>References:</p> <p>Fibre Channel SAN Concepts and iSCSI SAN Concepts section of the <i>vSphere Storage Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p> <p>Procedure:</p> <p>Review all non shared volumes for VMs that are not on shared storage.</p>
Item	Comments
Best Practice ID	ST-004
Recommendation	Zone Fibre Channel LUNs properly to the appropriate devices for vSphere vMotion compatibility, security, and shared services.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Security, Manageability
Justification	<p>Take into account the following zoning considerations:</p> <ul style="list-style-type: none"> • Soft versus hard zoning • Zone security • Zone size and merging issues <p>For all ESXi hosts in a vSphere DRS cluster or vSphere vMotion scope, verify that the appropriate initiators and targets are zoned according to the storage vendor's best practices.</p> <p>Single initiator zoning is encouraged to eliminate crosstalk between hosts. For active/passive arrays, confirm that each HBA has a path to the active and passive storage processor in their respective fabric. Systems that provide shared services, such as backup, must also be part of the zone.</p> <p>With ESXi hosts, single-initiator single-target zoning is a preferred zoning practice. Using more restrictive zoning prevents problems and misconfigurations that can occur on the SAN.</p> <p>References:</p> <p>vSphere Storage Guide for vSphere 7.0 - Using Zoning with FC Storage https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p>

[vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-E7818A5D-6BD7-4F51-B4BA-EFBF2D3A8357.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-E7818A5D-6BD7-4F51-B4BA-EFBF2D3A8357.html)

Procedure:

Review the physical configuration to virtual configuration ensuring LUNs are Zoned to appropriate hosts.

Item	Comments
Best Practice ID	ST-005
Recommendation	Minimize differences in datastores visible across hosts within the same cluster or vSphere vMotion scope.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Recoverability, Security, Manageability
Justification	<p>Having a consistent storage presentation allows virtual machines to run on any host in the cluster. This optimizes HA and DRS while reducing troubleshooting. Use LUN masking and zoning to determine which devices are visible to hosts.</p> <p>References:</p> <p><i>vSphere Storage Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p> <p>Procedure:</p> <p>Review the vMotion Scope and ensure that datastores are presented appropriately.</p>
Item	Comments
Best Practice ID	ST-006
Recommendation	Use the appropriate policy based on the array being used (MRU, Fixed, Round Robin, and so on).
Observation	
Priority	OK
Infrastructure Qualities	Storage, Availability, Recoverability, Manageability
Justification	<p>If the path selection policy is configured incorrectly for a given array architecture, availability and performance issues can occur. For example, setting Fixed for an active/passive array can cause path thrashing.</p>

The Fixed path policy is recommended for Active/Active arrays. It allows the user to configure static load balancing of paths across ESXi hosts.

The MRU policy is recommended for Active/Passive arrays. It prevents path thrashing due to a partitioned SAN environment.

Round robin can be configured for either Active/Active or Active/Passive arrays, but make sure that Active/Passive arrays are not configured to switch controllers automatically. If Active/Passive arrays are configured to switch controllers automatically (sometimes called pseudo Active/Active), performance may degrade due to path ping ponging.

Consult the storage array vendor documentation for further information.

References:

Path Selection Plug-Ins and Policies in vSphere Storage guide for vSphere 7.0

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-B7AD0CA0-CBE2-4DB4-A22C-AD323226A257.html>

Procedure:

Review the configured multi-pathing configuration for each LUN to ensure that it is configured appropriately.

Item	Comments
Best Practice ID	ST-007
Recommendation	Manage the differences in the number of storage paths between hosts including maximum paths per host.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Storage, Recoverability, Manageability
Justification	<p>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.</p> <p>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.</p> <p>Also make sure that there are not too many paths presented to a host. Maximum in vSphere 7.0 is 4096 with no more than 32 paths to a single fibre channel LUN and 8 to an iSCSI LUN</p> <p>References:</p> <p>Viewing and managing Paths the <i>vSphere Storage guide for vSphere 7.0</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-B7AD0CA0-CBE2-4DB4-A22C-AD323226A257.html</p>

[vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-98F0851E-12F2-4FB2-A794-7643DD2E6F9B.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-98F0851E-12F2-4FB2-A794-7643DD2E6F9B.html)

Procedure:

Review the steps in the References for details.

Item	Comments
Best Practice ID	ST-008
Recommendation	Verify that there is redundancy in storage paths and components to avoid single points of failure.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Availability, Recoverability
Justification	<p>Configuring multiple paths to storage improves availability and in some cases allows for load balancing. For Fibre Channel storage, redundant fabrics are highly recommended. For NFS or iSCSI, redundant networking connections are recommended.</p> <p>References:</p> <p><i>vSphere Storage</i> guide for vSphere 7.0 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-98F0851E-12F2-4FB2-A794-7643DD2E6F9B.html</p> <p>Procedure:</p> <p>Review the configuration to ensure that there are multiple paths to all datastores.</p>

Item	Comments
Best Practice ID	ST-009
Recommendation	Check that storage LUNs are not overloaded by verifying that the Command Aborts for all datastores is 0.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Performance
Justification	<p>If the Command Aborts value on any datastore is greater than zero, storage is overloaded on the storage device hosting that datastore. The main causes of overloaded storage are:</p> <ul style="list-style-type: none"> • Placing excessive demand on the storage device

- Misconfigured storage

References:

vSphere Storage guide for vSphere 7.0

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html>

Item	Comments
Best Practice ID	ST-012
Recommendation	Size datastores appropriately for the environment.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Recoverability, Manageability, Scalability, Performance
Justification	<p>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 the <i>Configuration Maximums</i> guide for vSphere for details.</p> <p>References:</p> <p><i>Configuration Maximums</i> for vSphere 7.0 https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0</p> <p><i>vSphere Storage</i> guide for vSphere 7.0 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p>
Item	Comments
Best Practice ID	ST-014
Recommendation	Align VMFS partitions.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Performance
Justification	<p>Like other disk-based filesystems, VMFS filesystems suffer a performance penalty when the partition is unaligned. Using the vSphere Web Client to create VMFS partitions avoids this problem because, beginning with ESXi 5.0, it automatically aligns VMFS3, VMFS5, or VMFS6 partitions along the 1MB boundary. If a VMFS3 partition was</p>

created using an earlier version of ESXi that aligned along the 64 KB boundary, and that file system is then upgraded to VMFS5, the partition retains its 64 KB alignment. 1 MB alignment can be obtained by deleting the partition and recreating it.

Before performing an alignment, carefully evaluate the performance impact of the unaligned VMFS partition on your particular workload. The degree of improvement from alignment is highly dependent on workloads and array types.

Check with your storage vendor's recommendations for alignment and the partition starting block setting. If your storage vendor makes no specific recommendation, use a starting block that is a multiple of 8 KB.

Refer to the alignment recommendations from your array vendor for further information.

References:

Partition Alignment section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	ST-015
Recommendation	Verify the queue depth of the HBA and the max outstanding disk requests per virtual machine parameter according to storage vendor best practices.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Storage, Scalability, Performance
Justification	<p>The driver queue depth can be set from some VMkernel drivers. For example, while the default queue depth of a driver may be 32, specifying a larger queue depth might yield higher performance. Setting the max outstanding disk requests per virtual machine parameter can also help equalize disk bandwidth across virtual machines.</p> <p>Be sure to contact the vendor and follow their recommendations.</p> <p>Also, verify that the queue depth is not different for the same LUN for different hosts in the cluster as this can manifest as a performance issue.</p> <p>References:</p> <p>ESXi Storage Considerations section in <i>Performance Best Practices for VMware vSphere 7.0</i></p> <p>https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>

Item	Comments
Best Practice ID	ST-016
Recommendation	Spread I/O loads over the available paths to the storage (across multiple HBAs and storage processors).
Observation	
Priority	OK
Infrastructure Qualities	Storage, Availability, Scalability, Performance
Justification	<p>Even if you are not using a path selection policy that employs load balancing, balance virtual machine workloads over available HBAs and storage processors accordingly. This reduces contention on the storage processors and minimizes the potential of overloading storage. Work with the storage team to develop an optimal storage configuration.</p> <p>References:</p> <p>Hardware Storage Considerations section in <i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>

Item	Comments
Best Practice ID	ST-017
Recommendation	Choose placement of data disks and swap files on LUNs appropriately for virtual machines.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Recoverability, Scalability, Performance, Virtual Machine
Justification	<p>Tiering storage improves cost while maintaining performance requirements. Higher tier storage can be used sparingly in this model based on the requirements of the virtual machine, whereas swap files can be placed on lower tier storage. In addition, swap files do not need to be stored on replicated storage as that can significantly increase bandwidth requirements.</p>

Item	Comments
Best Practice ID	ST-018

Recommendation	Prior to performing a VMware vSphere Storage vMotion operation, verify that there is sufficient bandwidth between the ESXi host running the virtual machine and both source and destination storage.
Observation	
Priority	OK
Infrastructure Qualities	Network, Storage, Performance
Justification	<p>During VMware vSphere Storage vMotion operations, the virtual machine continues to read from and write to the source storage array. At the same time, the virtual disk to be moved is being read from the source storage array and written to the destination storage array.</p> <p>Given insufficient storage bandwidth, a vSphere Storage vMotion operation can fail. With barely sufficient bandwidth, although a vSphere Storage vMotion operation succeeds, its performance can be poor. Therefore leaving some unreserved CPU capacity in a cluster can help vSphere Storage vMotion tasks to get the resources required to fully utilize available network bandwidth. vSphere Storage vMotion can have significantly better performance on VAAI-capable storage arrays.</p> <p>References:</p> <p>VMware vMotion and Storage vMotion section in <i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>

Item	Comments
Best Practice ID	ST-021
Recommendation	To maximize the fairness benefit from SIOC, avoid introducing non-SIOC-aware load on the storage.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Performance
Justification	<p>If SIOC detects an external load (for example, because of a different LUN with shared spindles, or backup), SIOC will disable its fairness enforcement to avoid placing SIOC-aware loads (virtual machines) with a load that does not cooperate in SIOC load balancing. Load sharing reduces performance of virtual machines with or without SIOC. In general, avoid load sharing.</p> <p>References:</p> <p>Storage I/O Resource Allocation section in <i>Performance Best Practices for VMware vSphere 7.0</i></p>

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	ST-023
Recommendation	When booting from SAN, verify that the datastore is masked and zoned to that particular ESXi host and not shared with other hosts.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Storage, Manageability
Justification	<p>This is a VMware Best Practice that prevents the boot device on shared storage from being accidentally or intentionally modified or deleted from other hosts that have access to the device. This also prevents other hosts from accidentally or intentionally booting using a different host's configuration.</p> <p>References:</p> <p><i>vSphere Storage Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p>

Item	Comments
Best Practice ID	ST-024
Recommendation	Keep the IP storage network physically separate from other traffic.
Observation	
Priority	OK
Infrastructure Qualities	Network, Storage, Security, Performance
Justification	<p>Keep the IP storage traffic on a physically separate network will prevent sharing network bandwidth and prevent performance and security problems.</p> <p>References:</p> <p><i>Security Hardening Guide</i> http://www.vmware.com/security/hardening-guides.html</p> <p>Best Practices for iSCSI Storage section of <i>vSphere Storage Guide for vSphere 7.0</i></p>

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-34297ED3-9D62-4869-BB9E-6EDFBEBD2E94.html>

Item	Comments
Best Practice ID	ST-025
Recommendation	Validate and optimize Non-Volatile Memory Express (NVMe) device performance.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Performance

Justification

vSphere 6.5 and beyond support a Non-Volatile Memory Express (NVMe) virtual storage adapter (virtual NVMe, or vNVMe). This allows recent guest operating systems that include a native NVMe driver to use that driver to access storage through ESXi, whether or not ESXi is itself using NVMe storage.

Flash storage on PCIe cards initially used SCSI or SATA interfaces and protocols, often limiting their performance to much less than what the underlying SSD devices were capable of. Some newer PCIe flash devices use the Non-Volatile Memory Express (NVMe) protocol, potentially allowing much higher performance.

NVMe performance considerations:

- NVMe devices are highly parallelized. Their maximum throughput is generally achieved when they are backing multiple virtual disks and/or multiple virtual machines.
- The high throughput of NVMe creates a correspondingly high CPU load. NVMe devices are thus a better fit for hardware configurations with many cores per socket (preferably at least eight) and multiple sockets (preferably at least two). High CPU frequencies are also desirable.
- The virtual storage adapters used by the guest virtual machines should be appropriately chosen. These will typically be either PVSCSI or the new vNVMe virtual adapter.
- Because the vNVMe virtual storage adapter has been designed for extreme low latency flash and non-volatile memory based storage, it is not best suited for highly parallel I/O workloads and slow disk storage. For workloads that primarily have low outstanding I/O, especially latency-sensitive workloads, vNVMe will typically perform quite well. Compared to virtual SATA devices, vNVMe virtual storage adapters access local PCIe SSD devices with significantly lower CPU cost per I/O and significantly higher IOPS.

References:

Performance Best Practices for vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	ST-026
Recommendation	Check ESXi Hosts for storage plugin version and consistency.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Availability, Performance
Justification	<p>All ESXi hosts accessing the same storage LUBs should be configured with a consistent storage plugin (VMware NMP or EMC Power Path) and these versions should be consistent.</p> <p>If there are inconsistencies among ESXi hosts in a DRS cluster it may impact performance and availability and should be changed to be consistent.</p> <p>Procedure:</p> <p>Command <code>esxcli storage core device list</code> will show <code>â€œMultipath Plugin: PowerPathâ€•</code> or <code>â€œMultipath Plugin: NMPâ€•</code> and these values should match across hosts in a cluster.</p>
Item	Comments
Best Practice ID	ST-027
Recommendation	Check for consistent VAAI settings on ESXi Hosts in a cluster.
Observation	
Priority	OK
Infrastructure Qualities	Storage, Performance
Justification	<p>If there are inconsistent settings for VAAI across hosts it can impact the performance. For example, if ten hosts in a cluster have the 3 VAAI settings enabled (set to <code>â€œ1â€•</code>) and another has one, two, or all three settings disabled this is a potential performance inhibitor.</p>

These are enabled by default and generally need to be enabled.

If all ESXi hosts in a cluster have the three settings disabled if the storage array supports VAAI, they should be assessed and enabled on the hosts.

The three settings are:

- DataMover.HardwareAcceleratedMove
- DataMover.HardwareAcceleratedInit
- VMFS3.HardwareAcceleratedLocking

4.1.1.6. Virtual Machines

Item	Comments
Best Practice ID	VM-001
Recommendation	Use NTP, Windows Time Service, or another timekeeping utility for all ESXi Hosts and virtual machines.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Manageability, Virtual Machine
Justification	<p>Time synchronization is important for many reasons, including easier correlation of information for troubleshooting and preventing erratic behavior of time-sensitive applications.</p> <p>For ESXi hosts:</p> <p>Configure each ESXi host to synchronize time with an NTP server.</p> <p>For virtual machines:</p> <p>The VMware Tools's time-synchronization option is a suitable choice. VMware recommends that within any particular virtual machine you use either the VMware Tools time-synchronization option or another timekeeping utility, but not both.</p> <p>References:</p> <p><i>Timekeeping best practices for Linux Guests</i> (1006427) http://kb.vmware.com/kb/1006427</p> <p><i>Timekeeping best practices for Windows including NTP</i> (1318) http://kb.vmware.com/kb/1318</p> <p>Guest Operating System General Considerations section in <i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/</p>

techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf

Item	Comments
Best Practice ID	VM-004
Recommendation	Do not specify CPU affinity rules unless needed.
Observation	
Priority	OK
Infrastructure Qualities	Scalability, Performance, Virtual Machine
Justification	<p>VMware recommends not using CPU affinity as it limits the scheduling options available to the ESXi scheduler. By specifying a CPU affinity setting for each virtual machine, you can restrict the assignment of virtual machines to a subset of the available processors in multiprocessor systems. By using this feature, you can assign each virtual machine to processors in the specified affinity set.</p> <p>CPU affinity specifies virtual machine-to-processor placement constraints and is different from the relationship created by a VM-VM or VM-Host affinity rule, which specifies virtual machine-to-virtual machine host placement constraints.</p> <p>In this context, the term CPU refers to a logical processor on a hyperthreaded system and refers to a core on a non-hyperthreaded system.</p> <p>The CPU affinity setting for a virtual machine applies to all of the virtual CPUs associated with the virtual machine and to all other threads (also known as <i>worlds</i>) associated with the virtual machine. Such virtual machine threads perform processing required for emulating mouse, keyboard, screen, CD-ROM, and miscellaneous legacy devices.</p> <p>In some cases, such as display-intensive workloads, significant communication might occur between the virtual CPUs and these other virtual machine threads. Performance might degrade if the virtual machine's affinity setting prevents these additional threads from being scheduled concurrently with the virtual machine's virtual CPUs. Examples of this include a uniprocessor virtual machine with affinity to a single CPU or a two-way SMP virtual machine with affinity to only two CPUs.</p> <p>For the best performance, when you use manual affinity settings, VMware recommends that you include at least one additional physical CPU in the affinity setting to allow at least one of the virtual machine's threads to be scheduled at the same time as its virtual CPUs. Examples of this include a uniprocessor virtual machine with affinity to at least two CPUs or a two-way SMP virtual machine with affinity to at least three CPUs.</p> <p>References:</p> <p>Using CPU Affinity sections of <i>vSphere Resource Management Guide for vSphere 7.0</i></p>

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-5FCC0AAA-9D58-4EDF-9A5F-8628F1C8B830.html>

Item	Comments
Best Practice ID	VM-008
Recommendation	Verify that the file system partitions within the guest operating system are aligned.
Observation	
Priority	OK
Infrastructure Qualities	Performance, Virtual Machine
Justification	<p>In addition to VMFS alignment with the storage system, align the guest OS file system. To get the best performance from a storage system, the storage blocks on the logical unit number (LUN) must be aligned to the file system on the operating system.</p> <p>Use <code>fdisk</code> for Linux or <code>diskpart</code> for Windows to align the data disks of the virtual machine. The aligned vmdk (or the virtual machine with the aligned disks) can be used as templates so that subsequent virtual machines deployed from these templates have aligned guest OS file systems.</p> <p>References:</p> <p>Partition Alignment section in <i>Performance Best Practices for VMware vSphere 7.0</i></p> <p>https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>
Item	Comments
Best Practice ID	VM-010
Recommendation	Use the default monitor mode chosen by the Virtual Machine Monitor unless it is necessary to change it.
Observation	
Priority	OK
Infrastructure Qualities	Performance, Virtual Machine
Justification	<p>The default monitor mode for each guest OS on each CPU is chosen by the virtual machine monitor and offers the best option for most workloads.</p> <p>If the virtual machine/workload is an exceptional case such that the default monitor mode does not offer the best performance, evaluate the</p>

performance of the application and use case against various execution modes to determine the most suitable option. Do this only for an exceptional case.

The virtual machine monitor modes are:

- Automatic (default and recommended)
- Binary translation (BT) and shadow page tables (swMMU)
- AMD-V or Intel VT-x (HV) and shadow page tables
- AMD-V with RVI, or Intel VT-x with EPT (RVI and EPT are hwMMU)

References:

Item	Comments
Best Practice ID	VM-013
Recommendation	Configure the guest operating system with sufficient swap space.
Observation	
Priority	OK
Infrastructure Qualities	Performance, Virtual Machine
Justification	<p>Allocating insufficient swap space can impact virtual machine performance when the guest OS does not have sufficient swap space. The size of the swap space varies based on the operating system and the amount of memory allocated to the virtual machine. Swap to host cache is a feature in ESXi 5.0 and later that uses a relatively small amount of SSD storage to significantly reduce the performance impact of host-level memory swapping. Using swap to host cache and putting the regular swap file in SSD are two different approaches for improving host swapping performance. Swap to host cache makes the best use of potentially limited SSD space while also being optimized for the large block sizes at which some SSDs work best.</p> <p>A system-wide memory space overhead for the VMkernel and various host agents (such as hostd and vpxa). ESXi allows the use of a system swap file to reduce this memory overhead by up to 1 GB when the host is under memory pressure. This system swap file is different from the per-virtual-machine swap files, which store memory pages from the VMX component of the per-virtual-machine memory space overhead.</p> <p>References:</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>
Item	Comments
Best Practice ID	VM-015

Recommendation	Use paravirtualized SCSI (PVSCSI) with a supported guest OS where additional performance is needed.
Observation	
Priority	NA
Infrastructure Qualities	Performance, Virtual Machine
Justification	<p>PVSCSI can provide performance improvements for I/O intensive guest applications by reducing the host CPU cost per I/O.</p> <p>PVSCSI adapters offer a significant reduction in CPU utilization per I/O as compared to the BusLogic or LSILogic virtual storage adapters, and are the best choice for environments with very I/O-intensive guest applications. For PVSCSI, the virtual machines must be using virtual hardware version 7 or later.</p> <p>References:</p> <p>Guest Operating System Storage Considerations section in <i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>

Item	Comments
Best Practice ID	VM-020
Recommendation	Consider using a 64-bit guest operating system to improve performance, if applicable.
Observation	
Priority	OK
Infrastructure Qualities	Scalability, Performance, Virtual Machine
Justification	<p>Consider using a 64-bit guest OS if you are running 64-bit applications. Do not assume that because an application is a 64-bit application, it runs better than its 32-bit version.</p> <p>Understand the processor requirements for running 64-bit applications. A 64-bit guest OS can offer better performance because a 64-bit operating system offers more registers, large kernel tables, and makes page table operations cheaper, all of which improves performance.</p> <p>A 64-bit guest OS requires more memory overhead than 32-bit guest OS.</p> <p>Note: This is typically only applicable to legacy applications and operating systems, most modern applications and operating systems are 64 bit.</p>

Item	Comments
Best Practice ID	VM-021
Recommendation	Consider setting the memory reservation value for performance-sensitive Java-based virtual machines (JVMs) to the operating system required memory plus the total JVM heap size.
Observation	
Priority	OK
Infrastructure Qualities	Performance, Virtual Machine
Justification	<p>All of the best practices that are used when running Java on physical systems apply equally to virtual machines. Java programs tend to be very intensive in their use of memory.</p> <p>Sizing the Java virtual machine (JVM) with the appropriate resources and confirming that the virtual machine has the appropriate memory reserved can improve the performance of the virtual machine.</p> <p>For performance-sensitive JVMs, consider setting the memory reservation for the virtual machine to the memory required for the operating system plus the total JVM heap size.</p> <p>Review actual virtual machine memory usage and adjust the reservation amount to avoid excessive memory reservation.</p> <p>References:</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>

Item	Comments
Best Practice ID	VM-022
Recommendation	Validate that there are no orphaned or invalid virtual machines in the inventory.
Observation	
Priority	OK
Infrastructure Qualities	Availability, Recoverability, Manageability, Virtual Machine
Justification	<p>Virtual machines that are in the inventory should not be orphaned or invalid. If there are any objects that are in this state, potential causes might include:</p> <ul style="list-style-type: none"> • Can be an indicator of storage connectivity • if a host failover is unsuccessful

- when the virtual machine is unregistered directly on the host

If any are detected, review the virtual machine for configuration errors such as storage connectivity.

References:

VM Troubleshooting for vSphere 7.0

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-BFD8C9BC-30FB-4A92-AFEC-2FC9FF387920.html

Item	Comments
Best Practice ID	VM-023
Recommendation	If virtual machine encryption is used, validate that the ESXi host processors support AES-NI, for improved performance.
Observation	
Priority	NA
Infrastructure Qualities	Security, Performance, Virtual Machine
Justification	<p>Virtual machine encryption, can encrypt disk files (.vmdk), snapshot files (.vmsn), NVRAM files (.nvram), swap files (.vswp), and portions of configuration files (.vmx). Encryption and decryption is performed by the CPU and therefore incurs a CPU cost. When possible, vSphere uses the AES-NI processor instruction set extensions (supported by many recent processors) to reduce that CPU cost.</p> <ul style="list-style-type: none"> • The resource overhead of virtual machine encryption is primarily in CPU utilization. Thus, with sufficient CPU resources, typical deployments (that is, those that do not use ultra-fast storage) will see no significant performance impact. • To significantly minimize additional CPU utilization due to VM encryption, choose processors that support AES-NI, especially some recent processor versions in which the AES-NI implementation is further optimized. • Make sure AES-NI is enabled in BIOS. In some cases a BIOS upgrade might be required for AES-NI support. • Because the encryption takes place on the host, storage devices see only encrypted data. Special features of some storage devices, such as deduplication or compression, might therefore be ineffective or not provide their full benefit. • When virtual machine encryption is used with storage having very low latencies (below about 200 microseconds), the time taken by the CPU to process encryption requests can begin to impact performance. <p>References:</p> <p>Performance Best Practices for vSphere 7.0 https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/</p>

techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf

4.1.1.7. vCenter Server

Item	Comments
Best Practice ID	VC-001
Recommendation	Deploy vCenter Server in compliance with all configuration maximums as documented in the most current vSphere Configuration Maximums document.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Configuration Maximums, Scalability
Justification	<p>VMware software functions within specified operating parameters. When the software is implemented out of compliance with recommended specifications, unpredictable results can occur.</p> <p>References:</p> <p><i>Configuration Maximums vSphere 7.0</i> https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0</p> <p>Procedure:</p> <p>Review applicable configuration maximum settings from the References link.</p>

Item	Comments
Best Practice ID	VC-002
Recommendation	Deploy vCenter Server appliance using an embedded platform services controller.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Availability, Recoverability, Manageability
Justification	<p>The installation and architecture of vCenter Server has been simplified in vSphere 7.0. The installation now is only available in appliance form, using an embedded Platform Services Controller. External services controllers, and Windows based vCenter installations are no longer available. The appliance now supports all components as previous installations:</p>

- VMware vCenter® Single Sign-On
- License Service
- Lookup Service
- VMware Directory Service
- VMware Certificate Authority
- VMware vCenter Server
- VMware vSphere Client
- VMware vSphere Auto Deploy
- VMware vSphere ESXi Dump Collector
- VMware vSphere Syslog Collector (Windows) / VMware Syslog Service (Appliance)

Therefore, when deploying vCenter 7.0, you must understand the implications of this change to properly architect the environment, whether that be a fresh installation, an upgrade or a migration from vCenter Server for Windows.

References:

vSphere Installation and Setup Guide

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-8DC3866D-5087-40A2-8067-1361A2AF95BD.html>

vSphere Upgrade Guide

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.upgrade.doc/GUID-9ED7B32A-019F-4A97-BC58-1A9BF7D16C57.html>

Procedure:

Review the configuration of the environment to make sure it meets business requirements and needs.

Item	Comments
Best Practice ID	VC-003
Recommendation	Use a consistent naming convention for all virtual data center objects.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Manageability
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 Server 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.

Procedure:

Review how objects are named in vCenter Server to validate consistency ensuring that all objects have a purpose and are not ambiguous.

Item	Comments
Best Practice ID	VC-004
Recommendation	Maintain compatible and homogeneous (CPU, memory, and storage when using vSAN) hosts within a cluster to support the required functionality for vSphere vMotion, vSphere DRS, VMware vSphere Distributed Power Management, vSphere HA, and vSphere FT.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Availability, Recoverability, Manageability
Justification	<p>Compatible and homogenous configurations of ESXi within a cluster allow for easier management and assist troubleshooting. Features such as vSphere vMotion, vSphere DRS, VMware vSphere Distributed Power Management, vSphere HA, and vSphere FT have additional requirements and having compatible and homogenous host configuration results in a more predictable performance of the environment.</p> <p>When using vSAN, it helps to ensure an equal component balance between hosts, so a single host does not become a point of failure for a bigger outage in the case of a hardware failure.</p> <p>References:</p> <p><i>vSphere Resource Management Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-98BD5A8A-260A-494F-BAAE-74781F5C4B87.html</p>

vSphere Availability Guide

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-63F459B7-8884-4818-8872-C9753B2E0215.html>

Procedure:

Review host hardware configurations to ensure that hardware is not dramatically different between servers in a cluster.

Item	Comments
Best Practice ID	VC-005
Recommendation	Verify that the number of hosts in a cluster is within limits for the required functionality (HA, vSphere DRS, and vSphere DPM).
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Configuration Maximums, Manageability, Scalability
Justification	<p>The actual allowable limits can vary based on multiple factors, however the maximum cluster size in vSphere 7.0 is 96 hosts. Check the configuration maximums document for the most current information.</p> <p>Verify that the size of the current environment plus future growth is within the specified limits to avoid performance and supportability issues.</p> <p>Combination of different limits can result in different overall limits.</p> <p>References:</p> <p><i>Configuration Maximums for vSphere 7.0</i> https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0</p> <p>Procedure:</p> <p>Review the configurations maximums to ensure maximums do not reduce available functionality of the platform.</p>

Item	Comments
Best Practice ID	VC-006
Recommendation	Verify that vSphere HA settings allow sufficient capacity for vSphere DPM to power down hosts.
Observation	
Priority	NA
Infrastructure Qualities	vCenter Server, Availability, Performance

Justification	<p>In a cluster with vSphere HA enabled, vSphere DRS and vSphere DPM maintain excess powered-on capacity to meet HA settings requirements. The cluster might therefore not allow additional virtual machines to be powered on in all situations. Also, some hosts might not be powered down even though the cluster might appear to be sufficiently idle. Consider these factors when configuring HA.</p> <p>References:</p> <p>VMware Distributed Power Management (DPM) section in <i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p> <p>Review available capacity to validate whether there is enough free capacity to use DPM given a host being powered down.</p>
Item	Comments
Best Practice ID	VC-007
Recommendation	Size VMware HA admission control policy considering the allowed host failures and available resources.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Availability, Recoverability
Justification	<p>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.</p> <p>There are three different admission control policies:</p> <ul style="list-style-type: none"> • The number of host failures that the cluster tolerates policy - In this policy, 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 it 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 policy, 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 be protected due to insufficient resources. • Use Failover hosts - In this policy, hosts are reserved as failover hosts. Sufficient capacity must be available on these

standby hosts so that recovery is possible in the event of a failure.

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*
<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-53F6938C-96E5-4F67-9A6E-479F5A894571.html>

Procedure:

Set the admission control policy by selecting the cluster, and choosing **Configure > vSphere Availability**.

Item	Comments
Best Practice ID	VC-008
Recommendation	Use reservations and limits selectively on clusters and resource pools that require them. Do not set reservations too high or limits too low.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Scalability, Performance
Justification	<p>Setting reservations on cluster resources makes sure that the resources are allocated and available for the virtual machines as long as the host/cluster has the resources available. This reduces the overall shared resources available and can impact consolidation ratios while increasing the need for management of individual virtual machine settings.</p> <p>Setting reservations also impacts slot size calculations for an HA cluster, which uses the Number of Host Failures setting and can result in a conservative admission control policy for the cluster.</p> <p>Limits specify an upper bound for CPU or memory resources. In most cases, it is not necessary to specify limits. Limits can be assigned to manage expectations and to prevent performance degradation as you add more virtual machines.</p> <p>References:</p> <p>Configuring Resource Allocation Settings section in <i>vSphere Resource Management</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resource.management.doc/GUID-53F6938C-96E5-4F67-9A6E-479F5A894571.html</p>

[vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-60077B40-66FF-4625-934A-641703ED7601.html](https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf)

General Resource Management section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Validate the cluster to see if there are resource pools. Select the VMs tab of the cluster to validate if there are any reservations for VMs in the cluster.

Item	Comments
Best Practice ID	VC-009
Recommendation	Verify that hardware meets the optimal configuration required by vCenter Server and add-ons.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Configuration Maximums, Performance
Justification	<p>With vCenter Server 7.0, all services are installed as a part of the Platform Services Controller, or the vCenter Server services installation. For optimal performance, use the following guidelines:</p> <ul style="list-style-type: none"> • vCenter Server 7.0 requires at least two 64-bit CPUs (two cores is also acceptable). For large environments, up to 24 CPUs might be required. • vCenter Server 7.0 requires between 12 and 56 GB of RAM. • vCenter Server 7.0 requires between 415 GB and 3665 GB of disk space depending on the services installed. • 1-Gbps network. <p>These requirements are inclusive of vSphere Lifecycle Manager which is included in the vCenter Server Appliance.</p> <p>References:</p> <p><i>vSphere Installation and Setup guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-752FCA83-1A9B-499E-9C65-D5625351C0B5.html</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p>

Review the vCenter Server hardware specifications and verify that they meet the requirements of the workload running in the environment.

Item	Comments
Best Practice ID	VC-010
Recommendation	Verify that DNS is configured for forward, reverse, short, and long lookups.
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, vCenter Server, Manageability
Justification	<p>As a general practice, set up DNS in your infrastructure to provide name resolution. VMware components require DNS resolution.</p> <p>DNS names should be defined for all ESXi hosts, vCenter Server instances, Platform Services Controller instances, as well as any other infrastructure component. VMware recommends enabling forward and reverse lookups and configuring long (FQDN) and short names in DNS. Manual editing of <code>/etc/hosts</code> is prone to error and is not recommended.</p> <p>After DNS is set up, test by using the <code>nslookup</code> command to verify that DNS is working correctly.</p> <p>References:</p> <p>DNS Requirements for vSphere section in the <i>vSphere Installation and Setup</i> Guide for vSphere 7.0 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-24D34C53-B00E-47B7-92A7-6B0155DF6889.html</p> <p>Procedure:</p> <p>Validate each host name for the environment in DNS. In addition, the following command can be used to test the resolution:</p> <pre>nslookup -nosearch -nodefname FQDN_or_IP_address</pre>

Item	Comments
Best Practice ID	VC-011
Recommendation	Use automatic mode for vSphere DRS, if possible, for optimal load balancing.
Observation	

Priority	OK
Infrastructure Qualities	vCenter Server, Performance
Justification	<p>vSphere DRS continuously 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.</p> <p>Use the automatic mode for vSphere DRS to maintain continuous and proper load balancing.</p> <p>Set the appropriate migration threshold between Conservative and Aggressive (starting with a level 2 or 3), and adjust as necessary.</p> <p>Set the migration threshold to more aggressive levels if the following conditions are satisfied:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>References:</p> <p>DRS Cluster Requirements section in <i>vSphere Resource Management Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-CAF3CDC4-469F-4FA4-ACFD-24F5F36847EA.html</p> <p>Procedure:</p> <p>The cluster DRS settings can be found by selecting the cluster, and then choosing Configure > vSphere DRS.</p>
Item	Comments
Best Practice ID	VC-012
Recommendation	Consider enabling vSphere DPM for clusters in which virtual machine demand varies greatly over time.
Observation	
Priority	NA
Infrastructure Qualities	ESXi Hosts, vCenter Server, Manageability, Performance

Justification

vSphere DPM is most appropriate for clusters in which composite virtual machine demand varies greatly over time. For example, clusters in which overall demand is higher during the day and significantly lower at night. If demand is consistently high relative to overall cluster capacity, vSphere DPM has little opportunity to put hosts into standby mode to save power.

References:

Performance Best Practices for VMware vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Cluster DPM settings can be found by selecting the cluster, and then choosing **Configure > vSphere DRS**.

Item	Comments
Best Practice ID	VC-013
Recommendation	Distribute vSphere FT VMs to multiple hosts, if the feature is in use.
Observation	
Priority	OK
Infrastructure Qualities	Availability, Recoverability, Performance, Virtual Machine
Justification	<p>The majority of vSphere Fault Tolerance (FT) traffic flows from the Primary FT virtual machine to the Secondary FT virtual machine. So, congestion on the NIC used for FT logging can be avoided by distributing FT primaries onto multiple hosts.</p> <p>To increase the bandwidth available for the logging traffic between Primary and Secondary virtual machines, use a 10 Gb NIC and enable jumbo frames.</p> <p>References:</p> <p>Best Practices for Fault Tolerance section in <i>vSphere Availability</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-2A87B967-5BBB-4394-B1E6-EE87D50A2A86.html</p> <p>Procedure:</p> <p>Validate the usage of FT in the environment, and make sure that VMs are distributed, and that 10Gbps networking is in use.</p>
Item	Comments
Best Practice ID	VC-014

Recommendation	Verify that the number of vSphere FT-enabled virtual machines does not saturate the vSphere FT logging network.
Observation	
Priority	NA
Infrastructure Qualities	Availability, Scalability, Performance, Virtual Machine
Justification	<p>In addition to non-fault tolerant virtual machines, have no more than four fault tolerant virtual machines with no more than eight virtual CPUs (primary and secondary) on any single host. The number of fault tolerant virtual machines that you can safely run on each host is based on the sizes and workloads of the ESXi host and virtual machines, all of which can vary.</p> <p>References:</p> <p>Best Practices for Fault Tolerance section in <i>vSphere Availability</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-2A87B967-5BBB-4394-B1E6-EE87D50A2A86.html</p> <p>Procedure:</p> <p>Validate the network utilization of the FT network, as well as that FT VMs are distributed amongst the hosts.</p>

Item	Comments
Best Practice ID	VC-015
Recommendation	Verify that the hosts on which the primary and secondary FT-enabled virtual machines run are relatively closely matched (CPU make, model, frequency, and version/build/patches).
Observation	
Priority	OK
Infrastructure Qualities	ESXi Hosts, Availability, Recoverability, Performance
Justification	<p>Homogenous Clusters are recommended when using vSphere FT. When constructing your cluster, verify that all hosts have the following:</p> <ul style="list-style-type: none"> Processors from the same compatible processor group Common access to datastores used by the virtual machines The same virtual machine network configuration The same ESXi version The same vSphere Fault Tolerance version number The same BIOS settings (power management and hyperthreading) for all hosts <p>References:</p>

Best Practices for Fault Tolerance section in *vSphere Availability*
<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-2A87B967-5BBB-4394-B1E6-EE87D50A2A86.html>

Procedure:

Review the hardware configuration for the hosts to make sure that each of the requirements for FT are met.

Item	Comments
Best Practice ID	VC-016
Recommendation	Verify that power management settings (BIOS, ESX) that cause CPU scaling are consistent on hosts running primary and secondary FT-enabled virtual machines.
Observation	
Priority	NA
Infrastructure Qualities	ESXi Hosts, Availability, Recoverability, Performance
Justification	<p>Hosts running the primary and secondary virtual machines should operate at approximately the same processor frequencies, otherwise the secondary virtual machine might be restarted more frequently. Platform power management features that do not adjust based on workload (for example, power capping and enforced low frequency modes to save power) can cause processor frequencies to vary greatly. If secondary virtual machines are being restarted on a regular basis, disable all power management modes on the hosts running fault tolerant virtual machines or verify that all hosts are running in the same power management modes.</p> <p>Apply the same instruction set extension configuration (enabled or disabled) to all hosts. The process for enabling or disabling instruction sets varies among BIOSes. See the documentation for your hosts' BIOSes about how to configure instruction sets.</p> <p>References:</p> <p>Best Practices for Fault Tolerance section in the <i>vSphere Availability Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-2A87B967-5BBB-4394-B1E6-EE87D50A2A86.html</p> <p>Procedure:</p> <p>Procedures vary, but typically are found in the host BIOS settings.</p>
Item	Comments
Best Practice ID	VC-017

Recommendation	Avoid making resource pools and virtual machines siblings in a hierarchy to avoid unexpected performance.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Manageability, Performance
Justification	<p>Resource pools help to improve manageability, grouping, and partitioning of CPU and memory resources. VMware recommends, however, that resource pools be used sparingly to avoid over-complication of the configuration and to allow the greatest flexibility for resources to be balanced with vSphere vMotion and vSphere DRS or failed over with vSphere HA.</p> <p>References:</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p> <p>Review the cluster to see if Resource Pools are in use and limit the usage as appropriate.</p>

Item	Comments
Best Practice ID	VC-018
Recommendation	Configure the vCenter Server statistics to a level appropriate for use. VMware recommends level 1 or 2.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Performance
Justification	<p>vCenter Server statistics levels:</p> <ol style="list-style-type: none"> 1. vCenter Server statistics level 1 includes the basic metrics but does not include statistics for devices. 2. vCenter Server statistics level 2 includes all the metrics including statistics for devices. 3. vCenter Server statistics level 3 includes all the metrics and all of the counter groups. 4. vCenter Server statistics level 4 includes all the metrics supported by vCenter Server. <p>vCenter Server performs basic statistics operations of insert, roll up, and purge. Higher statistics levels require that more work be performed</p>

by the vCenter Server for these operations, which can impact the performance of the vCenter Server database.

Higher statistics levels also increase the size of the vCenter Server database. Use the database sizing estimator when changing the statistics level so that you have adequate space in the vCenter Server database.

VMware recommends that the vCenter Server statistics level be kept at level 1 or 2.

References:

VMware vCenter Database Considerations section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Review the statistics collection interval by selecting the vCenter Server, and then **Configure > General**.

Item	Comments
Best Practice ID	VC-019
Recommendation	vSphere Auto Deploy HA configuration practices.
Observation	
Priority	NA
Infrastructure Qualities	vCenter Server, Manageability
Justification	<p>vSphere Auto Deploy supports <i>stateless</i> (also known as <i>diskless</i>), <i>stateless caching</i> and <i>stateful install</i> configurations.</p> <p>vSphere Auto Deploy is now installed as a part of the vCenter Server installation and therefore no configuration of an external server is required at this time.</p> <p>Run vCenter Server in a vSphere HA enabled cluster and configure the virtual machine with a vSphere HA restart priority of high. Include two or more hosts in the cluster that are not managed by vSphere Auto Deploy and pin the vCenter Server virtual machine to these hosts by using a rule (vSphere HA DRS required VM to host rule). You can set up the rule and then disable DRS if you do not want to use DRS in the cluster. The greater the number of hosts that are not managed by vSphere Auto Deploy, the greater your resilience to host failures.</p> <p>This approach is not suitable if Auto Start Manager is used because Auto Start Manager is not supported in a cluster-enabled vSphere HA environment.</p> <p>References:</p> <p>vSphere Auto Deploy and vSphere HA Best Practices section of the <i>vSphere Installation and Setup Guide for vSphere 7.0</i></p>

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-980D9E38-633E-4557-9144-AC422FA239C5.html>

Procedure:

Review the Auto-Deploy configuration for compliance with best practices.

Item	Comments
Best Practice ID	VC-020
Recommendation	Tasks and Events Retention Policy set in the environment.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Manageability, Scalability, Performance
Justification	<p>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 is executed through vCenter Server, it is stored in the database. For example, a task is created when a user powers on or off a virtual machine, or an event where something occurs, such as vCPU usage for a VM changing to red.</p> <p>Tasks and event data is stored indefinitely in the vCenter Server database. This can cause substantial growth of the database in large environments.</p> <p>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.</p> <p>In comparison to statistical data, these tables consume a relevantly small amount of database space. However, it is good practice to consider this option to further reduce the consumed space in the database.</p> <p>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.</p> <p>References:</p> <p><i>Retention of Events in the vCenter Server Database</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-F51002AE-6DA3-4161-B587-16CD6B94AEAC.html</p> <p>Procedure:</p>

From the vCenter Server **Configure > Settings** page, the retention policy can be set.

Item	Comments
Best Practice ID	VC-022
Recommendation	Validate that the supported scale for vCenter Server configuration is not exceeded.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Configuration Maximums, Manageability, Scalability
Justification	When designing the vCenter Server Architecture, one of the design considerations is Enhanced Linked Mode. This feature allows a single pane of glass showing the entire environment in many cases. There are scale limitations to this feature. Exceeding the scale numbers can produce unpredictable behavior and poor performance.

With vCenter Server 7.0, the supported sizing is as follows:

- Maximum of 15 vCenter Server instances, linked per Single Sign-On domain
- Maximum of 15,000 hosts in Linked vCenter Servers
- Maximum of 135,000 powered on virtual machines in the linked vCenter Server configuration
- Maximum of 150,000 registered virtual machines in the linked vCenter Server configuration

References:

Configuration Maximums for vSphere 7.0

<https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0>

Procedure:

Review the maximums for the different configurations to make sure that they do not exceed the thresholds.

Item	Comments
Best Practice ID	VC-023
Recommendation	Validate storage requirements are met for the vCenter Server Appliance Database.
Observation	

Priority	OK
Infrastructure Qualities	vCenter Server, Performance
Justification	<p>For best performance of the vCenter Database, follow these storage recommendations:</p> <ul style="list-style-type: none"> • If the vCenter appliance is placed on thin-provisioned or lazy-zeroed thick-provisioned storage, vCenter startup might be slower than it would be if placed on eager-zeroed thick-provisioned storage. • Large deployments can rapidly generate significant amounts of data. It's good practice to periodically monitor the database storage to avoid running out of storage space. For information about setting an alert for this in a vCenter Server Appliance, see VMware KB article 2058187. <p>References:</p> <p><i>vSphere 7.0 Performance Best Practices</i></p> <p>https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p><i>Monitor vCenter Server Appliance database disk usage (2058187)</i></p> <p>https://kb.vmware.com/s/article/2058187</p> <p>Procedure:</p> <p>Follow the instructions in the References.</p>
Item	Comments
Best Practice ID	VC-024
Recommendation	Follow vPostgress best practices when maintaining the vCenter Server Database.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Performance
Justification	<p>vCenter Server uses a PostgreSQL (vPostgres) database. Though many database optimizations are done automatically, the following can improve vCenter Server performance:</p> <ul style="list-style-type: none"> • The vCenter Server Appliance creates multiple virtual disks. For improved performance in large scale environments, make sure that the database virtual disk (/storage/db) and the virtual disks

- related to logs, statistics, events, and alarms (/storage/dblog, and /storage/seat) are all backed by different physical disks.
- The /storage/dblog virtual disk stores the database transaction log. While the performance of each partition is important to vCenter performance, vCenter is particularly sensitive to the latency and throughput of this partition. We thus recommend placing this partition on low latency, high throughput storage. VMware KB article [2126276](#), though primarily addressing resizing of virtual disks, also includes a table showing which VMDK corresponds to each mount point.
 - Though PostgreSQL does its own data caching, data is also cached at the operating system level. Performance can be improved by increasing the size of the OS-level cache. This can be accomplished by increasing the amount of memory allocated to the vCenter Server Appliance virtual machine; a portion of this additional memory will be automatically used for the OS-level data cache.
 - PostgreSQL periodically sets checkpoints to guarantee that preceding transactions have been flushed to disk. These checkpoints are triggered every time database writes cumulatively approach 90% of the size of the /storage/dblog/ partition. Increasing the size of this partition beyond its default size of 5GB therefore increases the time between checkpoints. This reduces the overall I/O load on the system, especially for large vCenter deployments, but increases recovery time after a crash. For information about changing the size of the /storage/dblog/ partition, see VMware KB article [2126276](#).
 - In order to avoid having the vCenter Server Appliance database run out of disk space, you can set alarms using the vpxd.vdb.space.errorPercent and vpxd.vdb.space.warningPercent parameters under the advanced vCenter Server settings. In addition to displaying warnings in the vSphere Client, these alarms can also be configured to send email notifications.
 - A vCenter Server plug-in, pgtop, can be used to monitor the PostgreSQL database and can help diagnose performance issues.

References:

vSphere 7.0 Performance Best Practices

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Increasing the disk space for the VMware vCenter Server Appliance in vSphere 6.0 (2126276)

<https://kb.vmware.com/s/article/2126276>

Procedure:

Follow the recommendations in the Justification and Reference KB articles. This may involve movement of disks to other volumes or increasing the size of the disks.

Item	Comments
Best Practice ID	VC-025
Recommendation	vSphere HA should be enabled on all clusters.
Observation	
Priority	OK
Infrastructure Qualities	vCenter Server, Availability
Justification	vSphere HA provides for hardware failure detection for VMs, and dramatically helps with availability of resources. It is Best Practice to have it enabled and configured to monitor the environment.

4.2 Fallas

4.2.1 172.16.63.37

4.2.1.1. ESXi Host

Item	Comments
Best Practice ID	ESXI-002
Recommendation	Verify that all hardware in the system is on the VMware Compatibility Guide for ESXi.
Observation	<p>https://www.vmware.com/resources/compatibility/search.php?deviceCategory=server&details=1&partner=41&cpuSeries=116&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc</p> <p>Based on VMware's compatibility matrix the ProLiant DL580 Gen9 server hardware supports or is compatible only up to the ESXi 7.0 U3 hypervisor version</p>
Priority	P3
Infrastructure Qualities	ESXi Hosts, HCL, Manageability, Scalability
Justification	It is important to use hardware in the <i>VMware Compatibility Guide</i> to be supported by VMware.

Check the online *VMware Compatibility Guide* for systems, I/O devices, operating systems, and storage arrays for compatibility with VMware products.

References:

VMware Compatibility Guide

<https://www.vmware.com/resources/compatibility/search.php>

Procedure:

Review the VMware Compatibility guide versus the hardware bill of materials for any hardware which is not supported.

Item	Comments
Best Practice ID	ESXI-005
Recommendation	Avoid unnecessary changes to advanced parameter settings.
Observation	1 cluster(s) have host advanced parameter settings configured inconsistently across ESX hosts.
Priority	P2
Infrastructure Qualities	ESXi Hosts, Manageability
Justification	<p>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.</p> <p>References:</p> <p><i>Configuring Advanced options for ESXi (1038578)</i> http://kb.vmware.com/kb/1038578</p> <p>Procedure:</p> <p>Review the advanced parameters by using HealthAnalyzer output (Recommended) or by manually following procedure:</p> <ol style="list-style-type: none"> 1. Login to the vSphere Client and select a host. 2. Select Configure > System > Advanced System Settings. 3. Review the settings between hosts for differences.

Item	Comments
Best Practice ID	ESXI-008
Recommendation	Place host devices in a consistent order and location.
Observation	1 cluster(s) have host NIC(s) configured inconsistently across ESX hosts.
Priority	P1

Infrastructure Qualities	ESXi Hosts, Manageability, Scalability
Justification	<p>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.</p> <p>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.</p> <p>References:</p> <p>vSphere Installation and Setup Guide: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-93D0227B-E5ED-40B0-B8E2-71141A32EB00.html</p> <p>Procedure:</p>

Item	Comments
Best Practice ID	ESXI-009
Recommendation	Use persistent and remote syslog logging to improve manageability.
Observation	Remote syslog logging is configured but not enabled for 2 host(s).
Priority	P1
Infrastructure Qualities	ESXi Hosts, Recoverability, Manageability
Justification	<p>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.</p> <p>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.</p> <p>VMware vRealize Log Insight has been developed for this log aggregation and analysis.</p> <p>References:</p> <p><i>Configure Syslog on ESXi Hosts</i> section of the <i>vSphere Monitoring Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-93D0227B-E5ED-40B0-B8E2-71141A32EB00.html</p>

[vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html](https://www.vmware.com/security/hardening-guides.html)

ESXi tab in the VMware Security Hardening Guides
<http://www.vmware.com/security/hardening-guides.html>

Procedure:

From the vSphere Client:

1. In the vSphere Web Client inventory, select the host.
2. Click **Configure**.
3. Under System, click **Advanced System Settings**.
4. Filter for syslog.
5. To set up logging globally, select the setting to change and click **Edit**.
6. Typically the setting that would need to be changed is the Syslog.global.LogHost setting however the size, rotation, log directory, and unique name settings can also be changed.
7. Click **OK**.

From PowerCLI:

- The `esxcli system syslog` command can be used to modify all the syslog settings.

Item	Comments
Best Practice ID	ESXI-010
Recommendation	Disconnect or disable unused or unnecessary physical hardware devices (COM and LPT ports, USB and storage controllers, CD/DVD/floppy drives, and NICs).
Observation	
Priority	P3
Infrastructure Qualities	ESXi Hosts, Security, Manageability, Performance
Justification	<p>To improve overall performance, disconnect or disable unused or unnecessary physical hardware devices such as:</p> <ul style="list-style-type: none"> • COM ports • LPT ports • USB controllers • Floppy drivers • Optical drives (that is, CD or DVD drives) • Network interfaces • Storage controllers

Disabling hardware devices (typically done in BIOS) can free interrupt resources. Also, devices such as USB controllers operate on a polling scheme that consumes extra CPU resources. Some PCI devices reserve blocks of memory, making more memory unavailable to ESXi.

References:

ESXi tab in the VMware Security Hardening Guides

<http://www.vmware.com/security/hardening-guides.html>

Performance Best Practices for VMware vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Procedure:

Review the host configuration, and disable any devices which are not used from the BIOS.

Item	Comments
Best Practice ID	ESXI-021
Recommendation	Check the active Swap in rate of virtual machines to verify that it is not greater than 0 at any point in the measurement period.
Observation	
Priority	P3
Infrastructure Qualities	Scalability, Performance, Virtual Machine
Justification	<p>Excessive memory demand can cause performance problems for one or more virtual machines on an ESXi host. If ESXi actively swaps memory of a virtual machine from disk, the performance of that virtual machine degrades. The overhead of swapping a virtual machine's memory from disk can also degrade the performance of other virtual machines.</p> <p>If the host is actively swapping virtual machine memory, look at the measurements for all virtual machines to determine the affected virtual machines that have values greater than 0.</p> <p>The following are possible solutions to the problem:</p> <ul style="list-style-type: none"> • Reduce the level of memory over-commit. • Enable the balloon driver in all virtual machines. • Reduce memory reservations. • Use resource controls to dedicate memory to critical virtual machines. <p>References:</p> <p><i>vSphere 7.0 monitoring guide</i></p> <p>https://docs.vmware.com/en/VMware-</p>

[vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-115861E6-810A-43BB-8CDB-EE99CF8F3250.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-115861E6-810A-43BB-8CDB-EE99CF8F3250.html)

Procedure:

Check the Swap In Rate for the hostname object in the Performance: Memory chart on vCenter Server. If this measurement is greater than 0 then the host is actively swapping virtual machine memory.

Item	Comments
Best Practice ID	ESXI-022
Recommendation	Use Host Profiles to ensure a consistent configuration across ESXi hosts.
Observation	
Priority	P3
Infrastructure Qualities	ESXi Hosts, Manageability
Justification	<p>Host Profiles provide an automated and centrally-managed mechanism for host configuration and configuration compliance. Host Profiles can improve efficiency by reducing reliance upon repetitive, manual tasks. Host Profiles capture the configuration of a pre-configured and validated reference host, store the configuration as a managed object and use the catalog of parameters contained within to configure networking, storage, security and other host-level parameters.</p> <p>By configuring and using them the ESXi host configuration can be managed for consistency of the configuration.</p> <p>References:</p> <p>vSphere Host Profiles Guide https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.hostprofiles.doc/GUID-78BB234A-D735-4356-9CCF-19DD55DB8060.html</p> <p>Procedure:</p> <p>To validate whether Host profiles are in use:</p> <ol style="list-style-type: none"> 1. Navigate from the vSphere client to Menu > Policies and Profiles. 2. Click Host Profiles. <p>If there are no profiles here, than they are not in use.</p>

4.2.1.2. Network

Item	Comments
Best Practice ID	NE-001

Recommendation	Deploy networking in compliance with all configuration maximums as documented in the most current vSphere Configuration Maximums document.
Observation	2 standard switch(es) have number of port groups that does not comply with VMware defined limit.
Priority	P1
Infrastructure Qualities	Network, Configuration Maximums, Scalability
Justification	<p>VMware software functions within specified operating parameters. If the software is implemented out of compliance with recommended parameters, unpredictable results can occur.</p> <p>References:</p> <p><i>Configuration Maximums for vSphere 7.0</i> https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0</p> <p>Procedure:</p> <p>Review the networking section of the Configuration maximum guide for details on maximums that should not be exceeded.</p>

Item	Comments
Best Practice ID	NE-002
Recommendation	Configure networking consistently across all hosts in a cluster.
Observation	1 cluster(s) have inconsistently configured distributed switches across ESX hosts.
Priority	P1
Infrastructure Qualities	ESXi Hosts, Network, Recoverability, Manageability
Justification	<p>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 vSphere 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.</p> <p>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.</p> <p>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.</p>

References:

vSphere Networking Guide

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-B57FBE96-21EA-401C-BAA6-BDE88108E4BB.html>

Security Hardening Guides

<http://www.vmware.com/security/hardening-guides.html>

Procedure:

Review the networking configuration for consistency between hosts.

Item	Comments
Best Practice ID	NE-005
Recommendation	If the physical switches that support PortFast (or equivalent), enable it on the physical switches that connect to the host.
Observation	
Priority	P3
Infrastructure Qualities	Network, Recoverability, Manageability
Justification	<p>PortFast (or equivalent) allows a port to avoid participating in the Spanning Tree Protocol (STP) listen and learn cycle. As a part of STP, the port is not brought up immediately, which allows the switch to ensure that there are no loops in the network. Services such as HA can be impacted by STP because the timeout by default is less than the amount of time that it takes for the listen and learn cycle.</p> <p>Due to the integration of the ESXi Server into the physical network, the physical network adaptors must have STP disabled or PortFast configured for external switches. This is because VMware virtual switches do not support STP (spanning tree protocol). Virtual switch uplinks do not create loops within the physical switch network. If these are not set, potential performance and connectivity issues might arise.</p> <p>To avoid HA isolation issues, enable PortFast (or equivalent) on the physical switches that connect to the host. After a reboot, sometimes the rebooted node is unable to join the vSphere HA cluster. The issue is that PortFast blocks outgoing traffic during STP listen and learn phases, and by the time traffic is enabled, vSphere HA might have given up waiting to hear from its peers, so it assumes it is alone (isolated). To avoid isolation issues, enable PortFast or equivalent on your physical network switches to prevent spanning tree isolations.</p> <p>References:</p> <p><i>vSphere Networking Guide</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-4D97C749-1FFD-403D-B2AE-0CD0F1C70E2B.html</p>

STP may cause temporary loss of network connectivity when a failover or failback occurs (1003804)

<https://kb.vmware.com/kb/1003804>

vSphere Security Hardening Guides

<http://www.vmware.com/security/hardening-guides.html>

Procedure:

Have the physical network team validate the configuration of the physical network.

Item	Comments
Best Practice ID	NE-006
Recommendation	Distribute vmnics for a port group across different PCI buses for greater redundancy.
Observation	2 ESX host(s) have one or more port groups with physical NICs that share the same PCI bus.
Priority	P2
Infrastructure Qualities	ESXi Hosts, Network, Recoverability, Manageability
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.
	<p>Note: If you are using a converged system such as a Cisco UCS, or the like, disregard this practice, as there is no physical PCI bus, and redundancy is taken care of by the platform itself.</p> <p>References:</p> <p>Procedure:</p> <p>When building the ESXi host configure ensure that NICs are distributed across busses appropriately.</p>

Item	Comments
Best Practice ID	NE-007
Recommendation	Configure networks so that there is separation of traffic (physical or logical using VLANs).
Observation	2 host(s) have standard port groups which use a network that is not dedicated to a single type of traffic.
Priority	P1

Infrastructure Qualities	Network, Security, Manageability
Justification	<p>Separate the following traffic where appropriate:</p> <ul style="list-style-type: none"> • Management • IP storage • vSphere vMotion • Fault Tolerance Logging • Virtual machine • VMware vSAN • Provisioning • VMware vSphere Replication <p>Traffic separation improves performance, prevents bottlenecks, and increases security.</p> <p>Use physical separation or logical separation using VLANs as appropriate. Configure the physical switch ports as trunk ports for VLANs.</p> <p>References:</p> <p><i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>Procedure:</p> <p>Review the network configuration to validate whether traffic is sharing the same network or whether it has been separated.</p>
Item	Comments
Best Practice ID	NE-017
Recommendation	Configure NICs, physical switch speed, and duplex settings consistently.
Observation	2 host(s) have Gigabit and above NICs that does not support auto-negotiate.
Priority	P3
Infrastructure Qualities	Network, Performance
Justification	<p>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 and above links, network settings should be set to auto-negotiate and not forced.</p>

You can set network adapter speed and duplex settings from the VMware vSphere Web Client, but a reboot is required for changes to take effect.

Note: The findings here can present false positives. Cisco UCS virtual NICs and IBM Server vUSB NICs for example, will sometimes be flagged here but the setting cannot be changed in ESXi or the blade management software. Hardware like this should be ignored, as this is not configurable and is handled outside of the control of ESXi.

References:

Solutions for Poor Network Performance section of *vSphere Monitoring and Performance vSphere 7.0*

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-C4EA86FD-95CB-4DE7-A9E3-63F6BFC1A268.html>

Procedure:

Review the network configuration of the cluster to validate that speed and duplex settings are correct.

Item	Comments
Best Practice ID	NE-024
Recommendation	Use Distributed Virtual Port Groups to apply policies to traffic flow types and to provide Rx (receive) bandwidth controls through the use of Traffic Shaping.
Observation	Outgoing traffic shaping is not enabled on 1 distributed virtual switches. Incoming traffic shaping is not enabled on 1 distributed virtual switches.
Priority	P1
Infrastructure Qualities	Network, Scalability, Performance
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 vSphere vMotion operation initiated on different vSphere hosts converge to the same destination vSphere server.
	<p>References:</p> <p><i>Network I/O Control Section of the vSphere Network Guide</i></p> <p>https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-ADEA0213-C969-43E4-B1F4-66D4A916EBDF.html</p> <p>Procedure:</p> <p>Review the Network I/O Control setting for the receive bandwidth to ensure traffic shaping is configured correctly.</p>

4.2.1.3. Security

Item	Comments
Best Practice ID	SEC-014
Recommendation	Use vCenter Server roles, groups, and permissions to provide appropriate access and authorization to the virtual infrastructure. Avoid using AD built-in groups such as the Domain Admins group.
Observation	2 default users/group(s) VMWARE.AEROCIVIL.GOV.COAdministrator are being used at the root/parent level in vCenter. 1 default users/group(s) VMWARE.AEROCIVIL.GOV.COAdministrators are being used at the root/parent level in vCenter.
Priority	P3
Infrastructure Qualities	vCenter Server, Security
Justification	<p>By default, the administrator access is defined as a part of the vCenter Server 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 to the infrastructure, if a dedicated group or user is not created.</p> <p>References:</p> <p>vSphere Users and Permissions section of the <i>vSphere Security Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-3B78EEB3-23E2-4CEB-9FBD-E432B606011A.html</p>
Item	Comments
Best Practice ID	SEC-015
Recommendation	Use Active Directory for local user authentication to ESXi Hosts.
Observation	
Priority	P3
Infrastructure Qualities	ESXi Hosts, Security, Manageability
Justification	<p>If console access to the ESXi host is required, VMware recommends configuring Active Directory authentication for security. This improves auditability and administrative separation in environments.</p> <p>References:</p> <p>VMware <i>vSphere Security Hardening Guide</i> http://www.vmware.com/security/hardening-guides.html</p>

Item	Comments
Best Practice ID	SEC-021
Recommendation	Limit sharing console connections if there are security concerns.
Observation	31 VM(s) have RemoteDisplay.maxConnections set to a value greater than 1. 109 VM(s) have not configured RemoteDisplay.maxConnections value.
Priority	P2
Infrastructure Qualities	Security, Virtual Machine
Justification	<p>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.</p> <p>References:</p> <p>VMware Security Hardening Guides http://www.vmware.com/security/hardening-guides.html</p>

Item	Comments
Best Practice ID	SEC-023
Recommendation	VMware Certificate Authority should be configured as a subordinate CA in the environment for additional security.
Observation	
Priority	P3
Infrastructure Qualities	ESXi Hosts, vCenter Server, Security
Justification	<p>VMware uses the VMware Certificate Authority for providing signed certificates for the environment. By default, it uses a self-signed root certificate and acts as a standalone certificate authority (CA) for the vSphere environment.</p> <p>For an added level of security, it can be configured as a subordinate CA from your corporate CA Server to issue signed certificates.</p> <p>References:</p>

vSphere PSC Guide for vSphere 7.0

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.authentication.doc/GUID-779A011D-B2DD-49BE-B0B9-6D73ECF99864.html>

4.2.1.4. Storage

Item	Comments
Best Practice ID	ST-010
Recommendation	Verify that Physical Device Read/Write Latency average is less than approximately 10 ms and peak is less than approximately 20 ms for all virtual disks.
Observation	
Priority	P3
Infrastructure Qualities	Storage, Performance
Justification	<p>If the peak is more than approximately 20 ms, storage might be slow or overloaded on that virtual disk. Actual latency values depend on the storage workload and the capabilities of the storage subsystems.</p> <p>Contact the array vendor for further information on appropriate storage latency.</p> <p>References:</p> <p><i>vSphere Storage Guide for 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p>
Item	Comments
Best Practice ID	ST-011
Recommendation	Allocate space on shared datastores for templates and media/ISOs separately from datastores for virtual machines.
Observation	2 datastore(s) have both VMs and Templates.
Priority	P2
Infrastructure Qualities	Storage, Manageability, Scalability, Virtual Machine
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.

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.

Note: Although, it is still recommended to separate these files, if there is only ever going to be a single datastore (such as in a vSAN environment), this recommendation can be ignored.

Item	Comments
Best Practice ID	ST-013
Recommendation	Configure NFS and iSCSI storage traffic for performance and security.
Observation	2 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	Storage, Security, Performance
Justification	<p>Storage traffic is potentially the most important of all for Virtual Machine performance. When configuring the network for storage traffic, it should:</p> <ul style="list-style-type: none"> • 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 <p>References:</p> <p><i>vSphere Storage Guide for vSphere 7.0</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-8AE88758-20C1-4873-99C7-181EF9ACFA70.html</p>

Item	Comments
Best Practice ID	ST-019
Recommendation	Consider scheduling vSphere Storage vMotion operations during times of low storage activity, when available storage bandwidth is highest and when the workload in the virtual machine being moved is least active.
Observation	
Priority	P3
Infrastructure Qualities	Storage, Availability, Performance

Justification This arrangement improves chances that vSphere Storage vMotion operations will succeed with the highest performance.

References:

VMware vMotion and Storage vMotion section in *Performance Best Practices for VMware vSphere 7.0*
<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	ST-020
Recommendation	Use Storage I/O Control (SIOC) to prioritize high importance traffic, such as virtual machine traffic.
Observation	8 datastore(s) do(es) not have Storage I/O Control enabled.
Priority	P2
Infrastructure Qualities	Storage, Performance
Justification	<p>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.</p> <p>References:</p> <p>Storage I/O Resource Allocation section in <i>Performance Best Practices for VMware vSphere 7.0</i> https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>
Item	Comments
Best Practice ID	ST-022
Recommendation	Optimize storage utilization through the datastore cluster and VMware vSphere Storage DRS features.
Observation	
Priority	P3
Infrastructure Qualities	Storage, Scalability, Performance

Justification

While grouping, choose datastores that are as homogeneous as possible in terms of host interface protocol (that is, FCP, iSCSI, NFS), RAID level, and performance characteristics. VMware recommends not mixing SSD and hard disks in the same datastore cluster.

Do not configure a datastore cluster with more datastores or virtual disks than the maximum allowed in the *Configuration Maximums for vSphere webpage*.

If a datastore cluster contains thin-provisioned LUNs, make sure those LUNs do not run low on disk space.

Enhance vSphere Storage DRS flexibility in I/O load balancing (potentially increasing performance) by overriding the default intra-VM affinity rule.

References:

VMware Storage Distributed Resource Scheduler (Storage DRS) section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Configuration Maximums for VMware vSphere 7.0

<https://configmax.vmware.com/guest?vmwareproduct=vSphere&release=vSphere%207.0&categories=1-0>

4.2.1.5. Virtual Machines

Item	Comments
Best Practice ID	VM-002
Recommendation	Use the correct virtual SCSI hardware for the operating system.
Observation	2 VM(s) have SCSI controllers which differ from the default SCSI controller for their guest OS.
Priority	P3
Infrastructure Qualities	Manageability, Performance, Virtual Machine
Justification	<p>Selecting incorrect virtual SCSI hardware can prevent the virtual machine from properly booting or impact the performance of the virtual machine. Check the <i>Guest Operating System Installation Guide</i> for the correct virtual SCSI hardware that is supported.</p> <p>vCenter Server automatically selects the default SCSI adapter that is supported for the guest OS of the virtual machine. In general:</p> <ul style="list-style-type: none"> • • LSI Logic SAS and VMware Paravirtual SCSI are available for virtual machines with ESXi 4.x and later compatibility. • AHCI SATA is available only for virtual machines with ESXi 5.5 and later compatibility.

- NVMe is available only for virtual machines with ESXi 6.5 and later compatibility.
- BusLogic Parallel controllers do not support virtual machines with disks larger than 2TB.
- Disks on VMware Paravirtual SCSI controllers might not experience optimal performance gains if they have snapshots or if the host's memory is overcommitted.

Note: Virtual appliances such as the vCenter Appliances, vRealize Appliances, or NSX Appliances, amongst other third party appliances, should be ignored from this recommendation. Appliances have the supported configuration as set by their vendor, and therefore should not have their hardware updated even if detected by this recommendation.

References:

SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-5872D173-A076-42FE-8D0B-9DB0EB0E7362.html

Configuring disks to use VMware Paravirtual SCSI (PVSCSI) adapters (1010398)

<http://kb.vmware.com/kb/1010398>

Guest Operating System Installation Guide

<http://partnerweb.vmware.com/GOSIG/home.html>

Item	Comments
Best Practice ID	VM-003
Recommendation	Verify that virtual machines meet the requirements for vSphere vMotion.
Observation	5 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).
Priority	P2
Infrastructure Qualities	Recoverability, Manageability, Virtual Machine
Justification	<p>To facilitate vSphere vMotion operations of virtual machines between hosts the following requirements must be met:</p> <ul style="list-style-type: none"> • 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 network interfaces will also need to be

migrated. This could impact connectivity if the 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 that prevent vSphere vMotion (CDROM, floppy, serial/parallel devices) are attached.

Prior to bringing an ESXi host into production, testing vSphere vMotion is recommended. Note that ISO files that are accessible on shared storage across ESXi hosts will not show a compatibility warning.

References:

VMware vMotion Best Practices in the VMware vMotion section of *Performance Best Practices guide for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	VM-005
Recommendation	Use the latest version of VMXNET that is supported by the guest operating system.
Observation	37 VM(s) are not using VMXNET3 even though their configuration and guest OS support it.
Priority	P2
Infrastructure Qualities	Network, Manageability, Performance, Virtual Machine
Justification	<p>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.</p> <p>If VMXNET3 is not supported by the guest OS, use Enhanced VMXNET (VMXNET2).</p> <p>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.</p> <p>Refer to information in the Knowledge Base article and product documentation for supported guest operating systems for the particular adapter.</p> <p>References:</p>

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 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	VM-006
Recommendation	Select the correct guest operating system type in the virtual machine configuration to match the guest operating system.
Observation	3 VM(s) have an installed OS that differs from the configured type.
Priority	P3
Infrastructure Qualities	Manageability, Scalability, Performance, Virtual Machine
Justification	<p>Selecting the guest operating system type determines the following:</p> <ul style="list-style-type: none"> • 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 <p>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.</p> <p>You can change the guest OS type only when the virtual machine is powered off.</p>

Item	Comments
Best Practice ID	VM-007
Recommendation	Disable screen savers and window animations.
Observation	
Priority	P3
Infrastructure Qualities	Scalability, Performance, Virtual Machine
Justification	<p>Screen savers are not necessary for virtual machines, and running screen savers wastes CPU resources.</p> <p>For virtual machines running Microsoft Windows:</p>

- Disable the pre-logon screensaver by changing HKEY_USERS\DEFAULT\Control Panel\Desktop\ScreenSaveActive to 0
- Disable all visual effects by disabling all effects in **Desktop Properties > Appearance > Effects**.
- Disable mouse pointer shadow from **Control Panel > Mouse > Pointers > Enable Pointer Shadow**. Set it to off.

References:

Disabling the Windows Login Screen Saver (9275881)

<http://kb.vmware.com/kb/9275881>

Guest Operating System General Considerations section in

Performance Best Practices for VMware vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	VM-009
Recommendation	Use as few vCPUs as possible to avoid over allocation of resources.
Observation	
Priority	P3
Infrastructure Qualities	Scalability, Performance, Virtual Machine

Justification

Configure only as many vCPUs as needed for the virtual machines. Do not use virtual SMP if the application is single threaded and will not benefit from additional CPUs.

Unused vCPUs in SMP virtual machines impose unnecessary scheduling constraints on ESXi and might be a waste of host resources (such as idle looping and process migrations, among others).

References:

Guest Operating System General Considerations section in

Performance Best Practices for VMware vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	VM-011
Recommendation	Check vCPU for saturation or sustained high utilization.
Observation	

Priority	P3
Infrastructure Qualities	Scalability, Performance, Virtual Machine
Justification	<p>High CPU utilization is not necessarily an indication of poor performance, but when high CPU utilization is detected along with queuing it might indicate a performance problem.</p> <p>If CPU average usage is above 75% or if there are peaks above 90%, then guest CPU saturation exists, though this does not necessarily indicate that a performance problem exists.</p> <p>If performance problems do exist during vCPU saturation and increasing vCPU resources to the OS and application does not help, investigate the tuning and behavior of the application and operating system.</p> <p>If host CPU average is above 75% or peak is above 90%, check VM vCPU ready:</p> <ul style="list-style-type: none"> For 1 vCPU VM: % ready > 10%, Ready (ms) > 2000ms might indicate CPU saturation. For 2 vCPU VM: % ready > 20%, Ready (ms) > 4000ms might indicate CPU saturation. For 4 vCPU VM: % ready > 40%, Ready (ms) > 8000ms might indicate CPU saturation. <p>The % ready varies based on the number of vCPUs. (The maximum % ready for a 4-vCPU VM is 400%.)</p> <p>It is important to understand baseline performance and unexpected deviations.</p> <p>References:</p> <p><i>Troubleshooting ESXi virtual machine performance related issues</i> https://kb.vmware.com/kb/2001003</p>
Item	Comments
Best Practice ID	VM-012
Recommendation	Allocate optimal memory to virtual machines, enough to minimize guest OS swapping, but not so much that unused memory is wasted.
Observation	
Priority	P3
Infrastructure Qualities	Scalability, Performance, Virtual Machine
Justification	It is much easier to add memory to a guest virtual machine than to a physical machine. Before configuring additional memory, confirm that the guest OS and applications can take advantage of the added

memory. For example, 32-bit operating systems can typically access only about 4 GB of memory, regardless of how much is configured.

When adding additional memory, check that the new allocation does not cause excessive memory overcommit on the host/cluster that leads to swapping.

References:

ESXi Memory Considerations section in *Performance Best Practices for VMware vSphere 7.0*

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

Item	Comments
Best Practice ID	VM-014
Recommendation	Use reservations and limits selectively on virtual machines.
Observation	1 VM(s) have Memory reservation resource settings configured.
Priority	P3
Infrastructure Qualities	Recoverability, Scalability, Performance, Virtual Machine
Justification	<p>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.</p> <p>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).</p> <p>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.</p> <p>References:</p> <p>General Resource Management section in <i>Performance Best Practices for VMware vSphere 7.0</i></p> <p>https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p>
Item	Comments
Best Practice ID	VM-016
Recommendation	Verify that VMware Tools is installed, running, and up to date for running virtual machines.

Observation	<p>1 VM(s) do not have VMware Tools installed. 27 VM(s) have VMware Tools installed that are not up to date. 2 VM(s) do not have VMware Tools running. 16 VM(s) have unmanaged by VMware Tools running. 91 VM(s) have supported, but newer VMware Tools version running.</p>
Priority	P1
Infrastructure Qualities	Manageability, Performance, Virtual Machine
Justification	<p>Install VMware Tools (including open-vm-tools where applicable) in all guests that have supported VMware Tools available.</p> <p>Note : <i>open-vm-tools</i> 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.</p> <p>VMware Tools optimize the guests to make them run better inside virtual machines by providing the following:</p> <ul style="list-style-type: none"> • 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) <p>For compatibility and optimal performance, upgrade VMware Tools for older virtual machines to the latest versions. VMware Supports VMware tools compatibility across ESXi versions. In these cases, if the environment has mixed versions of ESXi hosts, the version check may show out of date. This can be resolved by using a centralized location for the VMware tools ProductLocker for ESXi Hosts, that is always updated with the latest revisions of the tool. For more information see the VMware Tools Lifecycle link below.</p> <p>Consider using the automatic tools upgrade setting to be performed at powercycle of the VM to ensure the tools is always up to date.</p> <p>References:</p> <p>Performance Best Practices for vSphere 7.0 https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf</p> <p>VMware Tools Lifecycle</p>

<https://blogs.vmware.com/vsphere/2015/09/vmware-tools-lifecycle-why-tools-can-drive-you-crazy-and-how-to-avoid-it.html>

Automatically Upgrade VMware Tools on Reboot

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere-lifecycle-manager.doc/GUID-AA1EAF8-E386-48D6-9F7B-D06399742AAA.html>

Item	Comments
Best Practice ID	VM-017
Recommendation	Allocate only as much virtual hardware as required for each virtual machine. Disable any unused or unnecessary or unauthorized virtual hardware devices.
Observation	6 VM(s) has(ve) unnecessary virtual device(s) that is/are either connected or start connected.
Priority	P2
Infrastructure Qualities	Security, Manageability, Scalability, Performance, Virtual Machine
Justification	<p>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.</p> <p>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.</p> <p>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.</p> <p>Disabling or disconnecting unauthorized devices enhances the security levels of the virtual machines and their hosts.</p> <p>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.</p> <p>References:</p> <p>Best Practices for Virtual Machine and Host Security sections of the <i>vSphere Security Guide for vSphere 7.0</i></p> <p>https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/</p>

techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf

Item	Comments
Best Practice ID	VM-018
Recommendation	Consider the implications and use the latest virtual hardware version to take advantage of additional capabilities, when appropriate.
Observation	16 VMs are not using latest virtual hardware profile.
Priority	P2
Infrastructure Qualities	Manageability, Scalability, Performance, Virtual Machine
Justification	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>ESXi 7.0 introduces virtual hardware version 17. By creating virtual machines using this hardware version, or upgrading existing virtual machines to this version, a number of additional capabilities become available. This hardware version is not compatible with versions of ESXi prior to 7.0, however, and thus if a cluster of ESXi hosts will contain some hosts running pre-7.0 versions of ESXi, the virtual machines running on hardware version 17 will be constrained to run only on the ESXi 7.0 hosts. This could limit vMotion choices for Distributed Resource Scheduling (DRS) or Distributed Power Management (DPM).</p> <p>By creating virtual machines using this hardware version, or upgrading existing virtual machines to this version, additional capabilities become available.</p> <p>References:</p> <p><i>vSphere Virtual Machine Administration</i> Guide for vSphere 7.0 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-64D4B1C9-CD5D-4C68-8B50-585F6A87EBA0.html</p> <p>Procedure:</p> <p>Change the default compatibility setting of a virtual machine by performing one of the following actions:</p>

Right-click a virtual machine and click **Compatibility > Upgrade VM Compatibility**.

- Right-click a virtual machine and click **Compatibility > Schedule VM Compatibility Upgrade**.

Item	Comments
Best Practice ID	VM-019
Recommendation	Limit use of snapshots, and when using snapshots limit them to short-term use.
Observation	14 VM(s) have snapshot(s).
Priority	P1
Infrastructure Qualities	Manageability, Performance, Virtual Machine
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 the latest versions of VMFS, VMware recommends limiting use of snapshots, and when used, limiting them to short-term use.
Item	Comments
Best Practice ID	VM-024
Recommendation	Validate the schedule for recurring activities such as virus scans and backups is set appropriately to business policy.
Observation	
Priority	P3
Infrastructure Qualities	Availability, Performance, Virtual Machine
Justification	Backups and virus scanning programs in virtual machines should generally run at off-peak hours. This will help to avoid performance impact during production hours. In addition the scans should not be scheduled to run simultaneously in multiple virtual machines on the same ESXi host.
	In general, it is a good idea to evenly distribute CPU usage, not just across CPUs but also across time.
	For workloads such as backups and virus scanning, where the load is predictable, this is easily achieved by scheduling the jobs appropriately.

References:

Performance Best Practices for vSphere 7.0

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/performance/vsphere-esxi-vcenter-server-70-performance-best-practices.pdf>

4.2.1.6. vCenter Server

Item	Comments
Best Practice ID	VC-021
Recommendation	Configure HA Isolation addresses as appropriate for the configuration.
Observation	
Priority	P3
Infrastructure Qualities	vCenter Server, Availability, Recoverability
Justification	<p>Depending on how the ESXi cluster is set up, you can also specify an additional isolation response address for vSphere HA. This allows for HA to detect isolations from two separate networks, thereby making isolation detections more reliable.</p> <p>References:</p> <p><i>vSphere Availability Guide</i> https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-E0161CB5-BD3F-425F-A7E0-BF83B005FECA.html</p> <p>Procedure:</p> <p>Review the advanced settings of the HA Cluster to make sure that the isolation address has been set appropriately.</p>
Item	Comments
Best Practice ID	VC-026
Recommendation	vSphere HA feature, VM Component Protection (VMCP) should be enabled and configured appropriately to provide enhanced protection from failures.
Observation	<p>vSphere HA Datastore with PDL Failure Response is disabled for 1 cluster(s).</p> <p>vSphere HA All Paths Down (APD) Failure Response is disabled for 1 cluster(s).</p>
Priority	P1
Infrastructure Qualities	vCenter Server, Availability

Justification

VMCP provides protection against datastore accessibility failures that can affect a virtual machine running on a host in a vSphere HA cluster. When a datastore accessibility failure occurs, the affected host can no longer access the storage path for a specific datastore. You can determine the response that vSphere HA will make to such a failure, ranging from the creation of event alarms to virtual machine restarts on other hosts.

Review and configure the appropriate All Paths Down (APD) and Permanent Device Loss (PDL) settings for the desired response to an event.

References:

VM Component Protection

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-F01F7EB8-FF9D-45E2-A093-5F56A788D027.html>

Procedure:

Review the cluster vSphere HA configuration and validate that it is enabled and configured according to environmental requirements.

Apéndice A: Participantes en el chequeo

Equipo de ingeniería de infraestructuras de AEROCIVIL

Edward Christian Parra Velez

edward.parra@aerocivil.gov.co

Supervisor contrato de AEROCIVIL

Pedro Enrique Castro Hernandez

pedro.castro@aerocivil.gov.co

Servicios profesionales V2S COLOMBIA

Blanca Ramirez

Sr. Consultant

blanca.ramirez@v2s.us

Apéndice B: Inventario auditado

vCenter Server 1. vCenterServer- 172.16.63.37

vCenter Server

- Server name: 172.16.63.37
- Platform:
- OS:
- Number of CPUs:
- RAM:
- Cluster:

Host Configuration 1

Platform Specifications

- System: HP ProLiant DL580 Gen9
- CPU: 4 sockets, 96 total cores, Intel(R) Xeon(R) CPU E7-8890 v4 @ 2.20GHz
- RAM: 2048 GB
- HBAs: Smart Array P830i, QLE2692 Dual Port 16Gb Fibre Channel to PCIe Adapter
- NICs: Intel(R):82599 10 Gigabit Dual Port Network Connection, Broadcom Corporation:NetXtreme BCM5720 Gigabit Ethernet

ESX/ESXi Hosts

- esxi01.aerocivil.gov.co
- esxi02.aerocivil.gov.co

Networking Configuration

Networking Configuration 1

Virtual Data Center Name: Aerocivil

Cluster Name: Aerocivil

ESX/ESXi Hosts: esxi01.aerocivil.gov.co, esxi02.aerocivil.gov.co

Switch Name	Switch Type	Total Ports	Available Ports	Port Group	Active NICs/Uplinks	Standbyby NICs/Uplinks
vSwitch0	Std	9216	9140	VLAN_54	vmnic0, vmnic1	
vSwitch0	Std	9216	9140	VLAN_800	vmnic0, vmnic1	
vSwitch0	Std	9216	9140	VLAN_400	vmnic0, vmnic1	

vSwitch0	Std	9216	9140	Vmotion	vmnic0, vmnic1
vSwitch0	Std	9216	9140	Management Network	vmnic0, vmnic1
DSwitch	DVS	9216	9140	Vlan800	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan511	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan700	vmnic6, vmnic7
DSwitch	DVS	9216	9140	DPortGroup	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan2300	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan54	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan200	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan21	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan519	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan520	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan2500	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan400	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan20	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan72	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan24	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan518	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan517	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan10	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan850	vmnic6, vmnic7
DSwitch	DVS	9216	9140	HeartBeat_Vlan70	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan68	vmnic6, vmnic7
DSwitch	DVS	9216	9140	Vlan410	vmnic6, vmnic7
vSwitch0	Std	9216	9126	VLAN_54	vmnic0, vmnic1

vSwitch0	Std	9216	9126	VLAN_400	vmnic0, vmnic1
vSwitch0	Std	9216	9126	VLAN_800	vmnic0, vmnic1
vSwitch0	Std	9216	9126	Vmotion	vmnic0, vmnic1
vSwitch0	Std	9216	9126	Management Network	vmnic0, vmnic1
DSwitch	DVS	9216	9126	Vlan800	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan511	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan700	vmnic6, vmnic7
DSwitch	DVS	9216	9126	DPortGroup	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan2300	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan54	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan200	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan21	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan519	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan520	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan2500	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan400	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan20	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan72	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan24	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan518	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan517	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan10	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan850	vmnic6, vmnic7
DSwitch	DVS	9216	9126	HeartBeat_Vlan70	vmnic6, vmnic7
DSwitch	DVS	9216	9126	Vlan68	vmnic6, vmnic7

DSwitch	DVS	9216	9126	Vlan410	vmnic6, vmnic7
---------	-----	------	------	---------	----------------

Storage Configuration

Storage Specifications

Array: Storage Vendor, Model

Datastore Name	Type	Size (GB)	Free Space (GB)	Comments
CMPL_LUN08	VMFS	4096	3926	
DS_SANPURE_250	VMFS	20480	6109	
DS_SANPURE_251	VMFS	20480	6844	
DS_SANPURE_252	VMFS	20480	10226	
DS_SANPURE_253	VMFS	20480	10070	
DS_SANPURE_254	VMFS	20480	8143	
DS_SANPURE_HA_1	VMFS	5	3	
DS_SANPURE_HA_2	VMFS	5	3	
ESXI01_DATASTORE	VMFS	96	94	
ESXI02_DATASTORE	VMFS	96	94	
PURE_VVOL	VVOL	8388608	8280784	

Virtual Data Center 1

Specifications

- Virtual Data Center name: Aerocivil
- Physical Data Center:

Cluster	Enabled Features	Hosts Checked	No. of VMs
Aerocivil	HA, DRS		134

Apéndice C: Buenas prácticas para la evaluación del chequeo médico

The following is a list of all current vSphere best practices.

VMware vCenter 7.0

Component: ESXi Host

ESXI-001 Deploy VMware ESXi in compliance with all configuration maximums as documented in the most current VMware vSphere Configuration Maximums document.

ESXI-002 Verify that all hardware in the system is on the VMware Compatibility Guide for ESXi.

ESXI-003 Verify that hardware meets the optimal configuration supported by ESXi.

ESXI-004 Check CPU compatibility for VMware vSphere vMotion and VMware vSphere Fault Tolerance.

ESXI-005 Avoid unnecessary changes to advanced parameter settings.

ESXI-006 Maintain a similar version of ESXi within a cluster.

ESXI-007 Avoid using third-party agents on the ESXi host.

ESXI-008 Place host devices in a consistent order and location.

ESXI-009 Use persistent and remote syslog logging to improve manageability.

ESXI-010 Disconnect or disable unused or unnecessary physical hardware devices (COM and LPT ports, USB and storage controllers, CD/DVD/floppy drives, and NICs).

ESXI-011 Manage CPU oversubscription. Verify that the total CPU resources needed by virtual machines do not exceed the CPU capacity of the host.

ESXI-012 Monitor the ESXi hosts to verify that the CPU is not saturated or running with a sustained high CPU load.

ESXI-013 Check virtual machines to verify that CPU ready is less than 2000 ms.

ESXI-014 Confirm that hardware assisted virtualization features are enabled if the CPUs support them.

ESXI-015 Confirm that you are running the latest version of the BIOS available for your ESXi servers.

ESXI-016 Verify that the BIOS is set to enable all CPU sockets, and enable all cores in each socket.

ESXI-017 Enable Turbo Mode in the BIOS if your processors support it.

ESXI-018 Confirm that non-uniform memory access (NUMA) is enabled for NUMA-capable systems.

ESXI-019 Consider enabling hyperthreading if applicable and if the CPU and BIOS support it.

ESXI-020 Review ESXi hosts for driver and firmware consistency between hosts in a cluster.

ESXI-021 Check the active Swap in rate of virtual machines to verify that it is not greater than 0 at any point in the measurement period.

ESXI-022 Use Host Profiles to ensure a consistent configuration across ESXi hosts.

ESXI-023 Check that the appropriate Power Management Settings are configured for the ESXi Host which meet the power consumption versus performance characteristics desired.

Component: Licensing

LIC-001 Verify that adequate licenses are available for vCenter Server instances.
LIC-002 Verify that adequate CPU licenses are available for ESXi hosts.
LIC-003 Evaluation licenses should not be used in the environment.
LIC-004 Validate that proper licenses are installed for VMware vSAN clusters (if applicable).

Component: Network

NE-001 Deploy networking in compliance with all configuration maximums as documented in the most current vSphere Configuration Maximums document.
NE-002 Configure networking consistently across all hosts in a cluster.
NE-003 Verify that there is redundancy in networking paths and components to avoid single points of failure.
NE-004 Set up network redundancy for VMKernel network ports where required.
NE-005 If the physical switches that support PortFast (or equivalent), enable it on the physical switches that connect to the host.
NE-006 Distribute vmnics for a port group across different PCI buses for greater redundancy.
NE-007 Configure networks so that there is separation of traffic (physical or logical using VLANs).
NE-008 If beacon probing is used verify that there are at least three NICs.
NE-009 Use at least one 1 GbE adapter for workloads that have a small number of memory operations. Use at least one 10 GbE adapter if you migrate workloads that have many memory operations.
NE-010 Use static IP addresses for the management ESXi host management interface.
NE-011 Make sure that vSphere FT logging traffic is on at least a segregated 10-Gbps network.
NE-012 Single port 10-GbE network adapters should use PCIe x8 (or higher) or PCI-X 266. Dual port 10-GbE should use PCIe x16 or higher.
NE-013 Limit the number of installed NIC ports to recommended maximums.
NE-014 Minimize differences in the number of active NICs across hosts within a cluster.
NE-015 Check for dropped packets on vmnic objects.
NE-016 If jumbo frames are enabled, verify that jumbo frame support is enabled end-to-end on all intermediate devices so that there is no MTU mismatch.
NE-017 Configure NICs, physical switch speed, and duplex settings consistently.
NE-018 Avoid mixing NICs with different speeds and duplex settings on the same uplink for a port group/dvport group.
NE-019 Adjust load balancing settings from the default virtual port ID only if necessary.
NE-020 Verify that the network topology does not contain link oversubscription resulting in dropped packets.
NE-021 Use Network I/O Control (NetIOC) to prioritize traffic.
NE-022 Use shares instead of limits when using NIOC for bandwidth allocation. Do not impose limits unless addressing physical network capacity requirements.
NE-023 If Fault Tolerance is used, set Network I/O Control Fault Tolerance resource pool shares to High.

NE-024 Use Distributed Virtual Port Groups to apply policies to traffic flow types and to provide Rx (receive) bandwidth controls through the use of Traffic Shaping.

NE-025 Configure network appropriately when VMware vSphere Auto Deploy is used.

NE-026 Verify latency between vCenter Server and other network components.

Component: Security

SEC-001 Confirm integrated Windows authentication is configured when using Active Directory identity sources.

SEC-002 Confirm that time is synchronized on the SSO Server and on any server that connects to the SSO server.

SEC-003 Record the Single Sign-On administrator password in a safe place.

SEC-004 Avoid using local operating system users with vCenter Single Sign-On.

SEC-005 Set the vCenter Single Sign-On default domain to the identity source which is most frequently used.

SEC-006 Set the Single Sign-On password and lockout policies per customer security requirements.

SEC-007 Add only the necessary identity sources to the vCenter Single Sign-On configuration.

SEC-008 Set the base domain name for users and groups accordingly in Single Sign-On when using LDAP or OpenLDAP identity sources.

SEC-009 Limit remote access to all hosts by administrative users such as root.

SEC-010 Configure firewall rules and ports according to best practices.

SEC-011 Configure VMware vSphere ESXi Shell and SSH access per manageability requirements.

SEC-012 Enable the ESXi Shell timeout feature and configure it per customer security requirements.

SEC-013 Keep current with the latest VMware product versions and patches.

SEC-014 Use vCenter Server roles, groups, and permissions to provide appropriate access and authorization to the virtual infrastructure. Avoid using AD built-in groups such as the Domain Admins group.

SEC-015 Use Active Directory for local user authentication to ESXi Hosts.

SEC-016 Change port group security default settings for Forged Transmits, Promiscuous Mode, and MAC Address Changes to Reject unless required.

SEC-017 Enable bidirectional CHAP authentication for iSCSI traffic so that CHAP authentication secrets are unique.

SEC-018 Configure Management network Traffic on an isolated network.

SEC-019 Validate that copy/paste between the guest operating system and the remote console is disabled.

SEC-020 Verify that VMware isolation settings have not been disabled.

SEC-021 Limit sharing console connections if there are security concerns.

SEC-022 For additional security for NFS v4.1 shares, configure Kerberos authentication.

SEC-023 VMware Certificate Authority should be configured as a subordinate CA in the environment for additional security.

SEC-024 Configure Encrypted vSphere vMotion if the organization policy requires it.

Component: Storage

ST-001 Consult with the storage vendor for recommendations for use with the storage device in the environment.

ST-002 Deploy storage in compliance with all configuration maximums as documented in the most current vSphere Configuration Maximums document.

ST-003 Use shared storage for virtual machines instead of local storage.

ST-004 Zone Fibre Channel LUNs properly to the appropriate devices for vSphere vMotion compatibility, security, and shared services.

ST-005 Minimize differences in datastores visible across hosts within the same cluster or vSphere vMotion scope.

ST-006 Use the appropriate policy based on the array being used (MRU, Fixed, Round Robin, and so on).

ST-007 Manage the differences in the number of storage paths between hosts including maximum paths per host.

ST-008 Verify that there is redundancy in storage paths and components to avoid single points of failure.

ST-009 Check that storage LUNs are not overloaded by verifying that the Command Aborts for all datastores is 0.

ST-010 Verify that Physical Device Read/Write Latency average is less than approximately 10 ms and peak is less than approximately 20 ms for all virtual disks.

ST-011 Allocate space on shared datastores for templates and media/ISOs separately from datastores for virtual machines.

ST-012 Size datastores appropriately for the environment.

ST-013 Configure NFS and iSCSI storage traffic for performance and security.

ST-014 Align VMFS partitions.

ST-015 Verify the queue depth of the HBA and the max outstanding disk requests per virtual machine parameter according to storage vendor best practices.

ST-016 Spread I/O loads over the available paths to the storage (across multiple HBAs and storage processors).

ST-017 Choose placement of data disks and swap files on LUNs appropriately for virtual machines.

ST-018 Prior to performing a VMware vSphere Storage vMotion operation, verify that there is sufficient bandwidth between the ESXi host running the virtual machine and both source and destination storage.

ST-019 Consider scheduling vSphere Storage vMotion operations during times of low storage activity, when available storage bandwidth is highest and when the workload in the virtual machine being moved is least active.

ST-020 Use Storage I/O Control (SIOC) to prioritize high importance traffic, such as virtual machine traffic.

ST-021 To maximize the fairness benefit from SIOC, avoid introducing non-SIOC-aware load on the storage.

ST-022 Optimize storage utilization through the datastore cluster and VMware vSphere Storage DRS features.

ST-023 When booting from SAN, verify that the datastore is masked and zoned to that particular ESXi host and not shared with other hosts.

ST-024 Keep the IP storage network physically separate from other traffic.

ST-025 Validate and optimize Non-Volatile Memory Express (NVMe) device performance.

ST-026 Check ESXi Hosts for storage plugin version and consistency.

ST-027 Check for consistent VAAI settings on ESXi Hosts in a cluster.

Component: Virtual Machines

VM-001 Use NTP, Windows Time Service, or another timekeeping utility for all ESXi Hosts and virtual machines.

VM-002 Use the correct virtual SCSI hardware for the operating system.

VM-003 Verify that virtual machines meet the requirements for vSphere vMotion.

VM-004 Do not specify CPU affinity rules unless needed.

VM-005 Use the latest version of VMXNET that is supported by the guest operating system.

VM-006 Select the correct guest operating system type in the virtual machine configuration to match the guest operating system.

VM-007 Disable screen savers and window animations.

VM-008 Verify that the file system partitions within the guest operating system are aligned.

VM-009 Use as few vCPUs as possible to avoid over allocation of resources.

VM-010 Use the default monitor mode chosen by the Virtual Machine Monitor unless it is necessary to change it.

VM-011 Check vCPU for saturation or sustained high utilization.

VM-012 Allocate optimal memory to virtual machines, enough to minimize guest OS swapping, but not so much that unused memory is wasted.

VM-013 Configure the guest operating system with sufficient swap space.

VM-014 Use reservations and limits selectively on virtual machines.

VM-015 Use paravirtualized SCSI (PVSCSI) with a supported guest OS where additional performance is needed.

VM-016 Verify that VMware Tools is installed, running, and up to date for running virtual machines.

VM-017 Allocate only as much virtual hardware as required for each virtual machine. Disable any unused or unnecessary or unauthorized virtual hardware devices.

VM-018 Consider the implications and use the latest virtual hardware version to take advantage of additional capabilities, when appropriate.

VM-019 Limit use of snapshots, and when using snapshots limit them to short-term use.

VM-020 Consider using a 64-bit guest operating system to improve performance, if applicable.

VM-021 Consider setting the memory reservation value for performance-sensitive Java-based virtual machines (JVMs) to the operating system required memory plus the total JVM heap size.

VM-022 Validate that there are no orphaned or invalid virtual machines in the inventory.

VM-023 If virtual machine encryption is used, validate that the ESXi host processors support AES-NI, for improved performance.

VM-024 Validate the schedule for recurring activities such as virus scans and backups is set appropriately to business policy.

Component: vSAN

- VSAN-001 Review the Cluster section of the vSAN Health interface.
- VSAN-002 Review the Data section of the vSAN Health interface.
- VSAN-003 Review the Encryption section of the vSAN Health interface.
- VSAN-004 Review the Hardware Compatibility section of the vSAN Health interface.
- VSAN-005 Review the Hyper-converged Cluster Configuration Compliance section of the vSAN Health interface
- VSAN-006 Review the Limits section of the of the vSAN Health interface.
- VSAN-007 Review the Network section of the vSAN Health interface.
- VSAN-008 Review the Online Health section of the vSAN Health interface.
- VSAN-009 Review the Performance Service section of the vSAN Health interface.
- VSAN-010 Review the Physical Disk section of the vSAN Health interface.
- VSAN-011 Review the Stretched Cluster section of the vSAN Health interface.
- VSAN-012 Review the vSAN Build Recommendation section of the vSAN Health interface.
- VSAN-013 Review the vSAN iSCSI Target Service section of the vSAN Health interface.
- VSAN-014 Review the vSAN File Services section of the vSAN Health interface.
- VSAN-015 Verify that you are using high performing SSDs for best performance.
- VSAN-016 Use 10-Gigabit networks with vSAN.
- VSAN-017 Fault domains should be used to protect against a rack or chassis failure in the environment.
- VSAN-018 Verify that you have configured storage policies correctly.
- VSAN-019 CPU contention can adversely affect vSAN.
- VSAN-020 Separate VLANs for vSAN traffic.
- VSAN-021 Jumbo frames can increase vSAN performance
- VSAN-022 Avoid using Flash read cache policy reservations unless absolutely necessary.

Component: vCenter Server

- VC-001 Deploy vCenter Server in compliance with all configuration maximums as documented in the most current vSphere Configuration Maximums document.
- VC-002 Deploy vCenter Server appliance using an embedded platform services controller.
- VC-003 Use a consistent naming convention for all virtual data center objects.
- VC-004 Maintain compatible and homogeneous (CPU, memory, and storage when using vSAN) hosts within a cluster to support the required functionality for vSphere vMotion, vSphere DRS, VMware vSphere Distributed Power Management, vSphere HA, and vSphere FT.
- VC-005 Verify that the number of hosts in a cluster is within limits for the required functionality (HA, vSphere DRS, and vSphere DPM).
- VC-006 Verify that vSphere HA settings allow sufficient capacity for vSphere DPM to power down hosts.
- VC-007 Size VMware HA admission control policy considering the allowed host failures and available resources.

VC-008 Use reservations and limits selectively on clusters and resource pools that require them. Do not set reservations too high or limits too low.

VC-009 Verify that hardware meets the optimal configuration required by vCenter Server and add-ons.

VC-010 Verify that DNS is configured for forward, reverse, short, and long lookups.

VC-011 Use automatic mode for vSphere DRS, if possible, for optimal load balancing.

VC-012 Consider enabling vSphere DPM for clusters in which virtual machine demand varies greatly over time.

VC-013 Distribute vSphere FT VMs to multiple hosts, if the feature is in use.

VC-014 Verify that the number of vSphere FT-enabled virtual machines does not saturate the vSphere FT logging network.

VC-015 Verify that the hosts on which the primary and secondary FT-enabled virtual machines run are relatively closely matched (CPU make, model, frequency, and version/build/patches).

VC-016 Verify that power management settings (BIOS, ESX) that cause CPU scaling are consistent on hosts running primary and secondary FT-enabled virtual machines.

VC-017 Avoid making resource pools and virtual machines siblings in a hierarchy to avoid unexpected performance.

VC-018 Configure the vCenter Server statistics to a level appropriate for use. VMware recommends level 1 or 2.

VC-019 vSphere Auto Deploy HA configuration practices.

VC-020 Tasks and Events Retention Policy set in the environment.

VC-021 Configure HA Isolation addresses as appropriate for the configuration.

VC-022 Validate that the supported scale for vCenter Server configuration is not exceeded.

VC-023 Validate storage requirements are met for the vCenter Server Appliance Database.

VC-024 Follow vPostgress best practices when maintaining the vCenter Server Database.

VC-025 vSphere HA should be enabled on all clusters.

VC-026 vSphere HA feature, VM Component Protection (VMCP) should be enabled and configured appropriately to provide enhanced protection from failures.

Appendix D: Referencias

The following table provides references that are relevant for the vSphere health check.

Item	URL
<i>Featured VMware Documentation Sets</i>	http://www.vmware.com/support/pubs
Knowledge Base	http://kb.vmware.com
VMware Community VMTN Forums	http://www.vmware.com/community
VMware support	http://www.vmware.com/support
Support Phone Numbers	http://www.vmware.com/support/phone_support.html
VMware Training	http://mylearn.vmware.com/mgrreg/index.cfm
Certification	http://mylearn.vmware.com/portals/certification/
Technical Papers	http://www.vmware.com/vmtn/resources