CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN VMWARE VSPHERE 6.7

SEPTIEMBRE 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.09.23 15:34:17 +02'00'

NIPO: 083-20-181-1

Fecha de Edición: septiembre de 2020
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

septiembre de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional, siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

El conjunto de guías al que pertenece el presente documento se ha diseñado de manera incremental. Así, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. En este sentido, se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

No es objeto de esta guía determinar la plataforma sobre la que se instalarán los distintos elementos que corresponden al conjunto de aplicaciones contenidos en el producto *VMware vSphere* 6.7. Sin embargo, habrá de tenerse en cuenta el hecho de que el sistema operativo sobre el que se instalen dichos aplicativos deberá, de forma previa, haber sido configurado mediante los mecanismos correctos para la implementación de la seguridad requerida en dicho sistema.

Por ejemplo, en el caso de un entorno que le sea de aplicación el ENS, para un servidor miembro de un dominio con Microsoft Windows Server 2016, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN-STIC-870A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-873 Internet Information Services (IIS) 8.5.

c) Guía CCN-STIC-880 Microsoft Exchange Server 2013 en Windows 2012 R2.

Por ejemplo, en el caso de un entorno de red clasificada, para un servidor con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN STIC 560A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-563 Internet Information Services (IIS) 8.5.

c) Guía CCN STIC 552 Microsoft Exchange Server 2013 en Windows 2012 R2.

Nota: Estas guías están pensadas y diseñadas para entornos de máxima seguridad donde no existirá conexión con redes no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para garantizar la seguridad para el empleo de los elementos principales que componen el conjunto de herramientas que engloba la solución *VMware vSphere 6.7* independientemente del entorno sobre el que estén operando dichos elementos.

La presente guía tiene como objeto la implementación de todos los roles necesarios para el funcionamiento de VMware vSphere 6.7. Se establecerán también los procesos y tareas administrativas para hacer una administración segura de los mismo,

La instalación y configuración de la solución se ha diseñado de tal forma que la implementación sea lo más restrictiva posible, minimizando la superficie de ataque y, por lo tanto, los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del servidor, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las plantillas y normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

En el caso de la aplicación de seguridad sobre un entorno perteneciente a una red clasificada, se establece la máxima seguridad posible teniendo en consideración la guía “CCN-STIC-301 – Requisitos STIC”. Si su sistema requiere de otra configuración menos restrictiva, y está autorizado para ello, consulte el apartado “APLICACIÓN DE NIVELES DE CLASIFICACIÓN” correspondiente al sistema operativo donde se encuentren instaladas las herramientas. Por ejemplo, en caso de estar aplicando vCenter sobre Windows Server 2016, deberá hacer la consulta en el apartado “ANEXO B” de la guía codificada como “CCN-STIC-570A”.

Esta guía no contempla la plataforma sobre la que se implementará el conjunto de

aplicaciones, por lo que se deberá tener en cuenta el sistema operativo y las circunstancias del entorno donde va a ser implementado el conjunto de herramientas de *VMware vSphere* 6.7.

Al existir numerosas modalidades de licenciamiento y uso de las herramientas de *VMware vSphere 6.7* no es objeto de este documento, la descripción, implementación o aplicación de seguridad de cada uno de los elementos adicionales que componen el conjunto de herramientas. Por tanto, el alcance de este documento comprende las aplicaciones de seguridad sobre las herramientas principales, *vCenter Server* y *ESXi*.

Así mismo, no se contempla en esta guía la instalación del servicio de *VMware vSphere* en clúster, ni se han aplicado características de alta disponibilidad o protección ante fallos del servicio.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica para realizar la aplicación del servicio que proporciona *VMware vSphere* 6.7 a través de las herramientas *ESXi* y *vCenter Server*. en una configuración restrictiva de seguridad. En la guía no se ha tenido en cuenta un entorno específico de aplicación, por lo que los servicios que aplicaran debajo de la solución y a su alrededor podrían ser entornos seguros de sistemas operativos Windows o Linux, en dominio o como servicio independiente.

Así mismo, no se contempla la instalación de vSphere 6.7 en una arquitectura de alta disponibilidad ni la incorporación de mecanismos de balanceo de carga.

Este documento incluye:

a) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello, así como los pasos a seguir en aquellos mecanismos que no puedan ser totalmente automatizados.

b) **Descripción de los principales elementos que componen la solución.** Descripción de los propósitos y capacidades que proporcionan ESXi y vCenter Server.

c) **Descripción de la seguridad en los servicios de *VMware vSphere* 6.7.** Completa la descripción de los mecanismos de seguridad, autenticación y autorización utilizados en *ESXi* y *vCenter Server*, así como las medidas para reforzar dicha seguridad.

d) **Guía paso a paso.** Va a permitir establecer las configuraciones de seguridad de un servidor *ESXi* y un servidor *vCenter Server* tanto en entornos de redes clasificadas como en aquellos definidos por el Esquema Nacional de Seguridad.

e) **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía tanto en entornos de redes clasificadas como en aquellos definidos por el Esquema Nacional de Seguridad.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de aplicación de seguridad que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

a) Antes de comenzar a aplicar esta guía, debe tenerse en cuenta que, además de los requisitos a cumplir en la aplicación de la seguridad de *VMware vSphere* 6.7, será necesario cumplir los requisitos definidos para los sistemas operativos sobre los que se efectuará la instalación de las diferentes herramientas que componen el conjunto de servicios que proporciona. En el caso de *ESXi*, la instalación del servicio incluye también el sistema operativo sobre el que opera la herramienta. Es un servicio de tipo *appliance* (ofrece el servicio y el sistema operativo en conjunto) basado en *Linux* y, por tanto, se tomarán en cuenta las medidas de seguridad relacionadas.

b) Por otro lado, es necesario comprobar los requisitos de otros servicios y aplicaciones que se vayan a aplicar posteriormente, independientemente del sistema operativo sobre el que éstos sean instalados y se deberán tener en cuenta, de forma especial, aquellos requisitos relacionados con la creación y gestión de máquinas virtuales. En la mayoría de los productos y/o servicios se recomienda separar en particiones distintas el sistema operativo y el resto de los ficheros del servicio proporcionado.

c) Si el entorno sobre el que se está aplicando seguridad pertenece a una red clasificada, se deberá realizar la aplicación de seguridad del sistema operativo antes de implementar los servicios que compone *VMware vSphere* 6.7 para posteriormente aplicar la seguridad tal y como se describe en la presente guía.

d) En aquellos sistemas que les sea de aplicación el ENS estas medidas deberán adaptarse a las necesidades de cada organización.

e) El procedimiento establecido en este documento asume que está configurando un sistema a partir de un entorno limpio (formateado) en el caso de una red clasificada y un entorno ya en producción en el caso del ENS.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

El contenido de esta guía es de aplicación sobre equipos tipo puesto servidor en castellano, independiente del sistema operativo sobre el que se instale.

El objeto de la guía es el de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la guía CCN-STIC-301.

En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, podría darse el caso de que se deban incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

Sin embargo y teniendo en consideración la aplicación de seguridad específica a aplicar, se entiende que el sistema operativo sobre el que se realizará la instalación de *vCenter Server* es indiferente al funcionamiento seguro del mismo siempre y cuando se tenga en consideración que el fabricante especifique, en los sitios oficiales, la posibilidad de implementación sobre dicho sistema operativo y la correcta aplicación de la guía correspondiente al mismo.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima en caso de redes clasificadas y los estándares de seguridad mínimos siguiendo las normas descritas en el ENS. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios o características tanto en equipos servidores para las herramientas *ESXi* y *vCenter Server* como para equipos clientes para *vSphere Web Client*.

Así mismo, hay que tener en cuenta que los requerimientos de *Hardware*, para un entorno de producción, dichos requerimientos varían notablemente según la cantidad de hipervisores y máquinas virtuales a implementar. Dichos requisitos se encuentran especificados en el sitio oficial del fabricante:

a) Requisitos de hardware para *ESXi* (Basado en *Linux*):

   https://docs.vmware.com/es/VMware-vSphere/6.7/com.vmware.esxi.install.doc/GUID-DEB8086A-306B-4239-BF76-E354679202FC.html

b) Requisitos de hardware para *vCenter* para *Windows*:

   https://docs.vmware.com/es/VMware-vSphere/6.7/com.vmware.vcenter.upgrade.doc/GUID-D2121DC5-1FC8-48DC-A4BA-C3FD72D0BE77.html

c) Requisitos de hardware para *vCenter Appliance* (Basado en *Linux*):

   https://docs.vmware.com/es/VMware-vSphere/6.7/com.vmware.vcenter.upgrade.doc/GUID-88571D8A-46E1-464D-A349-4DC43DCAF320.html

Nota: Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad descritos anteriormente.

Para garantizar la seguridad de los clientes y servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, tanto de los sistemas operativos empleados para el uso de los servicios como en lo relativo a las actualizaciones de seguridad específicas de los propios elementos de la solución.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que, en ocasiones, se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado, en el cual se habrán aplicado las pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

Del mismo modo, tenga en consideración que los sistemas operativos (y productos desplegados en ellos) correspondientes a las máquinas virtuales que alberguen los servidores de *ESXi* deberán poseer un nivel de seguridad adecuado a su propósito teniendo en consideración la normativa aplicable. Por lo tanto, será necesario que en el caso de máquinas virtuales se implementen las medidas de protección establecidas en las guías de seguridad de aplicación. A modo de ejemplo, si el servidor *ESXi* posee una máquina virtual servidor MS *Windows* 2016 que implemente el rol de controlador de dominio, ésta deberá contar con las medidas de seguridad acordes a la guía codificada como "CCN-STIC-570A".

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones, sino a servir como línea base de seguridad que deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del producto VMWare vSphere 6.7 dependiendo del entorno sobre el que vaya a ser aplicado:

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) **Anexo A:** principales que compone *VMware vSphere* 6.7 a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar las herramientas principales que compone *VMware vSphere* 6.7 a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que en sus respectivos anexos se dotará de la información necesaria y concreta para cada tipo de aplicación de seguridad de los elementos que componen la solución de virtualización.

6. DESCRIPCIÓN GENERAL DE VMWARE VSPHERE 6.7

Los entornos virtuales proporcionan una gran flexibilidad y potencia a la hora de desplegar e implementar sistemas virtuales que son administrados de forma centralizada. Existen multitud de soluciones de virtualización entre las que se encuentra *VMware vSphere* 6.7.

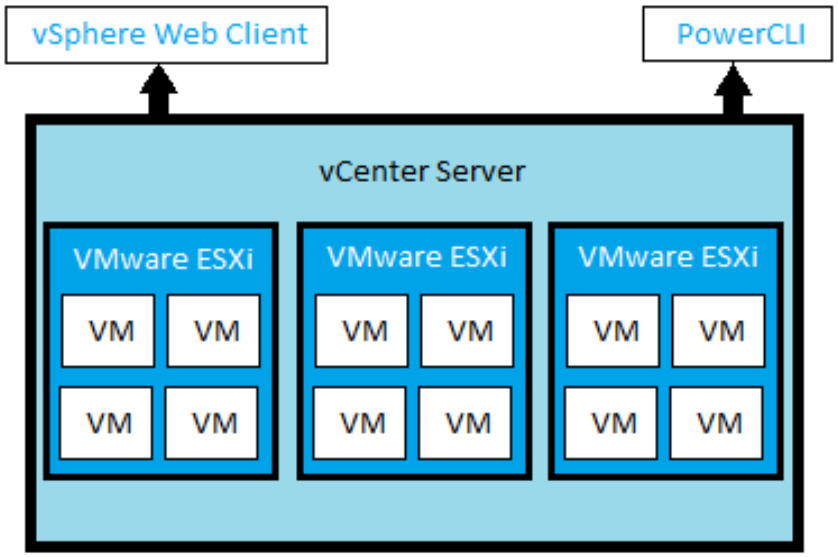
VMware vSphere 6.7 es un conjunto de herramientas que permiten la administración centralizada de múltiples hipervisores. Las herramientas básicas que comprenden este conjunto son las siguientes:

a) **vCenter Server:** Es una herramienta que permite tanto la gestión de los hipervisores como las máquinas virtuales que lo componen, así como una serie de redes virtuales y sitios para intercomunicar máquinas virtuales, elementos de almacenamiento y elementos de red. Así mismo, esta herramienta permite la migración de máquinas y la gestión de elementos que proporcionan alta disponibilidad.

b) **ESXi:** Es un hipervisor montado sobre un sistema operativo ligero. Un hipervisor permite la virtualización de diferentes sistemas operativos, que se ejecutan al mismo tiempo sobre un sistema físico, sin que se vean interferidos entre ellos. Esta separación de entornos se consigue mediante la creación de una capa de abstracción entre el *hardware* de la máquina física (también conocida como *host* o anfitrión) y el sistema operativo que se ejecuta dentro del entorno virtualizado (también conocido como máquina virtual, *guest* o huésped). De este modo, los diferentes recursos de la máquina física (tarjeta de red, memoria *RAM*, etc.) se dividen y se reparten entre uno o más entornos virtualizados.

c) **vSphere web Client y PowerCLI:** Aquellas herramientas mediante las cuales se puede acceder al vCenter o a los hosts ESXi para su administración.

En la siguiente imagen se puede observar un esquema de las herramientas mencionadas anteriormente que componen la arquitectura de vSphere 6.7



El hipervisor constituye una pequeña capa de software entre el hardware y los diferentes sistemas operativos instalados en el sistema. Es el encargado de ejecutar múltiples instancias de sistemas operativos de forma aislada a través del uso de múltiples instancias de ejecución conocidas como particiones. El hipervisor no acepta código de terceros, como drivers de dispositivos, situándose éste dentro de cada entorno virtualizado. De esta forma, se proporciona una mayor seguridad al hipervisor, ya que éste no tendrá contacto directo con el hardware de los sistemas operativos huésped y viceversa.

6.1 BENEFICIOS

La virtualización realizada por las herramientas que componen *VMware vSphere* 6.7 proporciona diferentes beneficios tanto técnicos como de gestión, los cuales se detallan a continuación:

a) Mayor eficiencia de los recursos de la máquina física.

b) Reducción de los costes de operación y mantenimiento de la máquina física.

c) Reducción del tiempo requerido para el despliegue y configuración del *hardware* y *software*, así como la realización de las pruebas correspondientes al entorno físico sobre el que se despliega el servicio.

d) Los recursos físicos son gestionados por el hypervisor para proporcionar entornos totalmente aislados.

e) Posibilidad de crear entornos de prueba sin que sea necesario obtener equipamiento *hardware* complejo y costoso.

6.2 CARACTERÍSTICAS

Las características principales de *VMware vSphere 6.7* incluyen lo siguiente:

a) Virtualización nativa de 64 bits basada en hipervisor.

b) Posibilidad de ejecutar máquinas virtuales de 32 o 64 bits de forma concurrente.

c) Posibilidad de usar máquinas virtuales de un único procesador o de múltiples procesadores.

d) Creación y gestión de puntos de control que contienen una copia del sistema en el momento de su creación.

e) Capacidad para gestionar grandes cantidades de memoria *RAM* y asignación dinámica de memoria *RAM* para equilibrar el consumo de memoria de las máquinas virtuales.

f) Soporte de redes de área local virtuales (conmutadores virtuales).

g) Migración en tiempo real.

h) Almacenamiento dinámico de máquinas virtuales.

i) Soporte mejorado del procesador.

j) Soporte mejorado de redes.

k) Canal de fibra virtual para establecer una comunicación directa con el almacenamiento de canal de fibra óptica desde el sistema operativo virtual.

l) Gestión de redes virtuales

m) Migración de máquinas entre hipervisores

n) Posibilidad de uso de herramientas de alta disponibilidad como migración de recursos en vivo, uso de hipervisores en clúster, etcétera.

Nota: Para obtener más información acerca de las características, o mejoras respecto a otras versiones, de *VMware vSphere 6.7* puede consultar la *Web* de *VMware* a través de la siguiente dirección:

https://docs.vmware.com/es/VMware-vSphere/6.7/rn/vsphere-esxi-vcenter-server-67-release-notes.html

6.3 LIMITACIONES

Si bien es cierto que un *vCenter Server* correctamente dimensionado puede gestionar cientos de *hosts ESXi* hasta un máximo teórico de 2000, el servicio de hipervisor que proporcionan los servidores ESXi posee una serie de limitaciones en cuanto a la cantidad de recursos que puede utilizar. Del mismo modo, cada una de las máquinas virtuales gestionadas por el servicio de virtualización posee una serie de limitaciones con respecto a sus recursos de tipo físico asignados.

Dichas limitaciones no deberían suponer un problema de cara a la implementación de la solución en el sentido de que los valores que se están manejando, siempre que el *hardware*, con el que cuentan los servidores de *ESXi* y *vCenter*, sea el adecuado responderían satisfactoriamente a demandas de 2000 hosts, 25000 máquinas virtuales encendidas y 35000 registradas por cada servidor de *vCenter* y a esto hay que añadirle el hecho de que se pueden vincular un máximo de 10 servidores de *vCenter*.

6.4 ADMINISTRACIÓN DE VCENTER SERVER

El servicio proporcionado por las herramientas que componen la solución de virtualización implementa la posibilidad de realizar su administración a través de una consola de gestión *web* denominada *vSphere Web Client* que permite la gestión mediante un entorno gráfico de los diferentes elementos correspondientes a *hosts* de virtualización, redes y máquinas virtuales, entre otros elementos.

De forma adicional, existe la posibilidad de administrar el servicio a través de una consola de comandos denominada *PowerCLI*.

En ambos casos, es necesario que se hayan instalado las características correspondientes en el sistema desde donde se va a realizar la administración, así como que se hayan aplicado las configuraciones de seguridad adecuadas tanto en el sistema operativo donde se ejecutarán los elementos como en el navegador *web* en caso de utilizar *vSphere Web Client*.

6.5 COMPONENTES FÍSICOS VIRTUALIZADOS

Los servicios proporcionados por *VMware vSphere* 6.7 se encargan de virtualizar los recursos físicos de los que dispone en la máquina que despliega el servicio de virtualización.

Los recursos principales virtualizados por el servicio se indican a continuación:

a) Procesadores virtuales.

b) Chipsets virtuales

c) Memoria *RAM*.

d) Interfaces IDE virtuales

e) Puertos paralelos virtuales

f) Puertos Serie virtuales

g) Controladoras PCI virtuales

h) Controladoras SATA virtuales

i) Controladoras SCSI virtuales

j) Dispositivos PCI virtuales

k) Dispositivos SCSI virtuales

l) Discos duros virtuales.

m) Adaptadores de red virtuales.

n) Unidades de CD/DVD virtuales.

o) Unidades de disquete virtuales.

p) Adaptadores de video virtuales.

q) Dispositivos de entrada de datos (ratón y teclado) virtuales.

Dentro de la arquitectura del servicio, la partición anfitriona es la encargada de realizar la virtualización de los recursos físicos indicados.

6.6 SISTEMAS OPERATIVOS VIRTUALIZADOS SOPORTADOS

El servicio de virtualización de vSphere 6.7 proporciona la creación de máquinas virtuales sobre las que se instala un sistema operativo determinado. La arquitectura del sistema operativo a virtualizar dependerá de la arquitectura hardware del sistema físico.

VMware vSphere 6.7 permite la virtualización de sistemas operativos Windows y otro tipo de sistemas operativos basados en Unix y Linux como por ejemplo Ubuntu, Suse, etc.

La lista de sistemas operativos soportados es amplia y es posible consultarla en el sitio de *VMware* a través del siguiente enlace:

a) https://www.vmware.com/resources/compatibility/search.php

6.7 VMWARE TOOLS

Una vez se ha creado e instalado el sistema operativo de una máquina virtual, existe la posibilidad de instalar de forma adicional un paquete software que incrementa la integración entre el servidor de virtualización y la máquina virtualizada. Este paquete software instala los servicios denominados *VMware Tools*.

Estos servicios de integración consisten en un conjunto de servicios que se integran en el sistema operativo de la máquina virtual y que permiten incrementar el rendimiento y la gestión de dicho sistema operativo virtual. Estos servicios dan acceso a los diferentes recursos físicos disponibles a través del servicio de virtualización.

Estos servicios de integración proporcionan soporte para varios componentes que requieren una interfaz de comunicación segura entre la partición anfitriona y la partición invitada, en la que se encuentra virtualizado el sistema operativo.

VMware Tools son una serie de servicios y módulos que permiten numerosas funciones adicionales en los productos de *VMware* para conseguir una mejor administración de los sistemas operativos invitados, así como una interacción fluida con ellos. Esta capacidad otorga la capacidad de:

a) Trasmitir mensajes, a nivel de sistema operativo entre el *host* y la máquina virtual.

b) Ejecutar scripts para la ayuda en la monitorización de las operaciones del sistema operativo invitado. Los scripts se ejecutan durante el cambio de estado de encendido de la máquina virtual.

c) Sincronizar la hora del sistema operativo invitado y la hora del sistema operativo host.

d) Empleo de controladores específicos que mejoran el rendimiento de almacenamiento, redes, gráficos y sonido.

El empleo de este conjunto de herramientas permite, entre otras, el auto escalado de la resolución de las máquinas virtuales, el uso de portapapeles entre el sistema operativo del host y el sistema operativo de las máquinas virtuales, el uso de recursos compartidos desde el *host* a la máquina virtual.

En definitiva, hacer uso de este conjunto de herramientas mejora la experiencia tanto de uso como de administración y, así mismo, mejora la relación entre el *host* y la máquina virtual.

Nota: Es posible consultar más detalle acerca del uso de *VMware Tools*, así como consultar qué sistemas operativos invitados soportan el uso de estas a través del sitio de *VMware* mediante el uso de este enlace:
https://docs.vmware.com/es/VMware-Tools/10.1.0/com.vmware.vsphere.vmwaretools.doc/GUID-14778D23-93A2-42F5-8F23-E19636827762.html

6.8 ALMACENAMIENTO DE MÁQUINAS VIRTUALES

Por cada máquina virtual gestionada por *VMware vSphere* 6.7, el servicio almacena y gestiona un conjunto de ficheros de configuración que definen las características de cada máquina virtual correspondiente.

Por defecto, los ficheros de configuración de las máquinas se encuentran alojados en el directorio *"/vmfs/volumes/"* del servidor *ESXi*. La localización de esta carpeta puede ser modificada.

Los ficheros de discos duros virtuales se encuentran alojados, por defecto, en la misma ruta donde se ha alojado la máquina virtual. Del mismo modo que con las máquinas virtuales, la localización de esta carpeta puede ser modificada.

6.9 REDES VIRTUALES

VMware vSphere 6.7 permite crear redes virtuales complejas, interconectarlas con redes físicas, establecer grupos de puertos para mejorar la eficiencia en la administración, segmentar redes, proporcionar tolerancia a fallos y conmutación por error, etcétera. La configuración de redes virtuales, a través de *vCenter,* permite hacer uso de una serie de elementos y administrarlos de forma centralizada. Los principales elementos que participan de las redes virtuales de *VMware vSphere* 6.7 son los siguientes:

a) **Redes físicas:** Interconexiones físicas entre los *hosts* ESXi y el resto de la infraestructura física. Se recomienda disponer de varias tarjetas de red físicas independientes para cada una de las posibles subredes.

b) **Redes virtuales:** Dentro de los ESXi se definen las diferentes redes virtuales que se conectan de forma lógica para enviar y recibir datos entre máquinas virtuales. Se pueden definir redes virtuales de diferentes tipos y conectar las máquinas virtuales a dichas redes mediante las tarjetas de red virtuales. Por ello, se recomienda encarecidamente realizar una segregación de redes para dividir el tráfico.

c) **Conmutadores físicos:** Administran el tráfico entre los elementos de la red física, incluidos los ESXi que participan del entorno. El conmutador detecta los *hosts* conectados a los diferentes puertos y utiliza esa información para el envío de tráfico a las máquinas físicas correctas.

d) **Conmutadores virtuales estándar:** Su funcionamiento es similar al de un conmutador ethernet físico. El conmutador detecta las máquinas virtuales conectadas de forma lógica a los diferentes puertos virtuales y utiliza esa información para el envío de tráfico a las máquinas virtuales correctas. A través de la solución *VMware vSphere* 6.7, es posible unir las redes virtuales a las redes físicas a través de los conmutadores virtuales estándar y hacia los conmutadores físicos mediante adaptadores de red físicos, denominados en *vCenter* como adaptadores de vínculo superior.

   Los conmutadores virtuales estándar no disponen de todas las capacidades que ofrece un conmutador físico. Es posible establecer **grupos de puertos estándar:** Los grupos de puertos permiten configurar parámetros como los límites de ancho de banda o directivas relativas al uso de VLAN y se establecen en cada puerto miembro del grupo. Es posible asociar un conmutador estándar a uno o más grupos de puertos.

e) **Conmutadores virtuales distribuidos:** Actúa como un solo conmutador en todos los hosts a los que ha sido asociado. Proporciona capacidades de administración, supervisión de redes virtuales y aprovisionamiento de forma centralizada. Cuando un *host* se asocia a un conmutador virtual distribuido, se crea un conmutador standard oculto, asociado a cada *host* conectado, este conmutador se denomina **Conmutador proxy** y replica la configuración de redes establecida en el conmutador distribuido a ese *host* en particular. Así mismo, por medio de estos conmutadores se puede hacer uso de **puertos distribuidos** que pueden ser conectados al host o a la tarjeta de red de una máquina virtual directamente. Este tipo de puertos, igualmente, pueden ser agrupados en **grupos de puertos distribuidos.**

f) **Equipos de *NIC*:** Es posible asociar varios adaptadores de vínculo superior a un solo conmutador, formando un equipo. Esta característica permite compartir la carga de tráfico entre redes virtuales y físicas y proporcionar conmutación por error en caso de corte de servicio de red.

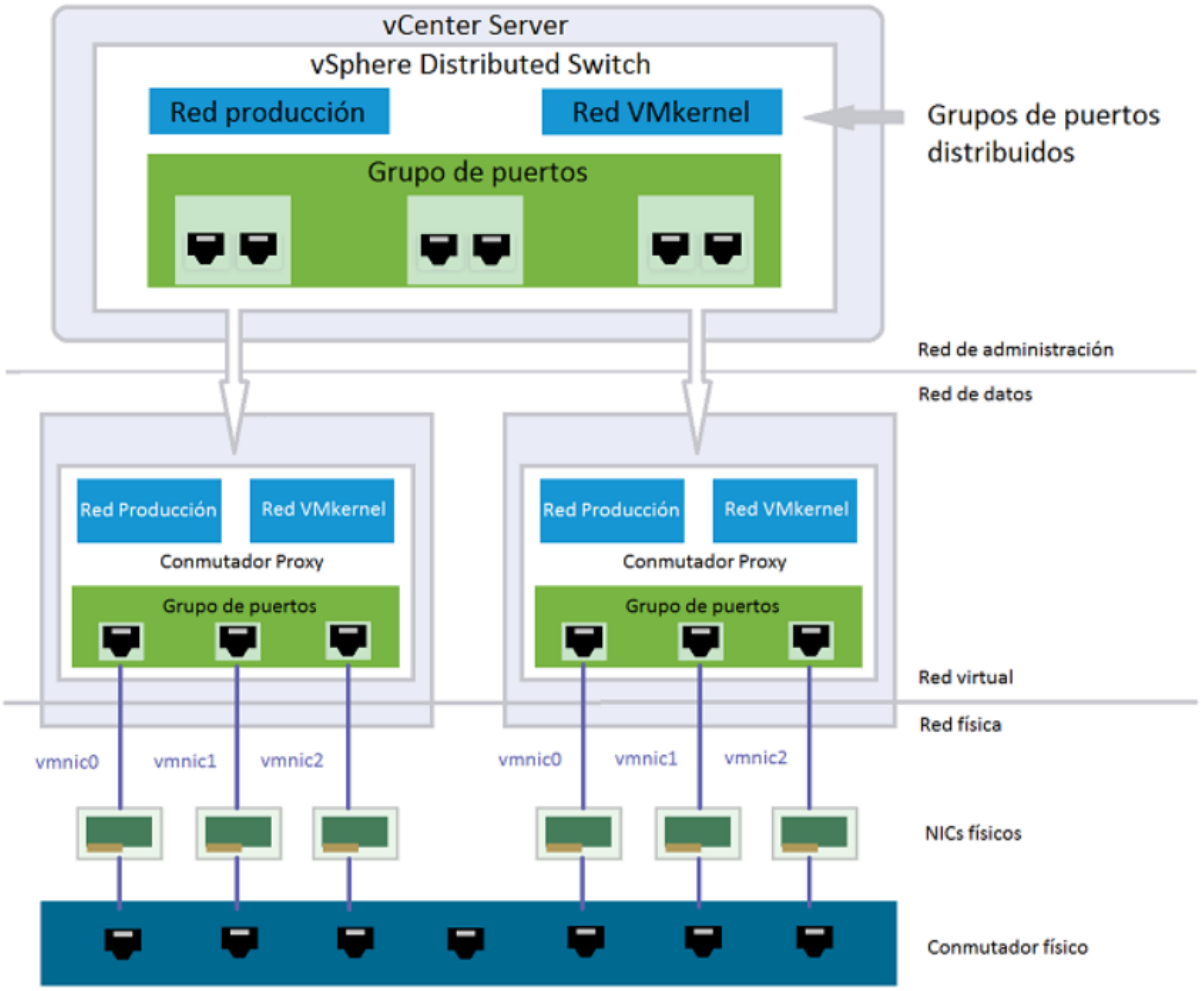
g) **VLAN**: Es posible realizar segmentos de red para que los grupos de puertos se mantengan aislados los unos de los otros. Las redes de área local virtuales son identificadas a través del uso de un número identificador (*VLAN ID*) que es utilizado para aislar el tráfico de las diferentes redes que comparten el mismo conmutador. El *VLAN ID* es un número que identifica de forma inequívoca a un segmento de red virtual. El adaptador de red configurado con el *VLAN ID* es considerado como perteneciente a una determinada red de área local virtual. Es encapsulado dentro de la trama de Ethernet. Esta es la forma por la que varias máquinas virtuales se pueden comunicar entre sí a través de diferentes redes virtuales de área local, usando el mismo adaptador físico de red.

h) **Dispositivos de filtrado:** Se recomienda desplegar dispositivos de filtrado de tráfico para

proteger tanto los interfaces de gestión del entorno VMware ESXi, como el tráfico de servicio hacia el servidor VMware ESXi y entre las máquinas virtuales. Las políticas de filtrado deberían permitir únicamente el tráfico mínimo necesario para las comunicaciones necesarias según las funcionalidades empleadas en el entorno específico de VMware ESXi.

i) **La capa de redes de VMKernel TCP/IP:** provee de conectividad a los *hosts* y controla el tráfico de diferentes elementos tales como almacenamiento IP, tolerancia a fallos o *Virtual SAN*.

Arquitectura de vSphere Distributed Switch
(Conmutador virtual distribuido)



6.10 USO DE INSTANTÁNEAS

Las instantáneas son capturas de estado de una máquina virtual para, en caso necesario, poder revertir configuraciones y volver a un estado anterior de la misma. La información que se recopila durante la creación de una instantánea incluye:

a) Propiedades de la configuración de la máquina virtual.

b) Propiedades de la red virtual.

c) El estado actual de todos los discos duros virtuales que se encuentran conectados con la partición.

d) Información del estado de la partición.

Aunque el uso esporádico aporta beneficios mayores frente a la pérdida de rendimiento, la existencia de múltiples puntos de control puede afectar muy negativamente al rendimiento debido a que la lectura de los discos duros virtuales puede requerir la comprobación de bloques ubicados en diferentes discos de diferenciación. Por lo tanto, para garantizar un buen rendimiento de E/S, se debe evitar el uso de múltiples puntos de control.

Nota: No se recomienda el uso de puntos de control en entornos de producción debido a los posibles fallos o penalización en el rendimiento del sistema.

6.11 MIGRACIÓN DE LAS MÁQUINAS VIRTUALES

Es posible mover máquinas virtuales desde una ubicación de un *host* o un almacenamiento a otra ubicación mediante una migración. Esta migración puede ser realizada "en caliente" o "en frío". Para cualquiera de los dos tipos de migraciones, deberá existir compatibilidad en lo que a tipo de procesador de *host* se refiere, si bien no es necesario que el tamaño de la memoria caché y el número de nucleos coincidan.

a) **Migración en frío:** Existe la posibilidad de mover una máquina virtual apagada o suspendida a un nuevo *host*. Del mismo modo, es posible también reubicar en nuevos lugares de almacenamiento archivos de configuración y discos para máquinas virtuales que estén apagadas o suspendidas. También es posible hacer uso de la migración en frío para mover máquinas virtuales desde un centro de datos a otro y automatizar las migraciones con tareas programadas. No es necesario que las máquinas virtuales estén en el almacenamiento compartido.

b) **Migración en caliente:** La migración en caliente se puede realizar mediante las herramientas *vMotion* o *Storage vMotion*, es posible mover una máquina virtual encendida a un *host* diferente y también mover sus discos o carpeta a un almacén de datos diferente sin que se interrumpa la disponibilidad de la máquina virtual. Es necesario que las máquinas virtuales estén en el almacenamiento compartido.

Existe la posibilidad de realizar varios tipos de migración de acuerdo con el tipo de recurso de máquina virtual, pudiendo mover todo el conjunto (máquina y almacenamiento) o solamente uno de los dos elementos.

Es posible migrar también a otro conmutador virtual o cambiar de centro de datos o de *vCenter Server*. Para poder hacer la migración entre diferentes servidores vCenter, hay que tener en cuenta una serie de requisitos:

a) Todas las instancias de origen y destino de *vCenter Server* y los *hosts ESXi* deberán utilizar la versión 6.0 o posterior de *VMware vSphere*.

b) Ciertas características de migración con *vMotion*, *vCenter* y/o instancias de *vCenter* requerirán licencia Enterprise Plus.

c) Las instancias de vCenter deberán estar sincronizadas en tiempo para que se realice correctamente la verificación de token de *vCenter SSO (Single sign on)*.

d) Ambas instancias deberán estar conectadas a un almacenamiento compartido.

e) En caso de realizar la acción a través de *vSphere Web Client*, ambas instancias deberán

estar en el mismo dominio de *vCenter SSO* para que el servidor de origen pueda autenticarse en el de destino.

6.12 CLONACIÓN DE MÁQUINAS VIRTUALES Y USO DE PLANTILLAS

La clonación de una máquina virtual consiste en la creación de una máquina virtual nueva que representa una copia de la original. La nueva máquina virtual se configura con el mismo *hardware* virtual, *software* instalado y otras propiedades configuradas para la máquina virtual original.

Las plantillas de máquina virtual se emplean para crear una imagen maestra de una máquina virtual a partir de la cual se puedan implementar varias máquinas virtuales. En definitiva, una plantilla es una máquina virtual, pero como su finalidad es utilizarla para la creación de nuevas máquinas virtuales, mientras el objeto sea una plantilla no se puede hacer uso de él hasta que no se realice la conversión a máquina virtual. Del mismo modo, las plantillas no aparecerán en "*Hosts* y Clústeres" de *vSphere Web Client* hasta que no sean convertidas en máquinas virtuales.

Las plantillas pueden ser convertidas en máquinas virtuales para hacer uso de ellas y mostrarlas como disponibles para su administración y control. Así mismo, las plantillas pueden ser clonadas para generar nuevas máquinas virtuales.

En todo momento se puede convertir una máquina virtual en plantilla y viceversa. Hay que tener en cuenta que una plantilla no está disponible en la infraestructura, por tanto, la máquina a convertir en plantilla deberá estar apagada y sin uso. En caso de querer hacer una plantilla de una máquina virtual sin perder su servicio, se puede optar por la opción de clonación a plantilla.

7. SEGURIDAD EN LOS SERVICIOS DE VMWARE VSPHERE 6.7

Las recomendaciones de seguridad detalladas a lo largo de la presente guía aplican a *VMware vSphere* 6.7. Existen una serie de elementos para tener en cuenta, relacionados con la seguridad, que son de aplicación en los distintos elementos que comprenden la solución. Los componentes que comprenden la solución deben ser seguros, en sí mismos, teniendo en cuenta los elementos de seguridad relativos a los sistemas operativos sobre los que están montados los servicios físicos (hipervisores), la seguridad de las comunicaciones de elementos físicos y elementos virtuales y la seguridad de las máquinas virtuales contenidas en la solución.

Para garantizar la seguridad, por tanto, se deberán tener en cuenta los elementos de seguridad definidos a través de la presente guía y aquellas otras guías que apliquen tanto para los sistemas operativos de máquinas físicas y virtuales como para los diferentes componentes que dichas máquinas comprendan.

Por ejemplo, a un entorno de dominio, en una red clasificada, compuesto por un servidor *vCenter* sobre Windows Server 2016 y un servidor *ESXi* que alberga un servidor Windows Server 2016 con rol de Controlador de Dominio, y a su vez un servidor miembro Windows Server 2016 con rol de servidor de impresión y una serie de equipos clientes Windows 10 1809 le serían de aplicación las siguientes guías (y todas aquellas relativas a servicios y aplicaciones adicionales que fueran instalados en los equipos):

a) La sección de la guía CCN-STIC-570A de Controlador de Dominio para el servidor virtual que contiene el rol de controlador de dominio.

b) La sección de la guía CCN-STIC-570A de servidor miembro tanto para el servidor que

alberga vCenter Server como para el servidor de impresión.

c) La guía CCN-STIC-572 para el rol de servidor de impresión sobre Windows Server 2016.

d) La presente guía para el servidor de ESXi y lo relativo al servicio de vCenter en el servidor Windows Server 2016 con rol de vCenter.

e) La guía CCN-STIC-599A19 para los equipos clientes Windows 10.

f) Todas aquellas guías que pudieran ser de aplicación atendiendo a las medidas de seguridad TIC a implementar en sistemas clasificados que se definen en la guía CCN-STIC-301.

El detalle y concreción de las medidas de seguridad que se deberán adoptar para el entorno, irán definidos por el nivel que se haya establecido atendiendo al definido siguiendo las directrices del Esquema Nacional de Seguridad, que serán especificadas en el anexo correspondiente, o a las normas establecidas para redes clasificadas si procede.

Sirva el contenido de este apartado como introducción a los parámetros de seguridad que se tendrán en cuenta para establecer las configuraciones que proporcionen el entorno adecuado al nivel de seguridad requerido mediante los anexos relativos a los distintos niveles de seguridad. En dichos anexos se abordarán los elementos de seguridad, aquí mencionados, de forma concreta e incluyendo los valores deseados según el nivel de seguridad a establecer. Así mismo, en dichos anexos se incluirá la guía paso a paso que permita implementar cada uno de los elementos de seguridad, así como una lista que permitirá comprobar el nivel de cumplimiento.

Existen múltiples características, de terceros, no proporcionadas por la solución y que será necesario gestionar para aportar la seguridad de los elementos que componen la infraestructura de *VMware vSphere* 6.7 al entorno en el que éstos operan. Tales como autenticación, autorizaciones y cortafuegos. Es posible utilizar dichas herramientas para alcanzar el nivel de seguridad deseado definiendo permisos en objetos relacionados con *vCenter* (Servidores *vCenter*, *hosts ESXi*, máquinas virtuales y elementos de comunicaciones y almacenamiento. En este apartado, se tiene este hecho en cuenta a la hora de enumerar y analizar los diferentes elementos que deberán intervenir en la seguridad.

7.1 SEGURIDAD EN EL SERVIDOR DE VCENTER

El servidor de *vCenter* se protege mediante la autenticación a través de *vCenter* SSO (*single sign on*) y a través del modelo de permisos. Es posible modificar los comportamientos y establecer unos parámetros adicionales que limiten el acceso al entorno.

Del mismo modo que se otorgan medios de protección al servidor *vCenter,* se ha de considerar que todos aquellos servicios relacionados y asociados a las instancias de *vCenter Server* deberán ser protegidos también.

7.2 SEGURIDAD EN LOS HIPERVISORES ESXI

La seguridad que deberá aplicar en los servidores *ESXi* debe ser tratada, en gran medida, mediante elementos externos a la solución. Si bien es cierto que es posible proteger los servidores haciendo uso del "*Lockdown Mode*" o "Modo de bloqueo" y de algunas otras características incluidas en la solución, como se podrá comprobar en los siguientes apartados. Se puede mejorar la protección de los *hosts ESXi* mediante las siguientes acciones:

a) **Acceso limitado a ESXi:** Por defecto, la shell de comandos de ESXi y el acceso por SSH no están habilitados, siendo únicamente el usuario root el que podría ejecutar comandos de administración mediante acceso directo al servidor a través de la DCUI (*Direct Console User Interface*). En caso de necesitar habilitar estos accesos, se pueden establecer tiempos de conexión para limitar el riesgo de acceso no autorizado al sistema.

   Existe la posibilidad de activar temporalmente tanto el acceso a través de SSH como el uso de la Shell de comandos pudiendo definir la cantidad de minutos que estará activo dicho acceso. Así mismo, es posible establecer el tiempo de inactividad para que se deshabilite el acceso remoto o incluso reiniciar los agentes de administración de modo que todos aquellos programas que permiten la administración remota sobre este host se reiniciarán y, de este modo, todas las conexiones realizadas al ESXi se desconectarán. Si bien es cierto, que dicho reinicio afectará a aquellos servicios que se encuentren en ejecución alterando la ejecución de los mismos.

b) **Usuarios y privilegios:** El usuario root puede ejecutar muchas tareas por defecto, por lo que se debería limitar o prohibir que los usuarios administradores emplearan la cuenta. En lugar de eso se deberían usar usuarios administradores nominales, individuales para cada usuario, y asignarle los privilegios específicos a su puesto. *vCenter* permite realizar estas tareas a través de la creación de roles personalizados.

   Es posible entregar permisos específicos a los usuarios que accedan al *host* mediante el servidor de *vCenter* que administra dicho *host*.

   En caso de administrar los usuarios directamente desde el *host,* las opciones de administración de roles son mucho más limitadas. Para ello, los diferentes roles y privilegios deberán ser tratados de forma personalizada estableciendo específicamente aquello a lo que se tiene permiso y, por tanto, se deberá evitar hacer uso de grupos o roles administrativos predefinidos.

   Para reforzar la seguridad de vCenter Server, VMware ha reemplazado el uso de la cuenta de servicio local por una serie de cuentas de servicio virtuales. Definiendo una cuenta de servicio individual para cada uno de los servicios que ejecuta. Este hecho limita la vulnerabilidad de la solución ya que en caso de que una cuenta se vea comprometida, esta no permite operar sobre el resto de los servicios.

   En caso de estar haciendo uso de un sistema de dominio de Directorio Activo, se deberá otorgar el privilegio de iniciar sesión como servicio tanto a la cuenta de servicio definida durante la instalación de vCenter como al grupo "NT SERVICES\ALL SERVICES".

   Así mismo, la cuenta de servicio definida como principal durante la instalación de la solución deberá tener privilegios de administración sobre el equipo servidor sobre el que se haya implementado vCenter Server.

c) **Puertos de Firewall:** Los puertos en el host solo se abren en el momento en el que se

inicia un determinado servicio. Es posible comprobar y administrar el estado de los puertos del firewall a través de *vSphere Client*, *ESXCLI* (consola de comandos específica de administración de *ESX*) o *PowerCLI (*Módulo de *PowerShell* de control remoto de *ESX* y *vCenter).*

Es por ello, que el servidor ESXi requiere una serie de puertos habilitados en el firewall para poder establecer las comunicaciones con el resto del entorno de virtualización. A continuación, se detallan los puertos requeridos según los diferentes protocolos que sea necesario utilizar, este hecho no implica la necesidad de apertura de los puertos enumerados. Solamente deberá abrirse la comunicación en aquellos puertos que sean requeridos porque se haga uso del protocolo específico. Esta lista deberá ser adaptada a las necesidades del entorno a implementar.

Descripción	Tipo de conexión	Protocolo	Puerto
Servidor CIM	Entrante	TCP	5988
Servidor CIM seguro	Entrante	TCP	5989
CIM SLP	Entrante, saliente	TCP, UDP	427
DVSSync	Entrante, saliente	UDP	8301, 8302
HBR	Saliente	TCP	44046, 31031
NFC	Entrante, saliente	TCP	902
WOL	Saliente	UDP	9
Servicio de clústeres de vSAN	Entrante, saliente	UDP	12345, 23451
Cliente DHCP	Entrante, saliente	UDP	68
Cliente DNS	Entrante, saliente	UDP	53
Fault Tolerance	Entrante, saliente	TCP, UDP	8200, 8100, 8300, 80
Cliente iSCSI de software	Saliente	TCP	3260
Transporte de vSAN	Entrante, saliente	TCP	2233
Servidor SNMP	Entrante	UDP	161
Servidor SSH	Entrante	TCP	22
vMotion	Entrante, saliente	TCP	8000
vSphere Web Client, vCenter Agent	Entrante, saliente	TCP	902, 443
vsanvp	Entrante, saliente	TCP	8080
vSphere Web Access	Entrante	TCP	80
protocolo RFB	Entrante	TCP	5900-5964
vSphere Update Manager	Entrante	TCP	80, 9000
Servicio de filtro de E/S	Saliente	TCP	9080

Se deberá establecer una auditoría que registre el uso de los diferentes puertos que usa ESXi.

El servidor con el rol VMware vCenter requiere una serie de puertos habilitados en el firewall para poder establecer las comunicaciones con el resto del entorno de virtualización. A continuación, se detallan los puertos que se pueden definir durante la instalación del producto.

Descripción	Puerto
Puertos comunes	

Descripción	Puerto
Puerto HTTP	80
Puerto HTTPS	443
Puerto de servicio Syslog	514
Puerto de servicio TLS Syslog	1514
Puertos de Platform Services Controller	
Puerto de servicio de token seguro	7444
Puertos vCenter Server	
Puerto de administración Auto Deploy	6502
Puerto de servicio Auto Deploy	6501
Puerto ESXi Dump Collector	6500
Puerto ESXi Heartbeat	902
Puerto vSphere Web Client	9443

A continuación, se detallan los puertos requeridos según los diferentes protocolos que sea necesario utilizar, este hecho no implica la necesidad de apertura de los puertos enumerados. Solamente deberá abrirse la comunicación en aquellos puertos que sean requeridos porque se haga uso del protocolo específico. Esta lista deberá ser adaptada a las necesidades del entorno a implementar.

Puerto por defecto			
22	53	80	88
389	443	514	636
902	1514	2012	2014
2015	2016	2020	5480
5580	5583	6500	6501
6502	7080	7081	8200
8201	8300	8301	8084
9084	9087	9443	10090
10095	10096	10097	12721

Puede consultar más información sobre los puertos que utiliza la solución a través del sitio web de VMware en el siguiente enlace:

https://docs.vmware.com/es/VMware-vSphere/6.7/com.vmware.vcenter.upgrade.doc/GUID-925370DD-E3D1-455B-81C7-CB28AAF20617.html

d) **El protocolo IPv6**: se encuentra habilitado por defecto en los servidores ESXi, ya que IPv4 sigue siendo el protocolo nativo y preferido por el sistema operativo. Con objeto de reducir la superficie de ataque del servidor, se recomienda deshabilitarlo siempre y cuando su uso no sea necesario.

e) **Uso del modo de bloqueo:** Cuando el *host* está operando en modo de bloqueo (*LockDown Mode*), éste solamente es accesible a través de *vCenter.* Es posible especificar entre dos modos de bloqueo, normal o estricto y es posible establecer un grupo con una lista específica de usuarios que pueden acceder directamente. Esto se utiliza, a menudo, para cuentas de servicio, como sería un agente de *backup*, de modo que el acceso de estas no quede bloqueado.

Una medida de seguridad importante sería auditar la pertenencia a este grupo para evitar accesos no autorizados.

f) **Uso de certificados:** Por defecto, la entidad certificadora *VMware Certificate Authority* (*VMCA*) aprovisiona a cada host *ESXi* con un certificado firmado por ella como entidad raíz. En caso de que sea requerido, existe la posibilidad de reemplazar dichos certificados por los que la política de la organización requiera, siendo válidas las entidades certificadoras de la organización o de terceros.

g) **Autenticación vía tarjeta inteligente:** *ESXi* 6.7 permite el uso de tarjetas inteligentes como método de autenticación. Para mejorar la seguridad es posible implementar este método e incluso establecer doble factor mediante RSA SecurID de autenticación a través de *vCenter*.

h) **Bloqueo de cuentas:** Es posible administrar el bloqueo de las cuentas de acceso al servidor *ESXi* a través de SSH o mediante los servicios *Web* de *vSphere*. Esta configuración está establecida por defecto en 10 intentos y dos minutos de bloqueo.

i) **Registros o logs:** Por defecto, los registros de eventos del sistema *ESXi* están configurados de modo que diariamente se vacían los ficheros que los mantienen. Se deberá modificar, por tanto y en caso de que así se necesite, dicho comportamiento para que el almacenamiento de los registros sea persistente. Así mismo, se pueden establecer parámetros para la recolección de logs según las necesidades. Esto es posible a través del vSphere client y también mediante comandos.

j) **Uso de *SNMP*:** En caso de no ser necesario su uso, debería permanecer deshabilitado por las implicaciones de seguridad que provoca. En caso de ser utilizado, se puede establecer un modo seguro para que el envío de información de monitorización solo sea recibido por el objeto adecuado. En caso de no configurar *SNMP* de forma correcta, un atacante puede extraer información que posteriormente pueda ser utilizada para planear un ataque. *VMware vSphere* 6.7 soporta *SNMPv3*. Su uso proporciona mayor seguridad que las versiones anteriores del protocolo, incluyendi autenticación porclaves y cifrado.

k) **Uso de *MOB:*** El *Managed Object Browser* o Navegador de objetos administrados, es una interfaz gráfica que permite la navegación entre objetos de un servidor que no solamente permite consultarlos sino también modificar comportamientos. Proporciona un modo de explorar el modelo de objetos utilizado por el VMkernel para administrar el *host*. En principio, esta interfaz no se debe usar habitualmente, solamente en caso de estar depurando la *SDK* de *vSphere* y, por defecto, se mantiene desactivada.

7.3 USO DE VCENTER SSO (INICIO DE SESIÓN ÚNICO)

El uso de *Single Sign On* proporciona protección de credenciales y accesos. Durante la primera instalación es posible establecer una contraseña para el dominio de *vCenter SSO*. En primera instancia solamente este dominio está disponible para poder realizar la gestión de identidades. Es posible establecer otras fuentes de origen de identidades como Directorio Activo o *LDAP* y establecer el método por defecto. De este modo, la gestión de identidades y privilegios puede ser más específica permitiendo el acceso a usuarios a objetos a los que están autorizados.

Mediante el dominio de SSO, es posible definir tiempo de expiración, complejidad de contraseña, política de bloqueo, etc.

7.4 USUARIOS Y PRIVILEGIOS

Del mismo modo que en los servidores *ESXi*, se debería asociar cada permiso que se entrega a un objeto nominal, sea usuario o grupo, que tenga asociado un rol, predefinido o personalizado, pero con privilegios concretos. El modelo de permisos de *VMware vSphere* 6.7 proporciona una gran flexibilidad a través de muchas formas de autorización de usuarios y grupos.

La restricción de privilegios administrativos y evitar el uso de la cuenta que posee el rol de administrador son métodos que permiten controlar los accesos pudiendo auditar los mismos y evitar accesos no autorizados. Por ello, se deberá de evitar el uso de usuarios genéricos como, por ejemplo, el usuario ROOT que deberá ser deshabilitado.

Los diferentes roles y privilegios deberán ser tratados de forma personalizada estableciendo específicamente aquello a lo que se tiene permiso y, por tanto, se deberá evitar hacer uso de grupos o roles administrativos predefinidos. Adicionalmente, se deberá establecer un control de pertenencia al grupo de excepción en modo de bloqueo.

En el caso de que se realicen implementaciones de configuraciones de hosts a través de los perfiles de host (cuyo uso está recomendado tanto por reducción de costes administrativos como por seguridad), se recomienda el uso de un servicio de vSphere Authentication Proxy para evitar el almacenamiento de credenciales en el perfil y la transmisión de éstas a través de la red. No es objeto de esta guía la configuración de este servicio adicional, pero se recomienda su uso en caso de que el entorno lo permita o requiera.

7.5 USO DE SERVICIO DE NTP

Desde *vCenter* es posible habilitar el uso del servicio *NTP* para cada nodo. Esta configuración es importante de cara al correcto funcionamiento de la infraestructura de certificados, ya que esta infraestructura no funciona correctamente en caso de que los nodos no tengan bien sincronizada la hora.

7.6 USO DE TLS

VMware vSphere 6.7, por defecto, solamente hace uso de *TLS* 1.2. Los protocolos anteriores se mantienen deshabilitados. Es posible hacer uso de la utilidad de configuración de *TLS* para habilitar las versiones anteriores del protocolo en caso de existir necesidades para ello. El comportamiento seguro sería mantener los protocolos anteriores, menos seguros, de forma temporal hasta que todas las conexiones estén habilitadas para utilizar *TLS* 1.2.

7.7 SEGURIDAD EN MÁQUINAS VIRTUALES

Para establecer las medidas de seguridad correctamente, las máquinas virtuales deberán ser actualizadas, así como los elementos de protección que se usan en condiciones normales para el bastionado de las máquinas físicas a las que corresponden.

Los principios que se tienen en cuenta de cara a la seguridad de la máquina virtual obedecen a deshabilitar las funcionalidades innecesarias, minimizar el uso de la consola de máquina virtual y seguir una serie de mejores prácticas definidas a continuación:

a) **Proteger el sistema operativo huésped:** Tal y como se ha descrito, la protección del sistema operativo huésped conlleva la aplicación de parches de seguridad y, si es de

aplicación en el entorno deseado, el uso de herramientas que impidan la ejecución de software malicioso. Así mismo, son de aplicación las medidas indicadas en la guía de seguridad que corresponda al sistema operativo. De este modo, en caso de disponer, por ejemplo, de una máquina virtual con sistema operativo huésped *Windows Server* 2016, le será de aplicación lo especificado en la guía de seguridad CCN-STIC-570 A o B según el entorno en el que se disponga.

b) **Deshabilitar funcionalidades innecesarias:** Se deberá comprobar que aquellas funcionalidades que no están en uso no se mantienen habilitadas para reducir la superficie de ataque. Muchas funcionalidades como roles, características, aplicaciones o protocolos, en el sistema operativo cliente, así como algunas funcionalidades desde el *host* hasta la máquina virtual como podrían ser HGFS *(host-guest filesystem*, recurso compartido entre el *host* y la máquina virtual) o la posibilidad de copiar y pegar entre la máquina virtual y aquella desde la que se está accediendo a la consola deberán ser deshabilitadas, si su uso no es necesario.

c) **Uso de la consola (*Virtual Machine Console*):** Los usuarios que pueden acceder a la consola tienen control sobre la máquina virtual para administrar la energía y la conectividad a dispositivos extraíbles. Conectar a las máquinas virtuales a través de la misma podría permitir ataques maliciosos a una máquina virtual.

d) **Uso de arranque seguro UEFI:** Las máquinas virtuales en VMware vSphere 6.7 permiten el uso del arranque seguro UEFI siempre que el sistema operativo invitado lo permita. Es posible seleccionar esta opción en las máquinas virtuales para añadir más seguridad. Se recomienda hacer uso de dicha característica debido a la comprobación que realiza de software no confiable, software no firmado a través de certificados por Microsoft y VMware, arrancando solo componentes con firma válida. El arranque se detendría en caso de que alguno de los componentes no mostrara una firma válida o esta no existiera.

e) **Uso de capacidades 3D:** VMware vSphere 6.7 entrega capacidades específicas de GPU virtual con el fin de ser utilizadas en máquinas virtuales que tengan mucha carga de trabajo en elementos gráficos, tales como equipos de diseño gráfico o modelado 3D. En caso de no ser necesario su uso, estas características deberían permanecer desactivadas.

f) **Configuración de componentes de uso poco frecuente:** Los puertos serie o paralelo, los disquetes virtuales y, en definitiva, cualquier componente que no esté en uso y no sea necesario para el funcionamiento de una máquina virtual, debería mantenerse desactivado. Cualquier componente activado representa un canal potencial de ataque.

g) **Información del *host* en la máquina virtual:** Existe la posibilidad de habilitar que la máquina virtual obtenga información del *host* a través de las opciones avanzadas de la configuración de dicha máquina virtual. Si no es necesaria la obtención de información, esta es otra característica que debería mantenerse deshabilitada, en cualquier caso.

h) **VMware Direct path I/O:** Esta característica permite hacer uso de un dispositivo *PCI* del *host* a la máquina virtual de forma directa. A nivel de rendimiento y operatividad puede suponer una ventaja, pero a nivel de seguridad puede resultar en una vulnerabilidad potencial conocida. Existen casos en los que el uso de esta característica puede resultar necesario. A través de *vSphere client* o la consola de comandos, es posible controlar el uso de dicha característica para auditarlo.

i) **Cifrado de máquinas virtuales:** *VMware vSphere* 6.7 permite el cifrado de máquinas virtuales. El cifrado no solamente se encarga de proteger la propia máquina virtual, sino

también los discos de las máquinas y otros archivos. Si se establece una conexión de confianza entre el servidor de *vCenter* y un servidor de administración de claves, se podrían recuperar claves del *KMS* en caso de ser necesario.

Los componentes que posibilitan este sistema son el *KMS*, *vCenter Server* y los *hosts ESXi*. Los diferentes aspectos del cifrado de las máquinas virtuales se administran de diferentes formas:

i. Es posible administrar la instalación de la conexión de confianza con el KMS a través de vSphere Client.

ii. Es posible hacer uso, así mismo, del comando *crypto-util* directamente a través del *host ESXi.*

Gracias a esta herramienta, es posible crear máquinas virtuales cifradas o cifrar máquinas ya existentes. Solamente los usuarios administradores con privilegios de cifrado podrán realizar tareas específicas de cifrado y descifrado de máquinas virtuales y sus discos.

7.8 SEGURIDAD EN LA CAPA DE RED VIRTUAL

La capa de red virtual incluye adaptadores de red virtuales, conmutadores de red virtuales, conmutadores virtuales distribuidos, puertos y grupos de puertos. *ESXi* emplea la capa de red virtual para el soporte de comunicaciones de las máquinas virtuales. Del mismo modo. *ESXi* hace uso de la capa de red virtual para las comunicaciones con iSCSI, SANs, almacenamiento NAS, etc.

vSphere incluye una serie de características necesarias para proporcionar una infraestructura de red segura. Es posible las medidas de seguridad a cada uno de los elementos de la infraestructura de red virtual como conmutadores, conmutadores distribuidos o adaptadores de red por separado.

a) **Aislamiento del tráfico de red:** El aislamiento del tráfico es esencial para la seguridad de un entorno de *ESXi.* Las diferentes redes requieren de diferentes accesos y niveles de aislamiento. Una red de administración aísla su tráfico de la red de clientes o de una red de almacenamiento, por ejemplo. Para un entorno seguro, se deberá asegurar que la red de administración solo sea accesible por usuarios autorizados tales como administradores de Sistemas, redes y seguridad.

b) **Uso de cortafuegos en elementos virtuales de red:** Es posible abrir y cerrar puertos del cortafuegos de forma separada en cada uno de los elementos de la red virtual. Para los hosts *ESXi*, las reglas de *firewall* asocian los servicios con los cortafuegos correspondientes de acuerdo con el estado del servicio.

   Así mismo, es posible abrir puertos en las instancias de *vCenter* específicamente.

c) **Uso de políticas de seguridad de red:** Las políticas de seguridad de red proporcionan protección del tráfico contra ataques de suplantación de *MAC* o escaneos de puertos. La política de seguridad aplicable a los conmutadores, tanto estándar como distribuidos, es implementada en la capa dos o de enlace. Los elementos que incluye la política de seguridad incluyen control sobre el modo promiscuo, los cambios de dirección *MAC* y las transmisiones forjadas. Si se rechazan las transmisiones forjadas el *host* comparará la *MAC* de origen y rechazará las transmisiones que impersonalicen la *MAC* y solo aceptará aquellas que estén identificadas con la *MAC* correcta.

d) **Seguridad en los elementos de red de la máquina virtual:** Se pueden emplear diferentes métodos para establecer seguridad en los elementos de red de la propia máquina virtual. En primer lugar, tal y como se especifica en la guía que corresponda al sistema operativo instalado en la misma, se modificarán parámetros tales como el impedimento del uso de IPv6 o deshabilitar aquellos protocolos en el propio adaptador de red que no vayan a ser utilizados. Así como que las máquinas virtuales funcionen en un entorno confiable. Los conmutadores estándar y distribuidos proporcionan una protección considerable si se usan en conjunto con otras prácticas de seguridad como la adición de cortafuegos.

e) **Uso de *VLAN*:** El uso de *VLAN* permite segmentar una red física. Es posible hacer uso de *VLANs* para proteger la red de la máquina virtual o la configuración de almacenamiento. Mediante el uso de *VLANs,* dos máquinas virtuales que se encuentren dentro de la misma red no podrán intercambiar paquetes entre ellas hasta que no se defina que las dos se encuentren en la misma *VLAN*.

f) **Seguridad en conexiones a almacenamiento virtualizado:** Las máquinas virtuales almacenan ficheros de sistema, archivos de programa y otros datos en los discos duros virtuales. Cada disco duro virtual se muestra a la máquina virtual como un dispositivo SCSI conectado a una controladora SCSI. La máquina virtual está aislada de los detalles del almacenamiento y no puede acceder a la información relativa a la LUN donde se encuentra el disco virtual.

   VMFS (Virtual Machine File System) o Sistema de ficheros de la máquina virtual es un sistema de ficheros distribuido que presenta volúmenes al *host ESXi.* Por ejemplo, en caso de que el almacenamiento que se esté utilizando sea de tipo iSCSI, la conexión a dicho almacenamiento podrá configurarse para hacerla segura mediante el uso de CHAP. Esto puede ser configurado a través de *vSphere Client* o la consola de comandos.

g) **Uso de *IPSec*:** No es posible hacer uso de *IPSec* a través de TCP/IPv4 en *ESXi*.

h) **Uso de filtro *BPDU*:** VMware vSphere 6.7 proporciona la posibilidad de habilitar el filtro de *BPDU (Bridge Protocol Data Unit)* o Unidad de Datos de Protocolo Puente. Activándolo, es posible detectar bucles en la red y evitar, por tanto, la recepción de paquetes de datos no autorizados que podrían contener software malicioso.

i) **Uso de NetFlow:** A través de la herramienta, es posible especificar la dirección o direcciones IP que podrán recolectar datos de monitorización a través de este protocolo.

j) **Uso del modo promiscuo:** Los interfaces de red pueden ser configurados en modo promiscuo, de modo que acepten todo el tráfico de red, tanto el destinado a su dirección *MAC* o a cualquier otra. Puede ser habilitado, del mismo modo, en conmutadores virtuales estándar y distribuidos.

   Cuando se habilita este modo en un conmutador virtual asociado a una interfaz de red, cualquiera de las máquinas virtuales conectadas a dicho conmutador podrá capturar el tráfico envidado a través de él o a través de la red física en que reside la interfaz de red asociada. El valor, por defecto, cuando se crean conmutadores de red y otros dispositivos es no permitir el modo promiscuo.