CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN MICROSOFT HYPER-V SOBRE WINDOWS SERVER 2016

FEBRERO 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.02.15 12:43:15 +01'00'

NIPO:083-19-118-7
Fecha de Edición: febrero de 2019

Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

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 en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su 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, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

febrero de 2019

Félix Sanz Roldán
Secretario de Estado
Director 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 para entornos basados en los productos y sistemas operativos de Microsoft (CCN STIC 500), 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.

La serie CCN STIC 500 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.

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 2012 R2, 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 Server 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 Server 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 implementar y garantizar la seguridad para una instalación de Hyper-V en un Sistema "Windows Server 2016" actuando como servidor miembro de un dominio.

La configuración que se aplica a través de la presente guía se ha diseñado para ser 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.

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" del "ANEXO B" de la guía codificada como CCN-STIC-570A para realizar los pasos adecuados.

Esta guía asume que el servidor de Hyper-V va a ser implementado sobre un equipo con Windows Server 2016 Standard de 64 Bits donde se ha seguido el proceso de implantación de seguridad definido en el documento codificado como "CCN-STIC-570A".

Cumpliendo con estos requisitos previos, puede iniciar la instalación del servidor de Hyper-V basado en Microsoft Windows Server 2016 Standard.

Así mismo, no se contempla en esta guía la instalación del servicio de Hyper-V 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 una implementación del servicio de Hyper-V sobre Microsoft Windows Server 2016 Standard en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración para el mantenimiento y gestión de máquinas virtuales, así como de la configuración de los servicios utilizados por los entornos virtualizados, entre otros aspectos, además de aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento del servicio.

El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo.

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del dominio en Windows Server 2016.

d) Un controlador de dominio basado en Windows Server 2016 Standard.

e) Un servidor miembro del dominio basado en Windows Server 2016 Standard.

f) La instalación del servicio de Hyper-V se realiza en modo limpio, es decir, no se contemplan procedimientos de migración desde versiones anteriores.

g) No se contemplan mecanismos de alta disponibilidad ni balanceo de carga en el escenario planteado.

Este documento incluye:

a) **Descripción de las nuevas funcionalidades** para todos aquellos operadores que tengan experiencia en la versión previa de Hyper-V.

b) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada en caso de ser necesario.

a) **Mecanismos para la aplicación de configuraciones**. Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello, tales como las plantillas de seguridad.

b) **Mecanismos para la creación de cuentas necesarias para la funcionalidad de la solución**. Tanto los procesos de implementación como de instalación requieren de cuentas específicas; se ha automatizado el proceso de creación de dichas cuentas.

c) **Descripción de la seguridad en el servicio de Hyper-V**. Completa la descripción de los mecanismos de seguridad, autenticación y autorización utilizados en Hyper-V sobre Windows Server 2016, así como las medidas para reforzar dicha seguridad.

d) **Guía paso a paso**. Va a permitir implantar y establecer las configuraciones de seguridad de un servidor de Hyper-V en Windows Server 2016.

e) **Guía de administración**. Va a permitir realizar tareas de administración en el entorno de seguridad establecido.

f) **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.

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 para la instalación de Hyper-V, será necesario cumplir los requisitos definidos para MS Windows Server 2016

además de ser necesario comprobar los requisitos de otros servicios y aplicaciones que se vayan a aplicar posteriormente, especialmente requisitos relacionados con la creación y gestión de máquinas virtuales. En la mayoría de los productos y/o servicios se recomienda tener en particiones distintas para el sistema operativo y el resto de ficheros del servicio proporcionado.

b) Si el entorno que el que está aplicando seguridad pertenece a una red clasificada, se deberá realizar la aplicación de seguridad del sistema operativo antes de instalar el rol de Hyper-V. Para ello será necesario aplicar la guía de seguridad codificada como CCN-STIC-570A y a continuación se deberá instalar y configurar el rol de servidor Hyper-V de Windows Server 2016 tal y como se describe en la presente guía.

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

d) 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

Los contenidos de esta guía son de aplicación a equipos tipo puesto servidor con Sistema Operativo Windows Server 2016, en castellano, con el objetivo 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 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, es posible que deba 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.

La guía ha sido probada y verificada con la versión de Hyper- V sobre el sistema operativo Windows Server 2016 Standard aplicando la guía CCN-STIC-570A para la configuración del Sistema operativo. También sería válida para una versión de Hyper V sobre Windows Server 2016 Datacenter. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2016 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor podría llegar a implementarse la siguiente guía sobre la versión Datacenter. Las diferencias entre estas versiones serán tratadas en el punto “6 HYPER-V” de la presente guía.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación del rol de Hyper-V en un entorno de dominio de Active Directory.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma Windows Server 2012 R2 con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320:

   i. Intel Pentium Xeon CPU ES 2430 2.20GHz.

   ii. HDD 1TB.

   iii. 64 GB de RAM.

   iv. Interfaz de Red 1 GB.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos mínimos de Windows Server 2016 Standard. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2048 MB (2GB) de memoria RAM.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios, roles o características deseadas.

Así mismo, hay que tener en cuenta que el rol de Hyper-V requiere, para un entorno de producción, un mínimo de 4 GB de memoria RAM para funcionar adecuadamente, aunque se recomienda implementar más, en función de los requisitos necesarios de virtualización.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima en caso de redes clasificadas y la seguridad mínima 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 deseadas en Microsoft Windows Server 2016.

Para garantizar la seguridad de los clientes y servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Microsoft Update. Las actualizaciones, por lo general, se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento.

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 albergue el servidor de Hyper-V 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 MS Hyper-V posee un servidor MS Windows 2016 que implemente el rol de controlador de dominio, éste deberá poseer la configuración de seguridad de 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 sistema Microsoft Windows Server 2016 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:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter con el rol de servidor Hyper-V a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter con el rol de servidor Hyper-V 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 implementación.

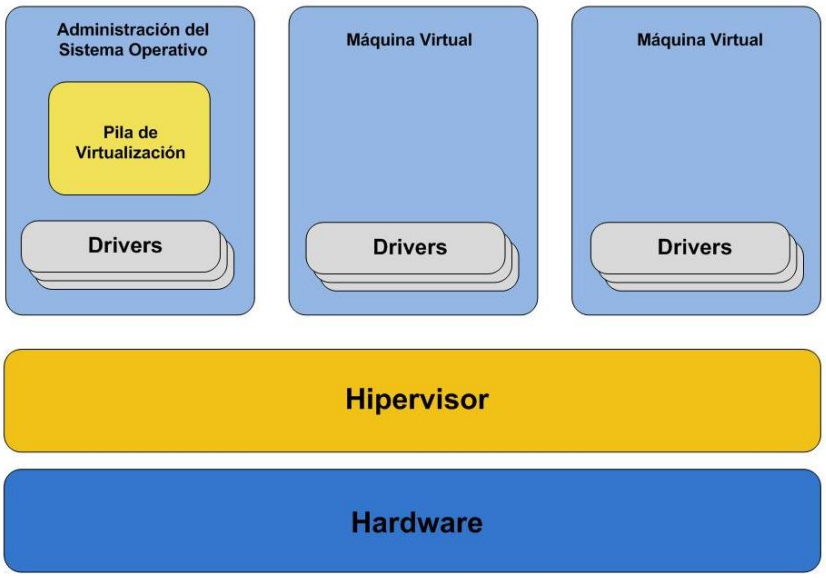
De manera adicional, en cada una de las carpetas “Scripts” que se adjuntan a los documentos, existe un directorio que almacena un informe en formato HTML con cada objeto de directiva de grupo (GPO) o directiva de grupo local (GPL) que se aplica durante el paso a paso de la guía.

6. HYPER-V

Los sistemas 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 la solución de virtualización propietaria de Microsoft, Hyper-V.

Hyper-V es un hipervisor que 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) y el sistema operativo que se ejecuta dentro del entorno virtualizado (también conocido como máquina virtual 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.

Una vez se ha habilitado el servicio Hyper-V por primera vez dentro del sistema MS Windows Server 2016, y éste se ha reiniciado, la instancia del sistema operativo se convierte en un entorno virtual. En concreto, esta instancia del sistema MS Windows Server 2016 se denomina "sistema operativo de administración", y es la encargada de gestionar y administrar el resto de máquinas virtuales creadas y desplegadas por el servicio Hyper-V.



El hipervisor (en inglés, hypervisor), 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. Tal y como se puede observar en la imagen, el hipervisor no acepta código de terceros (drivers de dispositivos, …), situándose éste dentro de cada entorno virtualizado. De esta forma, se proporciona una mayor seguridad al hipervisor.

El hipervisor se divide en dos capas diferentes. La capa inferior, corresponde a la implementación de un microkernel que soporta acceso a memoria, uso de hilos, uso de señales y un mecanismo de abstracción del hardware; mientras que la capa superior, se encarga de proporcionar los servicios de virtualización.

El hipervisor se puede invocar a través de:

a) Señales de interrupción (en inglés, interrupts), que son eventos asíncronos. Son redirigidas por el hipervisor al sistema operativo virtual correspondiente.

b) Señales de interceptación (en inglés, intercepts), que son eventos síncronos para comunicarse con uno de los sistemas virtualizados por el servicio.

c) Llamadas de hipervisor (en inglés, hypercalls), que es una interfaz programática con el hipervisor. Son análogas a las llamadas al kernel.

6.1 BENEFICIOS

La virtualización realizada por Hyper-V, proporciona diferentes beneficios tanto técnicos como de gestión, que 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 Hyper-V.
d) Los recursos físicos son gestionados por Hyper-V para proporcionar entornos totalmente aislados.
e) Implementación de entornos de escritorios virtuales a través de VDI.
f) Posibilidad de crear entornos de testing o prueba sin que sea necesario obtener equipamiento hardware complejo y costoso.

6.2 CARACTERÍSTICAS

Las características principales de Hyper-V se detallan a continuación:

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.

Nota: Para obtener más información acerca de las características de Hyper-V, puede consultar la Web de Microsoft a través de la siguiente dirección: https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/Hyper-V-on-Windows-Server
Si desea obtener información de las mejoras del servicio de Hyper-V con respecto a MS Windows Server 2012 R2, consulte la Web de Microsoft a través de la siguiente dirección: https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/what-s-new-in-hyper-v-on-windows

6.3 REQUISITOS

Hyper-V tiene determinados requisitos hardware específicos y algunas características de Hyper-V tienen características adicionales.

Las características obligatorias necesarias para el uso de Hyper-V son las siguientes:

a) Procesador de 64 bits con traducción de direcciones de segundo nivel (SLAT).

b) Procesador basado en arquitectura x64 con soporte VT en el caso de procesadores Intel, y soporte AMD-V en el caso de procesadores AMD.

c) Memoria RAM suficiente para ejecutar las máquinas virtuales necesarias al mismo tiempo. Deberá tener en cuenta el sistema operativo host (mínimo 4GB).

d) Soporte de virtualización activado en el BIOS o UEFI:

e) Soporte de virtualización activado en el BIOS o UEFI. Dicha característica debe poseer además las siguientes características:

   i. Virtualización asistida por hardware.

   ii. Prevención de ejecución de datos (DEP) aplicada por hardware disponible y habilitada.

Para ejecutar otras características como por ejemplo máquinas virtuales blindadas se requieren las siguientes características:

a) UEFI 2.3.1c. Permite el arranque seguro y medido.

b) TPM v2.0 (Opcional). Protege los activos de seguridad de la plataforma.

c) IOMMU (Intel VT-D) (Opcional). El hipervisor puede proporcionar protección de acceso directo a la memoria (DMA).

d) Las máquinas virtuales deben poseer la siguiente configuración:

   i. Generación 2.

   ii. Windows Server 2012 o posterior como sistema operativo invitado.

Nota: Puede obtener más información sobre los requisitos de Hyper-V a través del siguiente enlace: https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows

6.4 LIMITACIONES

El servicio Hyper-V 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.

Las limitaciones del servicio Hyper-V son las siguientes:

a) Número de procesadores lógicos, 512.
b) Procesadores virtuales por cada procesador lógico, sin limitación.
c) Máquinas virtuales en ejecución por servidor, 1024.
d) Procesadores virtuales por servidor, 2048.
e) Memoria RAM, 24 TB.
f) Capacidad de almacenamiento, sin limitación. Depende de la capacidad de almacenamiento del sistema operativo base.
g) Redes de área de almacenamiento (SAN) virtuales, sin limitación.
h) Adaptadores de red físicos, sin limitación.
i) Equipos de adaptadores de red (NIC Teaming), sin limitación.
j) Redes virtuales (conmutadores virtuales), sin limitación. Depende de los recursos del sistema físico.
k) Puertos de los conmutadores de red virtuales por servidor, sin limitación. Depende de los recursos del sistema físico.

En el caso de las máquinas virtuales, las limitaciones se indican a continuación:

a) Procesadores virtuales, 64 para la generación 1 de máquinas virtuales y 240 para la generación 2 de máquinas virtuales.
b) Memoria RAM, 1 TB para la generación 1 de máquinas virtuales y 12 TB para la generación 2 de máquinas virtuales.
c) Discos duros IDE virtuales, 4.
d) Controladoras SCSI virtuales, 4.
e) Discos duros SCSI virtuales, 256.
f) Capacidad del disco duro virtual: 64 TB en formato VHDX, 2040 GB en formato VHD.
g) Capacidad de los discos duros físicos conectados directamente a la máquina virtual, determinado por el sistema operativo de la máquina virtual.
h) Adaptadores de canal de fibra virtual, 4.
i) Puntos de control, 50. Depende también del almacenamiento físico del servidor que aloja la máquina virtual.
j) Adaptadores de redes virtuales, 12 (8 adaptadores de red sintéticos y 4 adaptadores de red heredados).
k) Disquetes virtuales, 1.
l) Puertos serie (COM), 2.

Nota: Aunque las máquinas virtuales tengan las limitaciones de uso de recursos físicos indicadas anteriormente, en conjunto no pueden utilizar más recursos de los que disponga la máquina física.
Adicionalmente, no se debe utilizar por completo los recursos de la máquina física ya que se provocará una interrupción del sistema. La máquina física deberá disponer de los recursos físicos necesarios para poder gestionar los servicios que ofrece sin bloquearse.
Ejemplo, si una máquina física que gestiona dos máquinas virtuales posee 4 GB de memoria RAM, la suma de la memoria RAM asignada a las dos máquinas virtuales no puede ser superior a 3 GB.
Para obtener más información acerca de las limitaciones del servicio Hyper-V y de las máquinas virtuales, se puede consultar la web de Microsoft a través del siguiente enlace:
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-hyper-v-scalability-in-windows-server

6.5 ADMINISTRACIÓN DE HYPER-V

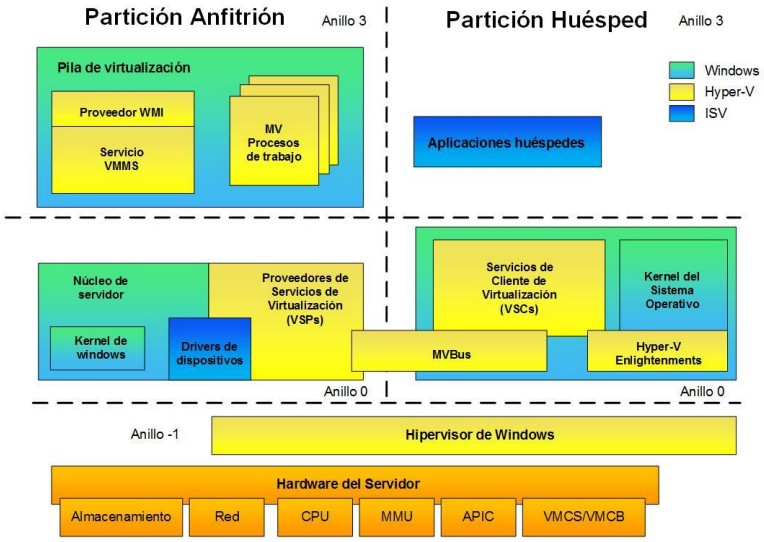
El servicio Hyper-V implementa la posibilidad de realizar su administración a través de una consola de gestión GUI, que corresponde con un complemento de la consola de gestión de Microsoft (Microsoft Management Console).

De forma adicional, existe la posibilidad de administrar el servicio a través de la ejecución y uso de los cmdlets de PowerShell específicos para Hyper-V.

En ambos casos, es necesario que se hayan instalado las características correspondientes en el sistema desde donde se va a realizar la administración.

6.6 ARQUITECTURA Y ANILLOS

La siguiente imagen muestra con detalle la arquitectura de los diferentes componentes de los que se encuentra compuesto el servicio.



Los componentes marcados en verde corresponden al sistema operativo MS Windows Server 2016. Los componentes marcados en amarillo corresponden al servicio Hyper-V. Por último, los componentes marcados en azul hacen referencia a software correspondiente a terceras partes (por ejemplo, drivers del sistema).

La arquitectura se divide en 3 anillos (en inglés, rings) que determinan el grado de privilegios asignados a los componentes contenidos dentro de cada anillo.

En el nivel de hipervisor (Anillo -1), únicamente se realizan tareas limitadas, sin permitir la posibilidad de ejecutar ningún tipo de código de terceros. De este modo se restringe la ejecución de código y se limitan los posibles fallos

de seguridad, proporcionando un aislamiento entre las diferentes particiones virtualizadas. Este anillo, se ejecuta en modo privilegiado.

En el nivel superior (Anillo 0) se encuentran varios componentes del servicio:

a) Los drivers de los dispositivos generados por terceros. De esta forma, no se permite la ejecución de drivers a nivel de kernel. Estos drivers no son parte del servicio de Hyper-V ya que son específicos de cada fabricante.

b) Los proveedores de servicio de virtualización (VSPs), son los responsables de proporcionar a la partición anfitriona la posibilidad de realizar tareas de virtualización.

c) Los clientes de servicio de virtualización (VSCs), se comunican a través del bus virtual (VMBus) con los proveedores de servicio de virtualización (VSPs).

d) El bus virtual (VMBus). Es un bus que permite la comunicación entre la partición anfitriona y las particiones invitadas de forma totalmente transparente y sin necesidad de utilizar el hipervisor. Con el objetivo de evitar ataques de hombre en el medio (Man-In-The-Middle), existe una pareja VSC-VSP por cada partición invitada.

e) Enlightenments. Estos componentes, son cargados por el kernel del sistema operativo con el objetivo de ayudar a reducir la carga de trabajo del hipervisor, como por ejemplo, la gestión de la memoria. De este modo se proporciona una mayor eficiencia al hipervisor y el rendimiento de los sistemas operativos virtuales aumenta. Los enlightenments son usados a través de llamadas de tipo hipervisor.

Por último, el nivel de usuario (Anillo 3), corresponde a la ejecución de servicios y aplicaciones, además de los siguientes componentes de virtualización:

a) Servicio de gestión de máquinas virtuales (VMMS). Gestiona el estado de las máquinas virtuales que se ejecutan en las particiones invitadas.

b) Proceso de ejecución de máquina virtual (VM Worker Process). Gestiona la comunicación entre la partición anfitriona y las máquinas virtuales existentes en el resto de particiones invitadas. Existe un proceso por cada máquina virtual, y se encargan de simular la placa base virtual del sistema operativo virtualizado.

c) Proveedor de interfaces WMI. Permite la interacción, gestión y monitorización del servicio y del entorno de particiones. Mediante el uso de la interfaz WMI, se pueden controlar los siguientes aspectos de Hyper-V:

   i. Servicio de gestión del sistema virtual. El perfil del sistema virtual describe los objetos que conforman una partición: sistema base, dispositivos, configuraciones y el servicio de gestión que realiza operaciones sobre el sistema.

   ii. Configuración de red. El perfil de red describe los objetos usados para la configuración del sistema permitiendo a las particiones comunicarse a través de la red.

   iii. Gestor de recursos. El perfil de virtualización de recursos establece la forma a través de la cual un cliente puede descubrir los recursos virtuales soportados por el sistema de virtualización. También indica la capacidad, o número de instancias que son soportadas por cada tipo de recurso virtual.

d) Servicio de máquinas virtuales (VM Service). Este componente implementa la funcionalidad específica de gestión del servicio Hyper-V.

6.6.1 PARTICIONES

La arquitectura del servicio Hyper-V se compone de un hipervisor y varias particiones:

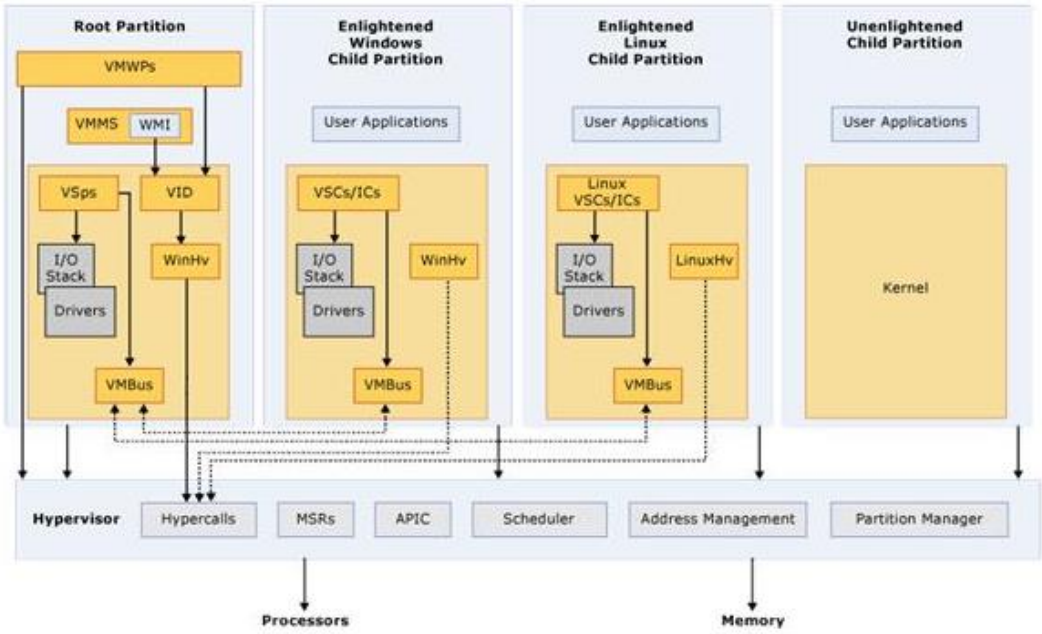
a) La partición anfitriona (en inglés, root partition). Se encarga de realizar tareas de administración y la virtualización de los dispositivos. Es considerada como la propietaria de los recursos hardware del sistema. Adicionalmente, se encarga de gestionar la energía del sistema, así como los fallos de hardware del sistema, además de crear y gestionar las particiones invitadas. En el caso de esta guía, esta partición aloja la instancia del sistema operativo MS Windows Server 2016.

b) Varias particiones invitadas (en inglés guest partitions). Cada una de las particiones invitadas corresponden a una máquina virtual creada y gestionada por Hyper-V.

c) El hipervisor. Es el responsable de proporcionar una separación entre las particiones invitadas y gestionar, así como controlar, el acceso a la capa hardware del sistema físico. El hipervisor proporciona un conjunto de funciones a las particiones, que éstas pueden usar.

Cada partición dispone de un conjunto propio de recursos de hardware (virtuales o físicos) tales como memoria RAM y procesadores.

Adicionalmente, cada partición tiene asociada una instancia de datos de configuración global del sistema virtual (en inglés, Virtual System Global Setting Data, VSGSD), y una o varias instancias de datos de configuración del sistema virtual (en inglés, Virtual System Setting Data, VSSD). Para cada VSSD, existen una serie de objetos de propiedades de los recursos (en inglés, Resource Allocation Setting Data, RASD), los cuales describen la configuración para cada partición. Todas estas instancias y objetos (VSGSD, VSSDs y RASDs) describen la configuración de la partición.



6.7 COMPONENTES FÍSICOS VIRTUALIZADOS

El servicio Hyper-V se encarga de virtualizar los recursos físicos de los que dispone en la máquina que despliega el servicio de virtualización.

Los recursos virtualizados por el servicio se indican a continuación:

a) Procesadores virtuales.

b) Memoria RAM.

c) Discos duros virtuales.

d) Adaptadores de red virtuales.

e) Unidades de CD/DVD virtuales.

f) Unidades de disquete virtuales.

g) Adaptadores de video virtuales.

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

i) Módulo de plataforma segura (TPM).

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

6.8 SISTEMAS OPERATIVOS VIRTUALIZADOS SOPORTADOS

El servicio de virtualización de Hyper-V proporciona la creación de máquinas virtuales sobre las que se instalan o despliegan un sistema operativo determinado. La arquitectura del sistema operativo a virtualizar dependerá de la arquitectura hardware del sistema físico.

Aunque Hyper-V es un servicio de sistemas Windows, permite no sólo la virtualización de sistemas operativos Windows, sino la virtualización de otro tipo de sistemas operativos como por ejemplo Ubuntu, Suse, etc.

Nota: Para obtener un listado de los sistemas operativos que se pueden virtualizar en Hyper-V, puede consultar las siguientes páginas web de Microsoft:
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-windows-guest-operating-systems-for-hyper-v-on-windows
https://technet.microsoft.com/library/dn531030(ws.12).aspx.

6.9 SERVICIOS DE INTEGRACIÓN

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 de integración de Hyper-V.

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 del sistema operativo virtual. Estos servicios dan acceso a los diferentes recursos físicos disponibles a través del servicio de virtualización.

En el caso de la instalación de determinados sistemas operativos en máquinas virtuales, éstos ya tienen por defecto instalados los servicios de integración por lo que no será necesario realizar la instalación de dichos componentes.

Nota: Para obtener un listado de los sistemas operativos que soportan los servicios de integración, tanto Windows como otros sistemas no Windows, puede consultar las siguientes páginas web de Microsoft:
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-windows-guest-operating-systems-for-hyper-v-on-windows
https://technet.microsoft.com/library/dn531030(ws.12).aspx.

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.

Estas funciones, cuya presencia depende de cada sistema operativo, también son conocidas como componentes de integración (en inglés, Integration Components, ICs):

a) Captura del foco del ratón. La transferencia del foco del ratón entre el sistema virtualizado y el sistema operativo base se realiza de forma transparente al usuario, sin necesidad de pulsar una combinación de teclas o seleccionar la ventana del sistema operativo virtualizado como paso previo a su utilización.

b) Conexión directa con el kernel. Permite la comunicación directa entre el sistema operativo virtualizado y la partición anfitriona a través del bus virtual (VMBus) cuando se accede a los dispositivos o se hacen peticiones de entrada/salida.

c) Sincronización de hora del sistema. Implementa un mecanismo de sincronización de las máquinas virtuales tomando como referencia la hora del servicio de virtualización.

d) Comprobación de estado (en inglés, heartbeat). El servidor de virtualización controla a través de mensajes de control el estado y disponibilidad de cada una de las máquinas virtuales desplegadas para determinar las acciones necesarias en el caso de que se pierda conexión con dichas máquinas, por ejemplo: registrando un evento de auditoría.

e) Apagado del sistema. Este servicio de integración permite el apagado controlado del sistema operativo virtual a través de la interfaz del servicio de virtualización.

f) Intercambio de pares clave/valor. Permite al servicio de virtualización la posibilidad de modificar un conjunto de entradas predefinidas en el registro del sistema operativo virtual. La información que se almacena se encuentra en la siguiente ruta del registro:

   i. HKLM\Software\Microsoft\Virtual Machine\Guest.

g) Servicio de copias de volúmenes de información (en inglés, Volume Shadow-Copy Service, VSS). Si el sistema operativo virtual soporta este servicio, el servidor de virtualización puede comprobar la inactividad y sincronización de una máquina virtual. Si todas las máquinas virtuales soportan el servicio, es posible realizar una copia de seguridad completa (punto de control) del servicio de virtualización completo, así como de las máquinas virtuales independientemente de si éstas se encuentran ejecutándose o no.

Adicionalmente, los servicios de integración proporcionan soporte para los drivers de dispositivos de almacenamiento de tipo IDE, SCSI; así como soporte para los drivers de red, video y ratón.

6.10 GENERACIONES DE MÁQUINAS VIRTUALES

En anteriores versiones del servicio de Hyper-V, las máquinas virtuales que se creaban disponían de las mismas características técnicas, no habiendo una diferencia entre ellas.

Con la nueva versión del servicio, se introduce el concepto de “generación” para identificar o categorizar las máquinas virtuales según éstas disponen de las características originales de versiones anteriores (Generación 1), o tienen a su disposición elementos y características adicionales (Generación 2).

Durante el proceso de creación y configuración de la máquina virtual el asistente solicita al usuario la elección de la generación de máquina virtual a utilizar, 1 o 2. Dependiendo de la elección, se creará una máquina de uno u otro tipo, no pudiéndose modificar esta elección a posteriori.

Dado que no es posible modificar el tipo de generación de una máquina virtual creada, se hace necesario tener en consideración la siguiente información como paso previo a la creación de la máquina.

Las características de las máquinas virtuales de generación 2 se indica a continuación:

a) Arranque PXE con un adaptador de red estándar.

b) Arranque desde un disco duro virtual SCSI.

c) Arranque desde un DVD virtual SCSI.

d) Arranque seguro (habilitado de forma predeterminada).

e) Compatibilidad con firmware UEFI.

La siguiente tabla define las ventajas y desventajas del uso de uno u otro tipo de máquina virtual.

Opción	Ventajas	Desventajas
Generación 1	– Admite todos los sistemas operativos invitados Hyper-V compatibles. – Permite adaptadores de red heredados	– No puede acceder a la nueva funcionalidad de las máquinas virtuales. – La seguridad es inferior. – No es posible hacer uso de arranque basado en UEFI.
Generación 2	– Permite el arranque seguro. – Es posible blindar las máquinas virtuales. – Mejora un poco los tiempos de instalación de invitados y arranque de máquinas virtuales. – Usa dispositivos SCSI o un adaptador de red estándar para arrancar las máquinas virtuales. – Impide que se ejecuten firmware, sistemas operativos o controladores UEFI no autorizados cuando el arranque seguro está habilitado. – Permite migrar máquinas virtuales basadas en versiones anteriores de Hyper-V. – Adición y eliminación en caliente de adaptadores de red. – Posibilidad de uso de Espacios de almacenamiento directo.	– Compatibilidad limitada con sistemas operativos invitados. – No es compatible con las máquinas virtuales de Azure. – No es compatible con RemoteFX. – No admite los disquetes virtuales.

Nota: Para más información acerca de la generación a utilizar para la creación de máquinas virtuales consulte los siguientes enlaces:
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/should-i-create-a-generation-1-or-2-virtual-machine-in-hyper-v
https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-feature-compatibility-by-generation-and-guest

6.11 ALMACENAMIENTO DE MÁQUINAS VIRTUALES

Por cada máquina virtual gestionada por Hyper-V, 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 **"%AllUsersProfile%\Microsoft\Windows\Hyper-V"**. La localización de esta carpeta puede ser modificada.

Los ficheros de discos duros virtuales (VHDX) se encuentran alojados por defecto en la ruta **"%SystemDrive%\Users\Public\Documents\Hyper-V\Virtual Hard Disks"**. La localización de esta carpeta puede ser modificada.

6.12 REDES VIRTUALES

El servicio Hyper-V permite la creación y gestión de diferentes redes virtuales que consisten en segmentaciones lógicas, de tal forma que se permite aislar el tráfico de las diferentes redes dependiendo de la criticidad del tráfico que se transmite en cada una de ellas.

En concreto, Hyper-V permite crear tres tipos de redes:

a) Redes externas. Se encuentran conectadas con el adaptador de red de la máquina física a través de mini puertos asociados con cada tarjeta de red. Estas redes, al estar conectadas con el adaptador de red físico, poseen una conectividad similar a la de la máquina física. El servicio que gestiona las redes crea en este caso, una red virtual, y un adaptador de red virtual en el sistema operativo de administración que está conectado con la red virtual.

b) Redes internas. No se encuentran conectadas con el adaptador de red de la máquina física, pero permite la conexión con el sistema operativo de la máquina física que aloja las máquinas virtuales.

c) Redes privadas. Al igual que en el caso de las redes internas, este tipo de redes no se encuentra conectado con el adaptador de red de la máquina física, pero en este caso tampoco lo están con el sistema operativo de la máquina física permitiendo la creación de entornos completamente aislados.

6.12.1 TIPOS DE ADAPTADORES DE RED

Hyper-V define dos tipos de adaptadores de red: adaptadores sintéticos y adaptadores heredados; que se utilizan de forma indistinta y de forma transparente al usuario. Cada adaptador tiene unas propiedades y funciones diferentes.

a) Los adaptadores de red sintéticos (en inglés, synthetic adapters), requieren de un driver para poder ser utilizados. Por el contrario, ofrecen un alto rendimiento ya que utilizan el bus VMBUS y no hay una virtualización por software del recurso. Los drivers están incluidos en la mayoría de los sistemas operativos, aunque también se encuentran disponibles tras instalar los servicios de integración.

b) Los adaptadores heredados o compartidos (en inglés, legacy adapters), funcionan sin necesidad de instalar un driver de máquina virtual ya que se encuentran en la mayoría de los sistemas operativos. Este tipo de adaptadores, son implementados desde cero para realizar las funciones de un adaptador de red de tipo multipuerto DEC 1140 10/100TX 100 MB. Estos adaptadores soportan instalaciones por red, ya que disponen de la opción de arranque mediante PXE. Al contrario que en el caso anterior, estos adaptadores son más lentos, por lo que únicamente se recomienda su uso cuando se requiera utilizar la función de instalación por red, o el sistema operativo no soporte el adaptador de red sintético. Su uso es obligatorio, en el caso de que el sistema operativo no soporte la instalación de los servicios de integración.

6.12.2 REDES DE AREA LOCAL VIRTUALES (VLAN)

Las redes de área local virtuales son identificadas a través del uso de un número identificador (en inglés, 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.

El VLAN ID 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.

El adaptador de la tarjeta de red debe soportar la configuración de red local virtual.

6.13 PUNTOS DE CONTROL

Anteriormente llamados “Instantáneas”, los puntos de control se componen de una colección de datos acerca de una determinada partición y su estado actual. Esta información permite el restablecimiento del estado de la máquina en el momento en que se creó el punto de control. En concreto, los puntos de control crean un disco duro virtual de diferenciación para almacenar las modificaciones realizadas en el sistema virtual.

La información que se recopila durante la creación del punto de control incluye:

a) Propiedades de la configuración de la partición (se encuentra en el fichero ".vmc").

b) Propiedades de la red virtual.

c) El estado actual de todos los discos duros virtuales (VHDXs) 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.

6.14 MIGRACIÓN EN TIEMPO REAL

La migración en tiempo real permite mover una partición de una instancia de un servicio de Hyper-V a una instancia de otro servicio Hyper-V. Ambas instancias, deben ser compatibles, y los discos duros virtuales deben residir dentro de un clúster de volúmenes compartidos accesibles por las dos instancias del servicio Hyper-V o en un recurso compartido por SMB 3.0 (ésta última característica es una novedad de la actual versión de Hyper-V).

La migración en tiempo real asegura que las propiedades de seguridad de una partición son mantenidas a lo largo del proceso de migración, así como en la instancia del servicio destino.

La funcionalidad de migración en tiempo real proporciona las siguientes características:

a) Mayor agilidad en la gestión y ejecución de las máquinas virtuales.

b) Reducción de los costes y un incremento de la productividad.

Para permitir la migración en tiempo real, el servicio de Hyper-V comprueba los prerrequisitos necesarios que deben ser satisfechos para realizar de forma satisfactoria la migración de la partición. Estos requisitos, comprueban que el hardware sobre el que se ejecuta la instancia a migrar es compatible con el hardware destino, además de verificar que los dos servicios de Hyper-V tienen acceso al mismo clúster de almacenamiento o recursos de red, donde se almacenan los discos duros virtuales de la instancia que se está migrando.

Esta funcionalidad de Hyper-V también permite aumentar o reducir el espacio de almacenamiento de una máquina virtual mientras se encuentra en ejecución.

Además de la migración en tiempo real, el servicio Hyper-V de MS Windows Server 2016, permite la realización de una migración de tipo rápido. Este tipo de migraciones se diferencia de la migración en tiempo real, en que la máquina virtual que es guardada en disco, es movida a otra localización, y posteriormente la máquina virtual es restaurada. A diferencia de la migración en tiempo real, este proceso requiere la parada de la máquina virtual.

6.14.1 PROCESO DE MIGRACIÓN EN TIEMPO REAL

El proceso de migración de una máquina en tiempo real se compone de 6 pasos:

a) Transferencia de la configuración de la máquina virtual al servicio destino.

b) Reserva de recursos para alojar la máquina virtual en el servidor destino.

c) Copia de la memoria virtual de la máquina virtual en el servidor destino.

d) Transferencia de los registros al servidor destino.

e) Transferencia del gestor de almacenamiento al servidor destino.

f) Configuración de la MAC del adaptador de red en el servidor destino.

El tiempo necesario para llevar a cabo una migración en tiempo real depende de los siguientes factores:

a) El tamaño de la memoria virtual a transferir.

b) Ancho de banda de la red de datos entre los servicios de virtualización origen, y destino.

c) Configuración del hardware sobre el que se ejecutan ambos servicios de virtualización.

d) Carga de trabajo de los sistemas físicos donde se despliegan ambos servicios de virtualización.

e) Ancho de banda de la red de datos entre los sistemas físicos donde se despliegan los servicios de virtualización y el dispositivo de almacenamiento compartido.

6.14.2 ESCENARIOS DE USO

Algunos de los escenarios en los que se puede utilizar la migración en tiempo real son los siguientes:

a) Es necesario realizar una parada de mantenimiento en el servidor donde se encuentran desplegadas las máquinas virtuales.

b) Se desea equilibrar el consumo y rendimiento de varios servidores. Si un servidor tiene demasiada carga de trabajo o consumo de energía, es recomendable, desde el punto de vista de la eficiencia, migrar alguna de sus máquinas virtuales a otro servidor para equilibrar su carga de trabajo.

c) Se desea reducir el consumo de energía. A mayor número de equipos que se encuentran encendidos, mayor será el consumo de energía, y la necesidad de refrigeración. Si se dispone de los recursos suficientes, es recomendable utilizar el menor número de servidores con el mayor número de máquinas virtuales desplegadas, sin que la eficiencia de dichas máquinas se vea afectada.

6.15 RÉPLICA DE HYPER-V

La funcionalidad de réplica de Hyper-V permite realizar la replicación de máquinas virtuales entre sistemas de almacenamiento, tales como clústeres y centros de datos que se encuentran en ubicaciones diferentes, principalmente para ofrecer una protección frente a incidentes y para garantizar una continuidad del negocio.

Dentro de este escenario de replicación, existirá un sitio principal, y uno o varios sitios de respaldo o de replicación.

El sitio principal corresponde a la ubicación donde se encuentran los servicios que proporcionan la operativa normal de la infraestructura. Por contra, el sitio de respaldo hace referencia a la ubicación donde se encuentra la copia de los datos y servicios del sitio principal, y que se activará en el caso necesario por una pérdida de servicio en el sitio principal, o se encontrará activo constantemente proporcionando un servicio de alta disponibilidad.

Independientemente del modo de replicación, es necesario mantener una copia actualizada de los datos en el sitio de respaldo.

Nota: Para más información acerca de la replicación de datos, puede consultar la Web de Microsoft https://technet.microsoft.com/es-es/library/hh831783.aspx.

En relación con la replicación de Hyper-V, en las nuevas versiones de Hyper-V sobre sistemas Windows Server 2016 se introduce el uso del disco duro virtual compartido, que es utilizado para que varias máquinas virtuales dentro de un clúster tengan acceso a un fichero de disco duro virtual (.vhdx) compartido.

Este elemento de disco virtual compartido se utiliza para crear la infraestructura de alta disponibilidad y resulta importante en implementaciones de tipo “nube privada” y otros entornos ubicados en la nube que se encargan de administrar grandes cargas de trabajo.

Estos ficheros de disco duro virtual compartido se pueden alojar en Volúmenes Compartidos de Clúster (CSV) o en recursos de red compartidos a través de SMB.

6.16 ESTRUCTURA DE CARPETAS

Cuando se realiza la instalación del rol de Hyper-V en un sistema MS Windows Server 2016, se crean y se instalan una serie de ficheros ejecutables, bibliotecas, de configuración y de otro tipo, los cuales están distribuidos en diferentes carpetas en el sistema operativo anfitrión.

Para una mayor comprensión de la estructura de carpetas que utiliza Hyper-V, así como para conocer el conjunto de ficheros que se instalan durante un proceso de implantación de Hyper-V a continuación, se muestra una tabla de referencia con todas las rutas utilizadas y los ficheros contenidos en cada carpeta.

Ruta	Ficheros
C:\Windows\inf	– wnetvsc.inf – ws3cap.inf – wstorflt.inf – wstorvsc.inf – wstorvsp.inf – wvid.inf – wvmbus.inf – wvmbushid.inf – wvmbusr.inf – wvmbusvideo.inf – wvms_mp.inf – wvms_pp.inf – wvms_vsft.inf – wvms_vspp.inf
C:\Windows\System32	– hvax64.exe → Hyper-V (hipervisor, versión AMD). – hvix64.exe → Hyper-V (hipervisor, versión Intel). – hypervisor.mof – rdp4vs.dll (API de servicios remotos de máquinas virtuales). – RemoteFileBrowse.dll – removehypervisor.mof – vid.dll (biblioteca de controladores de infraestructura de Hyper-V). – vmbuspipe.dll (bus de máquina virtual en modo de usuario). – vmbusvdev.dll (dispositivo bus de máquina virtual). – vmictimeprovider.dll (componente de tiempo de los servicios de integración). – vmms.exe (servicio de administración de Hyper-V). – vmprox.dll (componente proxy de Hyper-V). – vmwp.exe (proceso de trabajo de máquina virtual). – vmwpctrl.dll (módulo monitor de máquina virtual). – vsconfig.dll (módulo de configuración de máquina virtual). – WindowsVirtualizationUninstall.mof
C:\Windows\System32\drivers	– passthruparser.sys – storvsc.sys – storvsp.sys – vhdparser.sys – vid.sys (controlador de infraestructura de Hyper-V). – vmbus.sys (bus de máquina virtual). – vmbushid.sys – vmswitch.sys (proveedor de virtualización de redes). – winhv.sys (controlador de interfaz de hipervisor de Windows).
C:\Windows\System32\es-ES	– vmms.exe.mui – vmwp.exe.mui – vsconfig.dll.mui
C:\Program Files\Hyper-V	– SnapInAbout.dll

7. SEGURIDAD EN EL SERVICIO DE HYPER-V

El servicio Hyper-V constituye una solución para el mantenimiento y gestión de múltiples sistemas virtuales que conviven dentro de un mismo sistema hardware. Por ello, es importante planificar adecuadamente la seguridad de los diferentes aspectos, tanto de la máquina física que aloja el servicio, como cada una de las máquinas virtuales gestionadas y mantenidas por el servicio Hyper-V.

7.1 ASPECTOS DE LA SEGURIDAD EN HYPER-V

Los principales aspectos desde el punto de vista de la seguridad que se deben tener en cuenta son los siguientes:

a) Aplicación de seguridad sobre el servicio Hyper-V. Consiste en la instalación y configuración del servicio Hyper-V de manera segura, reduciendo la superficie de ataque del servicio.

b) Delegación de la gestión de las máquinas virtuales. Engloba la definición de las directrices a seguir para determinar las acciones disponibles para los administradores de las máquinas virtuales de tal forma que éstas sean las mínimas y necesarias para llevar a cabo las tareas asignadas a cada administrador.

c) Protección de las máquinas virtuales. Establece un nivel de seguridad adecuado para las máquinas virtuales, así como para los recursos asignados a dichas máquinas.

7.2 CONTROL DE ACCESO AZMAN

En anteriores versiones del servicio de Hyper-V, se utilizaba un modelo de control de acceso basado en roles que estaba proporcionado por un almacén de autorización AzMan (Windows Authorization Manager) y cuya configuración se realizaba a través de una política de roles y asignaciones de roles a usuarios definida en un fichero XML localizado en el disco duro local. En concreto, este fichero residía en la ubicación "C:\ProgramData\Microsoft\Windows\Hyper-V\InitialStore.xml" del servidor.

Sin embargo, en la nueva versión del servicio, no se permite el uso de este almacén ya que ha sido deprecada la característica.

Para obtener información acerca de la administración del servicio de Hyper-V, consulte la sección "7.3 USUARIOS DE ADMINISTRACIÓN".

7.3 USUARIOS DE ADMINISTRACIÓN

Al realizar la instalación del servicio de Hyper-V en un servidor MS Windows Server 2016, se crea un grupo local de administración de dicho servicio llamado "Administradores de Hyper-V".

Por defecto, los usuarios que se ubiquen dentro de este grupo tendrán la posibilidad de tener acceso completo a todas las características y configuración del servicio de Hyper-V, entre lo que se encuentra la administración del almacenamiento y la configuración de red de todas las máquinas virtuales. No obstante, este grupo de administradores deberá tener acceso y permisos sobre las ubicaciones del disco donde se encuentren los recursos utilizados (discos duros virtuales, ficheros de puntos de control, etc.).

De esta forma, a través del uso de este grupo de administración de Hyper-V, los usuarios de no requieren de la necesidad de pertenecer al grupo "Administradores" locales del servidor, lo que limita las tareas administrativas que se realizan sobre el sistema físico.

A diferencia de versiones anteriores, al no estar habilitado el almacén de autorización, no es posible realizar una segregación de funciones tan específica como se establecía dentro del apartado de tareas de administración de la guía de seguridad de Hyper-V CCN-STIC-528 sobre sistemas operativos MS Windows Server 2008 R2 Core.

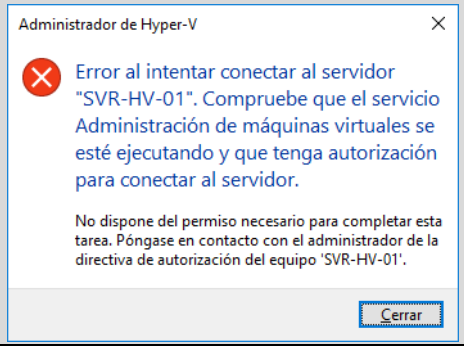
Por lo tanto, si se desea limitar las operaciones que un usuario puede realizar sobre el servicio de virtualización, una de las siguientes aproximaciones:

a) Incluir al usuario en concreto en el grupo local “Administradores de Hyper-V”.

b) Implementar una solución de gestión de usuarios a través de Virtual Machine Manager que permita segregar las operaciones y entidades a las que un usuario puede acceder dentro del servicio de virtualización, así como los privilegios que tiene asignados sobre las mismas.

Se recomienda que se restrinja la asignación de cuentas de administración (del servicio de Hyper-V o de las máquinas virtuales) a aquellas personas que tengan dicha responsabilidad.

Nota: Tenga en consideración que no solo es necesario conceder permisos de acceso al equipo que proporciona el servicio de Hyper-V ya que si no pertenece al grupo indicado anteriormente el usuario no podrá conectar con el propio servidor local mostrando el siguiente mensaje de error.



7.4 FUNCIONALIDAD DE SEGURIDAD EN HYPER-V

La funcionalidad proporcionada por Hyper-V teniendo en cuenta la seguridad del sistema principal, así como las particiones y los recursos, se puede englobar en diferentes apartados.

En general, el servicio Hyper-V implementa la siguiente funcionalidad de seguridad:

a) Generación de registros de auditoría específicos de Hyper-V.

b) Protección de los datos de usuario.

c) Identificación de particiones.

d) Gestión de la configuración de particiones.

e) Gestión de la cuota de uso de recursos y su aplicación.

f) Separación del espacio de direcciones.

7.4.1 PROTECCIÓN DE LOS DATOS DE USUARIO

La funcionalidad de seguridad de Hyper-V permite controlar y focalizar la seguridad sobre los datos, tanto de los usuarios, como de otros datos del sistema a través de las siguientes acciones:

a) El control de acceso de los administradores a los objetos de administración.

b) El control de acceso de las particiones a los recursos virtuales y recursos sintéticos.

c) La protección de los datos residuales.

d) Uso dedicado del procesador real (no almacenando información de diferentes instancias al mismo tiempo).

7.4.2 GESTIÓN DE LA SEGURIDAD

Hyper-V puede ser administrado mediante el uso de la funcionalidad de gestión que se encuentra disponible en la partición anfitriona, o de forma remota mediante el uso de una aplicación cliente que se conecta a WMI y realiza diferentes actividades de gestión a través de esta interfaz.

En ambos casos, el usuario que realiza las tareas de gestión es autenticado como un usuario normal a través de la funcionalidad de autenticación del sistema MS Windows Server 2016.

Los datos de configuración específicos de Hyper-V son almacenados en objetos del sistema que son protegidos por las funciones de control estándar de MS Windows Server 2016. Por lo tanto, el acceso directo a estos objetos se controla por las funciones de gestión del control de acceso de MS Windows Server 2016.

7.4.3 PROTECCIÓN DURANTE LA MIGRACIÓN EN TIEMPO REAL

Por defecto, la migración en tiempo real entre, y a un equipo de Hyper-V se encuentra deshabilitada. Esta migración puede ser habilitada por un administrador de Hyper-V.

Si se habilita, se recomienda realizar migraciones en tiempo real a través de medios de comunicación (interfaces) seguros, y estableciendo la configuración necesaria para que la migración en tiempo real se realice únicamente utilizando las interfaces securizadas.

Antes de realizar la migración hacia dentro/fuera de un clúster, es necesario verificar que los equipos que intervienen en la migración sean autenticados. En este sentido, Hyper-V permite el uso de Kerberos o CredSSP para realizar esta autenticación.

Por defecto, el tráfico que se genera durante la migración en tiempo real no se encuentra cifrado, por lo que se debe usar una red segura con el objetivo de proteger el tráfico generado. El aislamiento del tráfico generado por la migración, o el uso de IPSec para cifrar la comunicación, previene que la comunicación establecida durante el proceso se vea comprometida.

Las particiones que se migran en tiempo real entre diferentes servicios de Hyper-V deben conservar todas las propiedades necesarias para el mantenimiento de la integridad y disponibilidad del sistema virtual.

Entre las características que se migran durante el proceso, se encuentran las propiedades de seguridad de la instancia virtual. Estas características deben ser idénticas a las que se encuentran establecidas en la instancia original.

7.4.4 PROTECCIÓN DE LA RÉPLICA DE HYPER-V

La funcionalidad de réplica de Hyper-V, admite dos modos de comunicación: HTTP y HTTPs.

Dado que HTTP no implementa ningún medio de seguridad en la comunicación transmitida, es necesario utilizar el protocolo HTTPs para la implementación de la réplica del servicio, salvo que se utilicen otro tipo de mecanismos como pueden ser los túneles VPN o cifrado IPsec.

Es imprescindible realizar una verificación y autenticación de los servidores que intervienen en la replicación de datos con el objeto de asegurar la autorización de los mismos para llevar a cabo la replicación. En el caso de que no exista una relación de confianza, es posible utilizar certificados digitales que aseguren la identidad de los intervinientes en el proceso.

7.4.5 USO DE RECURSOS

Hyper-V proporciona la funcionalidad para que un usuario administrador defina los límites en el uso de la memoria y de las unidades de proceso en cada una de las instancias de las particiones invitadas.

Hyper-V comprueba en todo momento que ninguna de las particiones invitadas consuma la totalidad de los recursos proporcionados por un determinado recurso físico, causando, en este caso una denegación de servicio en otras máquinas virtuales. Además, se realiza un control del acceso a los recursos físicamente virtualizados.

7.4.6 IDENTIFICACIÓN Y SEGURIDAD DE LAS PARTICIONES DEL SERVICIO

El servicio Hyper-V se encarga de separar los diferentes sistemas virtualizados en particiones de tal forma que cada una de las particiones tenga un entorno de ejecución totalmente aislado del resto de instancias desplegadas por el servicio.

La partición anfitriona está especialmente protegida debido a su criticidad. En esta partición no se permite la instalación de aplicaciones no confiables. Este tipo de aplicaciones se deben instalar en las particiones invitadas, donde sus posibles efectos dañinos no afecten al servicio de virtualización, o a otras particiones.

Además de la información de gestión necesaria, cada partición del servicio de virtualización tiene asociadas unas propiedades de seguridad:

a) Cantidad de tiempo de uso del procesador reservado para la partición.

b) Máxima cantidad de tiempo de uso del procesador que la partición está autorizada a utilizar.

c) Posibilidad de crear particiones.

d) Acceso a la memoria a través de llamadas de hipervisor.

e) Habilidad para iniciar una comunicación entre procesos con otras particiones invitadas.

f) Acceso para trazar llamadas de hipervisor.

g) Acceso a la gestión de la energía de la unidad de procesamiento a través de llamadas de hipervisor.

Sobre las particiones se realizan diferentes controles de seguridad, como son el control de acceso a los objetos de administración en la partición anfitriona.

El servicio de Hyper-V necesita que cada una de las particiones sea identificada de forma inequívoca. Esta identificación se realiza por medio de identificadores únicos asignados a cada partición. De este modo, la partición es identificada cuando el hipervisor interactúa con ella, y cuando se establece un canal de comunicación entre la partición invitada y la partición anfitriona a través del bus virtual (VMBus).

Ya que las particiones invitadas son creadas y controladas por el servicio, la autenticación de las particiones no es necesaria.

En el momento en que una partición es ejecutada, los privilegios y los dispositivos virtualizados son asignados a la partición en función de la configuración establecida en el archivo de configuración de partición.

Determinados privilegios como el privilegio de crear particiones, o el privilegio para crear puertos que puedan ser usados para realizar una comunicación directa entre particiones invitadas, no son asignados a ninguna de las particiones invitadas. Este comportamiento por defecto no puede ser modificado.

7.4.7 SEGURIDAD PROPORCIONADA POR LA PARTICIÓN ANFITRIONA

La seguridad del servicio Hyper-V viene respaldada y complementada por los mecanismos de seguridad proporcionados por la instancia de MS Windows Server 2016 que se encuentra en la partición anfitriona.

La instancia principal del servicio proporciona la siguiente funcionalidad de seguridad:

a) Identificación y autenticación de los usuarios que solicitan acceder a una partición invitada.

b) Gestión y protección de los registros de auditoría.

c) Control de acceso de los usuarios administradores a los objetos de gestión de MS Windows Server 2016.

d) Control de acceso a ficheros y dispositivos.

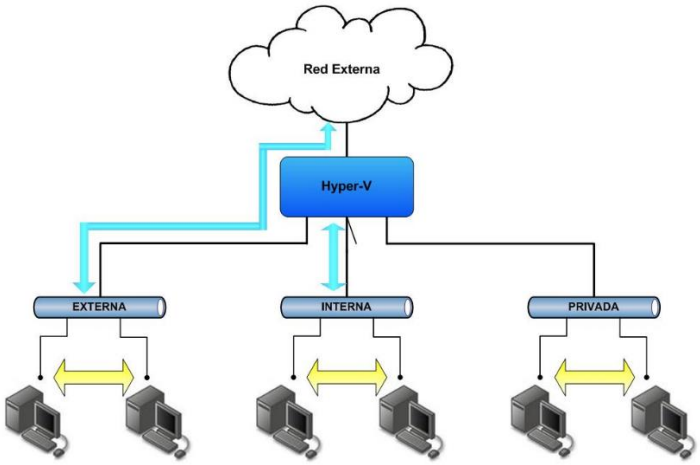
e) Gestión de usuarios y privilegios de acceso a objetos de MS Windows Server 2016.

7.4.8 SEGURIDAD DE REDES VIRTUALES

La funcionalidad de redes virtuales que proporciona el servicio de Hyper-V resulta de gran utilidad para segmentar las redes a las que se conectan las diferentes máquinas virtuales desplegadas en el servicio.

Esta segmentación permite el aislamiento de los datos que se transmiten en cada una de las redes, de tal forma que se crean diferentes redes virtuales en función de la criticidad de la información que se usa.

La siguiente figura muestra la gestión de un conjunto de redes mediante la utilización de redes virtuales aislando el tráfico entre diferentes redes.



Además del uso de diferentes redes virtuales, dependiendo del tipo de información que se transmita, es recomendable usar redes virtuales de área local, que permite segmentar de forma lógica una red virtual.

En el caso de redes de área local virtuales, se recomienda no configurar el identificador de red (VLAN ID) en el adaptador de red físico. Sin embargo, este identificador se debe configurar, bien en el conmutador virtual, o en las máquinas virtuales.

Adicionalmente, se recomienda seguir las siguientes indicaciones:

a) Usar una red virtual privada entre las máquinas virtuales si no es necesaria una comunicación con el exterior o con la máquina física.
b) Usar una red virtual interna si se necesita exclusivamente una comunicación con la máquina física.
c) Usar una red virtual externa si se necesita una comunicación con la red externa o con Internet.
d) Si se necesita separar la comunicación entre las máquinas virtuales y la máquina física, se debe usar un adaptador virtual que no se encuentre virtualizado, y disponible para las máquinas virtuales desplegadas.
e) Si se desea conectar dos máquinas virtuales que se encuentran en diferentes subredes, se debe utilizar un enrutador, ya que el conmutador virtual opera a nivel 2 del modelo de red ISO.
f) Cuando se utilice una red virtual interna, se recomienda crear una excepción para permitir que las máquinas virtuales se comuniquen con el servidor físico.
g) Comprobar, si es necesario una comunicación entre ellas, que las máquinas virtuales y el sistema operativo de administración se encuentran en la misma subred IP.
h) Si el tráfico de red es elevado, usar un adaptador de red físico de forma exclusiva para cada máquina virtual correspondiente.
i) Usar dispositivos de red de alta velocidad si es posible, habilitado los servicios de integración.

Por último, se recomienda, a través de la aplicación de seguridad sobre las redes, aislar las máquinas virtuales y recursos de red según la criticidad y clasificación de los servicios y datos que gestionen.

7.5 SEGURIDAD DE LAS MÁQUINAS VIRTUALES

A diferencia de un sistema físico, el cual dispone de los medios hardware adecuados para cifrar el disco duro utilizando la funcionalidad BitLocker, no es posible activar BitLocker en las máquinas virtuales.

Por este motivo, se hace necesario establecer los mecanismos oportunos para proteger la confidencialidad de los discos duros virtuales, a través del cifrado del soporte de almacenamiento físico donde se encuentran alojados los ficheros correspondientes a dichos discos virtuales.

A la hora de aplicar una configuración segura a las máquinas virtuales y seguir unas buenas prácticas, se debe cumplir una serie de requisitos:

a) Determinar la localización de los archivos de discos duros virtuales (VHDXs) y establecer los controles de acceso necesarios para preservar su seguridad. Se recomienda establecer la siguiente configuración.

Nombre	Permisos	Aplicar a
Administradores System (Sistema)	Control total.	Esta carpeta, subcarpetas y archivos.
Creator Owner (Creador propietario)	Control total.	Solo subcarpetas y archivos.

b) Asignar una cantidad de memoria RAM adecuada en cada máquina virtual para mantener la disponibilidad del servicio.

c) Establecer un tamaño fijo para los discos duros virtuales de las máquinas virtuales con el fin de evitar un llenado de los dispositivos de almacenamiento físico.

d) Imponer límites en el uso del procesador para mantener la disponibilidad del servicio.

e) Configurar los medios de almacenamiento necesarios para el correcto funcionamiento de cada máquina virtual.

f) Activar y configurar la sincronización de la hora de cada máquina virtual.

g) Desplegar la máquina virtual en el mismo nivel de seguridad que la máquina física en la que se aloja.

h) Almacenar de forma segura los ficheros correspondientes a los puntos de control generados.

i) Activar la auditoría sobre los ficheros utilizados por las máquinas virtuales (discos duros, puntos de control, etc.

j) Llevar un control y una gestión de la seguridad de las máquinas virtuales de forma equivalente a si fuera un sistema físico, a través, por ejemplo, de los siguientes puntos:

   i. Actualizar el sistema operativo de la máquina virtual.

   ii. Utilizar productos de seguridad como antivirus, antispyware, etc.

   iii. Implementar un control de acceso a la máquina.

8. AUDITORÍA DEL SERVICIO HYPER-V

Además de garantizar la seguridad de todo el entorno, tanto del host de Hyper-V como de las máquinas virtuales que se ejecutan sobre él, es importante conocer en todo momento que acciones y eventos se están produciendo.

Hyper-V mantiene un amplio conjunto de registros de eventos y de auditoría, los cuales muestran las acciones de cada uno de sus diferentes componentes.

La capa del hipervisor, así como los componentes específicos de Hyper-V que se encuentran dentro de la partición anfitriona son capaces de generar eventos de auditoría. Estos eventos son gestionados y almacenados a través de la función de auditoría de MS Windows Server 2016.

Los eventos de seguridad relevantes generados por el hipervisor son enviados a la partición anfitriona y ésta genera y almacena los registros de auditoría correspondientes para dichos eventos. Los eventos de seguridad relevantes indicados por el hipervisor son:

a) Creación de una partición.

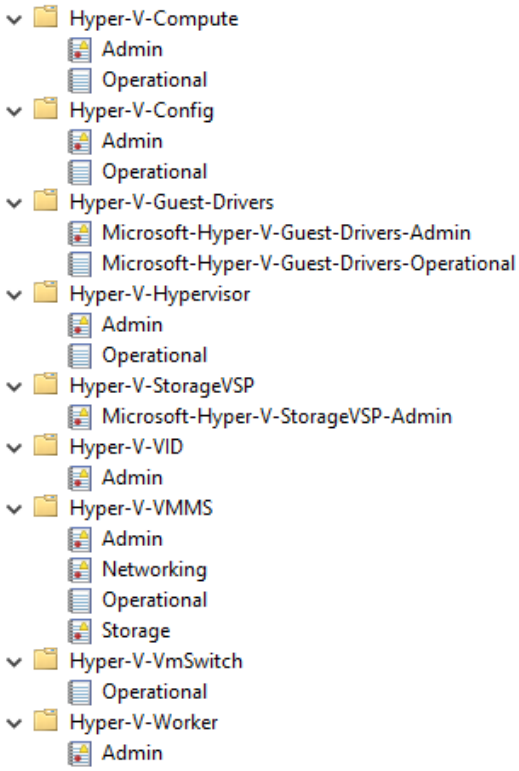
b) Borrado de una partición.

c) Detección de una condición de fallo interna del hipervisor.

Cada uno de los registros de auditoría son enviados al servicio de registro de eventos de MS Windows Server 2016 en la partición anfitriona, el cual inserta los detalles de la fecha y hora en que se ha producido el evento, así como almacenar el evento en el registro de eventos.

A continuación, se detallan técnicamente los diferentes registros de eventos que se crean cuando se instala la funcionalidad de Hyper-V en un servidor.

Hyper-V crea nueve categorías de eventos cuando se instala, las cuales se pueden acceder abriendo el visor de eventos del sistema y navegando a la carpeta Microsoft y posteriormente Windows. Dichas categorías son explicadas a continuación.



a) Hyper-V-Compute. Los eventos del Host Compute Service (HCS) se recopilan aquí. El HCS es una API de gestión de bajo nivel.

b) Hyper-V-Config. En esta sección se registra todo lo relacionado con la configuración de las máquinas virtuales, como la corrupción del archivo de configuración de la máquina virtual o la pérdida de dicho fichero.

c) Hyper-V-Guest-Drivers. Esta sección almacena y registra la información referente a problemas derivados de los componentes de integración de VM.

d) Hyper-V-Hypervisor. En esta sección se registran eventos específicos del hipervisor, como fallos en el inicio del servicio o problemas de configuración.

e) Hyper-V-StorageVSP. Se registran eventos del proveedor de servicios de virtualización de almacenamiento. Por lo general, son utilizados cuando es necesario depurar operaciones de almacenamiento de bajo nivel para una máquina virtual.

f) Hyper-V-VID. Recoge los eventos asociados con la gestión de la memoria de acceso no uniforme (NUMA).

g) Hyper-V-VMMS. En esta sección se registran eventos del servicio de administración de máquinas virtuales.

h) Hyper-V-VmSwitch. En esta sección se registran todos los eventos relativos a las redes virtuales o switches virtuales, como son la creación y configuración de redes virtuales.

i) Hyper-V-Worker. En esta sección se registran eventos del proceso de trabajo (worker process) en el que se ejecutan las máquinas virtuales.

Además, la mayoría de las secciones identificadas disponen de dos registros, “admin” y “operational”. En ellos se registran eventos relativos a las tareas de administración o eventos relativos a las tareas de operaciones.

En el caso de la sección Hyper-V-VMMS, se incluyen dos registros adicionales, “networking” y “storage”, correspondientes a eventos de gestión de redes virtuales y almacenamiento respectivamente.

9. NOVEDADES HYPER-V EN WINDOWS SERVER 2016

Hyper V sobre Windows Server 2016 constituye la última evolución de la versión de Hyper V ya existente en Windows Server 2012 R2. Para todos aquellos operadores que ya hayan implementado guías anteriores y se encuentren familiarizados con Hyper V en Windows Server 2012 R2, se exponen, a continuación, aquellos cambios significativos que bien a efectos de seguridad, de implementación o de experiencia en su manejo suponen un cambio en la versión de Windows Server 2016.

También es importante la lectura de este punto para el resto de operadores que nunca hayan trabajado con sistemas Windows y necesiten hacer una implementación en sus infraestructuras del servicio de Hyper V sobre Windows Server 2016.

Antes de comenzar y tal y como ya se ha indicado en puntos anteriores de la guía dependiendo de la versión del Sistema operativo de Windows Server 2016 utilizada, Hyper-V posee ciertos condicionantes a tener en cuenta a la hora de desplegar el servicio en cada organización.

Dependiendo de la edición de Windows Server 2016 instalada es posible encontrar las siguientes diferencias para Hyper-V:

a) Windows Server 2016 Standard

   i. Incluye un máximo de 2 contenedores para Hyper-V.

   ii. Puede utilizarse como invitado de virtualización, pero con un máximo de dos máquinas virtuales, más un host de Hyper-V por licencia.

b) Windows Server 2016 Datacenter

   i. Incluye contenedores ilimitados para Hyper-V.

   ii. Puede utilizarse de forma ilimitada como invitado de virtualización, más un host de Hyper-V por licencia.

   iii. Incluye soporte para virtualización de red, réplicas de almacenamiento, espacios de almacenamiento directos y máquinas virtuales blindadas.

En la siguiente tabla se definen las características definidas anteriormente

Diferencias Hyper-V Windows Server 2016		
	Datacenter	**Standard**
Máquinas virtuales	Ilimitadas	2 máximo
Contenedores de Hyper-V	Ilimitados	2 máximo
Máquinas virtuales blindadas	Si	No
Virtualización de red	Si	No
Réplicas de almacenamiento	Si	No
Espacios de almacenamiento directo	Si	No

9.1 COMPATIBILIDAD CON EL MODO DE ESPERA CONECTADO

Tras instalar el servicio de Hyper-V en un equipo que utiliza el modelo de alimentación "Siempre conectado" (Always On / Always Connected (AOAC)), la opción energía "modo de espera conectado" se encuentra disponible para su uso.

Este modo de funcionamiento evita que los componentes del equipo dejen de funcionar cuando no se encuentran en uso lo que evita retardos y problemas de comunicación cuando el equipo no se encuentra activo.

9.2 ASIGANCIÓN DE DISPOSITIVOS DISCRETOS

Esta nueva funcionalidad implementada en Hyper-V permite asignar directamente a una instancia de máquina virtual dispositivos hardware disponibles a través de PCIe (PCI Express) de forma exclusiva.

El uso de esta característica omite la capa de virtualización que implementa Hyper-V lo que se traduce en un acceso más rápido al dispositivo asociado.

Esta funcionalidad requiere de una capacitación por parte del equipo que soporta el servicio de Hyper-V por lo que no es posible hacer uso de sus beneficios si no se dispone de los elementos adecuados. Para consultar dichos requisitos consulte el siguiente enlace:

https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows

9.3 COMPATIBILIDAD DE CIFRADO

Hasta ahora solo las máquinas virtuales de generación 2 poseían la capacidad de cifrado para proteger los recursos que éstas contenían.

La nueva versión de Hyper-V sobre Windows Server 2016 permite proteger el disco del sistema operativo mediante el cifrado de unidad BitLocker en máquinas virtuales de generación 1. Esta nueva funcionalidad hace uso de una unidad pequeña y dedicada para almacenar la clave de BitLocker de la unidad del sistema.

Esta característica permite omitir el uso de un Módulo de Plataforma Seguro (TPM) tal y como se hace en las máquinas de generación 2.

Para descifrar el disco e iniciar la máquina virtual, el host de Hyper-V debe ser parte de un tejido protegido autorizado o poseer la clave privada de uno de los guardianes de la máquina virtual. El almacenamiento de claves requiere una maquina con al menos una versión 8.

Nota: Para obtener información acerca de la versión de la máquina virtual consulte el siguiente enlace: https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/deploy/upgrade-virtual-machine-version-in-hyper-v-on-windows-or-windows-server

Además de esta característica cabe mencionar el hecho de que elementos como Device Guard y Credential Guard se encuentran disponibles en máquinas virtuales de generación 2 a partir de la versión 8.

9.4 PROTECCIÓN DE RECURSOS FÍSICOS DE HYPER-V

Esta característica está enfocada en optimizar los recursos de hardware de la máquina que soporta el servicio de Hyper-V (host). Dicha opción ayuda a evitar que una máquina virtual use más recursos de los que le son asignados.

Con esto será posible evitar que la apropiación excesiva de dichos recursos por parte de una máquina virtual degrade el rendimiento del host u otras máquinas virtuales disponibles.

Con esta nueva funcionalidad, si la monitorización de Hyper-V detecta una máquina virtual con actividad excesiva, esta máquina virtual recibirá menos recursos. Esta característica está desactivada por defecto en Windows Server 2016. Para habilitarla será necesarios realizarlo por cada máquina que requiera monitorizar sus recursos. Es posible hacer uso de Windows PowerShell para activarlo o desactivarlo a través de la ejecución del siguiente comando.

```
Set-VMProcessor [nombre_maquina] -EnableHostResourceProtection {$true / $false}
```

9.5 MODIFICACIÓN DE CONFIGURACIÓN EN CALIENTE

Hasta ahora ciertas configuraciones de las máquinas virtuales de Hyper-V requerían que dicha máquina se encontrase apagada para poder modificar los parámetros. Esto cambia a partir de la nueva versión de Hyper-V.

La primera de las configuraciones de Hyper-V que se beneficia de esta funcionalidad es la posibilidad de agregar o eliminar un adaptador de red virtual mientras la máquina virtual se encuentra en ejecución sin necesidad de apagar dicha máquina lo que se traduce en eliminar el tiempo de inactividad de la máquina.

Del mismo modo esta nueva característica se aplica a la memoria virtual asignada a las máquinas virtuales independientemente de si ha establecido la configuración de memoria dinámica.

A pesar de esto es necesario tener en consideración que la adición y eliminación de adaptadores de red en caliente solo es posible sobre máquinas virtuales de generación 2 mientras que la modificación de memoria virtual es aplicable sobre máquinas virtuales de generación 1 y 2. También debe tener en cuenta que el Sistema operativo invitado debe ser Windows Server 2016 o Windows 10.

9.6 MEJORAS EN EL ADMINISTRADOR DE HYPER-V

El administrador de Hyper-V es la consola que permite gestionar todos los parámetros de las máquinas virtuales, crear o eliminar máquinas virtuales, iniciarlas y demás acciones de gestión.

La nueva versión de Hyper-V ha añadido nuevas mejoras a este administrador en Windows Server 2016 dentro de las cuales destacan:

a) **Soporte de credenciales alternativo.** Ahora es posible utilizar un conjunto diferente de credenciales en el Administrador de Hyper-V cuando se realiza una conexión a otro servidor remoto son sistemas operativo Windows Server 2016 o Windows 10.

b) **Administrar versiones anteriores.** Esta mejora en el Administrador de Hyper-V en Windows Server 2016 brinda la posibilidad de administrar equipos que ejecutan Hyper-V sobre sistemas operativos Windows Server 2012, Windows 8, Windows Server 2012 R2 y Windows 8.1.

c) **Protocolo de administración actualizado.** Esta mejora permite que el Administrador de Hyper-V se comunique con otros hosts Hyper-V remotos haciendo uso del protocolo WS-MAN, el cual permite la autenticación CredSSP, Kerberos o NTLM.

9.7 SERVICIOS DE INTEGRACIÓN A TRAVÉS DE WINDOWS UPDATE

Las actualizaciones de los servicios de integración para invitados de Windows son distribuidas a través de Windows Update, por ello para los proveedores de servicios y los hosts de las nubes privadas, esto pone el control de aplicar actualizaciones en las manos de los invitados propietarios de las máquinas virtuales.

Con esto, los inquilinos tendrán la capacidad de actualizar sus máquinas virtuales de Windows con todas las actualizaciones, incluidos los servicios de integración, utilizando un solo método.

9.8 ARRANQUE SEGURO

Con esta nueva característica en Hyper-V, los sistemas operativos Linux ejecutados en máquinas virtuales de generación 2 ahora pueden arrancar con la opción “Arranque seguro” habilitada.

Los sistemas operativos invitados que pueden hacer uso de dicha característica en Hyper-V sobre Windows Server 2016 son: Ubuntu 14.04 y posterior, SUSE Linux Enterprise Server 12 y posterior, Red Hat Enterprise Linux 7.0 y posteriores y CentOS 7.0 y posteriores.

Antes de arrancar la máquina virtual por primera vez, será necesario configurar dicha máquina para que haga uso de la autoridad de certificación Microsoft UEFI. Dicha acción es posible a través del Administrador de Hyper-V, el Administrador de la máquina virtual o una sesión de PowerShell de Windows con privilegios de administrador. En el caso de hacer uso de Powershell será necesario ejecutar el siguiente comando:

```
Set-VMFirmware [nombre_maquina] -SecureBootTemplate MicrosoftUEFICertificateAuthority
```

9.9 VIRTUALIZACIÓN ANIDADA

Esta nueva función de Hyper-V permite utilizar una máquina virtual como host de Hyper-V albergando otras máquinas virtuales permitiendo de este modo virtualizar sobre la virtualización.

Sin embargo, esta característica requiere de unos requisitos previos:

a) Tanto el host de Hyper-V como el invitado que pretenda virtualizar requiere como sistema operativo Windows Server 2016 o Windows 10.

b) Un procesador Intel VT-x.

Actualmente solo los procesadores Intel permiten realizar la virtualización anidada.

Nota: Puede obtener más información sobre la virtualización anidada a través del siguiente enlace: https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/user-guide/nested-virtualization

9.10 FUNCIONES DE RED

La virtualización en un servidor permite ejecutar simultáneamente en un único host físico varias máquinas virtuales con diferentes servicios.

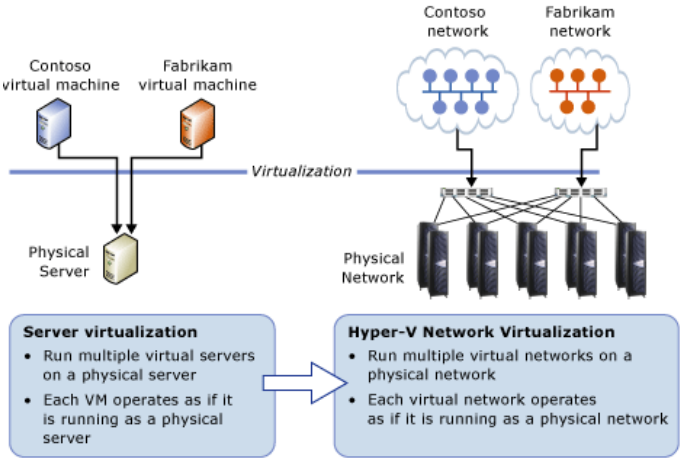


Figura 1: Virtualización frente a la virtualización de la red

En Hyper-V sobre Windows Server 2016 se han añadido nuevas funciones de red las cuales se resumen a continuación:

a) **Acceso directo a memoria remota (RDMA) e interconexión de equipos incrustados (SET):** Con esta función será posible configurar RDMA en los adaptadores de red vinculados a un conmutador virtual de Hyper-V, independientemente de si SET también se usa.

b) **Multicuotas de máquinas virtuales (VMMQ - Virtual machine multi queues):** Gracias a esta opción se mejora el rendimiento de VMQ ya que serán asignadas múltiples colas de hardware por máquina virtual. La cola predeterminada se convierte en un conjunto de colas para una máquina virtual y el tráfico se distribuye entre las colas optimizando su rendimiento.

c) **Calidad de servicio (QoS):** Esta función administra la clase predeterminada de tráfico a través del conmutador virtual dentro del ancho de banda predeterminado de la clase.

Nota: Puede obtener más información sobre las novedades de red en el siguiente enlace:
https://docs.microsoft.com/es-es/windows-server/networking/what-s-new-in-networking

9.11 PUNTOS DE CONTROL "EN PRODUCCIÓN"

A partir de Hyper-V en Windows Server 2016 es posible elegir entre puntos de control estándar o puntos de control de producción. Estos últimos son la opción predeterminada para las nuevas máquinas virtuales creadas.

A continuación, se definen las diferencias entre los citados puntos de control:

a) Puntos de control de producción. Este tipo de punto de control es una imagen "puntual" de una máquina virtual, que es posible restaurar en cualquier momento de forma que sea completamente compatible con todas las cargas de trabajo en ejecución. Esto es posible mediante el uso de la tecnología de respaldo dentro del huésped para crear el punto de control, en lugar de usar la tecnología de estado guardado.

b) Puntos de control estándar. Este tipo de punto de control captura el estado, los datos y la configuración de hardware de una máquina virtual en ejecución y están diseñados para usarse en escenario de desarrollo y prueba. Estos puntos de control son útiles para volver a un estado o condición específica tras la realización de una prueba que pueda provocar un problema en la máquina virtual.

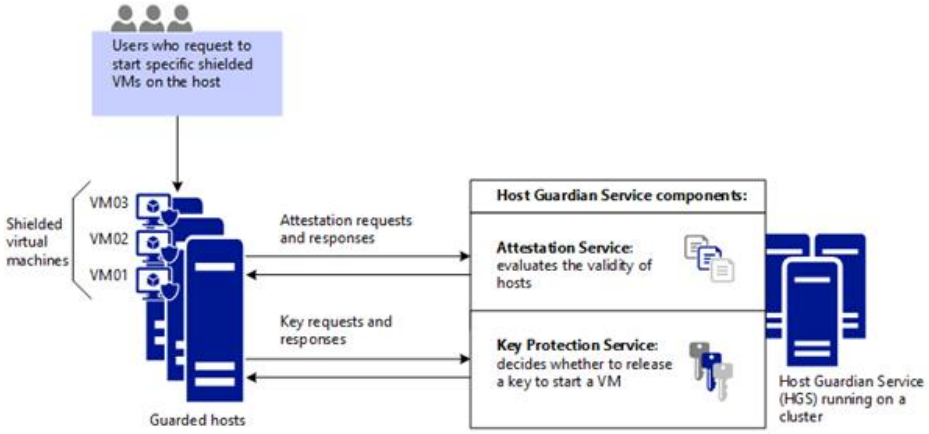
Los puntos de control en producción ofrecen una manera de aplicar un punto de control que cumple con las políticas de soporte técnico cuando una máquina virtual ejecuta una carga de trabajo de producción.

Los puntos de control de producción están basados en la tecnología de copia de seguridad dentro del invitado en lugar de un estado guardado. Para máquinas virtuales de Windows, se utiliza el Servicio de instantáneas de volumen (VSS). Para máquinas virtuales Linux, los búferes del sistema de archivos se vacían para crear un punto de control que sea consistente con el sistema de archivos.

9.12 MÁQUINAS VIRTUALES BLINDADAS

Esta nueva funcionalidad de Hyper-V utiliza diversas funciones que permiten hacer más difícil que los administradores de Hyper-V y el malware que pueda hospedarse en la máquina que alberga Hyper-V (host) inspeccionen, manipulen o roben datos del estado de una máquina virtual protegida.

Los datos de la máquina virtual y el estado de la misma están cifrados por lo que los administradores no pueden ver la salida de video y los discos. Adicional a esta seguridad es posible restringir la ejecución de las máquinas virtuales en host conocidos y confiables.



Nota: Puede obtener más información sobre el blindaje de máquinas virtuales en el siguiente enlace: https://docs.microsoft.com/es-es/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

9.13 CONTENEDORES DE WINDOWS

Los contenedores en Windows Server 2016 hacen posible que muchas aplicaciones aisladas sean ejecutadas en un sistema informático. Dichos contenedores son rápidos de crear, además de ser altamente escalables y portátiles.

Hay dos tipos de tiempo de ejecución de contenedor disponibles, cada uno con un grado diferente de aislamiento de aplicaciones. Los contenedores de Windows Server 2016 utilizan el espacio de nombres y aislamiento de procesos y los contenedores de Hyper-V usan una máquina virtual ligera para cada contenedor.

Las características fundamentales de los contenedores son:

a) Soporte para sitios web y aplicaciones utilizando HTTPS.

b) El servidor Nano puede alojar tanto Windows Server como Hyper-V Containers.

c) Posibilidad de administrar datos a través de carpetas compartidas de contenedores.

d) Capacidad para restringir los recursos del contenedor creado.

9.14 WINDOWS POWERSHELL DIRECT

Esta nueva función de Hyper-V en Windows Server 2016 proporciona una forma práctica de ejecutar comandos de Windows PowerShell en una máquina virtual desde el host.

Windows PowerShell Direct se ejecuta entre el host y la máquina virtual lo que implica la no necesidad de requisitos de conexión en red o firewall, y funciona independientemente de su configuración de administración remota.

Nota: Puede obtener más información de PowerShell Direct a través del siguiente enlace: https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/manage/manage-windows-virtual-machines-with-powershell-direct