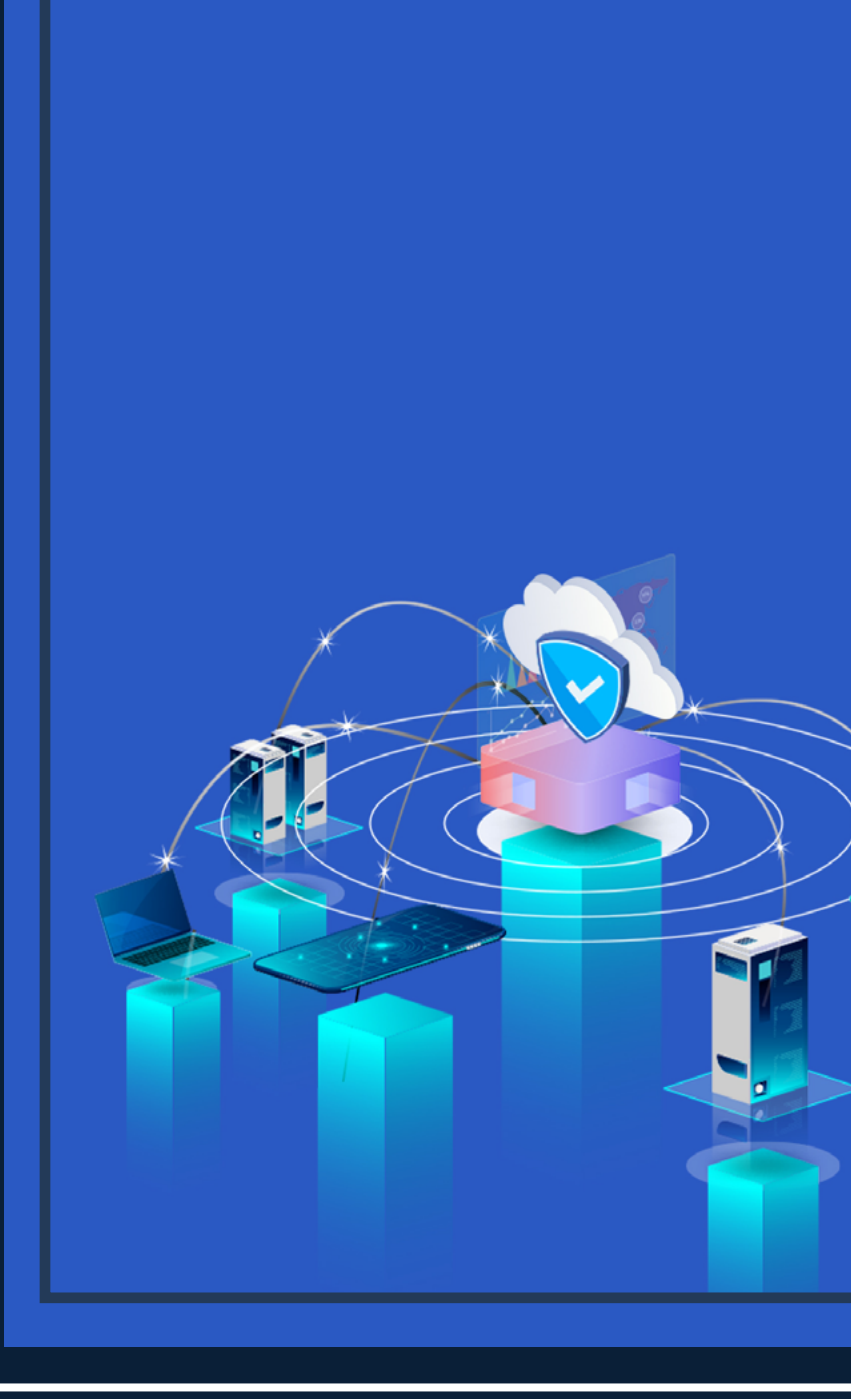
CCN-CERT

BP/15



Best Practices in Virtualisation

GOOD PRACTICE REPORT

AUGUST **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edit

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEDE-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.09.11 08:33:46 +02'00

Centro Criptológico Nacional, 2021

Date of edition: August 2021

Index

Index

1. About CCN-CERT, National Governmental Cert

The CCN-CERT is the Information Security Incident Response Team of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

The CCN-CERT is the Information Security Incident Response Team of the National Cryptologic Centre

Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, by being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centres.

Its ultimate aim is to make cyberspace more secure and reliable, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

2. Introduction

Virtualisation is a term that has been used for multiple technologies. In the world of computing, it is understood as the recreation of a physical (hardware) or logical (software) resource, by means of a hypervisor that allows the execution of more than one environment at the same time. In the virtual machine environment, the hypervisor allows the simultaneous use of hardware for more than one operating system, controls the physical layer (RAM, CPU, disk, etc.), which can be accessed only by it, and presents the virtual machines with a compatible hardware interface.

The system providing the physical media and on which the hypervisor is installed is known as the *host*. The virtual machine that interacts with the hypervisor and where a complete operating system is usually installed is called *guest*. The number of virtual machines that a *host* can support depends directly on the physical resources available and the demands of each *guest*.

The hypervisor manages access to different resources individually and with varying degrees of isolation, depending on the model and needs. Without it, the hardware would have decision-making problems when it comes to meeting usage demands from unconnected and uncoordinated systems.

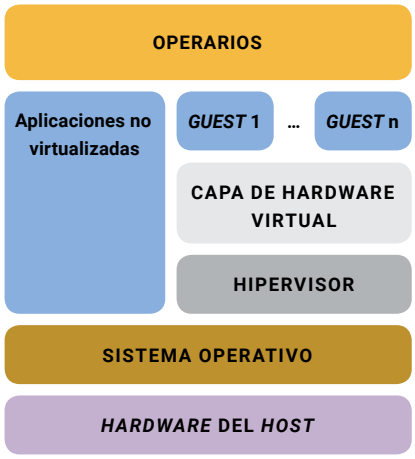
The rise of virtualisation has come with the use of the cloud, where a resource sharing system is indispensable. Although there were already multiple systems from many manufacturers, the development and progress of these systems has increased exponentially. Currently, Citrix's XenServer, Dell's VMware ESXi, Oracle's Oracle VM Server, Oracle's VirtualBox and Microsoft's Hyper-V, among others, are available.

The number of virtual machines that a *host* can support depends directly on the physical resources available and the demands of each *guest*

As far as Microsoft is concerned, the multinational has been incorporating virtualisation tools since the middle of the first decade of this century. With the distribution of the Windows Server 2008 operating system, the initial version of Hyper-V was released. Since then, each new version or release includes a hypervisor with more and better capabilities.

VMware started working with virtualisation in 1998. This company, a subsidiary of Dell, is currently one of the main providers of this type of software. Its hypervisor runs on the main operating systems of the market (Windows, Linux and Mac OS). In addition, it has a specific version that allows the hypervisor to run on the hardware of physical servers, without the need for an additional operating system. It also offers the possibility of installation from USB memory stick, so that computers with USB input can run it without using hard disks, which are freed up for virtual machines.

VirtualBox, on the other hand, started in 1997 to offer virtualisation software for all major operating systems, including Solaris. Its ease of use and GNU licensing (General Public License version 2) have made it very popular, especially in desktop environments. It is now owned by Oracle, which also owns another high-performance hypervisor (Oracle VM Server) designed for enterprise and cloud environments.



[Illustration 1]
Example of assembly diagram of several virtual machines.

The rise of virtualisation has come with the use of the cloud

3. Types of virtualisation

The main taxonomies of virtualisation depend on how the hardware is distributed and which element is virtualised. Regarding the first point, the partitioning of a physical resource such as RAM, CPU, etc. is known as partitioning. One way of doing this is by assigning absolute and static values (hard partitioning).

In these cases, the sum of the partial resources will always be equal to or less than the existing total value. As an example, if an eight-core *host* hosts three virtual machines that have each been assigned two cores, only one new machine with one core could be included (the other core should be for the operating system and the hypervisor). This way of allocation ensures resources and greater isolation, but does not optimise the hardware elements.

In certain cases, in order to optimise resources, the majority of hypervisors allow a distribution of resources with over-allocation (soft partitioning). Continuing with the previous example, in this environment the sum of the cores can be greater than the actual number of cores available on the machine. The rationale for allowing this is that all virtual machines will never reach maximum processing capacity utilisation simultaneously. If this were the case, a proportional distribution would proceed.

When categorisation is based on the virtualised element, the main virtualisation possibilities are hardware, applications or user sessions.

The focus of this guide is on the virtualisation of hardware, both with soft and hard partitioning.

The focus of this guide is on the virtualisation of hardware, both with soft and hard partitioning

4. Security challenges in Virtualisation

Security in virtualisation has the same premise as any other system, "minimise the exposure surface". However, it has particularities that hinder the securization of this surface, such as the multitude of shared resources or the operating systems that run simultaneously with their own applications on the same physical machine.

In a situation where you have a Windows 10 *host* where several guests are virtualised with the same operating system version, the protection of each machines (*host* and *guest*) will require to multiply efforts. If you include a diametrically different operating system, such as Oracle Linux, efforts increase proportionately, but the knowledge required of the system administrator is doubled. In addition, good security practices specific to hypervisors and their management shall be applied.

To reduce the complexity of managing this type of environment, manufacturers are applying their own (built in) measures, which are increasingly effective and secure: SMB 3.0 (with end-to-end encryption), network isolation, network extensions, etc.

General considerations that apply to non-virtualised systems must also be taken into account. For example, web browsing and e-mail are two of the main attack vectors for systems. There is no such thing as an "absolutely secure configuration", but a number of reasonably adequate security measures can always be implemented to achieve a reliable working environment of the hypervisor-host-guest set.

Ultimately, the main issue of virtualisation, as far as security is concerned, is to treat the system as if it were a complete data processing centre where perimeter measures (applied to the *host*) and individual measures for each of the machines hosted (applied to the *host* and to each of the virtual machines) are established.

For example, web browsing and e-mail are two of the main attack vectors for systems

5. Types of virtualised networks

When creating virtual machines on a single *host*, you can assign all physical network interfaces to a single *guest*, associate all virtual machines to a single adapter, or make a more balanced distribution.

As far as possible, one should try to rationalise the allocation of resources, as overloading a network card with many guests considerably penalises performance. This is observable on physical servers, but even more so on laptops or desktops where it is difficult to have more than one network connection, either because of the equipment itself or because of the lack of available connections at the users' workstations. Moreover, the individualised use of network interfaces runs counter to the spirit of virtualisation, where resource utilisation by more than one instance is almost the norm.

For all the above reasons, vendors have pursued network virtualisation strategies that allow the bandwidth of one or more interfaces to be shared across all machines that require it and are hosted on the *host*. The rationale is the creation of virtual network cards at the virtualisation abstraction layer, managed by the hypervisor, which are allocated to the guests. The network cards can then be left isolated or connected to the physical network devices.

The virtual switch adds additional features being one form of *host* network hardware sharing, the equivalent of which in a physical data network would be the installation of a conventional switch. It is created and managed by the hypervisor, has OSI model layer 2 functionalities, allowing, for example, the creation of VLANs.

In addition, having multiple virtual switches makes it possible to manage *guest* networks with a higher level of isolation.

The rationale is the creation of virtual network cards at the virtualisation abstraction layer, managed by the hypervisor, which are allocated to the *guest*

6. Hyper-V best practices

Hyper-V has two (2) server installation options: core mode and graphical mode. The fundamental difference is that the core mode does not have a graphical management environment from the local machine.

In terms of best practices, these should be host-oriented first and then aimed at each of the hosted machines.

Microsoft's hypervisor administration allows remote management. However, it is not recommended to do it only with the system's own measures, additional measures such as data encryption of the connection should be added. See section "Setting Namespace Security to Require Data Encryption for Remote Connections" in the article Securing a Remote WMI Connection available through the following link.

https://docs.microsoft.com/es-es/windows/desktop/WmiSdk/securing-a-remote-wmi-connection#setting-namespace-security-to-require-data-encryption-for-remote-connections

With regard to *guest* systems, the following good practices should be taken into account:

a. Establish a correct management of permissions, preventing access to files to any user who does not require it, either remotely or locally.

b. Synchronise time for reliable auditing and records.

c. Manage files securely. Files shall be encrypted with BitLocker and those that are not being used shall be deleted with secure tools such as Eraser for Windows or KillDisk for GNU/Linux, as well as others such as HDDEraser (self-booting for the total erasure of disks).

d. Keep *host*, *guest* and integration services up to date. At the very least, security patches considered important and critical should be installed.

e. Use a product to prevent malicious code and firewall solutions on *guest* computers or use switch extensions that integrate them. Simultaneous application of both options is not incompatible.

f. Avoid having active CDs or DVDs on clients, as the ISO images themselves mounted from the *host* hard disk could increase the exposure surface.

g. Maintain maximum isolation of the network, creating only those connections that are essential.

h. As far as possible, avoid sharing resources between virtual machines or with the *host*. Where absolutely necessary, maintain a permission policy as restrictive as possible.

Regarding the continuity of service, it is highly recommended to make backups. Backup files may be stored locally, on network resources or on removable media (e.g. an external USB hard disk). In these cases, data encryption is a must, a measure that must be imposed on all media used, whether internal or external.

Backup files may be stored locally, on network resources or on removable media

6.1 Virtual machine creation and resource allocation

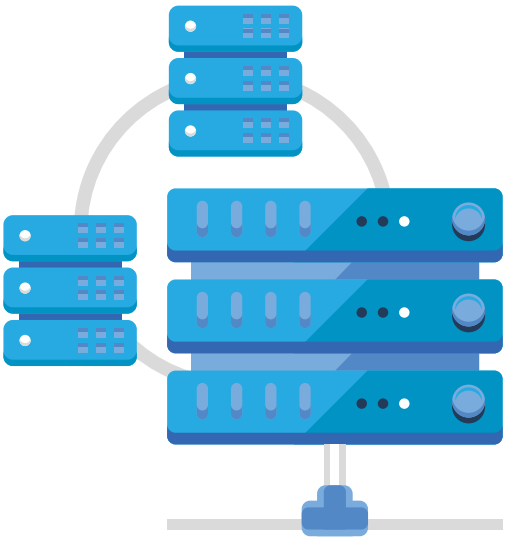
To create a *guest* in Hyper-V, a wizard is used that is very similar in Windows 10 Professional or Enterprise and in the server versions. This wizard allows both the quick creation of virtual machines and their import from other virtualisation environments. Microsoft's technology supports a wide variety of desktop and server operating systems, whether Windows or Linux.

The allocation of virtualised hardware resources can be done in two ways. On the one hand, from Hyper-V Manager and as soon as you run the wizard, type the name of the machine and then click on "Finish". In this case, the Hypervisor allocates RAM memory, disk space and network automatically. On the other hand, if you choose to continue with the wizard, you can manually define the resources and take into account the Microsoft article about Performance Optimisation for Hyper-V servers, available at the following link:

https://docs.microsoft.com/es-es/windows-server/administration/performance-tuning/role/hyper-v-server/

In order to use resource allocation correctly, it is necessary to know some concepts for better resource management.

In order to use resource allocation correctly, it is necessary to know some concepts for better resource management



6.1.1 RAM memory

In Hyper-V there are two (2) types of memory resource allocation, dynamic allocation and static allocation.

Dynamic memory is a feature of Hyper-V that allows the hypervisor to manage the RAM consumption of the host's guests in a flexible way. For example, the hypervisor can dynamically add more RAM to a *guest* when the operating system needs it or reclaim excess RAM when the *guest* is idle. This technology is especially useful when you have a lot of idle or under-workloaded virtual machines.

If you decide to use dynamic memory, you need to set some configuration values for it. If you opt for static allocation, you need to be especially careful with running machines, as the RAM chosen will be reserved for the *guest* once it starts up, even if it is not being used.

For this reason, it is necessary to be especially careful with the machines started, choosing only those that are essential.

- **Boot RAM:** is the amount of RAM allocated to a *guest* at boot time. This value can be the same as the "minimum RAM" or more, up to the "maximum RAM". The boot RAM value can only be changed when the virtual machine is off. Once the virtual machine boot is complete and the hypervisor has been started, it will attempt to use the amount of RAM configured as the minimum RAM.
- **Minimum RAM:** The minimum amount of RAM that the *host* should attempt to allocate to a virtual machine when started. When multiple memories demand memory, the Hyper-V *host* can reallocate virtual machine RAM until its minimum RAM value is met.
- **Maximum RAM:** is the maximum amount of RAM that the *host* will provide to the virtual machine. This option can only be increased while the virtual machine is running and cannot be decreased unless the virtual machine is turned off.
- **Memory Buffer:** This is the percentage of memory that Hyper-V should allocate to the virtual machine as a buffer. The value can be set in the range of 5% to 200% with 20% set by default.
- **Memory Weight:** The priority that is configured for a virtual machine compared to other virtual machines running on the same Hyper-V *host*.

Static memory allocation implies the reservation of the total memory available on the *host*, which translates into the need to properly size the allocation so that it does not exceed the total available memory, taking into consideration the guests that may be active at the same time.

Static memory allocation implies the reservation of the total memory available on the *host*, which translates into the need to properly size the allocation

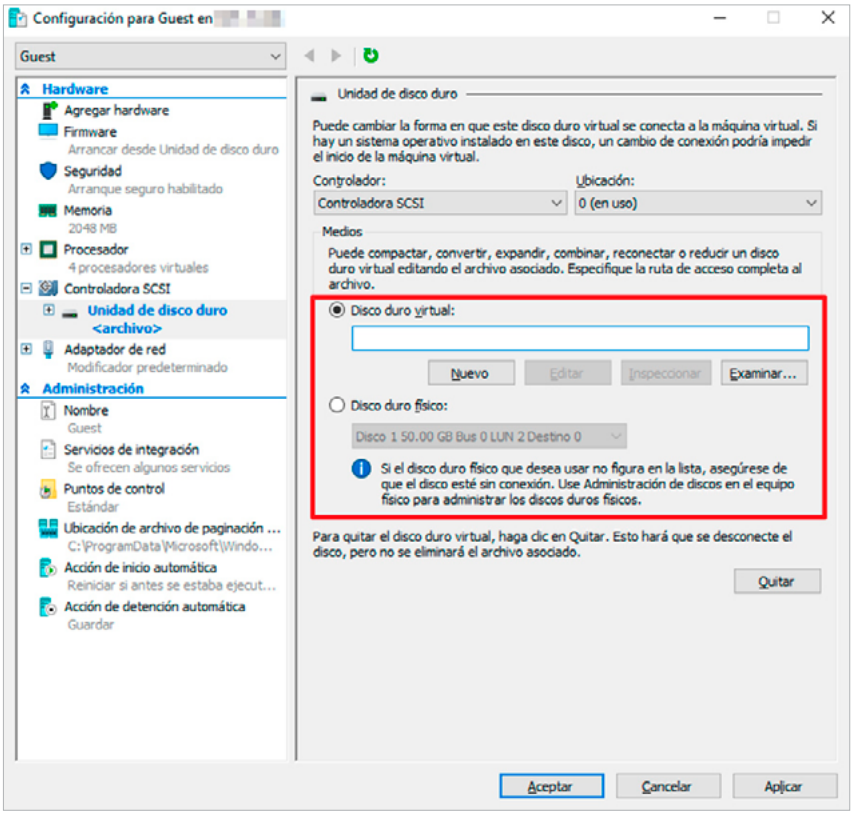
6.1.2 Disk

In terms of storage space allocation, there are several configurations regarding the disk and disk types to select in Hyper-V.

Two (2) disk models can be created or assigned as required:

- **Virtual hard disk:** this is a disk that is created in the *host* to be associated with the virtual machine where all the information generated can be stored. These disks are the most widely used as they generate their own file that can undergo various modifications while maintaining the storage capacity, being able to perform, for example, exports, checkpoints, etc.
- **Physical hard disk:** this configuration allows you to associate a disk belonging to the *host* (real hardware) to the virtual machine. This option can be useful in certain circumstances, however, the disk remains associated to the virtual machine and the *host* cannot use the disk for any other purpose. In addition, it must be taken into consideration that the performance provided by the disk in the *guest* depends directly on it. In order to select this option, the disk must be in "offline" mode on the *host*.

[Illustration 2] Selection of the hard disk in the wizard.



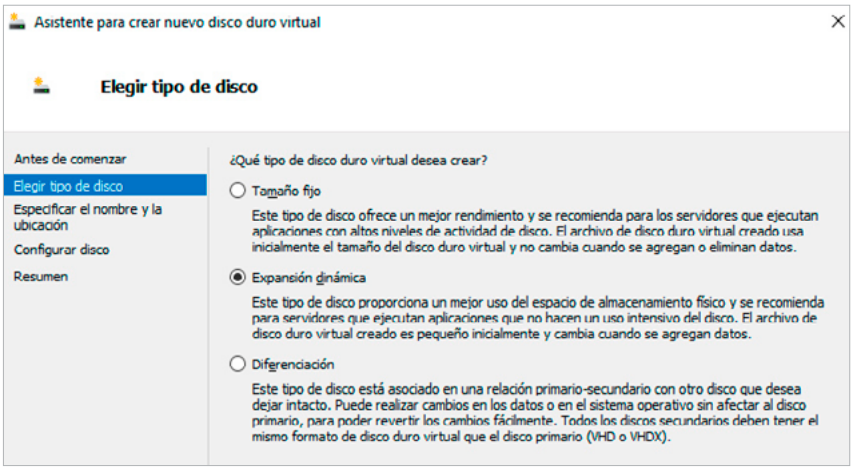
As for the type of virtual disk, the following options can be selected:.

a. **Fixed Size:** Fixed virtual hard disks provide storage capacity by using a file with a specified size for the virtual hard disk at the time of disk creation. The file size remains "fixed" regardless of the amount of data stored. However, the Wizard for editing the virtual hard disk can be used to increase the size of the virtual hard disk, which increases the file size. This setting is recommended when the implemented *guest* requires a lot of reading/writing of the disk itself.

b. **Dynamic Expansion:** Virtual hard disks of this type provide the storage capacity needed for the data. The file size is small when the disk is created and grows to the maximum allocated size as data is added to the disk. The file size does not automatically decrease when data is removed from the virtual hard disk. However, it is possible to compact the disk to reduce the file size after deleting data by using the edit virtual hard disk Wizard. This option is recommended for test or lab virtual machines, as well as in environments where little growth and low disk usage is expected.

c. **Differentiation:** These are hard disks that start from a primary virtual hard disk and allow the user to make changes from it without altering it. Their definition is exactly the same as that of the primary virtual disk in terms of type and size. The file size of a differencing disk grows as changes are stored on the disk.

[Illustration 3] Selection of the "Type" of hard disk in the virtual machine.

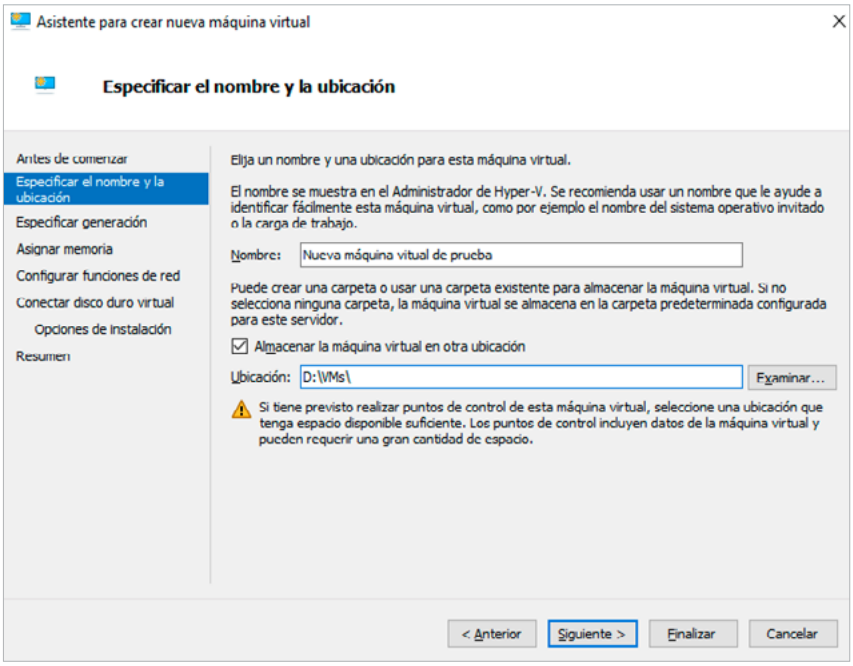


6.2 Protection of virtual machine resources

Each of the virtual machines created must be protected individually, both in the characteristics assigned from the creation wizard and within the machine itself.

After the first informative screen of the first step (where it is not advisable to opt for the creation of a machine with default values), in the second step you must select the location of the virtual machine. It is advisable to use a dedicated folder to facilitate the protection of the virtual machine by means of NTFS permissions, encryption, etc. If you are on a single hard disk machine, you should consider that the use of partitions may reduce the exposure surface, but this is detrimental to performance.

The choice of the location can help with the subsequent protection of the virtual machine



[Illustration 4]
Selection of the location of the virtual machine.

The choice of the location can help with the subsequent protection of the virtual machine. For this purpose, the folder where the virtual machine definition is stored and the hard disks must have at least the following permissions:

[Table 1] Directory permissions of virtual machines and hard disks.

ACCOUNT	PERMITS	APPLY TO
Administrators	Full control	This folder, subfolders and files
System	Full control	This folder, subfolders and files
Creator owner	Full control	Subfolders and files only

Once the final destination folder for the guests that will be created is chosen, the corresponding path can be set in the general properties of the hypervisor. To do this, click on "Hyper-V Configuration..." and **in the pop-up window you shall change the configuration of the sections "Virtual hard disks" and "Virtual machines".** This avoids having to make these modifications each time a virtual machine is created.

In cases where additional users or groups need to be added, it is recommended to use the minimum number of permissions necessary and remove them when they are no longer needed. Microsoft, during the hypervisor installation, creates the empty "Hyper-V Administrators" group account. If it is used, it should also be given full control permissions on the folders.

This management over the Access Control List (ACL) will prevent files related to virtual machines from being altered, copied or accessed over the network in an unauthorised way by anyone without high privileges. As an additional measure, **auditing of access to the folders hosting virtualisation files can be enabled to track access by authorised accounts** and even for failed access attempts to other accounts.

In the next step, what Microsoft calls the "Generation" is selected. If the *guest* operating system can work in UEFI environments, Generation 2 must be selected. UEFI provides additional security compared to classic BIOS.

NOTE:

To learn more about Extensible Firmware Interface, UEFI, and to obtain its specifications, please refer to the following link: https://www.intel.es/content/www/es/es/architecture-and-technology/unified-extensible-firmware-interface/efi-homepage-general-technology.html

The document *CCN-CERT IA-08/15 Amenazas BIOS Threats* available through the following link https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/789-ccn-cert-ia-08-15-amenaza-en-bios/file.html to increase security in this type of elements

6.3 Encryption

When required by the virtual machines hosted on the *host*, files should be protected using *BitLocker* encryption, provided that the machine has BitLocker encryption capability. To learn more about *BitLocker*, please review the background document on Microsoft's TechNet website, available via the following link.

https://docs.microsoft.com/es-es/previous-versions/windows/server/hh831713(v=ws.11)

Encrypting files by means of Encrypting File System (EFS) is not a valid option, as this would not allow the use of the disks or definition files by accounts other than the one providing the certificate used for encryption. In certain domain environments, master decryption accounts may exist, but should not be relied upon without certainty of their existence. More information on Encrypting File System (EFS) can be found here:

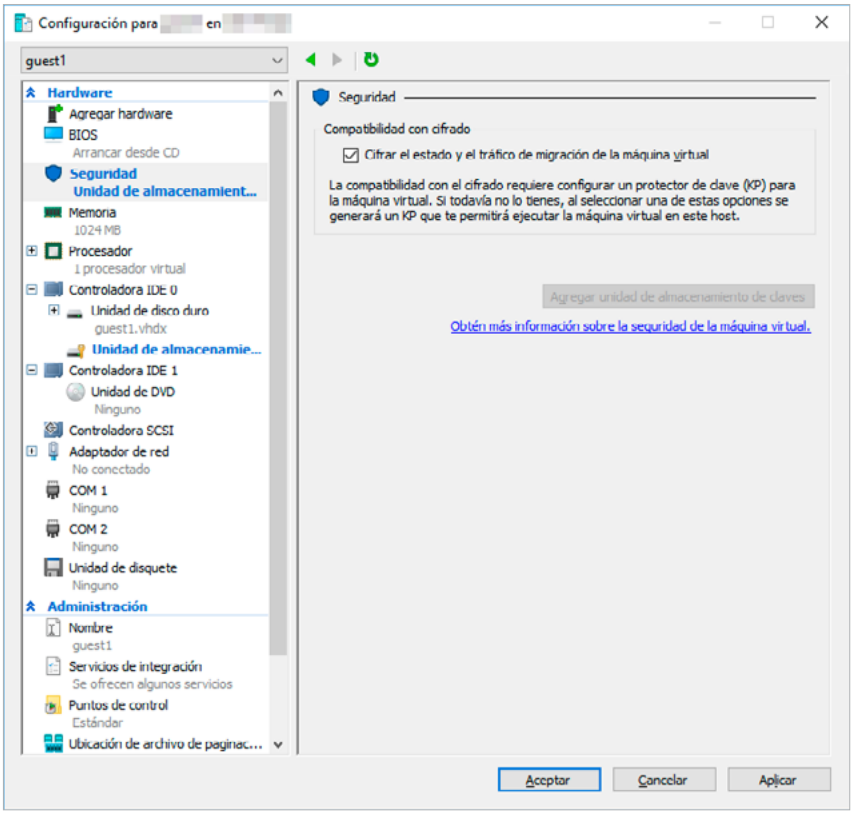
https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption

The use of BitLocker within a virtual machine is not generally available. However, the EFS system can be used, as usual, for the encryption of files containing sensitive information. However, always with the caveat indicated above, about the single user access.

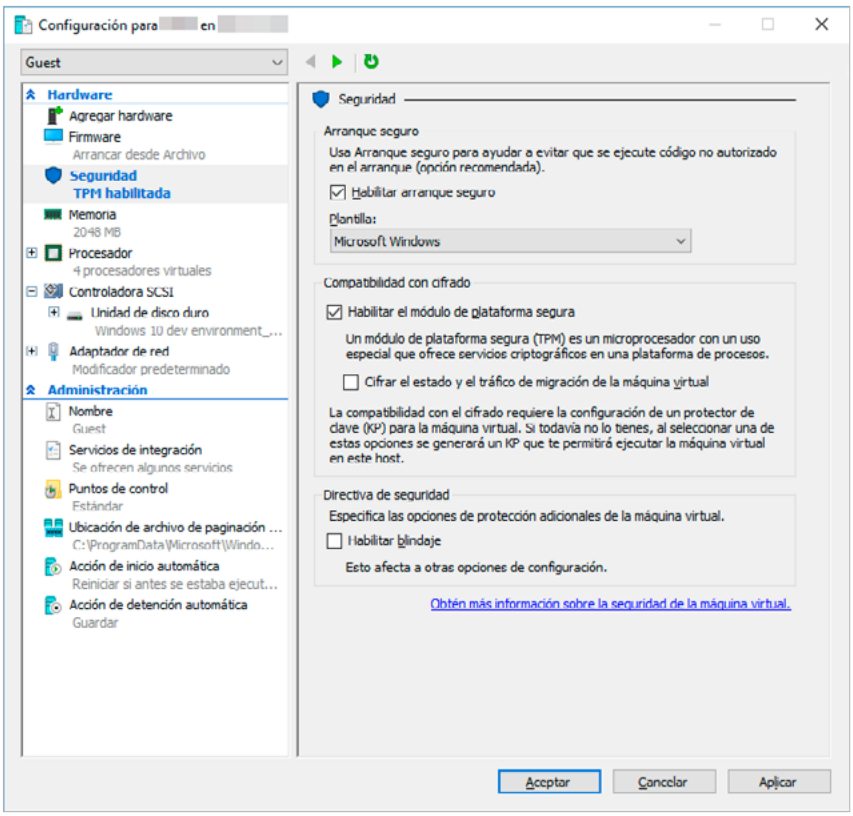
Until now, only generation 2 virtual machines have had the encryption capability to protect the resources they contain. **The new version of Hyper-V makes it possible to protect the operating system disk using BitLocker drive encryption on generation 1 virtual machines.** This new functionality makes use of a small, dedicated drive to store the BitLocker key of the system drive.

When required by the virtual machines hosted on the *host*, files should be protected using *BitLocker* encryption

[Illustration 5] Encryption configuration on Generation 1 machine.



As indicated above, Generation 2 virtual machines can still make use of the functionality of a virtual TPM that allows the virtual machine disk to be encrypted using *BitLocker* as if it were a physical machine.



[Illustration 6] Encryption configuration on Generation 2 machine.

Another novelty in Hyper-V 2016 is the so-called "Shielded Virtual Machines", which allows virtual machines and their state to be encrypted in a way that ensures that they only run on hosts authorised by the Host Protection Service. Further information can be found in the following links:

https://docs.microsoft.com/es-es/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

https://docs.microsoft.com/es-es/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms-top-node

Shielded virtual machines protect the data and state of the virtual machine against theft and manipulation of administrator privileges. Shielded virtual machines work with Generation 2 virtual machines, which provide the required secure boot, UEFI firmware and virtual TPM (vTPM) 2.0 support. The Hyper-V *host* must run Windows Server 2016 or Windows 10, and the *guest* operating system hosted in the virtual machine must be Windows Server 2012 or higher.

Shielded virtual machines protect the data and state of the virtual machine against theft and manipulation of administrator privileges

Shielded virtual machines offer the following benefits:

- **Disks are encrypted.**
- **The working process of the virtual machines is strengthened to help prevent possible manipulation (VMWP).**
- **PowerShell direct locking and console access.**

6.4 Network isolation and configuration

The creation of the virtual machine should, in most cases, rely on an unconnected virtual network adapter. Later, once all necessary security measures have been implemented, it will be attached to the appropriate switch. Microsoft implements, by default, a number of security measures that allow a high degree of isolation, but this shall be complemented by good practice, as this means of communication will constitute the majority of the surface area exposed by the virtual machines.

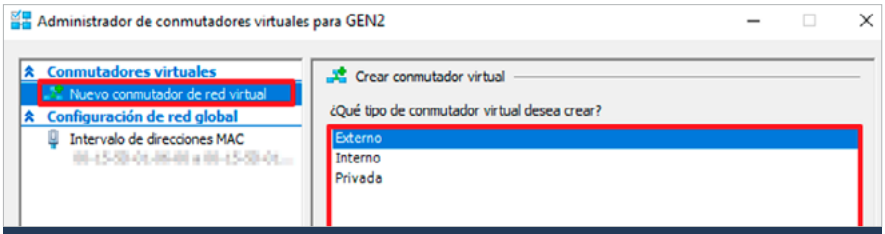
With regard to Hyper-V, this technology works with an abstraction layer of the host's physical network that creates virtual switches and network cards. It is a choice to connect these cards to these switches permanently, temporarily or not at all. You should always opt for the minimum required configuration and thus, if no connectivity is required, the virtual machine should remain with the default creation settings. Virtual network switches can be external, internal or private.

[Table 2] Description and examples of use of virtual switches.

TYPE	DESCRIPTION	EXAMPLES OF USE
External	Creates a virtual switch that is linked to the physical network adapter so that virtual machines can gain access to the physical network where it is connected.	Virtual machines need Internet connectivity. Virtual machines must be accessed by network users.
Internal	It does not connect to the host's physical network, but creates a junction point that can be used by any of the virtual machines running on it, in addition to the *host* itself.	A network of virtual machines that must interact with each other and where the *host* machine is used as a test client.
Private	It is the same as the internal one, but the host is not included as a member of this network.	A network of virtual machines that must interact with each other, but not with any other machine.

When a switch is connected to the physical network device, external switch, there are other parameters and variables that must be taken into account.

[Illustration 7]
Screen for creating an external switch.



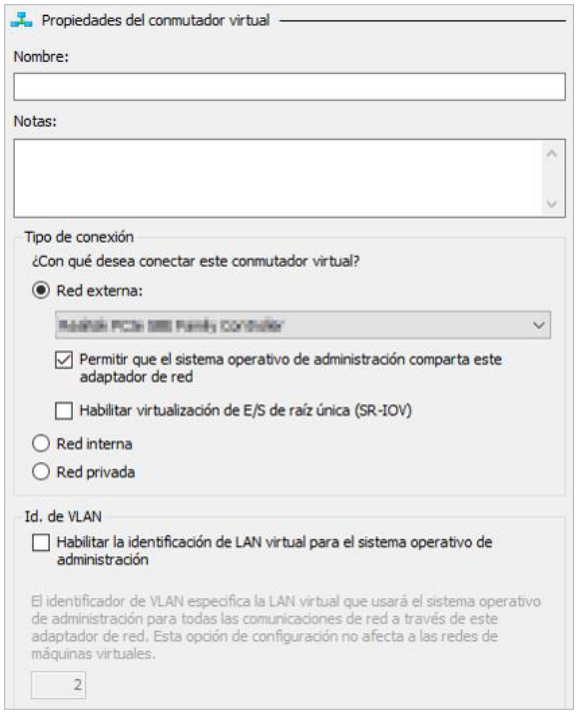
NOTE: In this example there will be connectivity to the network where the physical adapter is hosted.

The default checkbox, "Allow the management operating system to share this network adapter", confers soft partitioning values to this *host* element. Unchecking it results in a high network isolation value. But the physical adapter cannot be used on other switches or by the *host*.

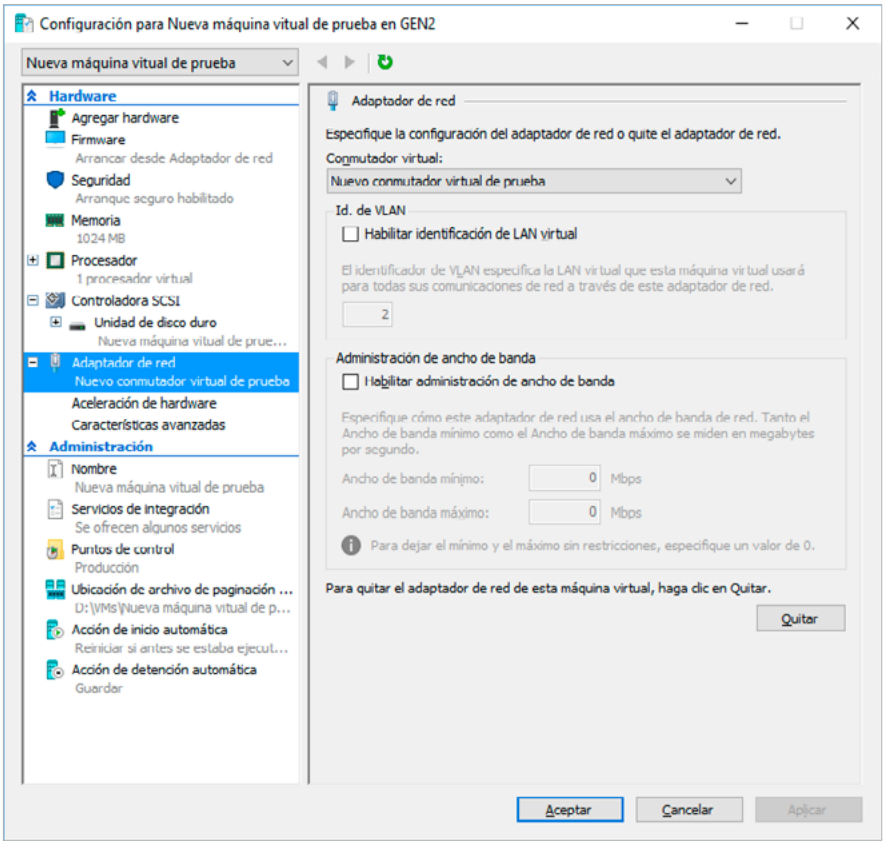
VLAN's ID", if enabled, will allow all communications from the *host* operating system to be tagged by the VLAN identifier that is selected in the box below (the default value is (2). This option will require that the physical switch port to which the host's physical network is connected allows traffic from the chosen VLAN, either because the port belongs to that network segment or because the port is a trunk connection and the VLAN is included in the list of allowed networks. It must also be ensured that the virtual machines use this switch and have a valid IP address in the chosen VLAN.

Once the disconnected virtual machine and the desired virtual network switches have been created, it is time to configure the virtual network devices as required. To do this, open the *guest* configuration and select "Network adapter".

[Illustration 8]
Properties of a virtual switch.



[Illustration 9] Configuration of a network adapter of a VM hosted on the *host*.



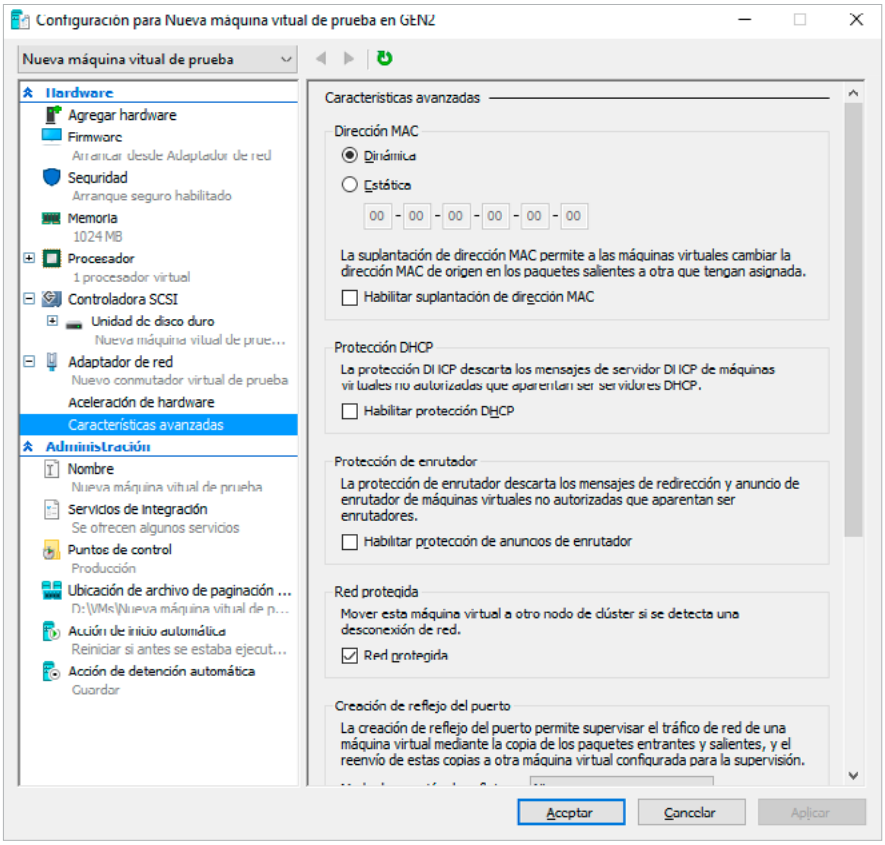
At the *guest* network adapter level, the "VLAN ID" allows you to select a Virtual Local Area Network identifier but only for that single device, not for the entire switch. It should not be selected if it iwas already configured on the virtual switch in VLAN mode.

Bandwidth management" allows the aforementioned "soft partitioning" of the physical network as well as the reservation of bandwidth for a given network adapter. In the case of the minimum, the sum of the partitions must be less than the value of the physical device to which the virtual switch is connected. **An amount reserved for the *host* itself must be deducted.** For example, for a GigaEthernet network, 100 Mbps would be blocked for the *host*.

The "Advanced Features" option leads to a window where you can enable or disable network variables that will manage protections of this element.

The "Advanced Features" option leads to a window where you can enable or disable network variables that will manage protections of this element

[Illustration 10] Advanced features of a virtual network card.



All the features in this window are necessary at some point in time in management, especially for servers, as there are generally no ideal values. Here are some quick tips that can be extrapolated to other individual cases.

[Table 3] Advanced Hyper-V network card features and usage examples.

FEATURE	DESCRIPTION	EXAMPLES OF USE
MAC address	Enables the assignment of a specific MAC or activates MAC Address Spoofing of the virtual machine.	Assign a static MAC in tests of virtual machines that are on the network device access control list.
DHCP protection	Protects against rogue DHCP servers on virtualised machines. It is advisable to activate this variable.	This option is disabled for a virtualised server aimed at testing with Active Directory and DHCP server, which is also connected to an internal network with other computers, some of them DHCP clients.
Router protection	Protects against fraudulent advertisements. It is advisable to activate this variable.	In a virtual machine forensic analysis environment it can be enabled to observe whether it sends such messages.
Protected network	It is a high availability measure.	Testing of virtual machines in high-availability clusters.
Creation of port mirroring	Activation creates a mirror port where traffic is doubled. Enabling it can increase the exposure area.	Traffic analysis for security auditing, without altering the network under study
NIC team building	The creation of "Network Teams" is a measure of high availability and increased resources.	Network high availability testing on a virtual machine that will later be put into production with this feature.
Device nomenclature	**Activating name propagation could lead to a leak of information, usually not serious, but unnecessary.** Do not activate this box without a specific need.	In a Windows test environment, without security data, you want to facilitate the task of connecting virtual machines in an internal network (it should not be activated on external switches in any case).

NOTE: More information, and PowerShell usage, on these features can be found in the article "What's New in the Hyper-V Virtual Switch in Windows Server 2012" via the following link:

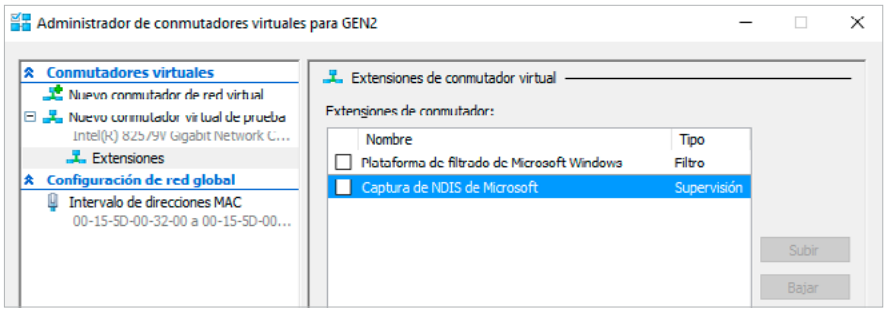
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj679878(v=ws.11)

6.5 Management of switch extensions

Virtual switch extensions allow the inclusion of third party software for filtering, capturing and forwarding network traffic. The secure configuration of each switch extension depends on the parameters of the individual vendors in general and the extension itself in particular.

With respect to Hyper-V it is provided with two extensions installed, but not enabled. These are the Microsoft Windows Filtering Platform (WFP) and the Microsoft NDIS Capture.

[Illustration 11]
Default extensions of a virtual switch in Hyper-V.



The first of these, WFP, should be enabled when required by a third party extension, with the conditioning that it could affect certain virtual machines. Please refer to the TechNet article "Hyper-V: The WFP virtual switch extension should be enabled if it is required by third party extensions" available at the following link for further information.

https://social.technet.microsoft.com/wiki/contents/articles/13071.hyper-v-the-wfp-virtual-switch-extension-should-be-enabled-if-it-is-required-by-third-party-extensions.aspx

This architecture enables network packet filtering and modification, monitoring, promiscuous connection and other functions. The NDIS Capture Extension is an API that allows extensions to be installed on the Hyper-V virtual switch driver.

Software vendors, such as "5NINE SOFTWARE", have extensions that allow the inclusion of virtual firewall, antivirus, intrusion detection system (IDS), network anomaly inspection, network traffic scanning, connection listing and statistics of virtual machines deployed on a Hyper-V server.

The NDIS Capture Extension is an API that allows extensions to be installed on the Hyper-V virtual switch driver

6.6 Integration services

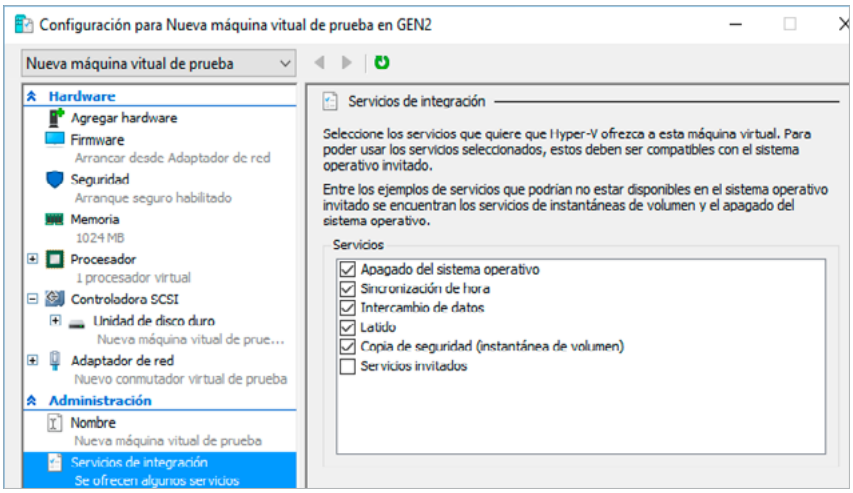
Hyper-V integration services enable the communication of virtual machines with the host. Their installation provides many advantages for performance improvement and the proper functioning of *guest* (e.g. time synchronisation), but increases the area exposed to attacks. More information can be found in the article "Managing Hyper-V integration services".

https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/manage/Manage-Hyper-V-integration-services

On Windows systems, each of the integration services is installed as a service and can be managed from the MMC as such

They work in two parts, so for a service to run it must be enabled on both ends, host and *guest*. Guests with Windows Server 2008 R2 and Windows Vista SP2 and subsequent versions incorporate the integration services by default.

Within the configuration of each Hyper-V virtual machine you can access the integration services. All of them are enabled by default, except "Guest Services".



[Illustration 12]
Integration services

On Windows systems, each of the integration services is installed as a service and can be managed from the MMC as such. You can check the services at the following link:

https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/reference/integration-services

NAME OF THE SERVICE	SERVER CONFIGURATION		GUEST OPERATING SYSTEM	
	DEFAULT VIRTUAL MACHINE CONFIGURATION	VERSIONS THAT CAN RUN ON WINDOWS HYPER-V	WINDOWS SERVICE NAME	LINUX DRIVER / DAEMON NAME
Shutting down the operating system	Enabled	Windows Server 2012 and later	Hyper-V Guest Shutdown Service	hv_utils
Time synchronisation	Enabled	Windows Server 2012 and later	Hyper-V Time Synchronisation Service	hv_utils
Data exchange	Enabled	Windows Server 2012 and later	Hyper-V Data Exchange Service	hv_utils and hv_kvp_daemon
Heartbeat	Enabled	Windows Server 2012 and later	Hyper-V Heartbeat Service	hv_utils
Backup (volume snapshot)	Enabled	Windows Server 2012 and later	Hyper-V Volume Snapshot Requester	hv_utils and hv_vss_daemon
***Guest* services**	Not enabled	Windows Server 2012 R2 and later	Hyper-V Guest System Services Interface	hv_utils and hv_fcopy_daemon

[Table 4] List of integration services.

The particular case of the data exchange integration service may require the installation of a ".cab" file, available from Microsoft's download centre. This service allows the exchange of relevant information and uses a registration key for these functions. For the download of the data exchange integration service please visit the following Microsoft link:

https://support.microsoft.com/es-es/help/3071740/hyper-v-integration-components-update-for-windows-virtual-machines-that-are-running-on-a-windows-10-based-host.

Enabling the integration service called "Guest Services" leads to communication between *host* and *guest*, even if there is no established network between them, and is therefore not recommended in sensitive environments.

6.7 Virtualisation-Based security for generation 2 virtual machines

Virtualisation-based security functionality is available in Hyper-V 2016, offering features such as *Device Guard and Credential Guard*, which provide increased operating system protection against malicious code attacks. Virtualisation-based security is available for generation 2 guests starting with version 8.

***Device Guard* is a group of key features designed to harden a computer system against malicious code.** Its focus is to prevent malicious code from executing by ensuring that only known good code can be executed..

***Credential Guard* is a specific feature, that is not part of *Device Guard*, which aims to isolate and harden key and user systems against compromise,** helping to minimise the impact and extent of "Pass the Hash" attacks in case malicious code is already executing via a local or network-based vector.

The first technology that needs to be understood before we can delve into these two features is Virtual Secure Mode (VSM). VSM is a feature that takes advantage of CPU virtualisation extensions to provide greater security for data in memory.

Further information on these features can be found at the following Technet link:

https://blogs.technet.microsoft.com/ash/2016/03/02/windows-10-device-guard-and-credential-guard-demystified/

VSM is a feature that takes advantage of CPU virtualisation extensions to provide greater security for data in memory

6.8 Control points

A critical point of any virtualisation environment is the creation and management of checkpoints or *guest* state. These cannot be thought of as backup of the machine; it is better to think of the checkpoint as a consistent state of a virtual machine at a specific point in time.

A *checkpoint* is a differential virtual hard disk, which has a special name and extension ". avhd [x]" and an xml configuration file with GUID name. In addition, there may be two additional files with virtual machine (VM) memory (.bin) and device status (.vsv) if the virtual machine was powered on during the checkpoint creation. Once the checkpoint is taken, the differencing disk (. avhd [x]) becomes a place where temporary changes to the original virtual machine disk are stored, while the original disk remains in read-only mode. It is not possible to checkpoint a virtual machine that uses pass-through virtual disks (i.e. does not use VHD-VHDX files as virtual disks).

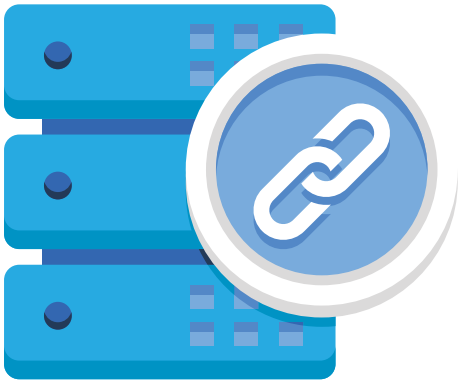
For this reason, it is necessary to control the generation of *checkpoints* of *guest* machines on a *host* due to the systems degradation they cause, both due to the creation of new files that not only the hypervisor must manage, but also due to the extra consumption of storage space they generate.

More information can be found at the following Microsoft link:

https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/user-guide/checkpoints

-

It is not possible to *checkpoint* a virtual machine that uses pass-through virtual disks



7. VMware Workstation / Player best practices

This section presents some of the most relevant information when it comes to establishing good practices in the process of creating and managing virtual machines with VMware Workstation.

The environment described in this document consists of the creation of virtual workstations, i.e. virtualisation on client computers through desktop applications such as Workstation Pro (which is purchased with a paid licence and allows the creation and management of virtual machines) and Workstation Player (free software that only allows the use of previously created virtual machines).

Within the products offered by VMware there are other versions of more professional virtual machine servers such as ESX and ESXi.

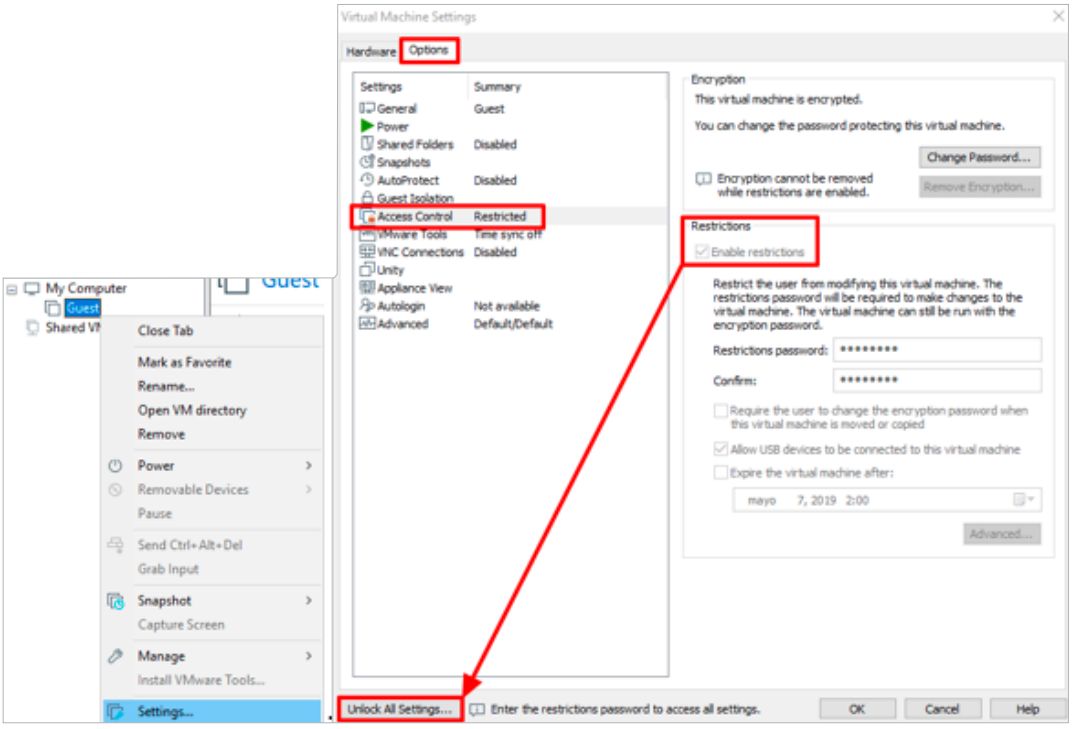
NOTE:

The examples shown below are taken from VMware WorkStation Pro v.15, licensed free of charge for 30 days.

7.1 Encryption and restriction of virtual machines

In a workspace with physical machines, whether in test phases or in production environments, there is a need to protect client machines to prevent unauthorised users from switching them on, taking them to other locations or removing components such as RAM memory, video or network cards, hard disks, etc. All these actions can lead to the malfunctioning of systems and, more compromising, to illegitimate theft of corporate information.

In virtual environments, after creating a virtual machine, the first recommended task is to protect access, as well as its basic configuration parameters, in order to prevent damage caused by inappropriate use. This can be done by means of the encryption and restriction options, which can only be configured when the virtual machine is switched off.



[Illustration 13] Encryption and Restriction Options.

Encryption makes it possible to secure access to the virtual machine, including the components assigned to it (RAM memory, external drives, hard disks, etc.). To do this, a password must be entered, which will be requested later each time it is started in the management console, when it is exported to another console or if the encryption process is to be reversed. The duration of the encryption process depends on the size of the virtual machine. Once completed, when the management console is restarted, the virtual machine will have a closed padlock icon and a dialogue box will appear asking the user to enter the corresponding password.

Restriction prevents users from accessing the configuration parameters of the virtual machine, unless they enter a specific password. If this section is not protected, users could perform actions such as allowing connections via VNC (a remote connection protocol that is not secure because it is not encrypted), sharing folders (with the corresponding risk of information loss) or modifying the working directory where virtual machines are stored.

Encryption and restriction options are closely related since if the former is not activated, the latter cannot be activated, and if the latter is activated, the former cannot be deactivated.

It is very important to store both encryption and restriction passwords conveniently in a secure registry, as VMware does not have a system for recovering lost keys.

This means that if passwords are lost, it will not be possible to start virtual machines, change their configuration or override encryption. Also, it must be clearly defined which users will have access to these keys, as they are enabled to operate corporate operating systems, which in some cases can be critical.

It is very important to store both encryption and restriction passwords conveniently in a secure registry

7.2 Resource configuration

Within the process of creating a virtual machine, it is recommended to make a correct prior planning of the hardware resources that are going to be allocated according to the physical characteristics available.

It is important to have a global view of the entire infrastructure, i.e. all virtual machines to be used on the same *host*, as well as the resources the *host* needs to continue to function properly, must be taken into account.

As a general rule, it is recommended to minimise the number of virtual machines you work with on the same *host* to avoid unnecessary use of resources. Likewise, once the working environment is well defined, only those virtual machines that are absolutely essential should be started. It is a waste of resources to keep running those virtual machines that you are not really working with, which is detrimental to the rest of the virtual machines and the *host* itself, as it could cause a slowdown in the execution of processes and even collapse the entire system.

Regarding disk space, a dynamic allocation is recommended, especially when working with multiple virtual machines, in order to minimise the amount of disk space occupied and to increase it only when needed.

For applications that are very sensitive to performance and disk writing, permanent space allocation is recommended, adjusted to the needs of the running software. There is also an option to split the disk archive into several 2 GB files, this is only recommended if the content of the virtual machine has to be stored on low capacity media or if it has to be transmitted over a network in a location where bandwidth is limited.

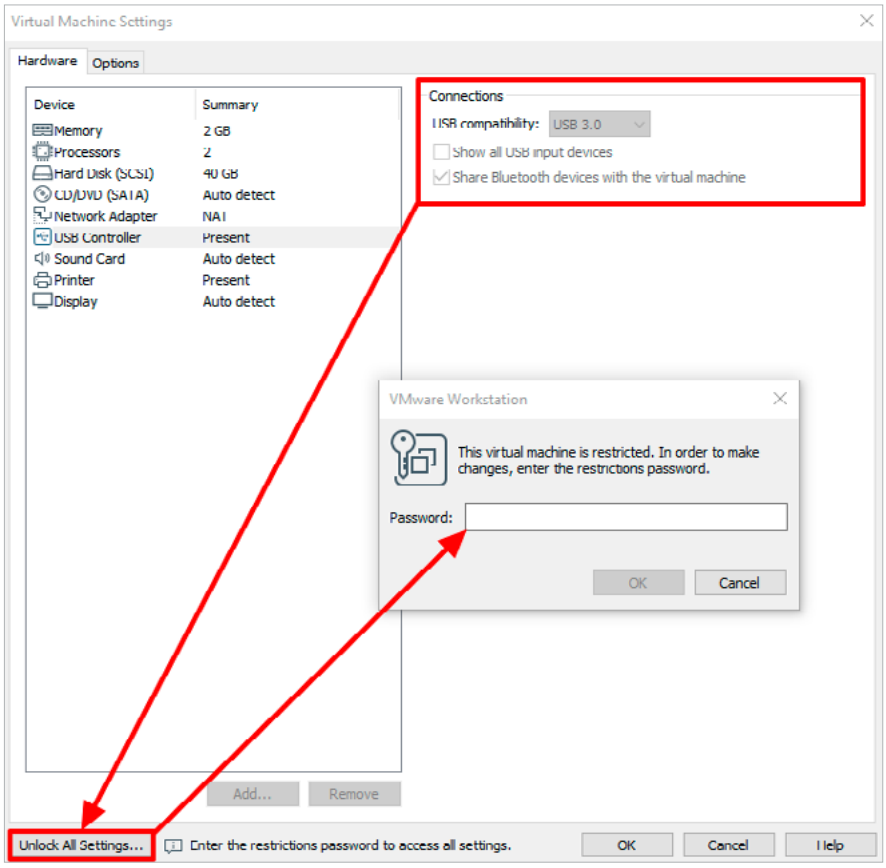
it is recommended to minimise the number of virtual machines you work with on the same *host* to avoid unnecessary use of resources

Whenever possible, a checksum tool (CheckSum) should be used to check the integrity of the files, and of course, encrypt the virtual disk.

On the other hand, **it is not advisable to leave open the possibility of connecting external media such as DVD or USB.** For this purpose, it is possible to restrict configuration options, as discussed in the previous section. If you allow a user to use an "iso" file as a boot DVD in a Linux operating system, you give him the possibility to chroot, which could give him access to and control of the virtual machine.

Similarly, allowing the use of USBs can lead to the unauthorised theft of information or the installation of malicious code, either voluntarily or accidentally. The best option, therefore, is to disable the use of external media through restrictions and enable them only when required, disabling them again after use.

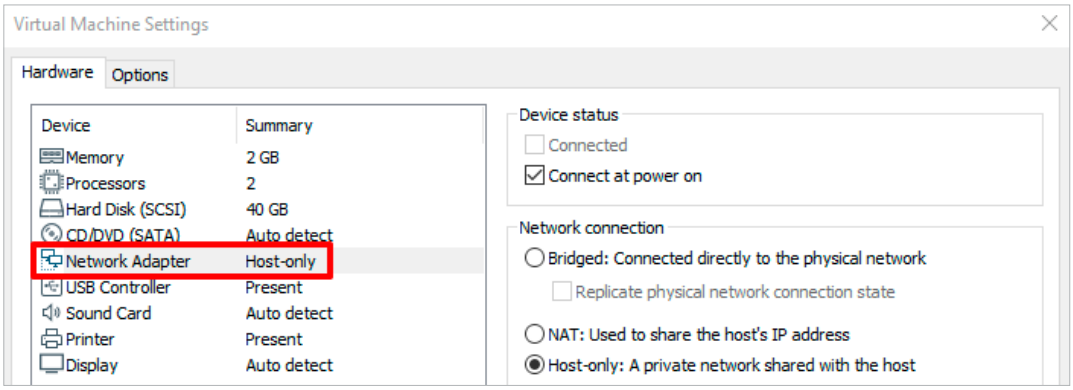
Allowing the use of USBs can lead to the unauthorised theft of information or the installation of malicious code, either voluntarily or accidentally



[Illustration 14] Password-protected hardware resources.

7.3 Network isolation and configuration

Virtual machines loaded on Workstation Pro and Player versions should be isolated from the rest of the network and work, as far as possible, only in "Host-Only" mode so as not to affect or be affected by the production infrastructure.



[Illustration 15] Red en modo "Host-only".

However, there are situations where virtual machines must have a presence on the network, either to interact with other machines or to download installation packages from the Internet. If this interaction is not absolutely necessary or constant, it is advisable to configure the main network device to act in "Host-Only" mode and add a second network device with presence on the external network which will be activated only when required, so it is recommended to keep it deactivated when not in use.

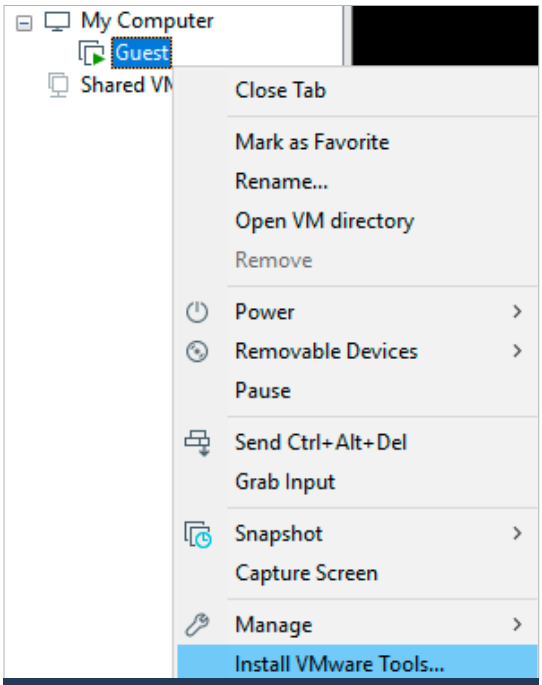
As far as the external connection is concerned, **the "NAT" mode is preferable as it allows more control over the network traffic,** as the virtual machines operate on an internal network created by the *host*. The "Bridge" mode configuration is easier to implement, but apart from less control, it may overload the network controller if there are a large number of virtual machines using the same physical interface simultaneously.

7.4 VMware tools

The installation of VMware tools is not essential for the operation of virtual machines. However, it is very necessary if you want to opt for certain interaction features between the *host* and the machine, such as file and text transfer.

Before installing the aforementioned tools, the operating system of the virtual machine to be used must be taken into account. Almost all Windows systems do not offer any problems when it comes to performing this action, but not all Linux distributions support it. With the latest versions of Debian and Ubuntu there are usually no difficulties.

When installing the VMware Tools, it should be borne in mind that they will need to be updated periodically to optimise their operation.



[Illustration 16] Installation of VMware Tools.

NOTE:

This document uses the current version of VMware WorkStation Pro v.15, with 30 days free licensing and you can consult the VMware Compatibility Guide at the following link: https://kb.vmware.com/s/article/2129859

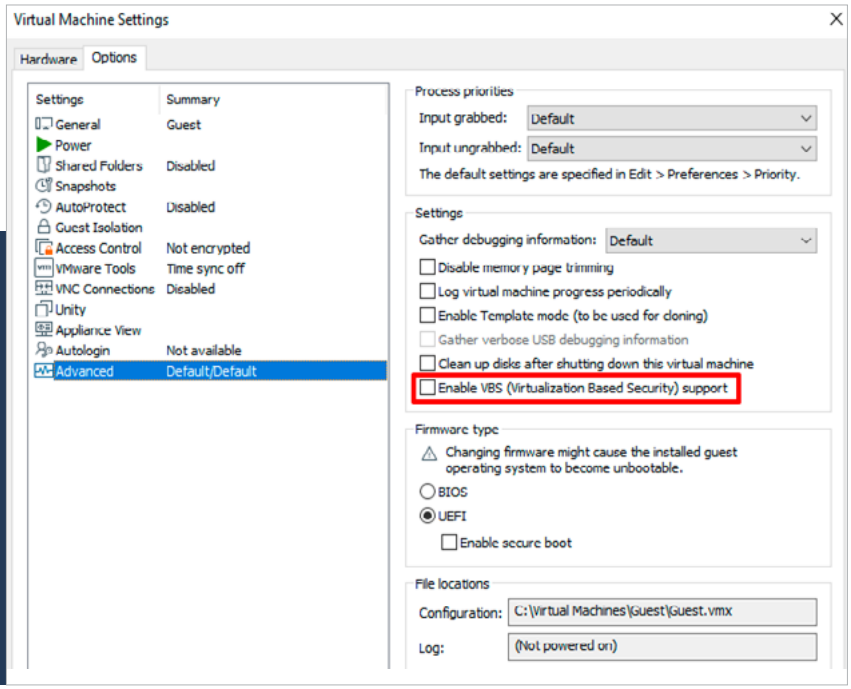
7.5 Protection of virtual machines on hosts

To increase security in virtual environments, virtualisation-based security (VBS) can be enabled for virtual machines running the latest Microsoft's operating systems Windows 10 and Microsoft Windows Server 2016.

Virtualisation-based security (VBS) uses Microsoft Hyper-V virtualisation technology to isolate the core services of Windows operating system in a segregated, virtualised environment. This isolation provides an additional level of protection by making it impossible for key services in your environment to be manipulated.

Enabling VBS in a virtual machine automatically enables the virtual hardware that Windows requires for VBS feature. When you enable VBS, a Hyper-V variant starts in the virtual machine and Windows starts running inside the Hyper-V root partition.

In VMware Workstation, VBS can be enabled during the creation of a virtual machine. Alternatively, VBS can be enabled or disabled for an existing virtual machine.



[Illustration 17] Option to enable VBS.

NOTE:

More information can be found at the following link: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.html.hostclient.doc/GUID-E2A6D2F4-BA66-48EC-98D5-35D8E2C3B192.html

7.6 File and text transfer

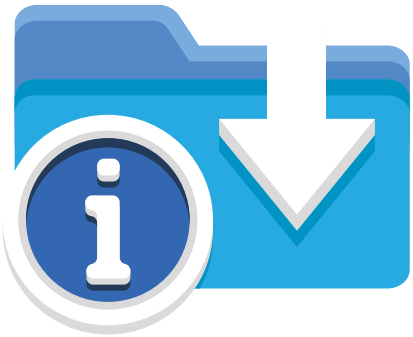
Once the VMware tools have been installed, the clipboard can be used jointly between the *host* and the virtual machines, and certain types of files can be transferred easily. For the latter, there are several methods, so you will have to choose one or more depending on the needs of each system.

The first one to mention is "drag and drop", i.e. dragging files from the *host* computer to the virtual machine or vice versa. It is easy to use, but can be problematic because of the size and format limitations of some files.

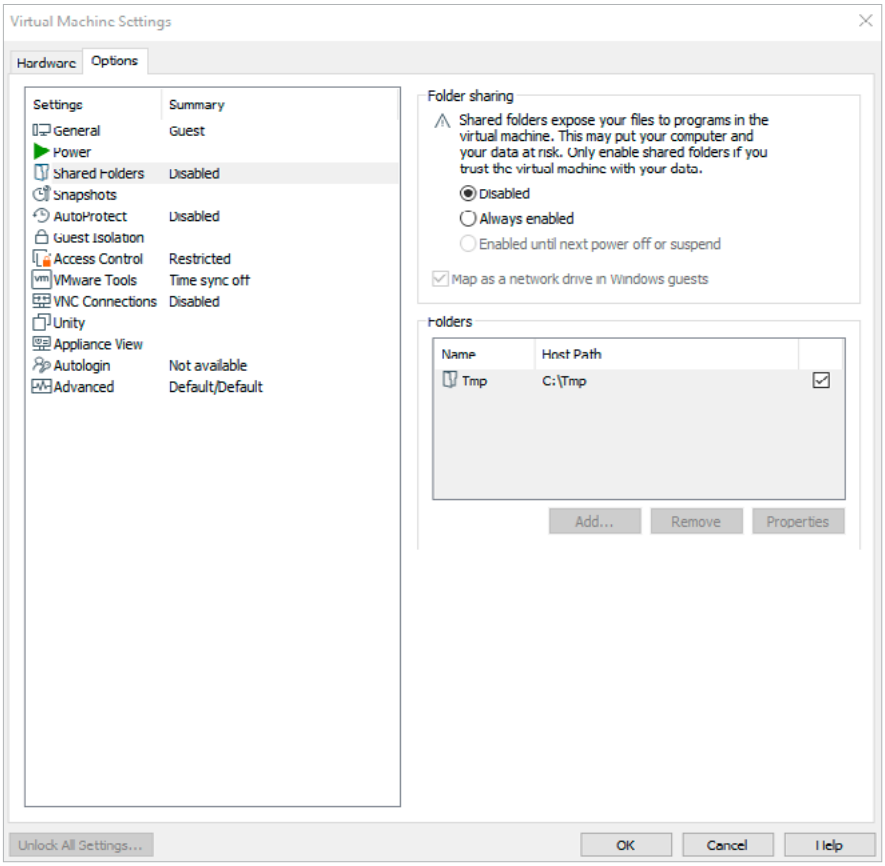
You can also opt to use the "copy and paste" feature. Apart from the limitation of the file format and size, as in the previous case, it has the disadvantage that it does not work between virtual machines.

Thirdly, there is the option to share folders. This solution is more complex to configure than the previous ones, but allows for easy deactivation when not in use. A major drawback is the possibility of files becoming corrupted if they are used by different machines simultaneously.

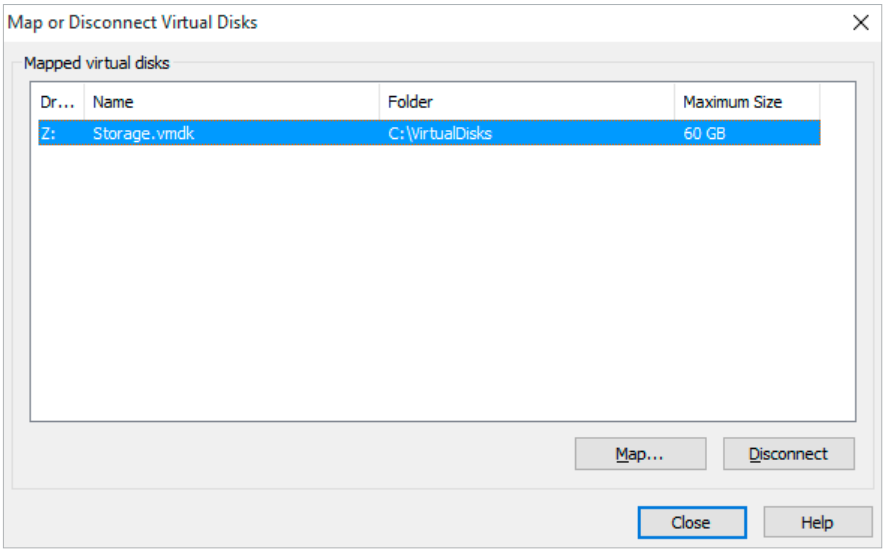
Finally, there is the option for the *host* to map a virtual hard disk on which to store the files. This has the advantage of allowing the use of a rendezvous point between several virtual machines and the *host* without leaving the virtualisation infrastructure. If this method is chosen, it is recommended to encrypt the virtual hard disk.



[Illustration 18] Sharing a *host* folder with one of the *guests*.



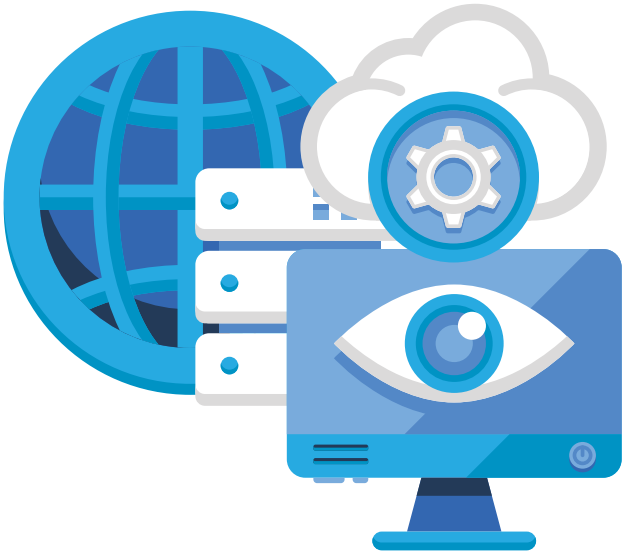
[Illustration 19] Virtual hard disk file mapped on the *host*.



Whenever possible, work should be done locally. But when it is necessary to share files with external users or computers, it is highly recommended to use a system that provides a robust validation method, such as those based on Directory Services (e.g. Windows Active Directory).

7.7 Snapshots of the virtual machines

As in all other virtualisation systems, checkpoints or status of virtual machines can be made. This option should not be used as a backup system for virtual machines, as VMware treats them as a registry where it stores the changes to the primary virtual hard disk, creating a new placeholder disk from the moment it is created.



NOTE:

Further information can be found at the following link from the vendor:

Best practices for using snapshots in the vSphere environment.

8. VirtualBox best practices

As with the other hypervisors, protection actions and, in general, best practices should be oriented first to the *host* and then to each of the hosted virtual machines.

Some of the general considerations to be taken into account are listed below:

a. **Keep the virtualisation software up to date.** This can be done by enabling the option in the VirtualBox preferences or by doing a manual check under "File" and then "Check for updates...".

b. **Keep "Guest Additions" updated on all virtual machines.** Similarly, the Extension Packs must be updated.

c. **VirtualBox should not be run with administrator privileges,** except for required actions that cannot be performed without privileges and, in general, the most restrictive permissions should be maintained.

d. **Restrict network connections so that *host* and guests have the minimum connectivity required.** Likewise, this connection must be secured with a firewall system on each of the installed computers.

e. **Audit security logs on a regular basis to detect anomalous behaviour and create a baseline for comparison if necessary.**

f. **Use only the official Oracle website as the source of installables.**

g. **In sandbox-antimalware environments, avoid installing "Guest Additions",** as they allow communication with the *host* and become a possible vector of infection.

Protection actions and, in general, best practices should be oriented first to the *host* and then to each of the hosted virtual machines

h. **Do not create *snapshots* that are not needed and delete them securely if necessary.**

i. **Use extreme caution when using USB storage devices, CDs or DVDs as they allow direct entry of software into virtual machines.** Especially the former are a common input vector for malicious code.

j. **Avoid the hypervisor manager in HTML mode because it does not use a secure connection.** It is preferable to use the client-server application "Oracle VM VirtualBox Administrator" (desktop application), which is more secure.

NOTE:

Official VirtualBox website for downloading their products:

- **https://www.oracle.com/virtualization/virtualbox/**

- **https://www.virtualbox.org/**

8.1 Encryption of virtual machines

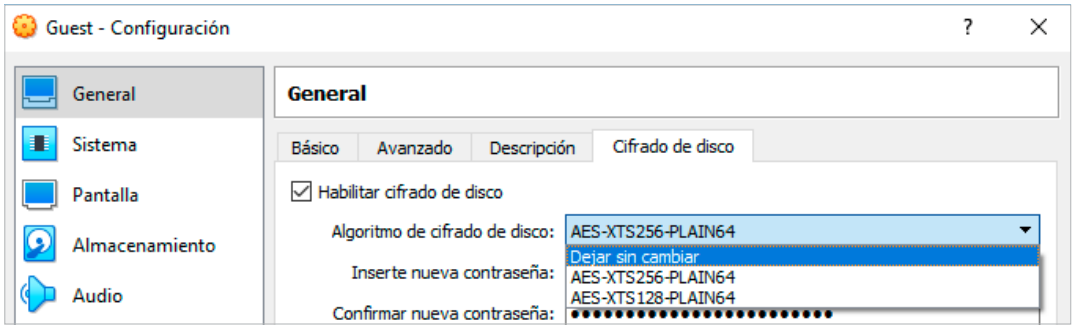
As far as the encryption of virtual machines is concerned, it is transparent to the *guest* and can be applied to the hard disk and to any of its available formats (VDI, VHD, VMDK).

VirtualBox, from version 5 onwards, already included the encryption of virtual machine hard disks as a security feature, however, it is necessary to install an extension package to be able to use the feature in the general configuration of virtual machines.

During the creation of the machine with the graphical wizard, encryption cannot be configured, so if the machine is critical, it is advisable not to add the disk until password-encryption is activated. Also, it should be noted that encryption adds workload to the host and that the machines created with this method in VirtualBox cannot be transported to other virtualisation systems without first decrypting them.

NOTE:

You can choose the most secure algorithm depending on the importance and/or criticality of the system



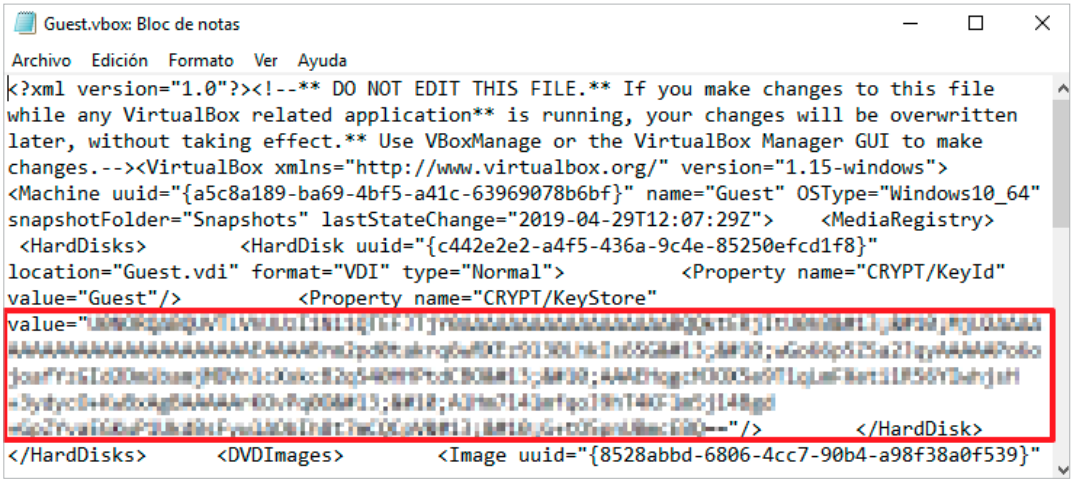
[Illustration 20] Activation of encryption in virtual machine.

It is essential to point out that the loss of the password implies the irremediable loss of the hard disks. The password is stored in the configuration file of the virtual machine, so it is advisable to have a backup of the same.

The machine definition file, which includes the encoding of the plaintext encryption password, has to be protected by NTFS permissions, and must be done before creating the password to avoid leaks in the exposure time window.

Windows EFS encryption protection is not an alternative, as the encryption is reverted at the first boot of the *guest* in VirtualBox.

It is essential to point out that the loss of the password implies the irremediable loss of the hard disks



[Illustration 21] Virtual machine configuration file.

On the other hand, **the assignment of permissions to the folder where the definition of virtual machines and hard disks is stored must be properly planned in order to avoid unauthorised access** (by accident or as a result of an attack). At least the following permissions must be configured:

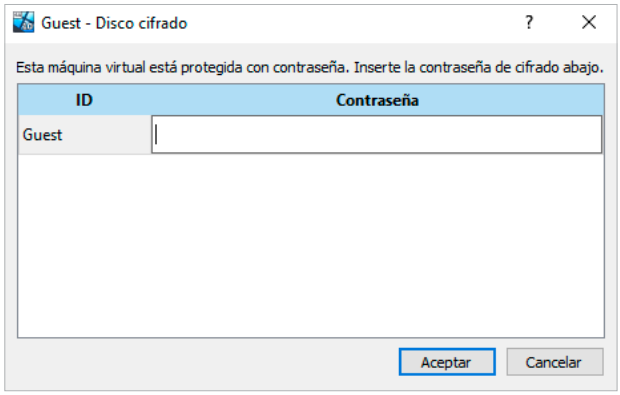
[Table 5] Minimum permissions for virtual machine directories and hard disks.

CUENTA	PERMISOS	APLICAR A
Administradores	Control total	Esta carpeta, subcarpetas y archivos
System (Sistema)	Control total	Esta carpeta, subcarpetas y archivos
Creator owner (Propietario creador)	Control total	Solo subcarpetas y archivos

NOTE: The inclusion of other users or groups should be assessed on a case-by-case basis

With the permissions in the table above, each user can generate their own virtual machines, but cannot access *guest* machines created by others. Any *host* administrator can access all machines.

When starting a virtual machine that has a password-protected disk, the password is required at every start of the virtual machine. **There are some limitations when using disk encryption, so it is advisable to consult the manual before using this functionality.** For example, it is incompatible with *snapshots*, or the password is loaded in memory and transferred flat during the use of the virtual machine.



[Illustration 22] Encryption key request window.

VirtualBox encryption is compatible with physical disk encryption via *BitLocker*, so for critical environments both should be used, and additional measures for password protection should be put in place.

8.2 Network isolation and configuration

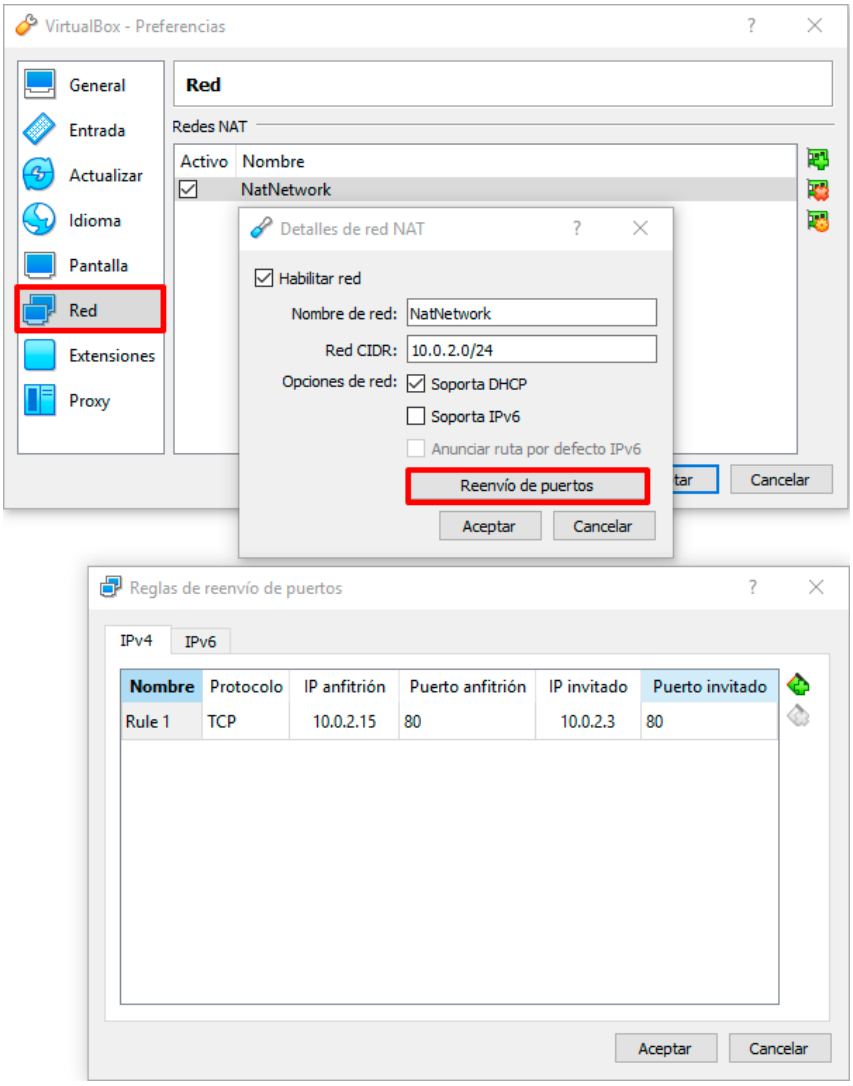
With respect to connectivity in VirtualBox, *guest* virtual network devices can be configured in one of the following states:

- **Not connected.**
- **NAT.**
- **NAT network.**
- **Bridge adapter.**
- **Internal network.**
- **Host-only adapter.**
- **Generic driver.**
- **Advanced.**

The default value assigned to a new creation is "NAT", so the hypervisor behaves like a router (layer 3 device of the OSI model). This gives the *guest* connection capabilities to the host's physical network, but hides the IP and MAC addresses from external computers.

The *host* firewall can provide protection for hosted virtual machines. This prevents the publication of services from hosted servers as a *guest*, except for the one for which this option has been selected. This can be seen as a security advantage, but also as an impediment if multiple *guest* connectivity from the network is required.

When server publishing is required, one can make VirtualBox work as a router with all possible router functionalities. To do this, a "NAT network" must be created, to which virtual *guest* adapters can then be connected.



[Illustration 23] Creation of a "NAT Network" with the publication of port 80.

The "Bridge adapter" option allows direct connection of guests via the physical connection, which behaves like a switch (layer 2 of the OSI model). This is a convenient configuration to achieve external connectivity, but it considerably increases the exposed surface, so each virtual machine must be protected by its own means (products to avoid malicious code, firewall, IDS, etc.).

"Internal network" allows virtual machines to connect to each other to hosted machines that have this option selected and that also match the same network identifier. It is therefore possible to create different internal networks. If you need to test machines as if they were in a network, this is a valid option, but you must create your own internal network and only connect the essential machines.

If the network visibility needed is with the *host*, the **"Host-only adapter"** option should be selected, which will link both *host* and *guest* computers.

"Generic driver" is not commonly used. Allows to present a network driver included in VirtualBox or in an **"Extension Pack"**.

When **"Advanced"** is enabled, each of the options enables MAC address management, promiscuous mode activation, adapter type and port forwarding (each as applicable).

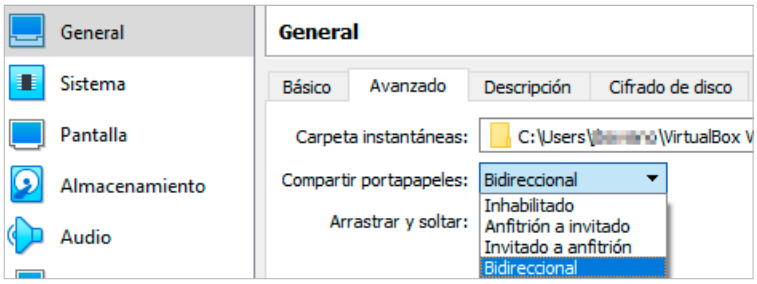
As with any other hypervisor, **it is recommended to use the "Not Connected" configuration whenever possible and to scale from lower connectivity to higher connectivity.** For example, move from **"Adapter only-host"**, to internal network, then to NAT, then to NAT network, etc.

In VirtualBox, up to four virtual network cards can be created per *guest* and the same precautions must be taken for all of them. It is important to take into account that cards that will not be used should not be defined.

8.3 Clipboard sharing

The shared clipboard tool presents an interesting functionality for fast and convenient work, but it could be a point of harmful code exchange. It works independently of the type of network used and can work in both directions or in one of them, between the *guest* and the *host* or vice versa. This tool requires the *guest* to have VirtualBox's "Guest Additions" installed.

The shared clipboard tool presents an interesting functionality but it could be a point of harmful code exchange



[Illustration 24] Clipboard configuration.

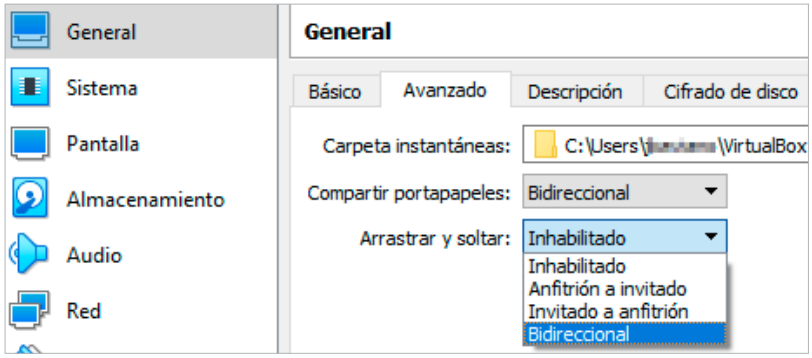
As a rule, this functionality should remain disabled, as a potential attacker could, for example, gain access to sensitive information stored in the host's clipboard by previously gaining access to an inadequately protected *guest*. If required for reasons of force majeure, it should be temporarily enabled only for the indispensable period.

NOTE:
In the virtual machine configuration in VirtualBox, you can select the clipboard operation mode (by default it is disabled).

8.4 Drag and drop

This functionality, known as "drag & drop", allows you to drag and drop an object (file, folder or plain text) in both directions, between the *guest* and the *host* or vice versa. This tool requires the *guest* to have VirtualBox's "Guest Additions" installed.

The choice of settings is the same as for the shared clipboard, as well as the default option, "Disabled", and the recommendation to keep it in that state. If its use is required, it should be activated as long as strictly necessary.



[Illustration 25] "Drag and drop" configuration.

NOTE:

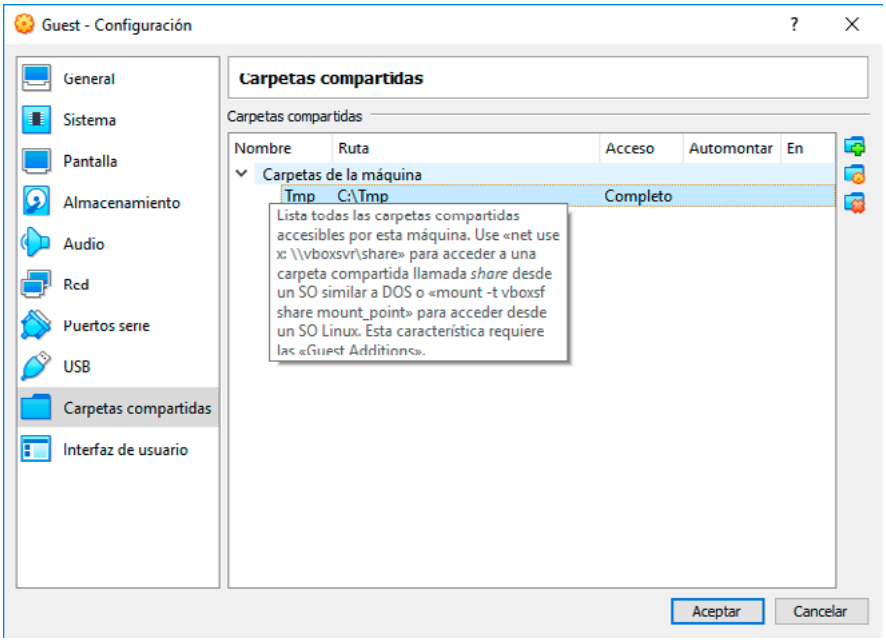
In the virtual machine configuration in VirtualBox, you can select "Drag and Drop" operation mode (disabled by default).

8.5 Shared folders

In this case the term "shared folder" does not refer to the network resource created by the operating system, but to the VirtualBox feature that is made available with the installation of "Guest Additions" on the *guest*. This allows a directory hosted on the *host* to be made available to the *guest*, which can be accessed via the Universal Naming Convention (UNC) paths used to access network resources.

For a description of UNC see the following link:

https://docs.microsoft.com/eses/dotnet/standard/io/file-path-formats#unc-paths



[Illustration 26] Configuration of shared folders.

By default, VirtualBox does not include any shared folders. The decision to create them must be considered, adopting the maximum security measures to protect the information handled.

Once a shared folder is defined, it behaves as a network resource. It is published with the name given during the creation and with the nomenclature "vboxsvr" for the server. If you choose to execute the "Automounting" instruction in Windows, the folder will be mounted immediately. It will be mounted in the same way in Linux in "/media" with the prefix "sf_".

Its use is discouraged as it increases the area of exposure (e.g. most ransomware would encrypt the Windows letter drive). To learn more about protection against ransomware, please consult *CCN-CERT* Threat Report *IA-11/18: Security measures against ransomware* and the Good Practice Guide CCN-CERT BP/04Ransomware on CCN-CERT's website.

In the latest versions of VirtualBox it is possible to define the mount point, thus ensuring that the mount point is different from the standard mount point and to apply additional security measures on the mount point.

In the latest versions of VirtualBox it is possible to define the mount point, thus ensuring that the mount point is different from the standard mount point

As noted in previous sections of this guide, **sharing information,** by whatever means, **is always considered an increase in the surface area exposed to potential attacks,** but is sometimes necessary.

Therefore, appropriate measures must be taken, **as an attacker accessing the *guest* would have access to the shared resources.** Among other actions, you can limit the sharing time (when the virtual machine is turned off, the shared resource disappears), minimise the information published, combine the permissions available in VirtualBox with the NTFS permissions of the *host*, making them as restrictive as possible, and, in critical environments, activate file auditing. Also, although it does not prevent information leakage, it is possible to set the permission to read-only (the default value is read-write).

8.6 Snapshots in VirtualBox

Virtual machines in VirtualBox are composed of a series of files in which information about hard disks, features and the current state of the machine is stored.

Each virtual hard disk corresponds to a file with the extension ".vdi", ".vhd" or ".vdmk" (depending on the type of disk selected when creating the virtual machine). The configuration parameters are stored in an XML file with the name of the machine in question. In versions of VirtualBox later than 4.0 this file has the extension ".vbox", which allows you to start the machine by double-clicking on it or via a shortcut. If instead of shutting it down, it is decided to save the state of a machine, there will also be a ".sav" file, which will be deleted as soon as the machine is active again.

Snapshots are a way of saving the state of the virtual machine at a given moment, and any change made to it will be stored in a new ".vdi" file for each existing hard disk, keeping the originals intact. Successive *snapshots* will repeat this process, which can considerably increase the space occupied by the machine on the *host* disk, so it is necessary to control their creation and manage both the number of *snapshots* and their maintenance over time.

***Snapshots* are a way of saving the state of the virtual machine at a given moment**

9. Safe navigation machine

In order to complement the purpose of this guide, a securely configured virtual machine has been implemented, which is oriented towards web browsing. In this way, independence and isolation between the virtual machine and the *host* computer is guaranteed.

The operating system used for the virtual machine is CentOS 7, which is licensed free of charge and the secure configuration guide applied is "CCN-STIC 619 Secure Configuration of CentOS 7 (Stand-alone Client)".

The data required to download the secure browsing virtual machine are listed below:

Link:
https://loreto.ccn-cert.cni.es/index.php/s/FpniMgp5Hx8Ml66

Download key: virtual

SHA256
49C16F00E00C91EEE30D634A1BFB4035E69C2ED4017D0DF8B5BFD7B635E61892

SHA1
209766E9771E375322F6A4EE3742A46C2DED5D0C

The secure browsing virtual machine is designed to be used with virtualisation software products (hypervisors) that are licensed free of charge, for example:

Oracle VirtualBox: www.virtualbox.org/wiki/Downloads

VMware Workstation Player:
www.vmware.com/products/workstation-player.html

10. Decalogue of recommendations

The following is a decalogue of generic best practices for all types of hypervisors.

Security Decalogue for virtual machines

1. **Keep the system up to date:** having the latest security updates installed on the operating system and using the latest version of the virtualisation software available drastically reduces exposure to attack vectors addressed by vendors through update patches.

2. **Physical network segregation:** if possible, have at least one dedicated network adapter for the virtualisation infrastructure to keep separate the network flow of the virtual machines and the physical machine containing them. In the event of an attack on the physical machine's network, the attacker will not see the network flow of the virtual machines, keeping them secure because of this separation of adapters.

3. **Segregation of roles and permissions:** it is advisable to create a specific security group for the use of virtual machines, restricting the use of the virtualisation program by member users which will not be allowed to perform actions that require privilege escalation not related to the use of virtual machines. In the same way, it is recommended to create a directory to *host* the virtual machine files, where permissions will be applied later, by means of ACLs.

4. **Plan the virtualised system:** making a preliminary outline of the virtualisation infrastructure will help implementing it. This planning should take into account sizing the creation of virtual machines to the real needs and the hardware resources available on the *host*, paying special attention to the type of disks to be selected according to the services provided by each virtual machine.

5. **Resource management:** Hypervisor resources are not unlimited. To free up these resources, it is advisable to keep active only the virtual machines that are absolutely necessary. Moreover, implementing a policy of creating "snapshots/checkpoints" of virtual machines also reinforces this management, as they imply a degradation of the hosts. This creation must be controlled, both in terms of the total number created and the time to keep them on the hypervisors.

6. **Information protection:** to keep secure the critical data hosted on virtualised media, it is advisable to encrypt virtual machine files, *snapshots* and virtual hard disks aimed at the storage of the virtualisation platform. As well as encrypting external storage media containing backup virtualisation files and guarding them appropriately. Similarly, encrypt and keep password books properly guarded to prevent possible exfiltration.

7. **Firewall implementation:** securing with a firewall solution, either physical or logical, to prevent malicious code and attack attempts against all *guest* operating systems.

8. **Implement a backup policy:** to avoid losing data or the functionality of the virtual machines in case of emergency, it is recommended to establish a backup policy that imcludes a complete copy of these virtual machines. These backups should be made from time to time or at critical moments in order to be able to recover information or even the functionality of the virtual machine. It should be taken into account that backups have a large size and because of this, it would be advisable to keep few complete backups and make use of incremental copies.

9. **Document the virtualisation platform:** keeping the system documented helps to quickly identify machines in disuse and makes it possible to free up resources and obtain better management of the system. It is advisable to update this documentation with every relevant change made to the system.

10. **Install the hypervisor agents:** consider installing these software add-ons such as "Guest Additions" or "Tools", as their implementation improves the performance of the virtual machines and adds functionalities such as the shared clipboard. If so, it is recommended to keep them and the virtualisation software up to date.

11. Glossary

This section contains a description of the terms most commonly used in this document for their identification and understanding during the course of the document.

TERM	DESCRIPTION
Virtualisation	It is the abstraction of the resources of a physical server, so that a layer is created between the hardware of the physical machine (*host* or hypervisor) and the operating system of the virtual machine (*guest*).
Guest	Software that simulates a computer and can run programs as if it were a real, physical computer.
Virtual Machine (VM)	Also referred to as the "*Guest*".
Hypervisor o *Host*	It is the physical platform that allows the application of various virtualisation control techniques to use, at the same time, different operating systems on the same computer.
Snapshot or *Checkpoint*	It represents the state of a virtual machine at the time it is taken. Basically, it is a snapshot of the virtual machine at a given time. This should not be taken as a backup of the virtual machine.
Switch	It is a device for interconnecting networks between other devices or equipment.
Virtual Local Area Network (VLAN)	It is a method of creating networks that are logically independent, even if they are within the same physical network.

CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


cn-cert
centro criptológico nacional
CCN
centro criptológico nacional