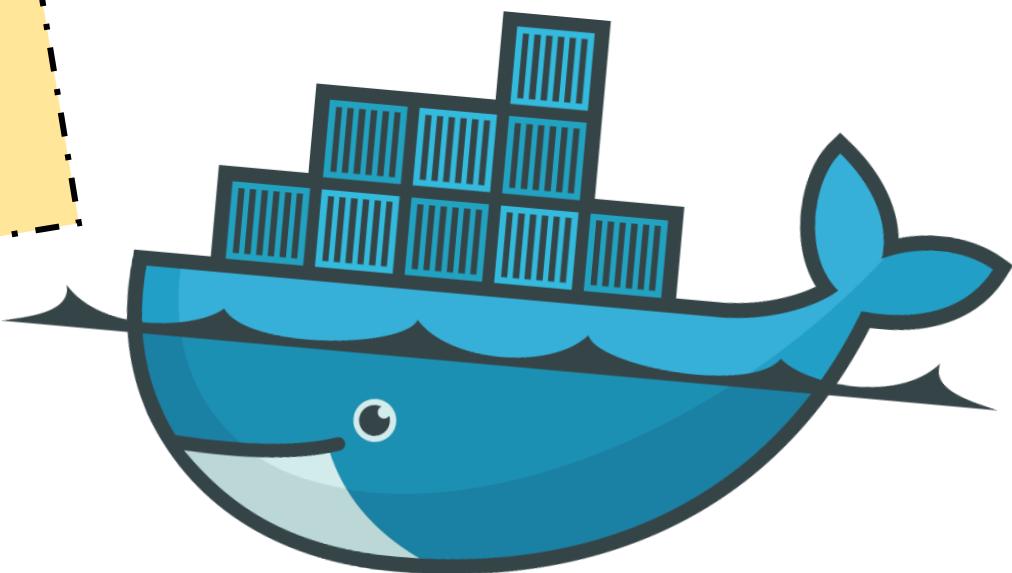


- Docker
- ESXI/Proxmox
- PfSense
- Zabbix



Docker

Docker es una plataforma que permite crear, testear e implementar aplicaciones rápidamente, mediante unidades estandarizadas llamadas **contenedores**.

Estos contenedores incluyen todo lo necesario para que el software se ejecute, por lo que pueden **implementarse aplicaciones o desplegarse servicios en cualquier entorno, con la seguridad de que funcionarán correctamente**.

Docker utiliza el núcleo Linux y es capaz de compartir recursos con el núcleo del host donde se instala. Esto lo hace, en muchos casos, **más eficiente que una MV convencional** (la misma utiliza su propio núcleo y S.O independiente del host).

Para instalar el Docker Engine se pueden seguir las instrucciones desde la web oficial. Aquí aparecen [los requisitos para la implementación del motor en varias distribuciones Linux](#).

* **También es posible utilizarlo en Windows mediante Docker Desktop (son necesarias las features WSL y Hyper-V).**

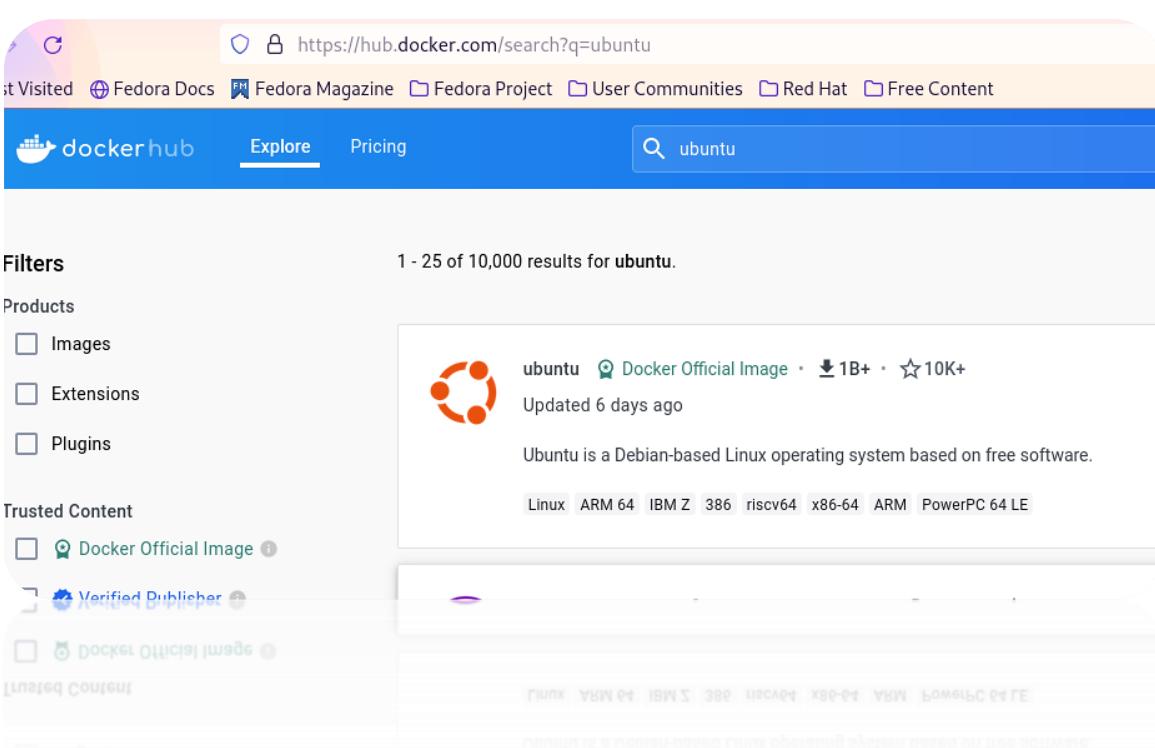
Una vez iniciado el servicio es posible comenzar a interactuar con el motor utilizando los **comandos propios de Docker**.

Es necesario contar con permisos de superusuario, o en su defecto, agregar a un usuario al grupo "docker".

Para iniciar un contenedor es necesario contar previamente con una imagen (plantilla).

Pueden descargarse desde el repositorio oficial (**Docker Hub**), crearse desde cero o es posible personalizar una imagen existente mediante un **Dockerfile**.

Existen imágenes oficiales de varios S.O, aplicaciones y servicios más utilizados, que pueden tomarse como base para la creación de nuestros contenedores.



Las imágenes utilizan **tags** para indicar diferentes versiones o variantes y pueden descargarse desde el terminal con el comando:

docker pull [imagen:tag]

Se pueden ver las imágenes descargadas con el comando

docker images y eliminarlas con ***docker rmi [imagen:tag]***

Por defecto suele aparecer hello-world como imagen predeterminada.

Con ***docker run hello-world*** podremos comprobar que el motor de Docker está funcionando y ver una descripción de su funcionamiento

The screenshot shows a terminal window with three visible command-line sessions:

- Session 1:** The user runs `docker pull ubuntu:24.04`. The output shows the image is being pulled from the library/ubuntu repository, with the digest and status of the download.
- Session 2:** The user runs `docker images`. The output lists the available images, including `ubuntu:24.04` and `hello-world:latest`.
- Session 3:** The user runs `docker run hello-world`. The output is a welcome message from Docker, detailing the steps it took to run the container, including pulling the image and creating a new container.

The terminal window has a dark background with light-colored text. The bottom right corner contains promotional text about Docker Hub and its features.

Iniciar un contenedor

Con **docker run [imagen:tag]** se puede iniciar un contenedor a partir de una imagen.

El lanzamiento del contenedor puede personalizarse mediante el uso de varios parámetros.



How to use this image

Start a mysql server instance

Starting a MySQL instance is simple:

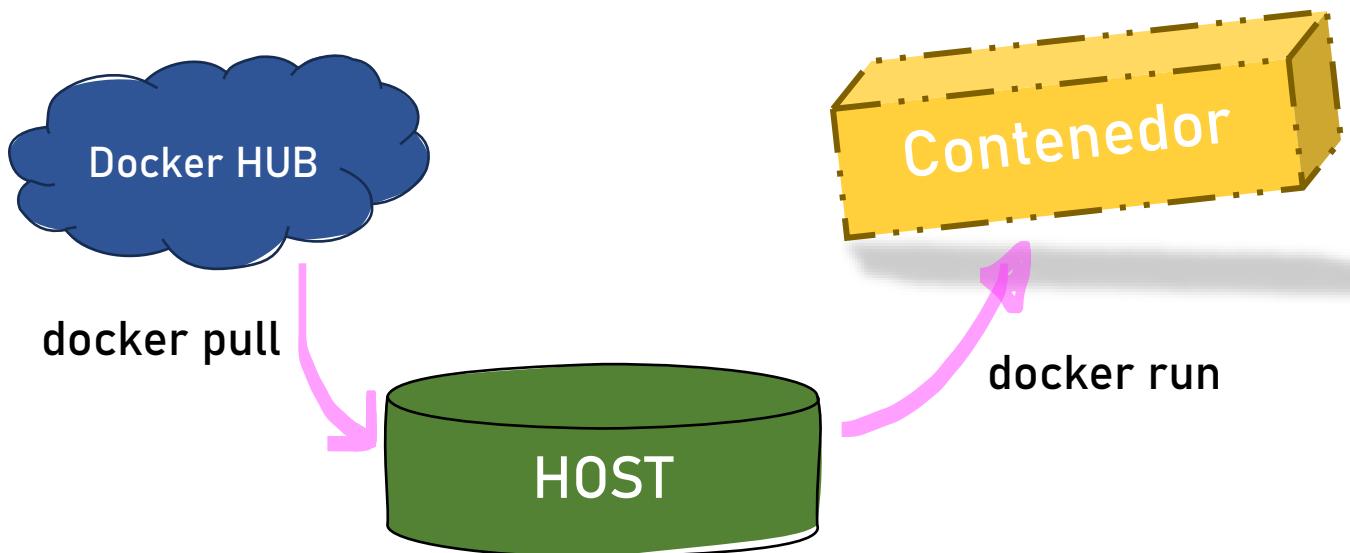
```
$ docker run --name some-mysql -e MYSQL_ROOT_PASSWORD=my-secret-pw -d mysql:tag
```

... where `some-mysql` is the name you want to assign to your container, `my-secret-pw` is the password to be set for the MySQL root user and `tag` is the tag specifying the MySQL version you want. See the list above for relevant tags.

Muchas imágenes utilizan parámetros especiales a la hora de iniciar el contenedor. Toda la documentación y las particularidades de cada servicio/aplicación suelen encontrarse en **Docker Hub**

* Si se inicia un contenedor con una imagen que no fue descargada, se descargará automáticamente desde el Hub.

** Si se inicia un contenedor sin nombre, Docker generará un nombre aleatorio (además del ID).



Gestión de contenedores

Se pueden **visualizar los contenedores** en ejecución e incluso los detenidos con el modificador **-a**.

Para *detener un contenedor* en ejecución se puede utilizar:

Docker stop nombreCT

Docker system prune

Elimina los contenedores que no están en uso, redes, imágenes sin referenciar y opcionalmente volúmenes.



Ejemplo contenedor apache+php

```
[santiago @ fedora in ~]
└─> docker run --name miserverweb -d -p 6480:80 php:apache
1a63c9978ee96444db2c417960ebe933c8489ad3a9f868c240743d31f36b4091

[santiago @ fedora in ~]
└─> docker ps
CONTAINER ID        IMAGE               COMMAND
1a63c9978ee9        php:apache         "docker-php-entrypoi...
                           ...
CREATED              STATUS
7 seconds ago        Up 6 seconds
```

Se inicia un **contenedor** en **segundo plano**, con el nombre **miserverweb**, utilizando la **imagen** **php:apache** y redireccionando el puerto **6480** del equipo físico al **80** del contenedor.

Se utiliza **docker cp** para copiar un archivo desde el equipo físico a una ruta dentro del contenedor.

[Most Visited](#) [Fedora Docs](#) [Fedora Magazine](#) [Fedora Project](#) [User Communities](#) [Red Hat](#) [Free Content](#)

Web dentro del contenedor

```
[santiago @ fedora in ~]
└─> docker run --name miserverweb -d -p 6480:80 php:apache
781b5746901bdaebb0e9974ccdf5c4677818c822192eb01f395cccf74c41337c

[santiago @ fedora in ~]
└─> docker cp index.html miserverweb:/var/www/html/
Successfully copied 2.05kB to miserverweb:/var/www/html/
```

docker cp - docker exec

Se pueden copiar archivos entre el host físico y un contenedor en particular utilizando **docker cp** de la siguiente forma:

```
[ santiago @  fedora in  ~
↳ docker cp --help

Usage: docker cp [OPTIONS] CONTAINER:SRC_PATH DEST_PATH|-|
       docker cp [OPTIONS] SRC_PATH|-| CONTAINER:DEST_PATH

Copy files/folders between a container and the local filesystem
```

Es posible ejecutar comandos dentro de un contenedor que se encuentra en segundo plano, utilizando **docker exec**.

Creo un archivo dentro del contenedor

```
[ santiago @  fedora in  ~
↳ docker exec miserverweb touch /var/www/html/index.html
```

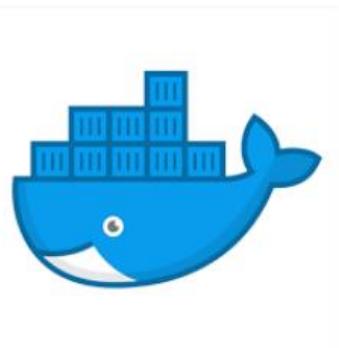
Ingreso al contenedor

```
[ santiago @  fedora in  ~
↳ docker exec -it miserverweb bash
root@1a63c9978ee9:/var/www/html# ls
index.html
root@1a63c9978ee9:/var/www/html#
```

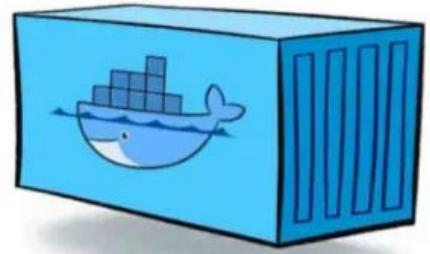
Dockerfile



Docker file



Docker Image



Docker Container

Se puede crear una **imagen personalizada**, mediante un Dockerfile.

De esta manera, Docker construirá la imagen leyendo las instrucciones en orden desde un archivo de texto.

Se pueden tomar como base las imágenes de Docker Hub y adaptarlas según nuestras necesidades mediante este archivo.

Un Dockerfile utiliza instrucciones particulares y un formato específico.

```
FROM php:8.1.19-apache-bullseye
RUN apt-get update && apt-get upgrade -y
RUN docker-php-ext-install mysqli
EXPOSE 80
```

Una vez creado el Dockerfile, se puede construir una nueva imagen con
docker build

Deberíamos indicar como parámetro el nombre de la imagen a crear (**-t**) y la ubicación del Dockerfile.

El punto “.” indica el directorio actual

```
[santiago @ fedora in Documents]
└ docker build -t imagen_custom .
[+] Building 60.9s (7/7) FINISHED
  => [internal] load .dockerignore
  => => transferring context: 2B
  => [internal] load build definition from Dockerfile
  => => transferring dockerfile: 215B
  => [internal] load metadata for docker.io/library/php
  => [1/3] FROM docker.io/library/php:8.1.19-apache-bu...
  => => resolve docker.io/library/php:8.1.19-apache-bu...
  => => sha256:662d8f2fcdb9ff5b9497538bdbb929df1cc5f1d...
  => => sha256:0bb33ced849a34e768aeceb2b09c9a6a0d2d3eb4...
  => => sha256:fd22bc8f8e13c635bff418a1d9416e6544bb6ce...
  => => sha256:f03b40093957615593f2ed142961afb6b54050...
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
imagen_custom	latest	4a341b492086	38 seconds ago	535MB
php	apache	f3d702d507c3	13 days ago	507MB
ubuntu	24.04	bfaf276bdd21	2 weeks ago	71.1MB
hello-world	latest	9c7a54a9a43c	7 months ago	13.3kB

Volúmenes

Cada contenedor es una nueva instancia de una imagen de Docker.

Esto implica que los datos que no formen parte de la imagen, o *cambios posteriores al inicio del contenedor no persisten cuando el mismo se detiene.*

Un **volumen** permite conservar los datos aunque se detenga/elimine el contenedor; además, facilitan el intercambio de información entre distintos contenedores.

```
santiago @ fedora in ~
└─ docker volume

Usage: docker volume COMMAND

Manage volumes

Commands:
  create      Create a volume
  inspect     Display detailed information on one or more volumes
  ls          List volumes
  prune       Remove unused local volumes
  rm          Remove one or more volumes

Run 'docker volume COMMAND --help' for more information on a command.
```

Una vez creado el volumen, *se puede asociar a una ruta dentro del contenedor, a la hora de iniciar lo.*

De esta manera, la información almacenada en dicha ruta pasa a formar parte del volumen y persistirá independientemente de lo que suceda con el contenedor.

```
santiago @ 192 in ~
└─ docker run -d --name serverweb -v volumenBD:/var/www/html -p 80:80 php:apache
159e35630fb339374ec4d53061ded30ea35917d20904632d603ccba25e389a5f
```

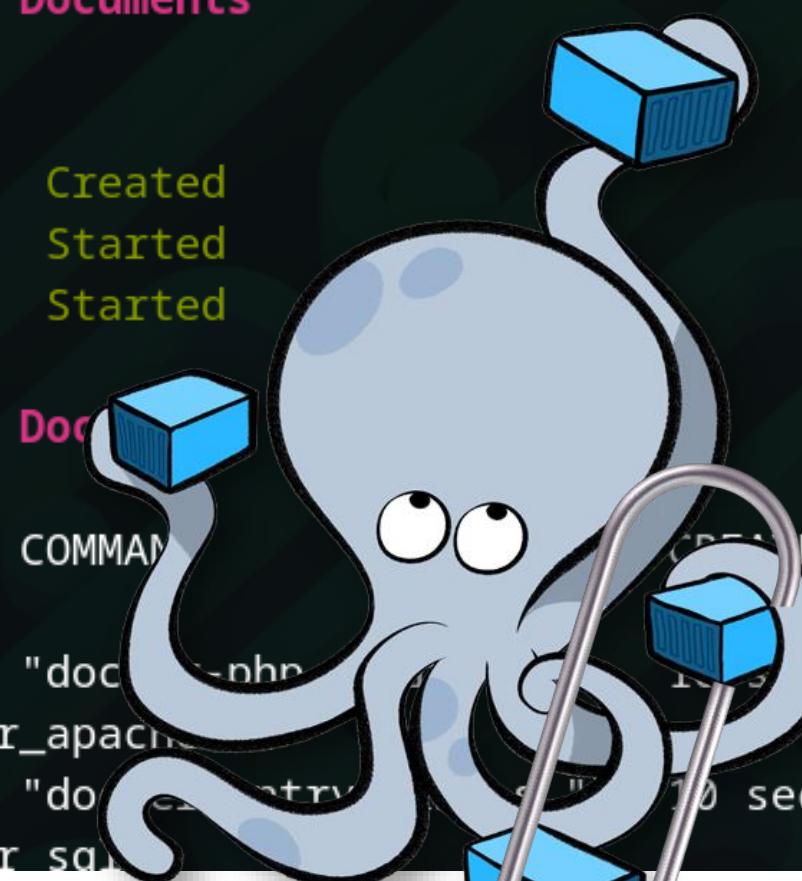
Docker compose

Compose es una herramienta para definir y ejecutar aplicaciones de Docker de **varios contenedores**. Esta extensión utiliza un archivo **YAML** para configurar todos los servicios necesarios. Después, con un solo comando, se crean y se inician todos los contenedores involucrados.

- Una vez creado el archivo docker-compose.yml se pueden iniciar todos los contenedores allí definidos con **docker compose up** (-d para iniciarlos en segundo plano) y detenerlos con **docker compose down**

```
[santiago@192 ~] $ docker compose up -d
[s+] Running 3/3
✓ Network documents_default      Created
✓ Container contenedor_sql       Started
✓ Container contenedor_apache    Started
```

```
[santiago@192 ~] $ docker ps
CONTAINER ID        IMAGE
NAMES
1c51ce9d95a2        documents-web
tcp
df4180c5e1f9        mysql:latest
":::6033->3306/tcp"  contenedor_sa
```



Video explicativo

docker-compose.yml



```
version: '3.8'

volumes:
  volumenBD:

services:
  web:
    build:
      context: /home/santiago
      dockerfile: Dockerfile
    container_name: contenedor_apache
    depends_on:
      - basedatos
    volumes:
      - /home/santiago/src:/var/www/html
    ports:
      - 8000:80

  basedatos:
    container_name: contenedor_sql
    image: mysql:latest
    command: --default-authentication-plugin=mysql_native_password
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: 123
    volumes:
      - volumenBD:/var/lib/mysql
      #MYSQL_DATABASE: test_based
    ports:
      - 6033:3306
```

Ejemplo

docker logs

Los logs son **registros cronológicos** de los eventos que afectan a un proceso o servidor en particular.

Usage: docker logs [OPTIONS] CONTAINER

Fetch the logs of a container

Aliases:

docker container logs, docker logs

Options:

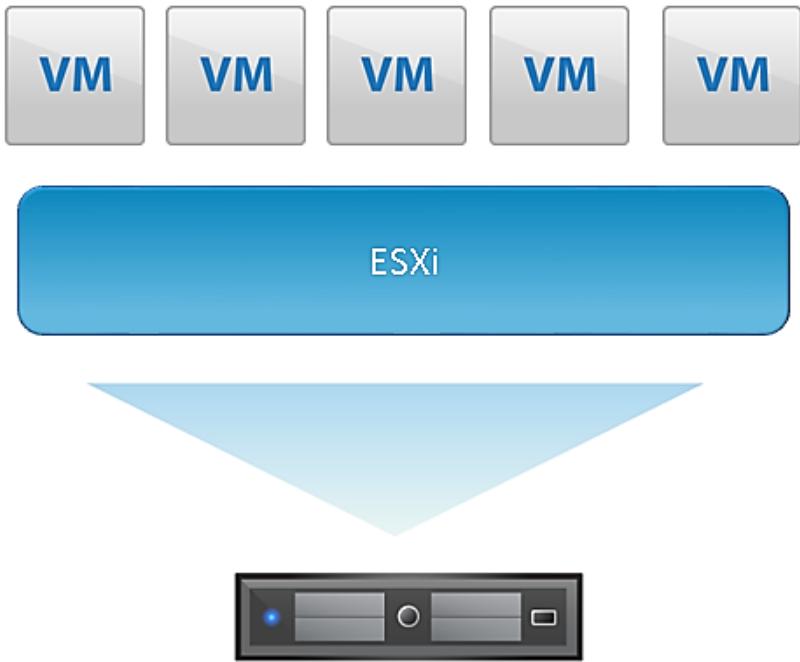
--details	Show extra details provided to logs
-f, --follow	Follow log output
--since string	Show logs since timestamp (e.g. "2013-01-02T13:23:37Z") or relative time
-n, --tail string	Number of lines to show from the end of the logs (default "all")
-t, --timestamps	Show timestamps
--until string	Show logs before a timestamp (e.g. "2013-01-02T13:23:37Z") or relative time

```
santiago @ 192 in Documents
→ docker logs -f contenedor_apache
AH00558: apache2: Could not reliably determine the server's fully qualified
Name' directive globally to suppress this message
AH00558: apache2: Could not reliably determine the server's fully qualified
Name' directive globally to suppress this message
[Mon Dec 11 18:24:37.986241 2023] [mpm_prefork:notice] [pid 1] AH00163:
assuming normal operations
[Mon Dec 11 18:24:37.986498 2023] [core:notice] [pid 1] AH00094: Command
172.20.0.1 - - [11/Dec/2023:18:26:00 +0000] "\x16\x03\x01\x02t\x01" 400
172.20.0.1 - - [11/Dec/2023:18:26:00 +0000] "\x16\x03\x01\x02t\x01" 400
172.20.0.1 - - [11/Dec/2023:18:26:08 +0000] "GET / HTTP/1.1" 200 429 "-"
0100101 Firefox/120.0"
172.20.0.1 - - [11/Dec/2023:18:26:08 +0000] "GET /favicon.ico HTTP/1.1"
Linux x86_64; rv:120.0) Gecko/20100101 Firefox/120.0"
```

Vmware ESXI (Hypervisor tipo 1)

ESXi es un *hypervisor bare metal* desarrollado por VMware para implementar y servir computadoras virtuales.

VMware ESXi puede gestionar los recursos de hardware de manera eficiente, virtualizando gran parte de la infraestructura IT para reducir los costes.



Este Hypervisor forma parte de una suite **vSphere** y puede utilizarse con **licencia gratuita por tiempo ilimitado** (incluye algunas restricciones, pero para un entorno pequeño puede ser suficiente).

[Home](#) / [Evaluate VMware Products](#) / [VMware vSphere Hypervisor 8](#)

Product Evaluation Center for VMware vSphere Hypervisor 8

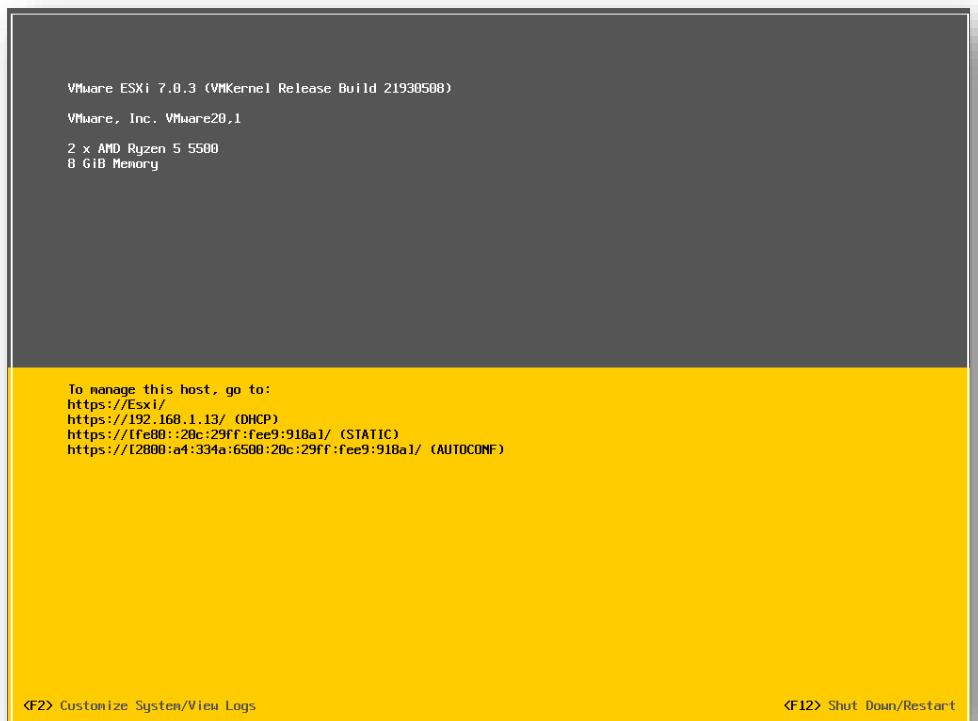
This download center features technical documentation and installation guides to make your use of vSphere Hypervisor a success.

Top vSphere Hypervisor Resources

- [VMware Hardware Compatibility Guide](#)

Instalación

La instalación es sencilla, apareciendo una guía detallada en el sitio oficial, junto con tablas de compatibilidad y un upgrade path para actualizar correctamente desde versiones anteriores.

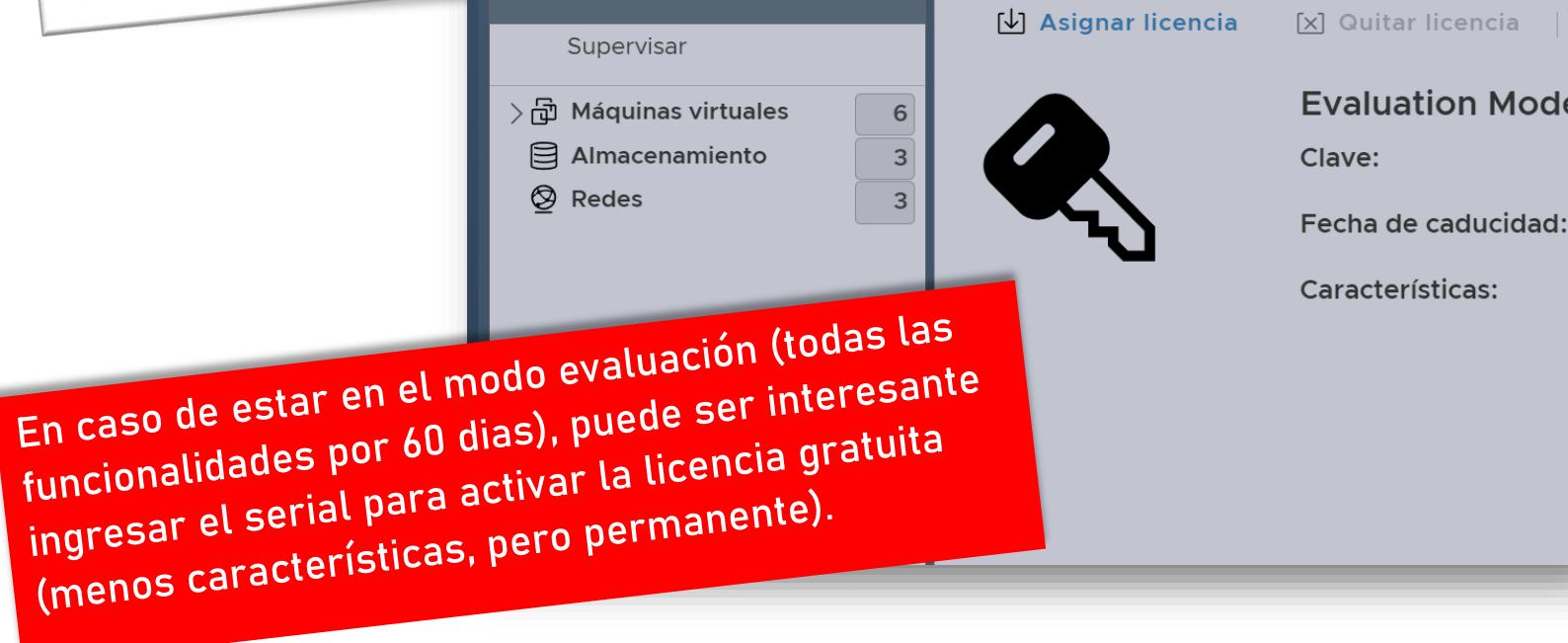
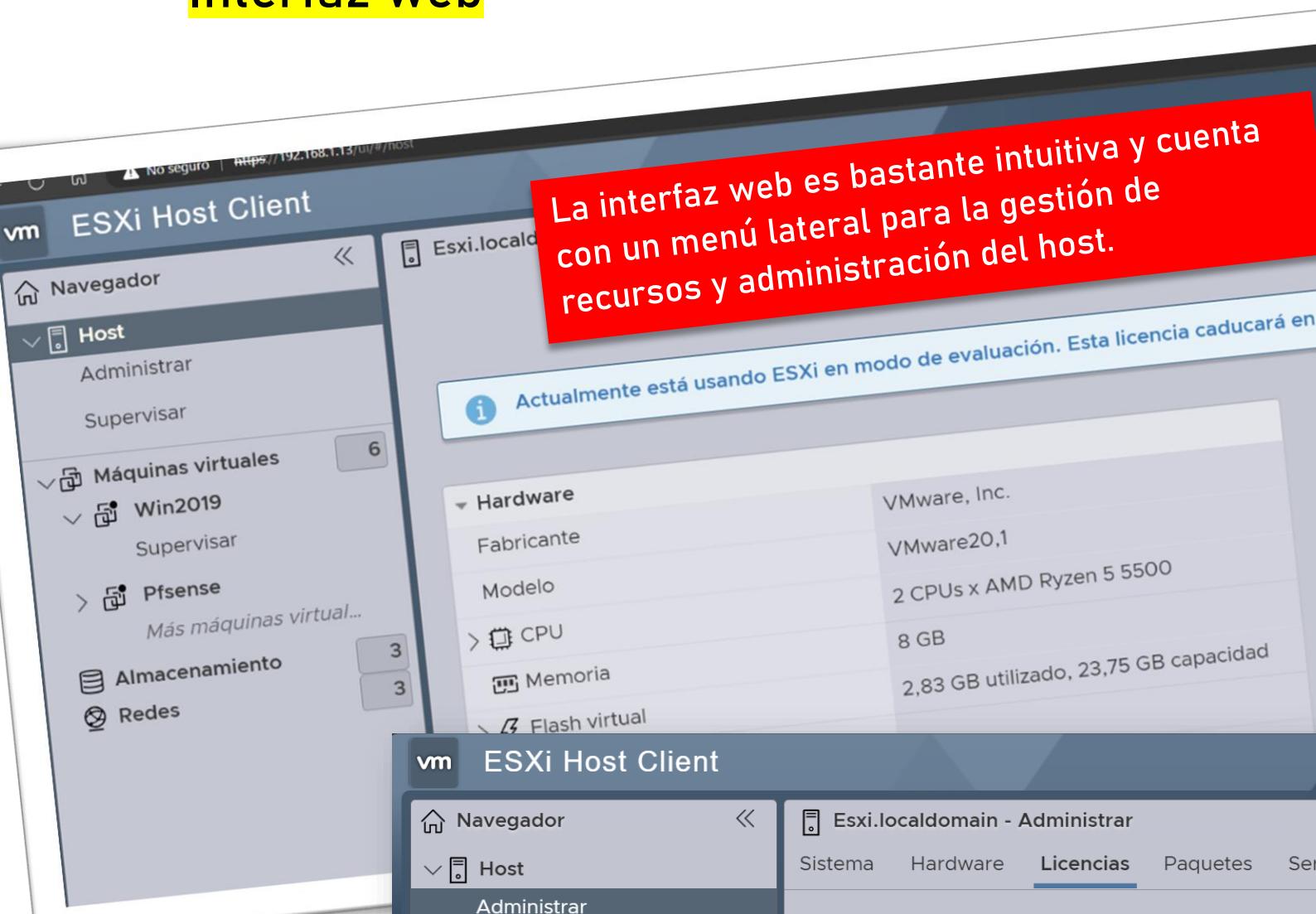


*Una vez instalado se podrá acceder a la configuración general y posteriormente (luego de configurar el apartado de red e interfaz de managment) **se podrá acceder desde otro equipo mediante una interfaz web, para tener acceso a todas las funcionalidades.***

Boot options para reducir particion VMFSL (tiny deploy)

	VMware ESXi								
	8.0U2	8.0U1	8.0	7.0U3	7.0U2	7.0U1	7.0	6.7 U3	6.7 U2
VMware ESXi 8.0	✓	✓							
VMware ESXi 7.0U3	✓	✓ ⁱ	✓ ⁱ						
VMware ESXi 7.0U2	✓	✓ ⁱ	✓						
VMware ESXi 7.0U1	✓	✓	✓		✓				
VMware ESXi 7.0	✓	✓	✓		✓	✓			

Interfaz web



En caso de estar en el modo evaluación (todas las funcionalidades por 60 días), puede ser interesante ingresar el serial para activar la licencia gratuita (menos características, pero permanente).

Crear MV

Antes de crear una MV es necesario cargar el archivo ISO desde el Explorador de almacenamiento de datos.

Una vez cargada se puede crear/registrar una máquina virtual desde el menú lateral.

Es posible crearla desde 0, listar una MV existente o crearla a partir de archivos OVF y VMDK



Explorador de almacenamiento de datos

↑ Cargar ↓ Descargar Eliminar

datastore1 (1)	.sdd.sf
datastore2	.vSphere-HA
COMPARTIDO	Alma
	Alma_1
	Fedora_clon
	Fedora_fino
	Imagenes
	Pfsense
	vCLS-cd653588-7...
	Win2019
	17763.3650.22110...
	AlmaLinux-9.3-x8...
	Fedora-Server-dv...

ESXi Host Client

Navegador

Host

Administrador

Supervisar

Máquinas virtuales

Win2019

Supervisar

Pfsense

Más máquinas virtuales

Almacenamiento

Redes

+ Nueva máquina virtual

1 Seleccionar tipo de creación

2 Seleccione un nombre y un sistema operativo invitado

3 Seleccionar almacenamiento

4 Personalizar configuración

5 Listo para completar

Seleccionar tipo de creación

¿Cómo desea crear la máquina virtual?

Crea una nueva máquina virtual

Implementar una máquina virtual a partir ...

Registrar una máquina virtual existente

Durante la personalización podemos asignar los recursos destinados para la MV, así como la configuración de red, tipo de aprovisionamiento para el VMDK y la ISO previamente cargada al host.

Personalizar configuración

Configure el hardware de la máquina virtual y las opciones adicionales de la máquina virtual

Hardware virtual **Opciones de máquina virtual**

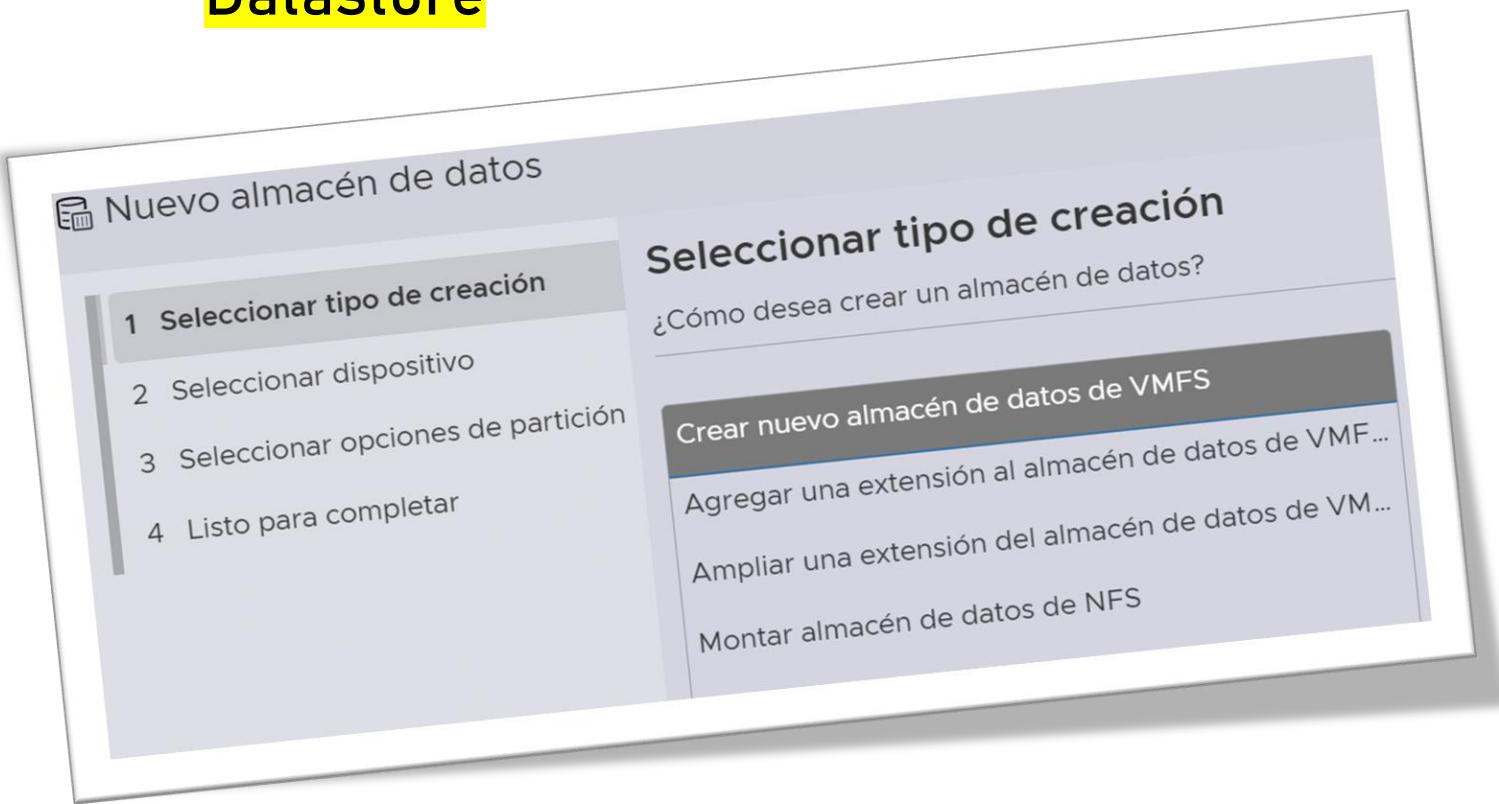
Agregar disco duro Agregar adaptador de red

Agregar otro dispositivo

> CPU	1	
> Memoria	1024	MB
> Disco duro 1	8	GB
LSI Logic Parallel		
> Controladora SCSI 0		
 Controladora USB 1	USB 2.0	
Red_INTERNA		

CANCELAR **ATRÁS** **SIGUIENTE** **FINALIZAR**

Datastore



Los almacenes de datos se utilizarán para alojar los discos y archivos de configuración de las MV.

Pueden ser unidades internas del host (utilizando el sistema de archivos **VMFS**) o conectar con datastores externos utilizando **NFS**.

Seleccionar almacenamiento

Seleccionar tipo de almacenamiento y almacén de datos

Estándar

Memoria persistente

Seleccione un almacén de datos para los archivos de configuración de la máquina virtual y todos sus discos virtuales.

Nombre	Capacida	Libre	Tipo	Aprovisio
COMPARTIDO	0 B	0 B	NFS41	Comp...
datastore1 (1)	147,75 ...	73,04 ...	VMFS6	Comp...
datastore2	29,75 ...	28,34 ...	VMFS6	Comp...

Aprovisionamiento

Disco duro 1	8	GB	v
Tamaño máximo	73,04 GB		
Tipo	Aprovisionado fino		
Archivo de disco	[datastore1 (1)] PfSense/PfSense.vmdk		

El disco duro de una máquina virtual ([archivo VMDK](#)) puede ser de 2 tipos:

- El **aprovisionamiento fino** es un método que optimiza la utilización del almacenamiento mediante la asignación del espacio de almacenamiento de forma flexible y a pedido. (Menor rendimiento de la MV pero gestión eficiente del almacenamiento).
- El **aprovisionamiento grueso**, se proporciona por adelantado el espacio de almacenamiento para anticipar necesidades futuras. Sin embargo, el espacio puede permanecer inutilizado, lo cual puede no resultar óptimo. (Mayor rendimiento de la MV pero gestión poco óptima del almacenamiento).

Es posible cambiar el tipo de aprovisionamiento de una MV ya creada, aunque puede implicar exportar e importar, o realizar una copia manual de los archivos de la misma.

Networking

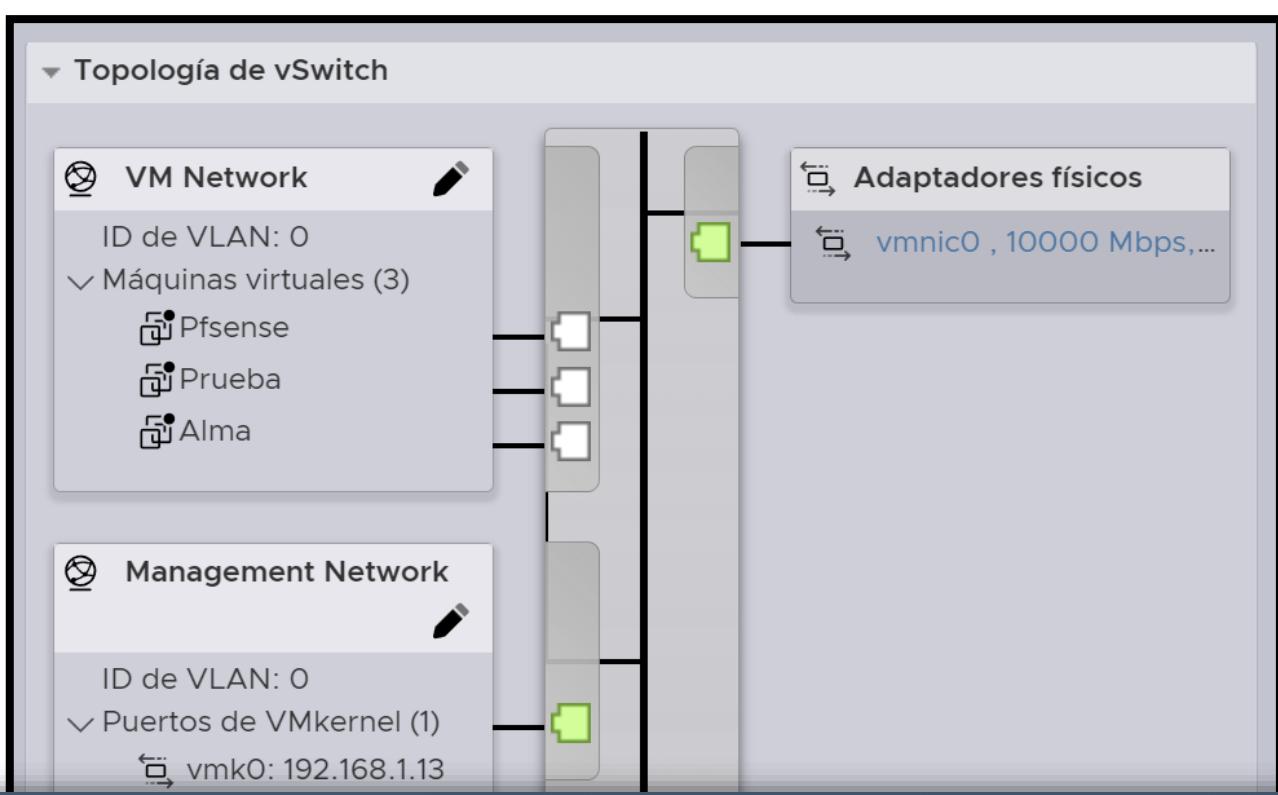
Vmnic -> Son tarjetas físicas. Es recomendable tener redundancia de administración.

VMkernel -> Interfaces virtuales que se utilizan para los diferentes servicios (administración web, vMotion, entre otros) y pueden asociarse a interfaces físicas).

vSwitches -> Todo lo que se conecta al mismo switch,

p pertenece a la misma red*. Se pueden asociar a interfaces físicas o virtuales

Grupos de puertos -> (hacen referencia a un switch en particular, y gestionan las VLANs*)

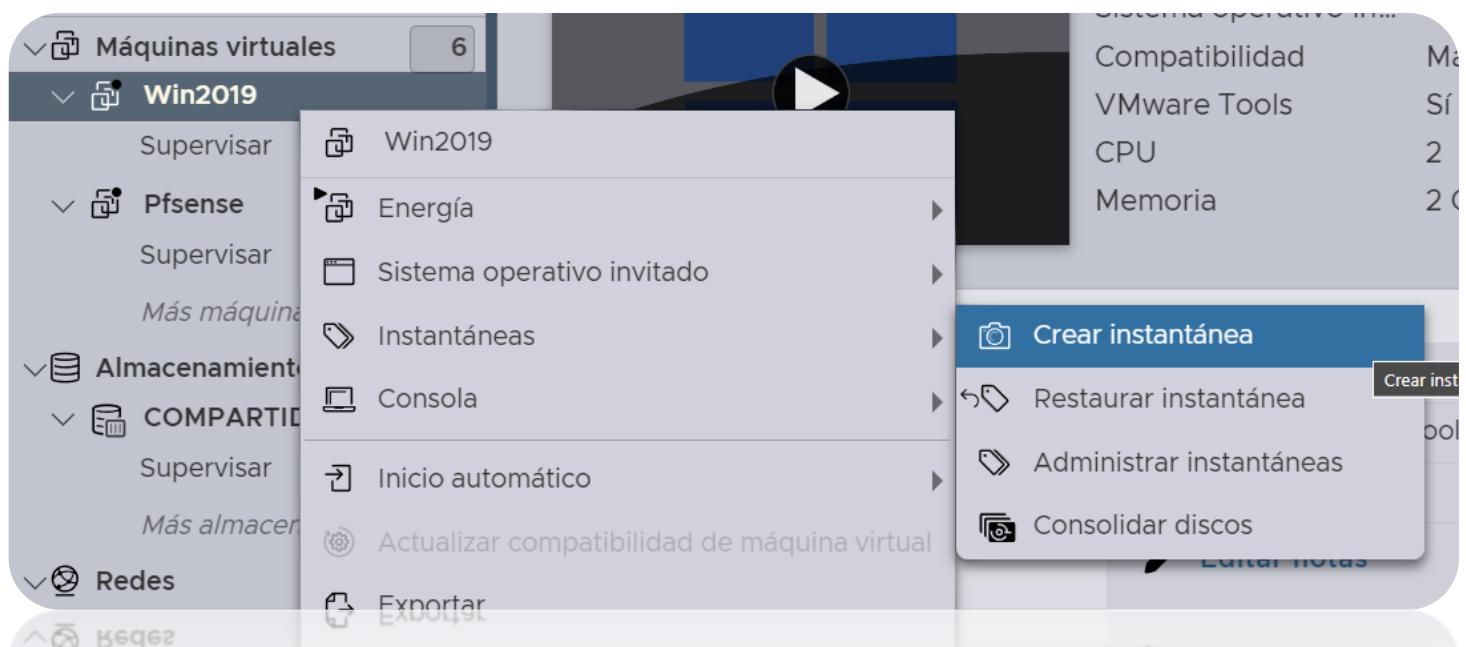


Esxi.localdomain - Redes

Grupos de puertos Comutadores virtuales NIC físicas NIC de VMkernel Pilas de TCP/IP Reglas de firewall

Agregar grupo de puertos		Editar configuración	Actualizar	Acciones
Nombre	Puertos activos..	ID de VLAN	Tipo	vSwitch
Red_SERVIDORES	0	0	Grupo de puertos estándar	SWITCH DMZ
Red_INTERNA	0	0	Grupo de puertos estándar	SWITCH LAN
VM Network	0	0	Grupo de puertos estándar	vSwitch0

Snapshots



Cuando se crea una instantánea de una máquina virtual, se copia y se almacena una **imagen de la máquina en un estado determinado**.

Las snapshots son útiles como una **solución a corto plazo** para probar software con efectos desconocidos o potencialmente dañinos.

No son adecuadas para copias de seguridad de máquinas virtuales a largo plazo, ya que **la creación de discos delta hace que el rendimiento de la MV de vea disminuido**.

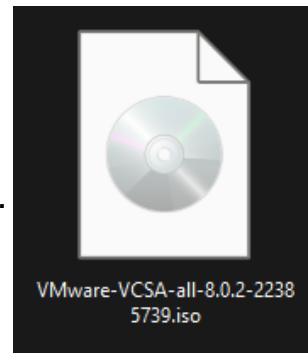


Vcenter

Permite administración centralizada de varios hosts ESXI.

Proporciona servicios/tecnologías de la suite vSphere (vMotion, HA).

En sus últimas versiones, VCSA es una MV preconfigurada pronta para desplegarse en un host ESXI.



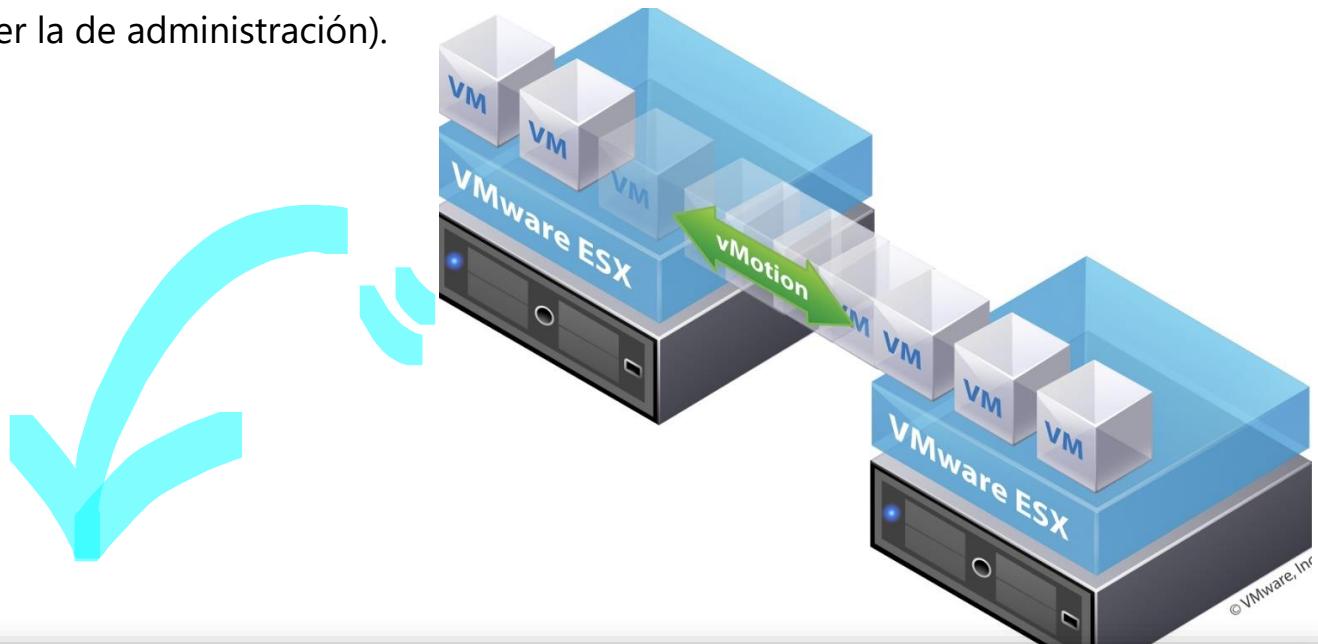
A screenshot of the vSphere Client interface. On the left, there's a sidebar with options like 'Supervisar', 'Máquinas virtuales' (which shows four items: 'VMware vCenter Server', 'Fedora_Aprov.fino', 'W2019', and 'vCLS-a811d5d7-24a0-4052-8167-0de8fc617860'), 'Almacenamiento', 'Redes', and 'Más almacenamiento...'. A green curved arrow points from the 'Máquinas virtuales' section towards the main content area. The main content area shows a terminal-like window for the 'VMware vCenter Server' appliance. The window displays system information: 'VMware vCenter Server 8.0.2.80000', 'Type: vCenter Server with an embedded Platform Services Controller', '2 x AMD Ryzen 5 5500', and '13.6 GiB Memory'. It also provides instructions: 'Please visit the following URL to configure this appliance: https://192.168.126.129:5480', 'Download support bundle from: https://192.168.126.129:443/appliance/support-bundle', and 'https://192.168.126.129/ (DHCP)'. At the bottom of the terminal window, there are F12 and F2 keys with labels 'Shut Down/Restart' and 'Customize System'. The bottom of the screen shows a navigation bar with tabs like 'Resumen', 'Supervisar', 'Configurar', etc., and a red banner across the bottom with the text 'Interfaz web vSphere Client'.

Vmotion

Migración de MV en caliente de un host ESXI a otro -> **SIN PÉRDIDA DE SERVICIO**

Debe estar **definido el clúster** (se instala agente vCLS en cada host)

- Es recomendable contar con algún datastore compartido entre nodos.
- Debe existir una interfaz VMkernel destinada a este servicio (puede ser la de administración).



Migrar |
Fedora_Aprov.fino

Seleccionar un tipo de migración

Cambie el almacenamiento, el recurso informático o ambos de las máquinas virtuales.

ORIGEN DE LA MÁQUINA VIRTUAL (i)

1 Seleccionar un tipo de migración

- 2 Seleccionar un recurso informático
- 3 Seleccionar redes
- 4 Seleccionar prioridad de vMotion
- 5 Listo para completar

Cambiar solo recurso informático

Migra las máquinas virtuales a otro host o clúster.

Cambiar solo almacenamiento

Migra el almacenamiento de las máquinas virtuales a un clúster de almacén de datos compatible.

Cambiar recurso informático y almacenamiento

Migra las máquinas virtuales a un clúster o un host específico y su almacén de datos específico.

Exportación entre instancias de vCenter Server

Migre las máquinas virtuales a una instancia de vCenter Server no vinculada.

ORIGEN DE LA MÁQUINA VIRTUAL (i)	
Clúster	Cluster-1
Host	192.168.126.128
Redes	Linux
Almacenamiento	VM Network
	datastore1

Existen 3 variantes de Vmotion

- Mover ejecución (CPU y RAM).

La MV pasa a ejecutarse en otro host ESXI, migrando el poder de cómputo (cambia de inventario).

El disco duro (vmdk) no cambia de ubicación.

Para este tipo de movimiento, el nodo que recibe la MV tiene que tener acceso al datastore donde se encuentra el vmdk.

- Mover almacenamiento.

Solamente se mueve el disco duro de la MV de un datastore a otro.

El movimiento puede ser en el mismo host donde se ejecuta la VM, o en otro nodo del clúster.

Sólo se podrá mover a un datastore al que tenga permiso de acceso el host que ejecuta la MV.

- Ejecución y almacenamiento al mismo tiempo.

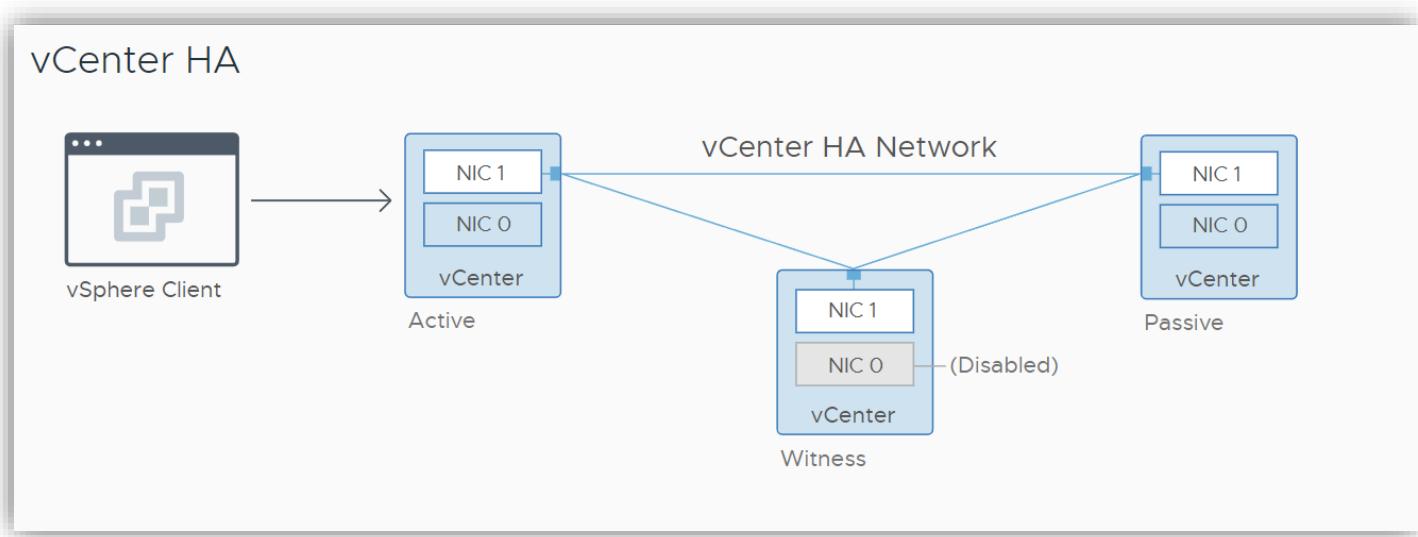
Es una combinación de las anteriores (suele demorar más tiempo).

Al migrar la capacidad de ejecución y posteriormente el almacenamiento, puede migrarse la MV a un host destino, sin necesidad de contar con un datastore compartido con el origen.

Es importante tener en cuenta que las operaciones de vMotion se realizan de forma manual y en caliente, y si bien la pérdida de servicio es casi inexistente, debería planificarse el momento de la migración en un horario de baja carga de los servidores.

Vsphere HA (High Availability)

El servicio de HA reaccionará automáticamente en caso de fallar uno de los nodos del clúster pudiendo reiniciar todas las MV en otro host (siempre y cuando sea posible y dependiendo de la configuración realizada).



Para activar Vsphere HA es necesario cumplir con **alguna de estas condiciones**.

- Crear una red HA (nodo activo, pasivo y testigo).
- Contar con 2 datastore compartidos por los nodos del clúster.

En caso de no utilizar un tercer nodo para la HA, basta con 2 datastores de acceso común para los host ESXI (realizamos pruebas con un solo storage compartido y funcionaba en la mayoría de los casos).

Estos datastores se utilizarán para enviar latidos (señales a las MV) que comprueban el estado de las mismas y la conexión con el host. -> **Es importante tener instaladas las Vmware Tools.**

Normalmente la comutación por error intentará reiniciar las MV afectadas en un nuevo host, aunque pueden configurarse por separado determinadas situaciones.

- Pérdida de comunicación con el host.
- Desconexión con el datastore.
- Apagado o reinicio.

vSphere HA está activado.
Se informa de los detalles del tiempo de ejecución para vSphere HA.

Proactive HA está desactivado

Condiciones de error y respuestas

Error	Respuesta
Error de host	✓ Reiniciar las máquinas virtuales
Proactive HA	⚠ Deshabilitado
Aislamiento del host	✓ Cerrar y reiniciar las máquinas virtuales
Almacén de datos con pérdida permanente de dispositivos	✓ Apagar y reiniciar las máquinas virtuales

Editar la configuración del clúster | Cluster-1

vSphere HA

Errores y respuestas

Puede configurar el modo en que vSphere HA responde a las condiciones de error en este clúster. Se admiten las siguientes condiciones de error: de host, aislamiento de host, protección de componentes de la máquina virtual (almacén de datos con PDL), máquina virtual y aplicación.

Habilitar supervisión de hosts

Respueta de error de host

Reiniciar las máquinas virtuales

Respueta para el aislamiento del host

Apagar y reiniciar las máquinas virtuales

Almacén de datos con PDL

Apagar y reiniciar las máquinas virtuales

Almacén de datos con APD

Apague y reinicie las máquinas virtuales (directiva de reinicio)

Supervisión de máquinas virtuales

Supervisión de máquinas virtuales y aplicaciones

Es importante tener en cuenta los recursos disponibles a la hora de admitir nuevas MV, la prioridad y recurrir a la documentación de VMware en caso de dudas.

Proxmox

Proxmox Virtual Environment, surge como alternativa a los hipervisores de tipo 1 propietarios.

Es una distribución de **GNU/Linux basada en Debian**, con una interfaz web incorporada, que permite administrar fácilmente **máquinas virtuales y contenedores**, almacenamiento, redes definidas por software, agrupación en clústeres de alta disponibilidad y múltiples herramientas listas en una única solución.

El proyecto incluye otros productos además del hipervisor y puede utilizarse con suscripción de pago (acceso a repositorios especiales) o de forma gratuita.



[Get Help ▾](#) [Buy now](#)



[Home](#)

[Virtualization](#)

[Backup](#)

[Email Security](#)

[Downloads](#)

[Services](#)

[Partners](#)

[About](#)

Simplify your data center.

Proxmox delivers powerful, enterprise-grade solutions with full access to all functionality for everyone - highly reliable and secure.

The software-defined and open platforms are easy to deploy, manage and budget for.

NEW: Version 8.1

NEW: Version 3.1

Proxmox Virtual Environment

Proxmox Virtual Environment is a complete open-source platform for enterprise virtualization. With the built-in web interface you can easily manage VMs and containers, software-defined storage and networking, high-availability clustering, and multiple out-of-the-box tools using a single solution.

[About Proxmox Virtual Environment](#)

Proxmox Backup Server

Proxmox Backup Server is an enterprise backup solution for backing up and restoring VMs, containers, and physical hosts. The open-source solution supports incremental backups, deduplication, Zstandard compression, and authenticated encryption.

[About Proxmox Backup Server](#)

Proxmox Mail Gateway

Proxmox Mail Gateway is an open-source email security solution that protects your mail server against all email threats from the moment they emerge. The full featured mail proxy can be easily deployed between the firewall and your internal mail server in just a few minutes.

[About Proxmox Mail Gateway](#)

X PROXMOX Virtual Environment 8.0.4 Search

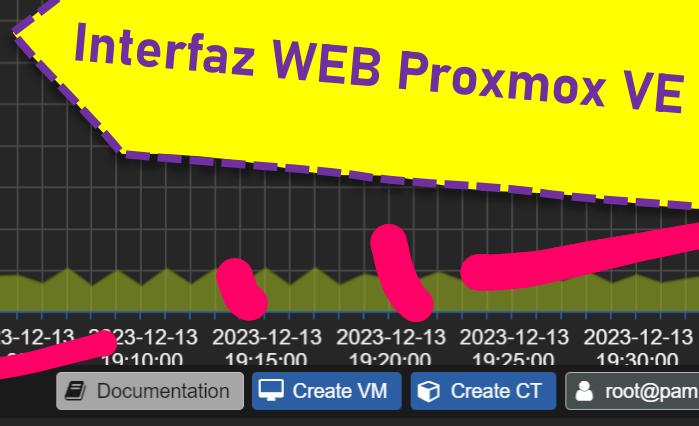
Server View Container 222 (debian) on node 'proxmox' No Tags

Datacenter
proxmox
111 (fedora)
222 (debian)
100 (TrueNAS)
254 (VPN)
localnetwork (proxmox)
Disco1 (proxmox)
local (proxmox)
local-lvm (proxmox)

Summary
Console
Resources
Network
DNS
Options
Task History
Backup
Replication
Snapshots
Firewall
Permissions

debian (Uptime: 19 days 00:40:55)
Status running
HA State none
Node proxmox
CPU usage 0.04% of 2 CPU(s)
Memory usage 4.60% (94.23 MiB of 2.00 GiB)
SWAP usage 0.00% (0 B of 512.00 MiB)
Bootdisk size 8.19% (2.41 GiB of 29.36 GiB)

CPU usage



Interfaz WEB Proxmox VE

2023-12-13 19:00:00 2023-12-13 19:05:00 2023-12-13 19:10:00 2023-12-13 19:15:00 2023-12-13 19:20:00 2023-12-13 19:25:00 2023-12-13 19:30:00

Documentation Create VM Create CT root@pam

Tags Start Shutdown Console More Help

Hour (average)

days 00:40:55)

running
none
proxmox
0.04% of 2 CPU(s)
4.60% (94.23 MiB of 2.00 GiB)
0.00% (0 B of 512.00 MiB)
8.19% (2.41 GiB of 29.36 GiB)

VNC Command Terminal - noVNC - Personal: Microsoft Edge

⚠ No seguro | https://192.168.1.100:8006/?console=lxc&novnc=1&vmid=222&vmname=debian&node=...

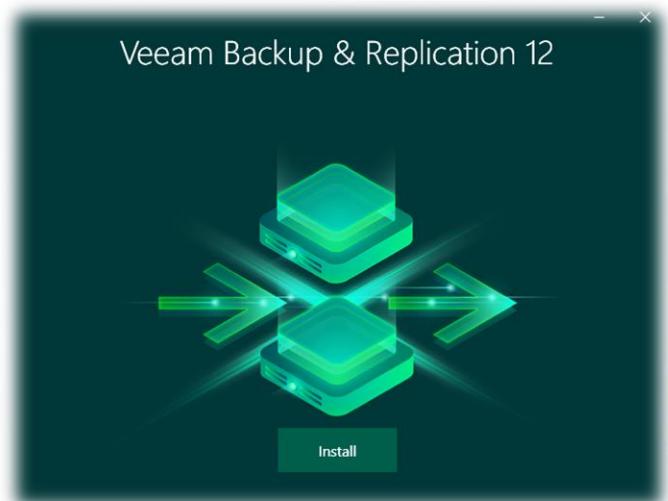
```
root @ debian in ~
root @ debian in ~
root @ debian in ~
```

CPU usage

Veeam-Backup (Community Edition)

Es una herramienta que permite automatizar backups, ya sea en entornos cloud, virtuales o físicos.

Cuenta con una [edición gratuita](#) con la mayoría de opciones disponibles, aunque limita la cantidad de instancias de respaldo.



A detailed screenshot of the Veeam Backup & Replication Community Edition software interface. The main window shows a 'Protection Group Tools' ribbon with tabs like Home, View, Protection Group, Actions, Statistics, and Report. Under the Protection Group tab, there are buttons for Add Group, Edit Group, Disable Group, Remove Group, Rescan, Add to Backup, and Details. On the left, there's an 'Inventory' pane with sections for Virtual Infrastructure, Physical Infrastructure (which is selected), and Manually Added. A 'Create Protection Group' dialog box is open in the center. It has a 'Create Protection Group' button with a plus icon. Below it, text explains that a protection group defines a set of computers (physical servers, workstations or cloud instances) to be backed up. It also mentions that groups can be populated with individual computers, Active Directory containers or a dynamic Cloud Service Provider. The 'Computers' step of the wizard is currently active. It shows a table with columns 'Computer' and 'Account'. There's a 'Add...' button and a 'Set User...' button. Below the table, there's a 'Host name or IP address:' input field and a 'Credentials:' dropdown with 'Select existing or add new credentials' and an 'Add...' button. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. At the very bottom of the interface, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The status bar at the bottom shows '0 hosts'.

Add Server

Before using Veeam Backup & Replication, you must register your protected data sources in the inventory. To start this process, click the Add Server button in the ribbon (or just click this text).

For VMware vSphere protection, add a vCenter Server. You can also add ESXi hosts individually. Adding vCenter Server is preferred, because it makes Veeam Backup & Replication vMotion-aware.

For Microsoft Hyper-V protection, add System Center Virtual Machine Manager (SCVMM) Servers, Hyper-V clusters, or standalone Hyper-V hosts.

For physical and cloud servers and workstations protection, create one or more Protection Groups listing all computers you want to backup. For NAS protection, add an NDMP server. Note that NDMP backups are only supported to tape or Virtual Tape Libraries (VTL).



Create Job

Veeam Backup & Replication provides different options to balance recovery time with storage requirements. Backup consumes less disk space but requires longer recovery time, making it ideal for long term data retention. Replication provides faster recovery time at the increased storage costs and shorter retention.

To create a new backup or replication job, go to the Backup & Replication tree tab, and click the corresponding button in the ribbon.



Restore

To restore a machine from a backup or a replica, click the Restore button in the ribbon and select the required restore type.

Alternatively, you can browse the Backups node of the Backup & Replication tab to locate the required machine by searching for its name. You can also start a restore by double-clicking the full backup (.VBK) file in the Windows Explorer.

Se pueden crear grupos de protección y agregar equipos a respaldar mediante agentes.

Permite crear tareas recurrentes, seleccionar el tipo de respaldo a realizar y convertir discos respaldados a formato VMDK

The screenshot shows the Veeam Backup & Replication software interface. In the center, a 'New Agent Backup Job' dialog is open under the 'Job Mode' section. The 'Type' dropdown is set to 'Server'. The 'Mode' dropdown is set to 'Managed by agent'. A note states: 'Veeam backup server deploys the protection policy to all agents, however the agent itself. This mode is recommended for workstations and servers located connectivity to the main data center.' At the bottom right of the dialog are 'Next >' and '< Previous' buttons. A yellow callout box with a dashed border points from the bottom left towards the 'Job Mode' section, containing the text: 'Para respaldar todas las MV de un ESXI y restaurarlas posteriormente en el mismo host, la licencia de ESXI no puede ser FREE'.

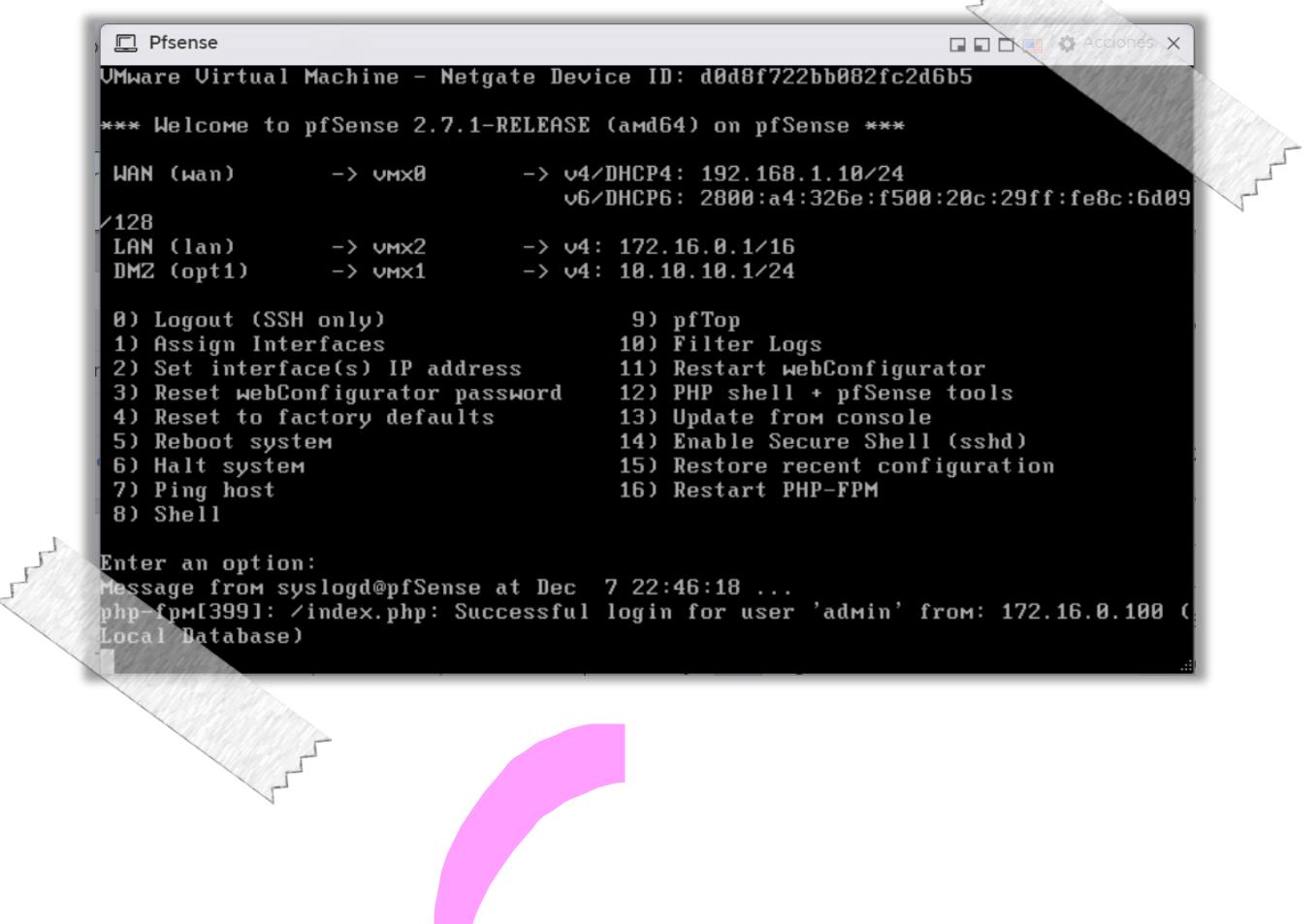
PfSense

Distribución personalizada de FreeBSD adaptada para su uso como **firewall** y **router**. Es un sistema **open-source** que puede ser instalado en gran variedad de dispositivos, y además cuenta con una interfaz web sencilla para su configuración.

WAN

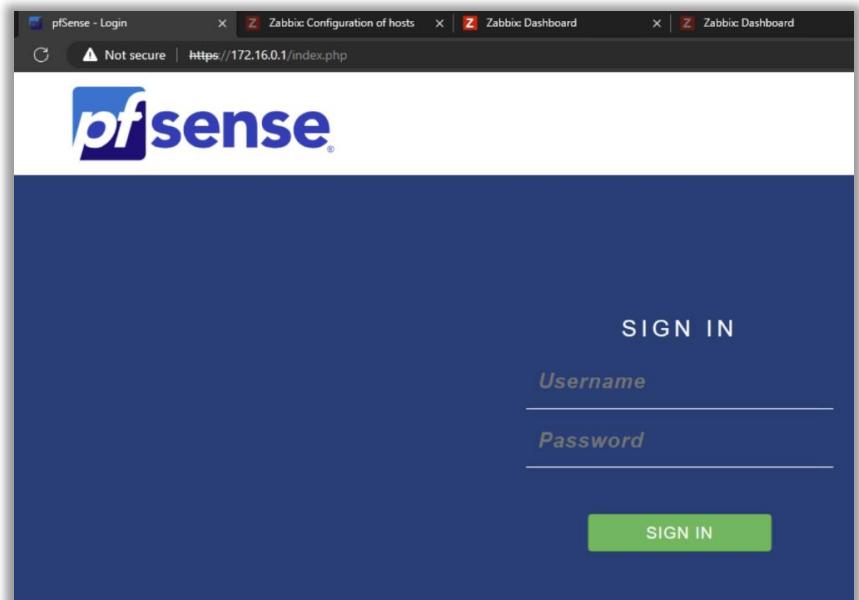
LAN

DMZ



Interfaz Web

Una vez terminada la configuración inicial, se podrá ingresar al equipo con PfSense desde una interfaz web (**por defecto solo disponible mediante la interfaz definida como LAN**).



Desde esta interfaz se puede visualizar el **dashboard** principal, configurar las **reglas del firewall**, definir **alias**, tipos de **NAT** y configurar otros servicios opcionales (**DDNS, OpenVPN**).

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard ✖ + ?

System Information

Name	pfSense.home.arpa
User	admin@172.16.0.100 (Local Database)
System	VMware Virtual Machine Netgate Device ID: d0d8f722bb082fc2d6b5
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.1-RELEASE (amd64) built on Wed Nov 15 17:06:00 UTC 2023 FreeBSD 14.0-CURRENT
CPU Type	AMD Ryzen 5 5500 AES-NI CPU Crypto: Yes (inactive)

Version 2.7.2 is available. ↻
Version information updated at Tue Dec 12 4:56:45 UTC 2023 ↻

Netgate Services And Support

Interfaces			
WAN	⬆️ autoselect	192.168.1.10	2800:a4:32a7:a200:20c:29ff:fe8c:6d09
LAN	⬆️ autoselect	172.16.0.1	
DMZ	⬆️ autoselect	10.10.10.1	

Alias

Los alias asocian nombres a puertos, hosts o redes completas. Se puede hacer referencia a los alias mediante reglas de firewall, reenvíos de puertos, reglas de NAT salientes y otros apartados. **El uso de alias simplifica la gestión del firewall y ayuda a documentar el funcionamiento del sistema.**

Firewall / Aliases / Edit

Properties

Name	<input type="text"/>	The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".									
Description	<input type="text"/> A description may be entered here for administrative reference (not parsed).										
Type	Host(s)										
Host(s) <table border="1"> <tr> <td>Hint</td> <td colspan="2">Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name. They will be re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.</td> </tr> <tr> <td>IP or FQDN</td> <td><input type="text"/> Address</td> <td><input type="text"/> Description</td> </tr> <tr> <td colspan="3"> <input type="button" value="Save"/> <input type="button" value="Add Host"/> </td> </tr> </table>			Hint	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name. They will be re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.		IP or FQDN	<input type="text"/> Address	<input type="text"/> Description	<input type="button" value="Save"/> <input type="button" value="Add Host"/>		
Hint	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name. They will be re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.										
IP or FQDN	<input type="text"/> Address	<input type="text"/> Description									
<input type="button" value="Save"/> <input type="button" value="Add Host"/>											

pfSense® COMMUNITY EDITION

System ▾ Interfaces ▾ **Firewall ▾** Services ▾ VPN ▾ Status ▾

WARNING: The 'admin' account password is set to the default value. Please change the password in the User Manager.

Firewall / Aliases / IP

IP Ports URLs All

Aliases

- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Firewall Aliases IP

Name	Type	Values	Description
Fedora	Host(s)	10.10.10.10	Servidor apache Fedora

Firewall

Se pueden crear reglas que apliquen para cualquiera de las interfaces que gestiona Pfsense.

Mediante la interfaz gráfica se pueden setear **origen y destino** (host, red, alias o interfaz), especificando el **tipo de comunicación** para cada caso (puerto y protocolo).

Permiten incluir una descripción y activar/desactivar la regla en cualquier momento.

Firewall / Rules / Edit



Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

Invert match

Any

Source Address

/

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination

Invert match

Any

Destination Address

/

Destination Port Range

(other)

From

(other)

To

Custom

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	13/5.43 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP any	Win2019	*	Fedora	*	*		none		
<input type="checkbox"/>	<input checked="" type="checkbox"/> 4/164.50 MiB	IPv4 *	LAN subnets	*	*	*	*		none	Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN subnets	*	*	*	*		none	Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

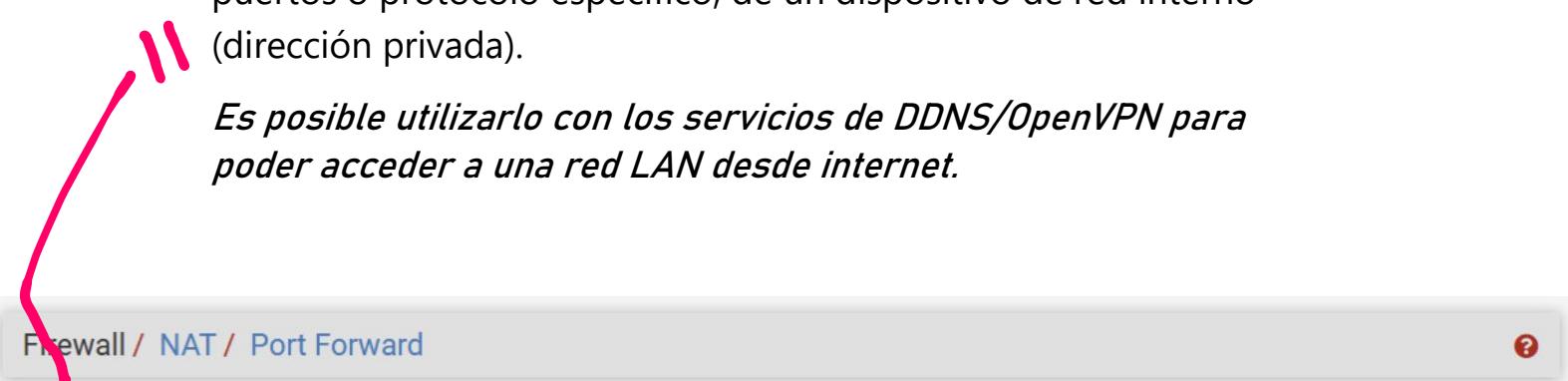
* Recordar que las reglas se evalúan en orden, por lo que es importante el lugar que ocupa dentro de la tabla.



Port Forward (NAT)

El reenvío de puertos permite el acceso a un puerto, rango de puertos o protocolo específico, de un dispositivo de red interno (dirección privada).

Es posible utilizarlo con los servicios de DDNS/OpenVPN para poder acceder a una red LAN desde internet.



Port Forward 1:1 Outbound NPT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	6480	Fedora	80 (HTTP)		

Add Add Delete Toggle Save Separator

Legend

Pass
 Deny

Outbound (NAT)

Firewall / NAT / Outbound

?

Port Forward 1:1 **Outbound** NPt

Outbound NAT Mode

Mode	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Automatic outbound NAT rule generation. (IPsec passthrough included)	Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)

 Save

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
										 Add  Add  Delete  Toggle  Save

Automatic Rules

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓ WAN	127.0.0.0/8 ::1/128	172.16.0.0/16	10.10.10.0/24	*	*	500	*	✓ Auto created rule for ISAKMP
✓ WAN	127.0.0.0/8 ::1/128	172.16.0.0/16	10.10.10.0/24	*	*	*	*	✗ Auto created rule

i

NAT saliente, controla cómo se traduce la dirección y puertos de origen que salen de una interfaz.

La opción predeterminada, realiza automáticamente NAT desde la interfaz interna (LAN) a la interfaz externa (WAN).

Desde este apartado se puede configurar, de manera sencilla, cuáles son las direcciones IP privadas que pueden salir a internet mediante el firewall.

ZABBIX

Zabbix es un sistema **open-source** que permite *monitorear* la capacidad, rendimiento y la disponibilidad de equipos, servicios y aplicaciones de una red.

Instalación de Zabbix según S.O

systemctl start zabbix-agent

systemctl start zabbix-server

Zabbix necesita una base de datos para su funcionamiento. Si bien las estructuras necesarias se crean mediante **zabbix-sql-scripts** (los comandos aparecen detallados en la documentación oficial) **Es necesario contar con el servicio previamente instalado y corriendo (MySQL o PostgreSQL).**

dnf install mysql-server

systemctl start mysqld

Desde terminal de Linux

mysqladmin -u root -h localhost password 'mi_password' -> password root por primera vez

Dentro de MySQL

ALTER USER root@localhost IDENTIFIED WITH mysql_native_password BY 'password';

FLUSH PRIVILEGES;

Cambiar contraseña root en mysql

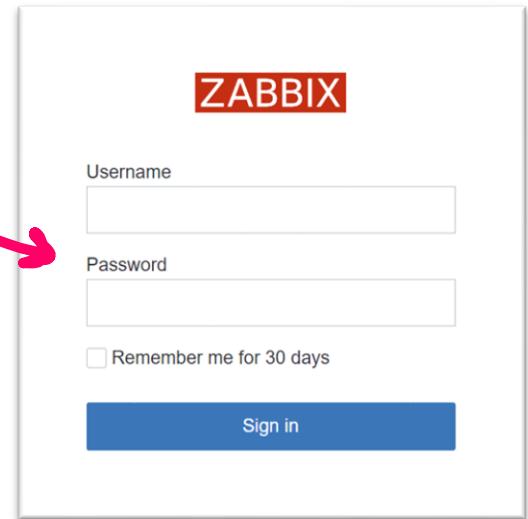
Una vez esta todo configurado se puede ingresar a la interfaz web de Zabbix

http://IP_servidor/zabbix

***Asegurarse de que el firewall no bloquea nada y que los servicios están iniciados.**

Admin(user) y **zabbix**(pass)
son las credenciales por defecto

Pueden surgir errores de paquetes de idioma y que deban agregarse manualmente en el servidor para visualizar los dashboards correctamente.



Comandos para distribuciones RedHat

locale -a
dnf install glibc-langpack-en

A screenshot of the Zabbix Global view dashboard. The top navigation bar shows the URL as "No seguro | 192.168.1.8/zabbix/zabbix.php?action=dashboard.view". The left sidebar contains links for Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, and Administration. The main area displays various metrics and graphs. A prominent green box in the center shows "1.55 ↑ Zabbix server Values per second". To the right, there's a "System information" table with details like "Zabbix server is running" and "Number of hosts (enabled/disabled)". On the far right, a large digital clock shows "12:14" and the location "Montevideo".

Zabbix permite instalar **agentes** para recopilar datos y métricas de diferentes sistemas.

Estos datos luego se envían al servidor y pueden visualizarse en una interfaz (**dashboard**) personalizable.

El agente puede funcionar de forma **activa o pasiva**, utilizando los puertos **10050** y **10051** respectivamente, para comunicarse con el servidor.

Permite además monitoreo mediante el protocolo **SNMP**.

Existen **templates** que permiten extraer datos de determinados parámetros (**items**) y generan alertas tras suceder determinados eventos (**triggers**) con diferentes niveles de criticidad.

Estos templates van a simplificar el monitoreo de algunos dispositivos, servicios y sistemas operativos en particular.

Para agregar un host nuevo (equipo a monitorear).

- Monitoring
- Services
- Inventory
- Reports
- Data collection**
- Template groups
- Host groups
- Templates
- Hosts**
- Maintenance
- Event correlation
- Discovery

0 selected

Al agregar un nuevo host se debe seleccionar un template y la interfaz de monitoreo.

New host

Host	IPMI	Tags	Macros	Inventory	Encryption	Value mapping
* Host name						
Visible name						
Templates	type here to search					Select
* Host groups	type here to search					Select
Interfaces	No interfaces are defined.					
Add						
Description	Agent SNMP JMX IPMI					
Monitored by proxy	(no proxy)					
Enabled	<input checked="" type="checkbox"/>					



Host groups		Status		Enabled		Disabled	
Templates		Monitored by		Any		Server	
Name		Proxy					Select
DNS		Tags	And/Or	Or			
IP		tag	Contains	value			R
Port		Add					
		Apply		Reset			

	Name ▲	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent e
	TrueNAS	Items 147	Triggers 55	Graphs 36	Discovery 7	Web	192.168.1.200:161		TrueNAS by SNMP	Enabled	SNMP	None
	Windows_Server	Items 109	Triggers 77	Graphs 11	Discovery 4	Web	172.16.0.100:10050		ICMP Ping, Windows by Zabbix agent active	Enabled	ZBX	None
	Zabbix server	Items 143	Triggers 78	Graphs 26	Discovery 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None

Agente en Windows

Para monitorear un equipo con Windows, se puede descargar el agente Zabbix dese la web oficial.

Una vez instalado, el servicio comenzará a ejecutarse y recopilará información para transmitirla al servidor (de forma activa o pasiva).

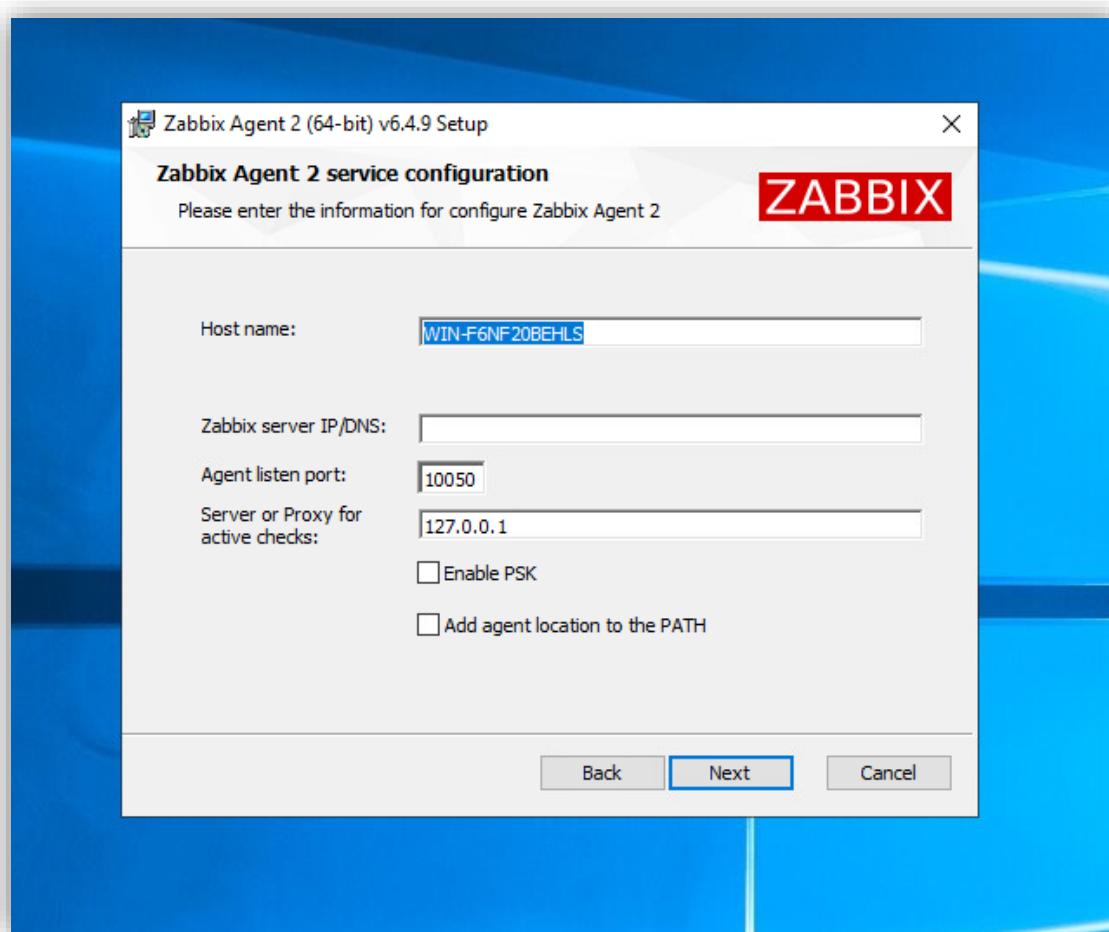
Download pre-compiled Zabbix agent binaries

For Agent DEBs and RPMs please visit [Zabbix packages](#)

Show legacy downloads



OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	6.4	OpenSSL	MSI
Linux		i386	6.2	No encryption	Archive
macOS			6.0 LTS		



Desde Windows se puede modificar el funcionamiento del agente de modo pasivo a activo.

```
#           ServerActive=zabbix.cluster.node1;zabbix.cluster.n
#
# Mandatory: no
# Default:
# ServerActive=
#
ServerActive=172.16.0.101
#
### Option: Hostname
#      List of comma delimited unique, case sensitive hostnames.
#      Required for active checks and monitoring hosts
```

Desde la interfaz WEB se agrega un nuevo host, se agrega el template y la interfaz de monitoreo.

The screenshot shows the Zabbix web interface with several sections:

- Hosts** list: Shows two hosts: "WIN-F6NF20BEHLS" (Windows) and "Zabbix server" (Linux). Each host has a status bar indicating items, triggers, graphs, discovery, and web interfaces.
- Host availability**: A summary bar showing 2 Available, 0 Not available, 0 Unknown, and a total of 2.
- Problems by severity**: A bar chart showing 0 Disaster, 0 High, 1 Average, 1 Warning, 0 Information, and 0 Not classified.
- Current problems**: A table listing three current problems. The first problem is "Windows: High swap space usage (less than 20% free)" for host "WIN-F6NF20BEHLS" at 16:30:19. The second problem is "Linux: High memory utilization (>90% for 5m)" for host "Zabbix server" at 14:54:04.

Integraciones/templates



[Watch Zabbix demo video](#)



FEATURES

Explore how Zabbix collects, processes, and visualizes data



INTEGRACIONES

See the list of monitoring templates and integrations



DOCUMENTACIÓN

Official manuals on how to install, configure, and run Zabbix

El uso de templates es una forma de reducir los tiempos de configuración a la hora de monitorear un host.

Existen plantillas preconfiguradas que incluyen:

- Ítems (elementos a monitorear).
- Triggers (alertas).
- Dashboards.
- Reglas de descubrimiento.

Es posible integrar Zabbix con la mayoría de servicios/sistemas más utilizados a nivel infraestructura.

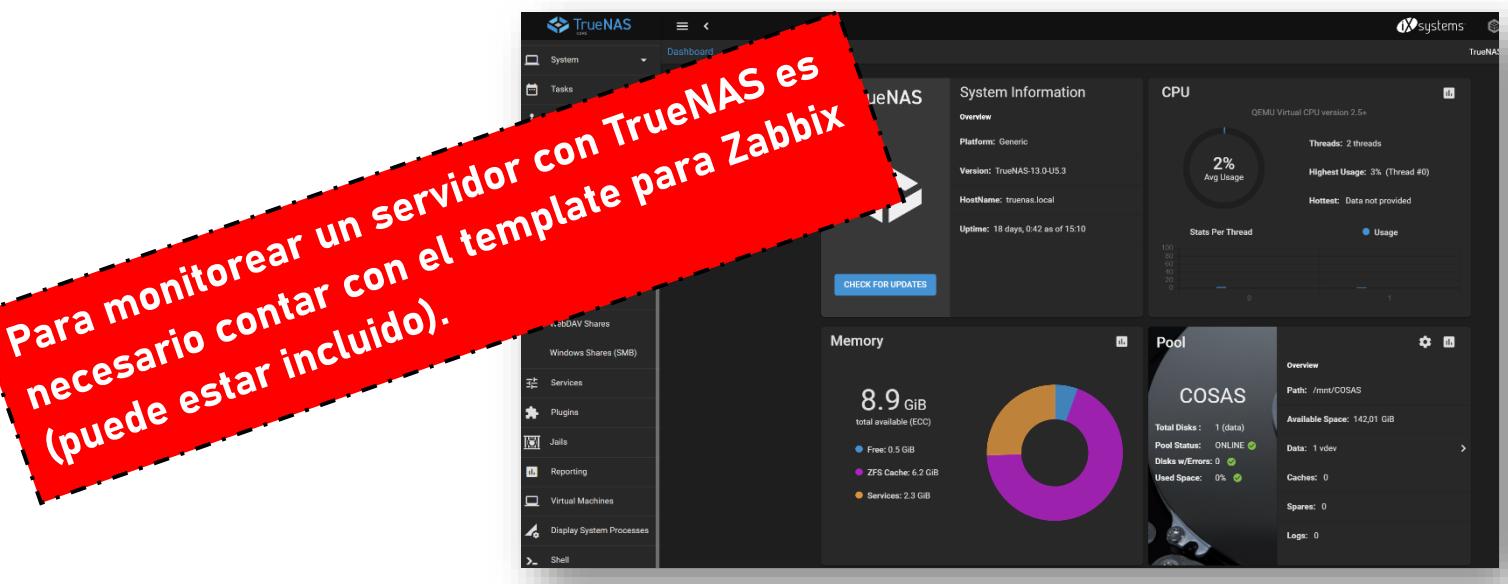
[Zabbix Integrations and Templates](#)



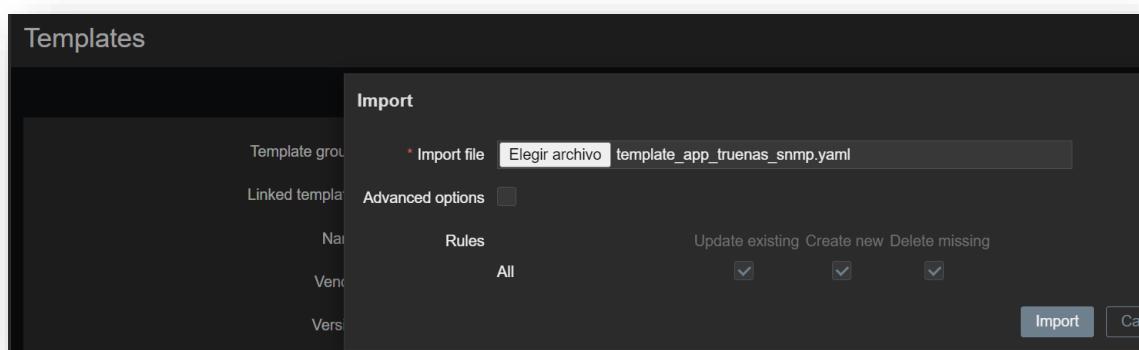
TrueNAS (integración con Zabbix)

Sistema operativo gratuito y open-source que proporciona servicios de almacenamiento en red (NAS).

Permite gestionar arreglos de discos (RAID) y compartir almacenamiento a toda la red mediante varios protocolos (SMB, NFS, FTP, entre otros).



Data Collection/templates (importar template en Zabbix).



Activar **SNMP** en TrueNAS.



En Zabbix damos de alta un nuevo host, utilizando el template correspondiente y seleccionamos la interfaz SNMP.

Debemos indicar la IP y los datos de conexión que establecimos desde TrueNAS.

* Host name

Visible name

Templates

Host groups

Interfaces

192.168.1.200 Remove

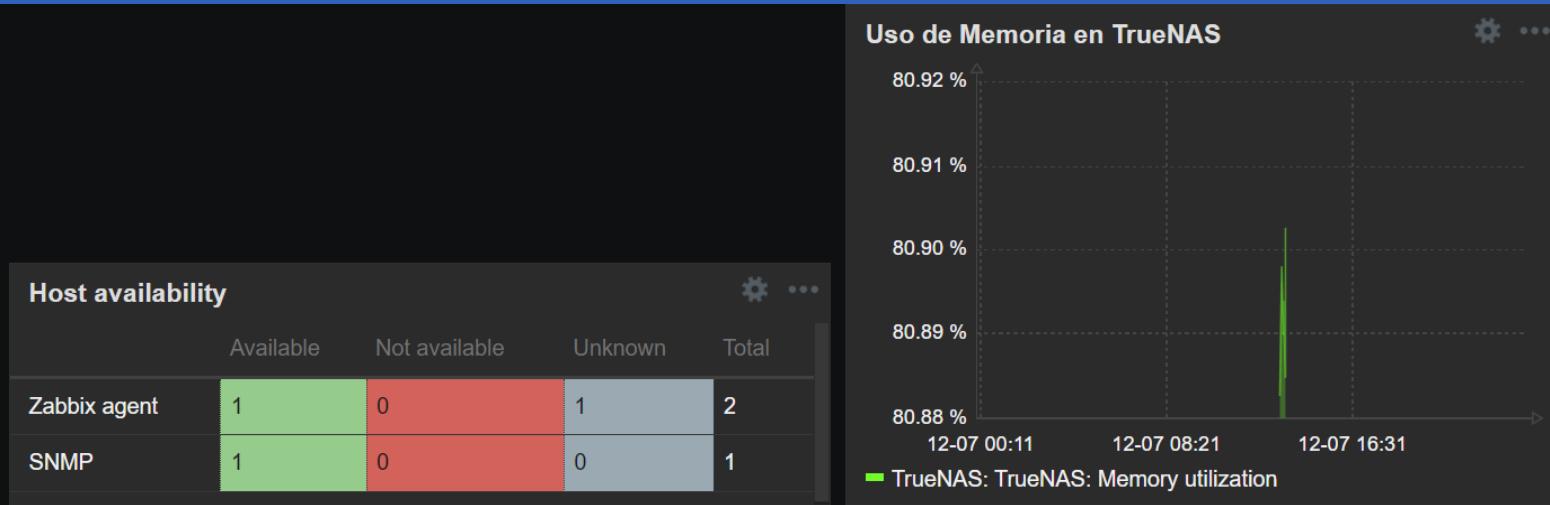
* SNMP version

* SNMP community

Max repetition count Use combined requests

Luego de unos segundos deberíamos tener la información de Zabbix lista para presentarse en el dashboard.

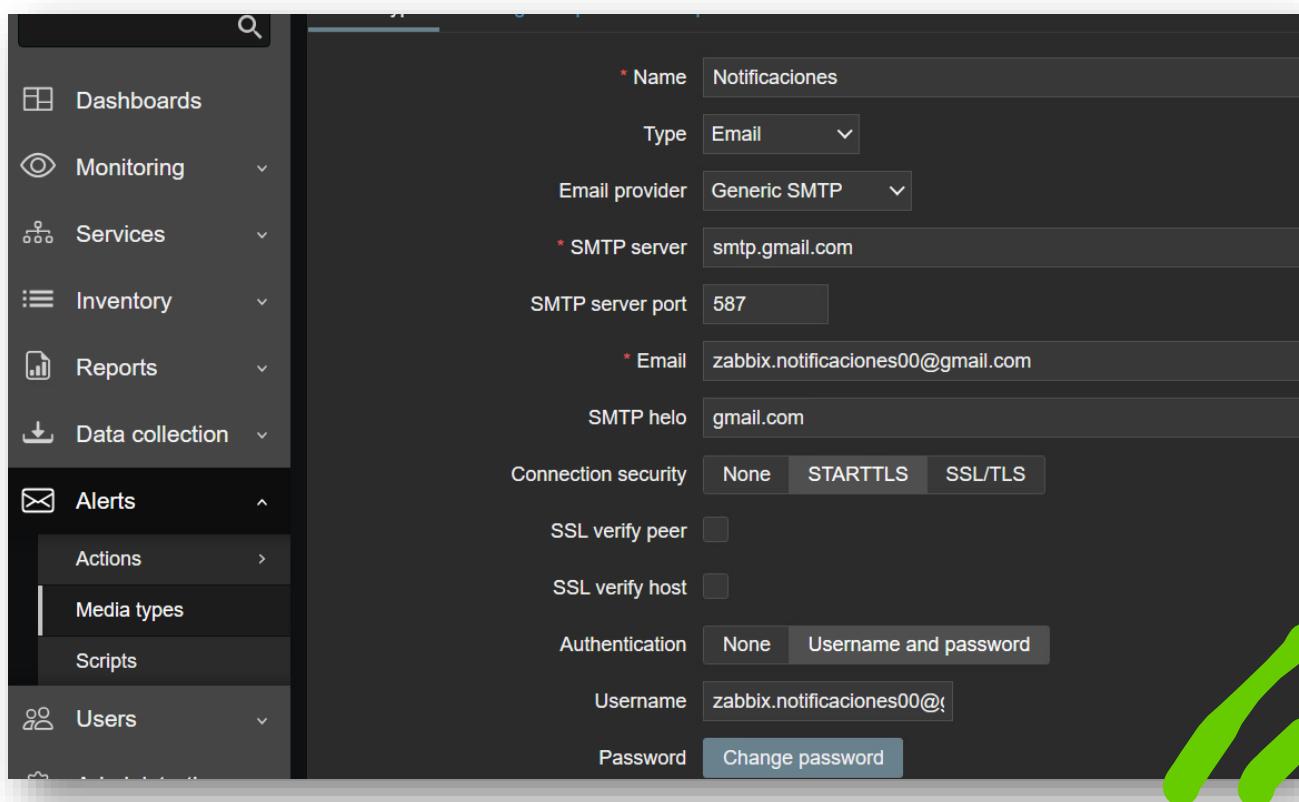
Siempre se puede comprobar que la información se está obteniendo correctamente desde el menú lateral *Monitoring/Latest Data*.



Enviar alertas (media types)

Se pueden configurar notificaciones por diferentes medios, según sucedan eventos críticos en los equipos monitoreados

Los medios de comunicación pueden ser correo electrónico, varios sistemas de gestión de tickets, SMS, Telegram, etc.



← Contraseñas de aplicaciones

Las contraseñas de la aplicación te permiten acceder a tu Cuenta de Google en apps y servicios más antiguos que no son compatibles con los estándares de seguridad modernos.

Las contraseñas de la aplicación son menos seguras que usar apps y servicios actualizados que cuentan con estándares de seguridad modernos. Antes de crear una contraseña de la aplicación, debes verificar si la app la necesita para acceder.

En el caso de GMAIL es necesario configurar contraseñas para aplicaciones para recibir los correos automáticos de Zabbix

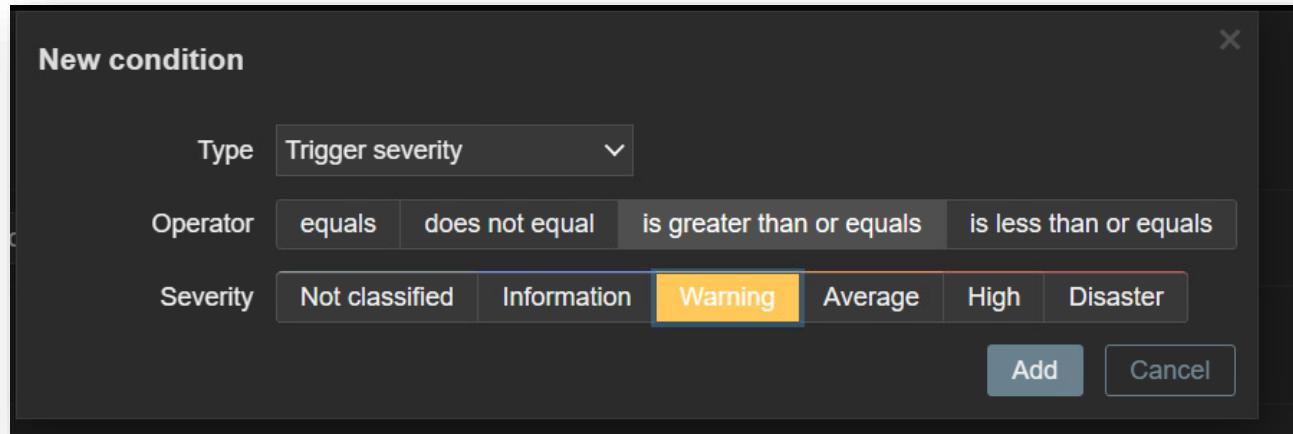
mación

contraseñas de la aplicación.

To create a new app specific password, type a name for it below...

App name

Alerts/Actions -> Se pueden configurar las notificaciones por diferentes medios al activarse un trigger determinado (el medio se debe especificar para cada usuario).



Problem • Severity

ICMP: Unavailable by ICMP ping

Windows: High swap space usage (less than 20% free)

Linux: High memory utilization (>90% for 5m)

Actions		Actions			
Time	User/Recipient	Action	Message/Command	Status	Info
2023-12-07 22:17:35	Admin (Zabbix Administrator)	Notificaciones		Sent	
2023-12-07 22:17:31					

Monitoreo de ESXI con Zabbix

Modificar en Zabbix el archivo /etc/zabbix/zabbix_server.conf

StartVMwareCollectors

VMwareCacheSize

VMwareTimeout

*Se deben descomentar y configurar estas
líneas; posteriormente reiniciar el servicio
de zabbix.*

```
#  
# Mandatory: no  
# Range: 0-250  
# Default:  
StartVMwareCollectors=5  
  
### Option: VMwareFrequency  
#           How often Zabbix will connect to VMware ser  
# Range: 10-86400  
# Default:  
# VMwareFrequency=60  
#           How often Zabbix will connect to VMware ser  
# Mandatory: no  
# Range: 10-86400  
# Default:  
# VMwarePerfFrequency=60  
### Option: VMwareCacheSize  
#           Size of VMware cache, in bytes.  
#           Shared memory size for storing VMware data.  
#           Only used if VMware collectors are started.  
# Mandatory: no  
# Range: 256K-2G  
# Default:  
VMwareCacheSize=32M
```

Es necesario obtener el **UUID** del host ESXI

<https://<IP del ESXI>/mob/?moid=ha-host&doPath=hardware.systemInfo>

Se da de alta el host normalmente utilizando el **template VMware Hypervisor** y se configuran los datos de acceso en el apartado de macros (agregando el UUID en caso de que no exista).

Macro	Value	Action
{\$VMWARE.HV.UUID}	6503a9af-05a6-453f-3ff8-000c29e9918a	T
{\$VMWARE.PASSWORD}		T
{\$VMWARE.URL}	https://192.168.1.12/sdk	T
{\$VMWARE.USERNAME}	root	T

Global view

All dashboards / Global view



Page 1 ...

Top hosts by CPU utilization

	Utilization	1m avg	5m avg	15m avg	Processes	
Zabbix server		1.61 %	0.08	0.13	0.20	270

6.01 ↑

Zabbix server
Values per second

Host availability

	Available	Not available	Unknown	Total
Zabbix agent	1	0	2	3
SNMP	1	0	0	1

Problems by severity



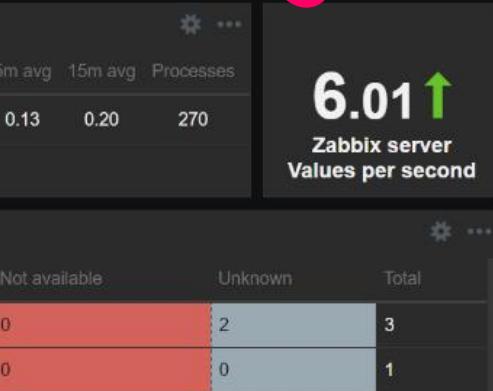
Problems

Time	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Action
15:05:04	•	PROBLEM		Zabbix server	Linux: High memory utilization (>90% for 5m)	9m 49s	Update	• ↗

?

Save changes

Cancel



System information

Parameter	Value	Details
Number of items (enabled/disabled/not supported)	438	428 / 0 / 10
Number of triggers (enabled/disabled [problem(ok)])	219	219 / 0 [1 / 218]
Number of users (online)	2	1
Required server performance, new values per second	5.97	
High availability cluster	Disabled	

15:26

Montevideo

