

PROYECTO DE SEGURIDAD Y ALTA DISPONIBILIDAD

ICA0-PRJ03|01



Paula Dolado, Miquel Romero y Iago Cabello

Bloque 0 Plan y Corporación	3
0.1Descripción del equipo.....	3
0.2Descripción de la empresa	3
0.3 Inventario del material.....	5
Bloque 1 Recursos	7
1.1Esquema teórico	7
1.2 Esquema físico.....	8
1.3 Plan de direccionamiento.....	9
1.4 Etiquetaje del sistema	11
Bloque 2 Intranet.....	12
2.1 Infraestructura	12
Configuración Switches	12
Instalación ESXI	14
vCenter	15
Configuración red VM	16
NAS	19
Zabbix	19
Grafana.....	22
Active Directory y Powershell	24
Bloque 3 DMZ	47
3.1 Infraestructura	47
DNS.....	47
Moodle	49
Ldap	52
Odoo.....	57
Bloque 4 Firewall frontal	59
Router Frontal	59
Router PfSense	63
Reglas del firewall y redireccionamiento	66
VPN	67
Proxy.....	70
Bloque 5 Clúster	75
5.1 Infraestructura	75
NFS.....	75
iSCSI	77
vMotion	79

HA.....	80
Bloque 6 Análisis de riesgos	81
Política de backup	81
Plan de emergencia.....	83

Bloque 0 | Plan y Corporación

0.1Descripción del equipo

Quiénes somos

Somos una empresa joven con 4 años en el sector, nuestros orígenes empezaron cuando queríamos plasmar nuestras capacidades aprendidas pero debido a la poca aceptación al mercado laboral de los jóvenes decidimos empezar un nuevo proyecto con el cual pueda tener un flujo de trabajo moderno con nuevas ideas y los últimos conocimientos.

Nuestra empresa experimentó un crecimiento exponencial a raíz de la pandemia con el teletrabajo y la importancia de las nuevas tecnologías como escritorios remotos o VPN internas, la cual han llegado para quedarse demostrando una relación con el aumento de productividad y reduciendo la emisión de CO2 al reducir los desplazamientos.

También estamos formados en las últimas tecnologías para poder ofrecerlas como: Minado de criptomonedas ético, Metaverso, realidad virtual e Inteligencia Artificial.

Somos partners Golden con Microsoft, VMware y Veeam backup.

CEO Paula



Vicepresidente Iago



Supervisor Miquel



0.2Descripción de la empresa



Nuestra empresa

Somos una empresa de servicios tecnológicos, ofrecemos servicios relacionados con la tecnología a nuestros clientes. Estos servicios pueden incluir:

Una empresa de servicios tecnológicos puede desempeñar varias funciones para sus clientes, algunas de las cuales incluyen:

1. Desarrollo de software: Crear y desarrollar programas y aplicaciones para satisfacer las necesidades específicas de los clientes.
2. Consultoría en tecnología: Proporcionar asesoramiento y recomendaciones a los clientes para ayudarles a tomar decisiones informadas sobre cómo utilizar la tecnología para mejorar sus negocios.
3. Implementación de sistemas: Instalar y configurar sistemas y aplicaciones en las instalaciones de los clientes para garantizar que funcionen correctamente.
4. Mantenimiento y soporte técnico: Proporcionar servicios de mantenimiento y soporte técnico para asegurar que los sistemas y aplicaciones funcionen correctamente y para resolver problemas técnicos cuando surjan.
5. Seguridad de la información: Proteger los sistemas y la información de los clientes contra posibles amenazas de seguridad, como el hacking o el robo de datos.
6. Servicios de nube: Ayudar a los clientes a adoptar y gestionar servicios en la nube, como el almacenamiento y la gestión de bases de datos, el análisis de datos y la inteligencia artificial.
7. Servicios de inteligencia artificial: Proporcionar servicios y soluciones de inteligencia artificial para mejorar la productividad y la eficiencia de los clientes.
8. Servicios de IoT : Proporcionar servicios y soluciones de IoT para mejorar la eficiencia en la empresa, automatizando procesos y obteniendo datos valiosos para la toma de decisiones.

Estas empresas pueden trabajar con diferentes tipos de tecnologías y en diferentes industrias.

Qué ofrecemos

Pim Pam Services es una empresa dedicada al sector de administración de redes donde nos encargamos de proporcionar soluciones para su gestión.

Establecimientos básicos.

- Configuración de redes: Diseñaremos e configuraremos tus Vlans para estabilizar y garantizar la disponibilidad.
- Alta Disponibilidad: Implementación de sistemas que permiten un uso sin cortes donde se focaliza que el usuario sufra el menor corta tiempo.
- VMware: Instalamos e configuramos sistemas informáticos virtuales basados en la tecnología VMware.
- Redes Wifi: Wifi para las oficinas, escuelas y eventos de multitud.

Mantenimiento y seguridad del sistema informático.

- Zabbix: Instalamos e configuramos sistemas de monitorización Cloud basados en la tecnología Zabbix.
- Seguridad Perimetral: Diseñaremos e implementaremos sistemas de seguridad perimetral e firewalls para tu empresa.
- Copias de Seguridad: Diseñaremos e configuraremos soluciones de copias de seguridad adaptando la tecnología a las necesidades para que su monitorización sea continua.
- DevSecOps: Integraremos la seguridad compartida para la seguridad en las aplicaciones mediante basados en la tecnología DevSecOps.

- Owasp zap: Escaneos de seguridad web y prueba de penetración pasiva basado en la tecnología Owasp zap.

Organización del lugar de trabajo.

- Tecnología Microsoft: Diseñaremos e implementaremos directorios activos, Microsoft Exchange, sincronización activa, Microsoft SQL i servicios WSUS.
- VPN IPsec y SSL: Configuraremos conexiones virtuales privadas para múltiples servicios i recursos.
- Migración de servidores: Migraremos servidores Microsoft

Suministro informático.

En primer lugar, ofrecemos productos de alta calidad con características avanzadas que pueden ayudar a mejorar la eficiencia y productividad de su negocio. También ofrecemos un estudio para determinar el material más adecuado con precios competitivos, opciones de servicio y soporte.

Además, nuestro equipo de atención al cliente está altamente capacitado y siempre dispuesto a ayudarlo con cualquier pregunta o problema que pueda tener.

- Financiación

Ofrecemos la posibilidad de financiamiento que se adaptan a sus necesidades y presupuesto. Esto le permite obtener los productos y servicios que necesita para su negocio sin tener que preocuparse por desembolsar un gran pago inicial.

Le generamos un contrato en menos de 24h y no supone ningún coste es estudio o la apertura de la acción.

Contacta con nosotros

C/ Passeig de Sant Joan Bosco, 42
08017 Barcelona

Tel: [93 266 88 23](tel:932668823)

Email: soporte@pimpam.com

Web: pimpam.com

0.3 Inventario del material

Nombre	ESXI 1
Modelo	HPe ProLiant ML30 Gen10
CPU	Intel Xeon E-2224 4 nucleos
Ram	Dual channel 16GB ram ddr4
Disco	240 GB SSD Kingston
Chipset placa base	Intel C246
Formato de placa	ATX
Socket	LGA 1151 (Zocalo H4)
N* tarjetas de red	2
N* de USB	6

Nombre	ESXI 2
Modelo	Dell optiplex 3020
CPU	Intel i5-4590 4 núcleos 3.30 GHz
Ram	Dual channel 16GB ram DDR3
Disco	500 GB HDD Seagate 7200 RP
Chipset placa base	H81
Formato de placa	ATX
Socket	LGA1150
N* tarjetas de red	3
N* de USB	8

Nombre	ESXI 3
Modelo	Dell optiplex 3020
CPU	Intel i5-4590 4 nucleos 3.30 GHz
Ram	Dual channel 16GB ram ddr3
Disco	500 GB HDD Seagate 7200 RP
Chipset placa base	H81
Formato de placa	ATX
Socket	LGA1150
N* tarjetas de red	3
N* de USB	8

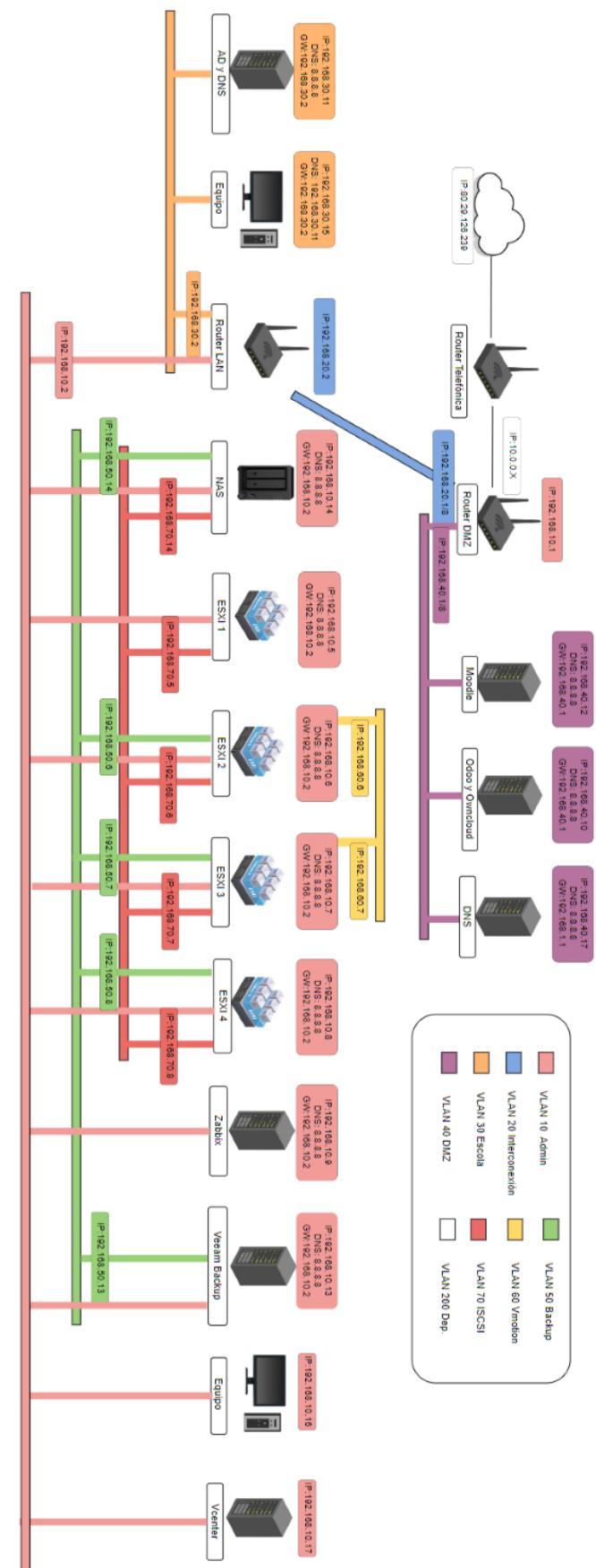
Nombre	ESXI 4
Modelo	Dell optiplex 3020
CPU	Intel i5-4590 4 nucleos 3.30 GHz
Ram	12GB ram ddr4
Disco	500 GB HDD Seagate 7200 RP 3'5
Chipset placa base	H81
Formato de placa	ATX
Socket	LGA1150
N* tarjetas de red	2
N* de USB	8

Nombre	NAS
Modelo	ProLiant MicroServer Gen10
CPU	AMD Opteron X3216 2 nucleos
Ram	8 GB DDR4
Disco	240 GB SSD Kingston 2 x 2TB HDD Seagate 7200 RPM
Formato de placa	MATX
Socket	LGA1150
N* tarjetas de red	2
N* de USB	6

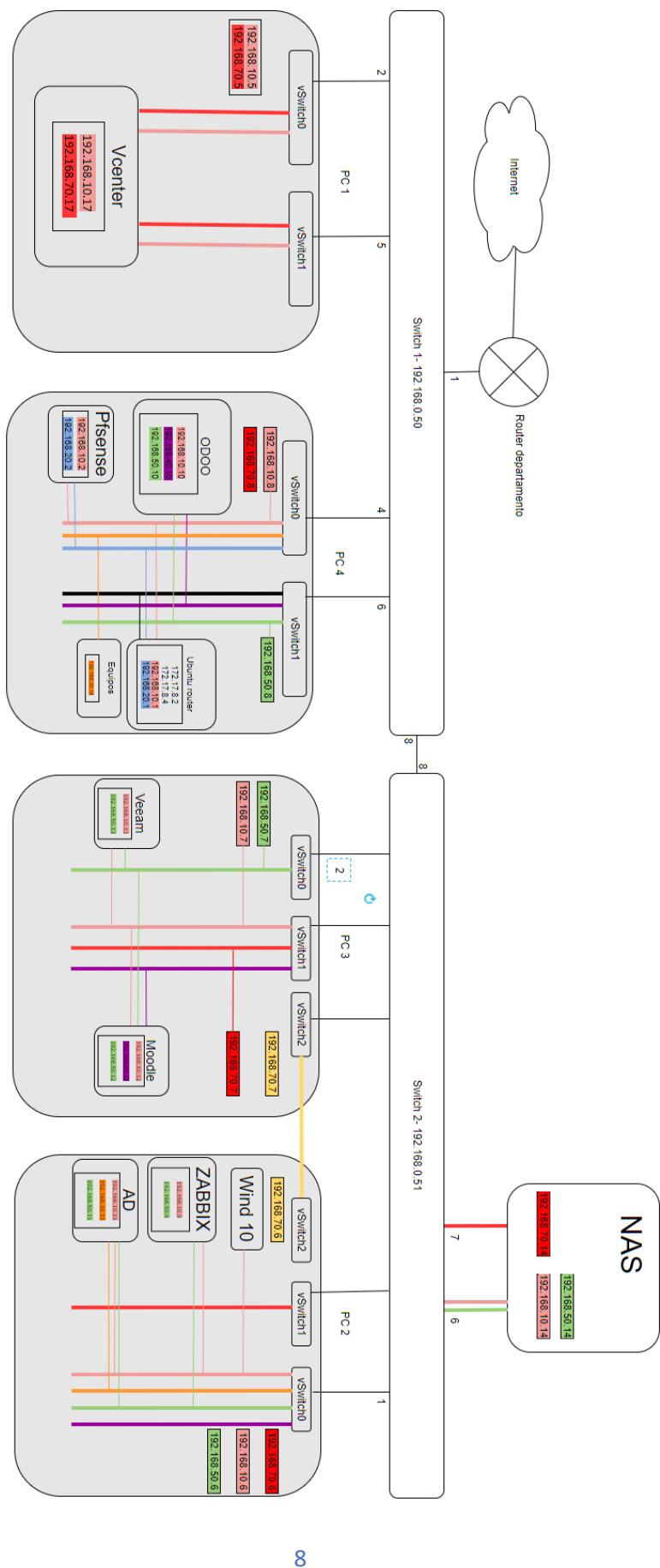
Periféricos
Teclado Dell KB216P
2 ratones Dell
2 monitores DELL E2014H 19'5 pulgadas

Bloque 1 | Recursos

1.1 Esquema teórico



1.2 Esquema físico



1.3 Plan de direccionamiento

En primer lugar, establecimos como equipo los dispositivos que son necesarios para nuestra red ya sean servidores y equipos como routers y switches. A raíz de eso nos planificamos como segmentar dichos dispositivos de manera que nuestra red se mostrase con cierto orden y funcionalidad.

Para optimizar lo máximo según su funcionalidad creamos las siguientes Vlans. Creamos 2 segmentaciones para realizar conexiones a todos los dispositivos necesarios de administración, la vlan1 (default) para la manipulación de los switches y la vlan10 (Admin) para configurar todos los equipos administrables.

Seguidamente, dividimos la red en 4 zonas compuestas por vlan30 (Escola) con la función de albergar el Directorio Activo además de los equipos de alumnos y profesores, vlan40 (DMZ) es aquel espacio administrativo que comporta un funcionamiento principalmente de servicios públicos como el odoo y Moodle. La vlan20 (Interconexión) se encarga de enlazar mediante los dos routers la zona DMZ con la zona de Escuela y la ya comentada Vlan de Administración que compondrá la zona final con el clúster y resto de servidores.

A continuación, el reparto de direcciones ip para las Vlans.

VLANS	NUM. VLAN	RANGO IP	GATEWAY
Default (Administración switches)	1	192.168.1.0 - 192.168.1.254	
Administración	10	192.168.10.0 - 192.168.10.254	192.168.10.2
Interconexión	20	192.168.10.0 - 192.168.10.254	192.168.20.1
Escuela	30	192.168.30.0 - 192.168.30.254	192.168.30.1
DMZ	40	192.168.40.0 - 192.168.40.254	192.168.40.1
Backup	50	192.168.50.0 - 192.168.50.254	192.168.50.1
Vmotion	60	192.168.60.0 - 192.168.60.254	
iSCSI	70	192.168.70.0 - 192.168.70.254	
Departamento	100	172.17.0.0 - 172.17.254.254	172.17.0.100

Para que no quiera lugar a duda, tenemos dos vlans de administración debido a que los switches que utilizamos no pueden ser controlados desde la vlan 10 planeada, frente a esta incidencia elegimos utilizar la vlan por defecto para controlar solo dichos dispositivos y mantener máquinas virtuales en la vlan 10.

Cambios en la práctica

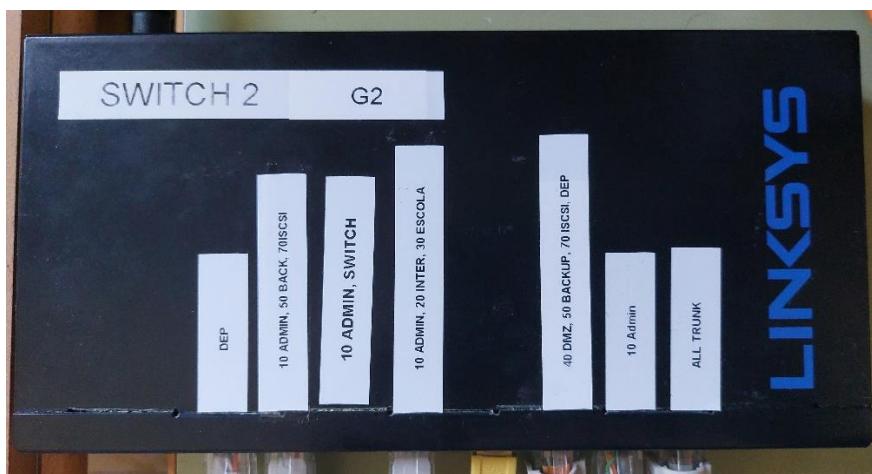
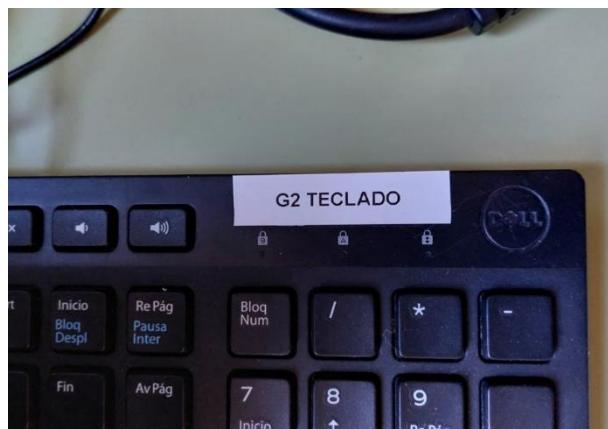
Al principio, planeamos repartir direcciones del rango de IP de clase B para tener un rango de IP más elevado, pero como la red privada (172.17.0.0) no nos dejaba configurar una IP con el mínimo número que la VLAN, pero nos hemos terminado decidiendo por una clase A. De esta manera la distribución se ve más visual con las VLAN asignada y están todas las IP en el mismo tramo de red y se ve más visualmente.

Por otro lado, teniendo en cuenta en qué departamento debe pertenecer cada dispositivo les hemos asignado direcciones ip fijas dentro del rango de la vlan correspondiente. A más a más, tienen a su lado de las cuales serán participes donde tendrán la misma nomenclatura.

DISPOSITIVO	VLAN CONECTADAS	DIRECCIONES IP
ROUTER EXTERNO	100	172.17.8.2 172.17.8.4
ROUTER DMZ	10, 20 40	192.168.10.1 192.168.20.1 192.168.40.1
SWITCH 1	1	192.168.0.50
ROUTER LAN	10 20 30	192.168.10.2 192.168.20.2 192.168.40.2
SWITCH 2	1	192.168.0.51
NAS	10 50 70	192.168.10.14 192.168.50.14 192.168.70.14
ESXI 1	10 70	192.168.10.5 192.168.70.5
ESXI 2	10 50 70	192.168.10.6 192.168.50.6 192.168.70.6
ESXI 3	10 50 70	192.168.10.7 192.168.50.7 192.168.70.7
ESXI 4	10, 50 70	192.168.10.8 192.168.50.8 192.168.70.8
ZABBIX	10 50	192.168.10.9 192.168.50.9
ODOO Y OWN CLOUD	10 40 50	192.168.10.10 192.168.40.10 192.168.50.10
AD Y DNS	10 30 50	192.168.10.11 192.168.30.11 192.168.50.11
MOODLE	10 40 50	192.168.10.12 192.168.40.12 192.168.50.12
VEEAM BACKUP	10 50	192.168.10.13 192.168.50.13
NAS	10 50 70	192.168.10.14 192.168.50.14 192.168.70.14
EQUIPO WIN	10 30	192.168.10.15 192.168.30.15
EQUIPO VPN	10	192.168.10.16

VCENTER	10 70	192.168.10.17 192.168.70.17
DNS	10 40	192.168.10.18 192.168.40.18

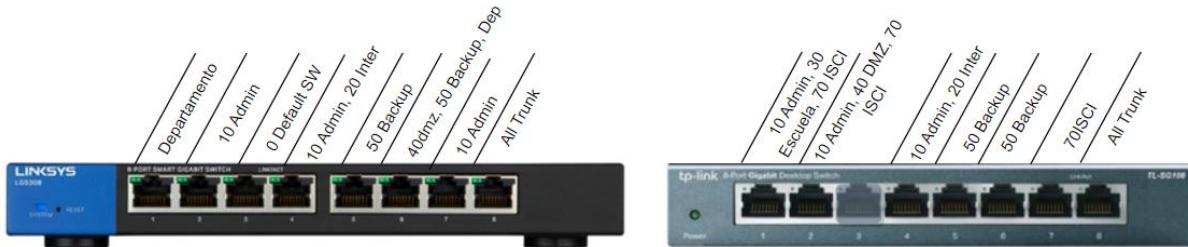
1.4 Etiquetaje del sistema



Bloque 2 | Intranet

2.1 Infraestructura

Antes de empezar la configuración realizamos un pequeño esquema de las vlans que transcurrirán por cada puerto. El diseño realizado es el siguiente.



En primer lugar, hemos realizado esta organización teniendo en cuenta las maquinas que estarán conectadas. En el caso del Switch Linksys también tiene el conector del departamento, haciendo así el primer puerto. Para el ESXI 1 haremos uso únicamente de una de dos tarjetas de red que tiene construyendo un puerto con la vlan de admin e iSCSI.

Por otro lado, la distribución del ESXI 2 y el ESXI 3 será idéntica. Así mismo, durante la migración entre los nodos en caso de necesitarse encontrara sin problemas las redes a las que se conectan al estar clonado. Siendo la primera tarjeta de red por la que pasaran todas las vlans, la segunda tarjeta se ocupará del iSCSI y finalmente tendremos un cable cruzado entre ambos dispositivos que se encargara de la vMotion.

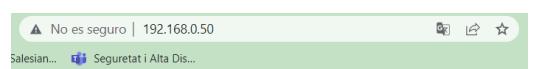
Para terminar la configuración de los switches en ESXI 4 utilizara dos tarjetas de red, una dedicada a Administración e interconexión y la otra a DMZ, Backup y el departamento.

Configuración Switches

Switch 1

Para empezar con la configuración deberemos conectarlos directamente al switch en cuestión a través de la dirección ip por defecto. Para crear las vlans indicaremos un número y nombre para después seleccionar en los puertos que irán etiquetados o sin etiquetar.

Este etiquetaje nos indicara si en ese mismo puerto transcurre más de una vlan, puerto troncal, deberá de llevar una etiqueta en el paquete enviado para que el próximo dispositivo sepa hacia donde se dirige y de donde proviene para enviar la respuesta. Si ese puerto del switch solo es utilizado por una única vlan le diremos que el puerto es de acceso y por lo tanto no llevara una etiqueta que lo identifique puesto a que no es necesario si todo lo que enviara o recibirá será él.



Copyright © 2016 TP-LINK Technologies Co., Ltd.
All rights reserved

Configuraremos los puertos siguientes para establecer las conexiones con los ESXI.

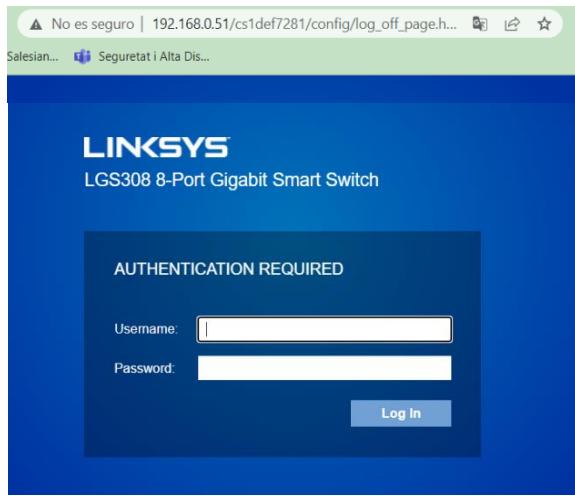
VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1	Default_VLAN	1-8		1-8	<input type="checkbox"/>
10	Admin	1-2,6,8	1-2,6,8		<input type="checkbox"/>
20	Intercon	8	8		<input type="checkbox"/>
30	Escuela	1-2,8	1-2,8		<input type="checkbox"/>
40	DMZ	1-2,8	1-2,8		<input type="checkbox"/>
50	Backup	1-2,6,8	1-2,6,8		<input type="checkbox"/>
60	Vmotion	8	8		<input type="checkbox"/>
70	ISCSI	3-5,7-8	8	3-5,7	<input type="checkbox"/>

Seguidamente, para los puertos que estarán en modo de acceso deberemos indicarle un PIV, esto hace referencia al número de la vlan que trascurrirá, en caso de los puertos trúncales haremos uso de la nomenclatura del puerto por defecto en el dispositivo, el 1.

Finalmente, para rematar la configuración le indicaremos la dirección ip y mascara que le corresponde (192.168.0.50 y 255.255.255.0) además de cambiar las credenciales por defecto a unas personalizadas para un mínimo de seguridad.

Select	Port	PVID
<input type="checkbox"/>		
<input type="checkbox"/>	Port 1	1
<input type="checkbox"/>	Port 2	1
<input type="checkbox"/>	Port 3	70
<input type="checkbox"/>	Port 4	70
<input type="checkbox"/>	Port 5	10
<input type="checkbox"/>	Port 6	1
<input type="checkbox"/>	Port 7	70
<input type="checkbox"/>	Port 8	1

Switch 2



Para nuestro segundo dispositivo haremos los mismos pasos que con el anterior salvo que algún método es diferente. Por ejemplo, la asignación a los puertos se mostrará con otro formato donde indicaremos los puertos que serán destinados a un troncal y los de acceso con las vlans pertenecientes.

Una vez son repartidas en otra interfaz de la consola web podremos ver que por defecto son marcadas todos los puertos como troncales. Deberemos seleccionar el puerto de acceso y cambiar el modo al correspondiente.

	Interface	Interface VLAN Mode	PVID	Acceptable Frame Type	Ingress Filtering	Administrative VLAN Memberships
<input type="radio"/>	GE1	Access	200	Admit All	Enabled	200UP
<input type="radio"/>	GE2	Trunk	1	Admit All	Enabled	1UP, 10T, 50T, 70T
<input type="radio"/>	GE3	Trunk	1	Admit All	Enabled	1UP, 10T
<input type="radio"/>	GE4	Trunk	1	Admit All	Enabled	1UP, 10T, 20T, 30T
<input type="radio"/>	GE5	Access	40	Admit All	Enabled	40UP
<input type="radio"/>	GE6	Trunk	1	Admit All	Enabled	1UP, 40T, 50T, 70T, 200T
<input type="radio"/>	GE7	Access	10	Admit All	Enabled	10UP
<input type="radio"/>	GE8	Trunk	1	Admit All	Enabled	1UP, 10T, 20T, 30T, 40T, 50T, 70T, 200T

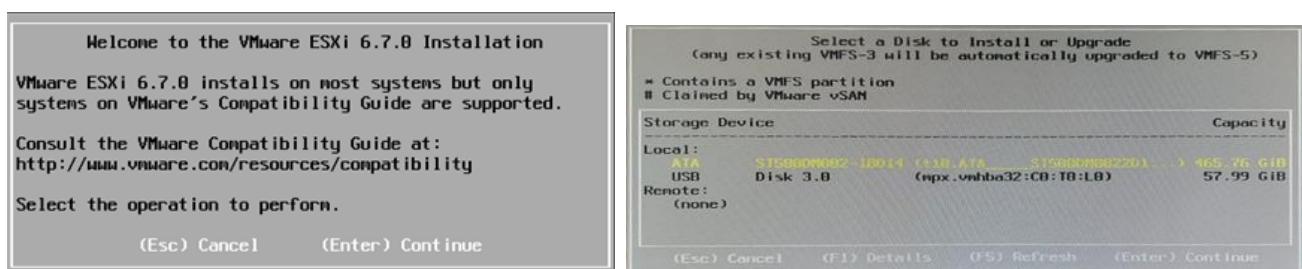
Instalación ESXI

Antes de iniciar con la instalación¹ comprobaremos en primer lugar sus requisitos y elegiremos en que ESXI lo querremos mantener. Se alojará en la primera máquina debido a que tiene la mayor cantidad de memoria.

Empezaremos visitando la web oficial, descargando la imagen iso que más nos interesa para nuestro rendimiento (versión 6.7).



Una vez listo procederemos a aceptar el acuerdo de licencias, seleccionaremos el disco en el cual queremos instalarlo.



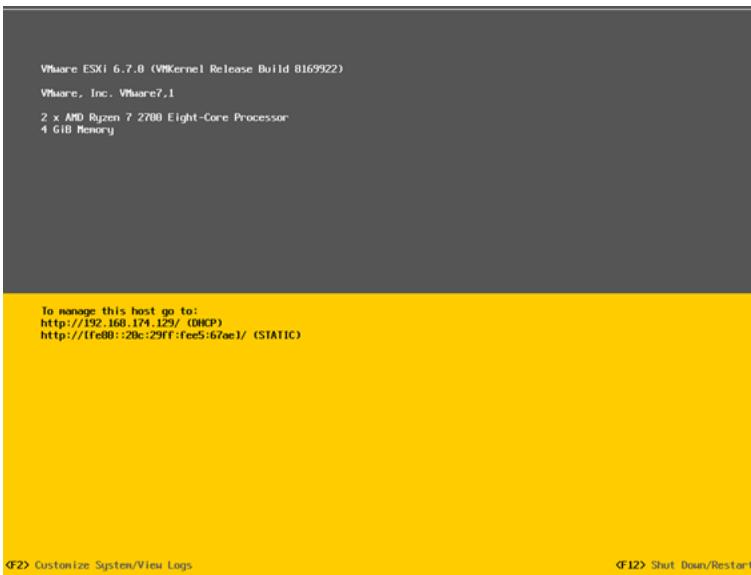
A continuación, habrá que configurar datos como el idioma del teclado, la contraseña para el super usuario root hasta confirmar la instalación con F11.



Cuando haya finalizado el proceso, tras reiniciarse la máquina, quitaremos la iso y estableceremos la dirección ip y la vlan en la que se etiqueta a través del botón F2.

¹ <https://alexariza.net/tutorial/como-instalar-vmware-esxi/>

Finalmente, ya podremos acceder al ESXI vía web.



vCenter

Para instalar el Vcenter² necesitaremos ejecutar el instalador en nuestra propia máquina, seleccionar la opción de instalar y rellenar la información necesaria de los ajustes de host, es decir, indicar la dirección ip del servidor del cual proviene junto a sus credenciales de acceso. Seguidamente, indicaremos el nombre de la máquina virtual y contraseña.

Dependiendo de los requisitos mostrados indicaremos cual es el espacio al que deseamos recurrir teniendo en cuenta nuestras especificaciones, en este caso se trataría de uno tiny.

Deployment size	Tiny				
Storage size	Default				
Resources required for different deployment sizes					
Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	12	415	10	100
Small	4	19	480	100	1000
Medium	8	28	700	400	4000
Large	16	37	1065	1000	10000
X-Large	24	56	1805	2000	35000

Continuando con el almacenamiento asignaremos la base de datos accesible por la máquina.

Hay que activar la opción de enable thin disk. De esta manera, ESXI aprovisiona todo el espacio necesario para las actividades actuales y futuras del disco, por ejemplo, 40 GB. Sin embargo, el disco delgado (thin disk) usa solo el espacio de almacenamiento que necesita el disco para sus operaciones iniciales. Si el disco de aprovisionamiento delgado ocupa solo 20 GB de almacenamiento y requiere más espacio, puede expandirse a los 40 GB de espacio.

² <http://vcloud-lab.com/entries/vcenter-server/how-to-install-vcenter-server-appliance-on-esxi-host>
<https://www.backup.com/enterprise-backup/install-vcenter-server-appliance-on-esxi-host.html>

Install on an existing datastore accessible from the target host

Show only compatible datastores

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
datastore1	VMFS-6	216 GB	214.59 GB	1.41 GB	Supported

1 item

Enable Thin Disk Mode ⓘ

Para acabar con la primera parte de la configuración deberemos indicar los detalles de red con la tarjeta de red por defecto siendo VM Network le pondremos al vcenter su dirección, mascara de red y puerta de enlace. Aunque utilizaremos más adelante un servidor DNS por el momento no lo añadiremos y al momento de su creación ya modificaremos estos ajustes para añadirlo.

En la etapa dos de la configuración del Vcenter se deberá especificar la hora del servidor, indicamos que se sincronice con el host ESXI que le toca y habilitamos el acceso vía SSH.

Además, nos ofrece la posibilidad de SSO, esto trata de una buena opción administrativa que se ocupa de identificarnos una única vez manteniendo la sesión iniciada. El usuario para el SSO será administrator@vsphere.local debido a que todavía no tenemos un DNS, más adelante se actualizará.

Network Details

Network configuration	Assign static IP address
IP version	IPv4
Host name	localhost
IP Address	192.168.10.17
Subnet mask	255.255.255.0
Gateway	192.168.10.1
DNS servers	

vCenter Server Details

Time synchronization mode	Synchronize time with the ESXi host
SSH access	Enabled

SSO Details

Domain name	vsphere.local
User name	administrator

Customer Experience Improvement Program

CEIP setting	Opted in
--------------	----------

Administración de VMware vCenter Server

administrator@vsphere.local

.....

INICIAR SESIÓN

Configuración red VM

Para la configuración de red³ de las máquinas virtuales se deberán tener varios conceptos claros:

- Comutador de kernel:

Un comutador de kernel hace referencia a la tarjeta física del ESXI. Se habrá que establecer la dirección ip además de un pequeño tag para mantener un orden más visual. En el caso del ESXI

³ <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-0BBDC715-2F93-4460-BF07-5778658C66D1.html>

<https://www.josemariagonzalez.es/video-tutoriales-trucos/que-es-un-switch-virtual-y-como-funciona-red-vmware.html>

1 tendrá únicamente el conmutador de Admin mientras que el ESXI 2 tendrá Admin, iSCSI y Backup.

The screenshot shows the configuration for interface vmk0. It includes fields for Group (Admin), MTU (1500), IP Version (IPv4), and a dropdown for IPv4 Configuration (DHCP is off, Estático is selected). Under static configuration, IP Address is set to 192.168.10.7 and Subnet Mask to 255.255.255.0. A stack dropdown is set to 'Pila de TCP/IP predeterminada'. Services section includes checkboxes for vMotion, Provisioning, Fault Tolerance, Administración (which is checked), Replication, and Replication NFC.

The screenshot shows the creation of a standard vSwitch named vSwitch2. It includes fields for MTU (1500) and a dropdown for the upper link (vmnic2 - Inactivo). Advanced sections for bonding detection and security are shown with expandable buttons.

- **Comutador virtual**

Los conmutadores virtuales estarán ligados como vínculo a la tarjeta de red física del equipo y proporciona conectividad de red a las máquinas virtuales. Hace la función de switch virtual.

- **Grupo de Puertos**

Los grupos de puertos son las organizaciones basadas en vlans que se deberán asociar a los conmutadores virtuales para ir más adelante al conmutador de kernel o no, dependiendo de su función para proporcionar la red indicada en ese grupo.

Es decir, dentro del conmutador físico vmk1 establecemos un conmutador virtual llamado vswitch1 y queremos que por ese puerto pase la vlan de Admin por lo que crearemos un grupo de puerto llamado Admin con su nomenclatura (10) y la vincularemos al puerto de kernel.

The screenshot shows the creation of a port group named Admin with VLAN ID 10. It is associated with the vSwitch0 virtual switch. Security settings are also visible.

En cambio, repitiendo el proceso anterior con el grupo de puerto llamado, por ejemplo, Escuela con el id 30 lo asignaremos al adaptador de red de la máquina virtual. De esta manera enlazamos el puerto físico, conmutador de kernel, a través del conmutador virtual al grupo de puertos, estableciendo la conexión de la máquina virtual hasta el exterior.

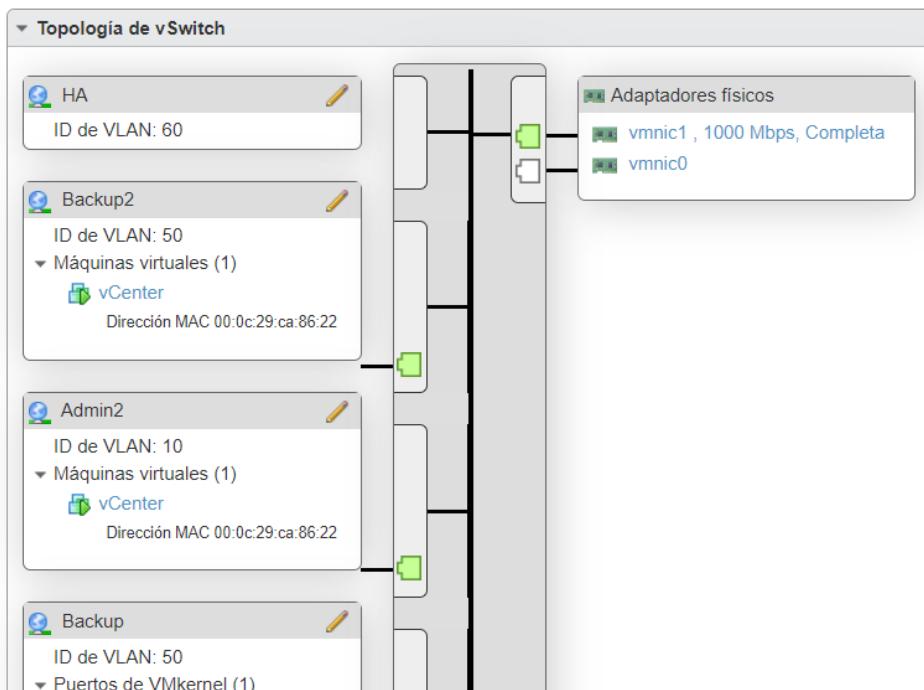
Editar comutador virtual estándar - vSwitch0

Agregar vínculo superior

MTU	1500									
Vínculo superior 1	vmnic0 - Inactivo									
Vínculo superior 2	vmnic1 - Activo, 1000 mbps									
► Detección de vínculos	Haga clic para expandir									
► Seguridad	Haga clic para expandir									
▼ Formación de equipos de NIC										
Equilibrio de carga	Enrutar según el hash de IP									
Detección de conmutación por error de la red	Solo estado de vínculo									
Notificar a comutadores	<input checked="" type="radio"/> Sí <input type="radio"/> No									
Comutación por recuperación	<input checked="" type="radio"/> Sí <input type="radio"/> No									
Orden de conmutación por error	<table border="1"> <thead> <tr> <th>Nombre</th> <th>Velocidad</th> <th>Condición</th> </tr> </thead> <tbody> <tr> <td>vmnic0</td> <td>Vínculo inactivo</td> <td>Activa</td> </tr> <tr> <td>vmnic1</td> <td>1000 Mbps, dúplex c...</td> <td>Activa</td> </tr> </tbody> </table>	Nombre	Velocidad	Condición	vmnic0	Vínculo inactivo	Activa	vmnic1	1000 Mbps, dúplex c...	Activa
Nombre	Velocidad	Condición								
vmnic0	Vínculo inactivo	Activa								
vmnic1	1000 Mbps, dúplex c...	Activa								
► Catalogación de tráfico	Haga clic para expandir									

Como en el ESXI 1 solo nos es necesario una tarjeta de red crearemos una redundancia utilizando la segunda de esta manera se nos permitirá proporcionar otro servidor adicional de forma rápida al momento de ejecución. De esta manera no se detendrá el sistema con el vCenter ya que si cae este perdemos toda la infraestructura del clúster.

Para aplicar esta característica le indicaremos a un mismo switch virtual ambas tarjetas de red.⁴



⁴ <https://www.josemariagonzalez.es/video-tutoriales-trucos/como-redundar-la-red-de-vmware-vsan.html>

NAS

Para nuestro servidor NAS hemos instalado de imagen la versión 22.04 de ubuntu server ya que su función es la de almacenar las copias de seguridad no nos es necesario ningún sistema diferente.

Para que el servidor de discos cumpla su prometido es muy importante que tenga conexión al resto de dispositivos de la red, ESXI, VCenter y máquinas virtuales, para ello hemos establecido el siguiente netplan donde conforme a la configuración de los switches podemos observar que tiene dos puertos de red, uno dedicada a la administración y backup y otro para el iSCSI que ocupa más recursos.

Hay que destacar que la estructura de este netplan se irá repitiendo en todas las máquinas virtuales cambiando las direcciones y las vlans.

```
network:
  version: 2
  ethernets:
    enp2s0f0:
      addresses:
        - 192.168.70.14/24
      gateway4: 192.168.70.1
      nameservers:
        addresses: []
        search: []
    enp2s0f1:
      dhcp4: false
  vlans:
    enp2s0f1.10:
      id: 10
      link: enp2s0f1
      addresses:
        - 192.168.10.14/24
      gateway4: 192.168.10.1
      nameservers:
        addresses: []
        search: []
    enp2s0f1.50:
      id: 50
      link: enp2s0f1
      addresses:
        - 192.168.50.14/24
      gateway4: 192.168.50.1
      nameservers:
        addresses: []
        search: []
```

Zabbix

En primer lugar, crearemos en una máquina virtual un servidor de zabbix en Linux con las instrucciones siguientes:

Descargamos el repositorio oficial.

```
# wget
https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_5.0-1+focal\_all.deb
```

Comprobamos las dependencias y evitaremos instalar paquetes cuyas dependencias no se cumplen.

```
# dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
```

Actualizamos el listado de paquetes e instalamos el servidor, agente, frontend y base de datos de Zabbix.

```
# apt update
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent mysql-server.
```

Accedemos a la base de datos para crear una base de datos y un usuario privilegiado.

```
# mysql -uroot -p
> CREATE DATABASE zabbixdb character set utf8 collate utf8_bin;
> CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'Pimpam683!';
> GRANT ALL PRIVILEGES ON zabbixdb.* TO 'zabbix'@'localhost' WITH
GRANT OPTION;
> FLUSH PRIVILEGES;
```

Para terminar la configuración por comando deberemos editar unos parámetros en los dos archivos siguientes.

```
# nano /etc/zabbix/zabbix_server.conf
```

```
DBName=zabbixdb DBUser=zabbix DBPassword=Pimpam683!
```

```
# nano /etc/zabbix/zabbix_agent.conf

Server=127.0.0.1 Hostname=Zabbix server

# systemctl restart zabbix-server zabbix-agent apache2

# systemctl enable zabbix-server zabbix-agent apache2
```

Importamos la base de datos.

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql
--default-character-set=utf8mb4 -uzabbix -p zabbix
```

Editamos unos parámetros del archivo del apache para cumplir los prerequisitos:

```
#nano /etc/php/8.0/apache2/php.ini
```

Cuando hayamos finalizado nos desplazaremos al navegador a través de la dirección ip del Zabbix (192.168.10.9/zabbix).⁵

Check of pre-requisites

	Current value	Required	
PHP version	7.4.3-4ubuntu2.18	7.2.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	Europe/Madrid		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK

Database type	MySQL
Database server	localhost
Database port	default
Database name	zabbix
Database user	zabbix
Database password	*****
Database TLS encryption	false
Zabbix server	localhost
Zabbix server port	10051
Zabbix server name	

Nos pedirán unos datos básicos sobre la instalación como los datos de la base de datos. Es importante tener en cuenta que zabbix utiliza el puerto 10051 para realizar las conexiones ya que se deberá crear una regla en nuestro firewall.

Para tener solo el servicio de agente en las maquinas Linux no hará falta instalar la base de datos ni el zabbix-server.

⁵ https://www-digitalocean-com.translate.goog/community/tutorials/how-to-install-and-configure-zabbix-to-securely-monitor-remote-servers-on-ubuntu-20-04-es?_x_tr_sl=es&_x_tr_tl=ca&_x_tr_hl=ca&_x_tr_pto=sc&_x_tr_hist=true & <https://www.zabbix.com/la/download>

Por otro lado, aunque ya hemos visto como se agregará por terminal el agente en Zabbix a continuación veremos cómo se agrega por el agente de Windows de manera mucho más sencilla.

En la misma ventana de configuración indicaremos el nombre de la maquina y la dirección del servidor Zabbix.



Para organizar los agentes en la consola crearemos unos grupos de host para categorizar como por ejemplo Servidores Windows, Servidores Backup, Servidores Linux y Dispositivos de Red.

Host groups

Una vez este la categoría creada desde la configuración crearemos un nuevo host indicándole el nombre del dispositivo, grupo y su dirección ip. Como en este caso el agente es el propio servidor lo podemos dejar con la dirección local, otro ejemplo sería el servidor de Backup en el que deberemos ingresar: 192.168.10.14.

En el apartado de templates seleccionaremos una con el mismo sistema operativo ya que no mostraran una serie de ítems, triggers y gráficos específicos.

Linked templates	Name	Action
	Template App Zabbix Server	Unlink Unlink and clear
	Template OS Linux by Zabbix agent	Unlink Unlink and clear

Seguidamente, se muestran una serie de triggers por defecto de las plantillas seleccionadas aportando información como el espacio de CPU utilizada.

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
16:57:06	Average	16:59:05	RESOLVED		NAS	Load average is too high (per CPU load over 1.5 for 5m)	1m 59s	No		
16:51:42	Warning	17:00:33	RESOLVED		Veeam Backup	Host has been restarted (uptime <10m)	8m 51s	No		
16:40:45	Average		PROBLEM		Zabbix server	Zabbix server. Utilization of discoverer processes over 75%	19m 49s	No		
2023-04-26 16:55:26	Warning		PROBLEM		Active Directory	System time is out of sync (diff with Zabbix server > 60s)	4d 5m	No		
2023-04-26 17:07:42	Warning		PROBLEM		Zabbix server	Disk space is low (used > 80%)	5d 23h 52m	No		

Finalmente, la visión global de la consola será la siguiente:

Name	Interface	Availability	Tags	Problems	Status	Latest data	Problems	Graphs	Screens	Web
Active Directory	192.168.10.11:10050	ZBX [SNMP] [JMX] [IPMI]		1	Enabled	Latest data	Problems 1	Graphs 3	Screens	Web
DNS	192.168.10.18:10050	ZBX [SNMP] [JMX] [IPMI]			Enabled	Latest data	Problems	Graphs 15	Screens 2	Web
Moodle	192.168.10.12:10050	ZBX [SNMP] [JMX] [IPMI]			Enabled	Latest data	Problems	Graphs 15	Screens 2	Web
NAS	192.168.10.14:10050	ZBX [SNMP] [JMX] [IPMI]			Enabled	Latest data	Problems	Graphs 27	Screens 2	Web
Odoo	192.168.10.10:10050	ZBX [SNMP] [JMX] [IPMI]			Enabled	Latest data	Problems	Graphs 15	Screens 2	Web
Router Pfsense	192.168.10.2:10050	ZBX [SNMP] [JMX] [IPMI]			Enabled	Latest data	Problems	Graphs 1	Screens	Web
Router Ubuntu	192.168.10.1:10050	ZBX [SNMP] [JMX] [IPMI]			Enabled	Latest data	Problems	Graphs 1	Screens	Web
Veeam Backup	192.168.10.13:10050	ZBX [SNMP] [JMX] [IPMI]		1	Enabled	Latest data	Problems 1	Graphs 3	Screens	Web
Windows Desktop	192.168.10.18:10050	ZBX [SNMP] [JMX] [IPMI]			Enabled	Latest data	Problems	Graphs 3	Screens	Web
Zabbix server	127.0.0.1:10050	ZBX [SNMP] [JMX] [IPMI]	1 1		Enabled	Latest data	Problems 2	Graphs 24	Screens 4	Web

Grafana

Paralelamente, como complemento al zabbix hemos instalado en la misma maquina el grafana para portarnos información de manera más grafica. ☰

En primer lugar, nos descargaremos la clave y la agregaremos en la lista de claves de confianza.

```
#wget -q -O - https://packages.grafana.com/gpg.key | apt-key add -
```

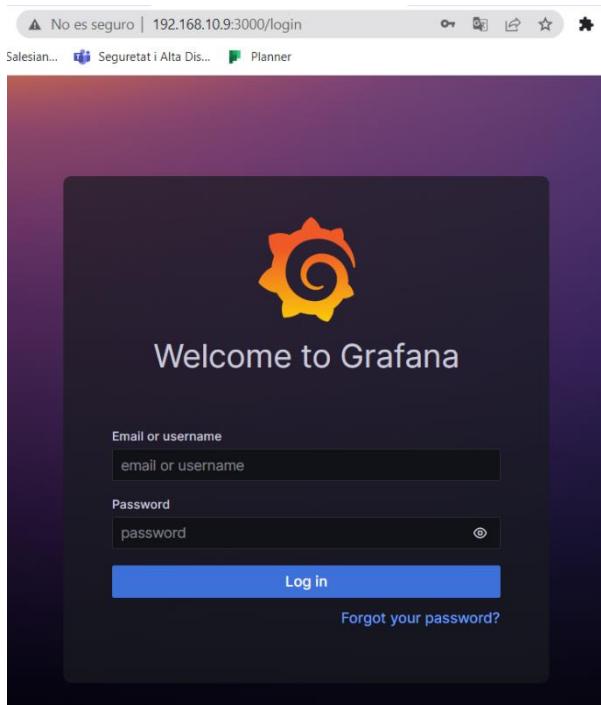
Agregamos el repositorio a las fuentes de APT

```
#sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
```

Actualizaremos la lista de paquetes e instalaremos el grafana con #apt install grafana.

Iniciamos el servicio y lo habilitamos: #sudo systemctl enable grafana-server.

Al terminar las ordenes podremos acceder a grafana a través 192.168.10.9:3000



Para habilitar la conexión con el servidor de Zabbix deberemos desplazarnos al apartado de Configuración para buscar el data source de este.

Lo descargaremos y habilitaremos.

Nos adentraremos a este una vez esté listo y le indicaremos los datos de conexión como la dirección ip y las credenciales

Cuando haya finalizado la configuración y se agregue correctamente importaremos nuestra plantilla con un json que cumpla nuestras necesidades.

Dentro de esta Dashboard ya podremos seleccionar el dispositivo que queramos mostrar y empezaremos a ver como estos se sincronizan a medida que pasa el tiempo de su adicción.

Active Directory y Powershell

Para crear la estructura de unidades organizativas, usuarios y grupos de seguridad ejecutaremos el siguiente script que cumple nuestras necesidades.

```
#Establecemos en una variable nuestro dominio
$ruta = "dc=pimpam,dc=local"
# Creamos carpeta principal c:\datos que centralizará en el servidor la información de los
usuarios vía recursos compartidos
New-Item -Path c:\ -Name Datos -ItemType Directory
Disable-NTFSAccessInheritance -Path c:\Datos
Clear-NTFSAccess -Path c:\Datos
Add-NTFSAccess -Path c:\datos -Account Administradores -AccessRights FullControl
Add-NTFSAccess -Path c:\datos -Account Backup -AccessRights Modify

#Importamos archivo CSV con los usuarios y crearemos las UO, Grupos y usuarios a través de
este.
$usuarios = Import-Csv -Path C:\Users\Administrador\Desktop\alumnos-escuela.csv -
Delimiter ";" -Encoding UTF8
#Aseguramso la UO de escola contra eliminaciones accidentales
New-ADOrganizationalUnit -Name Escola -Path "dc=pimpam,dc=local" -
ProtectedFromAccidentalDeletion $true
New-ADGroup -Name ("Grupo Escola") -Path ("ou=Escola," + $ruta) -GroupScope Global -
GroupCategory Security
$ciclos = $usuarios | Group-Object -Property ciclo -NoElement
foreach ($ciclo in $ciclos) {
    Write-Output ("Creando CICLO " + $ciclo.name)
    New-ADOrganizationalUnit -Name $ciclo.name -Path "ou=Escola,dc=pimpam,dc=local" -
ProtectedFromAccidentalDeletion $false
    New-ADGroup -Name ("Grupo " + $ciclo.Name) -Path ("ou=" + $ciclo.name + ",ou=Escola," +
$route) -GroupScope Global -GroupCategory Security
    Add-ADGroupMember -Identity "Grupo Escola" -Members ("Grupo " + $ciclo.Name)
    $usuariosCiclo = $usuarios | Where-Object {$_.ciclo -eq $ciclo.name}
    $grupos = $usuariosCiclo | Group-Object -Property grupo -NoElement
    New-Item -Path "C:\Datos" -Name $ciclo.Name -ItemType Directory
    foreach ($grupo in $grupos) {
        Write-Output (" Creando GRUPO " + $grupo.name)
        New-ADOrganizationalUnit -Name $grupo.name -Path ("ou=" + $ciclo.name + ",ou=Escola,dc=pimpam,dc=local") -ProtectedFromAccidentalDeletion $false
        New-ADGroup -Name ("Grupo " + $grupo.name) -Path ("ou=" + $grupo.name + ",ou=" +
$ciclo.name + ",ou=Escola," + $route) -GroupScope Global -GroupCategory Security
        #Añadiremos a los usuarios dentro den grupo de seguridad que les pertoque
        Add-ADGroupMember -Identity ("Grupo " + $ciclo.Name) -Members ("Grupo " +
$grupo.Name)
        $usuariosgrupo = $usuarios | Where-Object {$_.grupo -eq $grupo.Name}
        New-Item -Path ("C:\Datos\" + $ciclo.Name) -Name $grupo.Name -ItemType Directory
        New-Item -Path ("C:\Datos\" + $ciclo.Name + "\" + $grupo.Name) -Name comun -
ItemType Directory
        #Crearemos una estructura de carpetas de las cuales solo podrá acceder su mismo propietario
        New-Item -Path ("C:\Datos\" + $ciclo.Name + "\" + $grupo.Name) -Name usuarios -
ItemType Directory
```

```

Add-NTFSAccess -Path ("C:\Datos\" + $ciclo.Name + "\" + $grupo.Name + "\comun") -
Account ("Grupo " + $grupo.name) -AccessRights Modify
New-SmbShare -name ("_" + $grupo.Name) -Path ("C:\Datos\" + $ciclo.Name + "\" +
$grupo.Name + "\comun") -ChangeAccess todos
foreach($usuario in $usuariosgrupo) {
    $nombrecompleto = ($usuario.nombre + " " + $usuario.apellido)
    $loginusuario = $($usuario.nombre).Substring(0,1) + "." + $usuario.apellido
    Write-Output ("      Creando usuario " + $nombrecompleto)
    New-ADUser `

        -Name $nombrecompleto `

        -GivenName $usuario.nombre `

        -Surname $usuario.apellido `

        -DisplayName $nombrecompleto `

        -Path ("ou=" + $grupo.name + ",ou=" + $ciclo.name + ",ou=Escola," + $ruta) `

        -SamAccountName $loginusuario.ToLower() `

        -UserPrincipalName ($loginusuario + "@pimpam.local") `

        -AccountPassword (ConvertTo-SecureString "123-user!" -AsPlainText -Force) `

        -EmailAddress ($loginusuario + "@pimpam.local") `

        -MobilePhone $usuario.telèfon `

        -State $usuario.estados `

        -EmployeeID $usuario.EmployeeNumber `

        -PostalCode $usuario.cp `

        -City $usuario.ciudad `

        -StreetAddress $usuario.calle `

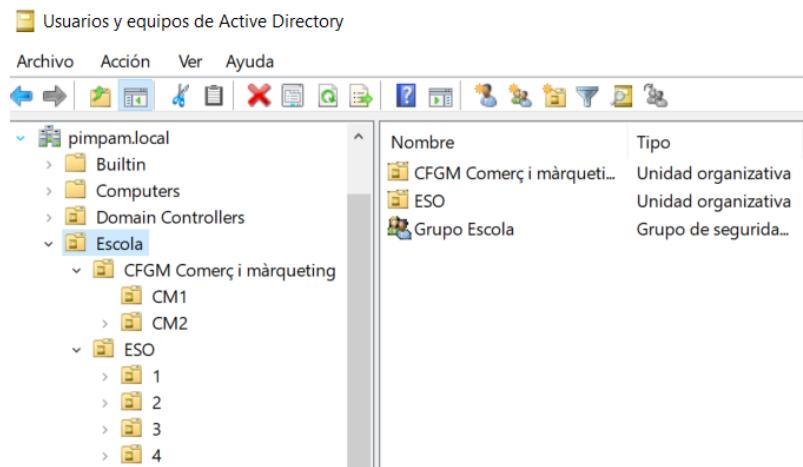
        -Department $ciclo.name `

        -Enabled $true `

        -ScriptPath ini.vbs
    Add-ADGroupMember -Identity ("Grupo " + $grupo.Name) -Members
$loginusuario.ToLower()
    New-Item -Path ("C:\Datos\" + $ciclo.Name + "\" + $grupo.Name + "\usuarios" ) -Name
$loginusuario.ToLower() -ItemType Directory
    Add-NTFSAccess -Path ("C:\Datos\" + $ciclo.Name + "\" + $grupo.Name + "\usuarios\" +
+$loginusuario.ToLower()) -Account $loginusuario.ToLower() -AccessRights Modify
    New-SmbShare -name ("_" + $loginusuario.ToLower()) -Path ("C:\Datos\" +
$ciclo.Name + "\" + $grupo.Name + "\usuarios\" + $loginusuario.ToLower()) -ChangeAccess
todos
}
}
}

```

Una vez ejecutado veremos la estructura siguiente donde la Raiz será nuestra escuela y de ahí partirán todos los cursos, en nuestro caso, veremos la ESO y un CFGM.



Dentro de cada unidad organizativa habrá un grupo de seguridad con los usuarios internos además de los propios usuarios. En el caso de la CFGM tendrán 4 grupos de seguridad: 1 para cada año, CM1 Y CM2, un grupo que envuelva ambos llamado CFGM y un último que se una con el otro curso ESO para tener a todos los usuarios centralizados en el grupo escola.

Usuarios en CM1:		Usuarios en 1ESO:	
Nombre	Tipo	Nombre	Tipo
Carles Gasia	Usuario	Aina Dolado	Usuario
Grupo CM1	Grupo de seguridad	Aitor Marcos	Usuario
Iago Cabello	Usuario	Grupo 1	Grupo de seguridad
Marc Pena	Usuario	Oscar Puig	Usuario
Miquel Romero	Usuario		
Paula Dolado	Usuario		

General Dirección Cuenta Perfil Teléfonos Organización

Nombre de inicio de sesión de usuario:
P.Dolado @pimpam.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):
PIMPAM\ p.dolado

Horas de inicio de sesión... Iniciar sesión en...

Desbloquear cuenta

Opciones de cuenta:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión
- El usuario no puede cambiar la contraseña
- La contraseña nunca expira
- Almacenar contraseña utilizando cifrado reversible

La cuenta expira
 Nunca

En relación con la configuración de los usuarios podremos ver en la izquierda un ejemplo de usuario en CM1.

Este usuario tiene varias condiciones como que no puede cambiar la contraseña, nunca expirara la cuenta ni la contraseña.

Además, en su membresía veremos como comentado antes que es participante del grupo de su año, CM1.

Miembro de:

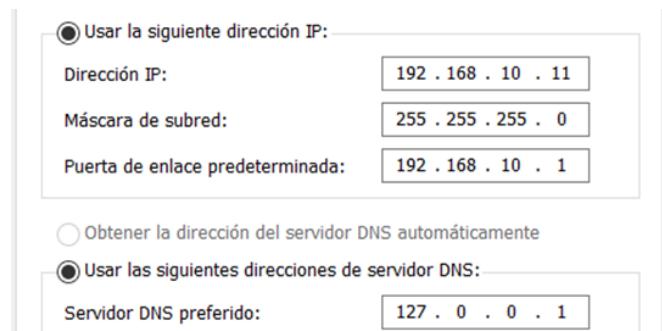
Nombre	Carpeta de los Servicios de dominio de Active Dir...
Grupo CM1	pimpam.local/Escuela/CFGM Comerç i màrqueting...
Usuarios del dom...	pimpam.local/Users

El mismo grupo de CM1 es miembro del grupo global CFGM y así con escuela.

The screenshot shows two windows side-by-side. On the left, a 'Miembros:' list shows several users from the 'pimpam.local/Escola/CFGM Comerç i màrqueting...' domain. On the right, the 'Propiedades: Grupo CM1' window shows the 'Miembro de:' section, which lists the 'Grup CFGM Comerç i màrqueting...' group as a member of the 'Carpeta de los Servicios de dominio de Active Dir...' group.

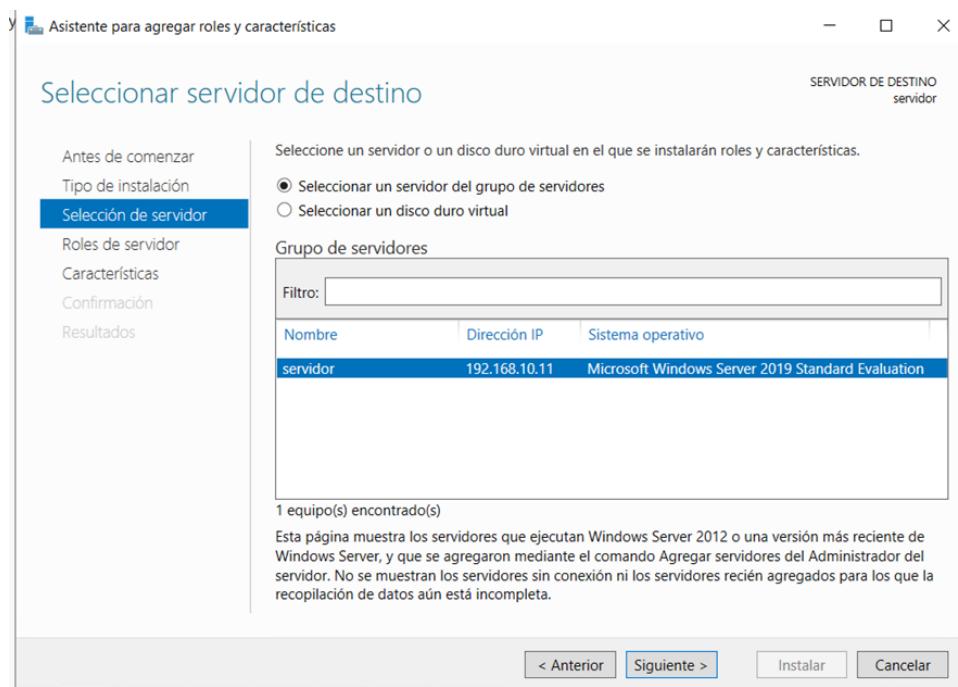
DNS SLAVE

Primero de todo cambiaremos la configuración de la tarjeta de red para cambiar la dirección del servidor DNS a su misma dirección ip ya que será el mismo servidor.

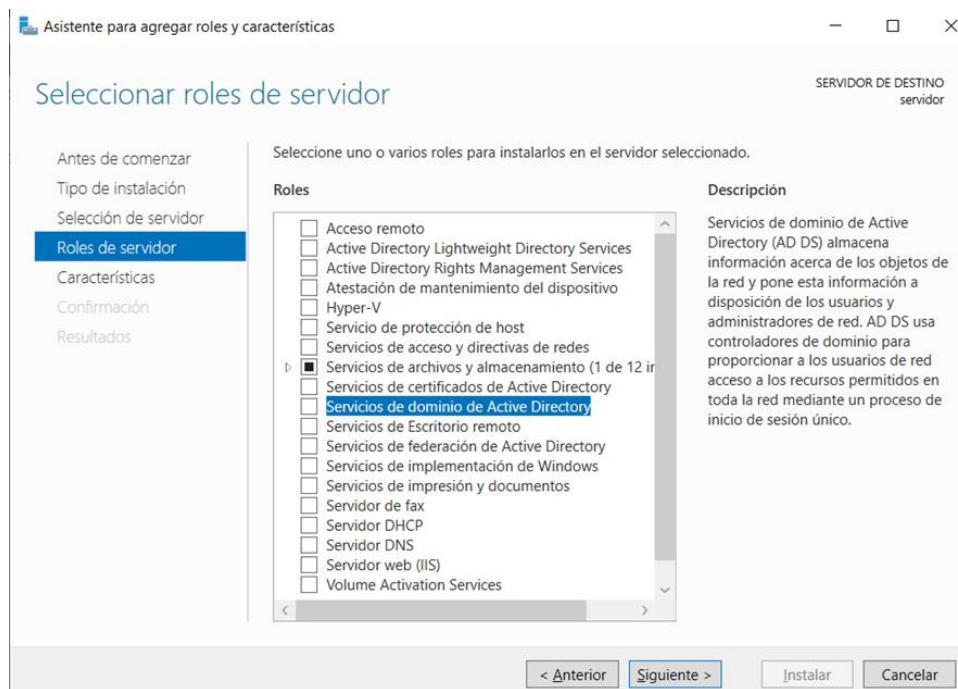


The screenshot shows the 'Seleccionar tipo de instalación' (Select Installation Type) step of a wizard. The 'Tipo de instalación' (Installation Type) section is selected. It shows a list of steps: 'Antes de comenzar', 'Selección de servidor', 'Roles de servidor', 'Características', 'Confirmación', and 'Resultados'. The main area describes the selection of installation type, mentioning physical, virtual, or VHD installations. It offers two options: 'Instalación basada en características o en roles' (Based on Features or Roles) and 'Instalación de Servicios de Escritorio remoto' (Remote Desktop Services Installation). The 'Instalación basada en características o en roles' option is selected.

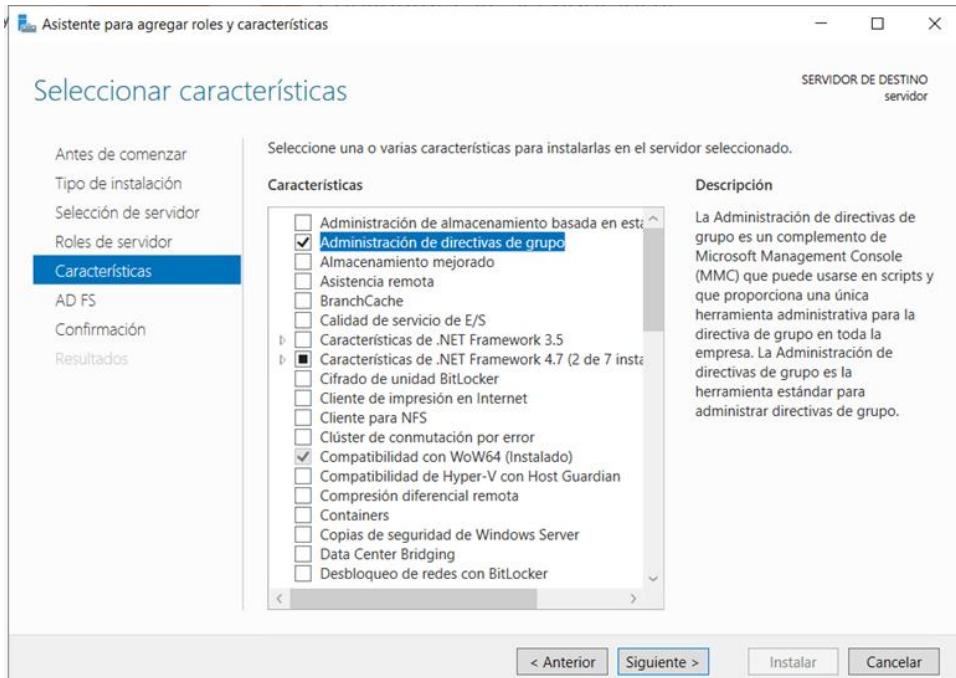
Seleccionaremos agregar roles y un tipo de instalación basado en roles, así podremos añadir el rol de Active directory y poder configurarlo.



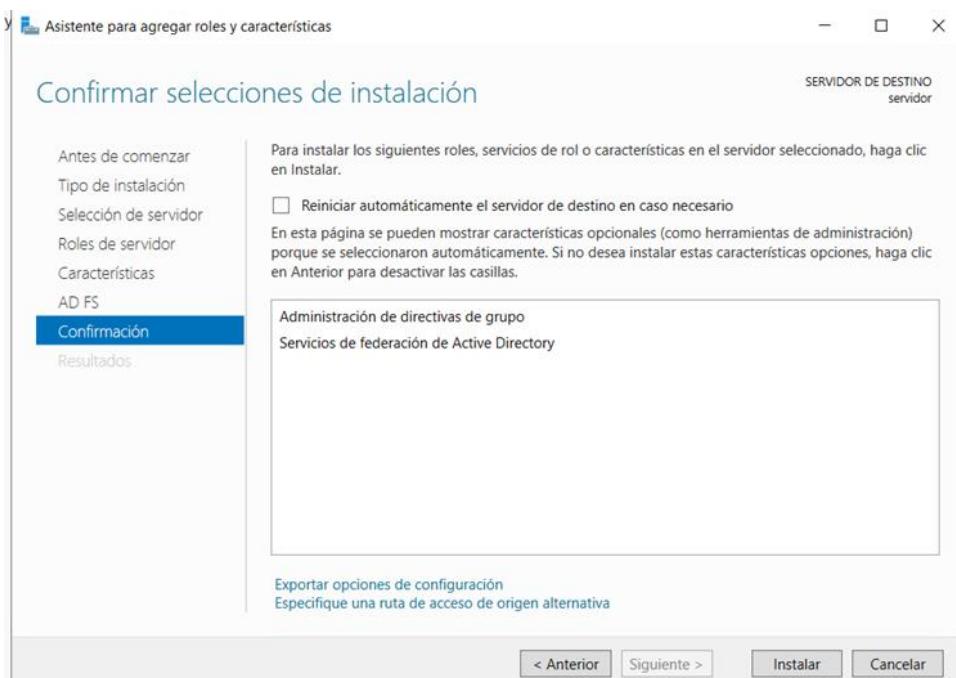
Seleccionaremos el mismo equipo ya que es sobre el dónde se va a instalar la máquina virtual.



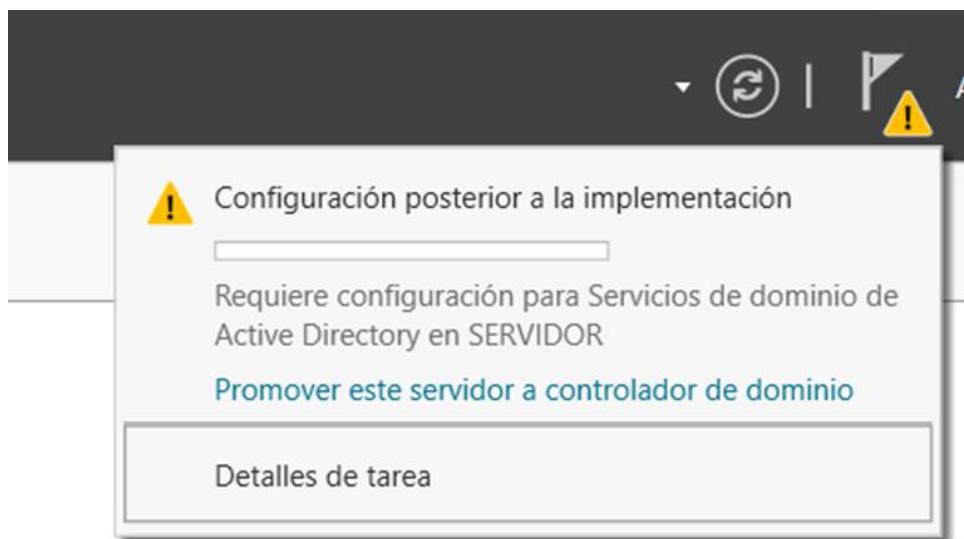
Y seleccionaremos el servicio de active directory.



En características tambien el administrador de directivas de grupo para poder realizar políticas para todo el dominio.

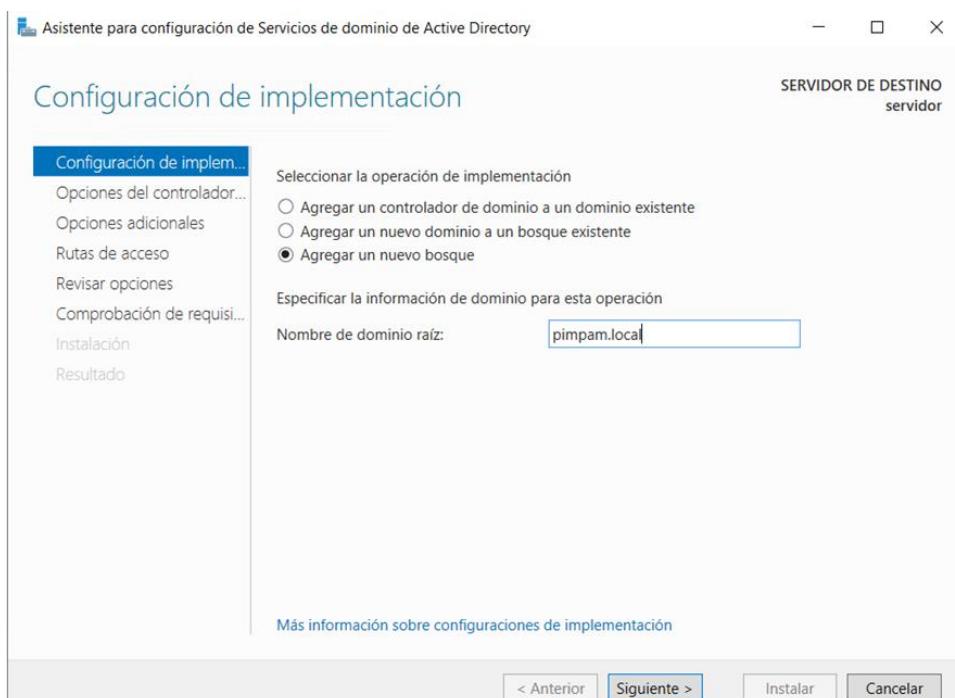


Seguiremos hasta la confirmación de instalación donde seleccionaremos la opción de instalación

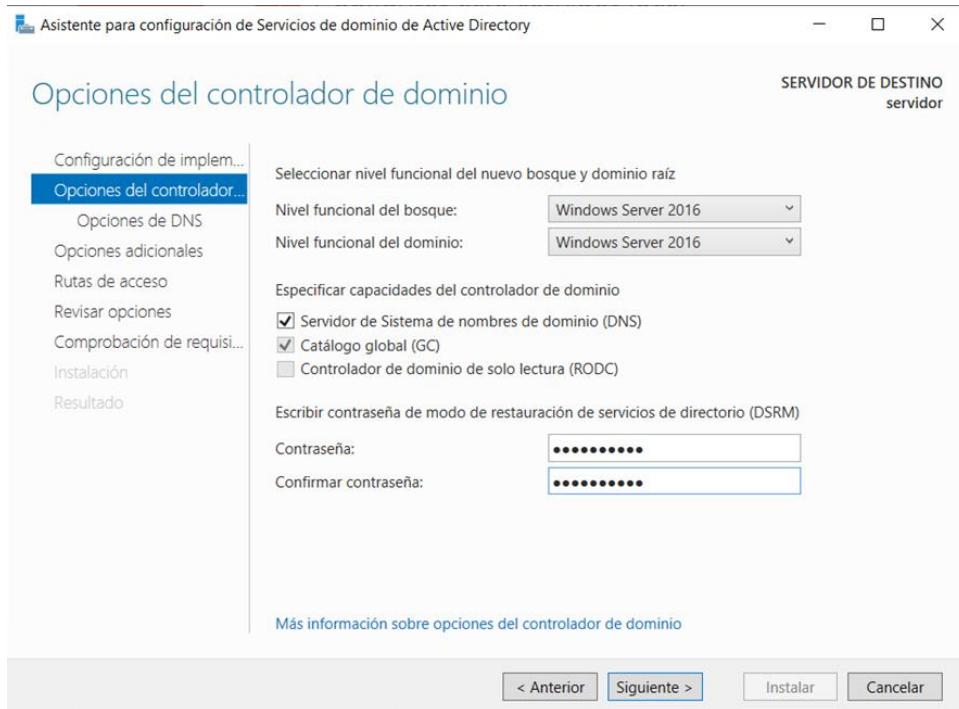


Tras terminarse la instalación ya permite promover el servidor a controlador de dominio.

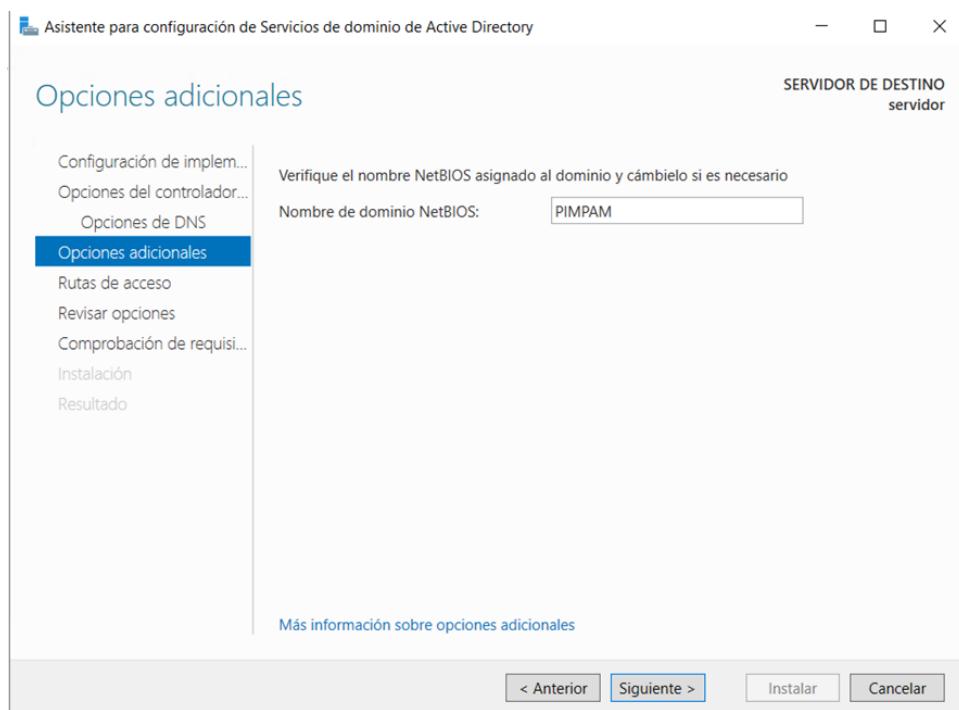
Aunque es muy recomendable tras instalarlo reiniciar el servidor.



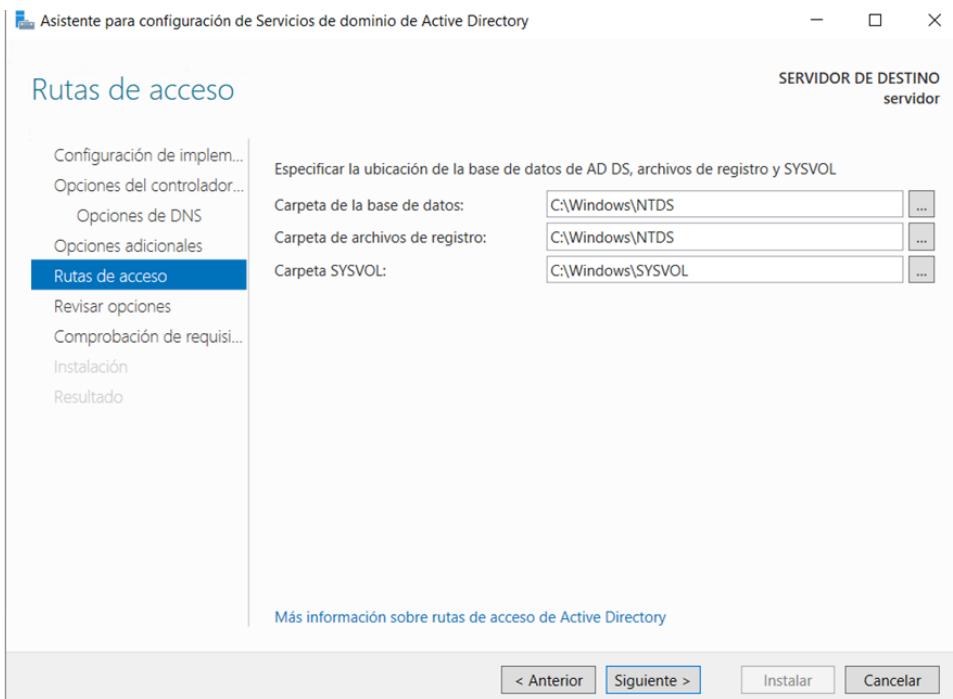
En la primera opción nos permiten añadirnos a un dominio o bosque ya existente, al ser un nuevo dominio seleccionaremos un nuevo bosque.



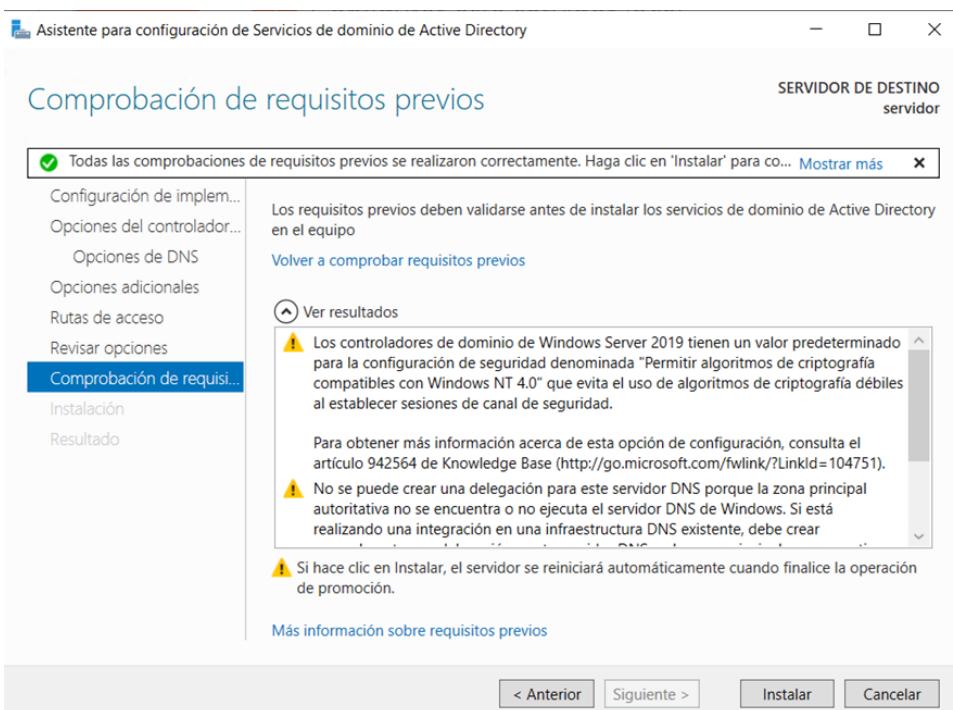
Indicaremos una contraseña de restauración y la versión funcional del dominio de bosque y dominio importante si se van a configurar más dominios dentro del bosque con otros servidores.



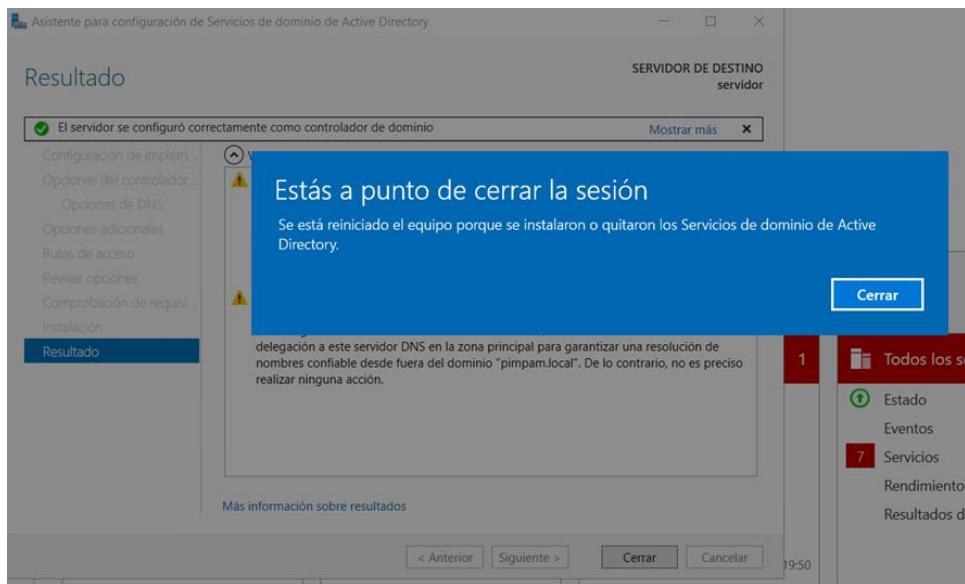
El nombre de NetBIOS



Dejaremos las rutas de acceso por defecto.



Y indicaremos instalar para que el aplique los cambios.

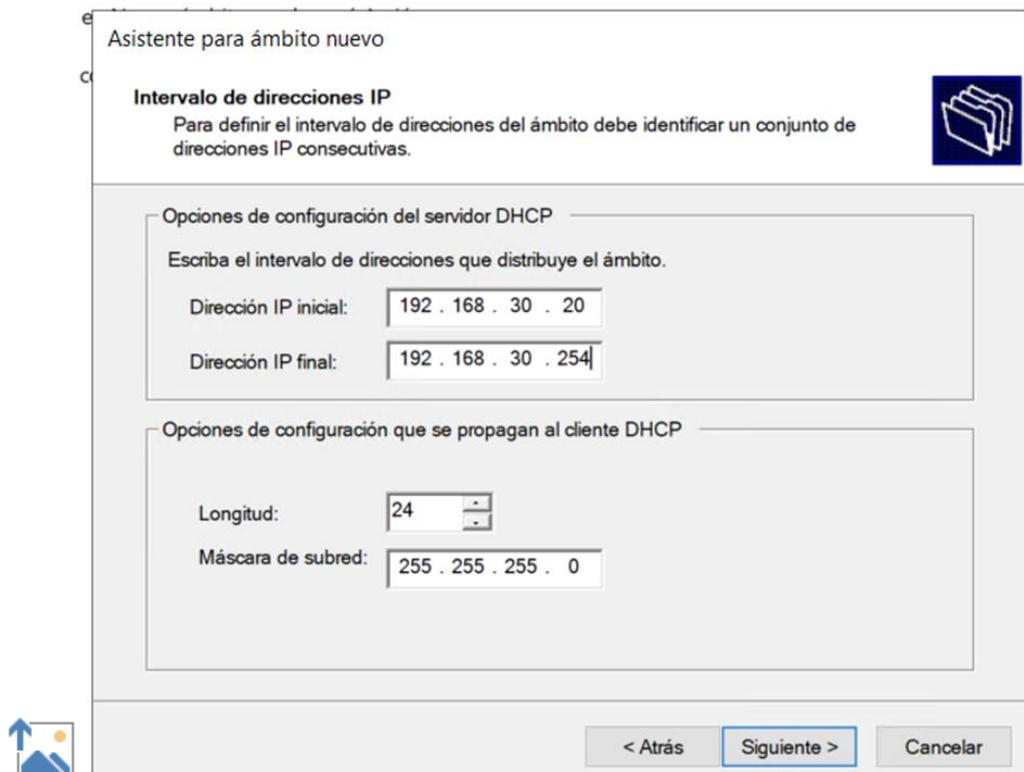


Tras terminar solicita volver a iniciar sesión ya que la cuenta de usuario local va a dejar de utilizarse y va a ser el usuario del dominio.

Es muy recomendable reiniciar el servidor y tras esto ya podemos conectarnos.

DHCP

Primero de todo para poder configurar un dhcp agregaremos el rol y lo instalaremos



Tras esto indicamos el rango el cual repartirá dhcp y la máscara

Asistente para ámbito nuevo

Duración de la concesión

La duración de la concesión especifica durante cuánto tiempo puede utilizar un cliente una dirección IP de este ámbito.



La duración de las concesiones debería ser típicamente igual al promedio de tiempo en que el equipo está conectado a la misma red física. Para redes móviles que consisten principalmente de equipos portátiles o clientes de acceso telefónico, las concesiones de duración más corta pueden ser útiles.

De igual modo, para una red estable que consiste principalmente de equipos de escritorio en ubicaciones fijas, las concesiones de duración más larga son más apropiadas.

Establecer la duración para las concesiones de ámbitos cuando sean distribuidas por este servidor.

LIMITADA A:

Días: Horas: Minutos:

< Atrás

Siguiente >

Cancelar

Indicamos el tiempo de concesión el tiempo que esta ip se reservara a ese equipo en este caso 1 día.

Asistente para ámbito nuevo

Configurar opciones DHCP

Para que los clientes puedan utilizar el ámbito debe configurar las opciones DHCP más habituales.



Cuando los clientes obtienen una dirección, se les da opciones DHCP tales como las direcciones IP de los enrutadores (puertas de enlace predeterminadas), servidores DNS y configuración WINS para ese ámbito.

La configuración que ha seleccionado aquí es para este ámbito e invalida la configuración de la carpeta Opciones de servidor para este servidor.

¿Desea configurar ahora las opciones DHCP para este ámbito?

Configurar estas opciones ahora

Configuraré estas opciones más tarde

< Atrás

Siguiente >

Cancelar

Asistente para ámbito nuevo

Enrutador (puerta de enlace predeterminada)

Puede especificar los enruteadores, o puertas de enlace predeterminadas, que se distribuirán en el ámbito.



Para agregar una dirección IP para un enruteador usado por clientes, escriba la dirección.

Dirección IP:

Agregar

192.168.30.2

Quitar

Arriba

Abajo

< Atrás

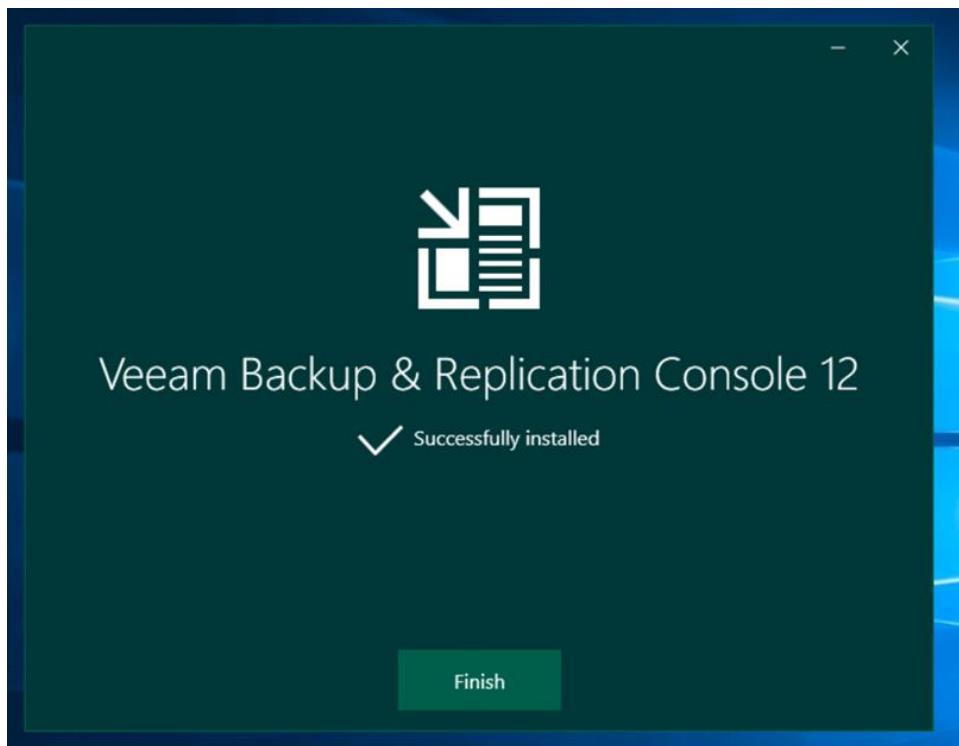
Siguiente >

Cancelar

E indicamos la puerta predeterminada.

VEEAM Backup

Antes de iniciar, es importante recalcar que el servidor de copias no está dentro del dominio para que en caso de ataque este no se pueda acceder con las mismas credenciales si ya han accedido al dominio, y que las políticas de grupo no le afecten intentando darle una capa más de seguridad.



Install Veeam Backup & Replication Console

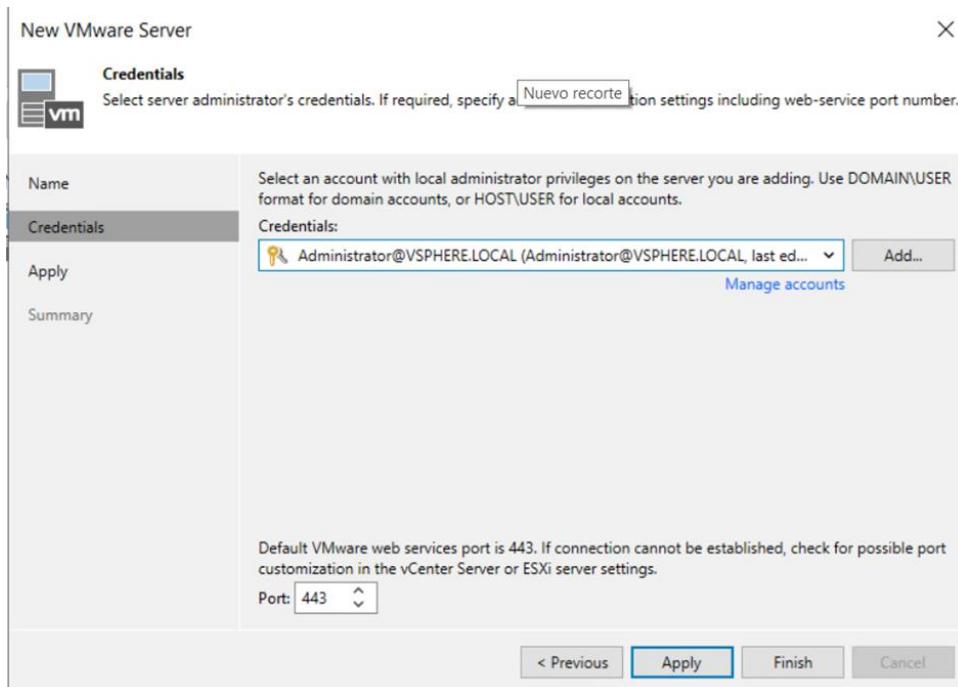
Veeam Backup & Replication console is a Windows-based graphical user interface client for managing backup servers.

Veeam Backup

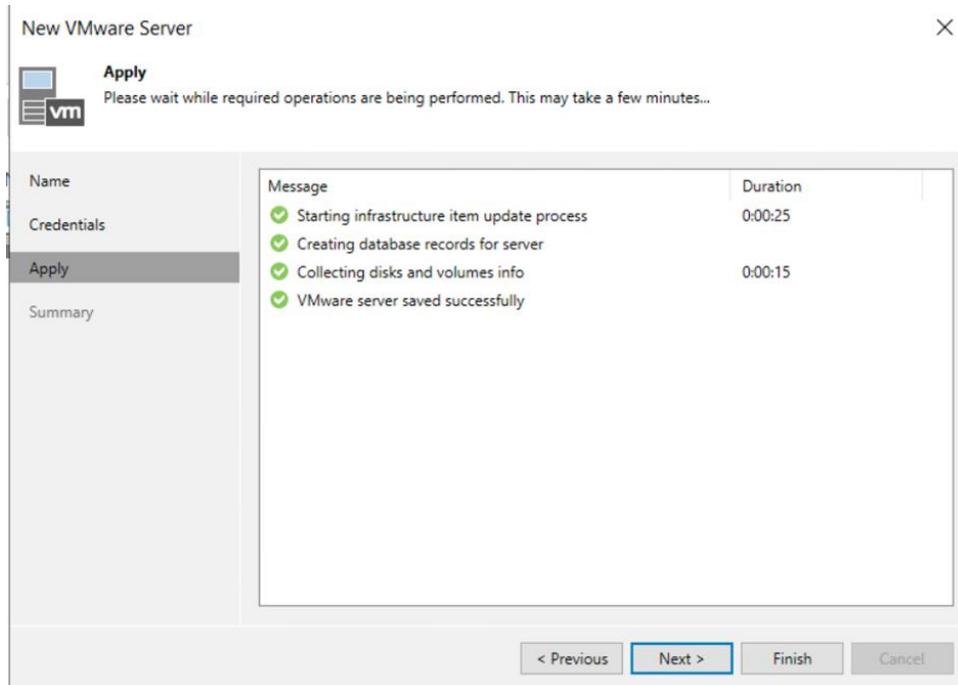
Tras iniciar el ejecutable

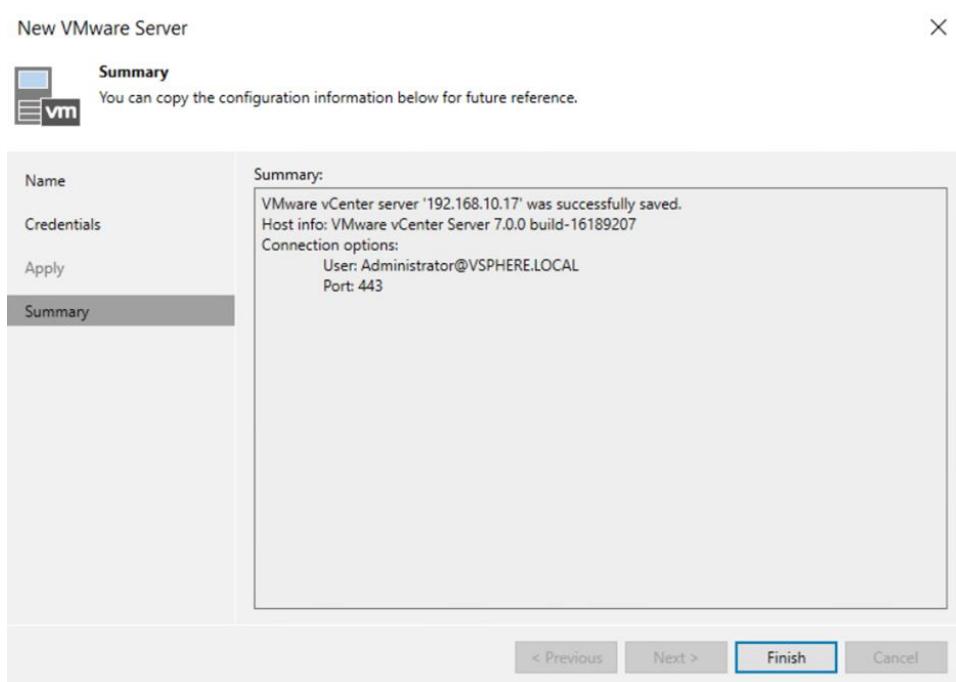
A screenshot of the Veeam Backup & Replication Console interface. The window title is "New VMware Server". The main area contains fields for "Name" (set to "VM") and "DNS name or IP address" (set to "192.168.10.17"). There are tabs for "Credentials", "Apply", and "Summary". At the bottom right are buttons for "< Previous", "Next >", "Finish", and "Cancel". On the left, there is a sidebar with navigation links: Home, Inventory, Backup Infrastructure (which is selected), Storage Infrastructure, Tape Infrastructure, and Files. The "Backup Infrastructure" section also includes sub-links for Backup Repositories, External Repositories, WAN Accelerators, Service Providers, SureBackup, Application Groups, and Virtual Labs.

Añadiremos un nuevo servidor repositorio indicando el vSphere



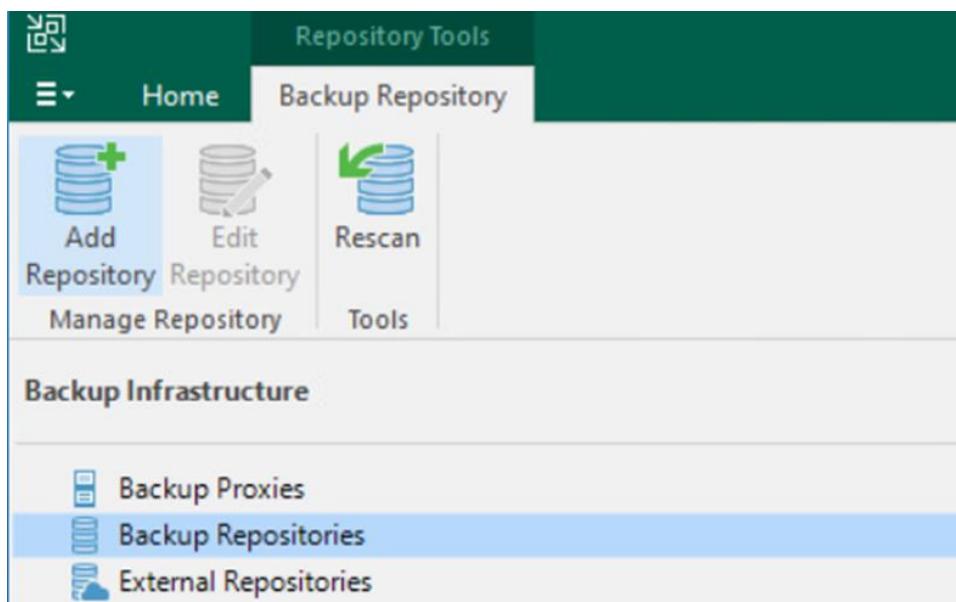
le introduciremos las credenciales para que pueda validarse.





Y tras verificar la conexión se añadirá correctamente

Backup repository:



añadiremos el repositorio de copias que será el NFS del NAS.

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell Data Domain, ExaGrid, Fujitsu ETERNUS CS800, HPE StoreOnce, Infinidat InfiniGuard or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider.

Cancel

Seleccionamos network Attached storage

Network Attached Storage

Select the type of a shared folder you want to use as a backup repository.



NFS share

Adds an NFS share. This is the recommended configuration for leveraging storage capacity provided by NAS devices.



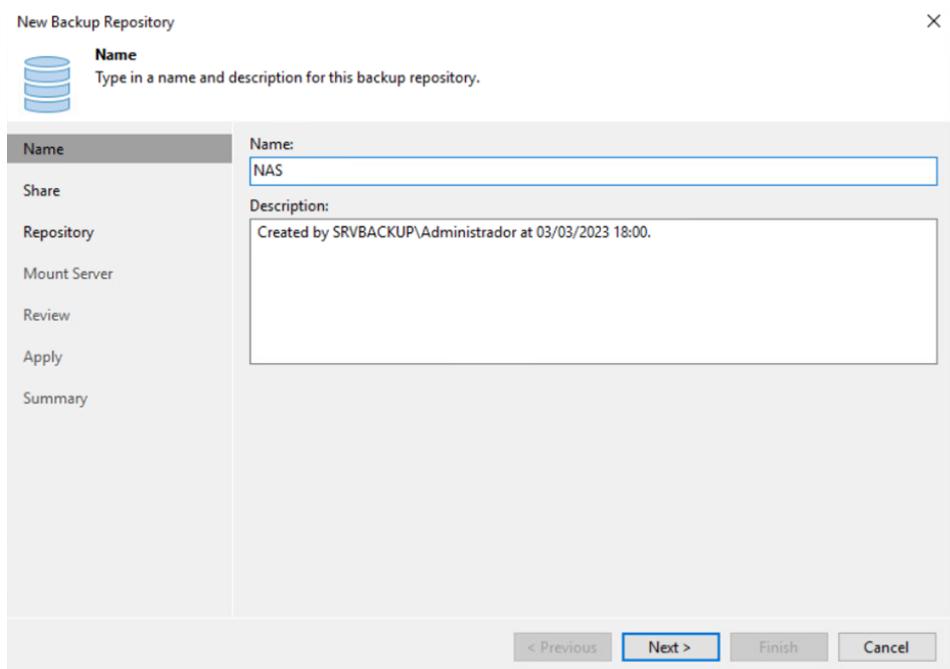
SMB share

Adds an SMB (CIFS) share. For reliability reasons, this configuration is recommended for continuously available (CA) network shares only.

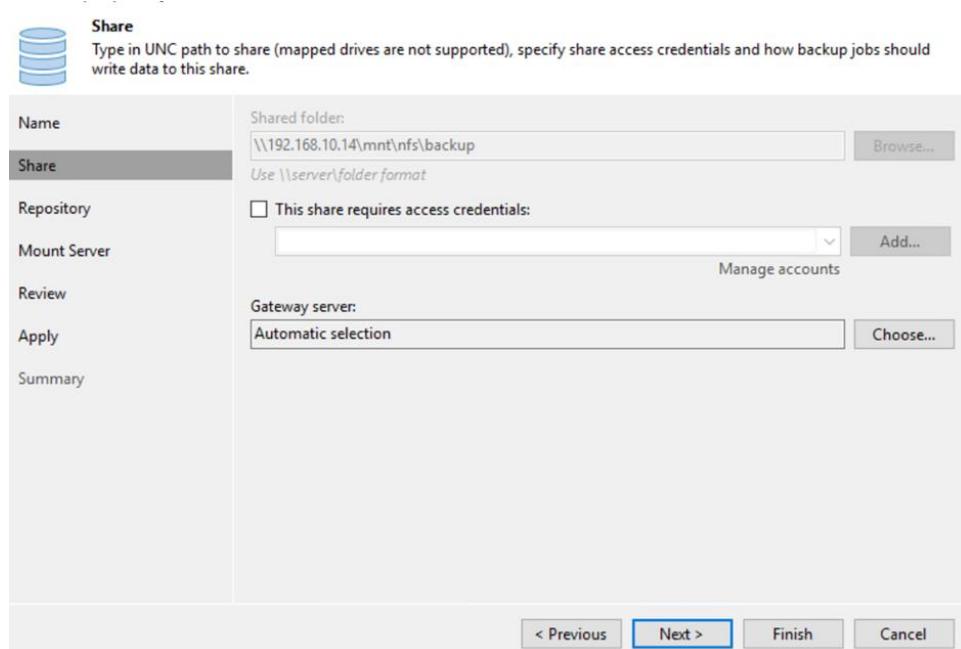
Cancel

Y seleccionaremos SMB share aunque nos parezca que NFS seria la opcion correcta ya que no permite conectarnos correctamente con veeam.

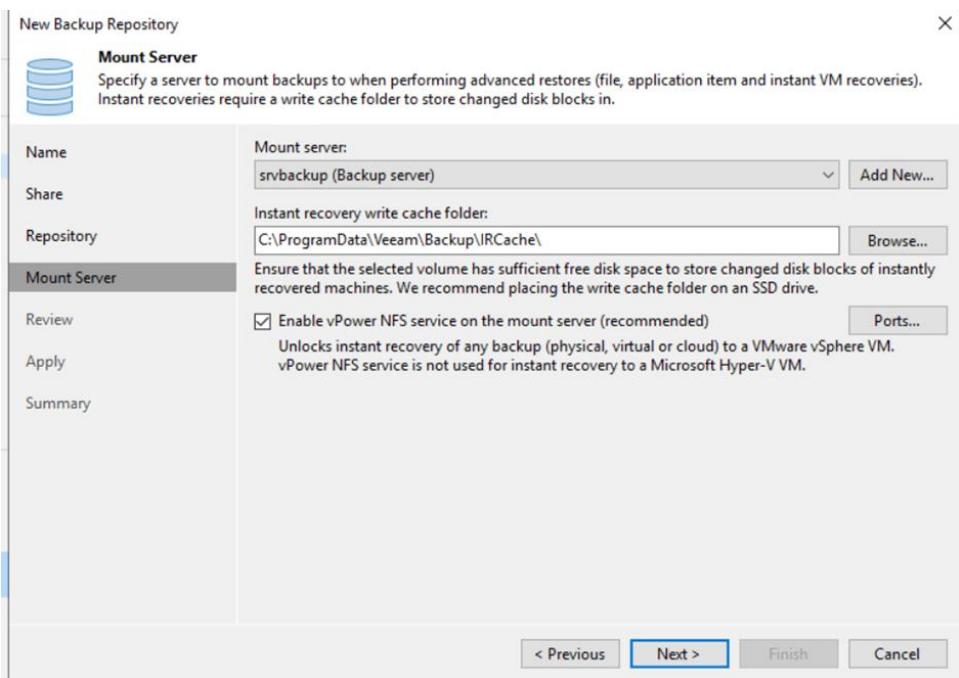
network



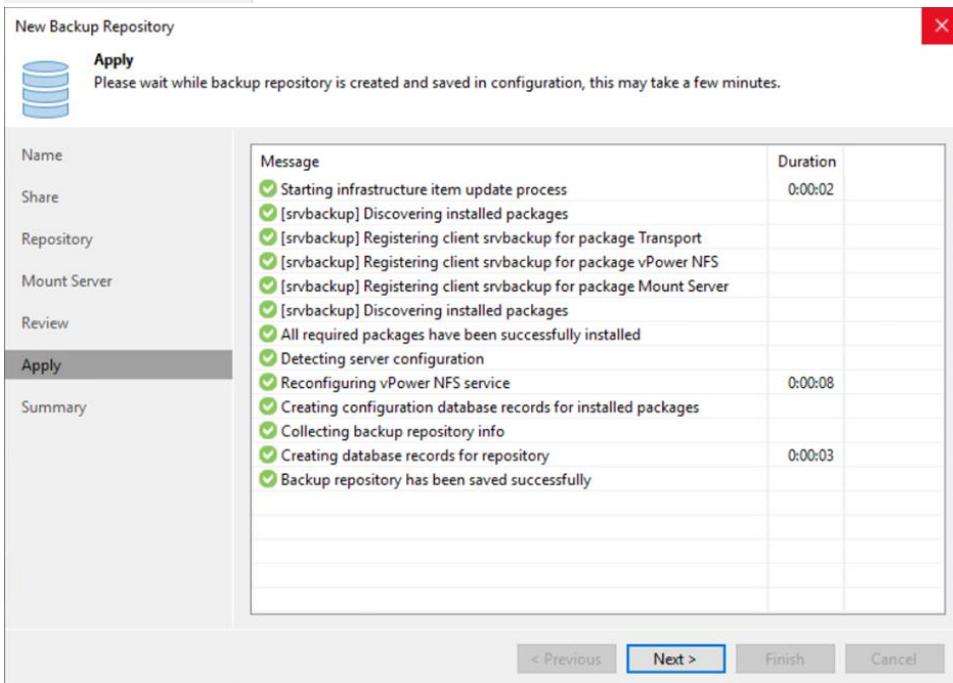
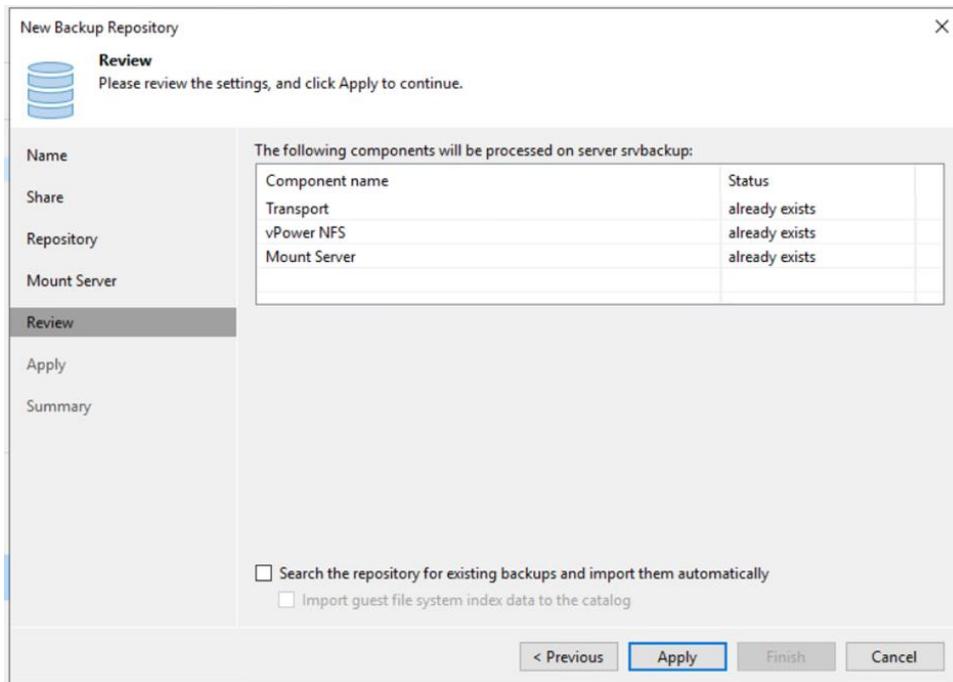
Seleccionamos el nombre del repositorio



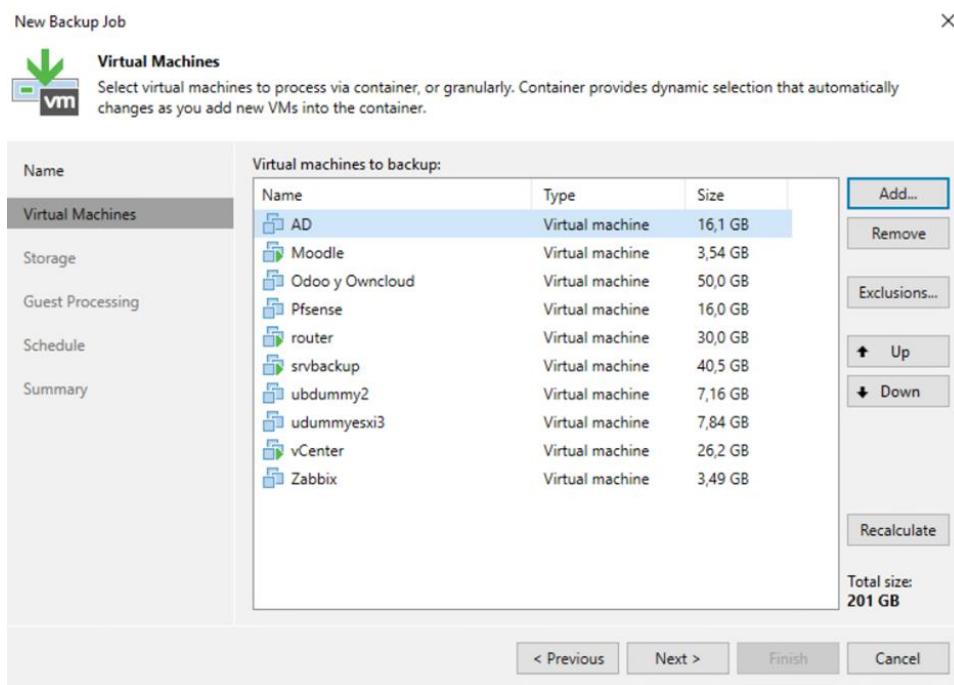
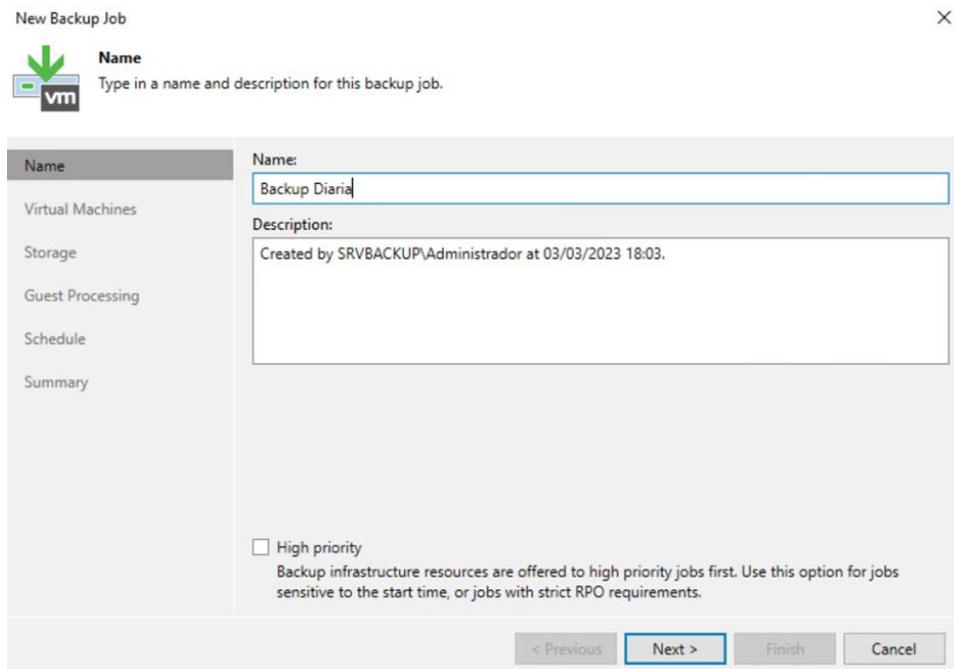
Indicaremos la dirección de la carpeta compartida



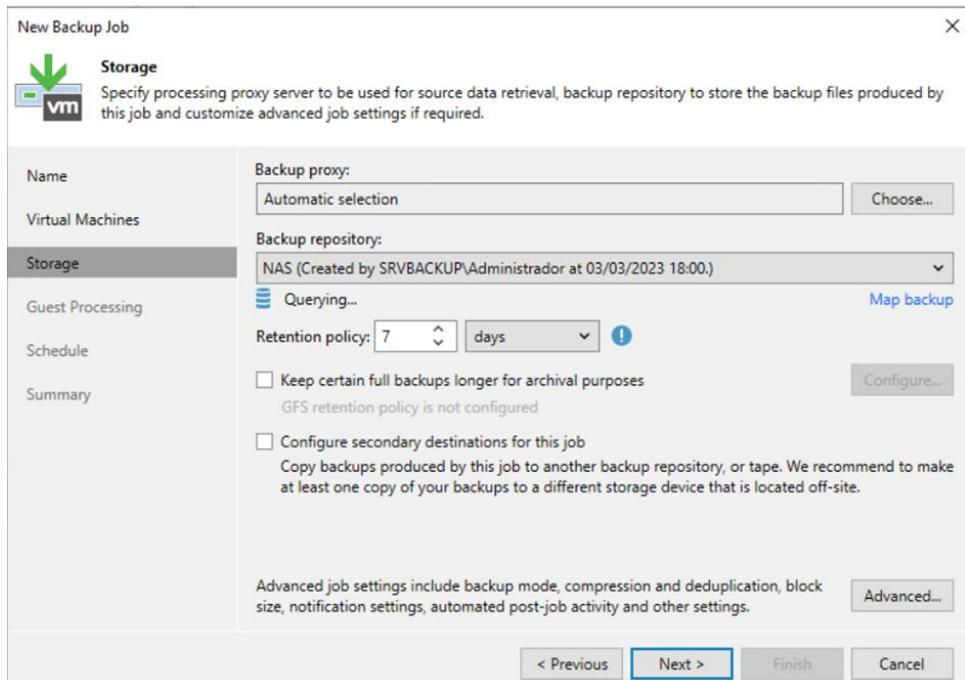
Habilitamos la opcion del servicio para NFS



Backup



La copia diaria seleccionamos todas VM



Y el nuevo repositorio de SMB

Add Roles and Features Wizard

Select features

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features**
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

- .NET Framework 3.5 Features
- .NET Framework 4.6 Features (2 of 7 installed)
- Background Intelligent Transfer Service (BITS)
- BitLocker Drive Encryption
- BitLocker Network Unlock
- BranchCache
- Client for NFS
- Containers
- Data Center Bridging
- Direct Play

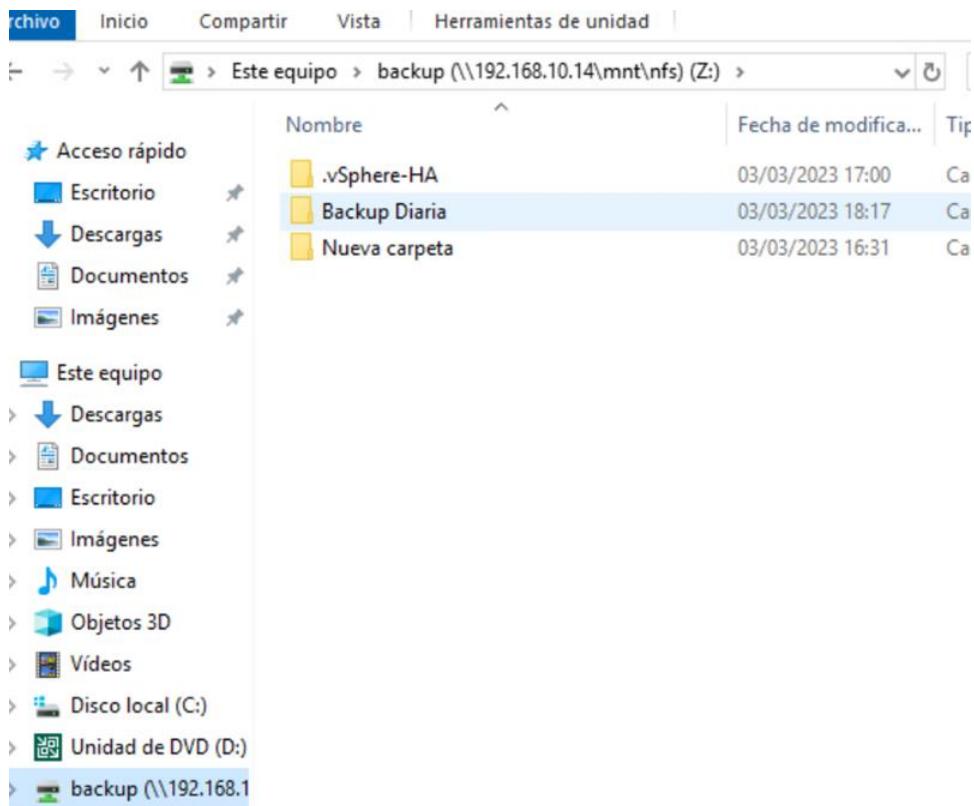
NFS conectarse cliente

```
C:\Users\Administrador>mount -o \\\\192.168.10.14\\mnt\\nfs\\backup Z:
Z: está conectado ahora correctamente a \\\\192.168.10.14\\mnt\\nfs\\backup

El comando se completó correctamente.

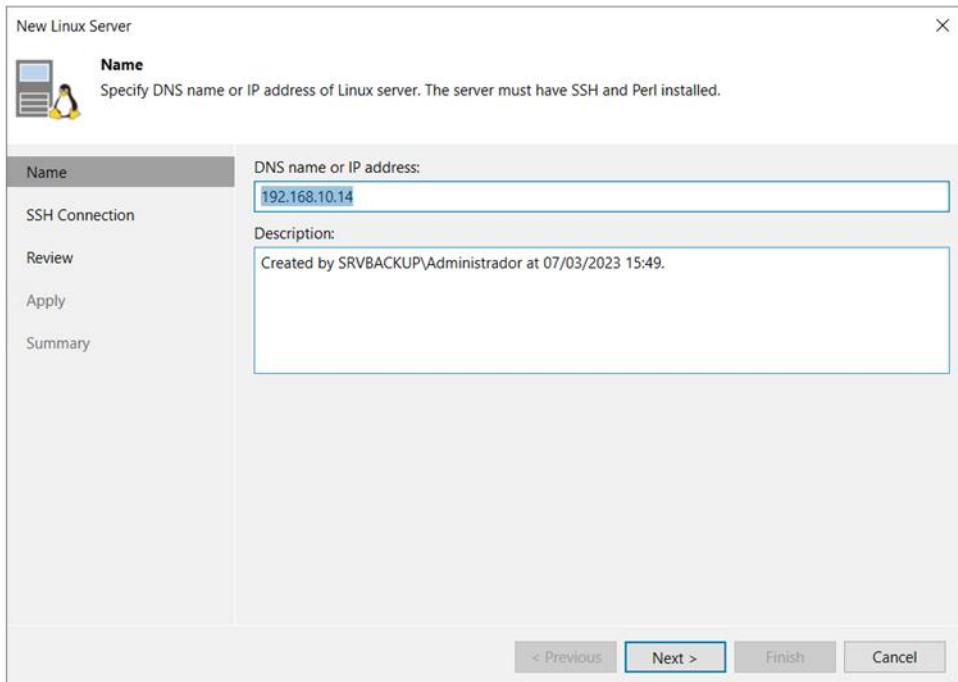
C:\Users\Administrador>
```

Instalaremos el cliente de NFS para poder conectarse

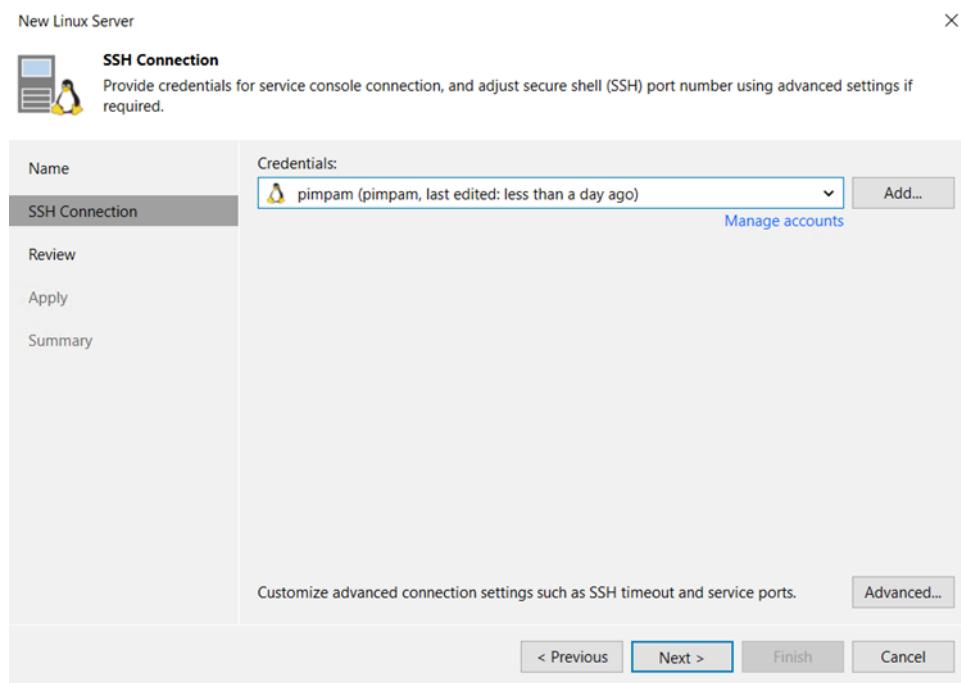


Y con el comando mount indicando nos conectaremos a la unidad de red para poder ver las copias realizadas.

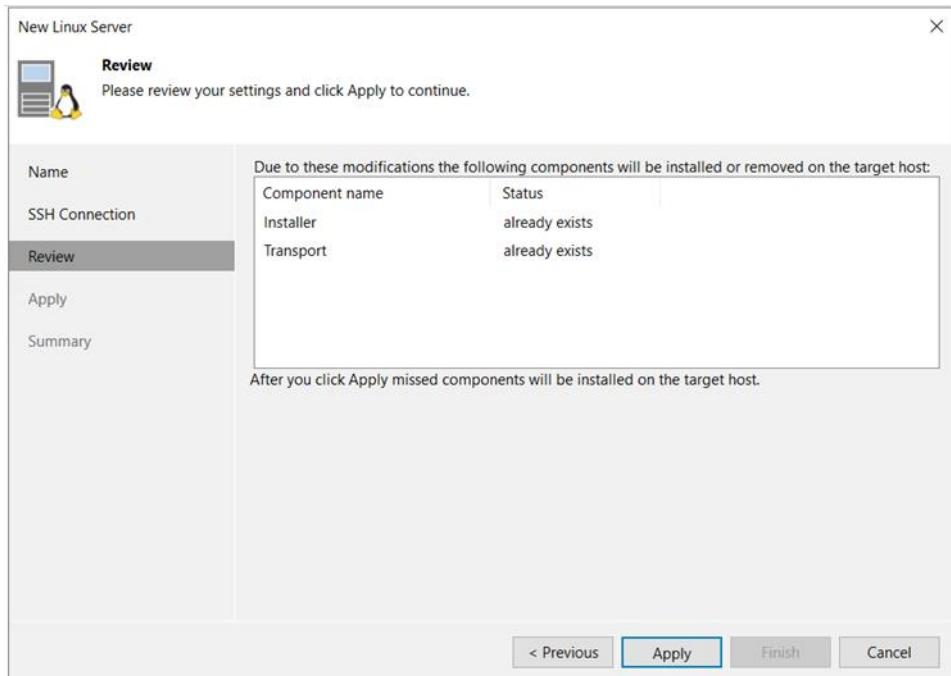
NAS Server



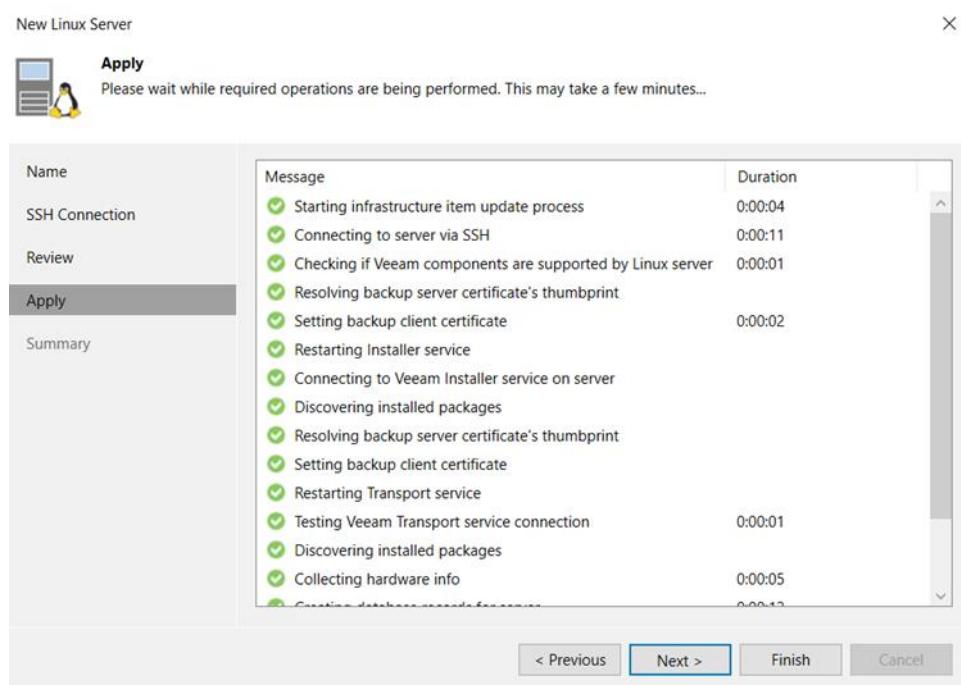
Indicaremos la ip del NAS



I introduciremos las credenciales para acceder.



El revisara si tiene instalador, el cual tiene por unas pruebas anteriores.



Y el intentara conectarse via ssh y realizara la instalación

Bloque 3 | DMZ

3.1 Infraestructura

DNS

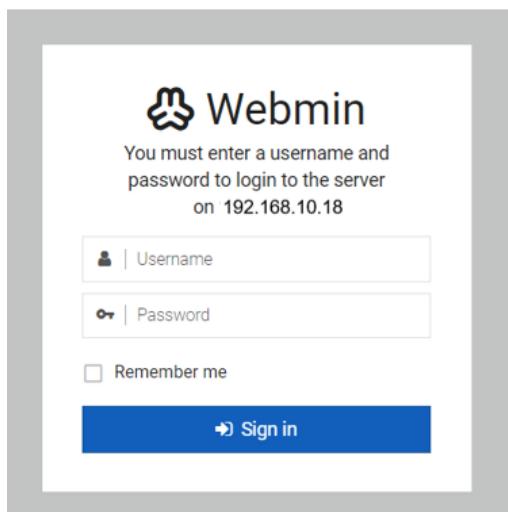
Para la función de DNS hemos utilizado la herramienta del webmin que de manera grafica nos servirá para configurar el sistema vía web.

En primer lugar, utilizando un Ubuntu 22.04 actualizaremos el listado de repositorios y nos descargaremos desde el repositorio oficial la clave.

```
#wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -
```

Después agregaremos el repositorio de webmin con el siguiente comando para proceder con la instalación.

```
#add-apt-repository "deb http://download.webmin.com/download/repository sarge contrib"
#apt install webmin
#systemctl enable webmin.service
```



Una vez accedamos con el usuario

The BIND DNS server /usr/sbin/named could not be found on your system. Maybe it is not installed, or your [BIND module configuration](#) is incorrect.
The BIND package can be automatically installed by Webmin using APT.

[Install Now](#)

Para realizar la asignación de dirección ip al nombre de una página web deberemos ir al apartado de Servidores, Servidor BIND DNS y crear una máster zona que englobara nuestro dominio `pimpam.com`.⁶

⁶ <https://blog.baehost.com/configuracion-dns-de-dominios-en-virtualmin/>

 Create Master Zone

New master zone options	
Zone type	<input checked="" type="radio"/> Forward (Names to Addresses) <input type="radio"/> Reverse (Addresses to Names)
Domain name / Network	pimpam.com
Records file	<input checked="" type="radio"/> Automatic <input type="radio"/>
Master server	dns.pimpam.com
Email address	pauladolado3@gmail.com
Use zone template?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Add reverses for template addresses?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Refresh time	3600 seconds
Expiry time	1209600 seconds
Transfer retry time	600 seconds
Negative cache time	3600 seconds
IP address for template records	

Seguidamente editaremos esta misma zona y le añadiremos una dirección. Por ejemplo, para el Moodle le asignaremos a la web de Moodle.pimpam.com su dirección ip.

Name	moodle.pimpam.com
Address	192.168.40.12
Update reverse?	<input checked="" type="radio"/> Yes <input type="radio"/> Yes (and replace existing) <input type="radio"/> No

Si nos fijamos en el archivo de configuración nos quedara así, pero debemos tener en cuenta que introduciendo la ip interna solo podremos acceder desde la red interna, modificando las direcciones a los comentadas (direcciones finales una vez realizado el firewall) al estar mapeadas podremos acceder desde fuera de la red interna al Moodle y Odoo.

```

1 $ttl 3600
2 pimpam.com. IN SOA dns.pimpam.com. pauladolado3@gmail.com. (
3                               2023050501
4                               3600
5                               600
6                               1209600
7                               3600 )
8 pimpam.com. IN NS dns.pimpam.com.
9 moodle.pimpam.com.   IN A    192.168.40.12
10 odoo.pimpam.com.   IN A    192.168.40.10
11 'moodle.pimpam.com. IN A    172.17.8.2'
12 'odoo.pimpam.com.   IN A    172.17.8.4'
```

Moodle

Utilizaremos el Moodle como plataforma de aprendizaje la cual nos proporcionara un sistema integrado único para crear nuestro ambiente de enseñanza.⁷

En primer lugar, antes de instalarlo nos hará falta un sistema de base de datos. Hemos elegido MySQL que nos permite almacenar y acceder a los datos a través de múltiples motores de almacenamiento.

Para obtenerlo, actualizaremos el índice de paquetes seguido de la instalación del paquete.

```
# apt install mysql-server
```

Una vez obtenido crearemos la base de datos sobre la que trabajaremos además de un usuario al que le proporcionaremos todos los privilegios asegurados con una contraseña.

```
root@moodle:/# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.32-0ubuntu0.22.04.2 (Ubuntu)

mysql> create database moodle character set utf8mb4 collate utf8mb4_unicode_ci;
Query OK, 1 row affected (0,35 sec)

mysql> create user moodle@localhost identified by 'Pimpam683!';
Query OK, 0 rows affected (0,33 sec)

mysql> grant all privileges on moodle.* to moodle@localhost;
Query OK, 0 rows affected (0,00 sec)

mysql> exit
Bye
```

Al terminar, instalaremos como requisito las extensiones del lenguaje PHP con la versión más actual.

```
# apt install graphviz aspell php8.1-pspell php8.1-curl php8.1-gd
php8.1-intl php8.1-mysql php8.1-xmlrpc php8.1-ldap php8.1-zip
```

Seguidamente, nos descargaremos el paquete desde el repositorio oficial de Moodle a través del comando wget.

```
root@srvmoodle:/# wget https://download.moodle.org/download.php/direct/stable401/moodle-latest-401.tgz
--2023-03-10 16:23:47--  https://download.moodle.org/download.php/direct/stable401/moodle-latest-401.tgz
Resolving download.moodle.org (download.moodle.org)... 172.67.26.233, 104.22.64.81, 104.22.65.81, ...
Connecting to download.moodle.org (download.moodle.org)|172.67.26.233|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 64815123 (62M) [application/gzip]
Saving to: 'moodle-latest-401.tgz'

moodle-latest-401.tgz      63%[=====]          ] 39,24M 11,2MB/s    eta 3s
```

Descomprimiremos, el paquete descargado y lo moveremos al repositorio siguiente. Además, en el mismo nivel crearemos otro directorio llamado moodledata al que le cambiaremos la propiedad.

```
# tar xf Moodle-latest-401.tgz -C /var/www/html
```

⁷ <https://comoinstalar.me/como-instalar-moodle-en-ubuntu-22-04-lts/>
https://docs.moodle.org/all/es/Guia_de_instalacion_paso-a-paso_para_Ubuntu

```
# mkdir /var/www/moodledata
# chown www-data: /var/www/{moodledata, html/moodle}
```

Una vez listo, accederemos vía web con la ip de la máquina virtual para iniciar la instalación del moodle.

En primer lugar, seleccionaremos el idioma con que el que querremos ver la configuración. Nos aseguraremos de que estén bien indicados los directorios en los que tenemos el Moodle e ingresar donde es almacenada los datos (/var/www/moodledata).

A continuación, escribiremos los datos para acceder y verificar el acceso a la base de datos.

Database host
localhost
Database name
moodle
Database user
pimpamadmin
Database password
Pimpam683!
Tables prefix
mdl_

Cuando los datos necesarios hayan sido ingresados se procederá a hacer una serie de comprobaciones antes de empezar el proceso. En nuestro caso, se nos muestra un error con el límite máximo de php.

Other checks

Information	Report	Plugin Status
max_input_vars	🔗 this test must pass ✗ PHP setting max_input_vars must be at least 5000.	Check
site not https	🔗 if this test fails, it indicates a potential problem ✗ It has been detected that your site is not secured using HTTPS. It is strongly recommended to migrate your site to HTTPS for increased security and improved integration with other systems.	Check

Solucionaremos este problema desde la terminal del dispositivo, en la ruta de /etc/php/8.1/apache2/php.ini buscaremos la línea que indica la constante max_input_vars del error y estableceremos 5000 para poder aprobar la comprobación.

```
; How many GET/POST/COOKIE input variables may be accepted
max_input_vars = 5000
```

Your server environment meets all minimum requirements.

x

[Continue](#)

Para finalizar, estableceremos una serie de datos generales como el nombre de la web además de un acrónimo y crearemos el usuario del Moodle.

Site home settings

Full site name fullname	Academia PimPam 2023
Short name for site (eg single word) shortname	Academia PimPam

Para el mantenimiento del Moodle crearemos una tarea programada en el servicio de cron llamado moodle con la siguiente linea como contenido.

```
root@moodle:~# nano /etc/cron.d/moodle
root@moodle:~# cat /etc/cron.d/moodle
*/1 * * * * www-data /usr/bin/php /var/www/html/moodle/admin/cli/cron.php
```

Una vez guardado, la tarea se lanzará de manera regular en un intervalo de 1 minuto.

Para no tener que acceder introduciendo /Moodle editaremos los siguientes archivos para que aparezca directamente con nuestro dominio.

En primer lugar, editaremos el archivo /var/www/html/Moodle/config.php y le indicaremos en el parámetro de CFG root la dirección.

```
$CFG->wwwroot = 'http://moodle.pimpam.com';
```

Y en el documento de la configuración del apache introduciremos en el DocumentRoot el directorio donde se encuentra el archivo de configuración del Moodle editarla anteriormente (/var/www/html/Moodle/).

Una vez hecho, reiniciamos el servicio del apache con el comando siguiente y ya funcionará.

```
# systemctl reload apache2
```

Ldap

Para vincular los usuarios del dominio con el Moodle deberemos habilitar el plug in de LDAP server.

Name	Users	Enable	Up/Down	Settings	Test settings	Uninstall
Manual accounts	2			Settings		
No login	0					
Email-based self-registration	0			Settings		Uninstall
LDAP server	0			Settings	Test settings	

Una vez activo, rellenaremos los datos siguientes dentro de la configuración del anterior. Siendo así, la dirección ip del active directory junto al usuario y contraseña de administrador con la siguiente estructura: cn=Administrador,cn=Users,dc=pimpam,dc=local

LDAP server settings

Host URL
auth_ldap | host_url Default: Empty

Bind settings

<p>Prevent password caching auth_ldap preventpassinDB</p> <p>Distinguished name auth_ldap bind_dn</p> <p>Password auth_ldap bind_pw</p>	<p>No <input type="button" value="▼"/> Default: No</p> <p>Select yes to prevent passwords from being stored in Moodle's DB.</p> <p>cn=Administrador,cn=Users,dc=pimpam <input type="button" value="▼"/> Default: Empty</p> <p>If you want to use bind-user to search users, specify it here. Something like 'cn=ldapuser,ou=public,o=org'</p> <p>..... <input type="button" value="▼"/> <input type="button" value="eye"/></p> <p>Password for bind-user.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Seleccionaremos el tipo de usuario del que se trata y como contexto le indicaremos a raíz de que unidad organizativa queremos que localice los usuarios, al tener una estructura en forma de árbol marcaremos las opciones siguientes para que también incluya los de dentro de otras unidades de Escola y todos sus alias.

<p>User type auth_ldap user_type</p> <p>Contexts auth_ldap contexts</p> <p>Search subcontexts auth_ldap search_sub</p> <p>Dereference aliases auth_ldap opt_deref</p> <p>User attribute auth_ldap user_attribute</p> <p>Object class auth_ldap objectclass</p>	<p>MS ActiveDirectory <input type="button" value="▼"/> Default: Default</p> <p>Select how users are stored in LDAP. This setting also specifies the context where users are located.</p> <p>ou=escola,dc=pimpam,dc=local <input type="button" value="▼"/> Default: Empty</p> <p>List of contexts where users are located. Separate different contexts by commas.</p> <p>Yes <input type="button" value="▼"/> Default: No</p> <p>Search users from subcontexts.</p> <p>Yes <input type="button" value="▼"/> Default: No</p> <p>Determines how aliases are handled during search. Select 'Yes' if you want to dereference aliases.</p> <p>samaccountname <input type="button" value="▼"/> Default: Empty</p> <p>(objectClass=user) <input type="button" value="▼"/></p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

A estos usuarios le asignaremos el atributo mostrado en la imagen y una clase que haga referencia a usuarios sin permisos, es decir, alumnos.

Además, también marcaremos la característica de caducidad y nos avisara con ciertos días de antelación.

System role mapping

<p>Manager context auth_ldap managercontext</p> <p>Course creator context auth_ldap coursecreatorcontext</p>	<p>cn=ESO,ou=Escola,o=pimpam;cn=CF <input type="button" value="▼"/> Default: Empty</p> <p>LDAP context used to select for Manager mapping. Separate multiple groups with ','. Usually something like "cn=manager,ou=first-ou-with-role-groups,o=myorg; cn=manager,ou=second-ou-with-role-groups,o=myorg".</p> <p> <input type="button" value="▼"/> Default: Empty</p> <p>LDAP context used to select for Course creator mapping. Separate multiple groups with ','. Usually something like "cn=coursecreator,ou=first-ou-with-role-groups,o=myorg; cn=coursecreator,ou=second-ou-with-role-groups,o=myorg".</p>
--------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Mapearemos las unidades organizativas principales para mantenerlas en grupos diferentes y organizadas:

cn=ESO,ou=Escola,o=pimpam;cn=CFGM Comerç i màrketin,ou=Escola, o=pimpam.

A continuación, mantendremos la sincronización de los usuarios activa, en caso de suspender una cuenta por algún motivo dicho usuario no podrá acceder al Moodle desde su desactivación.

Synchronise local user suspension status
auth_ldap | sync_suspended

Yes Default: No

Subnet
auth_ldap | ntimsso_subnet

192.168.40.0/24 Default: Empty

Para acabar con la configuración de red le indicaremos la subred de la que parte el Moodle.

Finalizando con la configuración, estableceremos unos atributos para que sean los datos de los usuarios bien seleccionados al campo correspondiente y le indicaremos que se actualice en cada inicio de sesión y en cada actualización, de esta manera siempre estará al día.

Data mapping (First name) auth_ldap field_map_firstname	givenname	Default: Empty
Update local (First name) auth_ldap field_updatelocal_firstname	On every login	Default: On creation
Update external (First name) auth_ldap field_updateremote_firstname	On update	Default: Never
Lock value (First name) auth_ldap field_lock_firstname	Unlocked	Default: Unlocked
Data mapping (Last name) auth_ldap field_map_lastname	sn	Default: Empty
Update local (Last name) auth_ldap field_updatelocal_lastname	On every login	Default: On creation
Update external (Last name) auth_ldap field_updateremote_lastname	On update	Default: Never
Lock value (Last name) auth_ldap field_lock_lastname	Unlocked	Default: Unlocked
Data mapping (Email address) auth_ldap field_map_email	mail	Default: Empty
Update local (Email address) auth_ldap field_updatelocal_email	On every login	Default: On creation
Update external (Email address) auth_ldap field_updateremote_email	On update	Default: Never
Lock value (Email address) auth_ldap field_lock_email	Unlocked	Default: Unlocked

Add new category

Una vez, los usuarios ya estén listos podremos crear unas categorías para englobar los cursos como, por ejemplo, idiomas.

Parent category

Category name

Category ID number

Cuando la etiqueta este creada, añadiremos un curso con el nombre de la asignatura y sus fechas de inicio a fin. Dentro de estos cursos se pueden añadir documentos, texto simple, imágenes e incluso medallas en forma de premio.

Add a new course

[Expand all](#)

General

Course full name ! ?	Anglès
Course short name ! ?	Anglès
Course category ! ?	x Idioma
Search ▼	
Course visibility ?	Show ▼
Course start date ?	5 ▼ September ▼ 2023 ▼ 00 ▼ 00 ▼ CALENDAR
Course end date ?	1 ▼ May ▼ 2024 ▼ 00 ▼ 00 ▼ CALENDAR <input checked="" type="checkbox"/> Enable
Course ID number ?	11

De forma general dentro de la categoría de Gestión podremos ver las unidades formativas siguientes en caso de ciclo junto a sus categorías.

Manage course categories and courses

Course categories

<input type="button"/>	Idioma	01	eye up down lock dropdown	1 grad	
<input type="button"/>	Gestió	02	eye up down lock dropdown	8 grad	
<input type="button"/>	Formació	03	eye up down lock dropdown	2 grad	
<input type="button"/>	Disseny	04	eye up down lock dropdown	2 grad	
<input type="button"/>	ESO	00	eye up down lock dropdown	7 grad	

Sorting

Selected categories ▼

Sort by Category name ascending ▼

Sort by Course full name ascending ▼

Sort ▼

Move selected categories to ▼

Choose... ▼ Move ▼

Gestió

<input type="button"/>	MP06 Investigació comercial	06	gear copy trash eye up down		
<input type="button"/>	MP08 Mitjans i suports de comunicació	08	gear copy trash eye up down		
<input type="button"/>	MP03 Gestió econòmica i finançera de l'empresa	03	gear copy trash eye up down		
<input type="button"/>	MP09 Aplicacions bàsiques d'ofimàtica	09	gear copy trash eye up down		
<input type="button"/>	MP10 Preparació de comandes i venda de productes	10	gear copy trash eye up down		
<input type="button"/>	MP04 Processos de venda	04	gear copy trash eye up down		
<input type="button"/>	MP05 Gestió de compres	05	gear copy trash eye up down		
<input type="button"/>	MP01 Dinamització punt de venda	01	gear copy trash eye up		

En la categoría de la ESO nos encontraremos las asignaturas siguientes vistas desde fuera de la configuración:

My courses

Course overview

The screenshot shows a grid of six course cards. Each card has a colored background (blue, grey, red, yellow, pink, blue) and contains the name of the subject and level (e.g., Biología ESO). There are three rows of two columns each. Each card has a vertical ellipsis icon on its right side.

Subject	Level
Biología	ESO
Educació Física	ESO
Geografía	ESO
Llengua Castellana	ESO
Llengua Catalana	ESO
Llengua Extrangera	ESO

A más a más, para que los usuarios vean las asignaturas que tienen asignadas por curso escolar los deberemos añadir como participantes.

First name / Last name	Username	ID number	Email address	Roles	Groups	Last access to course	Status
IC Iago Cabello	i.cabello		I.Cabello@pimpam.local	Student	No groups	Never	Active Info Settings Delete
PD Paula Dolado	p.dolado		P.Dolado@pimpam.local	Student	No groups	6 days 23 hours	Active Info Settings Delete
MR Miquel Romero	m.romero		M.Romero@pimpam.local	Student	No groups	Never	Active Info Settings Delete
AU Admin User	admin		pauladolado3@gmail.com	Teacher	No groups	2 secs	Active Info Settings Delete

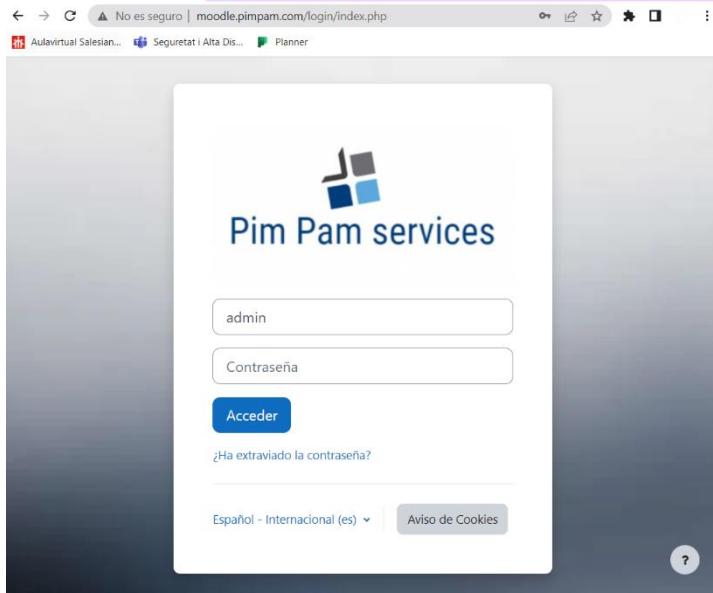
First name / Last name	Username	ID number	Email address	Roles	Groups	Last access to course	Status
AA Andrea Arandna	a.aranda			Student	No groups	Never	Active Info Settings Delete
AD Aina Dolado	a.dolado		A.Dolado@pimpam.local	Student	No groups	Never	Active Info Settings Delete
DL David Lopez	d.lopez		D.Lopez@pimpam.local	Student	No groups	Never	Active Info Settings Delete
AU Admin User	admin		pauladolado3@gmail.com	Teacher	No groups	4 secs	Active Info Settings Delete

De esta manera al momento de inicio de sesión podrán ver solo los cursos en los que están enrollados, en caso de no estar matriculado en ninguno no podrán acceder.

Para finalizar, hemos realizado una serie de ampliaciones que nos ayudaran a visualizar nuestro Moodle de manera más agradable además de facilitar o liminar otras acciones.

En primera instancia, la estructura del Moodle parte de una página principal, a raíz de esta puedes acceder iniciando sesión, pero como veíamos que la página principal es poco funcional el cuanto a conceptos ya que solo es una visualización previa modificamos la configuración para

que no apareciera y pese a escribir la dirección correcta te redirige instantáneamente al acceso para iniciar sesión.



Además, quisimos bloquear el acceso a usuarios invitados puesto que no estarían inscritos en ningún curso y en los mismos solo queremos que puedan ver y participar los propios usuarios.

Para que fuera más agradable en vez de contener un tema simple agregamos como logo nuestra propia empresa, pusimos un fondo y otro logo mostrado en la página inicial como botón inicio del menú.



Odoo

```
# pipenv run odoo
GNU nano 6.2
odoo install.sh
#!/bin/bash
#####
# Script for installing Odoo on Ubuntu 16.04, 18.04 and 20.04 (could be used for other version too)
# Author: Yenthe Van Ginneken
#
# This script will install odoo on your Ubuntu 16.04 server. It can install multiple Odoo instances
# in one Ubuntu because of the different xmlrpc ports
#
# Make a new file:
# sudo nano odoo-install.sh
# Place this content in it and then make the file executable:
# sudo chmod +x odoo-install.sh
# Execute the script to install Odoo:
# ./odoo-install
#####

OE_USER="odoo"
OE_HOME="/$OE_USER"
OE_HOME_EXT="/$OE_USER/$OE_USER-server"
# The default port where this Odoo instance will run under (provided you use the command -c in the terminal)
# Set to true if you want to install it, false if you don't need it or have it already installed.
INSTALL_WKHTMLTOPDF="True"
# Set the default Odoo port (you still have to use -c /etc/odoo-server.conf for example to use this.)
OE_PORT="8069"
# Choose the odoo version which you want to install. For example: 16.0, 15.0, 14.0 or saas-22. When using 'master' the master version will be installed.
# IMPORTANT! This script contains extra libraries that are specifically needed for Odoo 16.0
OE_VERSION="16.0"
# Set this to True if you want to install the Odoo enterprise version!
IS_ENTERPRISE="False"
# Installs postgresQL V14 instead of defaults (e.g V12 for Ubuntu 20.04) - this improves performance
INSTALL_POSTGRESQL_FOURTEEN="True"
# Set this to True if you want to install Nginx!
INSTALL_NGINX="False"
# Set the superadmin password - if GENERATE_RANDOM_PASSWORD is set to "True" we will automatically generate a random password, otherwise we use this one
OE_SUPERADMIN="admin"
# Set to "True" to generate a random password, "False" to use the variable in OE_SUPERADMIN
GENERATE_RANDOM_PASSWORD="False"
OE_CONFIG="$OE_USER-server"
# Set the website name
WEBSITE_NAME=""
# Set the default Odoo longpolling port (you still have to use -c /etc/odoo-server.conf for example to use this.)
LONGPOLLING_PORT="8072"
# Set to "True" to install certbot and have ssl enabled, "False" to use http
ENABLE_SSL="True"
# Provide Email to register ssl certificate
ADMIN_EMAIL="odoo@example.com"
```

Aquí indicaremos el puerto y cambiaremos el parámetro para que no realice una contraseña, si indicamos ninguna la del root automáticamente.

```

root@srvcon:/odo# sudo ./odoo_install.sh

---- Update Server ----
Adding component(s) 'universe' to all repositories.
Press [ENTER] to continue or Ctrl-c to cancel.
Obj:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Des:3 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Des:4 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:5 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [948 kB]
Des:6 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [890 kB]
Des:7 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [18,1 kB]
Des:8 http://archive.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [8,832 B]
Des:9 http://archive.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [710 kB]
Des:10 http://archive.ubuntu.com/ubuntu jammy-security/universe Translation-en [115 kB]
Des:11 http://archive.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [13,8 kB]
Des:12 http://archive.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [19,4 kB]
Des:13 http://archive.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [4.068 B]
Descargados 3.063 kB en 2s (1.425 kB/s)
Leyendo lista de paquetes... Hecho
Repository: 'deb http://mirrors.kernel.org/ubuntu/ xenial main'
Description:
Archive for codename: xenial components: main
More info: http://mirrors.kernel.org/ubuntu/
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.

```

Tras iniciar el script solo tendremos que aceptar las instalaciones que aparecerán.
Tras esto podremos acceder indicando el puerto que hemos seleccionado el 8069

Iniciaremos sesión con la cuenta que acabamos de añadir y nos dirigiremos a ajustes de compañías

Aquí cambiaremos el nombre y la imagen. Y ahora al acceder aparecerá el logo de la compañía



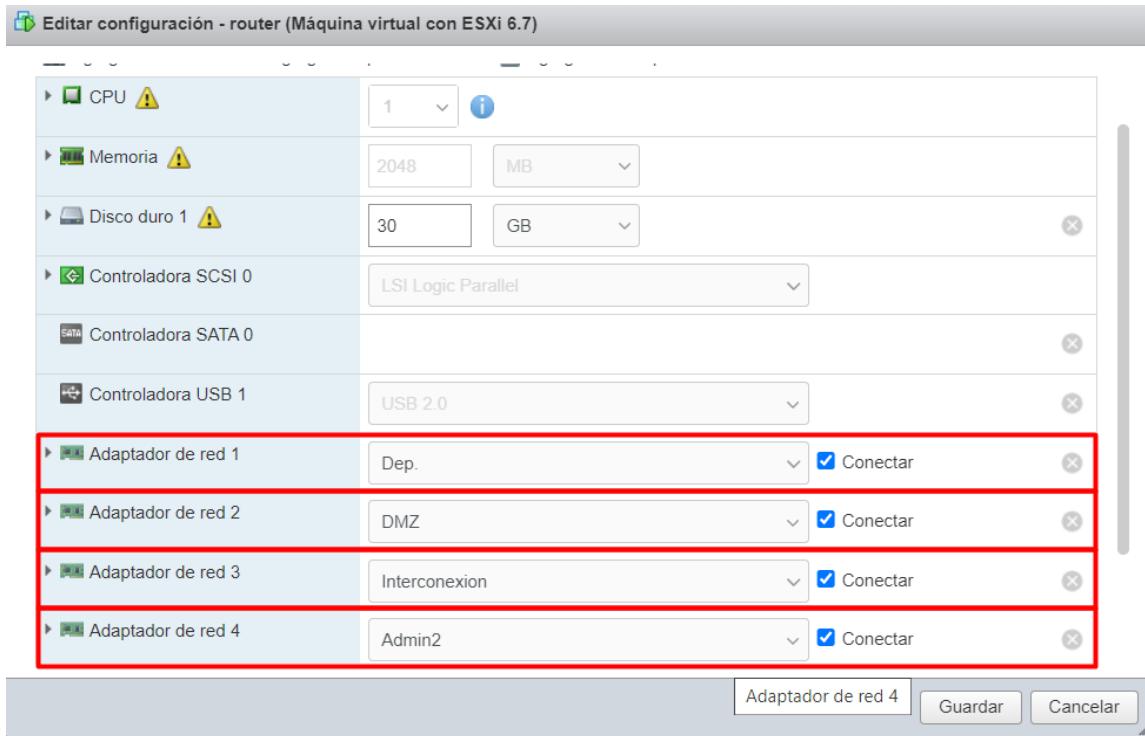
Bloque 4 | Firewall frontal

Router Frontal

Para el router frontal hemos optado por un servidor Ubuntu 22.04 ya que la configuración de este la tenemos muy por la mano.

Una vez instalada la máquina virtual en el ESXI pasamos a configurar las tarjetas de red que va a utilizar nuestra máquina. Este está conectado a tres redes, DMZ, interconexión y al departamento. Además, le añadiremos una cuarta tarjeta de red para poder administrarlo.

Como se puede observar en la siguiente imagen, hemos creado cuatro tarjetas de red para el router y les hemos asignado su correspondiente puerto de grupo.



Es entonces cuando encendemos el router y le vamos a configurar las IPs desde el netplan.

A continuación, se puede observar una captura de pantalla de la configuración de red del router.

En este punto ya tenemos conexión a internet.

```
# This is the network config written by 'pimpmam'
network:
  version: 2
  ethernets:
    ens160:
      dhcp4: false
      addresses: [172.17.8.2/16]
      gateway4: 172.17.0.100
      nameservers:
        addresses: [8.8.8.8]
    ens192:
      dhcp4: false
      addresses: [192.168.40.1/24]
      gateway4: 172.17.8.2
    ens224:
      dhcp4: false
      addresses: [192.168.20.1/24]
      gateway4: 172.17.8.2
    ens36:
      dhcp4: false
      addresses: [192.168.10.1/24]
      gateway4: 172.17.8.2
```

Como la maquina hará función de enrutador, con la configuración que está no reencaminará los paquetes que le vengan de otras máquinas. Para que así sea, debemos cambiar el valor de un archivo. Dicho archivo es `/proc/sys/net/ipv4/ip_forward` por defecto, en ese archivo encontraremos un 0, nosotros lo debemos cambiar a 1. Para ello se puede ir al archivo y modificarlo manualmente o podemos ejecutar este comando: `sudo echo "1" > /proc/sys/net/ipv4/ip_forward`

El siguiente paso es configurar el firewall, inicialmente para hacer pruebas vamos a permitir todo el tráfico. Para la configuración del firewall utilizaremos los [iptables](#). Creamos una carpeta llamada `fw` (firewall) en `/etc/` y creamos un archivo dentro llamado `fw.sh`.

A continuación, se muestra una imagen de la configuración de nuestro archivo.

```
sudo iptables -F  
sudo iptables -X  
sudo iptables -Z  
  
iptables -P INPUT ACCEPT  
iptables -P OUTPUT ACCEPT  
iptables -P FORWARD ACCEPT  
  
iptables -t nat -A POSTROUTING -o ens160 -j MASQUERADE
```

Una vez lo tengamos, le vamos a dar formato de ejecutable. Para ello utilizaremos el comando chmod de esta manera:

```
$ Sudo chmod +x fw.sh
```

Ahora que se puede ejecutar lo debemos ejecutar automáticamente cada vez que se inicie el router.

Para ello, introduciremos la ruta del script en el archivo crontab. Primero abrimos el archivo con el comando `sudo crontab -e` una vez dentro, introducimos el siguiente comando:

```
@reboot sudo /etc/fw/fw.sh
```

De esta manera cada vez que se inicie el sistema se ejecutará el archivo. Para comprobar que funciona reiniciamos el router y una vez iniciado miramos los logs del cron con el siguiente comando:

```
$ grep CRON /var/Log/sysLog
```

Como podemos ver en la imagen, se ha ejecutado correctamente nuestro script

```
Mar  3 16:12:46 router1 CRON[914]: (root) CMD (sudo /etc/fw/fw.sh)
```

En este punto ya tenemos conexión desde las máquinas de dentro hacia el exterior

```

Red_dmz=192.168.40.0/24
Red_ext=172.17.0.0/16
Red_admin=192.168.10.0/24
Red_inter=192.168.20.0/24

Nic_admin=ens36
Nic_ext=ens160
Nic_dmz=ens192
Nic_inter=ens224

Ip_pfSense=192.168.20.2
Ip_moodle=192.168.40.12
Ip_odoo=192.168.40.10
Ip_dns=192.168.40.18
Ip_router=172.17.8.2
Ip_router2=172.17.8.4

sudo echo "1" > /proc/sys/net/ipv4/ip_forward
sudo iptables -F
sudo iptables -X
sudo iptables -Z
sudo iptables -t nat -F

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD ACCEPT

#
iptables -A FORWARD -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -p udp --sport 53 -j ACCEPT

iptables -t nat -A POSTROUTING -s $Red_dmz -o $Nic_ext -j MASQUERADE
iptables -t nat -A POSTROUTING -s $Red_inter -o $Nic_ext -j MASQUERADE
iptables -t nat -A POSTROUTING -s $Red_admin -o $Nic_ext -j MASQUERADE

# Conexiones loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

```

```

# Ping desde cualquier sitio
iptables -A FORWARD -p icmp --icmp-type echo-request -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT

# Ping al router y desde el router
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

# trafico desde interconexion hacia fuera
iptables -A FORWARD -i $Nic_inter -o $Nic_ext -j ACCEPT
iptables -A FORWARD -i $Nic_ext -o $Nic_inter -j ACCEPT

# desde admin hacia fuera
iptables -A FORWARD -i $Nic_admin -o $Nic_ext -j ACCEPT
iptables -A FORWARD -i $Nic_ext -o $Nic_admin -j ACCEPT

# SSH router desde fuera y desde la red de admin
iptables -A INPUT -i $Nic_ext -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -o $Nic_ext -p tcp --sport 22 -j ACCEPT
iptables -A INPUT -i $Nic_admin -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -o $Nic_admin -p tcp --sport 22 -j ACCEPT

# Mapear puerto udp:53 del dns publico en la wan
iptables -t nat -A PREROUTING -i $Nic_ext -d $Ip_router -p udp --dport 53 -j DNAT --to-destination $Ip_dns
iptables -A FORWARD -i $Nic_ext -o $Nic_dmz -p udp --dport 53 -d $Ip_dns -j ACCEPT
iptables -A FORWARD -i $Nic_dmz -o $Nic_ext -p udp --sport 53 -s $Ip_dns -j ACCEPT
#iptables -t nat -A POSTROUTING -s 172.17.0.0/16 -p udp --dport 53 -d $Ip_dns -j SNAT --to $Ip_router

# Peticiones del DNS desde DMZ hacia WAN
iptables -A FORWARD -i $Nic_dmz -o $Nic_ext -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i $Nic_ext -o $Nic_dmz -p udp --sport 53 -j ACCEPT

# Peticiones DNS desde DMZ a la IP publica del enrutador
iptables -t nat -A PREROUTING -i $Nic_dmz -s $Red_dmz -d $Ip_router -p udp --dport 53 -j DNAT --to-destination $Ip_dns
iptables -A FORWARD -s $Red_dmz -d $Ip_dns -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -s $Red_dmz -d $Red_dmz -p udp --sport 53 -j ACCEPT
iptables -t nat -A POSTROUTING -o $Nic_dmz -s $Red_dmz -d $Ip_dns -p udp --dport 53 -j SNAT --to $Ip_router

```

```

# Moodle visible
iptables -t nat -A PREROUTING -d $Ip_router -p tcp --dport 80 -j DNAT --to-destination $Ip_moodle
iptables -A FORWARD -d $Ip_moodle -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s $Ip_moodle -p tcp --sport 80 -j ACCEPT
#iptables -t nat -A POSTROUTING -p tcp --dport 80 -d $Ip_moodle -j SNAT --to $Ip_router
iptables -t nat -A POSTROUTING -s $Red_dmz -p tcp --dport 80 -d $Ip_moodle -j MASQUERADE
iptables -t nat -A POSTROUTING -s $Red_admin -p tcp --dport 80 -d $Ip_moodle -j MASQUERADE

# Odoo visible desde fuera
iptables -t nat -A PREROUTING -d $Ip_router2 -p tcp --dport 80 -j DNAT --to-destination $Ip_odoo:8069
iptables -A FORWARD -d $Ip_odoo -p tcp --dport 8069 -j ACCEPT
iptables -A FORWARD -s $Red_dmz -p tcp --sport 8069 -j ACCEPT
iptables -t nat -A POSTROUTING -s $Red_dmz -p tcp --dport 8069 -d $Ip_odoo -j SNAT --to $Ip_router2

# Actualizaciones del sistema de las maquinas de DMZ
iptables -A FORWARD -s $Red_dmz -o $Nic_ext -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i $Nic_ext -o $Red_dmz -p tcp --sport 443 -j ACCEPT
iptables -A FORWARD -i $Red_dmz -o $Nic_ext -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i $Nic_ext -o $Red_dmz -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -s $Red_dmz -i $Nic_dmz -o $Nic_ext -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -i $Nic_ext -o $Nic_dmz -d $Red_dmz -p tcp --sport 21 -j ACCEPT

# Permitir actualizaciones de la zona slave DNS
iptables -t nat -A PREROUTING -d $Ip_router -i $Nic_ext -p tcp --dport 53 -j DNAT --to-destination $Ip_dns
iptables -A FORWARD -i $Nic_ext -o $Nic_dmz -d $Red_dmz -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s $Red_dmz -i $Nic_dmz -o $Nic_ext -p tcp --sport 53 -j ACCEPT

#Permitir VPN
iptables -t nat -A PREROUTING -d $Ip_router -i $Nic_ext -p udp --dport 51820 -j DNAT --to-destination $Ip_pfSense
iptables -A FORWARD -i $Nic_ext -o $Nic_inter -p udp --dport 51820 -j ACCEPT
iptables -A FORWARD -i $Nic_inter -o $Nic_ext -p udp --sport 51820 -j ACCEPT

#Actualizaciones de router
iptables -A INPUT -i $Nic_ext -p tcp --sport 80 -j ACCEPT
iptables -A INPUT -i $Nic_ext -p tcp --sport 443 -j ACCEPT
iptables -A INPUT -i $Nic_ext -p tcp --sport 21 -j ACCEPT
iptables -A OUTPUT -o $Nic_ext -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -o $Nic_ext -p tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -o $Nic_ext -p tcp --dport 21 -j ACCEPT

```

```

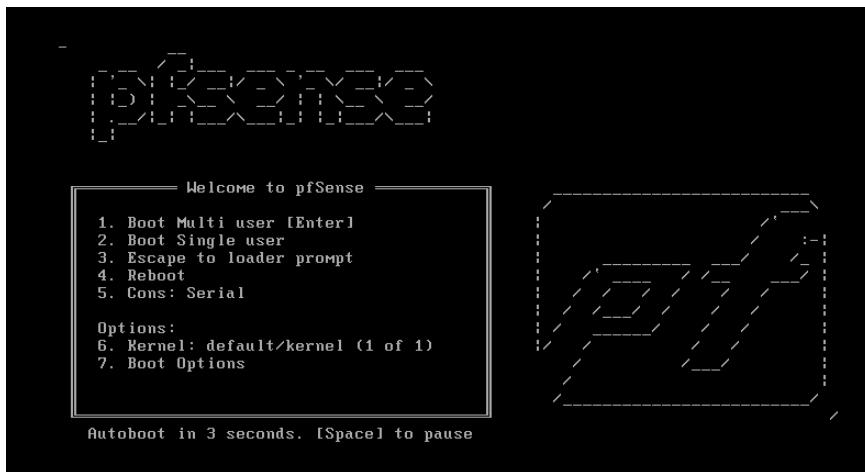
#Peticiones DNS del router
iptables -A INPUT -i $Nic_ext -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -o $Nic_ext -p udp --dport 53 -j ACCEPT

#Monitoreo zabbix
iptables -A INPUT -i $Nic_admin -p tcp --dport 10050 -j ACCEPT
iptables -A OUTPUT -o $Nic_admin -p tcp --sport 10050 -j ACCEPT

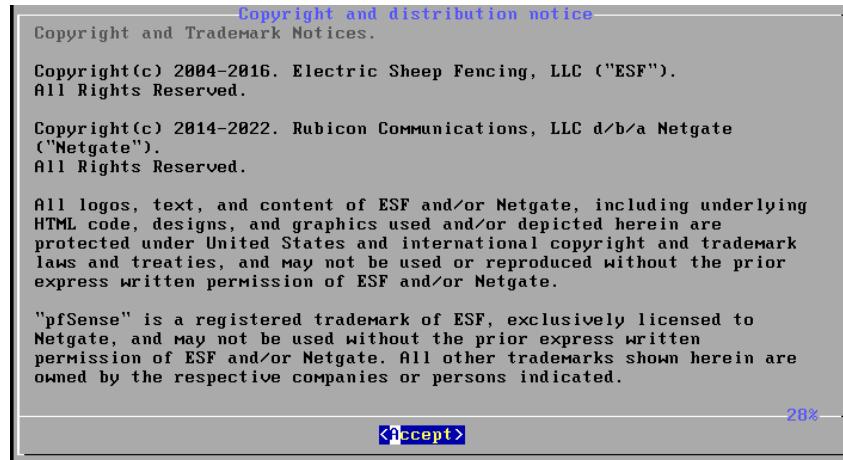
```

Router PfSense

Una vez encendida ya la máquina, no hace falta tocar una tecla, como vemos, al pasar tres segundos, se enciende sola.



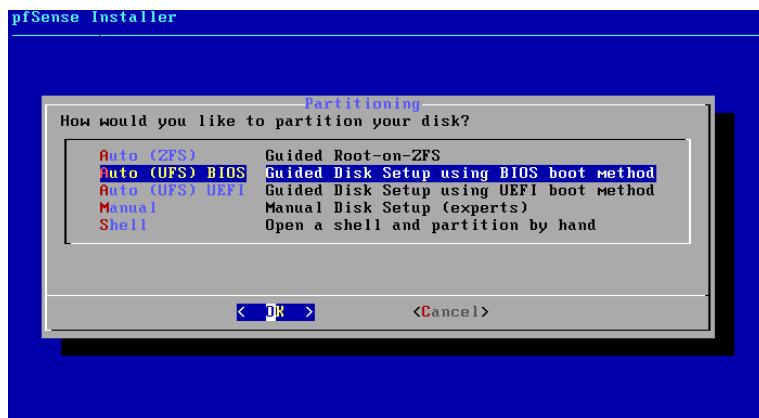
La primera pantalla hay que aceptarla, son las condiciones de uso.



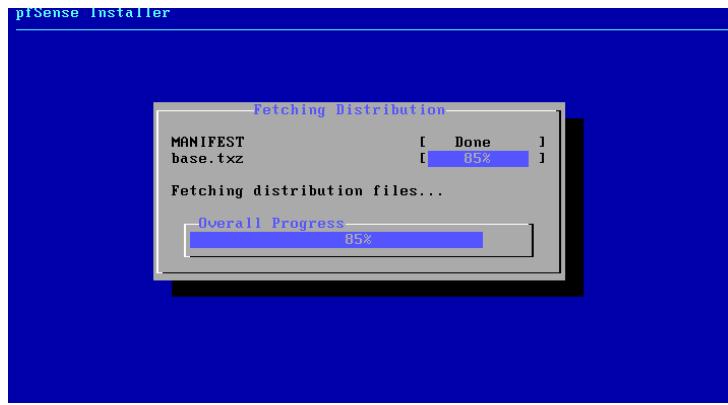
Seleccionamos que queremos instalar pfSense y en la siguiente pantalla, seleccionamos el teclado que tengamos.



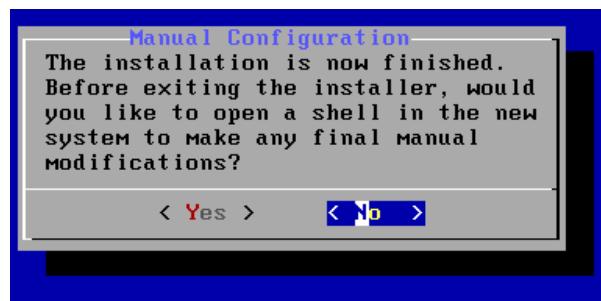
Por más facilidad, escogeremos la BIOS en este caso.



Y como se puede observar, la instalación comenzará automáticamente.



Una vez acabada la instalación decimos que no queremos hacer ningún cambio y procedemos a rebootear la máquina.



Al iniciarse la máquina, nos aparecerá el menú principal. Como se puede ver, aparecen ambas redes con sus correspondientes IPs.

```
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 6fe8b29ff1ceb36061f3

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

INTER (wan)      -> vmx1      -> v4: 192.168.20.2/24
ESCOLA (lan)     -> vmx0      -> v4: 192.168.30.2/24
ADMIN (opt1)     -> em0       -> v4: 192.168.10.2/24
WG_VPN (opt2)    -> tun_wg0    -> v4: 10.200.0.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

```

VMware Virtual Machine - Netgate Device ID: 2797efce2e4c82b645d2
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.93/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static) ←

Enter the number of the interface you wish to configure: 2

```

Y escoger la red que queremos editar, en mi caso la 2.

```

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.2.0/24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.2.100
Enter the end address of the IPv4 client address range: 192.168.2.200

```

Finalmente podemos ver que la ip ha cambiado

```

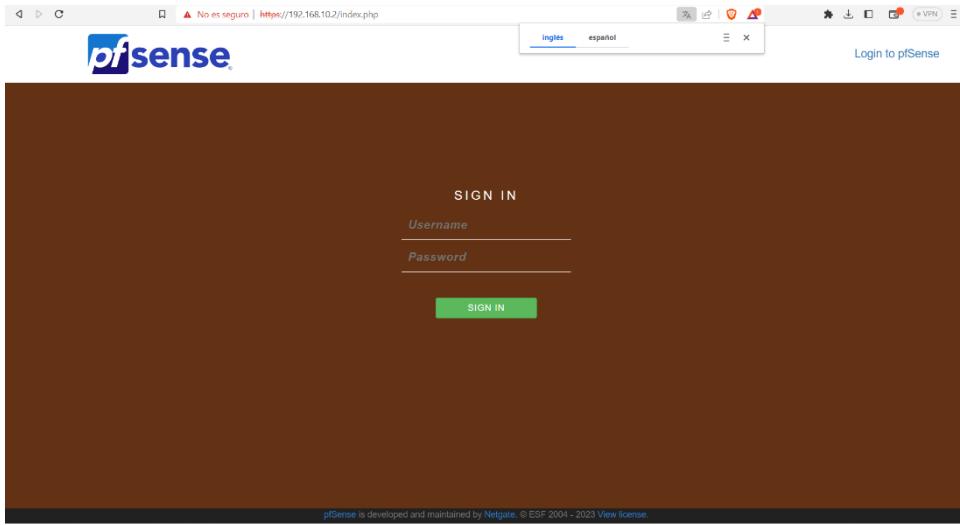
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.2.93/24
LAN (lan)      -> em1      -> v4: 192.168.2.1/24 ←

```

Reglas del firewall y redireccionamiento

Para la configuración del router, entraremos a la interfaz gráfica introduciendo la ip de nuestro router. El usuario por defecto es **Admin** y la contraseña **pfSense**. Una vez dentro cambiaremos la contraseña a una segura ya que la seguridad nos importa. La guardaremos en una aplicación como el **Keypass**.

Si la página no aparece puede ser por culpa del firewall. Para desactivarlo, nos vamos al menú del router, la opción 8 que es la Shell y escribimos “*pfctl -d*”.



Por defecto desactivaremos el firewall hasta crear las reglas definitivas.

VPN

Para la VPN vamos a utilizar Wireguard. WireGuard es un protocolo de red VPN (Virtual Private Network) de código abierto y de última generación. VPN es una tecnología que permite crear una conexión segura entre dos redes a través de Internet, de manera que los datos que se transfieren entre ellas estén protegidos y encriptados.

WireGuard se caracteriza por su simplicidad, eficiencia y seguridad. Utiliza criptografía moderna, como Curve25519 para el intercambio de claves y ChaCha20 para el cifrado, lo que lo hace más rápido y seguro que otros protocolos VPN como OpenVPN e IPsec. Además, tiene un diseño minimalista que facilita su configuración y mantenimiento.

WireGuard se puede utilizar en diversos sistemas operativos, como Linux, macOS, Windows, Android y iOS, y su implementación está disponible en forma de módulo de kernel para Linux y como una aplicación de usuario en otros sistemas.

Primero de todo tenemos que instalar el paquete de WireGuard desde la ventana de paquetes.

Podemos ver en las siguientes capturas la configuración por la que he optado

Name	Description	Public Key	Address / Assignment	Listen Port	Peers	Actions
tun_wg0	Test	k0UcfdhDVaSYI02Si2AQmBxk4MkOtean...	WG_VPN (opt2)	51820	2	

Peers	Description	Public Key	Tunnel	Allowed IPs	Endpoint
WINDOWS PC	G60BC0yHGZXKagUNajipF5IJak8Qwe5DT...		tun_wg0	10.200.0.5/32	Dynamic
Miquel	qa0ZRYo865vozBce5pzM8Vs78kdAvPNx...		tun_wg0	10.200.0.6/32	Dynamic

Primero de todo hay que crear un túnel al que le hemos asignado el nombre de Test.

El puerto lo hemos dejado por defecto, por seguridad estaría bien cambiarlo ya que cualquier programa malicioso probaría los puertos más utilizados y este es uno de ellos.

Vemos que el túnel genera una clave privada y una clave pública. Nos tenemos que guardar la clave publica ya que la utilizaremos posteriormente.

The screenshot shows the 'Tunnels' tab selected in the top navigation bar. The main section is titled 'Tunnel Configuration (tun_wg0)'. It includes fields for 'Enable' (checkbox), 'Description' (text input 'Test'), 'Listen Port' (text input '51820'), and 'Interface Keys' (private key and public key inputs with 'Generate' and 'New Keys' buttons). Below this is the 'Interface Configuration (tun_wg0)' section with 'Assignment' (WG_VPN opt2), 'Interface' (Interface Configuration), and 'Firewall Rules' (Firewall Configuration). At the bottom are 'Peer Configuration' and 'Actions' buttons.

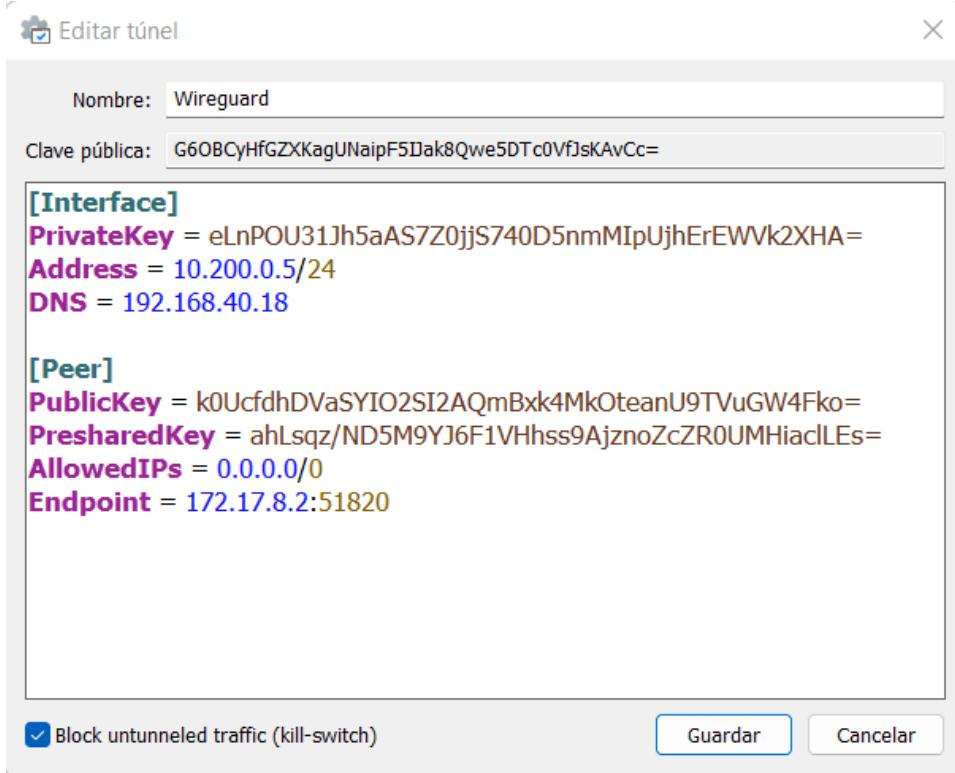
Una vez configurado el túnel vamos a configurar los peers. Un peer se refiere a un dispositivo o nodo que se conecta a la red VPN y que tiene el mismo nivel de acceso y funcionalidad que los demás dispositivos o nodos conectados.

En otras palabras, cada dispositivo o nodo que se conecta a la VPN es considerado un peer, y todos ellos tienen la capacidad de enviar y recibir datos en la red VPN, así como de establecer conexiones seguras entre ellos.

Cada peer tiene una dirección IP única en la red VPN, y puede comunicarse con los demás peers de forma segura a través de túneles encriptados. Esta comunicación segura es posible gracias al uso de protocolos de túnel como el mencionado WireGuard, que permiten el cifrado de los datos que se envían entre los diferentes peers de la VPN.

The screenshot shows the 'Peer Configuration' screen. It includes fields for 'Enable Peer' (checkbox), 'Tunnel' (dropdown 'tun_wg0 (Test)'), 'Description' (text input 'WINDOWS PC'), 'Dynamic Endpoint' (checkbox 'Dynamic'), 'Keep Alive' (text input 'Keep Alive'), 'Public Key' (text input 'G60BCyfHGZXKagUNaipF5lJak8Qwe5DTc0VfJskAvCc=') with 'Generate' and 'New Pre-shared Key' buttons, and 'Pre-shared Key' (text input 'ahLsqzND5M9YJGF1Vhss9AjznoZcZR0UMHiaclEs=') with 'Generate' and 'New Pre-shared Key' buttons. Below this is the 'Address Configuration' section with a hint about allowed IP entries and an 'Add Allowed IP' button.

Como ya hemos creado el túnel, se lo asignamos y en la descripción yo por ejemplo le he puesto el nombre del dispositivo que se va a utilizar el peer creado. Donde aparece la clave pública lo dejamos en blanco de momento y por más seguridad generaremos una pre-shared key. En allowed IPs introducimos la IP que va a tener el dispositivo dentro de la VPN.



Esta es la configuración que tendremos que crear en nuestro dispositivo para podernos conectar a la VPN. La clave privada se genera automáticamente, la clave pública la copiamos y la introducimos en la configuración del peer. Le ponemos la misma IP que hemos decidido en el paso anterior y el DNS.

La clave publica es la que se ha generado cuando hemos creado el túnel y la pre-shared key es la que también hemos generado en la configuración del peer. En allowed IPs introducimos las redes que queremos que pasen a través del túnel, en mi caso poniendo la 0.0.0.0/0 pasarán todas y en endpoint es la IP por donde tiene que entrar para conectarse a la VPN, en nuestro caso es la IP del router frontal en el cual hemos mapeado el puerto hacia el Pfsense

WireGuard Status								
Tunnel	Description	Peers	Public Key	Address / Assignment	MTU	Listen Port	RX	TX
↑ tun_wg0	Test	2	k0UcfdhDVaSYIO2S...	WG_VPN (opt2)	1500	51820	0 B	0 B
Peers								
	Description	Latest Handshake	Public Key	Endpoint	Allowed IPs	RX	TX	
	WINDOWS PC	never	G60BCyHfGZXKagUN...	(none)	10.200.0.5/32	0 B	0 B	
	Miquel	never	qa02RYo865vozBce...	(none)	10.200.0.6/32	0 B	0 B	
Package Versions								
Name	Version		Comment					
pfsense-pkg-WireGuard	0.1.6_2		pfsense package WireGuard (EXPERIMENTAL)					
wireguard-kmod	0.0.20211105		WireGuard implementation for the FreeBSD kernel					
wireguard-tools-lite	1.0.20210914_1		Fast, modern and secure VPN Tunnel (lite flavor)					

Como podemos observar el servidor VPN ya está acabado y activo para poder conectarse.

Proxy

Para el proxy hemos escogido Squid Proxy. Squid es un servidor proxy de código abierto y de alta calidad que se utiliza para mejorar el rendimiento de la red y la seguridad de las conexiones.

Un servidor proxy es un intermediario entre un cliente y un servidor, que se utiliza para mejorar la velocidad y la eficiencia de las conexiones, así como para proteger la privacidad y la seguridad de las comunicaciones.

Squid es un servidor proxy muy popular que funciona en sistemas operativos Unix y Linux, y que se utiliza para mejorar el rendimiento de las conexiones a Internet, acelerando el acceso a los sitios web más visitados y reduciendo el tráfico de red.

Squid también se utiliza para implementar políticas de seguridad en la red, como la restricción del acceso a sitios web específicos, el bloqueo de contenido inapropiado y el filtrado de virus y spam.

Primero de todo instalaremos los paquetes de Squid Proxy server y SquidGuard Proxy.

Vamos primero a la configuración del proxy server.

Squid General Settings	
Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version	IPv4 Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP	none Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.
Proxy Interface(s)	192.168.20.3 () INTER ESCOLA ADMIN The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface	Default (auto) The interface the proxy server will use for outgoing connections.
Proxy Port	3128 This is the port the proxy server will listen on. Default: 3128
ICP Port	 This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface	<input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal	This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First	<input type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP	<input type="checkbox"/> Check this to disable Squid ICMP pinger helper.
Use Alternate DNS Servers for the Proxy Server	 To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

Escogeremos la interfaz de red en el cual queremos aplicar el proxy, por lo demás lo dejamos por defecto.

Filtering									
Max lines:			10 lines	Max. lines to be displayed.					
String filter:									
Enter a grep-like string/pattern to filter the log entries. E.g.: username, IP address, URL. Use ! to invert the sense of matching (to select non-matching lines).									
Squid Access Table									
Date	IP	Status	Squid - Access Logs	User	Destination				
02.05.2023 17:06:28	192.168.30.16	TCP_TUNNEL/200	msftspeechmodelsprod.azureedge.net:443	-	152.199.19.161				
02.05.2023 17:04:53	192.168.30.16	TCP_TUNNEL/200	settings-win.data.microsoft.com:443	-	40.127.240.158				
02.05.2023 17:04:53	192.168.30.16	NONE/200	https:443	-	-				
02.05.2023 17:04:48	192.168.30.16	TCP_TUNNEL/200	settings-win.data.microsoft.com:443	-	40.127.240.158				
02.05.2023 17:04:48	192.168.30.16	NONE/200	https:443	-	40.127.240.158				
02.05.2023 17:04:48	192.168.30.16	TCP_TUNNEL/200	settings-win.data.microsoft.com:443	-	-				
02.05.2023 17:04:48	192.168.30.16	NONE/200	https:443	-	-				
02.05.2023 17:04:39	192.168.30.16	TCP_TUNNEL/200	geover.prod.do.dsp.mp.microsoft.com:443	-	23.51.237.56				
02.05.2023 17:04:39	192.168.30.16	TCP_TUNNEL/200	cp801.prod.do.dsp.mp.microsoft.com:443	-	23.51.237.141				
02.05.2023 17:04:39	192.168.30.16	TCP_TUNNEL/200	kv801.prod.do.dsp.mp.microsoft.com:443	-	23.51.237.141				

Ahora nos vamos al SquidGuard. Primero de todo vemos la configuración de LDAP que dejaremos para más tarde.

General Options	
Enable	<input checked="" type="checkbox"/> Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details .	
The Save button at the bottom of this page must be clicked to save configuration changes.	
To activate squidGuard configuration changes, the Apply button must be clicked .	
✓ Apply	
SquidGuard service state: STARTED	
LDAP Options	
Enable LDAP Filter	<input type="checkbox"/> Enable options for setup ldap connection to create filters with ldap search
LDAP DN	Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)
LDAP DN Password	>Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z]{8}[^`~!@#%^&?={}]
LDAP Cache Time	300 Number of seconds to cache LDAP Results (recommended value: 300)
Strip NT domain name	<input type="checkbox"/> Strip NT domain name component from user names (/ or \ separated).
Strip Kerberos Realm	<input type="checkbox"/> Strip Kerberos Realm component from user names (@ separated).
LDAP Version	Version 3
Service options	
Rewrite process children	16 Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates request queues. Using too many helpers wastes your system resources. (Default: 16)
Rewrite process children startup	8 Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)
Rewrite process children idle	4 Sets a minimum of how many SquidGuard processes Squid is to try and keep available at all times. (Default: 4)

En la pestaña de common ACL veremos las categorías que hemos creado con la opción de prohibirlas, permitirlas... Aquí también podemos configurar que cuando los alumnos busquen alguna url prohibida se les redirija hacia una URL que queramos como el Moodle.

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Target Rules !porn all

Target Rules List + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories

[porn]	access [deny]
[pimpam]	access [whitelist]
Default access [all]	access [allow]

Do not allow IP- Addresses in URL To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

Proxy Denied Error

The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by Sg[product_name] proxy"

Redirect mode ext url redirect (enter URL)

Select redirect mode here.
Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible.
Options ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'

Redirect info https://imgs.search.brave.com/-v7Np7z5VAM0arH5dfbfYhSubCoggnplWhY0CY0gY54/rs:fit:533:225:1/g:ce/aH

Enter external redirection URL, error message or size (bytes) here.

Use SafeSearch engine Enable the protected mode of search engines to limit access to mature content.
At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.
Note: This option overrides 'Rewrite' setting.

Rewrite none (rewrite not defined)

Enter the rewrite condition name for this rule or leave it blank.

Log Check this option to enable logging for this ACL.

Aquí hemos creado una Target categorie para bloquear porno, por si acaso no funcionaba nosotros hemos utilizado otras webs como mytcpip.com y ya cuando lo hemos comprobado hemos puesto las reales.

General Options

Name porn
Enter a unique name of this rule here.
The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Order -----
Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

Domain List mytcpip.com pornhub.com
Enter destination domains or IP-addresses here. To separate them use space.
Example: mail.ru e-mail.ru yahoo.com 192.168.1.1

URL List
Enter destination URLs here. To separate them use space.
Example: host.com/xxx 12.10.220.125/alisa

Aquí podemos también banear por palabras, en nuestro caso banearemos las palabras juegos casino discord y Linux.

Regular Expression	game casino discord linux mytcpip
Enter word fragments of the destination URL. To separate them use . Example: mail casino game \ .rsdf\$	
Redirect mode	ext url redirect (enter URL)
Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'	
Redirect	https://imgs.search.brave.com/-v7Nb715VA@0arH5dffBVhs1bCoggmpkhY0CY0gV54/rs:fit:533:225:1/g:
Enter the external redirection URL, error message or size (bytes) here.	
Description	
You may enter any description here for your reference.	
Log	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.

Limitación tiempo equipos

Podemos también controlar el acceso a la red mediante el tiempo, con la siguiente configuración realizada desde el squidGuard, podemos limitar el horario de uso al horario escolar.

Name	Description
escolar	 
	

General Options					
Name	escolar				
Enter a unique name of this rule here. The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.					
Values	Weekly	mon		07:00-17:15	
	Weekly	tue		07:00-17:15	
	Weekly	wed		07:00-17:15	
	Weekly	thu		07:00-17:15	
	Weekly	fri		07:00-17:00	
Time type	Days	Date or Date range	Time range		
Add					
Description	You may enter any description here for your reference. Note: Example for Date or Date Range: 2007.12.31 or 2007.11.31-2007.12.31 or *.12.31 or 2007.*.31 Example for Time Range: 08:00-18:00				

LDAP

Aprovechando el servicio de LDAP que hemos creado para el Moodle, configuraremos también el servicio para que quede registrado que usuario entra a donde.

Para configurarlo activamos la pestaña e introducimos la ruta y el usuario del AD.

LDAP Options

Enable LDAP Filter	<input checked="" type="checkbox"/> Enable options for setup ldap connection to create filters with ldap search
LDAP DN	<input type="text" value="cn=Administrador,cn=Users,dc=pimpam,dc=local"/> Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)
LDAP DN Password	<input type="password" value="....."/> Password must be initialize with letters (Ex: Change123), valid format: [a-zA-ZV][a-zA-Z0-9/_\.\%\+\?=8]
LDAP Cache Time	<input type="text" value="300"/> Number of seconds to cache LDAP Results (recommended value: 300)
Strip NT domain name	<input type="checkbox"/> Strip NT domain name component from user names (/ or \ separated)
Strip Kerberos Realm	<input type="checkbox"/> Strip Kerberos Realm component from user names (@ separated).
LDAP Version	<input type="text" value="Version 3"/>

En el apartado de autenticación del squid server creamos el método de LDAP. Ponemos la IP del AD y el puerto del LDAP que es el por defecto.

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt **Authentication** Users Real Time Status Sync

Squid Authentication General Settings

Authentication Method	<input type="text" value="LDAP"/>	Select an authentication method. This will allow users to be authenticated by local or external services.
Authentication Server	<input type="text" value="192.168.30.11"/>	Enter the IP or hostname of the server that will perform the authentication here.
Authentication server port	<input type="text" value="389"/>	Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.
Authentication Prompt	<input type="text"/>	This string will be displayed at the top of the authentication request window.
Authentication Processes	<input type="text" value="10"/>	The number of authenticator processes to spawn. If many authentications are expected within a short timeframe, increase this number accordingly.
Authentication TTL	<input type="text" value="360"/>	This specifies for how long (in minutes) the proxy server assumes an externally validated username and password combination to be valid. When the Time To Live expires, the user will be prompted for credentials again. Default: 5
Authentication Max User IP Addresses	<input type="text" value="10"/>	Enforces a limit to the number of unique IP addresses from which a single user can login. Attempts to login from additional IP addresses are denied until the Authentication TTL has expired Default: none 
Require Authentication for Unrestricted IPs	<input type="checkbox"/>	If enabled, even 'Unrestricted IPs' configured on the ACLs tab are required to authenticate to use the proxy.
Subnets That Don't Need Authentication	<input type="text"/>	
	Enter subnet(s) or IP address(es) (in CIDR format) that should NOT be asked for authentication to access the proxy. Put each entry on a separate line. 	

Introducimos el usuario administrador con la contraseña definida, el dominio del LDAP y el atributo con el que se van a loginar los alumnos, en este caso, samAccountName que es el usuario del AD.

Squid Authentication LDAP Settings

LDAP version	3	Select LDAP protocol version.
Transport	TCP - Standard	If 'SSL Encrypted' or 'TCP - STARTTLS' is selected, the CA certificate of the LDAP server must be trusted by the Operating System Trust Store. This is automatic for certificates signed by globally trusted CAs such as Let's Encrypt; self-signed CAs can optionally be added to the Trust Store on pfSense 2.5.
LDAP Server User DN	Administrador	Enter the user DN to use to connect to the LDAP server here.
LDAP Password	Enter the password to use to connect to the LDAP server here.
LDAP Base Domain	dc=pimpam,dc=local	Enter the base domain of the LDAP server here.
LDAP Username DN Attribute	samAccountName	Enter LDAP username DN attribute here.
LDAP Search Filter	(&(objectClass=person)(samAccountName=%s))	Enter LDAP search filter here.
LDAP not follow referrals	<input type="checkbox"/>	Do not follow referrals.

Bloque 5 | Clúster

5.1 Infraestructura

Para crear un clúster en el vCenter⁸ deberemos crear de antemano un centro de datos donde el único dato necesario es el nombre. Una vez esta creado añadiremos todos los ESXI para que estén centralizados.

Le indicaremos las direcciones ip de todos ellos, el usuario y contraseña con el que accederemos. Omitiremos la licencia ya que no hay ninguna que asignar ya que nos ofrecen un periodo de prueba bastante prolongado.

Agregar host

✓ 1 Nombre y ubicación	Listo para completar
✓ 2 Configuración de la cone...	Haga clic en Finalizar para agregar el host.
✓ 3 Resumen del host	
✓ 4 Asignar licencia	Nombre 192.168.10.6
✓ 5 Modo de bloqueo	Ubicación Datacenter
✓ 6 Ubicación de máquina vir...	Versión VMware ESXi 6.7.0 compilación: 15160138
7 Listo para completar	Licencia Licencia de evaluación
	Redes VM Network
	Almacenes de datos datastore1
	Modo de bloqueo Deshabilitado
	Ubicación de máquina virtual Datacenter

Una vez, estén todas las maquinas añadidas deberemos crear el Clúster asignándole un nombre y para introducir las maquinas nos servirá con selecciones el ESXI2 y el ESXI3 y arrastrarlo hasta que pertenezca a la jerarquía.

El propio hipervisor de vCenter y el ESXI4 se mantendrán en el datacenter pero fuera del clúster, ahí solo permanecerán los dos nodos

NFS

⁸ <https://docs.vmware.com/es/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-6A30F824-3702-4580-94A2-C20CA8501547.html>

<https://docs.vmware.com/es/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-BCDAEBCB-EAE4-4EAF-BC33-08977429E9C7.html>

NFS ⁹es un mecanismo para almacenar los archivos en la red, de esta manera se nos permitirá acceder a los archivos y tratarlos como si fueran locales. En nuestro caso, almacenaremos las iso utilizadas en las instalaciones.

Para que esto sea posible nos conectaremos al NAS y ejecutaremos la siguiente orden que se encargara de instalar el paquete de NFS tras asegurarnos que tenemos todos los paquetes actualizados.

```
$ sudo apt install nfs-kernel-server
```

```
root@nas:/mnt/nfs# ll
total 28
drwxr-xr-x 4 root      root      4096 Feb 23 16:34 .
drwxr-xr-x 3 root      root      4096 Feb 23 15:30 ..
drwxrwxrwx 3 nobody    nogroup   4096 Mar  1 14:51 backup/
drwx----- 2 root      root     16384 Feb 23 15:29 lost+found/
```

Una vez instalado, comprobaremos que el servicio esta iniciado y lo habilitaremos.

```
pimpam@nas:~$ sudo systemctl enable nfs-kernel-server
Synchronizing state of nfs-kernel-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nfs-kernel-server
pimpam@nas:~$ sudo systemctl status nfs-kernel-server
● nfs-server.service - NFS server and services
    Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset: enabled)
      Drop-In: /run/systemd/generator/nfs-server.service.d
                └─order-with-mounts.conf
    Active: active (exited) since Wed 2023-03-01 14:50:23 UTC; 58min ago
      Main PID: 2150 (code=exited, status=0/SUCCESS)
        CPU: 11ms

Mar 01 14:50:23 nas systemd[1]: Starting NFS server and services...
Mar 01 14:50:23 nas systemd[1]: Finished NFS server and services.
```

Por otro lado, editaremos el archivo /etc/exports indicando los hosts a los que le querremos dar acceso al sistema de archivos (ESXI y el Veeam backup). Indicaremos la ruta del directorio dedicado a las copias NFS, la dirección ip del ESXI con los permisos correspondientes, leer y escribir, mantenerse sincronizado y no hará comprobaciones de raíz.

```
GNU nano 6.2                               /etc/exports *
# /etc/exports: the access control list for filesystems which may be exported
#           to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/mnt/nfs/backup 192.168.50.5(rw,sync,no_subtree_check)
/mnt/nfs/backup 192.168.50.6(rw,sync,no_subtree_check)
/mnt/nfs/backup 192.168.50.7(rw,sync,no_subtree_check)
/mnt/nfs/backup 192.168.50.8(rw,sync,no_subtree_check)
/mnt/nfs/backup 192.168.50.13(rw,sync,no_subtree_check)
```

Para que los cambios tomen forma realizaremos un reinicio del servicio.

⁹ <https://docs.vmware.com/es/VMware-vSphere/7.0/com.vmware.vsphere.hostclient.doc/GUID-9F526FAE-A72E-462B-86CE-14078D3A3C67.html>
<https://mytcpip.com/lab-nfs-iscsi-server-ubuntu/>

Una vez completado, nos desplazaremos al apartado de almacenamiento de vCenter y crearemos nuevo almácen de datos NFS mediante recurso compartido por medio de red en la versión 3. Rellenaremos los datos que hemos establecido anteriormente.

Detalles de recurso compartido de NFS	
Nombre del almácen de datos:	NFS
Carpeta:	/mnt/nfs/backup
Servidor:	192.168.50.14
Ej.: /vols/vol0/datastore-001	Ej.: nas, nas.it.com o 192.168.0.1

iSCSI

Este protocolo de red¹⁰ define como trasmitimos los datos entre nuestros hosts y el dispositivo de almacenamiento permitiendo así que no haya una pérdida de conexión al momento de migrarse con vMotion. Se utiliza este método para tener centralizar el almacenamiento en disco

En primer lugar, instalaremos el paquete de iSCSI Target con la siguiente orden, nos aseguraremos de que el servicio esta iniciado y habilitado.

```
$ sudo apt install tgt
```

Seguidamente editaremos el archivo /etc/tgt/conf.d/target01.conf para añadir las direcciones ip iniciadoras de los ESXI.

Una vez guardado nos conectaremos a ambos ESXI que pertenecen al clúster y en el apartado de adaptadores dentro de

```
GNU nano 6.2                                     target01.conf
<target iqn.2022-11.loc.pimpam.nas:target01>

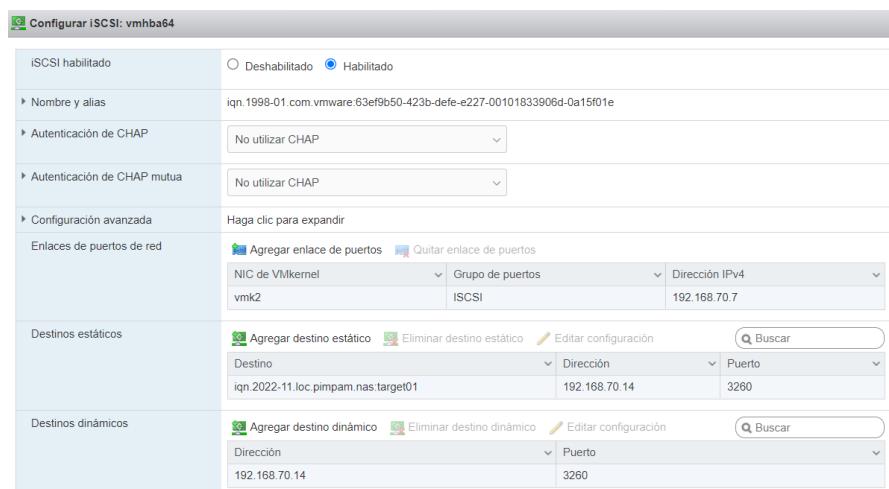
# provided device as a iSCSI target
backing-store /dev/sdc

# iSCSI Initiator's IQN you allow to connect
#initiator-name iqn.1993-08.org.debian:01:944868bdf19

# IP Initiator
initiator-address 192.168.70.6
initiator-address 192.168.70.7
initiator-address 192.168.70.8
initiator-address 127.0.0.1

# incoming user username password

</target>
```

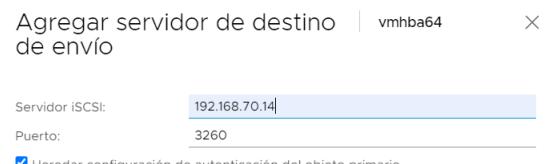


¹⁰ <https://blog.ragasys.es/configuracion-almacenamiento-iscsi-vmware-vsphere-6-7>
<https://mytcpip.com/lab-nfs-iscsi-server-ubuntu/>

almacenamiento, nos desplazaremos al botón de iSCSI de software con la configuración siguiente. Hay que añadir en destinos estáticos y dinámicos la dirección ip del NAS.

Una vez este detectado correctamente crearemos el almacen de datos. Indicaremos el nombre de este y seleccionamos el LUN (espacio de disco en bruto, es decir, sin formato)

A continuación, desde el panel del Vcenter para de una vez poder administrar ambas maquinas comprobaremos que se detecten los discos, en caso negativo volveremos a examinar y añadiremos las IP estáticas y dinámicas del NAS de nuevo.



Nuevo almacen de datos

✓ 1 Tipo
2 Selección de nombre y di...
3 Versión de VMFS
4 Configuración de particio...
5 Listo para completar

Selección de nombre y dispositivo
Seleccione un nombre y un disco o un LUN para aprovisionar el almacen de datos.

Nombre del almacen de datos: iSCSI

ⓘ El almacen de datos será accesible para todos los hosts que estén configurados con acceso al disco o LUN seleccionados. Si no se encuentran el disco o el LUN deseados, es posible que no sean accesibles para ese host. Intenta cambiar el host o configurar la accesibilidad de ese disco o LUN.

Selecciona un host para ver los discos o LUN que son accesibles para este host:
192.168.10.8

Nombre	LUN	Capacidad	Aceleraci...	Tipo de...	F
IET iSCSI Disk (naa.6000...)	1	1,82 TB	Compatible	HDD	5

Seguidamente, deberemos especificar la versión de VMFS 6 ya que no tenemos más de 2 TB de LUN.

Para las particiones de disco las dejaremos tal y como están, no crearemos ninguna y utilizaremos el máximo espacio del almacen.

Nuevo almacén de datos

✓ 1 Tipo
✓ 2 Selección de nombre y di...
✓ 3 Versión de VMFS
4 Configuración de particio...
5 Listo para completar

Configuración de particiones
Revise el diseño del disco y especifique los detalles de la configuración de particiones.

Configuración de particiones Utilizar todas las particiones disponibles

Tamaño de almacén de datos 1862,94 GB

Tamaño de bloque 1 MB

Granularidad de recuperación de espacio 1 MB

Prioridad de recuperación de espacio Bajo: los bloques eliminados o no asignados se recuperan en el LUN con la prioridad Bajo

MBR heredado: 1.8 TB

MBR heredado MBR heredado



Una vez se empiece a crear por las tareas visibles del vCenter podremos ver como procesa nuestro nodo.

Procesar las actualizaciones del almacén de datos de VMFS	192.168.10.7	✓ Completado	Systems
Procesar las actualizaciones del almacén de datos de VMFS	192.168.10.6	✓ Completado	Systems

vMotion

vSphere vMotion¹¹ es una migración dinámica de un servidor a otro sin tiempo de inactividad para cargas de trabajo.

En nuestro caso, decidimos establecer la relación de los servidores a través de un cable cruzado en vez del switch, pese a esto se tendrá que crear el conmutador de kernel como el resto de los puertos físicos.

Para comprobar que vMotion funciona probaremos a migrar una máquina virtual en caliente desde un ESXI a otro mientras realizamos un simple ping, de esta manera podremos ver que no se pierde en ningún momento la conexión hasta que es traspasada completamente. Es importante para que se realice que los discos de las máquinas virtuales del nodo estén almacenados en el iSCSI.

¹¹ <https://www.vmware.com/es/products/vsphere/vmotion.html>

<https://docs.vmware.com/es/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-D19EA1CB-5222-49F9-A002-4F8692B92D63.html>

Seleccionar un tipo de migración

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

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 almacenes de datos o un almacén de datos compatible.

Cambiar recurso informático y almacenamiento
Migra las máquinas virtuales a un clúster o un host específico y su almacenamiento a un clúster de almacenes de datos o un almacén de datos específico.

Es debido a esta característica que el nombre de los grupos de puertos en el servidor ESXI son muy importantes ya que al cambiarse buscara conectarse al mismo adaptador de red buscando el nombre del anterior.

Red de origen	Utilizado por	Red de destino
Admin2	1 máquinas virtuales/1 adaptadores de red	Admin2

HA

Habilitaremos la HA (High Availability) para proporcionarnos disponibilidad a las aplicaciones que se ejecutan en máquinas virtuales, con independencia del sistema operativo, para reducir automáticamente el tiempo de inactividad de estas aplicaciones al momento que uno de los ESXI portadores de esas máquinas pierda conexión.

Para activar esta característica nos situaremos en la configuración del clúster y activaremos el vSphere availability indicando que ante una respuesta de error del host (ESXI) se reinicen las máquinas y así continuar produciendo, en cambio, para el resto de las opciones las dejaremos deshabilitadas.

vSphere HA

Errores y respuestas Control de admisión Almacenes de datos de latidos Opciones avanzadas

Puede configurar la forma 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 y APD), máquina virtual y aplicación.

Habilitar supervisión de hosts (i)

> Respuesta de error de host	<input type="button" value="Reiniciar las máquinas virtuales"/>
> Respuesta para el aislamiento del host	<input type="button" value="Deshabilitado"/>
> Almacén de datos con PDL	<input type="button" value="Deshabilitado"/>
> Almacén de datos con APD	<input type="button" value="Deshabilitado"/>
> Supervisión de máquinas virtuales	<input type="button" value="Deshabilitado"/>

Finalmente, en el control de admisión toleraremos 1 único error del host y definiremos un porcentaje de CPU y de memoria para la conmutación por error, ese espacio será el recurso destinado para las máquinas virtuales al momento de “saltar” de host.

Errores y respuestas Control de admisión Almacenes de datos de latidos Opciones avanzadas

El control de admisión es una directiva utilizada por vSphere HA para garantizar la capacidad de conmutación por error en un clúster. El incremento en la cantidad de posibles errores de host aumentará las restricciones de disponibilidad y la capacidad reservada.

Errores del host que tolera el clúster	1	El valor máximo es uno menos que el número de hosts presentes en el clúster.
Definir la capacidad de conmutación por error según	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="Porcentaje de recursos del clúster"/> <input checked="" type="checkbox"/> Anule la capacidad de conmutación por error calculada.	
Degradación del rendimiento que toleran las máquinas virtuales	0	Porcentaje de degradación del rendimiento que las máquinas virtuales del clúster tienen permitido tolerar durante un error. 0% - Emite una advertencia si no hay suficiente capacidad de conmutación por error para garantizar el mismo rendimiento después de que se reinicen las máquinas virtuales. 100% - La advertencia se deshabilita.
	Capacidad reservada de CPU de comm... 25	% CPU
	Capacidad reservada de memoria de c... 25	% Memoria

Bloque 6 | Análisis de riesgos

Política de backup

MAQUINAS	RETENCIÓN	PERIODICIDAD
MAQUINAS DIARIAS	30 días	Diariamente a las 21h
NAS	30 días	Diariamente a las 4h
ODOO	30 días	Cada 2 h de 8-20h

Nuestra política de copias se basa en una retención de 30 días entre semana con una copia de las máquinas virtuales críticas y del disco del sistema operativo del NAS.

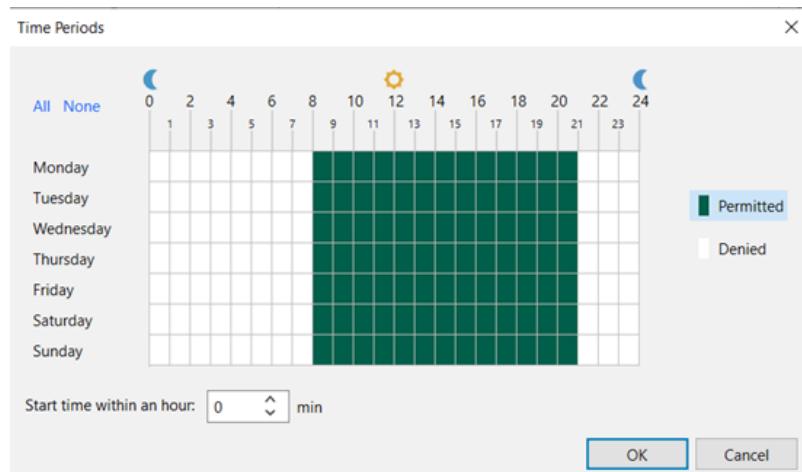
En primer lugar, iniciaremos los miércoles realizando una copia de seguridad de tipo full complementando el resto de incrementales dentro de 30 días.

La hora sin carga de trabajo para hacer las copias de seguridad es a las 21:00, el NAS a las 4:00 y Odoo cada 2 horas desde las 08:00 hasta las 09:00 ya que trata de un aplicativo de facturación es importante conseguir el máximo número de los pedidos en el mismo día y la pérdida de un día entero es muy grave.

The screenshot shows the Veeam Backup and Replication Community Edition interface. The top navigation bar includes 'Home' and 'View' tabs, along with icons for Backup, Replication, Job, CDP, Policy, and various actions like Import, Export, and Best Practices. Below the navigation is a search bar. The main area displays a table of backup jobs:

Name	Type	Objet...	Status	Last Run	Last Result	Next Run	Target
NAS BACKUP	Linux Agent Backup	1	Stopped	4 days ago	Success	03/05/2023 4:00	PIMPAM_NAS
Copia Diaria	VMware Backup	8	Stopped	4 days ago	Success	02/05/2023 21:00	PIMPAM_NAS
ODOO	VMware Backup	1	Stopped	3 days ago	Success	02/05/2023 18:00	PIMPAM_NAS

A continuación, podemos ver el periodo del Odoo junto a su ocupación.



Odoo	
Espacio copia Full	Espacio copia incremental
3.5 GB	200 MB

Copia diaria 210 GB 30 días miércoles full diaria

A modo de comparación, podremos ver lo que ocuparan las copias de seguridad de otras máquinas en las copias dirías.

Máquinas restantes	
Espacio copia Full	Espacio copia incremental
60 GB	8 GB

NAS	
Espacio copia Full	Espacio copia incremental
3.5 GB	500MB

Para tener un estudio del peso de todas las copias que realizamos en Veeam Backup hemos utilizado una función de este llamado Veeam Backup Capacity Calculator.

En la imagen a continuación podremos observar que aproximadamente utilizaríamos 2.7 Tb por copia, teniendo en cuenta que hacemos copias de unos 300GB por regla de 3 nos haría falta más espacio, específicamente 0.84 TB.

Veeam Backup Capacity Calculator

All calculation results are estimate and may differ from real-life usage scenario.

Source data

Source capacity (TB):	1	Scope for growth (years):	4
Daily change rate (%):	5	Reduction (%):	50
Yearly growth (%):	10	REFS / XFS	<input checked="" type="checkbox"/> On

Total

Disponible:

Calculation summary

Backup	2.77 TB
Full backup:	929.52 GB
Incremental backup:	1.09 TB
Weekly:	0 GB
Monthly:	0 GB
Yearly:	0 GB
Workspace:	787.1 GB

Primary backup policy

Daily	30	Weekly	1	Monthly	12	Yearly	2
-------	----	--------	---	---------	----	--------	---

Calculate

Calculation summary

Backup	5.17 TB
Full backup:	372.42 GB
Incremental backup:	1.09 TB
Weekly:	0 GB
Monthly:	2.34 TB
Yearly:	620.98 GB
Workspace:	787.1 GB

Al tener el estudio de estos datos hemos optado por mantener 1 copia semanal, 12 mensuales y 2 anuales.

De esta manera, nos daría aproximadamente necesario 1'6 TB por lo que durante 4 años con estas estimaciones de crecimiento no tendríamos inconveniente por crecimiento empresarial.

Plan de emergencia

1. En el caso de que algo falle, con el sistema de alertas que hemos montado a través del ZABBIX Server, nos llegará una alerta el telegram con una pequeña descripción del fallo y donde ha ocurrido.
2. Primero se comprobará si es accesible o tiene respuesta IP. (Máximo 2 minutos.)
3. Si no hay conectividad se tendrá que revisar físicamente si el equipo se encuentra encendido o apagado. (Máximo 5 minutos.)
4. En caso de que este apagado y no encienda se conectara a otra toma de corriente, si sigue sin funcionar se tendría que comprobar con un remplazo de fuente de alimentación o placa base. (Máximo 40 minutos.)
5. En caso de que encienda, pero no tenga sistema operativo se comprobara el estado del disco por si hay que sustituirlo y reinstalar el sistema operativo. (Máximo 20 minutos.)
6. En caso de fallo de máquina virtual si no enciende se utilizará veeam backup para restaurar la última copia. (Máximo 120 minutos.)
7. En caso de fallo del servidor de copia se instalará un nuevo ws2019 y se instalará la ISO de veeam que se encuentra en el NFS. (Máximo 60 minutos)
8. Se escaneará primero el repositorio de backup y se lanzará un resorte de las maquinas afectadas en los hosts que estén funcionando.
9. En caso de fallo del router se contactará con el ISP y se seguirán las instrucciones.

ORDEN DE RESTAURACIÓN DE MÁQUINAS

1	vCenter
2	Router
3	PFSENSE
4	DNS
5	Servidor
6	Odoo
7	Moodle
8	Servidor backup
9	Resto de máquinas.