



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA

CAMPUS D'ALCOI

# *Virtualización mediante entornos Open Source*

---

**MEMORIA PRESENTADA POR:**

**Mauro Domínguez Sanjuán**

GRADO DE INGENIERÍA INFORMÁTICA

**Convocatoria de defensa:** Septiembre de 2018



## Resumen

El objetivo de este trabajo ha sido la construcción de un sistema de virtualización con herramientas OpenSource a fin de dar soporte a dos casos de uso reales. Una vez elegida la herramienta de virtualización (Proxmox), se han creado dos clústeres con diferentes sistemas de almacenamiento (iSCSI y Ceph) para comprobar cual da mejor rendimiento para ambos casos. A continuación, se describe, a grandes rasgos, el diseño de los dos casos, su implementación en el sistema final y una pequeña muestra de cómo sería el funcionamiento de cada uno en el día a día. Finalmente, se ha añadido un sistema de copias de respaldo para asegurar el funcionamiento en caso de fallo de alguna de las máquinas virtuales del sistema.

Para conseguir el resultado propuesto, la memoria desarrolla toda la teoría relacionada con virtualización, clústering, herramientas Opensource y elementos relativos a la administración de sistemas y, a continuación explica, de manera práctica y desarrollando algunos conceptos importantes, todo el proceso detallado en el párrafo anterior. Finalmente, ofrece una conclusión personal del trabajo realizado y se añaden algunas futuras mejoras que se le puede hacer al sistema.

**Palabras clave:** Virtualización, OpenSource, Proxmox, iSCSI, Ceph

## Abstract

The objective of this work has been the implementation of a virtualization system with Open Source tools in order to support two real use cases. Once the virtualization tool has been chosen (Proxmox), two clusters with different storage systems (iSCSI and Ceph) have been created to verify which gives better performance for both cases. Next, it is described, in broad strokes, the design of the two cases, their implementation in the final system and a small sample of how the operation of each one would be on a day-to-day basis. Finally, a backup system has been added to ensure the operation in case of failure of any of the virtual machines of the system.

To achieve the proposed result, the memory develops all the theory related to virtualization, clustering, Opensource tools and elements related to system administration and then explains, in a practical way and developing some important concepts, the entire process detailed in the previous paragraph. Finally, it offers a personal conclusion of the work done and some future improvements that can be added to the system.

**Keywords:** Virtualization, OpenSource, Proxmox, iSCSI, Ceph

# Índice

Introducción.....	5
Motivación.....	5
Objetivos.....	6
Estructura de la memoria.....	6
Entorno teórico.....	6
Entorno práctico.....	7
Entorno teórico.....	8
Virtualización.....	8
Comparativa soluciones virtualización.....	9
Soluciones Open Source.....	9
Soluciones privativas.....	11
Estructura IT de una empresa.....	16
Entorno práctico.....	21
Ceph.....	21
Instalación del clúster Proxmox + Ceph.....	23
Esquema de red.....	23
Instalación de Proxmox.....	25
Configuración de Proxmox.....	25
Creación del clúster Proxmox.....	26
Instalación del servidor Ceph:.....	27
iSCSI.....	28
LVM.....	29
Instalación del clúster Proxmox + iSCSI.....	31
Esquema de red de iSCSI.....	31
Instalación de servidor iSCSI (FreeNAS).....	31
Montaje del servicio NFS para compartición de ISOs.....	33
Configuración del servicio iSCSI.....	34

Esquema de red de Proxmox. ....	35
Instalación del clúster Proxmox. ....	36
Descubrimiento de LUNs y creación de almacenamiento LVM. ....	36
Servidor de Backup.....	38
Esquema de la red. ....	38
Instalación del servidor de respaldo. ....	39
Instalación de CentOS. ....	40
Casos de aplicación para los sistemas implementados. ....	42
Entorno docente. ....	42
Infraestructura IT en una PYME. ....	51
Conclusiones y líneas futuras de trabajo (ampliaciones).....	60
Conclusiones. ....	60
Líneas futuras de trabajo. ....	61
Backups incrementales en Proxmox. ....	61
Monitorización de algunos de los sistemas implementados. ....	61
Bibliografía .....	63

## Introducción.

### *Motivación.*

Hasta hace unos años la disponibilidad de servicios informáticos, adecuados a las operaciones de negocio en una empresa u organización, venía ligada a la pertenencia por parte de la misma de una infraestructura física y licencias de uso y mantenimiento que solo estaba al alcance de muy pocas. Un claro ejemplo es que si había que montar una nueva base de datos X, se examinaban las distintas comparativas (benchmarks) y se compraba el servidor más potente para esa base de datos X, del fabricante y sistema operativos indicados. Si seguidamente había que montar un servicio de atención al cliente, se compraría el servidor mejor para la aplicación de CRM elegida, muy posiblemente de otro fabricante y otro sistema operativo. Y así sucesivamente.

La virtualización permite consolidar estos servicios sin tener pasar por todo el proceso anteriormente explicado y reducir tiempo y costos. Ésta se ha convertido en un pilar fundamental para las grandes empresas de cualquier país. Permite una serie de ventajas que hasta hace unos años eran impensables por tiempo, material o dinero. Dichas ventajas son:

- Aislamiento: Cada máquina virtual es completamente independiente de las otras y del propio hipervisor donde está alojada.
- Seguridad: Cada máquina tiene un acceso independiente.
- Flexibilidad: Cada máquina virtual se puede crear al gusto del usuario con sus propias características (CPUs, RAM, Disco duro, S.O., etc.) sin necesidad de "comprar" una igual con las mismas características.
- Agilidad: La creación de una máquina es un proceso muy rápido. Pensemos en el tiempo necesario para adquirir un servidor o un ordenador de sobremesa.
- Portabilidad: La configuración de una máquina virtual reside en varios ficheros que se pueden trasladar de un hipervisor a otro.
- Recuperación en caso de fallo: La recuperación de una máquina virtual reside en las copias de los ficheros de configuración de ésta. Si dichas copias están disponibles, la recuperación es mucho más rápida que en una máquina física.
- Ahorro de costes: El material adquirido para implementar un diseño TI es bastante inferior comparado con un diseño tradicional.

Estas ventajas permiten a empresas u organizaciones no tan grandes realizar una inversión inicial de manera que en un futuro puedan, en menor escala que las más

grandes, aprovechar el potencial que proporciona la virtualización Open Source. En este tipo de virtualización es posible dedicar inicialmente más presupuesto a la parte hardware que a la parte software obteniendo una mejor infraestructura de TI con la que trabajar y aplazar en el tiempo la adquisición del soporte.

En este trabajo se presenta un sistema que permite virtualizar los servidores requeridos por dos casos de uso, uno una PYME cualquiera y, el otro, las prácticas de una asignatura de universidad. En ambos casos se dispone de alta disponibilidad, tolerancia a fallos, balanceo de carga y mantenimiento fácil de los recursos.

### *Objetivos.*

El objetivo de este trabajo es implementar una solución que permita a los usuarios de los dos casos mencionados trabajar sin preocuparse de los problemas que puedan surgir. Proporcionará las características mencionadas en el apartado *Motivación* y para ello, se deberán conseguir los siguientes objetivos parciales:

- Diseñar e implementar un clúster de servidores con una herramienta Open Source asegurando el acceso desde el exterior mediante una conexión VPN.
- Diseñar e implementar la infraestructura de red que dé soporte al clúster y al acceso mediante la VPN
- Montar un servidor exclusivo para los backups de ambos casos sin que estos se estorben mutuamente.
- Configurar el sistema para que posea autogestión. Esto es, balanceo de carga según las necesidades del caso, recuperación del servidor virtual o físico en caso de fallo, etc.
- Realizar todo lo relacionado con la virtualización con software Open Source en la medida de lo posible.

### *Estructura de la memoria.*

A continuación, se resume en pocas líneas el contenido de la memoria. Ésta consta de dos grandes partes.

#### **Entorno teórico.**

Una explicación del contexto teórico en el que se basa el trabajo. Los conceptos a desarrollar son:

- Virtualización: Explicación de la virtualización y, de las ventajas y desventajas que tiene.

- Comparativa de las plataformas de virtualización Open Source y comerciales más usadas del mercado
- Razones que nos llevan a utilizar el entorno de virtualización implementado en la parte práctica
- La virtualización en la empresa. Se explica como ayuda la virtualización en el funcionamiento de una organización y se comentan algunos conceptos importantes que se han usado ampliamente en el proyecto. Estos conceptos son:
  - VSAN: Explicación de la tecnología utilizada en uno de los clústeres.
  - VLANs: Como se ha separado el tráfico de red entre los diferentes elementos del proyecto.
  - Backups: Solución de respaldo a utilizar para restaurar máquinas virtuales en caso de fallo.

### Entorno práctico.

Se desarrollará todo lo implementado en el proyecto. He aquí un pequeño resumen.

- Se realizará una explicación de las opciones de almacenamiento trabajadas y de sus opciones en la PYME.
- Se describirá el diseño y montaje de los dos clústeres de virtualización con el almacenamiento utilizado por cada uno.
- Diseño e implementación del servidor de respaldo o backup y su uso por parte de los clústeres anteriores.
- Soluciones almacenamiento: Zona de benchmarks.
- Presentación de dos casos de uso factibles para su implementación en cualquiera de los clústeres montados.

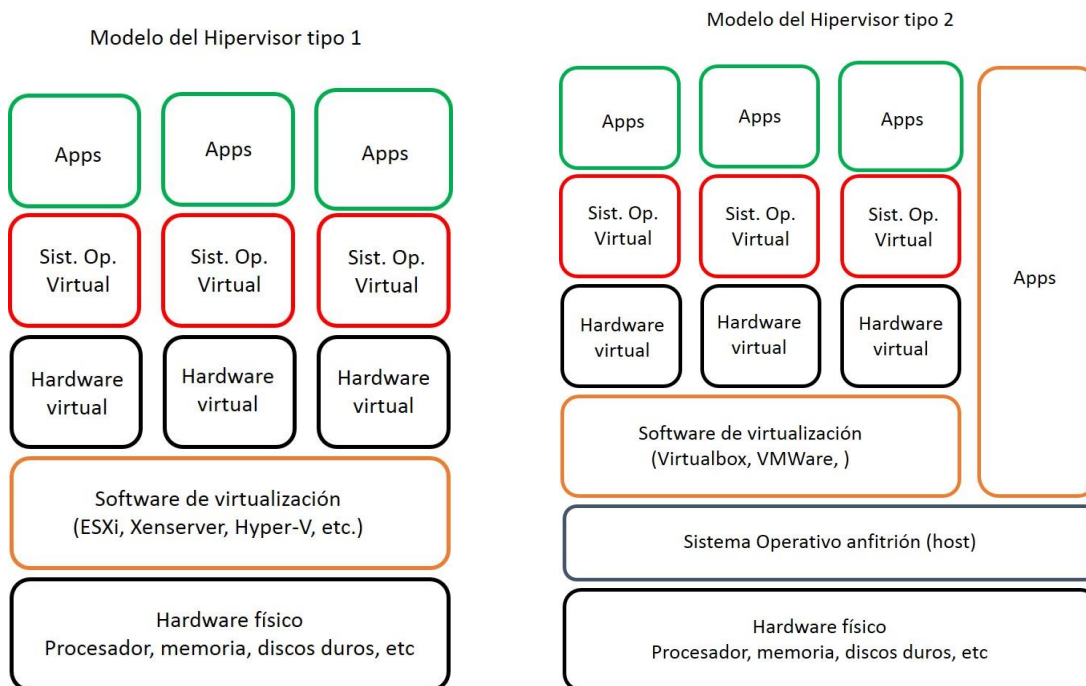


## Entorno teórico.

### *Virtualización.*

La virtualización permite, a grandes rasgos, emular mediante software toda una infraestructura física de servidores y elementos de red dentro de una máquina física. Existen dos formas de conseguir esto. una es mediante el uso de un hipervisor de tipo 1 y la otra mediante el uso de un hipervisor de tipo 2.

El primero está situado directamente sobre el hardware aprovechando todos los recursos que éste pueda ofrecerle. Por otro lado, el segundo tipo tiene una capa más por debajo. Esto quiere decir que se instala encima del sistema operativo que se haya sobre el hardware por lo tanto, su rendimiento depende de este sistema anfitrión.



### Ventajas e inconvenientes que supone la virtualización.

Hoy en día existen diferentes opciones en el mercado que permiten montar toda una infraestructura de virtualización en una empresa u organización. Lo importante es poder elegir según las necesidades de cada caso y poder aumentar las funcionalidades de dicha infraestructura a lo largo del tiempo según se necesite o se pueda por razones económicas.

Según el punto anterior la necesidad disponer de un hipervisor de tipo 1 en éste proyecto es obvia por las siguientes razones:

- Introduce menos capas intermedias entre el hardware real y las aplicaciones o servicios a implementar. Esto asegura un mayor rendimiento que el otro tipo.
- Agrupación de varios hipervisores en un mismo conjunto. Esta idea se llama clúster y permite más funcionalidades que uno sólo.
- Gestión remota de uno o varios hipervisores.
- Consolidación de servicios. Si antes cada servicio se ejecutaba en una sola máquina, ahora están agrupados en una sola o en un clúster.

Una vez se conocen las ventajas de la virtualización, es conveniente analizar que nos ofrece cada alternativa del mercado. La PYME es un entorno exigente en cuanto a resultados y existen pocas soluciones que soporten dicho requisito.

### *Comparativa soluciones virtualización.*

Antes de explicar las razones de la opción elegida, vamos a realizar un repaso de las opciones más usadas del mercado para ver qué ventajas y qué inconvenientes tenemos al elegirla.

#### Soluciones Open Source.

Se ha realizado una comparativa en base a las funcionalidades de los dos hipervisores Open Source más utilizados hoy en día en el mercado para luego comparar la opción elegida con los hipervisores comerciales. Éstos son Proxmox VE y XenServer. No se ha adquirido ninguna licencia o soporte para compararlos.

Comparativa de las configuraciones máximas de cada sistema.

		Proxmox 5.2	XenServer 7.5
Servidor físico	Núcleos hardware	320	288
	RAM	8 TB	5 TB
	CPUs virtuales	-	-
Máquinas virtuales (VM)	vCore	320	32
	vRAM	4 TB	1,5 TB
	vDisk	-	2 TB
	VM activas	-	1000

Clúster	Nodos totales	32	64
	VMs	-	4096

Comparativa de características generales.

	Proxmox 5.2	XenServer 7.5
Clustering	Sí	Sí
Alta disponibilidad	Sí	No
Tipos de almacenamiento	ZFS, NFS, CIFS, GlusterFS, LVM, iSCSI, Ceph, etc.	EXT3, NFS, iSCSI, FC HBA, open-FCoE, etc
Gestión de red	Modo Linux, OVS	OVS
SO invitados	Windows, Linux y otros	Windows, Linux y otros
Compartición de memoria entre VMs	Sí (KSM y Ballooning)	No
Firewall a nivel de host	Sí	Sí
Infraestructura hiper-convergente	Sí	No

Comparativa de la gestión del entorno.

	Proxmox 5.2	XenServer 7.5
CLI	SSH	SSH
GUI	Web	Cliente Windows
Monitorización	Sí	Sí
Gestión de usuarios y permisos	Sí	No
Consola individual por VM	VNC por HTML5, SPICE y consola xTERM	Cliente Windows

### Comparativa de la gestión de las VMs.

	Proxmox 5.2	XenServer 7.5
Backup/Restauración	Sí	No
Migración	Sí	Sí
Migración en vivo	Si	Sí
Migración en vivo del almacenamiento	Sí	No
Snapshots	Sí	Sí
Plantillas y clonado de VMs	Sí	Si
Replicación	Si (ZFS)	No
Exportar e importar	Sí	Si

La principal razón de la elección de Proxmox respecto a Xenserver es que en una versión anterior de XenServer (la 7.3) se eliminó de la edición "Free" varias funcionalidades importantes que se usan mucho en el día a día en un pool (clúster) XenServer. En las tablas se pueden ver algunas de estas funcionalidades eliminadas.

Otra razón importante, aunque no aparezca en la comparativa, es que al añadir nuevos hipervisores al clúster se debe tener en cuenta las características hardware del nuevo servidor físico. Muchas veces no se puede ampliar un clúster existente por las diferencias entre las máquinas físicas y se debe crear otro clúster diferente que coexista o reemplace al antiguo. Con Proxmox eso no ocurre. Proxmox puede agrupar dentro de un clúster máquinas más potentes con otras que no lo son tanto y mediante políticas de HA distribuir la carga de trabajo ente grupos de nodos diferentes.

Por éstas razones y por otras de índole personal se ha elegido Proxmox como sistema para desarrollar el trabajo explicado en esta memoria.

### Soluciones privativas.

Una vez decidida la plataforma podemos ver ahora como se compara ante los productos qué si requieren una licencia por su uso, o al menos adquirir un soporte que permita solucionar los problemas cuando estos aparecen. Proxmox también propone un sistema de soporte que se puede consultar en su página web. XenServer se ha eliminado de la comparativa por no pertenecer a la categoría Open source.

He aquí los Productos comparados en cuanto a funcionalidades:

- Proxmox 5.2 en su versión de no suscripción
- Hypervisor ESXi 6.5 de VMWare
- vSphere 6.5 Standard de VMWare
- Hyper-V 2016 de Microsoft

Comparativa máximos.

		Proxmox 5.2	Hypervisor ESXi 6.5	vSphere 6.5 Standard	Hyper-V 2016
Servidor físico	Núcleos hardware		576	576	512
	RAM		12TB	12TB	24TB
	CPUs virtuales		4096	4096	2048
VM	vCores soporta		128	128	240
	RAM virtual		6T	6T	16TB
	vDisk		62TB	62TB	64TB
	VMs activas	-	1024	1024	1204
Cluster	Nodos	32	N/A	64	64
	VMs	-	N/A	8000	8000

Comparativa de características generales.

	Proxmox 5.2	Hypervisor ESXi 6.5	vSphere 6.5 Standard	Hyper-V 2016
Clustering	Sí	No	No	No
Alta disponibilidad	Sí	Sí	Sí	Sí
Tipos de almacenamiento	ZFS, NFS, CIFS, GlusterFS, LVM, iSCSI, Ceph, etc.		SAN, NAS y sus contrapartes virtuales	
Gestión de red	Linux networking y OVS	vSwitch	Cross vSwitch	
SO invitados	Windows, Linux y otros	Windows, Linux y otros	Windows, Linux y otros	Windows, Linux y otros
Compartición de memoria entre VMs	Sí	Si	Si	No
Firewall a nivel de host	Sí	Sí	Sí	
Infraestructura hiper-convergente	Sí	N/A	Sí	Sí

Comparativa de la gestión del entorno.

	Proxmox 5.2	Hypervisor ESXi 6.5	vSphere 6.5 Standard	Hyper-V 2016
tiene CLI?	SSH	SSH	SSH	SSH
tiene GUI?	Web	Windows	Web/Windows	Windows
Monitorización	si	Sí	Sí	si
Gestión de usuarios y permisos	Sí	Sí	Sí	
Consola individual por VM	VNC por HTML 5, SPICE y consola xTERM	HTML 5 y Cliente Windows	HTML 5 y Cliente Windows	Cliente Windows

Comparativa gestión VMs.

	Proxmox 5.2	Hypervisor ESXi 6.5	vSphere 6.5 Standard	Hyper-V 2016
Backup/Restore	Sí	No	Sí	
Migración	Si	N/A	Si	Sí
Migración en vivo	Si	N/A	Sí	Sí
Migración en vivo del almacenamiento	Sí	N/A	Sí	NO
Snapshot	Sí	Sí	Sí	
Plantillas y clones	Sí	Sí	Sí	
Replicación	Sí	No	Sí	
Exportar/Importar	Sí	Sí	Sí	

Ahora se comparará el precio entre versiones equivalentes de los productos.

Comparativa costes (I): Versiones básicas de los productos.

	Proxmox 5.2 sin subscripción	Hypervisor 6.5	vSphere 6.5 Essentials Kit	Hyper-V 2016
Licencia permanente	0€	0€	639,94€ (6 CPU)	0€
Licencia + soporte 1 año	-	-	N/A	0€
Ampliar soporte 1 año	74,90€(opcional)	-	N/A	-
Soporte por incidencia (una al año)	-	341,83€	341,83€	179€(básica) 358€(completa)

Comparativa costes (II): Versiones más completas de los productos.

	Proxmox 5.2 Suscripción (4 modelos)	vSphere 6.5 Ess. Kit Plus	vSphere 6.5 Standard	Win Srv 2016 Standard
Licencia permanente	0€	N/A	N/A	753.54€ por bloque de 16 cores
Licencia + soporte 1 año	N/A	5160,54€	1448.72€	
Ampliar soporte 1 año	70-800€ por CPU	N/A	N/A	
Soporte por incidencia (una al año)	Las incidencias dependen del tipo de soporte y están incluidas	Incluido en la licencia	Incluido en la licencia	179€(básica) 358€(completa)



Razones que llevan a la elección de Proxmox como alternativa viable para su implementación en una empresa.

- Rendimiento. Interfaz web de gestión ligera y también por línea de comandos.
- Estabilidad.
- Coste. Tiene la funcionalidad de backup y snapshots integrada en el sistema. nada de aplicaciones de terceros.
- Escalabilidad. Cada nodo tiene toda la información del clúster.
- Simplicidad. Facilidad de instalación del clúster.
- Tecnología abierta / integradora. Su soporte de almacenamiento es bastante amplio: ZFS/Gluster/Ceph/LVM thin entre otros.
- Open Source

### *Estructura IT de una empresa.*

La virtualización es una parte más en el diseño IT de una empresa. Dentro de éstas podemos encontrar varios elementos comunes que interactúan con la plataforma de virtualización, desde sistemas de almacenamiento hasta elementos de red. La integración correcta entre todos ellos hace que la empresa pueda ofrecer sus servicios sin ningún problema para sus clientes.

Estos son la utilización de funciones avanzadas de red, el montaje y cableado de armarios, la gestión remota de los servidores, la SAN virtual montada en uno de los casos y el sistema de backups.

### **VLANs, trunk y bonding.**

Las VLANs son separaciones del tráfico de red mediante la capa 2. No es necesario un router (capa 3) para implementarse pero, si se desea conectar dos VLANs, si es necesario uno. Esto se realiza mediante etiquetado de la trama que se envía por parte del puerto del switch para que esta vaya a las interfaces de red asociadas con la misma VLAN.

Un ejemplo muy claro de ver es si un usuario normal de un sistema tiene acceso a la interfaz o consola de administración de un servidor, ese diseño no es correcto. Las VLANs permiten separar el tráfico generado por los usuarios normales respecto al generado por los administradores de un sistema.

Se ha realizado una separación del tráfico de red basado en VLANs para que cada tipo de tráfico del sistema funcione sin interferir con otro.

Las VLANs elegidas han sido:

- Producción (10): Representa todos los servicios operativos que ofrecen las VMs instaladas en cada clúster.
- Gestión (99): Es la elegida para administrar o gestionar los nodos de los clústeres o las VMs alojadas en ellos.
- Almacenamiento (253,101,102,103): Se ven cuatro por los siguientes motivos.
  - ✓ 253: VLAN Asignada al tráfico de la VSAN montada mediante Ceph.
  - ✓ 101 y 102: Asignada al tráfico de la SAN montada por iSCSI.
  - ✓ 103: Asignada a un servidor NFS para distribuir imágenes de SO de manera automática.
- Respaldo (254): Se ha montado un servidor independiente de respaldo para no perder las VMs en caso de accidente. Los nodos de cada clúster usan esta VLAN para este propósito.

## Trunk.

La cantidad de puertos de un switch o router es limitada (hay switches gestionados con solo 8 puertos) así que, un trunk o troncal permite agrupar VLANs por una misma boca física como si éstas estuviesen conectadas a puertos diferentes del switch. Este concepto es la aplicación más utilizada de las VLANs ya que, no es muy práctico usar una VLAN por puerto físico. De esa forma, usando troncales, se pueden implementar tantas VLANs como se necesite en una infraestructura de red.

## Bonding.

Bonding o teaming es la agrupación de dos o más tarjetas de red físicas para que funcionen como una sola. Ésta debe hacerse en ambos lados de la conexión (switch y servidor) y existen varios modos de hacerlo. De todos éstos hay uno que utiliza de una manera más eficiente las interfaces físicas involucradas en el bonding.

Éste se llama LACP (norma IEEE 802.3ad) y ha sido el utilizado en este trabajo. Permite el uso simultáneo de las interfaces agrupadas y sigue funcionando si una de las conexiones falla por cualquier razón (failover).

Aprovechando la explicación de las VLANs más arriba podemos decir que se ha aprovechado la realización de bonding para lanzar varias VLANs por los mismos. De esa manera se consigue un mayor “tubo” por donde enviar la información y un mayor rendimiento en los sistemas que utilizan la red para su funcionamiento.

VLANs que utilizan bonding:

- VLAN 253. Uno de los requisitos importantes de Ceph es la velocidad de la red.

- VLAN 10. Por aquí darán su servicio los servidores virtuales instalados en cada caso.
- VLAN 254. La realización de backups suele ser lenta. Poniendo esta VLAN en un bonding paliamos el problema.
- VLAN 99: Esta es una VLAN conflictiva porque no debería existir en un mundo ideal así que, sabiendo que no genera mucho tráfico y para no malgastar interfaces de red físicas se coloca por un bonding.

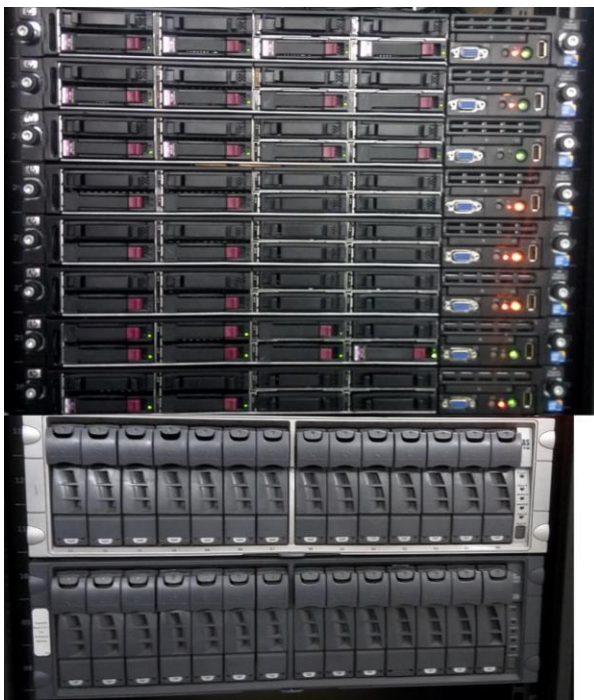
## Armarios de servidores y cableado.

Un servidor no tiene nada que ver con un ordenador normal de escritorio. A partir de ahí se entiende que se necesita una serie de elementos adicionales además de los propios servidores y elementos de red (switches o enrutadores).

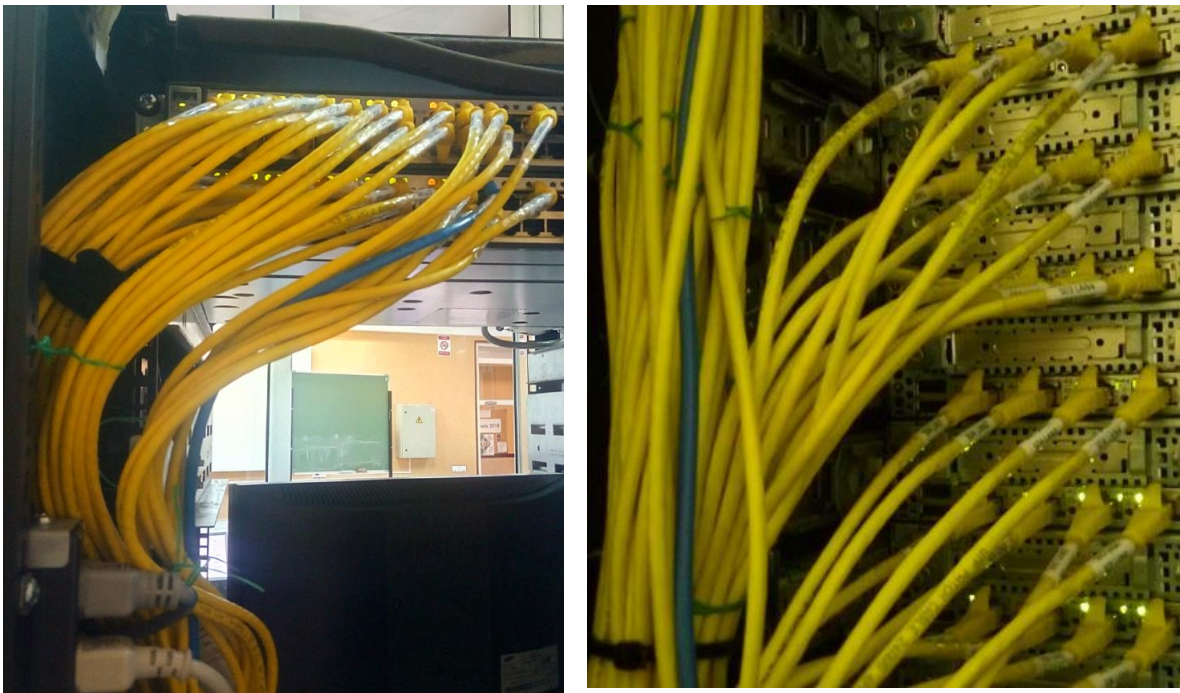
Se ha utilizado un armario de servidores con diferentes elementos de soporte para su instalación en los mismos. Los switches se han colocado en la parte superior y los servidores en la parte central para la comodidad en su manejo.

Se ha cableado por la parte trasera usando dos diferentes colores para distinguir el tráfico de gestión de los servidores (iLO) y el resto de VLANs. Se han etiquetado los cables para su mejor mantenimiento y se han “peinado” para que quede bien organizado.

Fotos de la parte delantera del armario y del peinado de los cables.



*Parte delantera del armario*



*Diferentes partes del peinado del cableado*

## VSAN.

Una SAN virtual es la agrupación de todo el almacenamiento físico al que puede acceder un clúster de servidores de manera que se vean como uno sólo. El tipo de almacenamiento puede ser cualquiera desde los discos duros de un servidor hasta una cabina comercial de discos que proporciona almacenamiento por diferentes tecnologías. Al final el clúster verá un solo disco virtual del que podrá disponer como se desee. Los elementos que forman una VSAN son los siguientes:

- Discos duros o SSDs que pueden estar en cualquier ubicación.
- Software que recoge la información de esos discos duros y los presenta como uno solo.
- Elementos de red que permiten al software mencionado conocer la ubicación de los discos y presentarlo al clúster de servidores que actuará de cliente.

Se ha implementado una SAN virtual para compararla con una SAN basada en iSCSI. Dicha VSAN está basada en Ceph e intenta incorporar todas las ventajas que éste proporciona:

- Open Source.
- Muy escalable (exabyte).
- Altamente disponible.

- Distribuido.
- Sencillo de gestionar.
- Autoreparable.

## Backups.

Los backups o copias de respaldo son clave en toda empresa. Estas permiten restaurar la información perdida ante cualquier fallo o contingencia en el sistema que estén instaladas.

En nuestro caso, aunque no es la mayor parte del trabajo, no se ha querido dejar de lado esta parte y se ha implementado un servidor de backup de la manera más sencilla posible aprovechando la capacidad de Proxmox de gestionar por sí mismo el espacio que le proporciona dicho servidor.

Se ha instalado en uno de los servidores disponibles, un servidor NFS dentro de la última versión de SO CentOS que proporciona espacio para las copias de respaldo. Se ha aprovechado la VLAN de respaldo para que todos los servidores tengan acceso al mismo. También, se han preparado diferentes zonas de backups para los dos casos del trabajo de manera que los diferentes usuarios de los dos casos no interfieran entre sí.

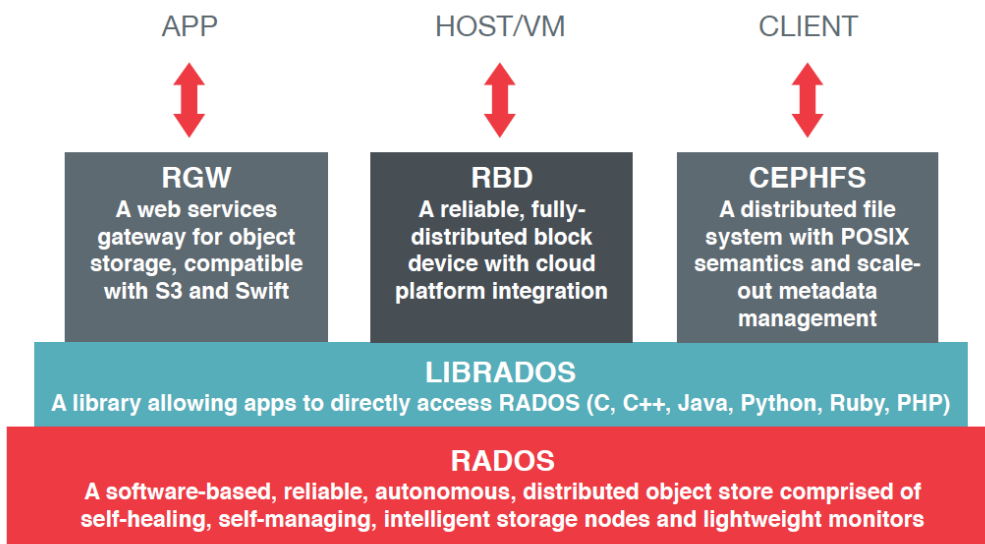
## Entorno práctico.

Como se ha hablado anteriormente, se han implementado dos tecnologías de almacenamiento para dar servicios a dos clústeres por separado. Una de ellas es Ceph, desarrollada en gran parte por una subsidiaria de RedHat llamada Inktank y, la otra es iSCSI, un protocolo de red que permite la utilización de dispositivos de almacenamiento a nivel de bloques. Para cada una se explicará cómo funciona el almacenamiento y su montaje con la opción de virtualización elegida.

### *Ceph.*

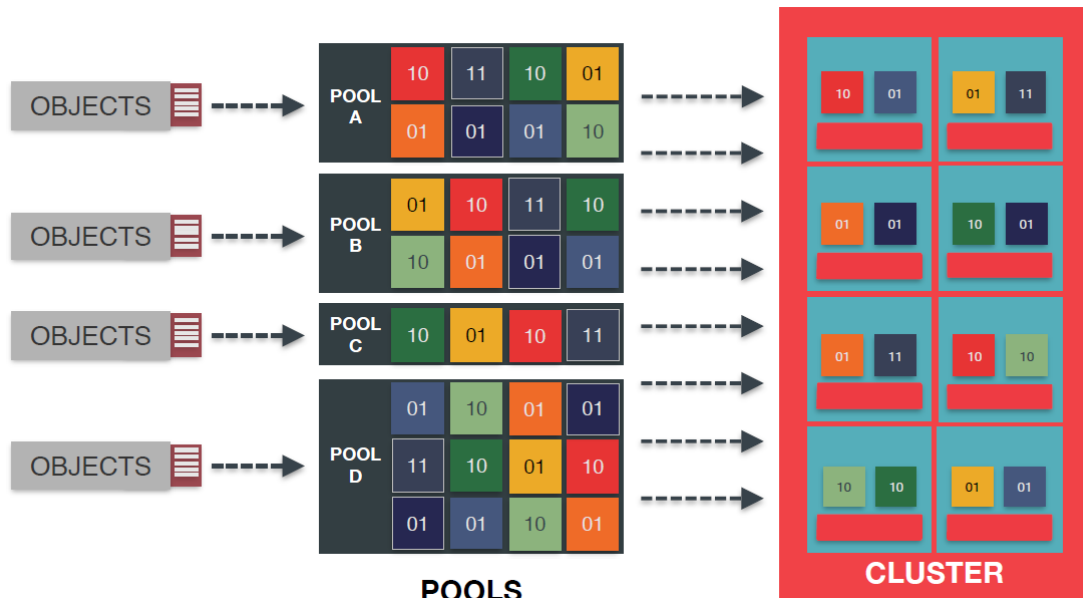
Ceph es un sistema software de almacenamiento libre diseñado para ofrecer objetos, dispositivos de bloques y sistemas de ficheros desde un único servidor o un clúster de almacenamiento.

Veamos la siguiente imagen para hacernos una idea general de su estructura.



Aquí se ven los tres tipos de elementos que puede ofrecer Ceph aunque para el trabajo solo se ha usado de la parte de RBD. Ésta nos ofrece dispositivos de bloques que serán los discos de nuestras VMs.

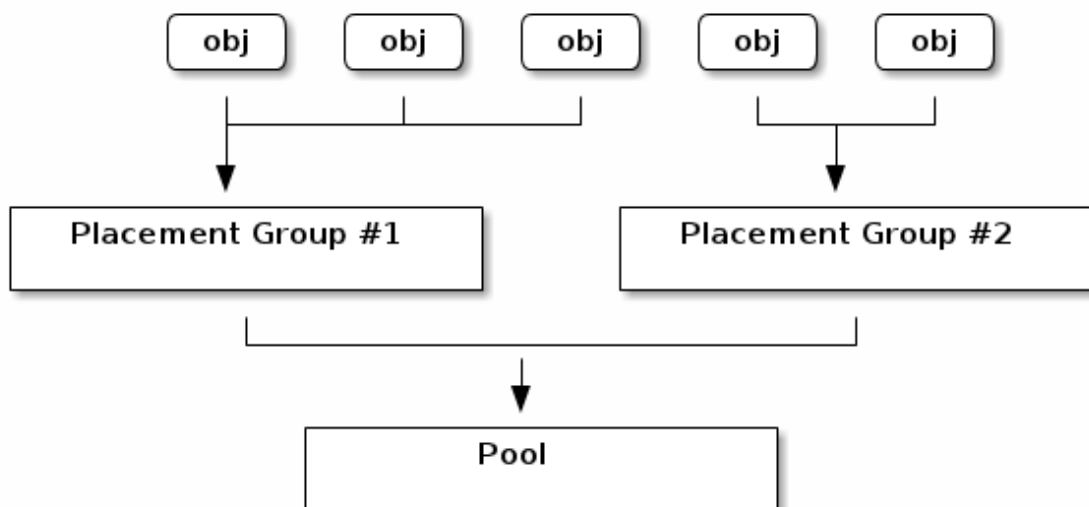
Ahora veamos como distribuye Ceph nuestros datos en el servidor para acceder más tarde a ellos. echemos un vistazo a la siguiente imagen.



Los bloques azules de la derecha son los discos que se introducen en los servidores. Ceph los llama OSD (Object Storage Daemons) y dentro de ellos están repartidos los datos de las VMs según unas reglas predeterminadas. A su vez, los discos de las VMs están representados por los objetos grises de la izquierda que se reparten dentro de los pools que hay en medio.

Los pools son la manera en la Ceph agrupa los objetos servidos a sus clientes para distribuirlos posteriormente a los OSDs según un algoritmo de mapeado llamado CRUSH (Controlled Replication Under Scalable Hashing).

Esta otra imagen aclarará un poco más el concepto.



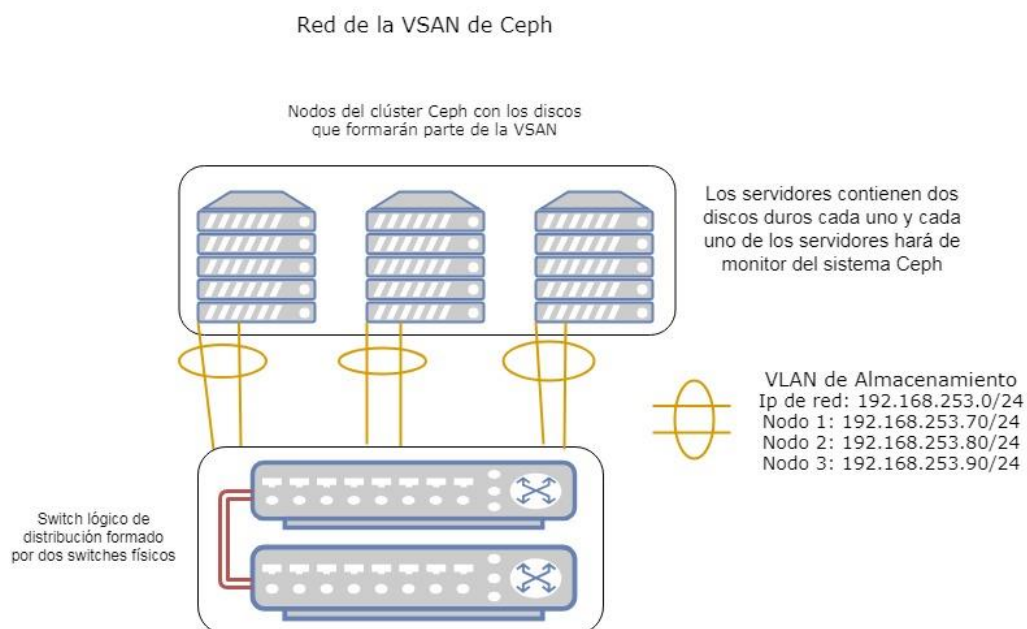
En resumen, en un primer nivel están los discos duros o SSDs, llamados OSD por Ceph, en un segundo nivel están los pools (es la parte que debemos configurar para definir nuestras zonas de almacenamiento) y, por último, tenemos los datos (discos virtuales) de nuestras VMs.

Toda la explicación anterior se verá más clara después de la instalación de Ceph con Proxmox.

### *Instalación del clúster Proxmox + Ceph.*

#### Esquema de red.

Aunque no se ha dicho en su explicación Ceph adopta muchas formas. En este proyecto se ha utilizado la que se ve en la imagen.



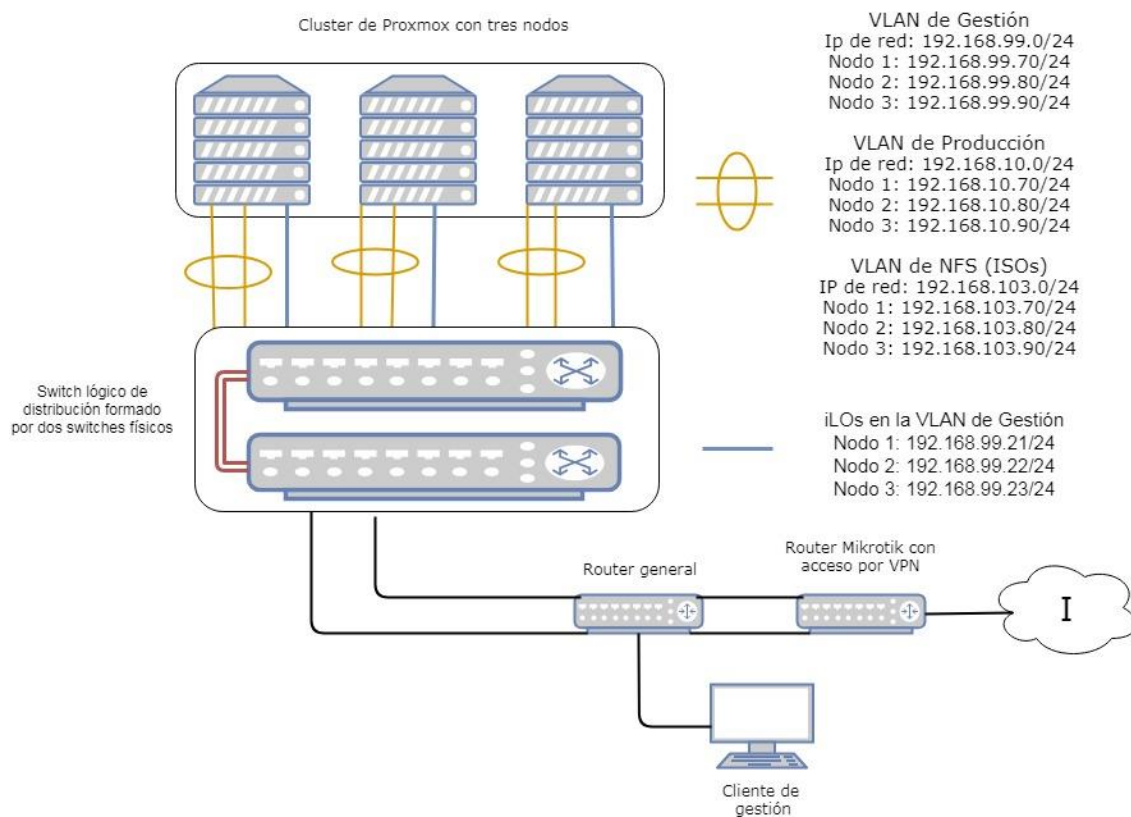
Como se ve en la imagen tenemos tres servidores a los que se les ha instalado dos discos duros para formar un servidor Ceph. Éste formará la VSAN que proporcionará los discos a las VMs del clúster de Proxmox.

Cada uno de los servidores actuará también de monitor, esto quiere decir que cada uno almacenará el mapa CRUSH mencionado anteriormente donde se explicó cómo están distribuidos en los discos los objetos que Ceph sirve al clúster Proxmox.



Ahora véase la siguiente imagen que completará el conjunto.

Red del clúster Proxmox que usa Ceph como almacenamiento



Como se muestra en la imagen, los servidores son los mismos que en la anterior ya que en ellos está instalada la dupla Proxmox + Ceph. Por otra parte, hay que recalcar que cada servidor tiene cuatro tarjetas de red pero, en cada diagrama se ha detallado la que es más importante para su entendimiento.

En cuanto al cliente de gestión y al acceso VPN no son más que elementos que se han utilizado para acceder al sistema descrito en diferentes momentos y poder gestionarlo adecuadamente.

Respecto a las VLANs detalladas, habría que añadir las siguientes:

- Las VLANs de gestión, producción y NFS van por el mismo bonding. Con esto conseguimos aprovechar mejor las tarjetas disponibles en los servidores.
- La VLAN de Almacenamiento es la que más tráfico soportará. De ahí que se haya dejado únicamente para Ceph con un bonding.

## Instalación de Proxmox.

Detalles del material a utilizar:

- 3 servidores HP con las siguientes características:
  - Dos procesadores Intel Xeon modelo E5620. Proporcionan 16 núcleos en total cada uno.
  - Cuatro discos instalados. Dos en RAID 1+0 para Proxmox y dos en RAID 0 para Ceph.
  - 16 GB de RAM
  - 4 tarjetas de red.
  - iLO3 para gestión del servidor. Por aquí utilizaremos las siguientes ISOs:
    - ✓ Proxmox 5.2
    - ✓ Gparted 0.31

Conocida la distribución de los discos en el servidor el hipervisor y los restantes en RAID 0 cada uno para el clúster Ceph. Nos aseguramos con una ISO de Gparted que las tablas de particiones de todos los discos sean GPT, de otra manera no funcionará.

Hacemos uso de la iLO para instalar el servidor. Con la versión 3 de ésta podemos instalar Proxmox desde una interfaz web o una aplicación que nos proporciona HP.

La instalación de Proxmox en cada servidor mediante la iLO es muy sencilla y solo requiere de unos pocos pasos. Una vez introducida la información pedida por el asistente se instalará el sistema y reiniciará por sí mismo.

## Configuración de Proxmox.

A partir de aquí, es necesario hacer unos pasos para dejar el sistema accesible por web.

Se configuran todas las interfaces de red, bondings, puentes para las VMs y VLANs como se ha especificado anteriormente. Existe un fichero llamado `/etc/network/interfaces` donde está toda la información que Proxmox necesita para que la red funcione.

Como se ha mencionado en la comparativa, Proxmox utiliza dos herramientas para la configuración de la red. Linux Networking y OVS (OpenvSwitch). Aquí se han utilizado las dos para aprovechar las bondades de ambas.

Se establece el nombre de la máquina editando el fichero `/etc/hosts` y se reinicia el servidor para que los cambios tengan efecto.

Una vez el servidor es accesible por web, se probará el comando ping en la terminal que ofrece la interfaz web, para verificar que la red está bien y que el resto de servidores contestan al comando. Se establece la VLAN de gestión para que sea la única por la se pueda acceder a la interfaz web y al servicio SSH.

Como se tiene una versión sin soporte, se deben deshabilitar los repositorios "enterprise" que vienen por defecto y añadir los de la comunidad y de pruebas. El primero está en este archivo:

```
/etc/apt/sources.list.d/pve.enterprise.list
```

Y los nuevos a añadir son:

```
deb http://download.proxmox.com/debian stretch pve-no-subscription
deb http://download.proxmox.com/debian stretch pvetest
```

Se actualizan los servidores aprovechando los nuevos repositorios y se procede a la creación del clúster propiamente dicho.

## Creación del clúster Proxmox

Requisitos antes de la instalación del clúster:

- Comprobar que la VLAN de gestión vaya bien entre todos los nodos y no dé problemas. La comunicación del clúster irá sobre esa VLAN.
- La hora y fecha de los servidores debe ser la misma o dará problemas de sincronización.
- El servicio SSH debe estar activo en todos los nodos y los nombres de cada uno de los nodos deben poder ser vistos por todos los nodos. Comprobar fichero /etc/hosts
- Debe haber una red de almacenamiento completamente separada de la de comunicación ente nodos.
- Para que exista Alta Disponibilidad (HA en adelante) debe haber mínimo tres nodos. Existe una alternativa en la que se pueden utilizar dos nodos pero la HA queda muy comprometida.
- Todos los nodos deben tener la misma versión de Proxmox.

Con la última versión se ha simplificado mucho la creación del clúster y se puede hacer desde la web. Los pasos son:

- Crear el clúster en uno de los nodos dentro de la sección de "Datacenter"
- Unir el resto de nodos al primero mediante la copia de una clave que te da el primer nodo cuando se crea el clúster.

Eso es todo. A partir de ahora se tiene un clúster Proxmox manejable desde cualquier nodo y mediante la misma interfaz web anterior.

Cluster Information					
<a href="#">Create Cluster</a> <a href="#">Join Information</a> <a href="#">Join Cluster</a>					
Cluster Name:	proxmox-ceph	Config Version:	3	Number of Nodes:	3
Cluster Nodes					
Nodename	ID ↑	Votes	Ring 0	Ring 1	
proxmox-S70	1	1	192.168.99.70		
proxmox-S80	2	1	192.168.99.80		
proxmox-S90	3	1	192.168.99.90		

*Cluster Proxmox creado*

## Instalación del servidor Ceph:

Requisitos antes de su instalación

- Comprobar que los discos para Ceph estén disponibles en cada nodo (lo ideal es tener igual número de discos por nodo).
- Comprobar que la VLAN de almacenamiento (nº 253) sea accesible en todos los nodos.

Una vez, cumplidos éstos, se ejecutan los siguientes comandos por consola antes de pasar a la interfaz web.

- Ejecutar comandos de instalación de ceph e inicialización de la red

```
# pveceph install --version luminous
```

```
# pveceph init --network IP_VLAN_Almacenamiento/24
```

- Crear el primer monitor de Ceph por línea de comandos.

```
# pveceph createmon
```

- Volver a la interfaz web y crear el resto de monitores (uno por nodo).
- Crear OSDs para almacenamiento compartido.
- Crear pool en apartado de pools. Aquí depende bien de lo que se necesite. Es una buena práctica crear primero un pool temporal para ejecutar sobre él los siguientes comandos de benchmark y ver en primera instancia que rendimiento ofrece el pool.

```
# rados -p nombre_pool bench 60 write --no-cleanup
```

```
# rados -p nombre_pool bench 60 seq
```

```
# rados -p nombre_pool bench 60 seq
```

Todos estos comandos se pueden ejecutar en varios pools de prueba para considerar cual es que da un mejor rendimiento. En nuestro caso eran dos y nos hemos decantado por uno de ellos.

- Por último, crear almacenamiento de bloques RBD (donde se crearán los discos de las VMs) y copiar clave en carpeta /etc/pve/priv/ceph/ para que funcione. La clave copiada debe tener el mismo nombre que pool y el almacenamiento RBD).

Ya se pueden crear VMs con Ceph como almacenamiento compartido y con las características del clúster.

ID ↑	Type	Content	Path/Target	Shared	Enabled
Backup-Pruebas-Ceph	NFS	VZDump backup file	/mnt/pve/Backup-Pruebas-Ceph	Yes	Yes
ISOs_VMs	NFS	ISO image	/mnt/pve/ISOs_VMs	Yes	Yes
PYME	RBD (external)	Disk image		Yes	Yes
PYME-backups	NFS	VZDump backup file	/mnt/pve/PYME-backups	Yes	Yes
local	Directory	VZDump backup file, ISO image	/var/lib/vz	No	Yes
local-lvm	LVM-Thin	Disk image, Container		No	Yes

*Zona de almacenamiento RBD proporcionada por Ceph*

## iSCSI

iSCSI no es más que una extensión de SCSI, un protocolo de comunicación entre dispositivos. En SCSI esos dispositivos suelen estar dentro de una misma máquina pero en iSCSI están en máquinas diferentes comunicándose a través de una red. La velocidad de esa red más la rapidez de los dispositivos proporciona el rendimiento del sistema iSCSI instalado.

Conceptos importantes de iSCSI a tener en cuenta:

- **Iniciador iSCSI:** Es análogo al cliente en una comunicación TCP/IP. Empieza la comunicación y envía las órdenes necesarias para recibir la información que desea. Tiene un nombre único ante el mundo.
- **Objetivo(target) iSCSI:** Es el análogo al servidor en una comunicación TCP/IP. Posee el almacenamiento requerido por el iniciador y responde a las órdenes del mismo. Al igual que el iniciador, tiene un nombre único ante el mundo para poder identificarlo.
- **IQN:** Es el nombre que identifica a un target o iniciador y posee la siguiente estructura: `iqn.fecha.nombre_autorizado.subnombre_autorizado`

- LUN: Representa un dispositivo lógico iSCSI individualmente direccionable. En otras palabras, el disco que nos ofrece el target. Un mismo target puede ofrecer varias LUNs.

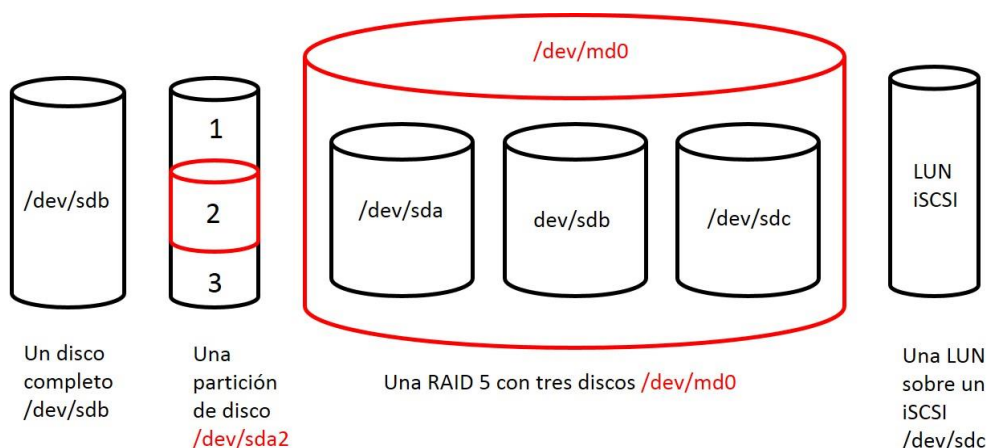
Una vez explicado esto, hay que hacer un pequeño inciso. Aunque nuestro servidor iSCSI nos proporcione varias LUNs, el clúster Proxmox no las usará directamente sino que, montará sobre ellas un sistema LVM para que las VMs sean recuperables desde nuestro servidor de respaldo.

## LVM

LVM es un sistema de gestión de dispositivos de almacenamiento que agrupa uno o más discos o particiones de disco, llamados volúmenes físicos, en lo que se llama grupo de volúmenes para más adelante crear nuevas zonas de almacenamiento denominadas volúmenes lógicos. Veamos los conceptos clave por separado:

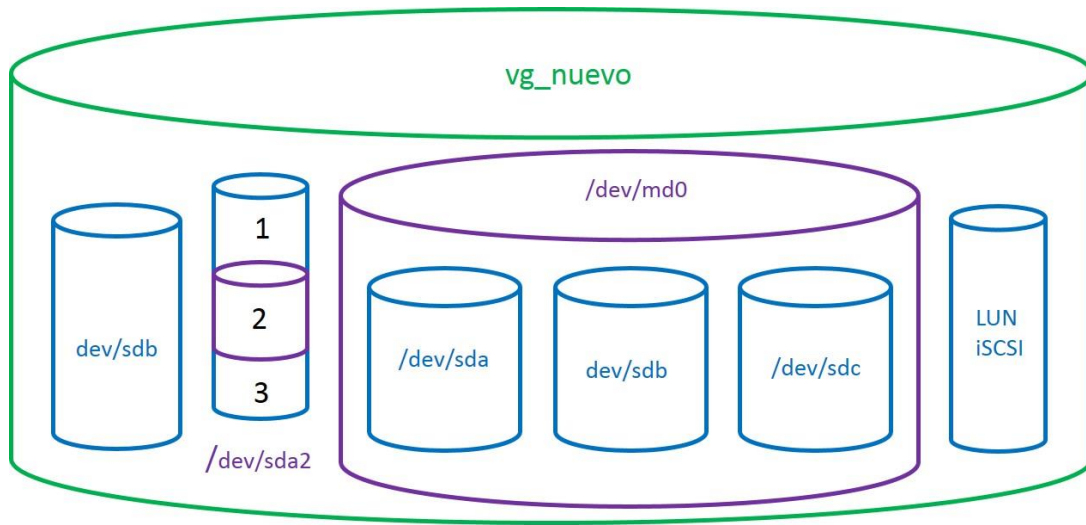
- Volumen físico: Son los dispositivos físicos que agruparemos y pueden ser desde un disco entero pasando por una partición del disco a, las LUNs que nos ofrece nuestro servidor iSCSI. De estos, pueden ser uno o más volúmenes físicos.
- Grupo de volúmenes: Es la agrupación propiamente dicha de los volúmenes físicos. En un servidor o clúster pueden haber más de un grupo de volúmenes.
- Volumen lógico: es el último nivel de la estructura y es donde se crean los sistemas de ficheros que usarán las aplicaciones o sistemas operativos.

He aquí unas imágenes que aclararán el funcionamiento del sistema.



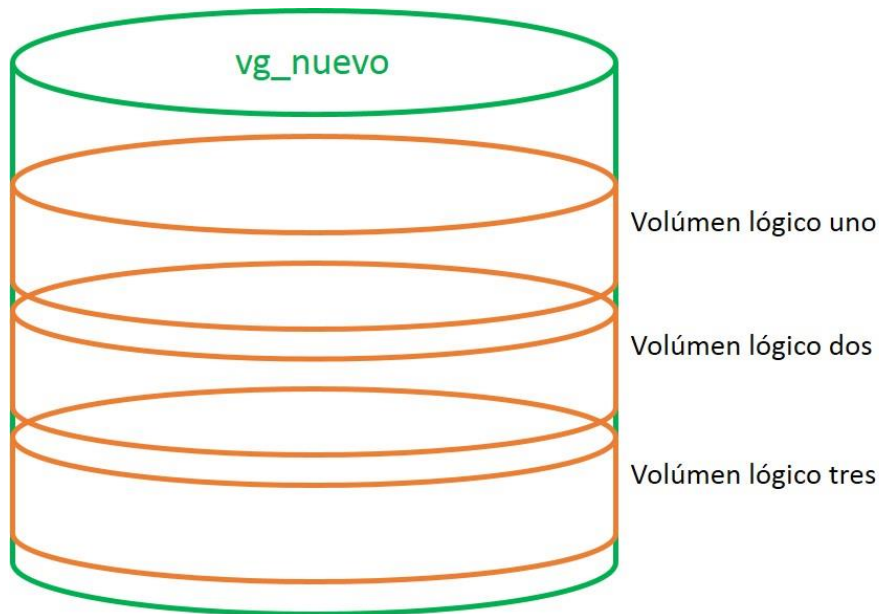
Dispositivos que pueden usarse como volúmenes físicos

## Volúmenes físicos



Un grupo de volúmenes (VG) compuesto por cuatro PV diferentes

Grupo de volúmenes



Tres volúmenes lógicos (LV) en un grupo de volúmenes (VG) usando el espacio de los cuatro volúmenes físicos (PV) anteriores

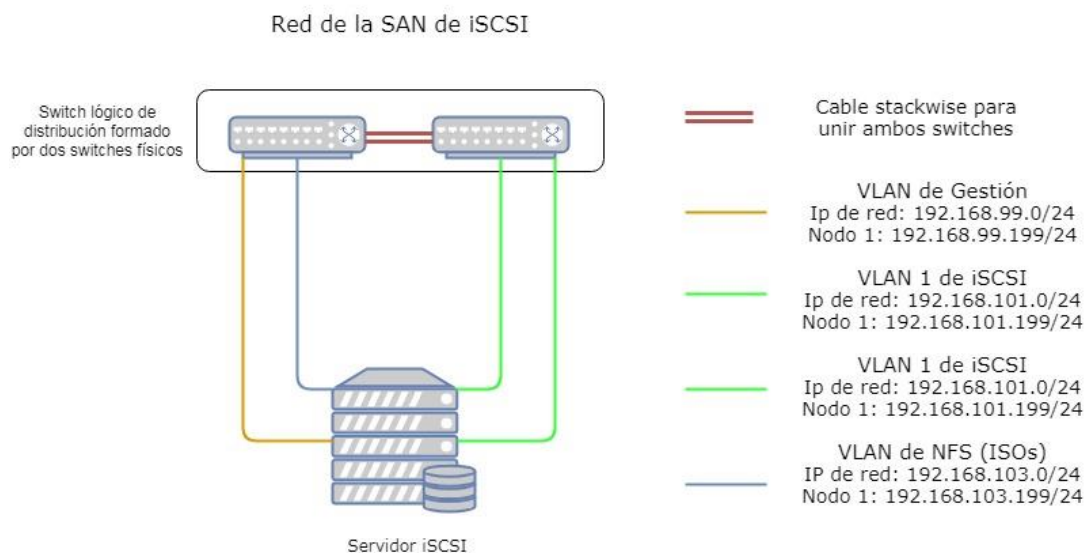
Volúmenes lógicos

Con esto tenemos una idea del sistema de almacenamiento que queremos implementar. Ahora veamos su montaje.

## Instalación del clúster Proxmox + iSCSI

### Esquema de red de iSCSI

Al igual que en el otro sistema, veamos una imagen del diseño de la red del servidor de iSCSI.



Hay que aclarar que los dos cables por los que van las VLANs de iSCSI deben de ir por separado. iSCSI desaconseja el uso de bonding para realizar multipath. Este concepto, se aclarará más adelante.

Comentar que, aunque no aparece, este servidor posee una iLO igual que los servidores del clúster que accederán a su almacenamiento.

### Instalación de servidor iSCSI (FreeNAS)

Detalles del material a utilizar:

- 1 servidor HP con las siguientes características:
  - Dos procesadores Intel Xeon modelo E5620. Proporcionan 16 núcleos en total cada uno.
  - Siete discos instalados. Dos en RAID 1+0 para FreeNAS y cuatro en RAID 0 para el servicio de iSCSI y uno en RAID 0 para el servicio NFS de imágenes de disco.
  - 16 GB de RAM.
  - 4 tarjetas de red.
  - iLO3 para gestión del servidor. Por aquí utilizaremos las siguientes ISOs:



## ✓ FreeNAS 11.1

En cuanto a la distribución de los discos, se aprovechará que FreeNAS puede hacer RAID software (la “best practice” de FreeNAS recomienda usar RAID software) para implementar un RAID 10 en 4 de esos discos y el disco restante se creará un espacio para servir imágenes de SO a las VMs de los dos clústeres.



*Servidor iCSI listo para instalación con los discos preparados*

Se instala FreeNAS mediante la iLO. Al igual que Proxmox es muy sencilla y solo hay que seguir unos pocos pasos.

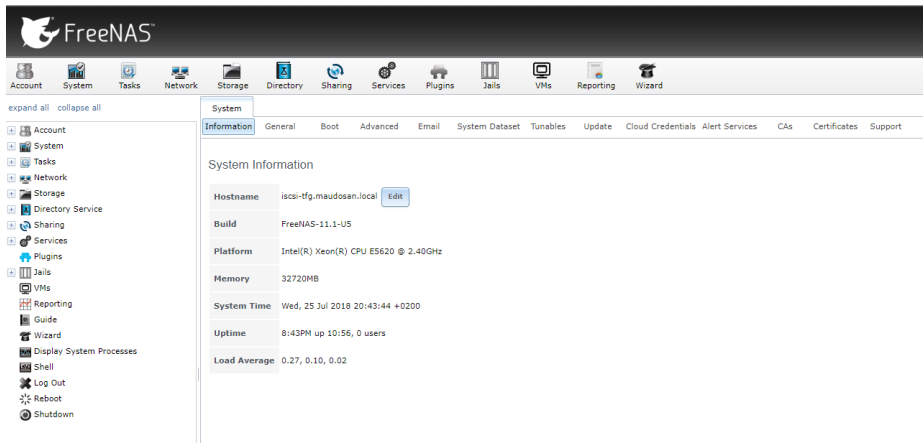
Una vez instalado FreeNAS se llegará a una consola de administración. En ella hay que configurar la IP de gestión y acceder a la interfaz web de FreeNAS para configurar el resto de funciones del servidor.

Dentro de la interfaz, es conveniente asegurarse de que la web y el servicio SSH solo son accesible desde la VLAN de gestión.

Ahora se puede configurar el resto de VLANs descritas en el diagrama. Las VLANs a configurar serían:

- VLAN de NFS
- VLAN iSCSI1
- VLAN iSCSI2

La razón por la que iSCSI funciona por dos VLANs es porque se va a implementar multipath. Las LUNs que proporcionará el servidor las verán los nodos del clúster desde dos rutas diferentes. Esto quiere decir que Proxmox verán dos discos en lugar de uno. Como este funcionamiento puede ocasionar problemas en la información guardada en la LUN se instalará en los nodos del clúster un software llamado multipath. Este detectará que las dos rutas provienen de la misma LUN y le informará a Proxmox que solo hay un único dispositivo. Además, las dos rutas proporcionan un mecanismo de redundancia en el que si una de las rutas falla por la razón que sea, la LUN seguirá estando disponible por la ruta restante.



*Aspecto de FreeNAS instalado*

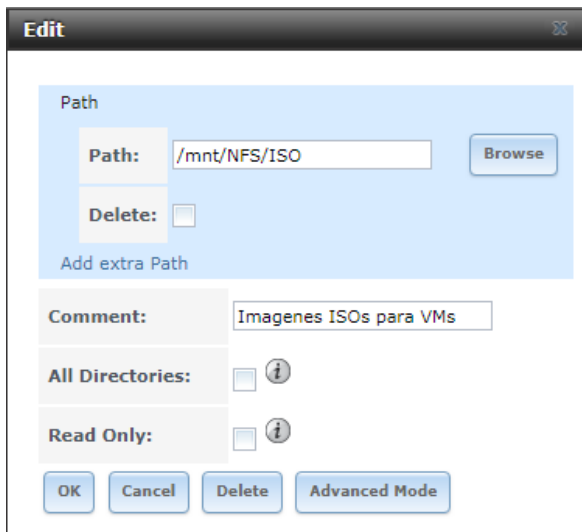
Comprobación de los discos y creación de la RAID deseada.

Name
DATA
mirror-1
da1p2
da4p2
mirror-0
da3p2
da2p2

*Distribución de los discos en RAID 1+0*

Montaje del servicio NFS para compartición de ISOs.

Mediante el disco restante crear zvol (volumen) y sobre éste la carpeta para compartir por NFS. Configurar servicio NFS y activarlo es muy sencillo mediante la web



*1 Carpeta donde residirán las ISOs*

### Configuración del servicio iSCSI.

Para tener las LUNs disponibles por los nodos del clúster se deben seguir los siguientes pasos:

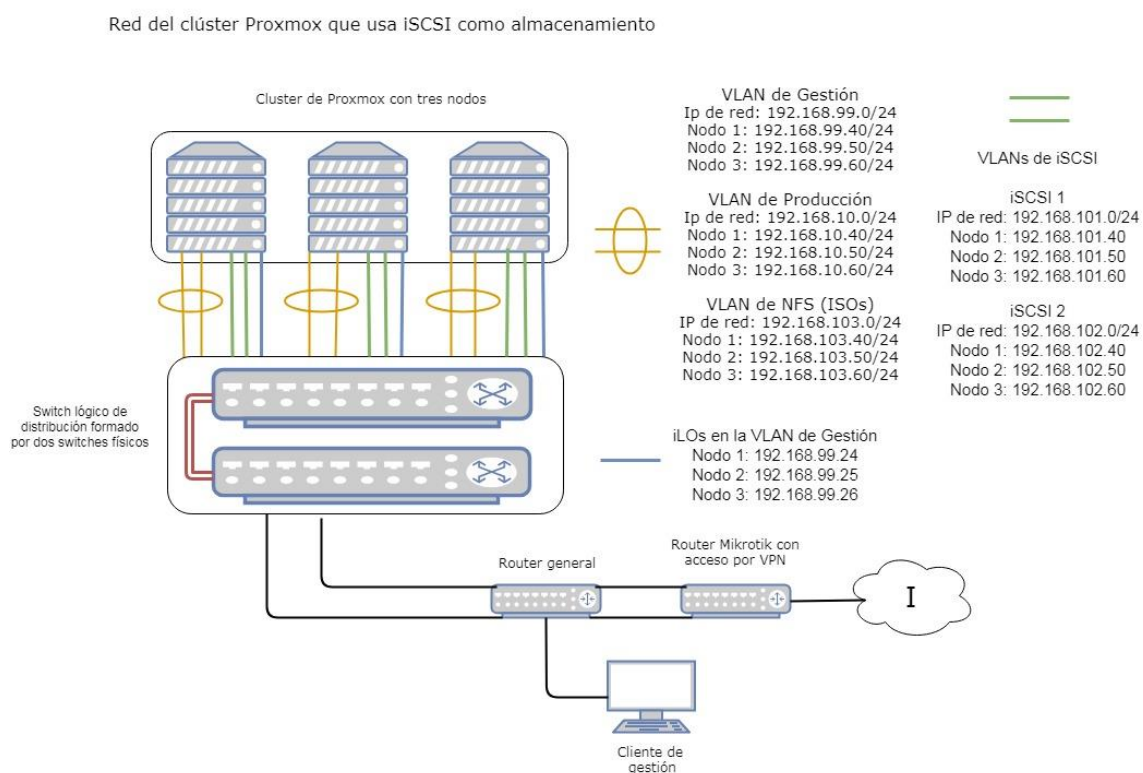
- Activar el servicio iSCSI en la pestaña de servicios y dejarlo que se inicie al arrancar el servidor.
- Establecer el nombre base del iqn del target (objetivo)
- Definir los portales por los que se accederá al target.
- Definir la seguridad del target. Esto es el usuario y contraseña para poder acceder al target (Opcional).
- Establecer el nombre del target. Es la parte final del nombre completo del target.
- Definir la propia LUN que se verá dentro del target.
- Y asociar la LUN con el target correspondiente. Puede haber varios targets con varias LUNs cada uno.

Sharing						
Apple (AFP) UNIX (NFS) WebDAV Windows (SMB) <b>Block (iSCSI)</b>						
Target Global Configuration Portals Initiators Authorized Access Targets <b>Extents</b> Associated Targets						
<b>Add Extent</b>						
Extent Name	Serial	Extent Type	Path to the extent	Logical Block Size	Disable Physical Block Size Reporting	
docencia1	e83935b82e0c00	ZVOL	/dev/zvol/DATA/DOCENCIA1	512	false	
docencia2	e83935b82e0c01	ZVOL	/dev/zvol/DATA/DOCENCIA2	512	false	
iscsi-pruebas	e83935b82e0c02	ZVOL	/dev/zvol/DATA/ISCSI_PRUEBAS	512	false	

Captura de las LUNs

## Esquema de red de Proxmox.

Veamos cómo está diseñada esta parte del sistema



He aquí una explicación que completa la información sobre las VLAN detalladas en este diagrama y el anterior de la red de iSCSI:

- VLAN de gestión: Por ella se gestionarán los nodos del clúster y las iLOS de los servidores. Es la numero 99.

- VLAN de producción: Con ella daremos servicio a las VMs alojadas en el clúster y si hace falta podemos dar de alta en su momento IPs temporales para las actualizaciones de los nodos del clúster. Comparte troncal con la anterior y es la nº 10.
- VLANs de iSCSI: El servidor de iSCSI hará uso de estas VLANs. Debido a exigencias del protocolo iSCSI, no utilizan bonding. Una de ellas va por acceso y la otra en una troncal compartiendo cable con la VLAN siguiente. La intención es tener dos rutas de acceso al servidor para tener redundancia a fallos. Son la 101 y la 102.
- VLAN de Backup: Es la conexión al servidor NFS que sirve de respaldo. Aprovecha el bonding hecho para la VLAN de almacenamiento comparte troncal con la segunda VLAN de iSCSI (la 102) y es la nº 254.

### Instalación del clúster Proxmox.

Los detalles en cuanto al material utilizado y la instalación de esta parte son los mismos que los de la parte de Proxmox cuando se instala del clúster de Proxmox + Ceph. Volver a esa sección para realizar los mismos pasos pero usando la información del esquema de red explicado para este caso.

Una vez se tenga el clúster de Proxmox en marcha hay que hacer que vea las LUNs del servidor de iSCSI.

### Descubrimiento de LUNs y creación de almacenamiento LVM.

Comprobar que desde los hipervisores Proxmox se puede acceder a los targets. Instalar y configurar software de multipath en los hypervisores. Usar identificador wwid para las LUNs en la configuración del multipath. Una vez comprobado esto, se deben realizar estas acciones para tener almacenamiento iSCSI en Proxmox:

- Descubrimiento de LUNs mediante la interfaz web de Proxmox.
- Configuración del servicio multipath mediante el uso de los identificadores wwids proporcionados por las LUNs para que el multipath detecte las rutas.
- Inserción de los módulos de multipath y round robin en el kernel
- Reinicio del servicio de multipath. Estos tres últimos pasos deben hacerse desde consola en todos los nodos del clúster.
- Creación por consola en solo uno de los nodos de los volúmenes físicos y grupos de volúmenes necesarios.
- Creación en la web de los volúmenes lógicos según se necesite

ID ↑	Type
Backup-Docencia1	NFS
Backup-Docencia2	NFS
Backup-pruebas-iSCSI	NFS
Docencia1	LVM
Docencia1-LUN	iSCSI
Docencia2	LVM
ISO_VM	NFS
iSCSI-pruebas	LVM
local	Directory
local-lvm	LVM-Thin

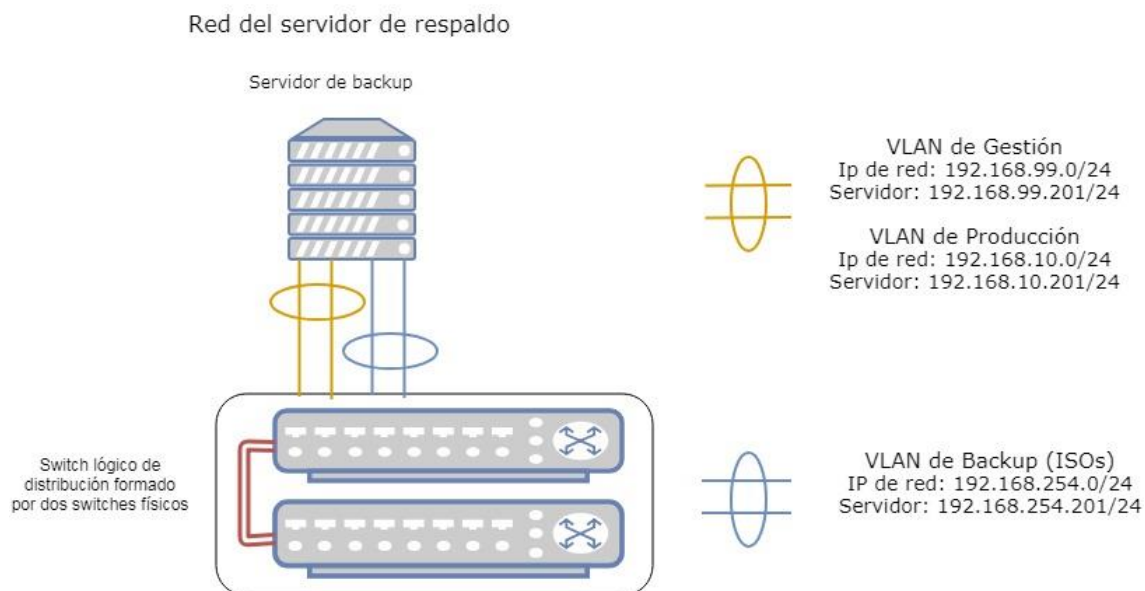
*Captura de los espacios vistos por el clúster donde se aprecian los volúmenes lógicos sobre las LUNs*

A partir de aquí ya podremos crear VMs usando esos volúmenes y utilizando todas las características avanzadas del clúster.

### *Servidor de Backup.*

Esta máquina se ha montado con el propósito de proporcionar seguridad a los dos clústeres implementados en el trabajo. No es el objetivo principal del proyecto pero ofrece un plus más a la hora de trabajar en entornos IT de cualquier tipo.

### Esquema de la red.

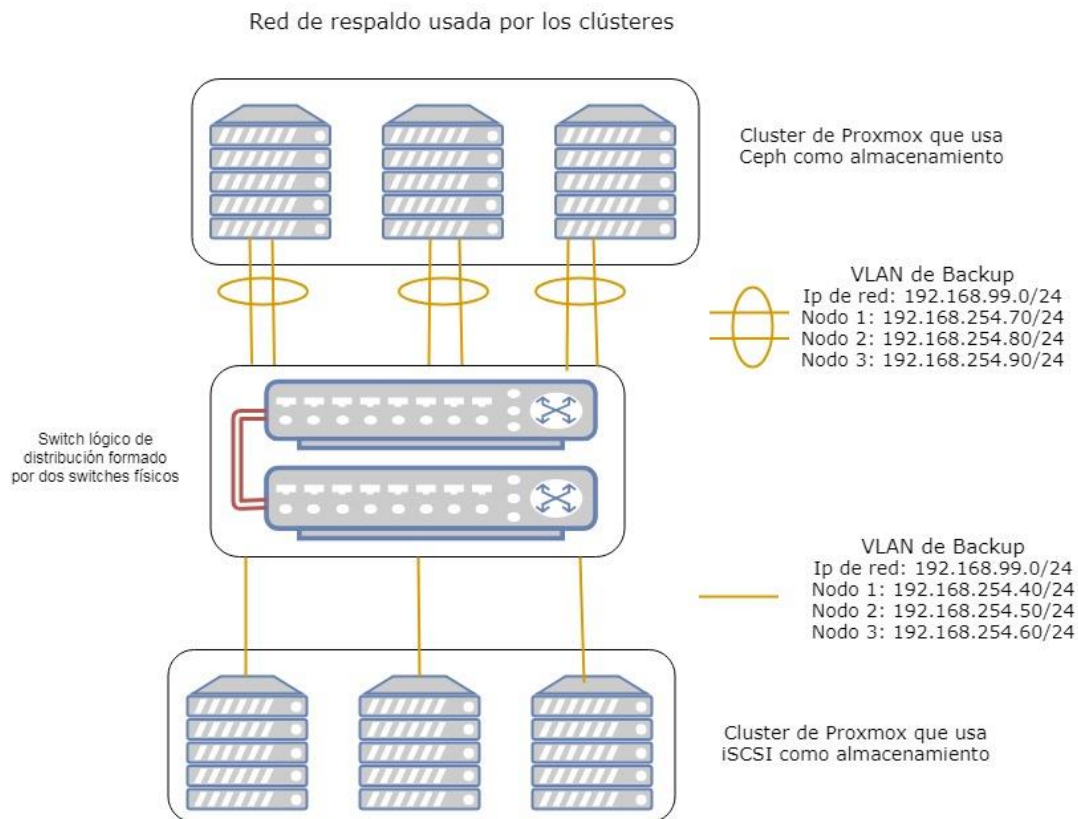


Por lo que respecta a las VLAN el diseño es muy sencillo. Solo hacen falta las VLANs de backup y la de gestión.

Se puede ver que el servidor de backups tiene VLAN de producción. Ésta se puede deshabilitar ya que no es importante para su función. Se podría habilitar en momentos puntuales para actualizaciones del sistema operativo del servidor.

Faltaría añadir que este servidor también posee una iLO, la cual, estaría dentro de la VLAN de gestión y desde la que se puede gestionar.

Veamos ahora como quedarían los dos clústeres en esta red.



Por razones de espacio se ha obviado el resto de información de red de los nodos de los dos clústeres. Por otra parte, es interesante ver como por razones de diseño de la red de iSCSI solo se dispone de una conexión a la VLAN de backup por cada nodo mientras que en el clúster de Ceph se ha aprovechado el bonding por donde va Ceph para compartirlo con el backup.

## Instalación del servidor de respaldo.

### Descripción del material a utilizar

- 1 servidor HP con las siguientes características:
  - Dos procesadores Intel Xeon modelo E5620. Proporcionan 16 núcleos en total cada uno.
  - Dos discos instalados. Uno en RAID 0 para el SO y otro para los backups.
  - 16 GB de RAM
  - 4 tarjetas de red.
  - iLO3 para gestión del servidor. Por aquí utilizaremos las siguientes ISOs:
    - ✓ ISO de CentOS 7.3





*Servidor de backup listo para instalar con los discos preparados*

Respecto a la distribución de los discos se quiere recalcar que la función de backup no es la parte más importante del proyecto pero se ha querido implementar porque proporciona tranquilidad para el funcionamiento diario de este tipo de sistemas. Si añadimos a esto qué por razones de disposición de material, la distribución de discos es la que es. Aun así, resulta suficiente para la presentación del trabajo.

### Instalación de CentOS.

Se aprovecha la iLO para introducir la imagen e instalar el sistema.

Como la instalación del SO se va a realizar mediante lo que se llama una instalación por red, se necesita habilitar la interfaz de red asociada a la VLAN de producción (salida a Internet) y elegir un repositorio desde el que instalar todo lo necesario de CentOS. Todo esto se realiza desde el asistente de instalación de CentOS.

Una vez instalado el sistema y reiniciado el servidor se procede a configurar el resto de interfaces de red, bondings y VLANs descritas en la infraestructura de red. Comentar de nuevo la necesidad de modificar el fichero `/etc/modules` para que las VLANs configuradas funcionen correctamente. También, como en el resto de servidores, es conveniente establecer el nombre de la máquina. Realizar un reinicio después de estos pasos para que todo funcione como debe ser.

Pruebas con el comando ping para verificar que todo está bien y que los dos clústeres tienen acceso al servidor.

Configuración del servicio SSH para su gestión por la VLAN correspondiente.

Configuración del segundo disco para que el servicio de NFS lo tenga siempre disponible (archivo `/etc/fstab`). Creación de sistema de ficheros XFS (“best practices” de RedHat) y montaje del mismo.

Creación de los espacios correspondientes a cada backup. Básicamente son carpetas con un nombre descriptivo relacionado con el área de almacenamiento que respaldan.

Instalación y configuración del servicio NFS para su uso por parte de los dos clústeres.

Los pasos son:

- Instalamos el paquete `nfs-kernel-server`:
- Creamos un directorio (el que queramos) que se va a exportar o compartir (share):
- Se le dan los permisos necesarios. En nuestro caso será el usuario root el único que tenga acceso al directorio.

Lo que viene ahora se puede hacer de varias formas. Nosotros permitiremos la entrada a cualquier IP de la VLAN.

- Editamos el archivo `/etc/exports` para que NFS sepa que carpeta tiene que compartir y como las tiene que compartir
- Se le comunica al servicio NFS que nuestro directorio está listo para compartir.

Para finalizar. Estos servicios son los que tienen que estar en marcha para que los clientes NFS (los nodos de los dos clústeres) puedan acceder al share creado.

- Servicio `nfs-kernel-server`
- Servicio `rpcbind`

Al llegar a este punto ya se puede hacer uso de los ficheros que proporciona el servidor NFS.

### *Casos de aplicación para los sistemas implementados.*

En este punto se presentan unos casos reales de uso en los que los sistemas de virtualización implementados pueden desempeñar su función de una manera satisfactoria.

Entorno docente.

#### **Motivación del caso.**

En una asignatura de universidad se necesita por parte de los alumnos una serie de recursos hardware para la realización de unas prácticas relacionadas con la asignatura. El profesor no sabe, ni debe, si sus alumnos poseen esos recursos para realizar dichas prácticas.

Para facilitarles la tarea, el profesor puede ofrecer a demanda de los alumnos y dentro de unos límites, una serie de recursos hardware virtuales para que los alumnos realicen dichas prácticas y el profesor corrija el trabajo realizado.

Como los recursos reales son limitados, el profesor anunciaría desde el principio de la asignatura la disponibilidad de esos recursos y, según la demanda de los alumnos, desplegaría los recursos demandados.

#### **Diseño.**

Para simplificar el diseño y explicar el propósito del caso de uso se utilizarán dos grupos de dos alumnos (usuarios) de la asignatura. Cada grupo dispondrá de sus respectivos recursos de VMs y almacenamiento. Se pueden aprovechar los nombres de usuarios y contraseñas otorgados por la Universidad.

<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/> <input type="button" value="Password"/>					
User name ↑	Realm ↑	Enabled	Expire	Name	Comment
amarin	pve	Yes	never		
arando	pve	Yes	never		
arcanmol	pve	Yes	never		
asolbes	pve	Yes	never		
root	pam	Yes	never		

*Gestión de usuarios de la asignatura*

<span>Create</span> <span>Edit</span> <span>Remove</span>	
Name ↑	Comment
grupo1	Grupo 1 de alumnos
grupo2	Grupo 2 de alumnos
profesores	Profesores de la asignatura

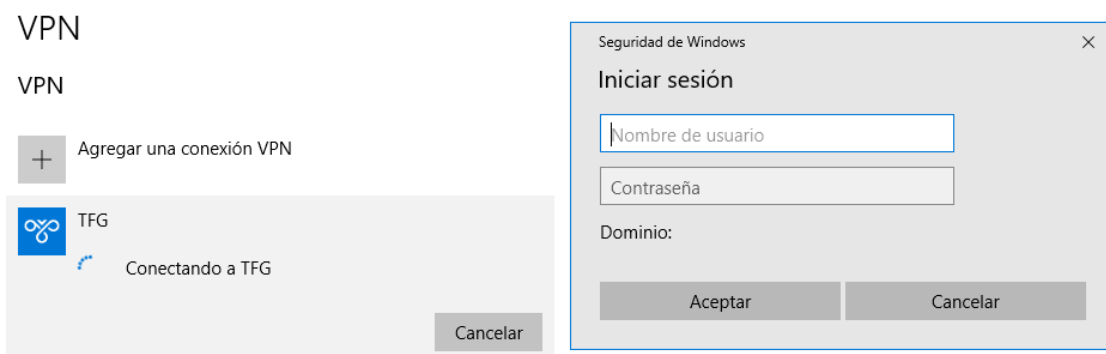
#### *Gestión de los grupos de la asignatura*

Es posible asignar usuarios a más de un profesor en el caso de que varios impartan la asignatura. Éstos quedarían en grupo con más privilegios para que tengan acceso a las prácticas realizadas por los alumnos y a acciones de administración sobre el clúster.

#### Gestión del acceso por parte de los alumnos.

Los alumnos podrán acceder a sus recursos de dos maneras:

- A través de la propia VLAN de gestión del laboratorio. Solo haría falta autenticarse una vez y sería en la interfaz web del clúster.
- La otra manera sería desde Internet a través de una VPN. Sería un poco engorroso para el profesor porque tendría que dar de alta en el router que proporciona la VPN a todos los alumnos que soliciten el acceso. También tendrían que autenticarse una segunda vez para acceder a la interfaz web.



#### *Acceso desde Internet en una máquina cualquiera*

Proxmox VE Login

User name:

Password:

Realm:

Language:

Save User name:

*Autenticación del alumno al entorno de virtualización*

PROXMOX Virtual Environment 5.2-6 Search

Server View

Datacenter

Search

Storage

Users

Type ↑	Description	Disk usage...	Memory us...	CPU usage	Uptime
node	proxmox-S40	3.7 %	3.9 %	0.3% of 16...	01:25:33
node	proxmox-S50	3.7 %	3.9 %	0.2% of 16...	01:25:21
node	proxmox-S60	3.7 %	3.9 %	0.3% of 16...	01:25:10
qemu	20000 (server01)				-
qemu	20002 (server01)				-
storage	Backup-Docencia2 (proxmox...	39.9 %			-
storage	Docencia2 (proxmox-S40)	10.5 %			-
storage	ISO_VM (proxmox-S40)	3.8 %			-
storage	Backup-Docencia2 (proxmox...	39.9 %			-
storage	Docencia2 (proxmox-S50)	10.5 %			-
storage	ISO_VM (proxmox-S50)	3.8 %			-
storage	Backup-Docencia2 (proxmox...	39.9 %			-
storage	Docencia2 (proxmox-S60)	10.5 %			-
storage	ISO_VM (proxmox-S60)	3.8 %			-

*Aspecto general de la vista de alumno*

## Gestión de almacenamiento.

En este apartado, el profesor tendría dos opciones igualmente válidas:

- Reservar la LUN más grande que pueda ofrecer su cabina iSCSI y, mediante aprovisionamiento LVM crear volúmenes lógicos para cada grupo de alumnos. En nuestro caso hay dos grupos de alumnos así que, los discos virtuales que pueda generar y gestionar el grupo 1 no los verá el grupo 2 y, a la inversa. Ésta opción es la más sencilla de configurar, pero la más problemática de mantener porque, si algo falla en la conexión a la LUN, se pierde todo el sistema LVM que hay por encima y los alumnos pierden todo el trabajo hecho hasta la fecha del último backup. Tiene el problema añadido de que la copia de seguridad no se puede restaurar directamente sobre la LUN con lo que se convierte en el sistema más rápido pero el más inestable.
- Reservar LUNs dedicadas para cada grupo y sobre cada una realizar aprovisionamiento mediante LVM. En cuanto a seguridad, sabemos que lo que ve un grupo no lo ve el otro y sería la opción más engorrosa de configurar en un

principio, pero la más sencilla de mantener porque si se pierde la conexión a una LUN, solo afecta al grupo que la utiliza, el resto pueden seguir funcionando.

En nuestro caso se ha elegido la segunda opción. Veamos algunas imágenes del resultado.

ID:	Docencia1-LUN	Nodes:	All (No restrictions)
Portal:	192.168.101.199	Enable:	<input checked="" type="checkbox"/>
Target:	iqn.2018-06.local.maudosan:freenas-iscsi	Use LUNs directly:	<input type="checkbox"/>

*Target iSCSI donde residen las LUNs*

Name	Format	Type	Size
Disk image (3 Items)			
CH 00 ID 0 LUN 1	raw	Disk image	190.00 GiB
CH 00 ID 0 LUN 2	raw	Disk image	190.00 GiB

*LUNs de los grupos a asignar*

Status	
Enabled	Yes
Active	Yes
Content	Disk image
Type	LVM
Usage	10.53% (20.00 GiB of 190.00 GiB)

*Capacidad que verá uno de los grupos en su volumen lógico*

## Funcionamiento diario con las máquinas virtuales.

No existe restricción en el número de VM a crear por parte de cada grupo. Dicha restricción la impone la cantidad de máquinas virtuales que es capaz de generar el clúster y el espacio de almacenamiento que ocupe dicha VM. Lo único que hay que tener en cuenta es que al crear una VM el usuario tendrá que asignarla a su grupo si no, el clúster no le dejará continuar.

**Create: Virtual Machine**

General OS Hard Disk CPU Memory Network Confirm

Node: proxmox-S40 Resource Pool:

VM ID: 100

Name:

*Asignación de una VM al grupo que pertenece el alumno*

**Add: Hard Disk**

Bus/Device: SATA Cache: Default (No cache)

Storage:

Disk size (GiB): 32

Format: QEMU image format (q)

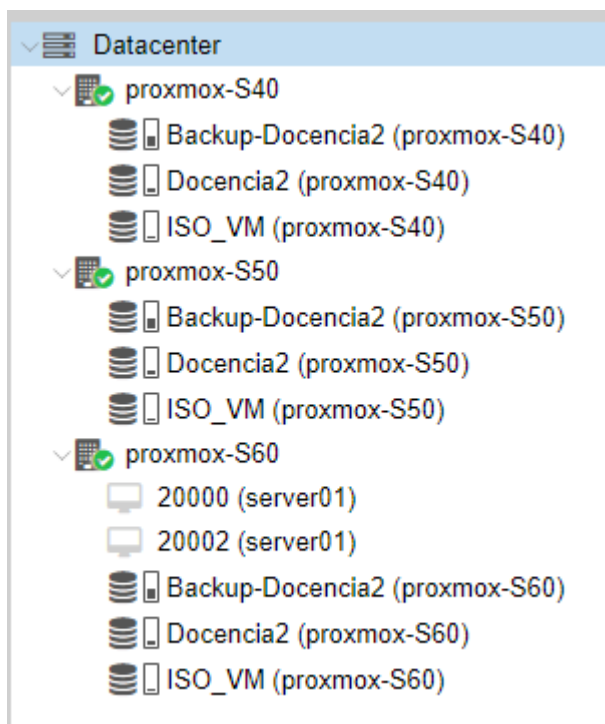
Help Advanced  Add

*El alumno puede gestionar sus recursos según le pida la práctica*

## Gestión de permisos de los grupos de alumnos.

Proxmox permite administrar permisos como cualquier otro sistema operativo que se precie. Los permisos sobre los recursos se pueden asignar a usuarios o a grupos. De esa manera los alumnos obtienen unos permisos sobre los recursos con los que trabajan.

Ahora bien, hay otro concepto que ayuda todavía más a la administración de los permisos. Se llama pool de recursos y permite agrupar recursos virtuales (almacenamiento y VMs) para asignarles al mismo tiempo grupos de usuarios y permisos. De esta manera los pools de recursos ayudan a distribuir de manera mucho más eficiente entre los grupos de usuarios permisos que les permitan acceder a unos recursos mientras que a otros no.



En la imagen vemos los recursos de VM y almacenamiento asignados a uno de los grupos de alumnos. Además, se aprecia que los alumnos del grupo no pueden acceder a los recursos del otro grupo

## Asignación de recursos a la HA.

El clúster de Proxmox tiene una manera muy simple de asignar recursos virtuales a la HA. Puede crear unos grupos llamados “grupos de HA” a los que se puede asignar dichos recursos. Por otra parte, si recordamos el concepto de pool y su relación entre los grupos, usuarios, permisos y recursos virtuales, podemos asociar de manera simbólica por el nombre dichos pools con los grupos de HA. De esta manera obtenemos todo un conjunto de elementos relacionados que nos permite administrar de manera cómoda qué recursos de qué alumnos están incluidos en la HA del clúster.



He aquí una imagen que aclara las relaciones entre todos elementos explicados hasta ahora.



Sabiendo todo esto, lo único que queda por explicar de este punto es que un clúster Proxmox tiene activada la HA por defecto así que, es responsabilidad del profesor asignar las VMs (recursos) que vayan creando los alumnos a los grupos de HA. Para ello, solo tiene que crear los grupos de HA necesarios y a continuación, asociar los recursos del grupo de alumnos con el grupo de HA correspondiente. Así cada alumno sabrá si su VM está dentro del sistema de Ha del clúster.

<input type="button" value="Create"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>	
Name ↑	Comment
grupo1	Grupo 1 de alumnos
grupo2	Grupo 2 de alumnos
profesores	Profesores de la asignatura

*Gestión de los grupos de HA por parte del profesor*

Como se comenta en el pie de foto. Aquí se definen los grupos en los que se incluirán los nodos del clúster que tienen permisos para ejecutar los recursos de esos grupos. A continuación, se muestra la ventana de asignación de nodos.

Resources					
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>					
ID	State	Node	Max. Restart	Max. Reloc...	Group
vm:10000	stopped	proxmox-S40	1	2	grupo1_alumnos
vm:10001	stopped	proxmox-S40	1	2	grupo1_alumnos
vm:20000	stopped	proxmox-S40	1	2	grupo2_alumnos
vm:20002	stopped	proxmox-S40	1	2	grupo2_alumnos

*Asignación de recursos por parte del profesor a grupos de HA*

Por su parte, el profesor tendrá que estar pendiente (se le puede avisar a través del correo de la Universidad) para ver si hay algún recurso que asignar a algún grupo de HA.

Por último, el clúster reparte sus recursos de igual manera a todos los grupos de usuarios suponiendo que éstos tengan la misma configuración en su grupo de HA. Además, si un grupo está solo en el clúster en un momento determinado, obtendrá todo el rendimiento que el clúster pueda proporcionarle pero, en el momento que entre un usuario de otro grupo, el rendimiento se dividirá entre los grupos de alumnos.

## Puntos opcionales del caso.

### Escalabilidad del caso.

Es muy deseable que una infraestructura IT donde se utiliza la virtualización permita la ampliación de recursos físicos para, en consecuencia, poder aumentar los virtuales. Para este caso esto es posible ya que cada sistema montado en el proyecto permite un tipo de escalabilidad.

Veamos algunos ejemplos:

- Sistema Proxmox + Ceph.

En cuanto a almacenamiento, este sistema puede ser esalable verticalmente u horizontalmente. Esto significa que si añadimos más discos duros o memoria RAM a los nodos existentes del clúster se estará realizando un escalado vertical, en cambio, añadir más nodos (servidores) al clúster existente hará que se escale horizontalmente.

- Sistema Proxmox + iSCSI.

En este sistema también existen los dos tipos de escalabilidad. Si añadimos más memoria RAM a los nodos existentes, será un escalado vertical. Por otro lado, si se adquieren nuevos servidores o una nueva cabina de discos se estará escalando horizontalmente.

Hay que añadir que solo se ha hablado de mejorar la memoria RAM o el almacenamiento, pero otros recursos igualmente importantes pueden permitir un escalado igual de importante. Por ejemplo, la red puede escalar el sistema adquiriendo mejores elementos de red (escalado horizontal) y beneficiando así a ambos tipos de clúster.

### Autenticación por directorio Activo de Windows.

Proxmox permite integrar su sistema de autenticación al de un controlador de dominio de Windows. Como se ha mencionado anteriormente, si los alumnos utilizan sus credenciales de la Universidad y ésta, a su vez, gestiona a sus usuarios mediante Directorio Activo, se puede aprovechar la situación para facilitar la tarea a los profesores.

En esta imagen se puede ver como se haría la integración al dominio.

The image shows a configuration window titled "Add: Active Directory Server". It contains the following fields:

- Realm: [Empty text box]
- Domain: [company.net]
- Default:
- Server: [Empty text box]
- Fallback Server: [Empty text box]
- Port: [Default]
- SSL:
- TFA: [Empty dropdown menu]
- Comment: [Empty text box]

An "Add" button is located at the bottom right of the window.

*Utilización del clúster por parte de los alumnos y de las opciones que tienen para su funcionamiento cada día*

## Infraestructura IT en una PYME.

Montaje de un caso “real” de la infraestructura de virtualización de servicios de una PYME

### Motivación del caso.

Una empresa PYME llamada Mugiwara desea montar una infraestructura IT con los siguientes servicios:

- Un servicio de directorio (Directorio activo)
- Políticas de grupo gestionadas por el servicio anterior
- Un servidor de ficheros con sus correspondientes cuotas por usuario
- Servicio de DNS
- Respaldo de la información para casos de contingencia.

### Requisitos del caso.

Los empleados de la empresa pertenecen a varios departamentos. En cada uno de ellos podrán realizar unas determinadas acciones. Los espacios relativos a cada usuario son:

- Carpeta de la empresa (Mugiwara) donde se dejarán archivos relacionados con la empresa en general: Procedimiento, Informes, formularios, etc. En ella todos los empleados tendrán permisos de lectura y, los jefes de departamento junto con el presidente de la empresa podrán además escribir.
- Carpeta personal. Tendrá el mismo nombre que el empleado y en ella podrá hacer lo que desee.
- Estructura de carpetas del departamento. Son las siguientes:
  - Carpeta “Compartido”: Es la carpeta de colaboración de grupo. Cada usuario podrá hacer lo que desee con sus ficheros y con los de los demás. Soporta archivos y subcarpetas.
  - Carpeta “Departamento”: Es la carpeta en la que el jefe de departamento deja archivos importantes para que los demás los puedan revisar. Solo el jefe puede escribir y borrar en ella. Soporta archivos y subcarpetas.
  - Carpeta “Confidencial”: Es una carpeta donde se establece una “comunicación” jefe-empleado. Los empleados pueden escribir en ella pero no pueden leer ni escribir en los ficheros de los demás. El jefe puede hacer lo que desee con cualquier archivo. A diferencia del resto de carpetas departamentales, aquí solo pueden entrar ficheros, no subcarpetas.

Un ejemplo de cómo quedaría la estructura para el departamento de Logística sería:

- X:\ Logística \Compartido
- X:\ Logística \Departamento
- X:\ Logística \Compartido

La misma información será para el resto de departamentos.

#### Información de los empleados de la empresa

- Empleados de departamento de Ventas:
  - Bea González Valls (nombre de usuario: bzalez)
  - Joaquín Pérez Antich (nombre de usuario: jperez)
  - Noelia López Prats (nombre usuario: nlopez): Jefe del departamento
- Empleados de departamento de Logística:
  - Ramón Rodríguez Jiménez (nombre de usuario: rguez)
  - María Sáez Guijarro (nombre de usuario: msaez):
  - Ana Rando Ramirez (nombre de usuario: arando): Jefe del departamento
- Empleados de departamento de IT:
  - Jorge Ruiz Prado (nombre de usuario: jruiz)
  - Juan Santos SantaMaria (nombre de usuario: jsantos)
  - Mauro Domínguez Sanjuán (nombre de usuario: maudosan). Jefe del departamento

Las carpetas personales de los empleados y las carpetas de departamento tendrán un espacio máximo que no se podrá rebasar. Éstos límites son:

- Los empleados que no sean del departamento de IT tendrán un límite de 1 GB en su espacio personal mientras que los empleados del departamento de IT tendrán un límite de 2 GB.
- Cada departamento tendrá un límite de 20 GB independientemente del usuario que realice operaciones en alguna de sus carpetas.
- La carpeta de la empresa no tiene límite alguno.

Existen unas restricciones generales aplicadas a los empleados cuando entran al dominio.

- No pueden administrar nada importante de la máquina.

- No se permite cambios en la pantalla del escritorio
- No se permite cambiar de IP en la máquina.
- No se puede instalar software alguno salvo el que ya viene instalado para trabajar.

La única excepción a esas restricciones son los empleados del departamento de IT. Es su trabajo mantener el sistema y deben poder realizar cualquier gestión en los clientes de trabajo, bien de forma remota o local.

Hay que recalcar que las restricciones son a demanda del cliente. Esto significa que si en un momento determinado desea cambiar, añadir o eliminar alguna solo tiene que pedirlo. El sistema es lo suficientemente flexible como para cumplirlas.

Comprobación de todos los servicios desde una VM Windows en el propio servidor o desde una máquina Windows del laboratorio.

### **Descripción de los servidores implementados.**

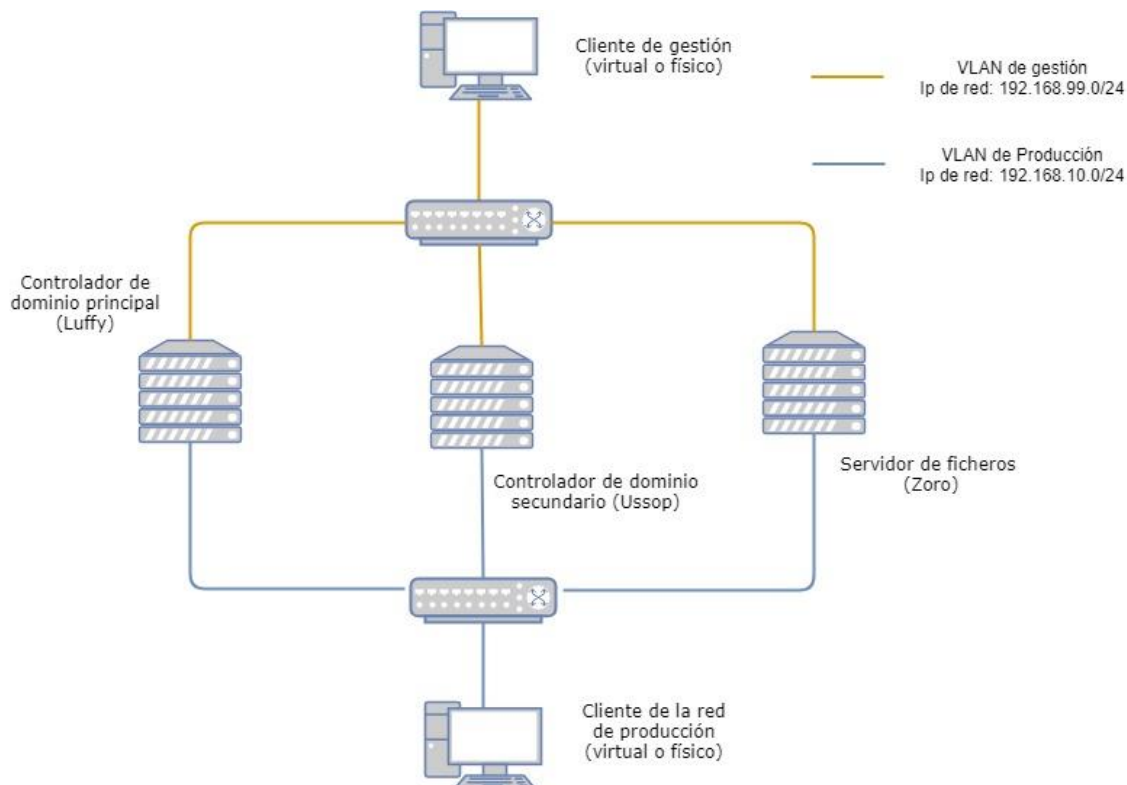
Las VMs donde se alojarán los servidores virtuales que ofrecen los servicios a la PYME son las siguientes:

- Servidor Windows Server 2016 llamado Luffy con 8 cores, 8 GB de RAM y un disco duro de 50 GB de espacio para el SO. Posee dos tarjetas de red y alojará el controlador de dominio principal.
- Servidor Windows Server 2016 llamado Zoro con 8 cores, 8 GB de RAM y dos discos duros. El primero de 50 GB de espacio para el SO y otro de 100 GB (con capacidad de poder ampliarse en un futuro) para la estructura de carpetas. Posee dos tarjetas de red y alojará el servidor de ficheros de la empresa. Añadir que el segundo disco vendrá de una LUN sobre la cual se implementará un LVM para evitar problemas de restauración de backup en caso de fallo de la VM o del hipervisor. En las “best practices” de FreeNAS se recomienda encarecidamente que no se virtualice el SO de una cabina de discos para entornos de producción. De ahí el uso del sistema LVM sobre una LUN para el servidor de ficheros.
- Servidor opcional: Un servidor Windows Server 2016 llamado Ussop con las mismas características que Luffy para realizar la función de controlador de dominio secundario. Este añadiría redundancia al sistema en caso de que el principal falle.

Se virtualizarán dos máquinas de prueba que simulan los ordenadores de trabajo de los empleados y del administrador del sistema.

## Esquema de red de los servidores virtuales.

El diagrama siguiente muestra la conexión entre servidores dentro del clúster y su conexión con las máquinas clientes que los administran o hacen uso de los servicios que proporcionan.



Hay que resaltar que el cliente de producción siempre será una máquina del mundo real. Por el contrario, el cliente de gestión admite ambas posibilidades. Preparar una máquina externa para gestionar los servidores desde fuera del clúster o crearla como máquina virtual y realizar las tareas de gestión desde dentro del clúster. En nuestro caso, no se ha preparado, pero se considera mejor opción dejarla como máquina física.

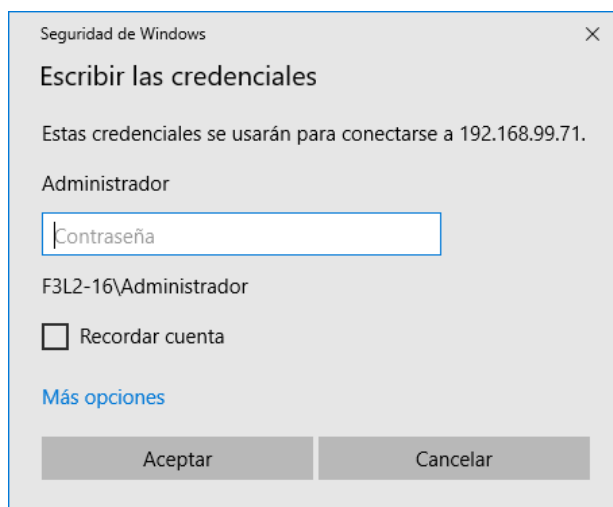
## Implementación de los servicios demandados por la PYME.

Configuración de direccionamiento IP y nombres de servidores y clientes.

- Controlador de dominio principal (Luffy):
  - VLAN de gestión 192.168.99.71/24
  - VLAN de producción: 192.168.10.71/24
- Servidor de ficheros (Zoro):
  - VLAN de gestión: 192.168.99.72/24

- VLAN de producción: 192.168.10.72/24
- Cliente Windows 7 (Nami):
- VLAN producción: 192.168.10.73/24
- Controlador de dominio secundario (Ussop):
- VLAN de gestión: 192.168.99.74/24
- VLAN de producción: 192.168.10.74/24

Los servidores se administrarán mediante Escritorio Remoto por la VLAN de gestión.



Promoción de un Windows Server 2016 a controlador de dominio.

Además de la instalación del rol de servicios de directorio activo, los datos importantes para la promoción a DC son:

- Crear un nuevo dominio en un nuevo bosque
- El dominio raíz del dominio es: mugiwara.local
- Nivel funcional: Windows Server 2012 R2 (si especificamos el más alto, no podremos añadir nuevos controladores de dominio con versiones previas).
- Contraseña del administrador del dominio.
- Hay que instalar el servicio DNS en el controlador de dominio.



Instalación de los roles "Servicios de archivo y almacenamiento" Y "Administrador de recursos del servidor de archivos" en la máquina llamada Zoro.

Al igual que la función de servicios de directorio en Luffy, este servicio se instala desde el panel de administración del servidor.

## Estructura de las Unidades organizativas (OUs), grupos y usuarios en el controlador de dominio

La distribución de los elementos de la PYME a manejar dentro del dominio es:

- OU para los otros servidores que forman parte del dominio (Servidores): Aquí estará Zoro, el servidor de ficheros y Ussop (controlador de dominio secundario) en caso de que sea necesario.
- OU para las máquinas compartidas (Ordenadores compartidos):
  - ✓ Nami. Es el cliente con el que se efectuarán las pruebas.
- OU para los permisos de la carpeta de empresa (ACL\_Grupo02):
  - ✓ ACL\_Grupo02\_R: Dentro de este grupo van los tres grupos donde están los usuarios de cada departamento.
- OU para cada departamento (se pondrá como ejemplo la de Logística) en la que dentro de cada una debería haber:
  - ✓ OUs para los usuarios (Usuarios)
  - ✓ OUs para las máquinas de los usuarios del departamento (Ordenadores)
  - ✓ OUs para los grupos de usuarios (Grupos):
    - Grupo global para todos los usuarios del departamento. Ej. Logística\_Grupo
    - Grupo global para los jefes de departamento. Ej. Logística\_Jefes
  - ✓ OU para los grupos de ACLs de cada carpeta del departamento. Ej. Logística\_ACL\_Grupo
    - ACL\_Logística\_R: Con estos permisos se consigue que los empleados puedan entrar a la estructura de carpetas de su departamento. Permiso normal de lectura.
    - ACL\_LogísticaCOMPARTIDO\_M: Carpeta de colaboración de grupo.
    - ACL\_LogísticaDEPARTAMENTO\_M: Permisos del relativos al jefe en esta carpeta
    - ACL\_LogísticaDEPARTAMENTO\_R: Permisos relativos a los empleados

- ACL\_LogísticaCONFIDENCIAL\_M: Permisos relativos al jefe en esta carpeta
- ACL\_LogísticaCONFIDENCIAL\_W: Permisos de escritura relativos a los empleados (solo pueden operar sobre archivos de su propiedad)
- ACL\_LogísticaCONFIDENCIAL\_R: Permisos de lectura relativos a los empleados (solo pueden operar sobre archivos de su propiedad)

Introducción del servidor de ficheros y los clientes de trabajo en el dominio.

La mecánica es la misma para cada máquina:

- Establecer a Luffy (DC) como servidor DNS principal.
- Decirle a la máquina el nombre del dominio en la ventana de "propiedades del sistema". Pedirá contraseña de administrador del dominio para este último paso.

Si quiere comprobar que entra al dominio se puede autenticar con un usuario del dominio. El usuario no tendrá carpeta personal todavía.

Creación de carpetas en el servidor de ficheros.

En este punto se creará la estructura de carpetas de cada departamento, la carpeta de empresa y la carpeta home. Dentro de la carpeta home no hay que crear nada. Las carpetas personales de los usuarios se crearán en los perfiles de usuario en el DC (Luffy). La letra a asignar a estas carpetas es la Z.

Captura de un perfil de usuario activando su carpeta personal.

Las carpetas "Mugiwara S.L.", "home" y las de cada departamento se han de compartir con los permisos habilitados como "control total" para que se puedan mapear a los usuarios y que estos las puedan ver en sus sesiones.

Una vez llegados a este punto, se deben configurar las cuotas de disco de las carpetas personales de los empleados según los límites especificados anteriormente.

Asignación de permisos en las carpetas del servidor de ficheros

Se utilizarán los permisos del sistema de ficheros NTFS de Windows. Además, y como "best practice", se seguirá la estrategia IGDLA del Directorio Activo para asignar de manera cómoda dichos permisos a los usuarios según los requisitos mencionados arriba.

## Configuración de políticas de grupo

Aquí se implementarán las restricciones que se han detallado anteriormente y que no se pueden realizar por medio de los permisos.

Antes de nada, recordar que los empleados tienen acceso a diferentes carpetas según su relación con la empresa y que hay que habilitar con las políticas de grupo. Dichas carpetas son:

- La carpeta de departamento: asignarla como unidad a la letra X
- La carpeta de la empresa: asignarla como unidad a la letra Y

La 1ª política de grupo será mapear las carpetas de departamento y la carpeta global de la empresa.

Captura con las carpetas asignadas

Las cosas importantes a introducir en el diálogo de asignación de unidades son:

- La ruta de la unidad.
- Seleccionar la casilla "reconectar".
- El nombre con el que queremos que se vea la unidad.
- Elegir la letra de unidad.
- Seleccionar opción "mostrar esta unidad".

Una vez mapeadas las carpetas recordemos las restricciones a habilitar en las políticas de grupo:

- No pueden administrar nada importante de la máquina.
- No se permite cambios en la pantalla del escritorio
- No se permite cambiar de IP en la máquina.
- No se puede instalar software alguno salvo el que ya viene instalado para trabajar.

Colocar captura de la activación de alguna política

## Aprovechamiento de la HA de Proxmox

Dado que los servicios de la PYME están montados sobre VMs, es obvio que estas aprovecharán esa característica del hipervisor. Esto responde frente a dos casos diferentes:

- Fallo de la VMs por la razón que sea. Se reinicia en otro de los nodos del clúster.
- Fallo de uno de los hipervisores (host físico): Este caso es más crítico y responde de igual manera que el anterior aunque con un tiempo de fallo en el servicio.

Se ha probado apagar de manera abrupta uno de los hipervisores donde estuviese ejecutándose una o varias VMs del montaje virtual y se ha visto que aparece de nuevo y funcionando en otro nodo del clúster.

En este caso hay que añadir que esta funcionalidad hace muy buena pareja con la que se explica a continuación.

## Implementación de políticas de respaldo

Como se ha explicado en otra sección, Proxmox puede programar backups según las necesidades del cliente. Como Proxmox soporta únicamente backups completos, en este caso se realizará uno semanal todos los viernes por la noche a las tres de la madrugada.

Además, por cuestiones de espacio, vamos a restringir los backups de manera que solo haya cuatro por cada VM, es decir solo se salvará el contenido de las VMs del último mes. Esto último es así a no ser que en la mitad de una semana se desee realizar un backup temporal por cualquier razón. En ese caso, solo se tendrían las tres últimas semanas ya que el backup no programado machacaría el espacio asignado al de hace un mes.

Veamos unas capturas para entender la programación de los backups y la restricción de espacio.

**Create: Backup Job** ✕

Node: <input type="text" value="-- All --"/>	Send email to: <input type="text"/>
Storage: <input type="text" value="PYME-backups"/>	Email notification: <input type="text" value="Always"/>
Day of week: <input type="text" value="Saturday"/>	Compression: <input type="text" value="LZO (fast)"/>
Start Time: <input type="text" value="03:00"/>	Mode: <input type="text" value="Snapshot"/>
Selection mode: <input type="text" value="Include selected VMs"/>	Enable: <input type="checkbox"/>

	ID ↑	Node	Status	Name	Type
<input checked="" type="checkbox"/>	60000	proxmox-S80	running	Luffy	qemu
<input type="checkbox"/>	60001	proxmox-S70	stopped	Win-Server-2016-baseline	qemu
<input checked="" type="checkbox"/>	60002	proxmox-S70	stopped	Sanji	qemu
<input type="checkbox"/>	60003	proxmox-S70	stopped	Zoro	qemu

### *Programación de backups*

Por último, comentar que esta política solo salva los datos desde el backup realizado en la semana anterior. Por poner un ejemplo, si el backup está programado para hacerse los viernes por la noche y la VM falla el miércoles siguiente, se perderán los cambios de tres días.

## Conclusiones y líneas futuras de trabajo (ampliaciones).

### *Conclusiones.*

Este proyecto ha sido muy interesante porque me ha permitido integrar en un mismo trabajo diferentes conceptos, tecnologías, hardware diverso, protocolos, software y procedimientos actuales en el mundo IT, en concreto de la virtualización y de todo lo relacionado con la misma.

El desarrollo de los casos de uso me ha permitido aplicar los conocimientos adquiridos en la Universidad al mundo real y comprobar que en el mundo empresarial el diseño, implementación y mantenimiento posterior de soluciones de virtualización requieren amplios conocimientos, experiencia y capacidad de trabajo personal y en equipo para llevarlos adelante.

Un aspecto muy importante del que me he dado cuenta es la importancia del soporte para cualquier empresa que desee una solución de virtualización. En general resulta más práctico adquirir ese soporte para quedarse uno tranquilo que intentar solucionar un problema que, sabiendo que tiene solución, puede quitar tiempo y dinero a la empresa.

Otra de las cosas que me he dado cuenta en la fase de implementación es la importancia de la automatización de tareas y la documentación simultánea para un profesional. Ya tenía una idea de su importancia al empezar este TFG pero al finalizarlo, me he dado cuenta que es, quizás, la mejor manera de ahorrar tiempo y disgustos en un entorno real.

Por la parte negativa, solo lamento no poder haber realizado a tiempo unas pruebas que hubiesen sido muy importantes para aclarar de manera cuantitativa cuál de los sistemas de almacenamiento era más viable para los casos presentados. También hubiese sido interesante poder implementar las medidas que se comentan en la sección “Líneas futuras de trabajo” pero el tiempo es limitado.

Reiterar de nuevo la satisfacción por el trabajo realizado y saber que todo lo adquirido con este TFG será mucha ayuda en mi carrera como profesional.

### *Líneas futuras de trabajo.*

#### **Backups incrementales en Proxmox.**

Proxmox realiza únicamente backups completos de las VMs que aloja. Esto puede ser un problema cuando las VMs tienen un tamaño considerable y llevan bastante tiempo funcionando. Resumiendo todo sistema tiende a empeorar con el tiempo.

Mediante la generosidad de un usuario en el foro de Proxmox, se ha encontrado la posibilidad de implementar backups diferenciales para este tipo de VM. La política sería la siguiente:

Cambiar la restricción de espacio para que guarde los backups para una semana. Habría que averiguar si el número permitido de backups por VM coincide con la secuencia de Backup completo más el resto de backups diferenciales.

- VMs más ligeras: Backups completos semanales
- VMs más pesadas: Backups completos semanales + backups diferenciales diarios

A falta de instalar más espacio en el servidor de backup hasta la capacidad de 1TB

Esto permitiría varias mejoras en el sistema:

- Rapidez a la hora de realizar backups de VMs con más recursos.
- Pérdida de menor información ante una contingencia. Solo se perdería lo del día actual.

A falta de más cálculos relativos al espacio que ocuparía la nueva política de backups, sería una mejora muy importante para el entorno de virtualización.

#### **Monitorización de algunos de los sistemas implementados.**

Todo sistema necesita de alguna herramienta de monitorización para comprobar su buen funcionamiento y proponer mejoras en su conjunto. He aquí algunas herramientas que se podrían utilizar para este propósito.

#### **Monitorización del clúster Proxmox.**

Existen varias herramientas de monitorización que se pueden probar para comprobar en todo momento el uso de los recursos reales y virtuales por parte de Proxmox. Algunas son:

- Nagios: es un veterano y está desde las primeras versiones de Proxmox. <https://exchange.nagios.org/>
- Graphite. Pertenece a nueva generación de monitores escritos con lenguajes de programación más actuales. <https://graphiteapp.org/>
- InfluxDb para recolección de datos y Grafana para su presentación. <https://www.influxdata.com/> <https://grafana.com/>

### Monitorización del clúster de Ceph.

Debido al rendimiento mostrado por Ceph, sería una buena idea implementar Calamari para monitorizar exclusivamente su rendimiento mediante esta herramienta. Está recomendada por los desarrolladores de Ceph y entraría dentro de las “best practices” de todo administrador de sistemas.

<https://calamari.io/>

Mejora en general de los dos casos de uso en cuanto a servicios ofrecidos y facilidad de mantenimiento de los mismos.

## Bibliografía

- Página web de Ceph: <https://ceph.com/>
- Página web de Proxmox incluyendo su wiki y su foro:
  - ✓ [https://pve.proxmox.com/wiki/Main\\_Page](https://pve.proxmox.com/wiki/Main_Page)
  - ✓ <https://www.proxmox.com/en/>
  - ✓ <https://forum.proxmox.com>
- Documentación de Debian 9: <https://www.debian.org/doc/>
- Página web de XenServer: <https://xenserver.org/>
- Página web de Citrix: <https://www.citrix.com/>
- Página web de VMWare: [www.vmware.com](http://www.vmware.com)
- Página web de Windows Server 2016:  
<https://www.microsoft.com/es-es/cloud-platform/windows-server-pricing>
- Página web de FreeNAS y su foro:
  - ✓ <http://www.freenas.org/>
  - ✓ <https://forums.freenas.org/index.php>
- <http://911-ubuntu.weebly.com/proxmox-iscsi/proxmox-iscsi-y-nfs>
- <http://911-ubuntu.weebly.com/proxmox-ceph>
- <https://icimov.github.io/blog/virtualization/Adding-iSCSI-shared-volume-to-Proxmox-to-support-Live-Migration/>
- Mastering Proxmox. Second Edition. Wasim Ahmed. 2016 PACKT Publishing.
- Proxmox High Availability. Simon M. C. Cheng. 2014 PACKT Publishing