



UNIVERSIDAD DE MÁLAGA



Análisis, diseño e implantación de un sistema de virtualización con VMWARE en un entorno docente educativo de grado medio

Analysis, design and implementation of a virtualisation system with VMWARE in a high school educational environment

Realizado por
Ángel Diego Pacheco Reyes

Tutorizado por
Sergio Gálvez Rojas
Enrique Soler Castillo

Departamento
Lenguajes y Ciencias de la Computación

MÁLAGA, enero de 2020

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA
GRADO EN INGENIERÍA DE COMPUTADORES

**Análisis, diseño e implantación de un sistema de virtualización
con VMWARE en un entorno docente educativo de grado medio**

**Analysis, design and implementation of a virtualisation system
with VMWARE in a high school educational environment**

Realizado por
Ángel Diego Pacheco Reyes

Tutorizado por
Sergio Gálvez Rojas
Enrique Soler Castillo

Departamento
Lenguajes y Ciencias de la Computación

UNIVERSIDAD DE MÁLAGA
MÁLAGA, enero de 2020

Fecha defensa:

Fdo.: El Secretario del Tribunal

Resumen: El propósito de este trabajo es mostrar los extraordinarios beneficios que conlleva la virtualización de sistemas, entre los que cabe destacar la drástica reducción en el número de servidores, la facilitación de las tareas de administración o la creación de entornos de test que permiten poner en marcha nuevos servicios y aplicaciones sin impactar en la producción. Además, aporta grandes ventajas como son un mejor aprovechamiento del hardware, ahorro de energía, de espacio y de refrigeración entre otras.

El análisis se realizará en un entorno que cuenta con los recursos necesarios para dar servicio a un escenario compuesto por 12 laboratorios TIC y 342 equipos informáticos, así como los múltiples servicios necesarios para el normal desarrollo de la docencia en dicho entorno. Por este motivo, los servicios que se van a virtualizar son: DHCP, proxy, samba y openGnSys. Para ello, se procederá al diseño e implementación del sistema de dicho escenario docente en un entorno virtualizado con VMware.

La elección de los servicios mencionados, de entre los múltiples implementados en un entorno mucho mayor (véanse los recursos hardware utilizados), viene determinada por la intención de hacer de este TFG una guía que haga el modelo virtualizado, trasladable y dimensionable a un entorno educativo de grado medio. La gran cantidad de laboratorios y equipos informáticos elegida cubre de sobra la práctica totalidad de escenarios que pueden encontrarse en cualquier instituto, ya sea de la ESO, Bachiller o de Formación Profesional de Grado Medio o de Grado Superior.

Palabras claves: Virtualización, Aula TIC, VMware, DHCP, proxy, samba, OpenGnsys.

Abstract: The purpose of this work is to show the extraordinary benefits of system virtualization, among which we may highlight the drastic reduction in the number of servers, to make easier the management tasks or the creation of test environments that allow the implementation of new services and applications with no drawback in production services. In addition, it provides many advantages, some of which could be: better use of hardware, energy savings, space and cooling, among others.

The analysis will be executed in an environment that has the required resources to provide service to a scenario composed of 12 ICT laboratories and 342 computers, as well as the multiple services needed for the normal teaching environment. For this reason, the virtualized services will be DHCP, proxy, samba and openGnSys. For this purpose, the system design and implementation of this teaching scenario will be virtualized with VMware environment.

The aforementioned services have been chosen among multiple ones implemented in a much larger environment (see the hardware resources used). The rationale of this is the intention of making this TFG a guide that makes the model virtualized, transferable and scalable to a medium grade educational environment. The large number of laboratories and computer equipment chosen covers the most of the scenarios that can be found in any school, whether it is a high school, or Vocational Training school.

Keywords: Virtualization, ICT classroom, VMware, DHCP, proxy, samba, OpenGnsys.

ÍNDICE

1. INTRODUCCIÓN	3
1.1. Antecedentes	3
1.2. Objetivos	4
1.3. Herramientas y Tecnologías	5
1.3.1. Software de VMware	5
1.3.2. Hardware de HP Enterprise	6
1.3.3. Protocolo DHCP	7
1.3.4. Servicio Proxy	7
1.3.5. Protocolo CIFS. Implementación Samba	8
1.3.6. Aplicación OpenGnsys	8
1.4. Conceptos preliminares	9
1.4.1. Conceptos de Redes & Redes Virtuales	9
1.4.2. Conceptos de almacenamiento	12
1.5. Características del sistema	14
1.5.1. Servidores	14
1.5.2. Conmutadores	14
1.5.3. Almacenamiento	15
1.5.4. PCs	15
1.6. Metodología	15
1.7. Estructura de la memoria	16
2. ANÁLISIS	17
2.1. Análisis del modelo de aula TIC	17
2.1.1. Equipos clientes	17
2.1.2. Interconexión de red	18
2.1.3. Servicios y aplicaciones necesarios	19
2.2. Dimensionamiento	20
3. DISEÑO	23
3.1. Espacio de direccionamiento de red	23
3.1.1. Direccionamiento de las Aulas TIC	23
3.1.2. Direccionamiento de la infraestructura de virtualización	24
3.2. Esquema conceptual de la infraestructura de virtualización	25
3.3. Esquema de interconexión de dispositivos	26
3.4. Diseño del modelo de aula TIC	27
3.5. Servicios básicos para la docencia	29
4. IMPLEMENTACIÓN	31
4.1. Instalación y Configuración de la Infraestructura de Virtualización	31
4.1.1. Flujo de trabajo	31
4.1.2. Interconexión del sistema	32
4.1.3. Implementación del almacenamiento	37
4.1.4. Implementación de VMware vSphere (ESXi)	42

Análisis, diseño e implantación de un sistema de virtualización con VMWARE en un entorno docente educativo de grado medio

4.1.5. Implementación de VMware vCenter Server	51
4.1.6. Administración de los ESXi con vCenter Server	55
4.2. Instalación y configuración de servicios y aplicaciones	57
4.2.1. Servidor de DHCP	57
4.2.2. Servidor de OpenGnsys	61
4.2.3. Servidor Proxy	68
4.2.4. Servidor Samba	73
5. CONCLUSIONES	77
5.1. Logros alcanzados	79
5.2. Futuras líneas de trabajo	79
5.2.1. Respecto al sistema de virtualización	79
5.2.2. Respecto a los servicios y aplicaciones	80
6. BIBLIOGRAFÍA	81

1. INTRODUCCIÓN

1.1. Antecedentes

Los laboratorios docentes compuestos por **aulas TIC** constituyen un escenario con características especiales.

TIC son las siglas de **Tecnologías de la Información y la Comunicación**. Un Aula TIC es por tanto, un aula de docencia en un contexto tecnológico, donde los equipos o servicios se encuentran habitualmente conectados a Internet.

Un aula TIC requiere la implementación de ciertos servicios informáticos para el normal desarrollo de la docencia y para la gestión, administración y mantenimiento de la misma. Algunos de estos servicios son: la asignación dinámica de direcciones IP, la autenticación de los alumnos, almacenamiento compartido, clonación de equipos informáticos, páginas web departamentales, plataformas educativas, horarios, wikis, y un largo etcétera.

El modelo tradicional en dichos escenarios docentes (VER FIGURA 1) consiste en la implementación de los servicios informáticos en servidores físicos donde cada uno de ellos tiene su propio hardware y por tanto sus propios recursos: procesador, memoria, almacenamiento, red, etc.

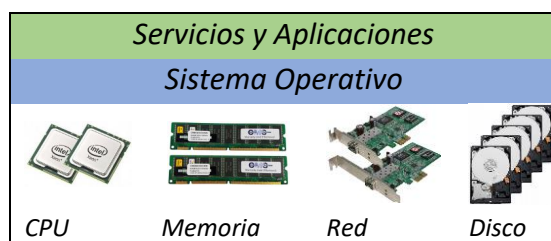


Figura 1. Modelo tradicional.

Esto produce que muchos servidores se encuentren infrutilizados mientras otros operan al límite de sus capacidades. Tareas de administración de sistemas como la migración de servicios, la implementación de nuevas aplicaciones, actualizaciones, copias de seguridad o la recuperación ante desastres entrañan, en ocasiones, gran complejidad y un alto coste en horas de trabajo.

La virtualización de estos servidores (VER FIGURA 2) posibilita la concentración del hardware permitiendo que los recursos se agrupen y pasen a disposición de un **hipervisor** como VMware vSphere, Microsoft Hyper-V, oVirt, OpenNebula, OpenStack KVM o Citrix Xen.

El hipervisor tiene la capacidad de dosificar dicho hardware en recursos virtuales para ejecutar diferentes sistemas operativos. [1][2][3]

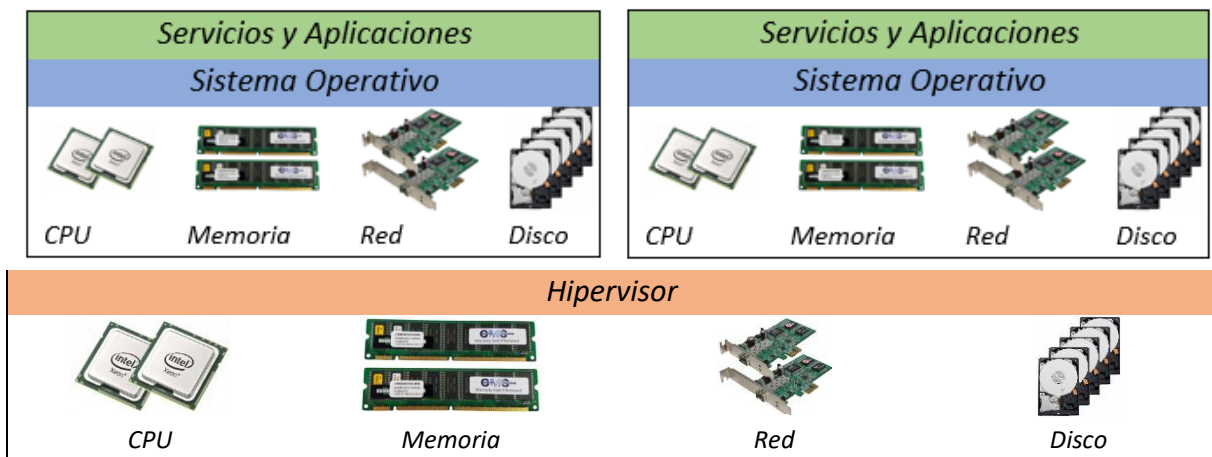


Figura 2. Virtualización con hipervisor.

Además, existen aplicaciones que permiten la administración centralizada de hipervisores (VER

FIGURA 3) lo que proporciona una visión de conjunto del sistema, facilita la tarea de administración, mayor control de las operaciones y optimiza la distribución de recursos entre otras ventajas. [4]

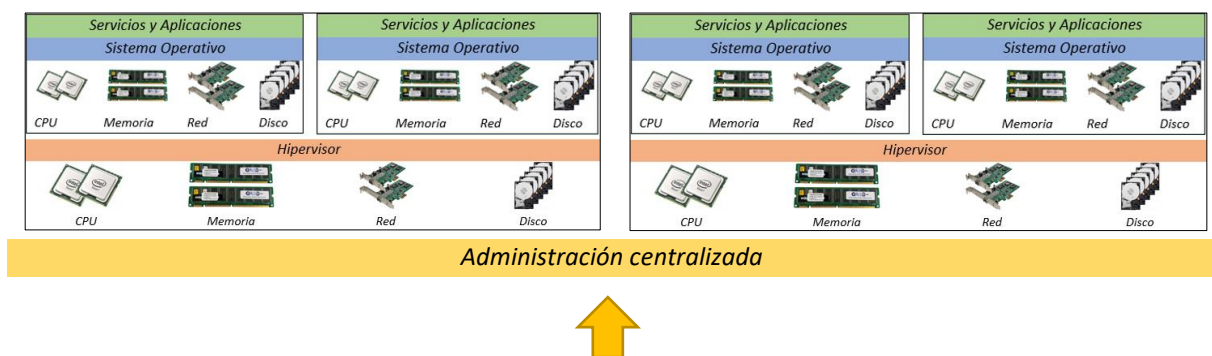


Figura 3. Administración centralizada de hipervisores.

Esto hace que las máquinas virtuales se vuelvan enormemente portátiles; un administrador de sistemas puede pausar una máquina virtual y moverla o copiarla a otro servidor, para allí reanudar la ejecución en el mismo punto de suspensión. De hecho, existen soluciones para migración de máquinas virtuales en caliente (sin pausar), de forma transparente para los usuarios de la máquina virtual en el momento en que se migra.

En definitiva, la **concentración de todo el sistema en una infraestructura virtualizada** aporta beneficios que van desde la eficiencia en la administración hasta la reducción de costes o una menor huella ecológica.

1.2. Objetivos

El propósito de este trabajo fin de grado es mostrar los extraordinarios beneficios que conlleva la virtualización de sistemas, entre los que cabe destacar la drástica reducción en el número de servidores, la facilitación de las tareas de administración o la creación de entornos de test que permitan poner en marcha nuevos servicios y aplicaciones sin impactar en la producción.

Además, aporta grandes ventajas como son: mejor aprovechamiento del hardware, ahorro de energía, de espacio y de refrigeración entre otras.

El análisis se realizará en un entorno que cuenta con los recursos necesarios para dar servicio a un escenario compuesto por **12 laboratorios TIC y 342 equipos informáticos**, así como los múltiples servicios necesarios para el normal desarrollo de la docencia en dicho entorno.

La elección de los servicios, de entre los múltiples implementados en un entorno mucho mayor (véanse los recursos hardware utilizados), viene determinada por el objetivo de hacer de este TFG¹ una guía que haga el modelo virtualizado, trasladable y dimensionable a un entorno educativo de grado medio.

La elección de los servicios tiene la intención de alcanzar el objetivo de hacer trasladable el modelo, como se expone en el párrafo anterior, por lo que constituyen un núcleo mínimo para el funcionamiento del aula TIC, el desarrollo de la docencia y las tareas de administración. Los servicios que se van a virtualizar son: DHCP, proxy, samba y openGnsys [10]. Para ello, se procederá al diseño e implementación del sistema de dicho escenario docente en un entorno virtualizado con VMware.

La gran cantidad de laboratorios y equipos informáticos elegida cubre de sobra la práctica totalidad de escenarios que pueden encontrarse en cualquier instituto, ya sea de la ESO, Bachiller o de Formación Profesional de Grado Medio o de Grado Superior.

1.3. Herramientas y Tecnologías

A continuación, las principales herramientas y/o tecnologías utilizadas en este TFG.

1.3.1. Software de VMware

VMware es una compañía de software cuyos principales productos son la virtualización y la computación en la nube. VMware es líder global tanto por su amplio abanico de productos de virtualización como por el alcance y difusión de los mismos.

Existen versiones del software de escritorio de VMware para Microsoft Windows, Linux y macOS mientras que el **hipervisor de VMware** corre sobre un sistema operativo dedicado conocido como **ESXi** (actualmente **vSphere**).

Los principales productos de **virtualización de VMware** (es decir, sin incluir software de gestión en la nube, de almacenamiento, de disponibilidad, de redes, de seguridad y otros) son los siguientes: [5]

- **VMware Workstation** (software de escritorio). Fue el primer producto lanzado por VMware. Permite ejecutar diferentes instancias de sistemas operativos con arquitectura x86 en un solo equipo físico.

¹ TFG son las siglas de Trabajo Fin de Grado.

- **VMware Fusión** (software de escritorio). Similar al producto anterior, pero para equipos Macintosh con procesador Intel.
- **VMware Workstation Player** (software de escritorio). Es una versión gratuita similar a los anteriores, pero con funcionalidad reducida.
- **VMware vCenter Converter** (software de escritorio). Herramienta gratuita de VMware que permite convertir máquinas físicas basadas en Windows o Linux en máquinas virtuales compatibles con VMware ESXi o Workstation y subirlas al sistema virtualizado con VMware, incluso sin parada. También permite convertir máquinas virtuales de terceros como Hyper-V o KVM.
- **VMware vSphere** (software servidor). Se denomina **Host** a un equipo con el hipervisor de VMware (más conocido como **ESXi**). VER FIGURA 4.

El *Host* se ejecuta directamente sobre el hardware del servidor, es decir que no se instala sobre un sistema operativo si no que incorpora su propio Kernel para su ejecución. ESXi es la base sobre la que se construye el resto de la infraestructura.

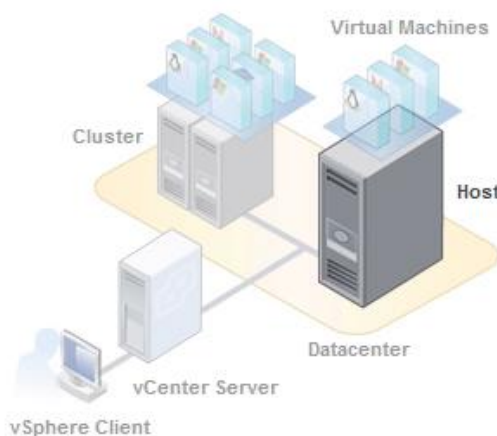


Figura 4. Host de VMware

- **VMware vCenter Server** (software servidor). Es el software de administración centralizada de VMware (VER FIGURA 5) desde una única consola.

Proporciona las herramientas necesarias para monitorizar y gestionar diferentes *Hosts* (hipervisores ESXi) y las máquinas virtuales diseminadas en ellos.

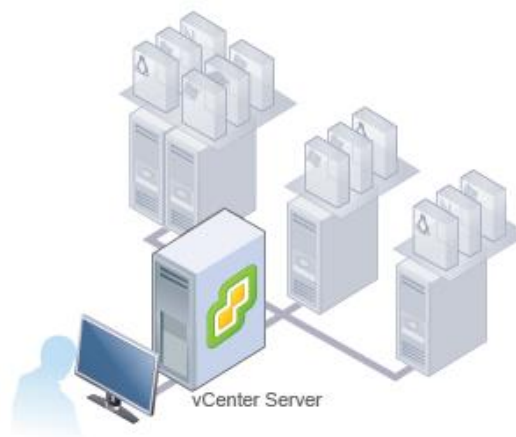


Figura 5. vCenter Server

1.3.2. Hardware de HP Enterprise

Hewlett Packard Enterprise Company (**HPE**) es una empresa de servidores, sistemas de almacenamiento y software; no confundir con HP Inc, dedicada a la venta ordenadores, impresoras y otros dispositivos.

HPE [6] tiene múltiples líneas de productos entre los que destacamos los siguientes, por estar directamente relacionados con este TFG:

- **Intelligent Edge** con sistemas de conectividad y elementos de red como ProCurve y 3com.
- **HPE Server** (*en español: Servidores HPE*) con diversas familias de servidores entre la que destacamos Proliant DL; servidores versátiles, optimizados para rack de fácil expansión y capacidad de gestión con diferentes cargas de trabajo.
- **HPE Storage** (*en español: Almacenamiento HPE*) con diferentes plataformas y dispositivos de almacenamiento que ofrecen gestión e integración, pero sobre todo la disponibilidad y el rendimiento que la virtualización requiere.

1.3.3. Protocolo DHCP

DHCP (*Dynamic Host Configuration Protocol*) o protocolo de configuración dinámica de *hosts* es un servicio que permite asignar información de red a un conjunto de equipos conectados a una red de área local eliminando la necesidad de configuración manual de cada uno de ellos.

El servidor de DHCP **proporciona configuración de red** en un rango prefijado, evitando conflictos de direcciones IP repetidas y utilizando para ello un modelo cliente-servidor de administración centralizada.

Los equipos, clientes del servicio DHCP, solicitan al servidor de DHCP la configuración de sus interfaces de red, lo que permite asignar dinámicamente direcciones IP (asociadas a las direcciones MAC de los equipos clientes).

También pueden ser asignados otros parámetros de configuración de red como máscaras de red, dirección de broadcast, dirección del router, direcciones de servidores de DNS y un largo etcétera entre los que destacamos el parámetro **next-server** que permitirá a los equipos clientes recibir instrucciones en el arranque una vez obtenida su dirección IP. [7]

1.3.4. Servicio Proxy

Proxy es un programa que se encarga de realizar peticiones en nombre de un cliente utilizando un protocolo determinado. En concreto, en el ámbito del protocolo **HTTP**², el servidor proxy es un intermediario conocido como proxy web. VER FIGURA 6.

Un servidor proxy web en un escenario compuesto por múltiples Aulas TIC tiene múltiples ventajas entre las que destacamos las siguientes:

- **Protección de los clientes** ante ataques del exterior de la red, puesto que los equipos sólo son accesibles en la red local.

² **HTTP** (*Hypertext Transfer Protocol*) son las siglas en inglés del protocolo de transferencia de hipertexto que permite la transferencia de información en la **WWW** (*World Wide Web*).

- **Caché**, al almacenar en su disco copia de los datos que retransmite a los clientes, con el consiguiente ahorro de comunicaciones antes peticiones repetitivas de mismas direcciones, situación típica en escenarios docentes.
- **Filtrado**, al ofrecer la posibilidad analizar peticiones a nivel de cadenas de caracteres o servir las **peticiones sólo de determinados clientes**. Esta última opción muy a tener en cuenta en Aulas TIC a las que se quiera cortar los accesos a interne en determinados momentos, por ejemplo, durante la celebración de exámenes.

Squid [8] es el servidor proxy web más popular y extendido por ser software libre y formar parte de la mayoría de distribuciones Linux, además de por sus innumerables opciones de configuración que incluyen listas de control de acceso y definición de reglas, entre otras.

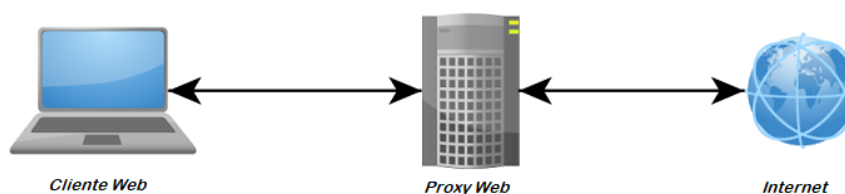


Figura 6. Esquema de conexión mediante Proxy web

1.3.5. Protocolo CIFS. Implementación Samba

Samba [9] es un servicio software libre presente en distribuciones GNU/Linux, Mac OS o Unix que incorpora el protocolo de compartición de recursos de Microsoft Windows (**SMB / CIFS**)³ para la compartición de archivos o impresoras.

Samba permite la integración de Windows con sistemas Linux/Unix en una misma red, de tal forma que se puedan intercambiar archivos o se puedan utilizar diferentes impresoras independientemente del sistema operativo de los ordenadores. También provee de administración centralizada de dichos recursos estableciendo privilegios a nivel de autenticación de usuarios o de permisos sobre los recursos compartidos.

La integración de Samba en redes Microsoft Windows es tal, que puede funcionar como controlador principal de dominio (*en inglés Primary Domain Controller o simplemente PDC*), como miembro del dominio e incluso como un dominio Active Directory⁴.

1.3.6. Aplicación OpenGnsys

OpenGnsys [10] (pronunciado “open-génesis”) es un proyecto de software libre para la gestión y el despliegue de sistemas operativos en aulas TIC.

³ En 1998, **SMB** (*Server Message Block*) fue renombrado por Microsoft como **CIFS** (*Common Internet File System*).

⁴ **Active Directory** (*en español: Directorio activo*) es la implementación de Microsoft de un servicio de directorio.

El proyecto es el resultado del trabajo conjunto de diferentes universidades públicas españolas (entre las que se encuentra la **Universidad de Málaga**) para el desarrollo de una aplicación intuitiva que provea de herramientas para la gestión y clonación de equipos.

La clonación de equipos consiste en generar una imagen del sistema de ficheros de un equipo modelo con todo el software completamente instalado y configurado, y estamparla en otros equipos de la organización.

La consola de administración de OpenGnsys está basada en una interfaz web fácil e intuitiva que permite de forma centralizada la gestión de aulas TIC con diferentes sistemas operativos, así como la clonación de los equipos uno a uno, o todos a la vez, con diferentes protocolos de comunicaciones, como **Unicast**, **Multicast** o **P2P**. VER 1.4.1. CONCEPTOS DE REDES & REDES VIRTUALES.

También es posible la clonación offline (sin comunicación con un servidor OpenGnsys) accediendo directamente a una caché de datos local al cliente o a un dispositivo externo de almacenamiento.

Una de las grandes ventajas de OpenGnsys sobre otros productos similares es la posibilidad de configuración de los equipos de destino una vez estampada la imagen como, por ejemplo: el nombre de equipo, la detección del inventario hardware, el software instalado e incluso, la copia o borrado de ficheros y directorios o la modificación del registro de Windows.

La información, documentación, código y software para la descarga está disponible en la web del proyecto en <https://opengnsys.es/web>

1.4. Conceptos preliminares

Son necesarios ciertos conocimientos para la comprensión integral del presente trabajo. A continuación, se presentan algunos conceptos esenciales:

1.4.1. Conceptos de Redes & Redes Virtuales

Una red virtual está compuesta por máquinas virtuales que se ejecutan en máquinas físicas y que están interconectadas de manera lógica para poder enviar y recibir datos. Diferentes máquinas virtuales pueden conectarse a diferentes redes virtuales. [12][13]

Un equipo físico se conecta a la red mediante una o varias **NIC**⁵ cada una con una dirección **MAC**⁶ distintiva. Del mismo modo una máquina virtual lo hace a través de una o varias **vNIC** (*en inglés virtual NIC*).

Un **conmutador** (también conocido por su nombre en inglés; **switch**) es un dispositivo que permite la conexión de periféricos por lo que constituye el núcleo de una red ya que determina

⁵ **NIC** son las siglas en inglés de Network Interface Card e identifican un adaptador de red.

⁶ La dirección **MAC** - **ethernet** (*Media Access Control*) es un identificador que corresponde de forma única a un adaptador de red.

qué equipos (*hosts*) están conectados a sus puertos y utiliza esa información para enviar tráfico a las máquinas correctas.

De la misma forma, un conmutador de red virtualizado (**vSwitch**) detecta qué máquinas virtuales están conectadas de manera lógica a cada uno de sus puertos virtuales y utiliza esa información para enviar y recibir tráfico de las máquinas virtuales correctas. (VER Figura 7). [13]

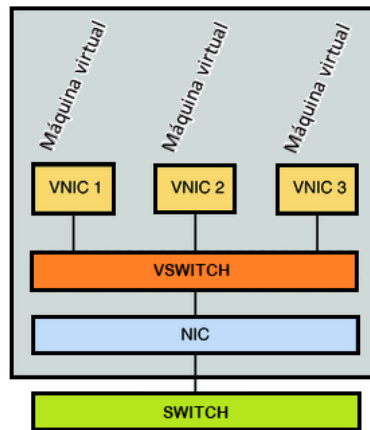


Figura 7. Conexión de Máquinas virtuales a una red

Si **LAN** son las siglas en inglés de para definir una red de área local (*en inglés: Local Área Network*), el método para crear diferentes redes lógicas dentro de una misma red se conoce como **VLAN** (*del inglés: Virtual LAN*).

Las VLAN permiten que los grupos de puertos de una red lógica queden aislados del resto de redes como si estuvieran en segmentos físicamente diferentes lo que facilita la definición de subredes en dominios de difusión. Las directivas de etiquetado VLAN permiten identificar cada red lógica dentro de una red física o virtual.

Los modos de acceso a la red habituales para las máquinas virtuales son **BRIDGE** (*Bridge networking*) y **NAT** [14] (*Network address translation*), por lo que ambos métodos están incorporados en las aplicaciones de escritorio VMware Workstation Player y VirtualBox.

Mediante la configuración en modo **BRIDGE** se replica en la NIC virtual de la máquina virtual una configuración de red válida en dicha red. Típicamente en una máquina virtual en un PC se replica la del equipo en el que se hospeda con el mismo identificador de red, máscara y dominio de difusión, pero con una dirección IP diferente que no esté asignada en la misma LAN. El modo bridge posibilita que la máquina virtual se comporte como una máquina física más dentro de la red.

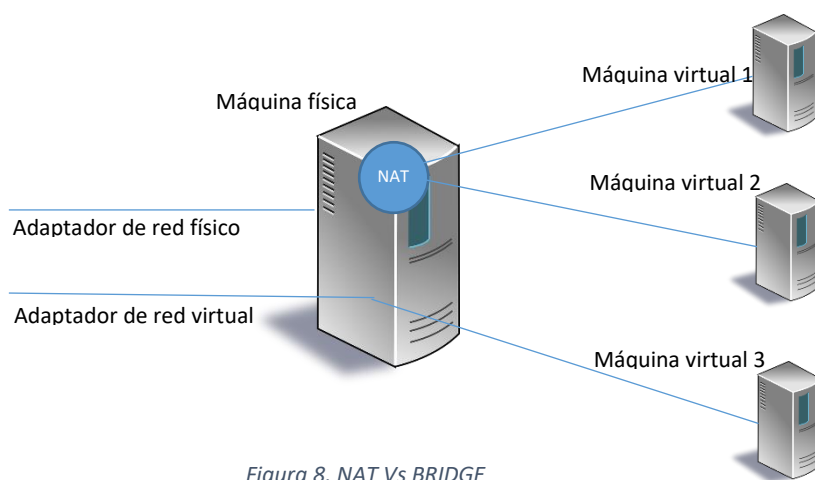
En el caso de configuración de máquinas virtuales en modo BRIDGE dentro de una **red privada**⁷, estas necesitan de un proxy web para acceder a internet, al igual que las máquinas físicas de la misma subred.

⁷ Una red privada usa un espacio de direccionamiento IP privado, es decir, un rango de direcciones sin conexión al exterior (a internet).

NAT, también conocido como enmascaramiento de IP es un mecanismo para intercambiar paquetes de red entre redes con dominios de difusión incompatibles. Este método posibilita a equipos de redes privadas acceder a internet ya que permite alcanzar direcciones de red fuera de la red privada mediante el enmascaramiento.

La configuración del modo NAT en las máquinas virtuales de aplicaciones de escritorio como VMware Workstation Player o Virtualbox típicamente asignan una IP de un direccionamiento de red interno y enmascaran la salida con la IP del equipo físico.

En el siguiente ejemplo (VER FIGURA 8) las máquinas virtuales 1 y 2 acceden a la red mediante NAT y se encuentran en una red diferente a la máquina virtual 3 que accede en modo BRIDGE y se encuentra en la misma red que la máquina física.



Respecto a los modos de difusión de la información, también necesitaremos los siguientes conceptos:

- **Unicast** o difusión única, es el envío de información desde un único nodo emisor a un único nodo receptor.
- **Multicast** o multidifusión, es el envío de información desde un único nodo emisor a un grupo de nodos receptores de manera simultánea. Requiere de un rango de direcciones de clase D que no identifican a nodos sino a subredes.
- **Broadcast** o difusión, es el envío de información desde un único nodo emisor a todos los nodos receptores de manera simultánea. Alcanza a todos los nodos que se encuentran en la misma subred.
- **P2P** (siglas en inglés de peer to peer) es una comunicación que permite intercambiar información de forma directa entre pares de nodos sin arquitectura cliente – servidor.

1.4.2. Conceptos de almacenamiento

El mundo del almacenamiento es apasionantemente extenso, mucho más que lo que abarca este trabajo. A continuación, se exponen algunas referencias exclusivas a tecnologías de almacenamiento utilizadas en la implantación que se desarrollará más adelante. [15]

Un modelo de red de almacenamiento **SAN** (*en inglés: Storage Area Network*) lo constituye uno o varios equipos (**Hosts**) conectados mediante uno o varios conmutadores de red (**Switches**) a una o varias unidades de almacenamiento de datos nombradas y enumeradas como **LUN** (*en inglés: Logical Unit Number*), mediante los protocolos Fibre Channel⁸ o **iSCSI**. VER FIGURA 9).

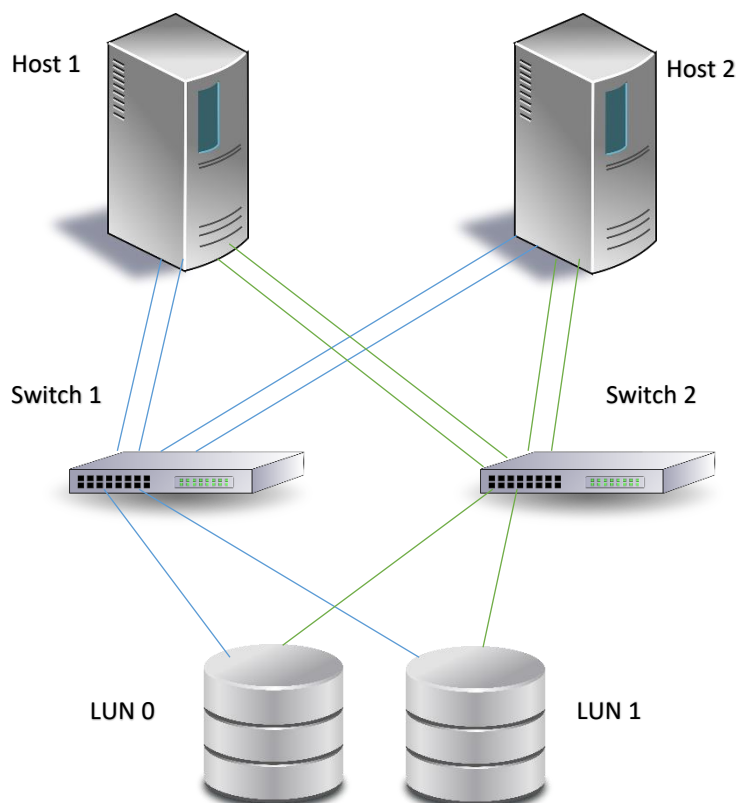


Figura 9. SAN redundante

iSCSI (abreviatura de **Internet SCSI**) es una es la estructura de comunicación de datos del protocolo **SCSI** para transmisión de información entre dispositivos en un bus de datos, pero sobre **TCP/IP**.

Los controladores **RAID** (*siglas en inglés de Redundant Array of Independent Disks*) permiten configurar y administrar **Virtual disks** (*en español: Discos virtuales*) cuyo almacenamiento puede distribuirse en una agrupación de discos físicos y utilizar parte de la capacidad de almacenamiento para almacenar datos redundantes que permitan reconstruir los datos en caso de fallo de alguno de los discos físicos que componen el disco virtual.

⁸ **Fibre channel** (en español: canal de fibra) es una tecnología de red para redes de almacenamiento.

Un **Volumen lógico** (o simplemente volumen) es una porción de un **Virtual disk** que puede ser identificado por los **Hosts** mediante un **LUN** (siglas en inglés de *Logical Unit Number*) y que lo consideran como un solo disco de gran tamaño.

Existen múltiples configuraciones diferentes de RAID. Las utilizadas en este trabajo son:

- **RAID 0:** Máximo aprovechamiento del espacio de almacenamiento y gran velocidad de transferencia en patrones secuenciales.
- **RAID 1:** Conocido como *mirror* (en español: espejo), usa un número par de discos para copiar cada bloque del volumen lógico en discos físicos distintos. Aporta mejora de rendimiento en lectura de datos al poder leerse en paralelo además de tolerancia a un fallo de un disco.
- **RAID 5:** Necesita un mínimo de 3 discos para ser implementado. Distribuye los datos con paridad entre los discos con bajo coste de redundancia y gran velocidad de transferencia por lo que se ha convertido en la implementación más popular.

Un **DataStore** es un repositorio para el almacenamiento de datos y es el término que utiliza **VMware** para referirse al lugar donde se almacenan las máquinas virtuales, las plantillas, los ficheros ISO⁹ o cualquier otra información. El formato nativo de VMware para el sistema de archivos de los DataStores es **VMFS** (en inglés: *VMware File System*). Este almacenamiento en uno o varios DataStores es, por tanto, el contenedor de máquinas virtuales ejecutadas por uno o varios hipervisores. VER FIGURA 10.

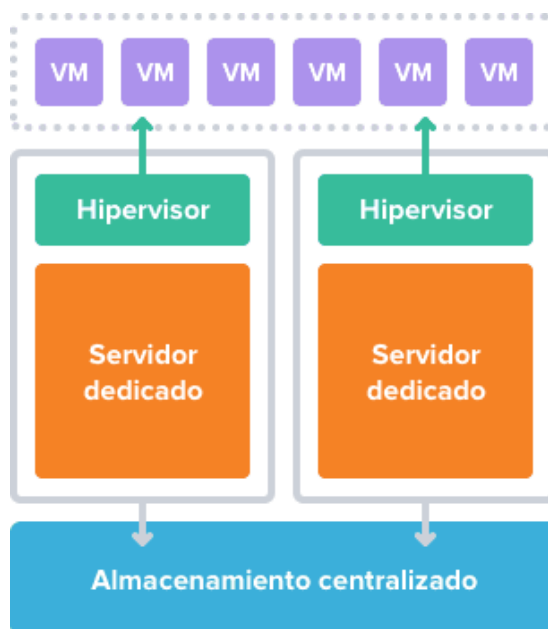


Figura 10. SAN & Virtualización

⁹ Una **ISO** es un archivo que contiene una imagen de un sistema de archivos. Su uso más común es para la distribución de sistemas operativos.

1.5. Características del sistema

Las características del sistema donde se ha llevado a cabo el desarrollo de este trabajo están pensados y dimensionados para dar servicios adicionales en un entorno mucho mayor, cuyo desarrollo va más allá de la temporización de un TFG. Los dispositivos empleados son los siguientes:

1.5.1. Servidores

El sistema virtualizado se ha montado en dos servidores HPE **Proliant DL380p Gen8** (VER FIGURA 11).

Estos servidores cuentan con 2 procesadores Intel Xeon de 16 núcleos, 128GB de memoria RAM y 2 discos HDD¹⁰ de 2,5" SAS¹¹ hot swap¹² de 300GB a 10K (10.000 rpm).



Figura 11. Proliant DL380 G8

Cuenta también con una controladora de almacenamiento (*smart array P410i*) que permite montar diferente niveles de RAID (VER 1.4.2. CONCEPTOS DE ALMACENAMIENTO) en los discos e integra además 8 NIC (VER 1.4.1. CONCEPTOS DE REDES & REDES VIRTUALES) Gigabit¹³ ethernet integrados.

1.5.2. Conmutadores

Los conmutadores del sistema son dos switches HP **ProCurve 2810-24G J9021A**. (VER FIGURA 12). Estos conmutadores cuentan con 20 puertos 10/100/1000 Mbps y disponen también de 4 puertos de doble personalidad para conexiones RJ-45 10/100/1000 o Gigabit de fibra.



Figura 12. HP ProCurve 2810-24G

¹⁰ **HDD** (Hard Disk Drive) es la forma de almacenamiento de datos estándar en discos frente a **SSD** (Solid State Drive) construidos con chips de memoria.

¹¹ **SAS** (Serial Attached SCSI) Es una tecnología para transferencia de datos que implementa el nivel físico de SCSI pero con línea de datos en serie. Alcanza gran velocidad y permite conexión y desconexión rápida de discos duros, usando conectores del interfaz SATA.

¹² Un disco duro **hot swap** permite intercambio en caliente, por lo que en caso de fallo puede ser reemplazado sin parada del sistema.

¹³ **Gigabit** (Gbit) es una unidad de medida equivalente a 10^9 bits habitualmente relacionado con velocidades de transmisión de datos por segundo, por lo que lo correcto es **Gbit/s** o **Gbps**.

1.5.3. Almacenamiento

El almacenamiento se ha llevado a cabo en una cabina HPE **P2000 G3 FC MSA System SFF** (VER FIGURA 13) que proporciona un sistema modular array SAS de 24 bahías para discos de 2,5'' y 2 controladoras.



Figura 13. P2000 G3 MSA

Esta, es una solución de alto rendimiento que proporciona confiabilidad, disponibilidad, flexibilidad y facilidad de administración.

La cabina cuenta con **24 discos HDD SAS hot swap** de 900GB a 10K (10.000 revoluciones por minuto), lo que en bruto supone 21TB.

1.5.4. PCs

Los 342 equipos de los laboratorios (Aulas TIC) tienen un perfil hardware heterogéneo debido a que su renovación se produce de forma secuencial.

El tipo más representativo es **HP ProDesk 400 G1 SFF** (VER FIGURA 14). Estos cuentan con procesador Intel Pentium i3-4160 de 4ª generación, 8 GB de memoria RAM, SSD de 250GB y HDD de 500GB.



Figura 14. HP ProDesk 400 G1

1.6. Metodología

No hemos encontrado una metodología estandarizada para el análisis, diseño e implementación de aulas TIC, para la implantación de virtualización de sistemas ni para la interconexión de dispositivos. A pesar de ello, se ha utilizado un modelo metodológico mixto en cascada + espiral, propios de ingeniería del software, pero aplicados a sistemas.

La **metodología en cascada** consiste en un proceso secuencial de desarrollo a través del análisis de necesidades, el diseño, la implantación, las pruebas, la integración y el mantenimiento. Es por lo que se divide en fases secuenciales planificadas con el objetivo final de la ejecución del sistema de una sola vez.

La **metodología en espiral** consiste en el establecimiento de objetivos clave, así como la evaluación y **reducción de riesgos** mediante su fraccionamiento. Para ello se realizan iteraciones alrededor de una espiral que atraviesa cuatro cuadrantes básicos:

1. Determinación de objetivos y alternativas, así como identificación de los riesgos.
2. Evaluación de las alternativas y análisis de riesgos.
3. Desarrollo y verificación de resultados, aplicando alguna metodología (por ejemplo; en cascada).
4. Planificación de la próxima iteración.

La tradicional **metodología en cascada** aplicada al presente trabajo fin de grado ha consistido en la ordenación de las etapas de desarrollo en fases de **análisis, diseño e implementación**, finalizando con la puesta en marcha del sistema resultante. Sin embargo, esta metodología conllevaría una secuenciación de las diferentes etapas, lo que implicaría que el inicio de cada etapa se sincronizara con la finalización de la etapa anterior, además de que la ejecución del sistema fuera absoluta, cuando lo deseable es una puesta en marcha gradual.

El presente trabajo ha contenido muchos factores de riesgo durante su implantación, dado que ha sido el resultado de virtualizar un sistema en producción. Su naturaleza crítica ha dado lugar a que la **metodología en espiral** también tenga cabida durante su fase de implantación, dado que reduce los riesgos del proyecto, además de aportar mayor flexibilidad y adaptabilidad, permitiendo de esta forma un mejor ajuste.

En este sentido cabe destacar que, tras la puesta en marcha del sistema de virtualización, no todos los servicios se han instalado en paralelo, sino que su puesta en producción ha tenido lugar de uno en uno, de manera progresiva.

1.7. Estructura de la memoria

El documento correspondiente a la memoria de este TFG se ha estructurado de la siguiente manera:

En la **Introducción** se detalla el punto de inicio que suscita este trabajo y los objetivos que se pretenden alcanzar con la realización del mismo. Es decir, **antecedentes y objetivos**.

También, se realiza una descripción de las **herramientas y tecnologías** utilizadas, **conceptos preliminares** necesarios para entender el desarrollo del TFG, las **características del sistema** donde se ha llevado a cabo y la **metodología** aplicada.

En el siguiente capítulo se desarrollan dos **Análisis**, con sus respectivos **dimensionamientos**: i) en un entorno para dar servicio en un escenario mucho mayor al referenciado en este TFG (**entorno docente educativo de grado superior**) y ii) en un entorno dimensionado para dar servicio en el escenario objeto de este TFG (**entorno docente educativo de grado medio**).

El **Diseño**, para la posterior implementación del sistema, se realiza en dos líneas. La primera trata los dispositivos y el sistema de virtualización e incluye, por tanto, dos **esquemas del sistema**; uno **conceptual** y otro de **interconexión de dispositivos**.

La otra línea de diseño es respecto del **modelo de aula TIC**, por lo que incluye los **servicios básicos** necesarios para el normal desarrollo de la docencia.

En el capítulo de **Implementación** se describe con detalle el trabajo realizado para la **puesta en marcha** de los **dispositivos y los servicios** analizados y diseñados en los capítulos anteriores.

Por último, se exponen las **Conclusiones** obtenidas en el desarrollo de este trabajo fin de grado y posibles **líneas futuras** de trabajo.

2. ANÁLISIS

La fase de análisis es especialmente crítica tanto por las características diferenciales de las **Aulas TIC**, como por el correcto dimensionamiento del sistema que contiene los servicios necesarios para su puesta en marcha.

El análisis es el primer paso necesario para el diseño de las aulas TIC y su interconexión de red. Además, facilita la generación del esquema conceptual del sistema de virtualización y por tanto del esquema de interconexión de los dispositivos.

2.1. Análisis del modelo de aula TIC

Son muchas las herramientas existentes a disposición del profesorado y del alumnado que facilitan los procesos de enseñanza y aprendizaje. Sin embargo, nuestro análisis no va encaminado a la didáctica si no a la administración de sistemas, por lo que nuestra descripción del modelo constituye un manual técnico para la instalación, despliegue, administración y gestión de los equipos informáticos que componen un aula TIC.

El análisis del modelo de laboratorio o aula TIC se realiza en un escenario de educación superior, en concreto en los **doce laboratorios** (con un total de 342 equipos informáticos) del *Departamento de Lenguajes y Ciencias de la Computación* ubicados en la *Escuela Técnica Superior de Ingeniería Informática* de la *Universidad de Málaga*.

Esta peculiaridad cubre sobradamente cualquier otro escenario en un entorno educativo de grado medio.

2.1.1. Equipos clientes

Los equipos clientes son los PC ubicados en los laboratorios o aulas TIC a disposición de los alumnos y del profesorado.

En principio se valora la posibilidad de que estos cuenten con una partición de Windows y otra de Linux con objeto de dar mayor cobertura a las necesidades docentes.

Sin embargo, precisamente por la mayor cobertura a estas necesidades docentes y dado que es necesario ofrecer gran cantidad de software en Windows y en diferentes distribuciones de Linux optamos por la siguiente configuración:

- Un disco o partición principal con **el sistema operativo y el software común**. Optamos por Windows 10, Office 2016, VMware Workstation Player, VirtualBox¹⁴ [16] y una selección de software de mayor uso, común al mayor número de asignaturas desarrolladas en el laboratorio.

¹⁴ **VirtualBox** es un software de virtualización de Oracle similar a VMware Workstation Player.

- Otro disco o partición secundaria, **contenedor de máquinas virtuales** locales al equipo para ser ejecutadas con VMware Workstation Player o con VirtualBox. El hecho de que las máquinas virtuales con diferentes sistemas operativos y distribuciones puedan ser ejecutadas localmente hace que el modelo sea muy flexible y polivalente.

El objetivo de dicha configuración será establecer la instalación sobre un **equipo modelo** que será tomado como imagen mediante un sistema de clonación para su posterior estampación en el resto de equipos.

Como resultado del análisis para los equipos cliente, (VER 1.5.4. PCs), el sistema operativo y el software común se almacenará en un disco SSD de 240GB y el contenedor de máquinas virtuales en un disco HDD de 500GB.

2.1.2. Interconexión de red

En este apartado se realiza el análisis de interconexión de red tanto para las Aulas TIC como para la infraestructura de virtualización.

2.1.2.1. Red de las Aulas TIC

En un escenario con **342 equipos** clientes (más **24 Raspberry Pi**¹⁵, además de algunos servicios y aplicaciones en la misma VLAN) sería necesaria una subred capaz de direccionar 512 direcciones (realmente 510, ya que la primera y la última son el identificador de red y la dirección de broadcast – VER 1.4.1. CONCEPTOS DE REDES & REDES VIRTUALES). Estamos hablando por lo tanto de una subred cuya máscara red será 255.255.254.0 (/23 en formato CIDR¹⁶)

Sin embargo, en nuestro escenario los equipos de los usuarios en las Aulas TIC cuentan con una partición repleta de máquinas virtuales de las cuales muchas se ejecutan en modo **bridge**. Esto implica que en cada equipo cliente pueden ser necesarias dos direcciones IP válidas en la subred por lo que es necesario dimensionar el espacio de direcciones al doble.

En este caso, es necesaria una subred cuya máscara sea 255.255.252.0 (/22 en formato CIDR), con espacio de direcciones para 1024 *hosts* (realmente 1022).

2.1.2.2. Red de la Infraestructura de virtualización

La infraestructura de virtualización está compuesta por dos servidores (VER 1.5.1. SERVIDORES), dos conmutadores (VER 1.5.2. CONMUTADORES) y una cabina de almacenamiento (VER 1.5.3. ALMACENAMIENTO). Para estructurar mejor la gestión de su direccionamiento IP es deseable que no comparta espacio de direcciones con las Aulas TIC.

- Servidor 1 (ESXi 1): dos direcciones IP; una de gestión y otra para la iLO¹⁷.

¹⁵ **Raspberry Pi** es una placa computadora de bajo coste desarrollado por Raspberry Pi Foundation.

¹⁶ **CIDR** (Classless Inter Domain Routing) define (entre otras cosas) la sintaxis para especificar la longitud de una red indicando cuantos bits se dedican a la máscara de red.

¹⁷ La **iLO** de HPE es una herramienta de gestión remota que permite configurar, supervisar y actualizar servidores.

- Servidor 2 (ESXi 2): dos direcciones IP; una de gestión y otra para la iLO.
- Conmutador 1: una dirección IP de gestión.
- Conmutador 2: una dirección IP de gestión.
- Cabina de almacenamiento: dos direcciones IP de gestión (una por controladora).
- vCenter Server Appliance: una dirección de gestión.

Para la gestión de los dispositivos descritos anteriormente son necesarias 9 direcciones IP y reservar algunas otras para funcionalidades futuras, como servidores de copia de seguridad de máquinas virtuales. En cualquier caso, una subred pequeña; por ejemplo: /26 o /27 con espacios de direcciones para 64 y 32 *hosts* respectivamente (menos red y difusión), sería más que suficiente.

2.1.3. Servicios y aplicaciones necesarios

Tal y como avanzamos anteriormente (VER 2.1. ANÁLISIS DEL MODELO DE aula TIC) el análisis de nuestro modelo no lo realizamos desde el punto de vista de la didáctica, si no de la administración del sistema por lo que los servicios y aplicaciones objeto de análisis son aquellos necesarios para la puesta en marcha, el funcionamiento, la administración y la gestión del Aula TIC.

A continuación, se presenta el análisis de necesidades que genera la elección de los servicios y aplicaciones que consideramos indispensables para nuestro propósito:

- Necesidad de asignar la configuración de red al parque de equipos y dispositivos (342 PC + 24 Raspberry pi); **DHCP**. VER 1.3.3. PROTOCOLO DHCP.
- Necesidad de acceso web al parque de equipos a pesar de tener direcciones IP privadas (sin acceso a internet). **Proxy**. VER 1.3.4. SERVICIO PROXY.
- Necesidad de difundir enunciados de prácticas o cualquier otro material docente en formato digital. Servidor **Samba**. VER 1.3.5. PROTOCOLO CIFS. IMPLEMENTACIÓN SAMBA.
- Necesidad de un sistema de clonación eficiente que permita el despliegue de sistemas en los equipos. Servidor **OpenGnsys**. VER 1.3.6. APLICACIÓN OPENGNSYS.

Aunque todos los servicios y aplicaciones podrían compartir servidor (y sistema operativo) en una misma máquina virtual, estimamos conveniente que cada uno constituya un servidor independiente en máquinas virtuales diferentes.

Algunas de las ventajas de no compartir sistema operativo son las siguientes: servicios y aplicaciones más robustas (al aislar posibles catástrofes), reducción de la complejidad, facilitar el mantenimiento y las copias de seguridad.

2.2. Dimensionamiento

El dimensionamiento de la infraestructura de virtualización ha sido realizado con la configuración necesaria de procesamiento, memoria y almacenamiento para que soporte la totalidad de los servicios en explotación existentes en el momento de su implantación.

Dicho dimensionamiento se ha realizado de forma generosa para que permita acometer la puesta en marcha de nuevos servicios o proyectos sin interferir en el desempeño de los que se encuentren en producción.

En concreto, la infraestructura de virtualización del departamento soporta 58 Máquinas Virtuales de diferente propósito (*en el momento de confección de la memoria de este trabajo*), distribuidas en las siguientes categorías:

- Genéricas => Máquinas para clonar y desplegar.
- Proyectos & Pruebas => Máquinas de proyectandos o de prueba.
- Servidores de BBDD => Servidores o pasarelas de Oracle.
- Servidores de Departamento => Directorio, documentación, congresos, etc.
- Servidores de Docencia => Servidores de licencias, de control de versiones, etc.
- Servidores de Investigación => Máquinas de diferente propósito.
- Servidores Web => Web del departamento y otras.
- Servidores de Laboratorios => DHCP, OpenGnsys, Proxy, Samba, etc.
- Servidores Virtualización => vCenter Server Appliance y Aplicación de copias de seguridad de máquinas virtuales.

Para el desempeño de sus funciones, la infraestructura de virtualización del departamento cuenta con 32 núcleos de procesamiento, 256GB de RAM (VER 1.5.1. SERVIDORES) y un almacenamiento en bruto de 21TB (VER 1.4.2. CONCEPTOS de almacenamiento) a los que descontaremos más adelante, los que se pierdan por la redundancia de datos del RAID una vez montado.

El exiguo almacenamiento local con el que se han configurado los servidores *HPE Proliant DL380p Gen 8* (VER 1.5.1. SERVIDORES) se debe a que su propósito es contener sólo su propio sistema (*VMware vSphere Hypervisor – ESXi ver 6.5*) y no máquinas virtuales. Todas las máquinas virtuales expuestas anteriormente residen en la cabina de almacenamiento *HPE MSA P2000 G3* (VER 1.5.3. ALMACENAMIENTO).

Lo servidores de los laboratorios – Aulas TIC del departamento, objeto de este trabajo, suponen un subconjunto del total de máquinas virtuales que corren en la infraestructura de virtualización del departamento.

El consumo de recursos de estas máquinas virtuales es el siguiente:

- Servidor DHCP (VER 1.3.3. PROTOCOLO DHCP) => 1 procesador de 1 núcleo, 400 Mb de RAM y 10 GB de disco.
- Servidor Proxy (VER 1.3.4. SERVICIO PROXY) => 1 procesador de 1 núcleo, 1 GB de RAM y 10 GB de disco.
- Servidor Samba (VER 1.3.5. PROTOCOLO CIFS. IMPLEMENTACIÓN SAMBA) => 1 procesador de 1 núcleo, 1 GB de RAM y 100 GB de disco.
- Servidor OpenGnsys (VER 1.3.6. APLICACIÓN OPENGNSYS) => 2 procesadores de 1 núcleo, 2GB de RAM y 750 GB de disco.

Hay que tener en cuenta que el análisis realizado para el dimensionamiento del servidor Samba y del Servidor de OpenGnsys en lo referente a almacenamiento, son particulares para cubrir las necesidades de los laboratorios – Aulas TIC del departamento de Lenguajes y Ciencias de la Computación de la Universidad de Málaga.

Este dato es importante pues del tamaño asignado al almacenamiento del servidor OpenGnsys dependerá el tamaño y la cantidad de imágenes diferentes para equipos de los laboratorios – Aulas TIC que pueda albergar. En concreto, dependiendo del modelo de PC de laboratorio operativo (VER 2.1.1. EQUIPOS CLIENTES) las imágenes de la primera partición o primer disco con el sistema ocupan entre 80 y 94GB y las imágenes de segunda partición o segundo disco duro con las máquinas virtuales locales, entre 101 o 104GB. Es por lo que con 750GB es posible almacenar 6 imágenes del tipo descrito.

Igualmente dependiendo del propósito para el que se diseñe el servidor Samba dependerá su tamaño de almacenamiento. En nuestro modelo, el servidor Samba sólo se usa para la distribución de algunas prácticas por lo que 20GB cubre sobradamente nuestras necesidades.

En total, los servidores para los laboratorios suponen 5 núcleos de procesamiento, 4,4GB de RAM y 790GB de almacenamiento. Además, habría que sumar los requerimientos necesarios para la administración centralizada de los servidores con ESXi mediante vCenter Server Appliance. En concreto, la versión instalada en el departamento requiere lo siguiente:

- Servidor VMware vCenter server (VER 1.3.1. SOFTWARE DE VMWARE) => 2 procesadores de 1 núcleo, 10GB de RAM y 240GB de almacenamiento.

Por todo lo anterior, concluimos en esta fase de análisis que para hacer trasladable este trabajo de forma holgada a un entorno docente de grado medio es necesario un sistema con unos requerimientos totales de 7 núcleos, 14,4GB de RAM y 990GB de almacenamiento.

Esto no quiere decir que el sistema de virtualización asigne dichos recursos de forma permanente, (lo hace bajo demanda), pero sí qué representa una medida indicativa para el dimensionamiento del sistema pues revela un techo máximo de consumo de recursos.

3. DISEÑO

En este capítulo se detallan todos los estudios y diseños realizados con anterioridad (y a veces en paralelo) a la implementación de este trabajo fin de grado.

3.1. Espacio de direccionamiento de red

Diferenciamos dos direccionamientos de red: uno para el funcionamiento de los equipos y máquinas virtuales en los Laboratorios - Aulas TIC y otro para la gestión de los dispositivos de la infraestructura de virtualización

3.1.1. Direccionamiento de las Aulas TIC

Se solicita, a la autoridad de red competente una subred con las características descritas en la **fase de análisis** (VER 2.1.2.1. RED DE LAS AULAS TIC) y se concede al departamento el uso de la red 192.158.164.0/22.

A continuación, **diseño de un espacio de direcciones disjunto** en dicha red (VER TABLA 1 Y TABLA 2) para evitar **conflictos de IP**¹⁸.

Lab. /Aula TIC	Equipos Físicos	Máquinas Virtuales	Direcciones
Laboratorio 3.1.1	192.168.164.1 a 40	192.168.165.1 a 40	40 + 40
Laboratorio 3.1.2	192.168.164.41 a 80	192.168.165.41 a 80	40 + 40
Laboratorio 3.1.3	192.168.164.81 a 120	192.168.165.81 a 120	40 + 40
Laboratorio 3.1.4	192.168.164.121 a 160	192.168.165.121 a 160	40 + 40
Laboratorio 3.1.5	192.168.164.161 a 200	192.168.165.161 a 200	40 + 40
Laboratorio 3.1.6	192.168.164.201 a 240	192.168.165.201 a 240	40 + 40
Laboratorio 3.1.7	192.168.166.1 a 40	192.168.167.1 a 40	40 + 40
Laboratorio 3.1.9	192.168.166.41 a 80	192.168.167.41 a 80	40 + 40
Laboratorio 3.1.10	192.168.166.81 a 120	192.168.167.81 a 120	40 + 40
Laboratorio 3.1.11	192.168.166.121 a 160	192.168.167.121 a 160	40 + 40
Laboratorio 3.1.12	192.168.166.161 a 200	192.168.167.161 a 200	40 + 40

Tabla 1. Espacio de direcciones en las Aulas TIC

Cometido	Equipos	Equipos Físicos	Direc.
Servicios y Aplicaciones	192.168.166.201 a 225	192.168.167.201 a 225	25 + 25
Aula TIC Avanzada		192.168.167.226 a 249	24
Raspberry Pi	192.168.166.226 a 249		24

Tabla 2. Espacio de direccionamiento de características especiales.

Las direcciones IP de las máquinas físicas se asignan mediante DHCP dando de alta todas las direcciones MAC de los equipos y asociando a cada una la dirección IP correspondiente.

No es posible hacer lo mismo con las direcciones IP de las máquinas virtuales puesto que sus direcciones MAC también son virtuales y dada su naturaleza volátil se hace impracticable. Es

¹⁸ Un conflicto de IP ocurre cuando dos o más dispositivos de la red tienen la misma dirección IP.

por lo que la asignación de IP a las máquinas virtuales en modo bridge se hace por convención. Sólo es necesario consultar la IP del equipo físico y cambiar el tercer octeto en la máquina virtual sin alterar el resto. Veamos un par de ejemplos:

- La máquina virtual en modo bridge para el equipo físico del Laboratorio 3.1.2, cuya IP es 192.168.164.41 sería 192.168.165.41.
- La máquina virtual en modo bridge para el equipo físico del Laboratorio 3.1.7, cuya IP es 192.168.166.1 sería 192.168.167.1.

3.1.2. Direccionamiento de la infraestructura de virtualización

Se solicita, a la autoridad de red competente una subred con las características descritas en la **fase de análisis** (VER 2.1.2.2. RED DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN) y se concede el uso de la red 192.168.198.0/24 que cubre de forma amplia las necesidades de direccionamiento.

A continuación, **diseño de un espacio de direcciones** en dicha red. VER TABLA 3. ESPACIO DE DIRECCIONAMIENTO DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN.

Dirección IP	Dispositivo	Propósito
192.168.198.1	Servidor 1	iLO Servidor 1
192.168.198.2	Servidor 2	iLO Servidor 2
192.168.198.3	Servidor 1	Acceso Servidor 1
192.168.198.4	Servidor 2	Acceso Servidor 2
192.168.198.5		
192.168.198.6		
192.168.198.7	Switch 1	Toma de gestión
192.168.198.8	Switch 2	Toma de gestión
192.168.198.9	Cabina almacenamiento	Toma de gestión de la controladora A
192.168.198.10	Cabina almacenamiento	Toma de gestión de la controladora B
192.168.198.11		
192.168.198.12		
192.168.198.13		
192.168.198.14		
192.168.198.15	vcsa2	vCenter Server Appliance 6.5

Tabla 3. Espacio de direccionamiento de la infraestructura de virtualización.

Cabe destacar que **existen otros dispositivos** y aplicaciones en la red de la infraestructura de virtualización con diferentes propósitos como son servidores programación y gestión de copias de seguridad de máquinas virtuales, máquina virtual para gestión de SAI¹⁹ e incluso otros servidores de virtualización, pero estos **no se han representado en la tabla** por no ser objeto de este trabajo.

¹⁹ **SAI** son las siglas de Sistema de Alimentación Ininterrumpida (*en inglés UPS de Uninterruptible Power Supply*) y se trata de un dispositivo que proporciona alimentación eléctrica durante un tiempo limitado, además de filtrar subidas o bajadas de tensión, gracias a sus baterías.

3.3. Esquema de interconexión de dispositivos

El diseño de la interconexión de red de los dispositivos físicos que cumple con el esquema conceptual descrito anteriormente (VER 3.2. ESQUEMA CONCEPTUAL DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN) es el siguiente: (VER FIGURA 15)

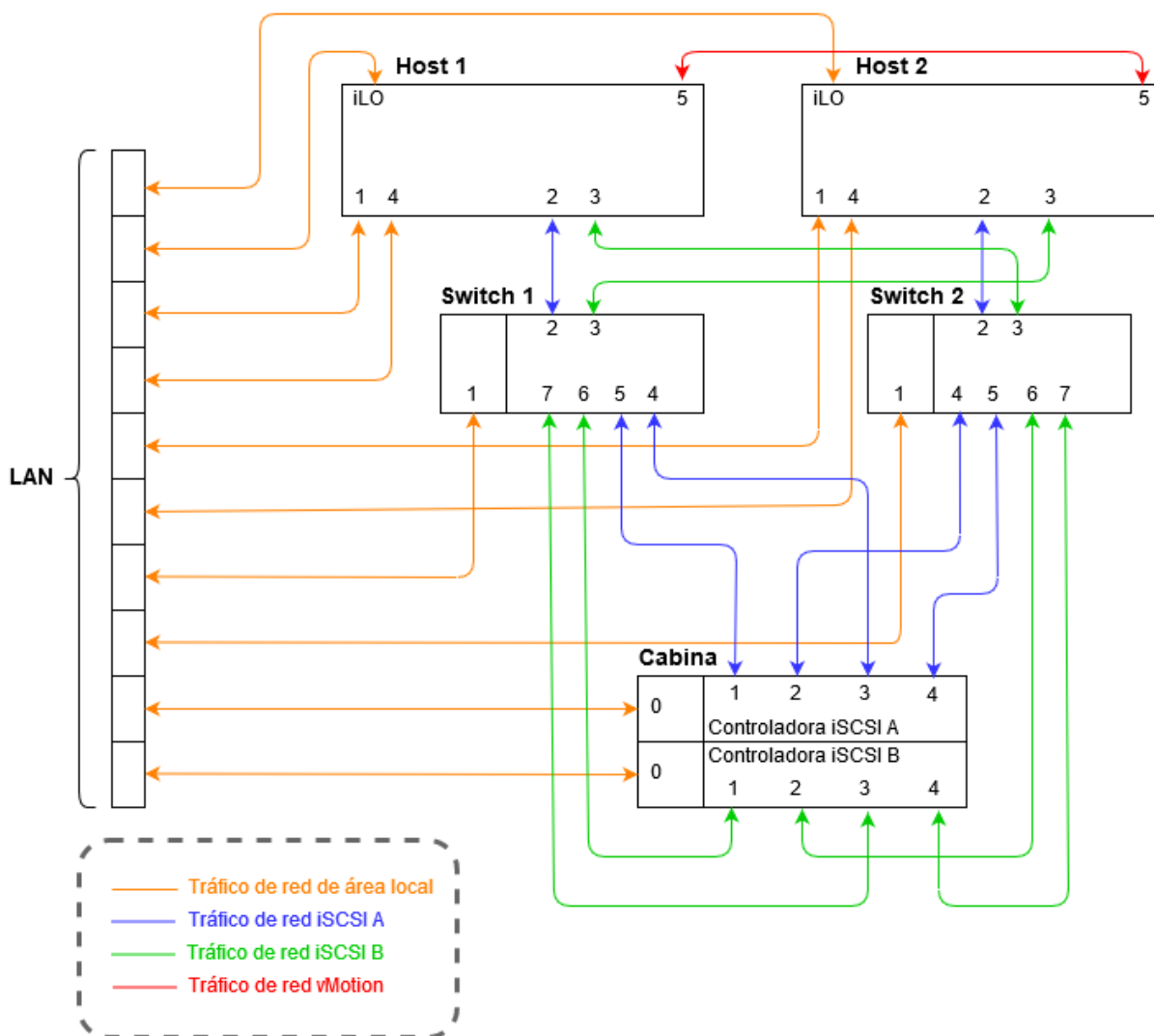


Figura 15. Esquema de interconexión de dispositivos.

En nuestro esquema de interconexión definiremos cuatro redes diferentes:

192.168.198.0/24 ⇔ Tráfico de red de área local (VER 2.1.2.2. RED DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN), representado en la FIGURA 15 en color **naranja**, que comunica la infraestructura de virtualización con el exterior para su administración y gestión mediante el direccionamiento propuesto anteriormente (VER 3.1.2. DIRECCIONAMIENTO DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN).

A esta red conectaremos inicialmente el NIC 1 (el primer interfaz de red) de cada **Host** (VER 1.5.1. SERVIDORES) y posteriormente, también el NIC 4 ya que implementaremos una agregación de enlace de ambos NIC para conseguir mayor desempeño de las máquinas virtuales.

Asimismo, conectaremos también las interfaces iLO de cada *Host*, el puerto número 1 de cada **Switch** (VER 1.5.2. CONMUTADORES) y los interfaces de administración de cada controladora de la **cabina** de almacenamiento (VER 1.5.3. ALMACENAMIENTO).

10.10.10.0/24 ⇔ Tráfico de red iSCSI A representado en la FIGURA 15 en color azul y que tiene como destino la comunicación con la controladora (que hemos identificado como A) de la **cabina** de almacenamiento. Para ello, comunicaremos el NIC 2 de cada *Host* con el puerto 2 de cada **switch** y además, los puertos 4 y 5 del switch 1 con los interfaces iSCSI 1 y 3 de la controladora iSCSI A de la **cabina** de almacenamiento y los puertos 4 y 5 del switch 2 con los interfaces iSCSI 2 y 4 de dicha controladora.

10.10.11.0/24 ⇔ Tráfico de red iSCSI B representado en la FIGURA 15 en color verde y que tiene como destino la comunicación con la controladora (que hemos identificado como B) de la **cabina** de almacenamiento. De igual modo, comunicaremos el NIC 3 de cada *Host* con el puerto 3 de cada **switch** y además, los puertos 6 y 7 del switch 1 con los interfaces iSCSI 1 y 3 de la controladora iSCSI B de la **cabina** de almacenamiento y los puertos 6 y 7 del switch 2 con los interfaces iSCSI 2 y 4 de dicha controladora.

10.10.12.0/24 ⇔ Tráfico de red vMotion. Se trata de una característica de VMware vCenter Server que permite trasladar el procesamiento de máquinas virtuales entre *hosts* (o el almacén de datos donde están contenidas), sin necesidad de parada. En la FIGURA 15 está representado en color rojo y conectará directamente el NIC 5 de cada *Host*, uno con el otro.

3.4. Diseño del modelo de aula TIC

Nuestra propuesta de aula TIC incluye administración centralizada mediante **DHCP** (VER 1.3.3. PROTOCOLO DHCP) y **OpenGnsys** (VER 1.3.6. APLICACIÓN OPENGNSYS). Conceptualmente, ambos elementos están estrechamente relacionados.

El funcionamiento de DHCP es sobradamente conocido por lo que no profundizaremos demasiado. De una forma resumida (VER FIGURA 16), un cliente envía un mensaje de difusión a toda la red y si existe en dicha red un servicio de DHCP, contesta al cliente ofreciendo configuración de red.

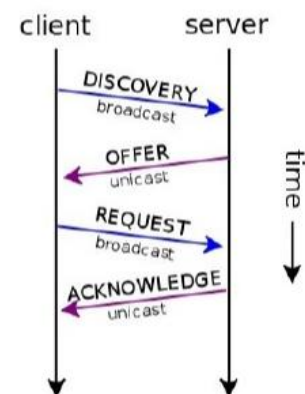


Figura 16. Sesión DHCP.

En nuestro escenario, los equipos de las Aulas TIC realizarán arranque **PXE**²¹. El servidor de **DHCP** les ofrecerá la configuración de red y mediante los parámetros **Next-server** y **filename** (fundamentales para nuestra arquitectura) también les indicará, la dirección de red de un servidor (en nuestro caso el **servidor de OpenGnsys**), del que recibirán instrucciones de que es lo que deben hacer a continuación y el nombre de un archivo de arranque.

²¹ **PXE** son las siglas de Preboot eXecution Environment (en español: Entorno de ejecución de prearranque) y se trata de un sistema para arrancar e instalar el sistema operativo en los equipos a través de una red.

A continuación, en la siguiente figura (VER FIGURA 17) puede verse una representación muy simplificada del arranque de un equipo cliente en el modelo de Aula TIC que estamos diseñando.

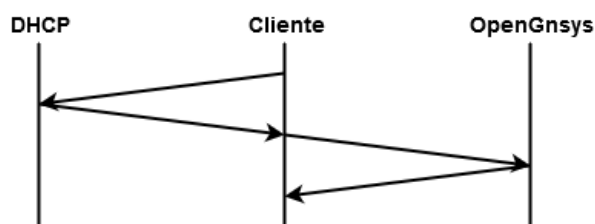


Figura 17. Inicio de equipo cliente

OpenGnsys indicará al equipo cliente si debe ejecutar un sistema operativo de su disco duro local o ejecutar **el cliente de OpenGnsys** que recibirá del **servidor OpenGnsys**.

El cliente de OpenGnsys es un pequeño Kernel de Linux que se carga en la memoria del equipo cliente y puede recibir instrucciones desde la consola de administración del servidor de OpenGnsys para realizar diferentes tareas de administración y gestión; entre ellas podemos destacar la tarea de generar (o recibir) una imagen del sistema operativo o de la partición de máquinas virtuales (VER 2.1.1. EQUIPOS CLIENTES) ya sea de disco completo o de una partición.

Además, gracias a al parámetro **next-server** de **DHCP** es posible disponer fácilmente de más de un servidor de **OpenGnsys** en la red. Simplemente, hay que indicar las direcciones de red de diferentes **next-server** para diferentes grupos de equipos identificados por sus MAC, lo que facilita la puesta en funcionamiento de nuevos servidores sin incidir en la producción de los anteriores.

```
group {                                     <= Grupos
  next-server [ip_servidor_OpenGnsys_1];   <= Dirección del servidor OpenGnsys
  host pc1 {                                <= Equipo pc1 de un Aula TIC
    option host-name "xxx.es";             <= Nombre de equipo
    hardware ethernet xx:xx:xx:xx:xx:xx;   <= Dirección MAC
    fixed-address xxx.xxx.xxx.xxx;         <= Dirección IP para el equipo
    filename "grldr";                      <= Archivo cargador del arranque
  }
  host pc2 ...                              <= Equipo pc2...
}
group {                                     <= Siguiente grupo
  next-server [ip_servidor_OpenGnsys_2];   <= Dirección del servidor de OpenGnsys
  host pc3 {                                <= Equipo pc3 de otro Aula TIC
    option host-name "xxx.es";             <= Nombre de equipo
    hardware ethernet xx:xx:xx:xx:xx:xx;   <= Dirección MAC
    fixed-address xxx.xxx.xxx.xxx;         <= Dirección IP para el equipo
    filename "grldr";                      <= Archivo cargador del arranque
  }
  host pc4 ...                              <= Equipo pc4...
}
```

Por todo lo anterior, implementaremos un DHCP en una máquina virtual con Linux (la distribución no es relevante) donde habilitaremos las peticiones desde PXE y realizaremos agrupaciones de equipos (mediante sus MAC) que representarán los laboratorios – Aulas TIC y definiremos los parámetros de red para dichos equipos (incluidos Next-server y filename), no de forma global, si no para cada una de las agrupaciones.

La implementación del servidor OpenGnsys, la realizaremos sobre una máquina virtual con una versión **LTS**²² de **Ubuntu Server** y definiremos las Aulas TIC utilizando las mismas agrupaciones del servidor de DHCP.

Respecto a los equipos de los laboratorios - Aulas TIC, será necesario habilitar el arranque PXE en la BIOS²³ de todos ellos.

3.5. Servicios básicos para la docencia

Nuestra propuesta de Aula TIC incluye servidores **Samba** y **Proxy**. VER 2.1.3. SERVICIOS Y APLICACIONES NECESARIOS.

En el **servidor Proxy**, diseñaremos **listas de control de acceso** que nos permitan control independiente sobre todos y cada uno de los laboratorios, así como de las máquinas virtuales de cada uno de ellos. Las etiquetas para nuestro direccionamiento (VER 3.1.1. DIRECCIONAMIENTO DE LAS AULAS TIC) será el siguiente:

```
# Agrupaciones de PCs por laboratorios
acl AulaTic_x src IP_inicio-IP_fin/255.255.255.255
acl AulaTic_y src IP_inicio-IP_fin /255.255.255.255
...
# Agrupaciones de máquinas virtuales de laboratorios
acl vmAulaTic_x src IP_inicio-IP_fin/255.255.255.255
acl vmAulaTic_y src IP_inicio-IP_fin/255.255.255.255
...
```

Gracias a las definiciones de las etiquetas anteriores, será posible permitir o denegar el acceso a internet de forma independiente a cada aula TIC sustituyendo en la línea del laboratorio correspondiente **allow** (en inglés: permitir) por **deny** (en inglés: denegar) y reiniciando (o recargando) el servicio a continuación.

```
http_access allow AulaTic_x
http_access allow AulaTic_y
...
http_access allow vmAulaTic_x
http_access allow vmAulaTic_y
...
```

²² **LTS** son las siglas de Long Term Support (*en español: soporte a largo plazo*).

²³ La **BIOS** es un programa instalado en los chips de los equipos y que guarda la configuración de arranque.

El servidor **proxy squid** es una aplicación muy popular en *Linux*, por lo que cualquier distribución será válida para crear una máquina virtual en la que implementar el servicio que atienda las peticiones. Sin embargo, si será importante la consideración del espacio de almacenamiento pues habrá que tener en cuenta el dimensionamiento realizado en la fase de análisis. VER 2.2. DIMENSIONAMIENTO.

Respecto al **servidor Samba**, implementaremos un **recurso compartido** llamado **practicas** donde los profesores podrán subir los archivos necesarios para la docencia y los alumnos puedan acceder para descargarlos.

Otro recurso compartido llamado **VM** contendrá un repositorio de máquinas virtuales para ser descargadas y ejecutadas localmente en los equipos de las Aulas TIC, donde tanto profesores como alumnos sólo tengan permisos de lectura y serán los técnicos los que tengan permiso de escritura para poder subir las máquinas virtuales.

Para ello, estableceremos diferentes permisos, según el usuario que realice la conexión y el recurso al que acceda.

Recursos compartidos

- VM => Para alojar máquinas virtuales
- Practicas => Software proporcionado por profesores para sus clases

Estructura de **directorios**

- /DATOS/practicas => Prácticas en laboratorios docentes.
- /DATOS/VM => Backup de Máquinas virtuales de los laboratorios.

Usuarios

- alumno
- profesor
- tecnicos

Permisos sobre los recursos smb

- \\samba.lcc.uma.es\practicas
 - tecnicos > lectura, profesor > escritura y alumno > lectura
- \\samba.lcc.uma.es\VM
 - tecnicos > escritura, profesor > lectura y alumno > lectura

Para establecer dichos permisos de los usuarios sobre los recursos compartidos utilizaremos en la fase de Implementación las credenciales de autenticación de los usuarios Samba, además de los permisos de usuarios sobre los directorios a nivel del sistema operativo. VER 4.2.4.2. CONFIGURACIÓN DE SAMBA.

4. IMPLEMENTACIÓN

La implementación de este trabajo se compone de dos fases:

- En la primera fase afrontaremos la instalación y configuración de la infraestructura de virtualización.
- En la segunda fase (una vez tengamos la infraestructura en producción), abordaremos la instalación y configuración de todos los servicios y aplicaciones propuestos para el funcionamiento del sistema en un entorno educativo de grado medio.

4.1. Instalación y Configuración de la Infraestructura de Virtualización

El primer paso para la implementación de la infraestructura es un plan de trabajo, seguido de las instalaciones y configuraciones necesarias.

4.1.1. Flujo de trabajo

Comenzaremos con la interconexión del sistema según el diseño establecido (VER 3.3. ESQUEMA DE INTERCONEXIÓN DE DISPOSITIVOS) seguido de la instalación y configuración del almacenamiento (VER 1.5.3. ALMACENAMIENTO).

A continuación, iniciaremos la instalación y configuración de vSphere recomendado por VMware (VER FIGURA 18) consistente en la implementación de los *hosts*, es decir, los hipervisores **ESXi** (VER 1.3.1. SOFTWARE DE VMWARE) en los servidores (VER 1.5.1. SERVIDORES). [17][18]

Finalmente, la aplicación de administración centralizada de todo el conjunto (VER 1.3.1. SOFTWARE DE VMWARE) propuesta por VMware para un **entorno pequeño** con una sola instancia de **vCenter Server** que incluye **Platform Services Controller**.

Platform Services Controller está disponible en el archivo ISO de **Windows vCenter Server** o dentro del archivo ISO de **vCenter Server Appliance (VCSA)**.

Dado que nuestro entorno no es grande, optaremos por la instalación y configuración de **VCSA**.

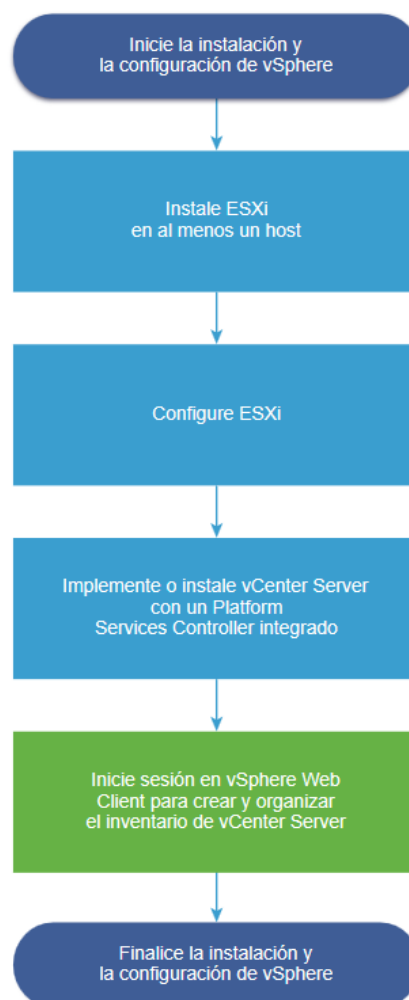


Figura 18. Flujo de instalación vSphere

4.1.2. Interconexión del sistema

Procedemos a realizar el conexionado de red de toda la infraestructura siguiendo el diseño propuesto en el punto 3.3. ESQUEMA DE INTERCONEXIÓN DE DISPOSITIVOS. A continuación, realizaremos la configuración de los conmutadores.

4.1.2.1. Configuración de los conmutadores

Es posible configurar Los conmutadores *HP ProCurve 2810-24G* de nuestra infraestructura (VER 1.5.2. CONMUTADORES) mediante una interfaz web o mediante un puerto de gestión (VER FIGURA 19).

Accederemos a la consola de administración mediante el puerto de gestión. Posteriormente, una vez configurada una IP de gestión para cada conmutador, estos serán accesibles mediante sus respectivas interfaces web.



Figura 19. Puerto de administración Switch ProCurve 2810-24G

Para realizar la configuración mediante el puerto de administración del switch utilizaremos un ordenador portátil y necesitaremos un cable con conector RJ45 a conector serie.

Hay que tener en cuenta que los portátiles actuales no suelen incorporar puerto serie (como en nuestro caso), por lo que además, también necesitaremos un cable con conector serie a USB. La unión de ambos cables nos da un conector de RJ45 a USB. VER FIGURA 20.

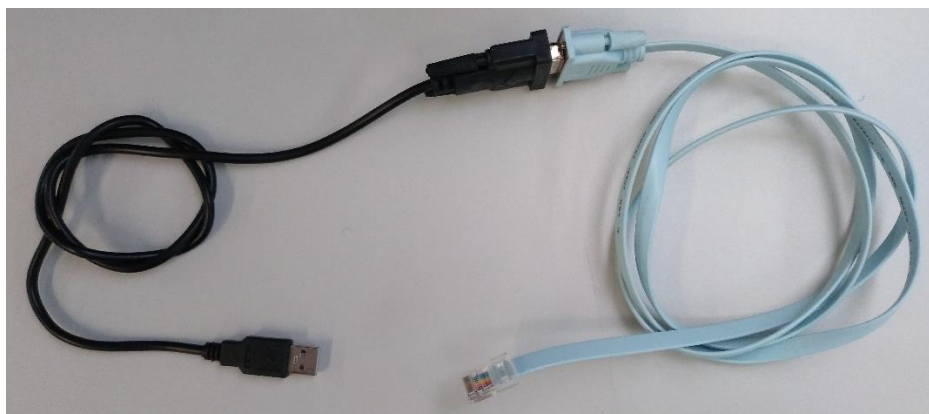


Figura 20. RJ45 a USB.

Es muy importante, antes de establecer la sesión de conexión con el conmutador, conocer en el sistema operativo de origen qué puerto ha identificado el sistema.

Conectamos el cable al conmutador y al ordenador portátil (conector RJ45 al puerto de gestión del switch y USB al portátil). El portátil cuenta con un sistema operativo Microsoft Windows 10 pro, por lo que realizamos la consulta en la siguiente ruta:

- ⇒ Panel de control
- ⇒ Sistema y seguridad
- ⇒ Sistema
- ⇒ Administración de dispositivos

El sistema reconoce USB-SERIAL en el COM5 (VER FIGURA 21), así que realizaremos la sesión de conexión mediante el popular cliente de conexión **Putty**²⁴ contra dicho puerto. (VER FIGURA 22).

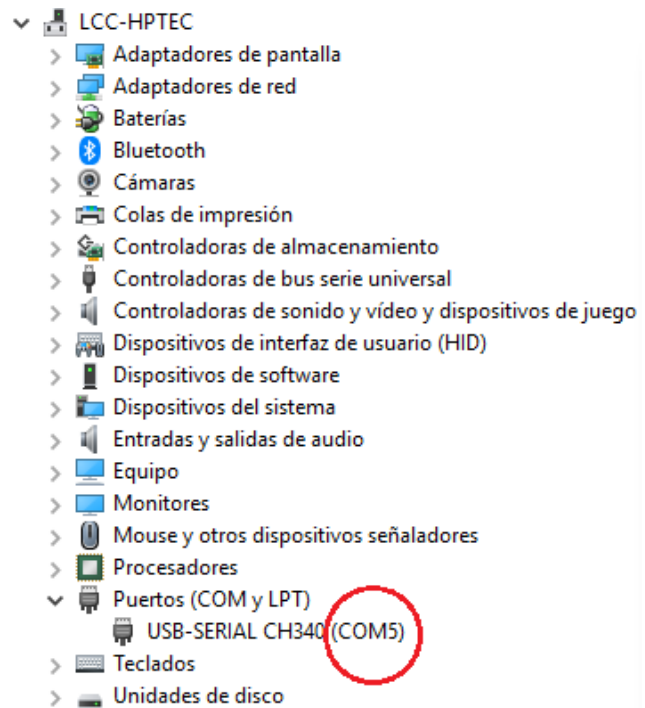


Figura 21. Conexión en COM5

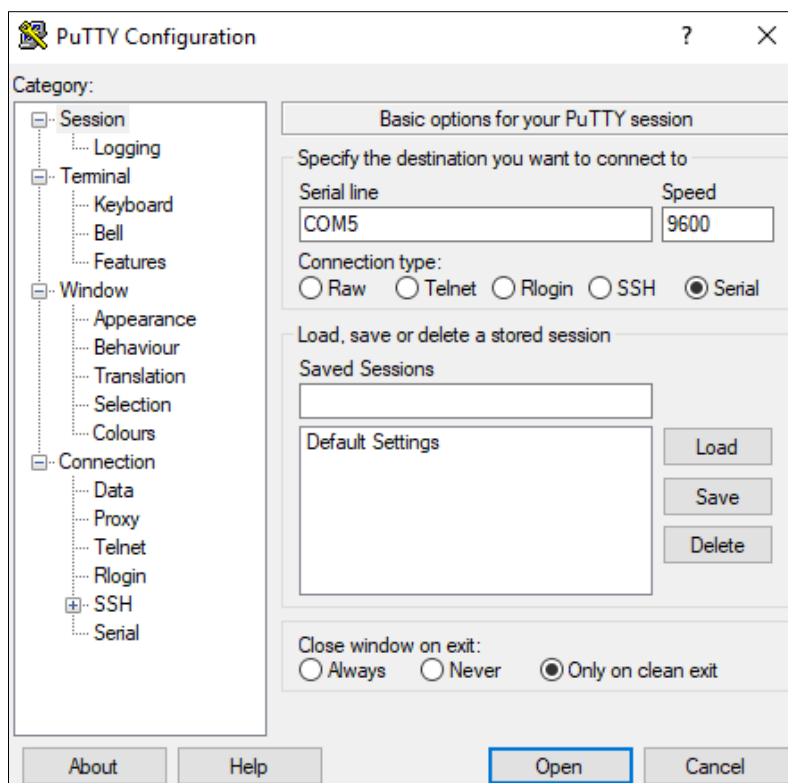


Figura 22. Sesión de conexión con Putty

²⁴ **Putty** es un cliente para realizar conexiones remotas que permite realizar las sesiones de conexión con diferentes tipos de conexión. Putty es una aplicación de código abierto bajo licencia MIT.

El switch *ProCurve 2810-24G* muestra una pantalla de información y bienvenida (VER FIGURA 23) y a continuación, tras pulsar cualquier tecla, la línea de comando del sistema.

```
ProCurve J9021A Switch 2810-24G
Software revision N.11.15

Copyright (C) 1991-2008 Hewlett-Packard Co. All Rights Reserved.

                RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the Government is subject to restrictions
as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and
Computer Software clause at 52.227-7013.

                HEWLETT-PACKARD COMPANY, 3000 Hanover St., Palo Alto, CA 94303

We'd like to keep you up to date about:
* Software feature updates
* New product announcements
* Special events

Please register your products now at: www.ProCurve.com

Press any key to continue █
```

Figura 23. Bienvenida ProCurve 2810-24G

Ejecutamos la orden “*menu*” (VER FIGURA 24) y accedemos al directorio principal del conmutador (VER FIGURA 25).

```
ProCurve Switch 2810-24G# menu █
```

Figura 24. Orden menu

```
ProCurve Switch 2810-24G                                     1-Jan-1990   0:08:46
===== CONSOLE - MANAGER MODE =====
                          Main Menu

 1. Status and Counters...
 2. Switch Configuration...
 3. Console Passwords...
 4. Event Log
 5. Command Line (CLI)
 6. Reboot Switch
 7. Download OS
 8. Run Setup
 9. Stacking...
 0. Logout

Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figura 25. Directorio principal ProCurve 2810-24G

Aunque es posible realizar la configuración completa mediante la interfaz anterior (VER FIGURA 25), es demasiado espartano por lo que optamos por una configuración mínima y acceder posteriormente mediante la interfaz web, mucho más amigable, para finalizar la configuración.

Nuestra configuración mínima consiste en el establecimiento de usuario y contraseña de acceso al conmutador en la opción *Console Passwords* (VER FIGURA 25) y configurar una dirección IP en la opción *Internet (IP) Service* que se encuentra en *Switch Configuration*. (VER FIGURA 25)

La interfaz de administración web del switch *ProCurve 2810-24G* está desarrollada en **Java**²⁵. Para que corra en el navegador de nuestro equipo de trabajo, es necesario tener instalada alguna versión de Java en nuestro sistema y añadir una **excepción de seguridad** para las direcciones IP que acabamos de configurar (una para cada conmutador) en el **Panel de Control de Java**. (VER FIGURA 26)

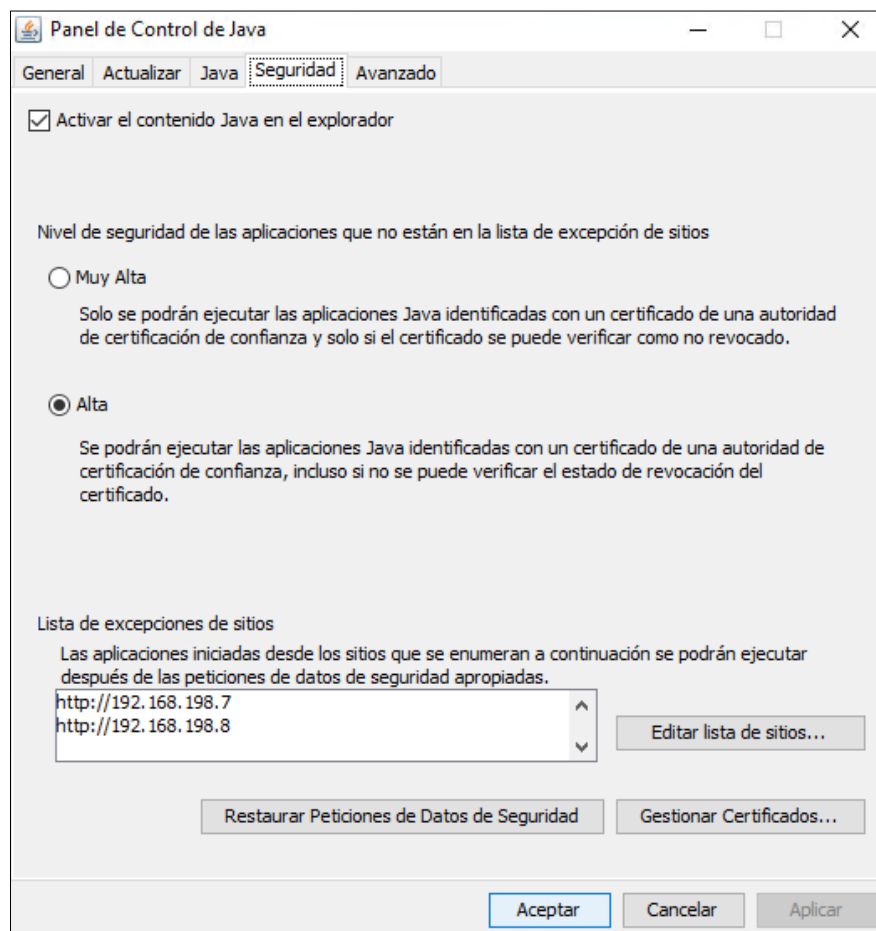


Figura 26. Panel de Control de Java

²⁵ **Java** es un lenguaje de programación multiplataforma muy popular, particularmente en aplicaciones cliente-servidor.

Al acceder con un navegador a la dirección IP de administración del conmutador y tras introducir el usuario y contraseña (VER FIGURA 27) configurados anteriormente (VER FIGURA 25) el navegador mostrará una alerta de seguridad, (a pesar de la excepción de seguridad VER FIGURA 26) y solicitará permiso para ejecutar el contenido Java, que debemos aceptar.

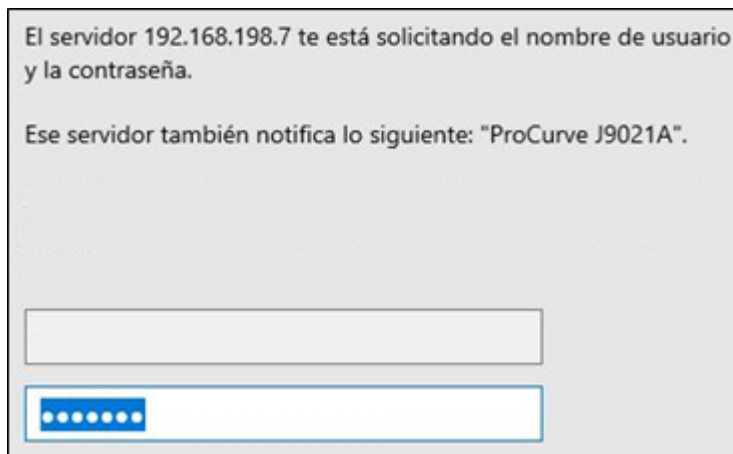


Figura 27. Usuario y contraseña

Finalmente, accedemos a la aplicación de la interfaz web y completamos la configuración. VER FIGURA 28.



Figura 28. Identidad del Switch

Inhabilitamos el tráfico del protocolo Spanning Tree²⁶ por exigencia de la autoridad de red en cada conmutador e inhabilitamos los puertos que no vamos a utilizar. VER FIGURA 29

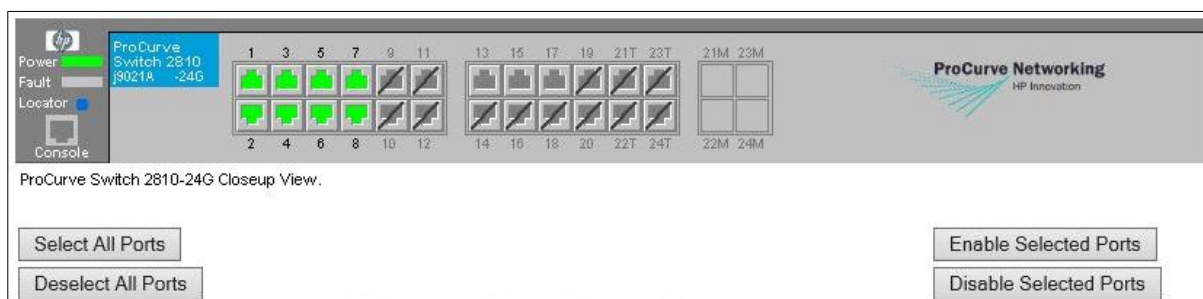


Figura 29. Configuración de puertos

²⁶ Spanning Tree (también conocido como STP es un protocolo de red de nivel de enlace cuya función es gestionar la presencia de bucles en la red.

Etiquetamos la VLAN de la red 192.168.198.0/24 para que sólo pueda usarse en el puerto 1 de cada conmutador que será el que comuniquemos a la LAN. (VER FIGURA 30) El resto de puertos los destinaremos a tráfico de datos en el interior de la infraestructura. (VER 3.3. ESQUEMA DE INTERCONEXIÓN DE DISPOSITIVOS).

Device View			Fault Detection				System Info
Port Configuration			Quality of Service				Monitor Port
Stacking			VLAN Configuration				Support/Mgmt URL
VLAN ID	VLAN Name	VLAN Type	Tagged Ports	Untagged Ports	Forbid Ports	Auto	
1	DEFAULT_VLAN (Primary)	STATIC	(STATIC) None (GVRP) None	1-24	None	None	<input type="button" value="Modify"/>
336	192.168.198	STATIC	(STATIC) 1 (GVRP) None	None	2-24	None	<input type="button" value="Modify"/>

Figura 30. Configuración de VLAN

4.1.3. Implementación del almacenamiento

La configuración de la cabina **P2000 G3 MSA** (VER 1.5.3. ALMACENAMIENTO) la llevaremos a cabo mediante una aplicación web propietaria conocida como **SMU**, siglas en inglés de Storage Management Utility (*en español: Utilidad de administración de almacenamiento*). [19]

La cabina cuenta con dos controladores y cada uno de ellos contiene un servidor web que da acceso a todas las funciones de la **SMU**, por lo que si uno no está disponible es posible continuar la administración del sistema mediante el otro. Accedemos a SMU (VER FIGURA 31) con el usuario predeterminado (*manage*) y la configuración de red establecida de fábrica. Cada controlador tiene la siguiente configuración IP predeterminada:

- Dirección IP del controlador A: 10.0.0.2
- Dirección IP del controlador B: 10.0.0.3

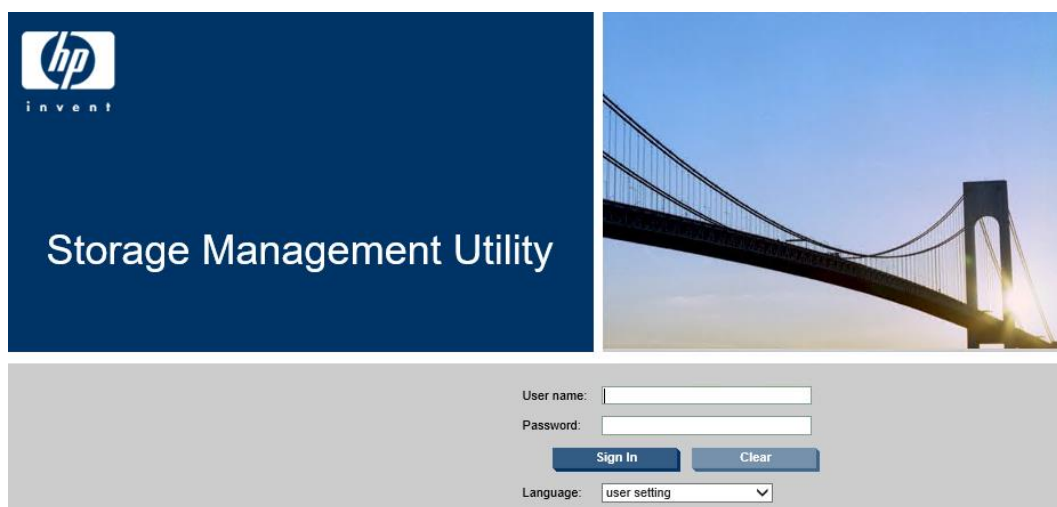


Figura 31.SMU

Para la configuración del sistema de almacenamiento, seguimos los pasos del **asistente de configuración**. [19]

Tras iniciar sesión, el siguiente paso es asegurar el sistema, cambiando las contraseñas de los usuarios predeterminados. Para ello accedemos al panel *Vista de configuración* y con el botón secundario, seleccionamos *Configuración* y a continuación *Modificar usuario*.

Es posible configurar múltiples opciones respecto de las funciones que puede realizar el usuario en la cabina de almacenamiento, pero sólo **cambiamos la contraseña**.

A continuación, cambiamos la configuración de las direcciones IP de ambas controladoras por las propuestas en nuestro diseño. VER 3.1.2. DIRECCIONAMIENTO DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN. VER FIGURA 32.

RAID Controller A		RAID Controller B	
IP address:*	192.168.198.9	IP address:*	192.168.198.10
IP mask:*	255.255.255.0	IP mask:*	255.255.255.0
Gateway:*	192.168.198.254	Gateway:*	192.168.198.254

Figura 32. Direcciones de las controladoras de la cabina P2000

Añadimos información del sistema. VER FIGURA 33.

System Name:	cabina
System Contact:	tecnicos@lcc.uma.es
System Location:	CPD 3.3.8
System Information:	Cabina discos P2000

Figura 33. Información de la cabina P2000

A continuación, se configuran los puertos de *hosts* a fin de habilitar la comunicación entre el almacenamiento y los servidores de virtualización según nuestro diseño (VER 3.3. ESQUEMA DE INTERCONEXIÓN DE DISPOSITIVOS). Para ello, establecemos las direcciones IP de los puertos iSCSI. VER FIGURA 34.

The screenshot shows a web interface for configuring host interfaces. The breadcrumb path is: *cabina (P2000 G3 iSCSI) > Configuration > System Settings > Host Interfaces*. The main heading is "Configure Host Interface" with the subtext "Modify the settings for the host interface".

Port	IP Address	Netmask	Gateway
Port A1 (iSCSI)	10.10.10.251	255.255.255.0	10.10.10.251
Port A2 (iSCSI)	10.10.10.252	255.255.255.0	10.10.10.251
Port A3 (iSCSI)	10.10.10.253	255.255.255.0	10.10.10.251
Port A4 (iSCSI)	10.10.10.254	255.255.255.0	10.10.10.251
Port B1 (iSCSI)	10.10.11.251	255.255.255.0	10.10.11.251
Port B2 (iSCSI)	10.10.11.252	255.255.255.0	10.10.11.251
Port B3 (iSCSI)	10.10.11.253	255.255.255.0	10.10.11.251
Port B4 (iSCSI)	10.10.11.254	255.255.255.0	10.10.11.251

Common Settings for iSCSI

iSCSI IP Version:	Version 4
Link Speed:	Auto

Figura 34. Direcciones iSCSI de la cabina P2000

Configuramos **fecha y hora de la cabina de almacenamiento** a partir de un servidor horario facilitado por la autoridad de la red corporativa. VER FIGURA 35.

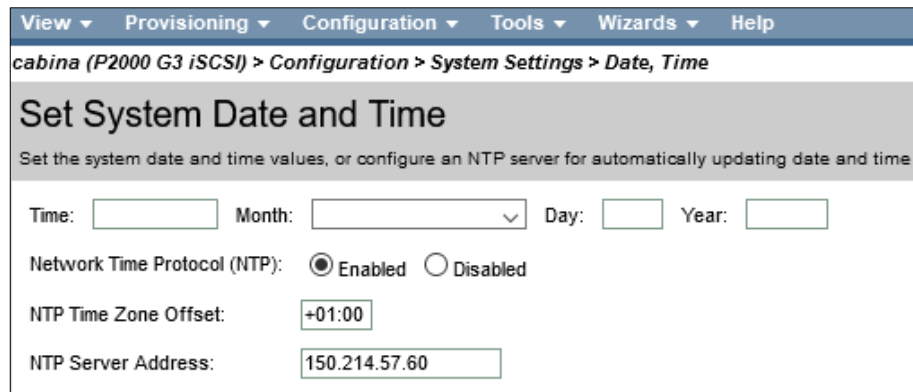


Figura 35. Date & Time de la cabina P2000

Creamos **dos discos virtuales en RAID 5** (VER FIGURA 36), cada uno compuesto por un solo volumen (VER FIGURA 37) que será el que presentemos a los *Hosts*, ya que el sistema de almacenamiento sólo presenta volúmenes a los *Hosts*, no discos virtuales.

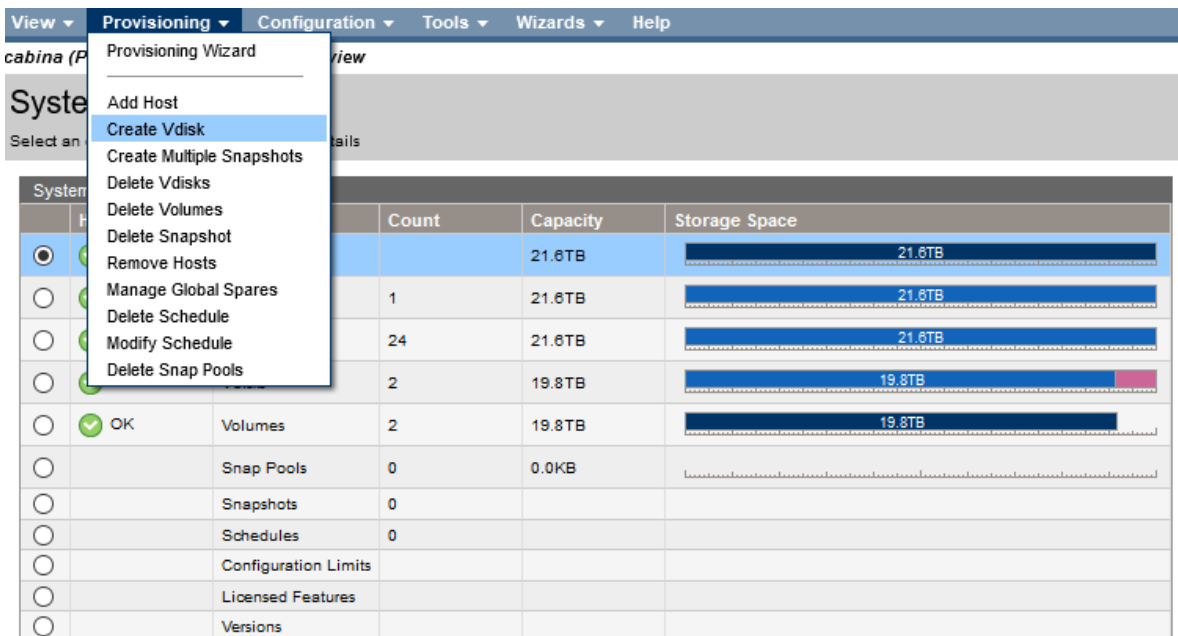


Figura 36. Vdisk de la cabina P2000

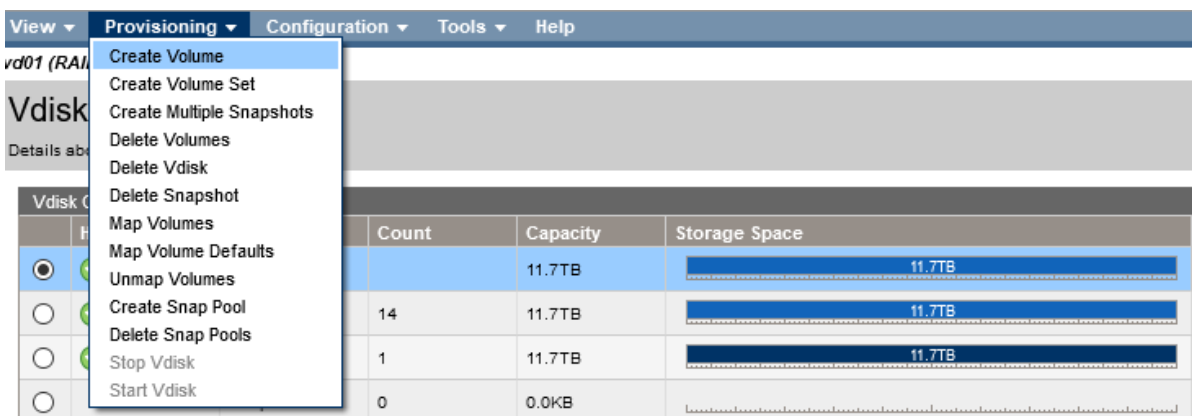


Figura 37. Volumen del Vdisk 1

Como resultado, obtenemos un volumen de **11,6TB** en el disco virtual 1 y otro de casi **8TB** en el disco virtual 2. VER FIGURA 38.

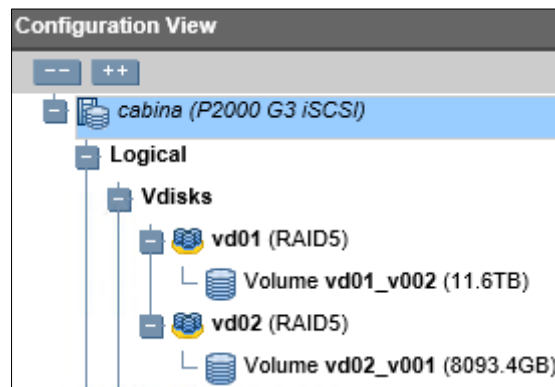


Figura 38. Vdisk & Volumes en la cabina P2000

Finalmente, **verificamos** todas las configuraciones anteriores, asignación de los discos y que todos los puertos iSCSI están levantados. VER FIGURA 39.

Enclosure Overview

Details about a specific enclosure and contained components. Select a component from the front or rear to view the details.

Select the front or rear view of the enclosure and select an item to display properties:

Front Graphical | Front Tabular | Rear Graphical | Rear Tabular

Front Graphical | Front Tabular | Rear Graphical | Rear Tabular

Enclosures Rear View						
	Health	Name	Type	Location	Serial Number	Status
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Enclosure-1	Enclosure	-	500c0ff0150ace3c	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Controller-A	Controller	Enclosure-1 - Top	CN8227M474	Operational
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Controller-A Network Port	Network Port	Controller-A	00:c0:ff:15:11:e1	
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-A1	iSCSI Port	Controller-A	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-A2	iSCSI Port	Controller-A	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-A3	iSCSI Port	Controller-A	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-A4	iSCSI Port	Controller-A	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input type="checkbox"/> N/A	Controller-A Out Port	Expansion Port	Controller-A	-	Disconnected
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Controller A CompactFlash	CompactFlash	Controller-A	-	Installed
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Controller-B	Controller	Enclosure-1 - Bottom	CN8227M494	Operational
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Controller-B Network Port	Network Port	Controller-B	00:c0:ff:15:11:b5	
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-B1	iSCSI Port	Controller-B	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-B2	iSCSI Port	Controller-B	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-B3	iSCSI Port	Controller-B	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Port-B4	iSCSI Port	Controller-B	iqn.1986-03.com.hp:storage.p2000g3.1224150ace	Up
<input type="radio"/>	<input type="checkbox"/> N/A	Controller-B Out Port	Expansion Port	Controller-B	-	Disconnected
<input type="radio"/>	<input checked="" type="checkbox"/> OK	Controller B CompactFlash	CompactFlash	Controller-B	-	Installed
<input type="radio"/>	<input checked="" type="checkbox"/> OK	PSU 1, Left	Power Supply	Enclosure 1 - Left	CN8224T553	Up
<input type="radio"/>	<input checked="" type="checkbox"/> OK	PSU 2, Right	Power Supply	Enclosure 1 - Right	CN8224T554	Up

Figura 39. Salud de la cabina P2000

4.1.4. Implementación de VMware vSphere (ESXi)

4.1.4.1. Instalación del software ESXi

Encendemos uno de los servidores (VER 1.5.1. SERVIDORES), tras las opciones de configuración de BIOS e iLO, iniciamos HP **Smart Array Utility**²⁷ (pulsando **F8**) y seguimos los pasos del asistente para crear una unidad lógica en **RAID 1** (espejo) con los dos discos de 300GB con los que cuenta el equipo. VER FIGURA 40.



Figura 40. Menú Principal HP Smart Array

Introducimos el instalador de VMware ESXi 6.5 en el lector de DVD y comienza la carga de archivos en memoria para realizar la instalación.

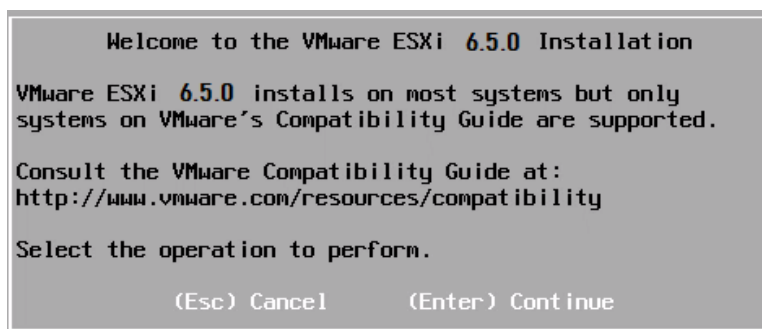


Figura 41. VMware ESXi 6.5.0 Installer

A continuación, aceptamos los términos de licencia de VMware (pulsando **F11**); el instalador detecta la unidad de 300GB creada anteriormente, la cual seleccionamos, y, tras la elección de idioma, introducimos una contraseña para el root (VER FIGURA 42). Confirmamos y comienza la instalación de archivos en la unidad.



Figura 42. root password para ESXi

²⁷ Utilidad de HP que incorpora controladores y utilidades para crear y gestionar diferentes Arrays de discos.

4.1.4.2. Configuración básica de ESXi

Finalizada la instalación de archivos, se produce un reinicio y se presenta una pantalla como la de la FIGURA 43 donde accederemos, pulsando **F2** e introduciendo la contraseña de root (VER FIGURA 42), para realizar la configuración.

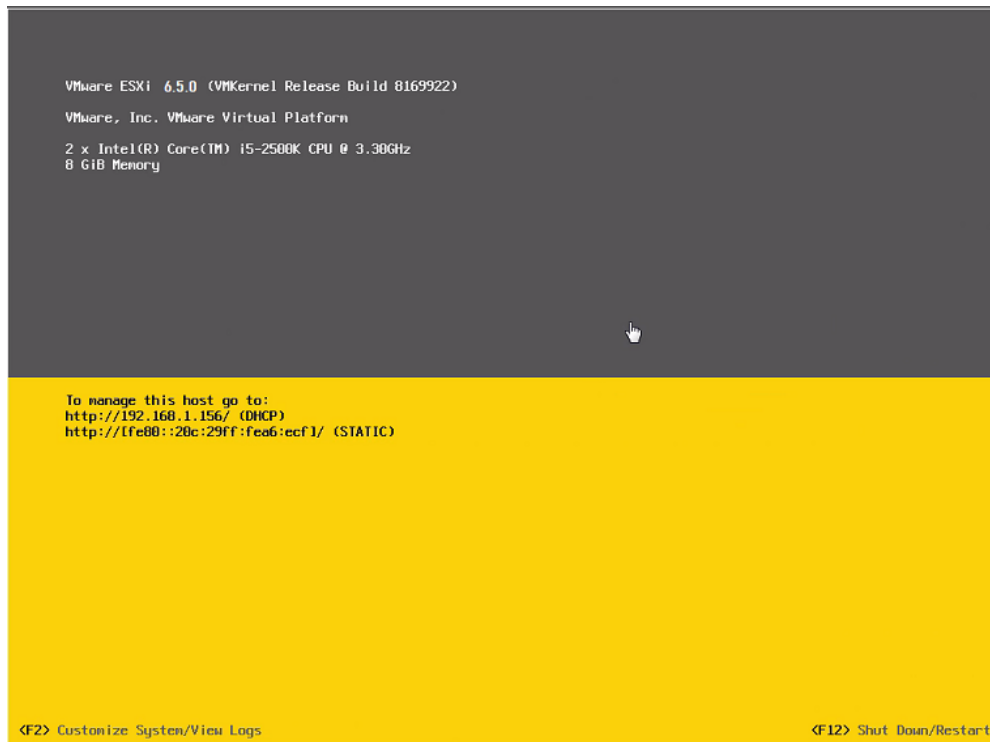


Figura 43. Consola de ESXi

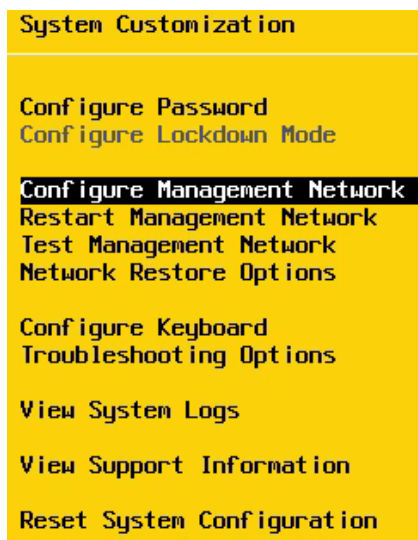


Figura 44. System Customization de ESXi

En el menú principal (VER FIGURA 44), entramos en **Configure Management Network** para configurar la red IPv4 según nuestro diseño (VER 3.1.2. DIRECCIONAMIENTO DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN), inhabilitar la red IPv6, configurar el servidor de DNS, añadir nuestro sufijo de DNS e introducir el **identificador de la VLAN** de la red 192.168.198.0/24.

Este último paso es necesario, ya que hemos solicitado a la autoridad de red que los puntos de red donde vamos a conectar nuestros *Hosts* tengan acceso en **modo TRUNK** lo que nos permitirá gestionar máquinas virtuales en varias VLAN. Si no introdujéramos el identificador de VLAN nos quedaríamos sin acceso por red.

Aplicamos los cambios y reiniciamos el *Host* (necesario por inhabilitar IPv6) y ya es posible acceder mediante el **Web Client** (VER FIGURA 45) o mediante la aplicación **VMware vSphere Client** (VER FIGURA 46), aunque algunas funcionalidades incorporadas a partir de la versión 6 de vSphere sólo están disponibles en **Web Client**).

Análisis, diseño e implantación de un sistema de virtualización con VMWARE en un entorno docente educativo de grado medio

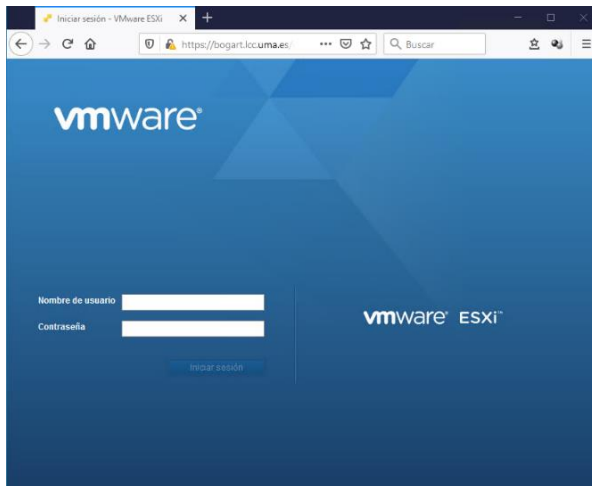


Figura 45. vSphere Web Client



Figura 46. vSphere Client

Accedemos mediante **VMware vSphere Client** (VER FIGURA 47) para configurar las diferentes redes e incorporar el almacenamiento. La elección de la aplicación cliente frente al cliente web es sólo una cuestión de gusto ya que, para las tareas que vamos a realizar, ambos son igualmente válidos.

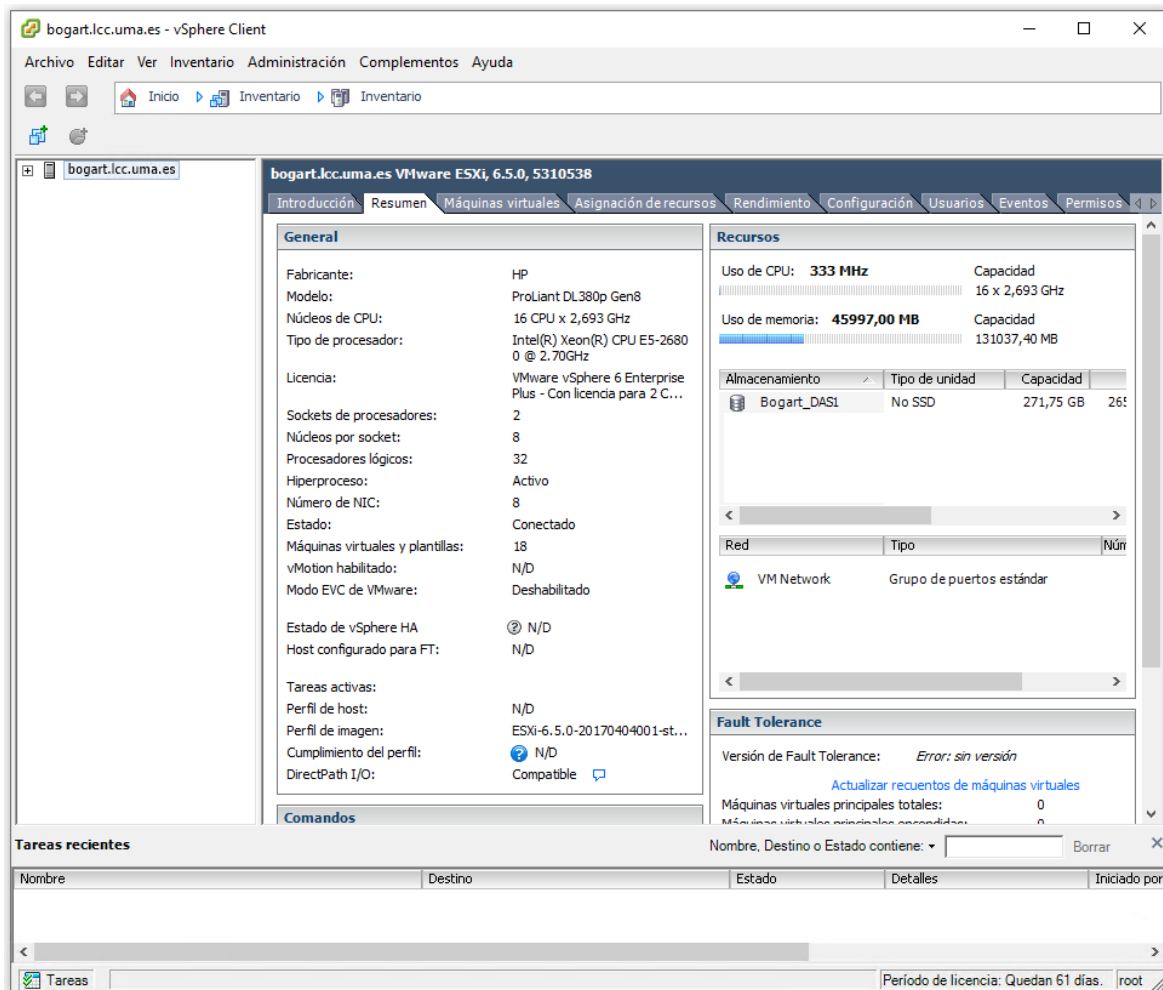


Figura 47. Resumen del Host

4.1.4.3. Configuración de red en ESXi

Realizamos una agregación de enlace con un segundo NIC (VER 3.3. ESQUEMA DE INTERCONEXIÓN DE DISPOSITIVOS) añadiendo un segundo adaptador de red al conmutador estándar **vSwitch0**. Seleccionamos la pestaña *Configuración => Redes* (VER FIGURA 48. REDES ESXi) y a continuación, clic en *Propiedades*.

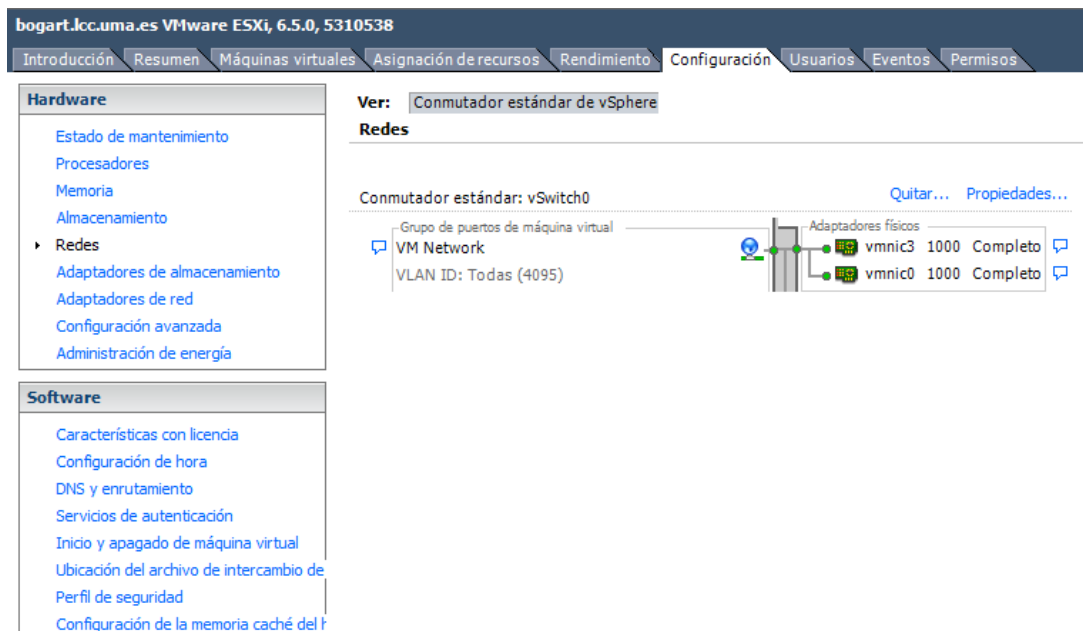


Figura 48. Redes ESXi

En la ventana de *Propiedades de vSwitch0*, pestaña *Adaptadores de red*, clic en *Agregar* y seleccionamos *vmnic3*. VER FIGURA 49. AGREGACIÓN DE ENLACE ESXi.

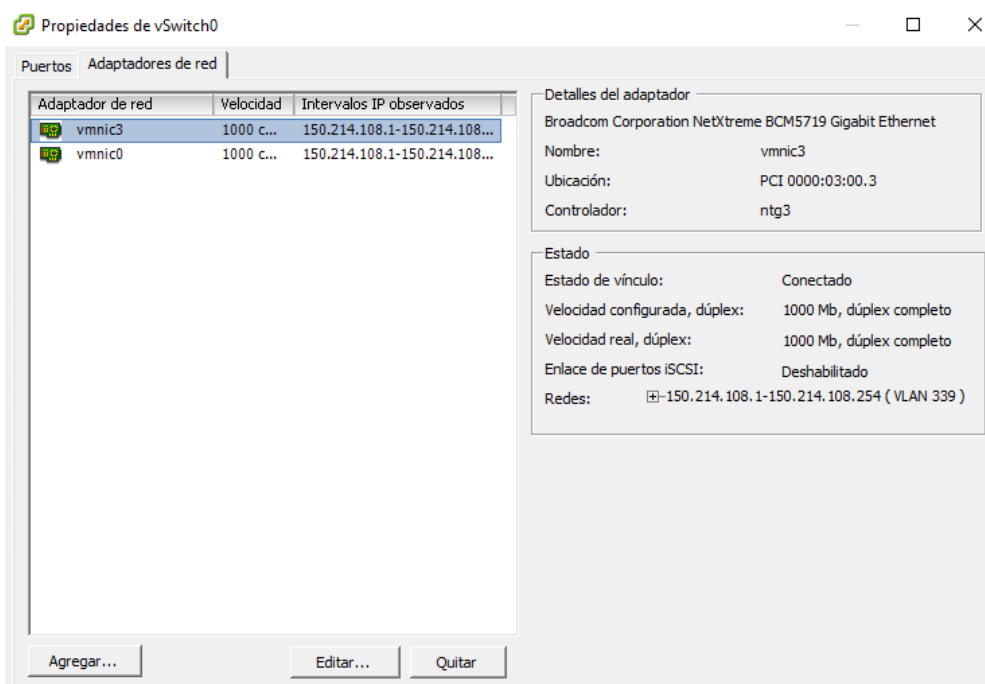


Figura 49. Agregación de enlace ESXi

A continuación, añadimos los identificadores de las VLAN que hemos solicitado a la autoridad de red que incluyan en los puntos de red en modo TRUNK.

Seleccionamos la pestaña *Configuración => Redes* (VER FIGURA 48. REDES ESXi) y a continuación, clic en *Propiedades*.

En la ventana de *Propiedades de vSwitch0*, pestaña *Puertos*, clic en *Agregar* y agregamos las siguientes etiquetas: VER FIGURA 50, FIGURA 51 Y FIGURA 52.

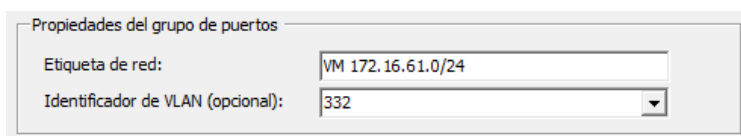


Figura 50. VLAN 332 en ESXi

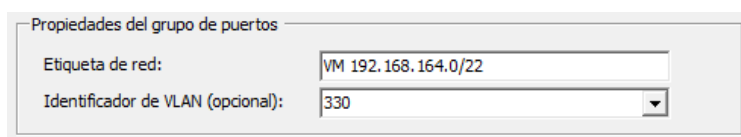


Figura 51. VLAN 330 en ESXi

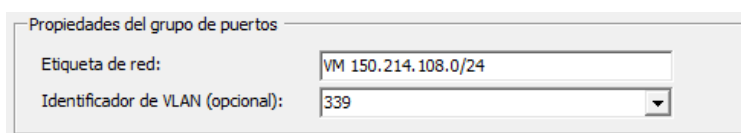


Figura 52. VLAN 339 en ESXi

Una vez incorporadas las VLAN de las subredes y realizada la agregación de enlace de red, el resultado es el de la FIGURA 53.

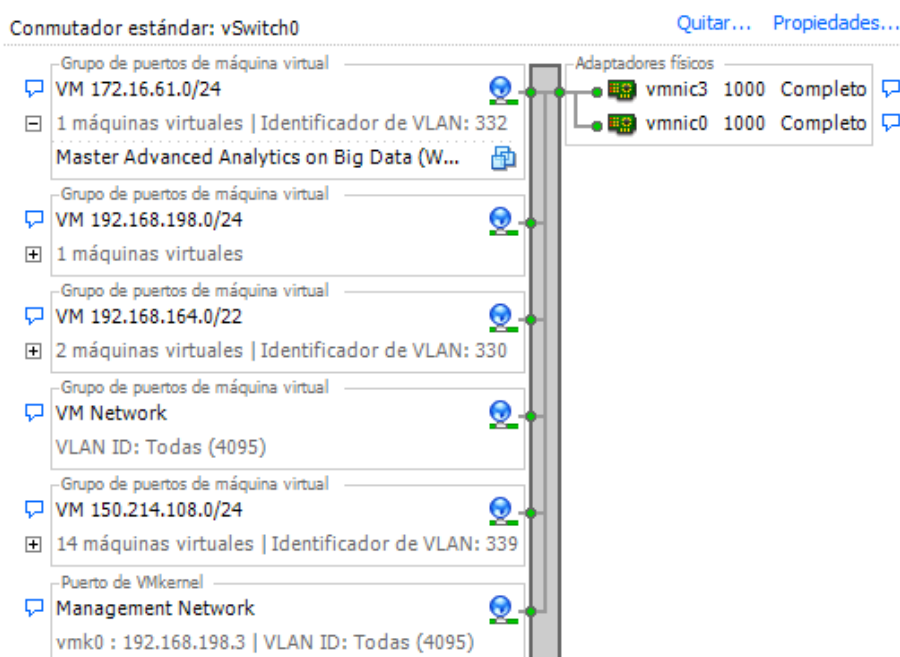


Figura 53. Redes en vSwitch0 de ESXi

4.1.4.4. Configuración iSCSI en ESXi

Dedicaremos dos NIC de cada *Host* a la conexión iSCSI por diferentes rutas, teniendo en cuenta que las NIC físicas deben estar en la misma subred que el sistema de almacenamiento iSCSI al que se conectan. VER 3.3. ESQUEMA DE INTERCONEXIÓN DE DISPOSITIVOS.

Para conectar ambas NIC necesitamos añadir un **adaptador iSCSI de Software** en la pestaña *Configuración* => *Adaptadores de almacenamiento*, clic en *Agregar* y a continuación, seleccionamos **Software iSCSI Adapter**.

El adaptador de iSCSI y las NIC físicas se conectarán a través de un adaptador de red virtual o puerto VMkernel, por lo que crearemos un adaptador VMkernel (*vmk*) en un conmutador de vSphere (*vSwitch*) con una asignación 1:1 entre cada adaptador de red físico y virtual. VER FIGURA 54.

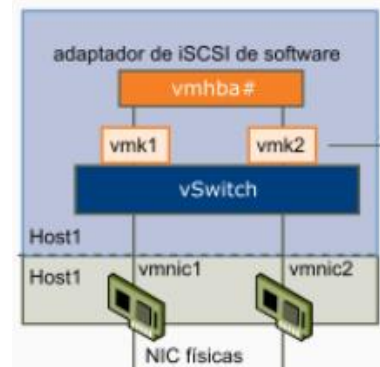


Figura 54. Esquema iSCSI en ESXi

Para lograr la asignación 1:1 con dos NIC agregaremos cada uno a un adaptador VMkernel diferente, y ambos a un solo conmutador estándar de vSphere. Es importante comprobar que cada adaptador VMkernel se asigna a solo un adaptador físico activo que le corresponde.

Seleccionamos la pestaña *Configuración* => *Redes* => *Agregar redes* => seleccionamos VMkernel (lo llamaremos *iSCSI1*) y a continuación, el adaptador *vmnic1*. A continuación, dentro del nuevo *vSwitch* que acabamos de crear, clic en el botón **Agregar**, de nuevo escogemos *VMkernel* (lo llamaremos *iSCSI2*) y a seleccionamos el otro adaptador, *vmnic2*. VER FIGURA 55.

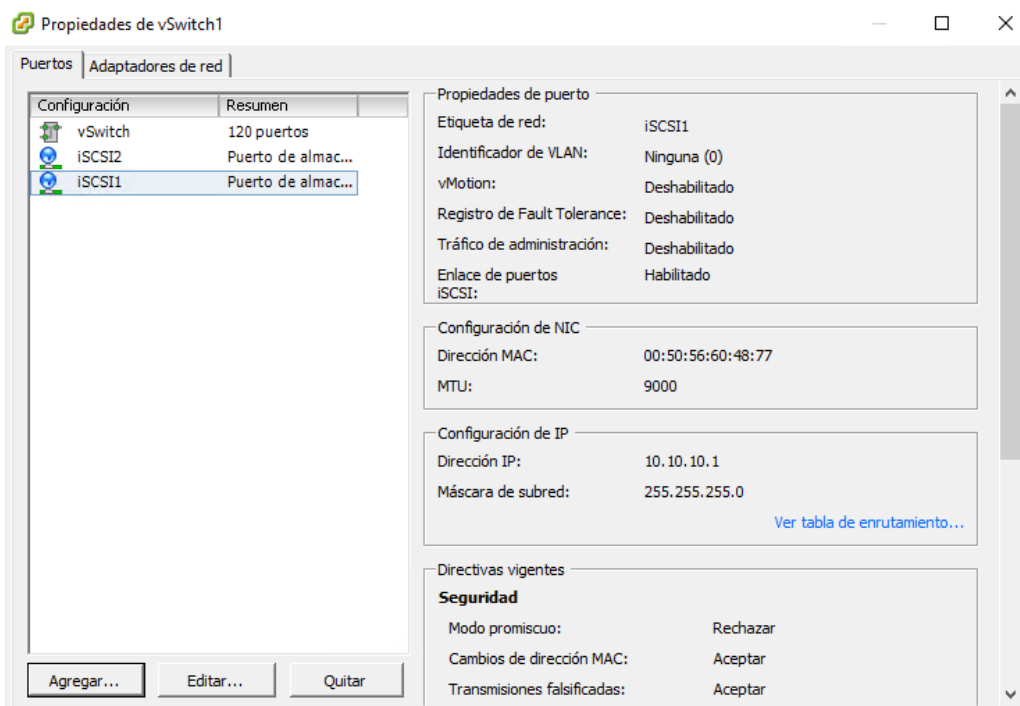


Figura 55. Propiedades de vSwitch1

Editar *iSCSI1* y, en la ventana de *Propiedades*, pestaña *Configuración de IP*, aplicamos la configuración de la FIGURA 56.

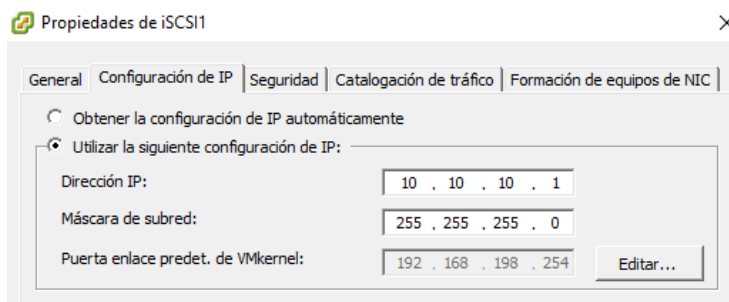


Figura 56. Configuración de red *iSCSI1*

Seleccionamos la pestaña *Formación de equipos de NIC*, aplicamos la configuración de la FIGURA 57 para que cada adaptador de red utilice un VMkernel diferente.

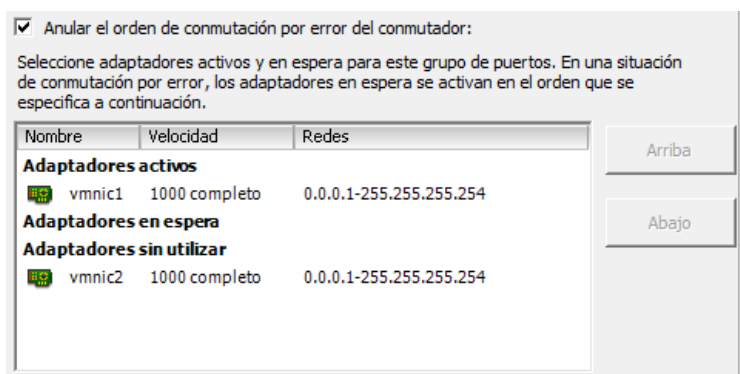


Figura 57. Orden de conmutación de los adaptadores para *iSCSI1*

De forma análoga, clic en *Editar iSCSI2* y, en la ventana de *Propiedades*, pestaña **Configuración de IP**, aplicamos la configuración de la FIGURA 58.

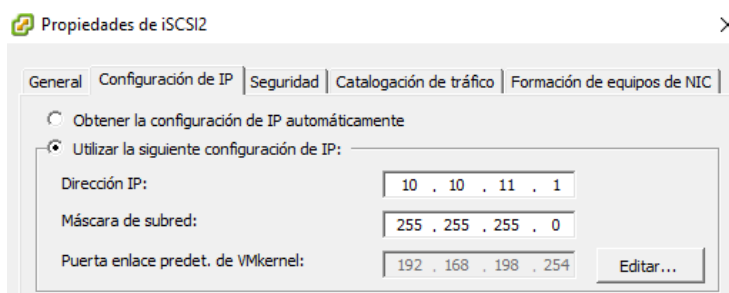


Figura 58. Configuración de red para *iSCSI2*

De nuevo, en la pestaña *Formación de equipos de NIC*, aplicamos la configuración de la FIGURA 59 para que cada adaptador de red utilice un VMkernel diferente.

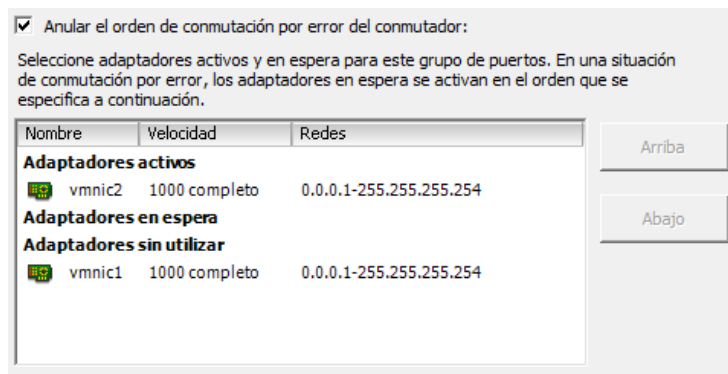


Figura 59. Orden de conmutación de los adaptadores para iSCSI2

Volvemos a *Configuración* => Adaptadores de almacenamiento, seleccionamos el **adaptador software iSCSI**, clic con el botón derecho del ratón y accedemos a las *propiedades*.

Seleccionamos la pestaña *Configuración de red* y añadimos los dos VMKernel (*iSCSI1* e *iSCSI2*). VER FIGURA 60.

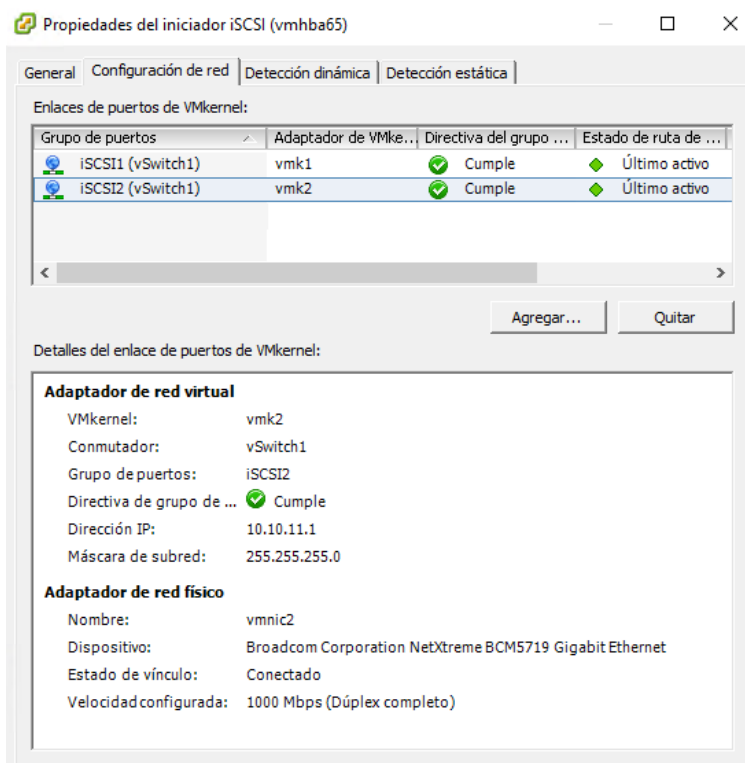


Figura 60. Grupo de puertos iSCSI

A continuación, en la Pestaña *Detección dinámica*, añadimos las direcciones IP de las controladoras iSCSI de la cabina de almacenamiento. VER 3.3. ESQUEMA DE INTERCONEXIÓN DE DISPOSITIVOS Y FIGURA 61.

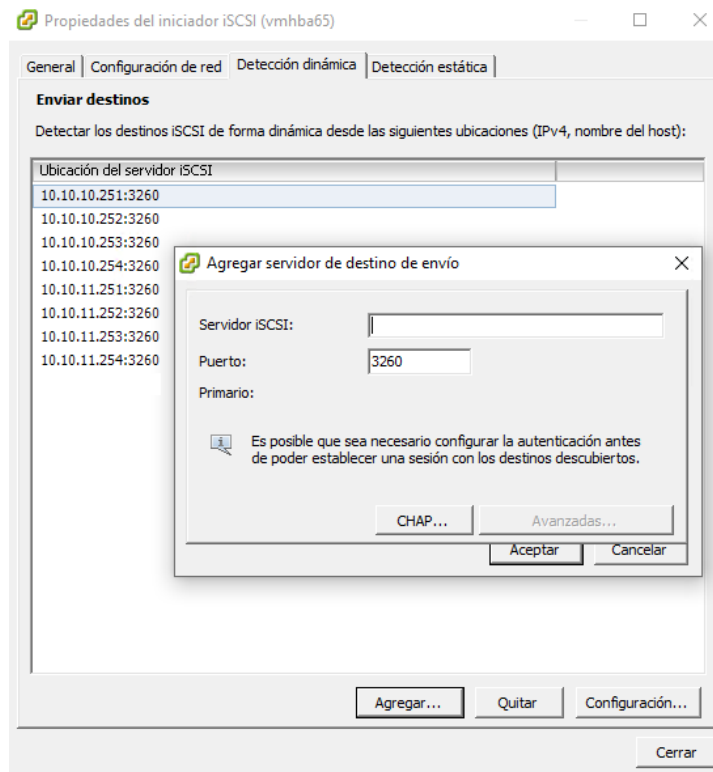


Figura 61. Detección dinámica del servidor iSCSI

Clic en **Reescanear todos** y si todo está bien configurado montará los LUN que referencian los dos volúmenes de la cabina de almacenamiento. VER FIGURA 62.

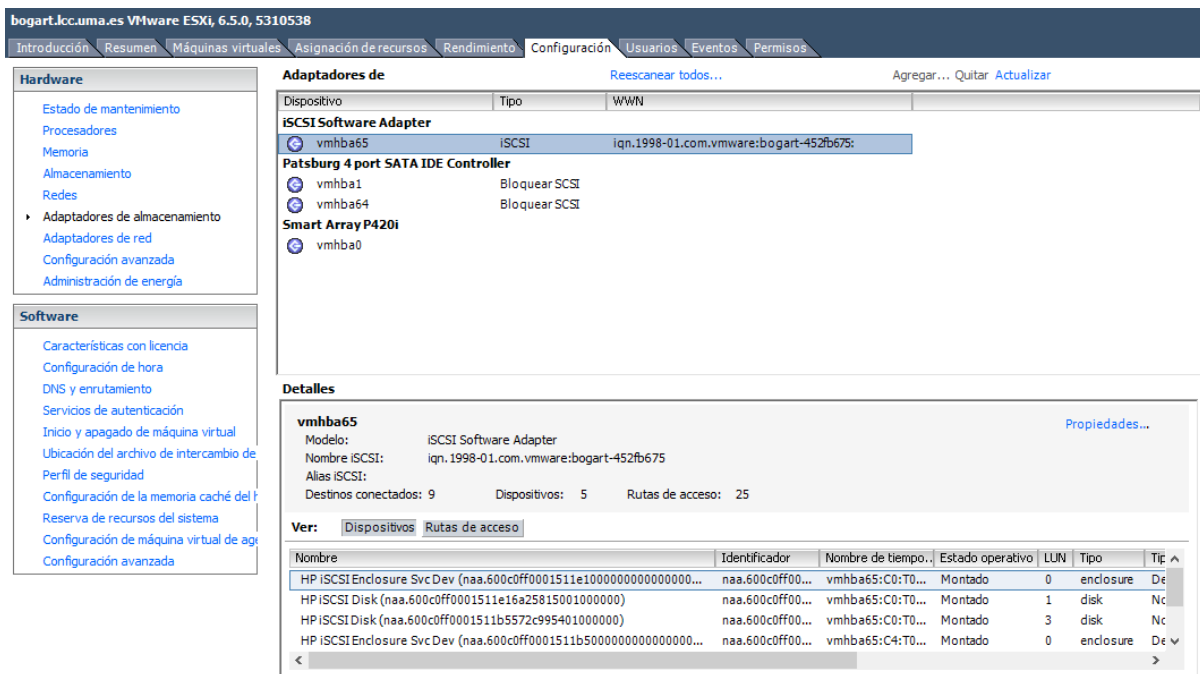


Figura 62. Identificación de LUN

Finalmente, crearemos el sistema de archivos en el almacenamiento y lo incorporaremos al inventario de almacenes de datos. Pestaña *Configuración* => *Almacenamiento* => *Agregar*

almacenamiento y seguir el asistente para la creación del sistema de archivos VMFS que finaliza con la creación de un almacén de datos que llamaremos **Datastore_01**. VER FIGURA 63.

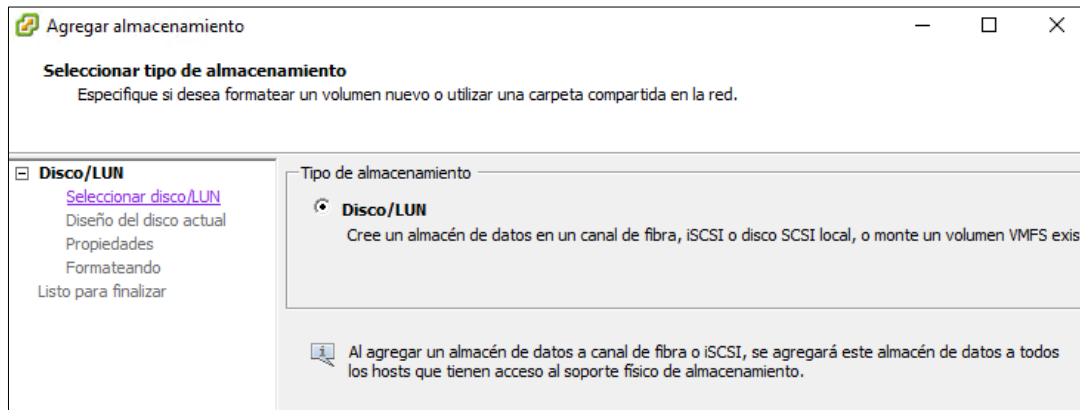


Figura 63. Creación de DataStore

Repetir el procedimiento anterior para crear el almacén de datos **Datastore_02** sobre el segundo volumen de la cabina de almacenamiento.

Como resultado final, tenemos disponibles tres almacenes de datos (VER 1.4.2. CONCEPTOS DE ALMACENAMIENTO): DataStore_01 y DataStore_02 de la cabina de almacenamiento y Bogart_DAS1 del propio servidor. VER FIGURA 64.

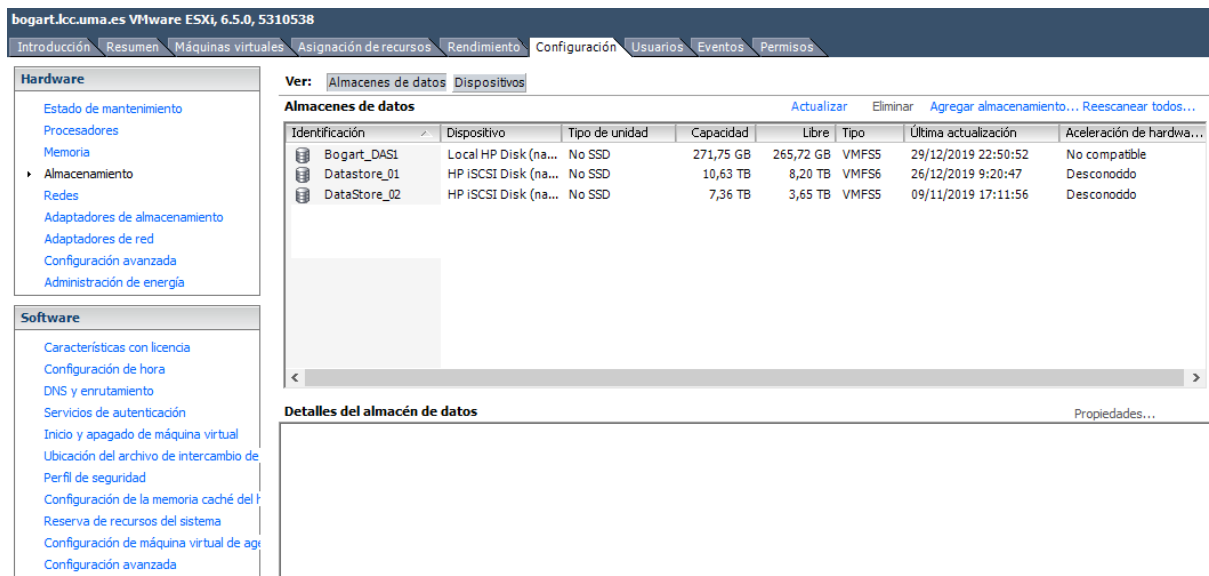


Figura 64. Datastore_01 y Datastore_02

Antes de instalar y configurar el segundo realizaremos la implementación de *VMware vCenter Server* (VER FIGURA 5) y añadiremos el *Host* que acabamos de instalar y configurar.

4.1.5. Implementación de VMware vCenter Server

Introducimos el CD de instalación VMware **VCSA** (*siglas en inglés de Virtual Center Server Appliance*) en un equipo de trabajo. Encontraremos la carpeta `vcsa-ui-installer` donde seleccionamos la carpeta del sistema operativo desde el que realizamos la instalación; en

nuestro caso win32 y ejecutamos installer.exe. A continuación, seleccionamos “Install a new vCenter Server Appliance or Platform Services Controller Appliance” ya que se trata de una nueva instalación.

La instalación consta de dos etapas: Deploy y Setup. Es decir, una para el despliegue de la aplicación (Deploy) y otra para la configuración (Setup). Tras aceptar los términos de licencia comienza la primera etapa.

4.1.5.1 Despliegue de vCenter

La primera decisión importante es seleccionar el tipo de despliegue que queremos realizar.

En nuestro caso (un entorno pequeño) optaremos por una instalación independiente que contendrá su propio dominio. VER FIGURA 65.

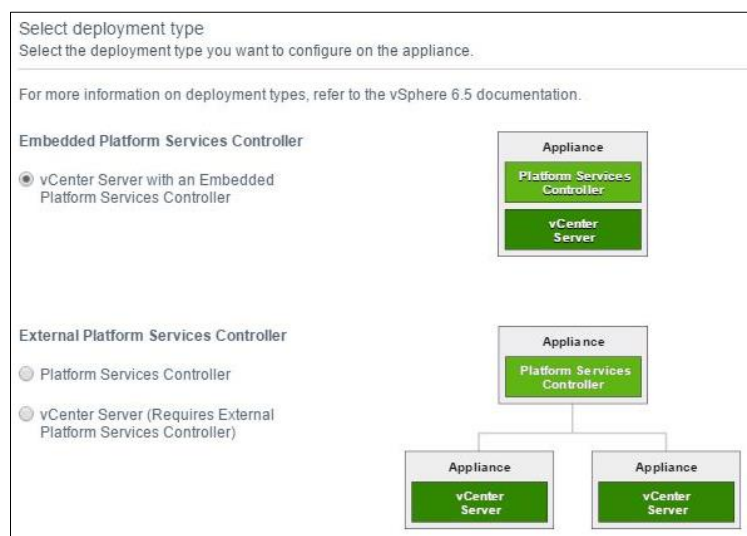


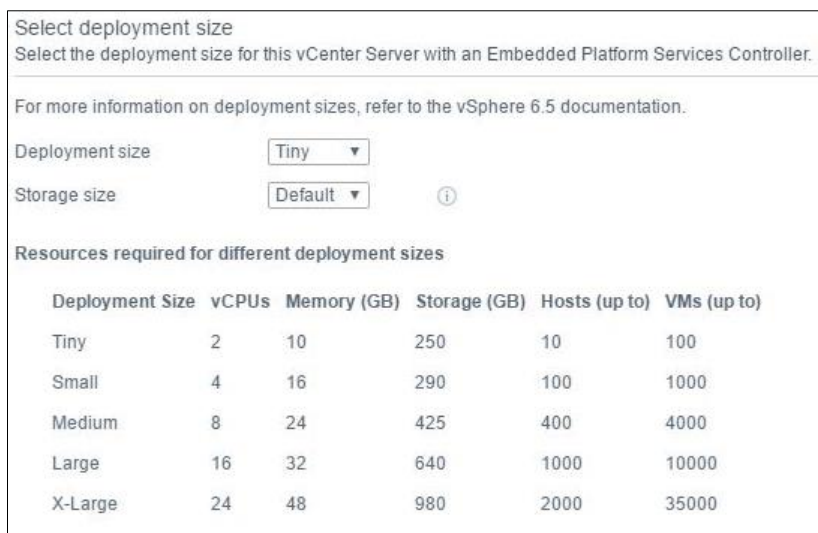
Figura 65. Tipo de despliegue de vCenter

A continuación, indicaremos los datos de conexión del servidor ESXi (VER FIGURA 66) objetivo del despliegue de la máquina virtual que contendrá el vCenter Server. En nuestro caso el Host que acabamos de instalar (VER 4.1.4. IMPLEMENTACIÓN DE VMWARE VSPHERE (ESXi)). También indicaremos el nombre de la máquina virtual y la contraseña de root.

Appliance deployment target	
Specify the appliance deployment target settings. The target is the ESXi host or vCenter Server instance on which the appliance will be deployed.	
ESXi host or vCenter Server name	<input type="text" value="FQDN or IP Address"/> ⓘ
HTTPS port	<input type="text" value="443"/>
User name	<input type="text" value="root or UserName@DomainName"/> ⓘ
Password	<input type="password"/>

Figura 66. Datos de conexión para Deploy de vCenter

En el siguiente paso debemos indicar el tamaño de la infraestructura de virtualización para la que estamos desplegando un vCenter. Para ello, contamos con una tabla de diferentes dimensionamientos de **VCSA** (VER FIGURA 67). En el departamento hemos seleccionamos **Small** (*en inglés: pequeño*) con el almacenamiento por defecto dado que podrían alcanzarse más de 100 máquinas virtuales. En la implementación para un entorno docente educativo de grado medio sería suficiente con el tamaño de despliegue **Tiny** (*en inglés: minúsculo*). VER FIGURA 67.



Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	10	250	10	100
Small	4	16	290	100	1000
Medium	8	24	425	400	4000
Large	16	32	640	1000	10000
X-Large	24	48	980	2000	35000

Figura 67. Selección del tamaño de instalación de vCenter.

Una vez seleccionados el *Host* de destino y el tamaño de despliegue, debemos seleccionar el almacenamiento en el que generar el despliegue y el tipo de aprovisionamiento: **thin** o **thick**.

El **aprovisionamiento thick** asigna previamente en el almacenamiento físico la cantidad completa de la capacidad de almacenamiento del disco virtual mientras que el **aprovisionamiento thin** consume solo el espacio que necesita inicialmente y crece bajo demanda con el tiempo. Tomamos la opción por defecto para instalaciones de VCSA: **thick**.

A continuación, la configuración de red. Muy importante que el *FQDN*²⁸ del sistema esté dado de alta en el DNS de la organización con la dirección IP que vayamos a asignarle.

Finalmente, se realiza el despliegue, que puede llevar varios minutos. Una vez finalizada la primera etapa (VER FIGURA 68), ya podríamos ir al puerto 5480 de la *FQDN* de vCenter para realizar algunas gestiones como *root*.

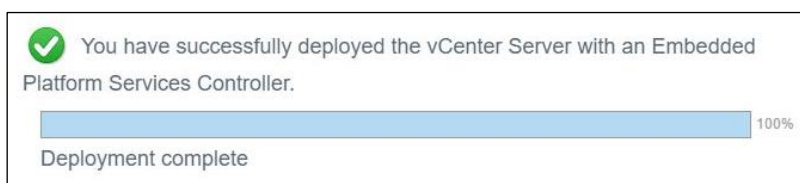


Figura 68. Despliegue de vCenter completo

²⁸ **FQDN** son las siglas en inglés de *Fully Qualified Domain Name* (en español: Nombre cualificado de dominio completo)

4.1.5.2. Configuración de vCenter

Comienza la 2ª etapa, la configuración de *vCenter Server Appliance* con *Platform Service Controller* embebido. En el primer paso, sincronizamos la hora con el *Host* (podríamos haber sincronizado con algún servidor horario) y dejamos inhabilitado el acceso por **SSH**.

Appliance configuration	
Time synchronization mode	Synchronize time with the ESXi host ▼
SSH access	Disabled ▼

Figura 69. Configuración horaria de vCenter

A continuación, si tuviéramos un dominio **SSO**²⁹ ahora sería el momento de ponerlo. Como no lo tenemos, creamos una configuración para *Single-Sign-on*. VER FIGURA 70.

SSO configuration	
Single Sign-On domain name	lcc.local ⓘ
Single Sign-On user name	administrator
Single Sign-On password ⓘ
Confirm password
Site name	Vcenter ⓘ

Figura 70. Dominio SSO para vCenter

Finalmente, tras preguntar si queremos unirnos al programa de mejora de VMware, comienza el proceso de configuración del *VCSA* que también puede llevar varios minutos. Una vez finalizado, es posible acceder a la aplicación web, por IP o por *FQDN*, donde encontraremos dos modos de acceso: mediante **Flash** o mediante **HTML5**. VER FIGURA 71.



Figura 71. Modos de acceso Web a vCenter

²⁹ **SSO** son las siglas en inglés de **Single Sign-On**. Se trata de un servicio de autenticación que permite al usuario identificarse una sola vez para acceder a múltiples aplicaciones.

4.1.6. Administración de los ESXi con vCenter Server

La interfaz web de vCenter Server ya está funcionando, sólo queda construir la organización del sistema virtual y agregar los *Hosts*.

Seleccionamos el acceso **HTML5**, introducimos las credenciales configuradas para SSO (VER FIGURA 70) y accedemos a la interfaz de administración.

Para que nuestra organización virtual sea un reflejo de nuestra organización real en el departamento, creamos un **Nuevo centro de datos**, con el menú de contexto del botón derecho y lo llamamos **CPD_338**, dado que nuestro CPD³⁰ se encuentra en las dependencias del laboratorio 338. VER FIGURA 72.

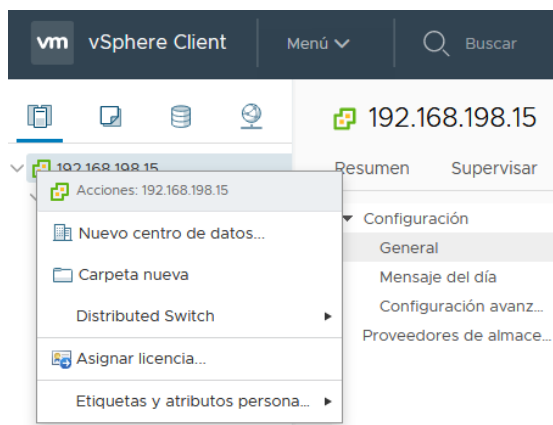


Figura 72. Nuevo Centro de datos en vCenter

A continuación, con el botón derecho sobre **CPD_338**, seleccionamos **Agregar host** en el menú de contexto y seguimos el asistente. (VER FIGURA 73) Tendremos que introducir los datos de conexión y las credenciales del *Host* que hemos instalado en el APARTADO 4.1.4.

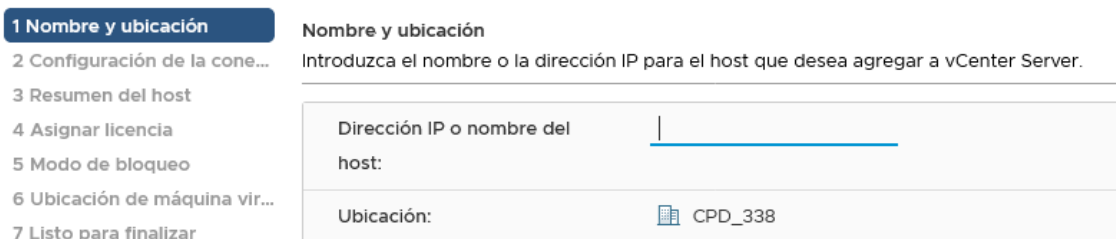


Figura 73. Agregar host a vCenter

Una vez integrado el primer *Host*, todos sus recursos están disponibles a través de vCenter, es decir que tanto las redes que definimos en el APARTADO 4.1.4.3 como el almacenamiento configurado en el APARTADO 4.1.4.4. VER FIGURA 74.

³⁰ CPD son las siglas de Centro de Proceso de Datos (también conocido como Centro de cálculo) y hace referencia al espacio donde se concentran los recursos computacionales y de comunicación de una organización.

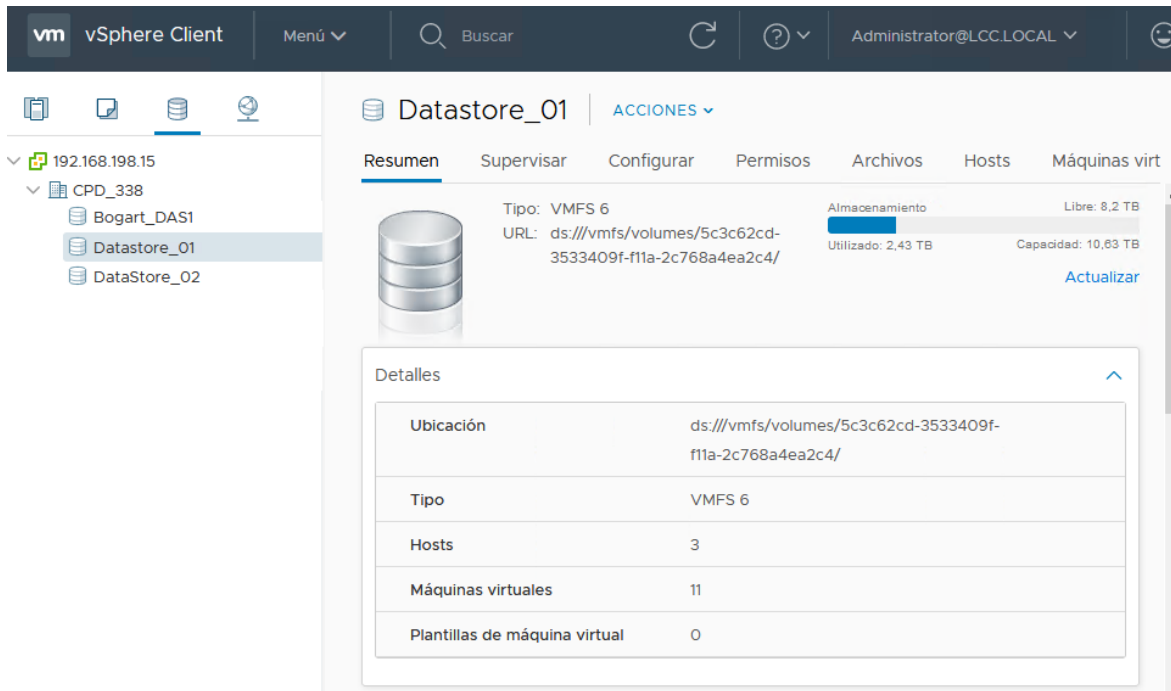


Figura 74. Almacenamiento en vCenter

Respecto al segundo *Host* seguiremos los mismos pasos que para la instalación del primero, pero cambiando ligeramente el orden: Instalación del software (VER APARTADO 4.1.4.1) y configuración básica (VER APARTADO 4.1.4.2).

A continuación, lo añadiremos al vCenter y seguiremos con la configuración de red (VER APARTADO 4.1.4.3) y la configuración *iSCSI* (VER APARTADO 4.1.4.4), teniendo en cuenta que los almacenes de datos no necesitarán ser formateados porque ya contendrán un sistema de archivos **VMFS**.

Una vez integrados ambos *Hosts*, a los que hemos llamado *Bogart* y *Bacall* (VER 3.2. ESQUEMA CONCEPTUAL DE LA INFRAESTRUCTURA DE VIRTUALIZACIÓN), tenemos disponibles en única consola los recursos de ambos. VER FIGURA 75.

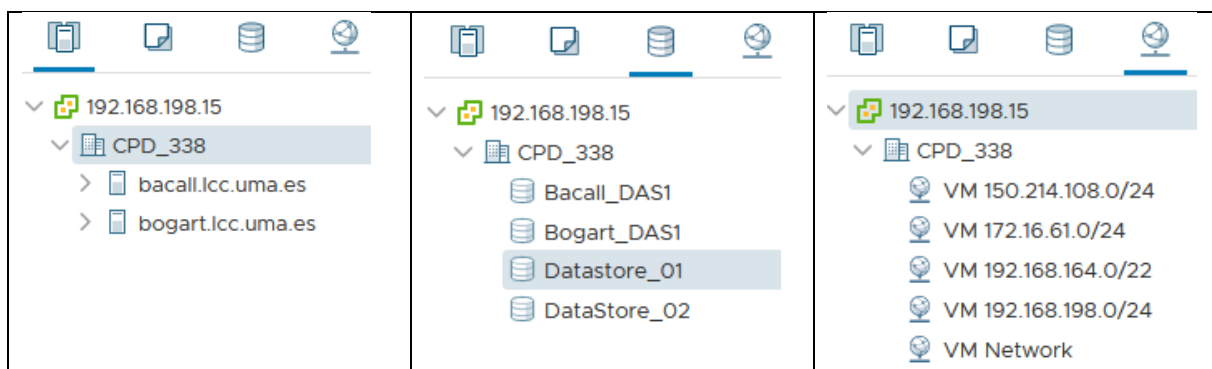


Figura 75. Hosts, Almacenamiento y Redes disponibles en vCenter

4.2. Instalación y configuración de servicios y aplicaciones

En este apartado trataremos la instalación y configuración de los servicios y aplicaciones propuestos en el **Análisis**. VER APARTADO 2.1.3.

4.2.1. Servidor de DHCP

Ya existe en nuestro escenario docente un servidor DHCP en producción que cumple con los requerimientos de nuestro **Diseño** (VER 3.5. SERVICIOS BÁSICOS PARA LA DOCENCIA) por lo que nuestra **Implementación** consistirá en su conversión de físico a virtual con objeto de mostrar el funcionamiento de **vmWare Converter** (VER 1.3.1. SOFTWARE DE VMWARE). VER FIGURA 76.

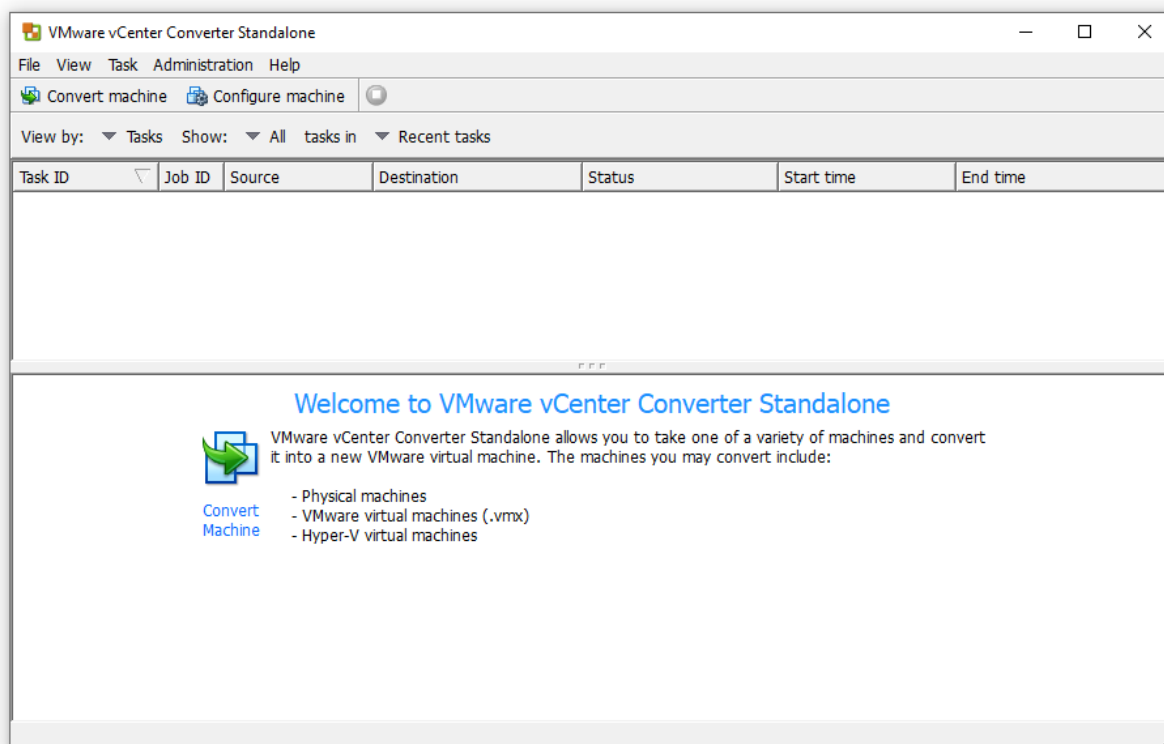


Figura 76. Pantalla principal de VMware Converter

Hacemos clic en el botón **Convert machine**, especificamos que el equipo *Fuente* está en producción y los datos de conexión. VER FIGURA 77.

Select source type: Powered on Powered off

Remote Linux machine

Convert any powered on physical or virtual Linux machine.

Specify the powered on machine

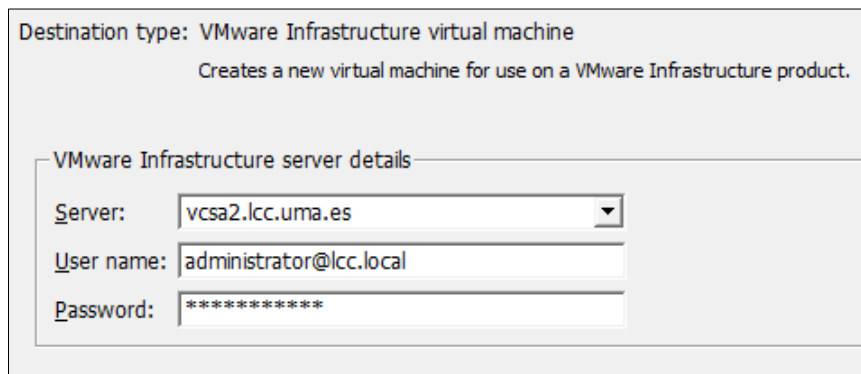
IP address or name: 192.168.166.204

User name: root

Password: *****

Figura 77. Datos de conexión del equipo Fuente

A continuación, los datos de conexión de la infraestructura de virtualización de destino. En nuestro caso, los datos de conexión del *vCenter*. VER FIGURA 78.



Destination type: VMware Infrastructure virtual machine
Creates a new virtual machine for use on a VMware Infrastructure product.

VMware Infrastructure server details

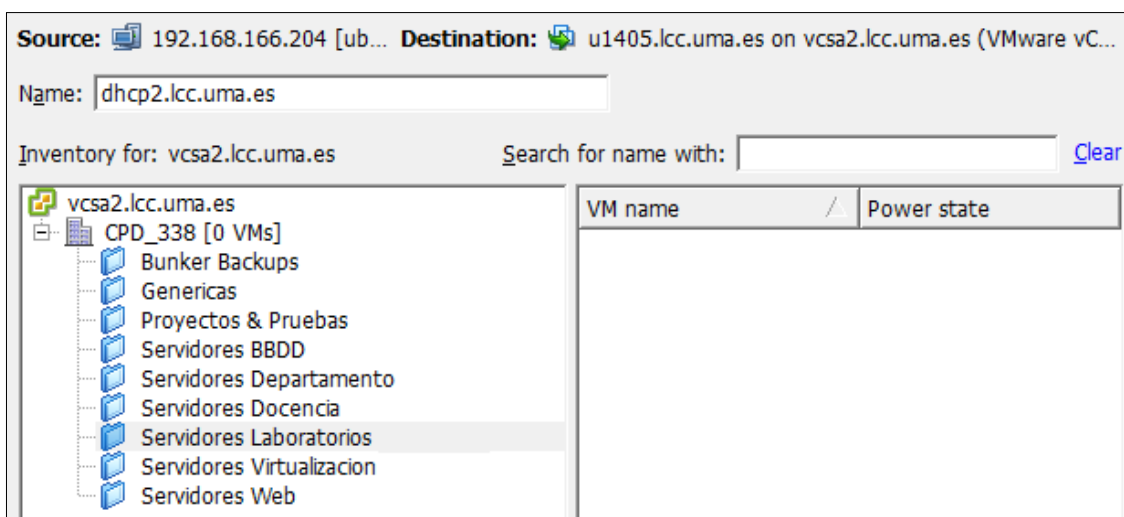
Server:

User name:

Password:

Figura 78. Datos de conexión del destino

Una vez realizada la conexión con *vCenter*, solicita lugar del inventario en el destino donde deseamos acomodar la máquina virtual. VER FIGURA 79.



Source: 192.168.166.204 [ubuntu] Destination: u1405.lcc.uma.es on vcsa2.lcc.uma.es (VMware vCenter)

Name:

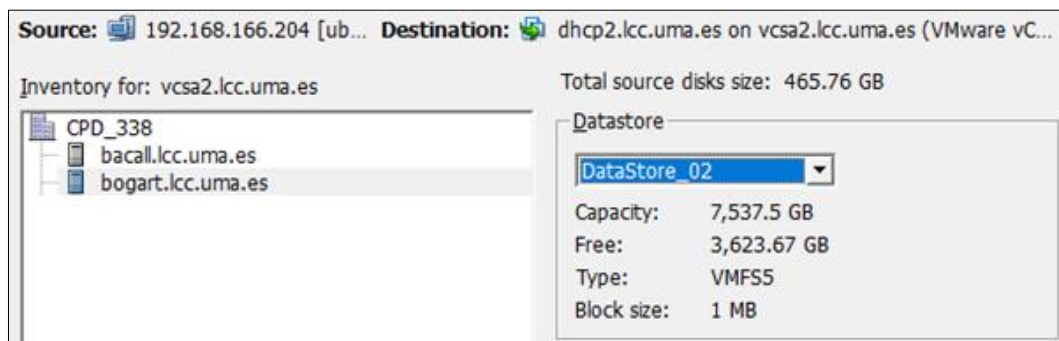
Inventory for: vcsa2.lcc.uma.es Search for name with: Clear

- vcsa2.lcc.uma.es
 - CPD_338 [0 VMs]
 - Bunker Backups
 - Genericas
 - Proyectos & Pruebas
 - Servidores BBDD
 - Servidores Departamento
 - Servidores Docencia
 - Servidores Laboratorios
 - Servidores Virtualizacion
 - Servidores Web

VM name	Power state
---------	-------------

Figura 79. Inventario de vCenter

Nuestro *vCenter* se compone de dos *hosts* y dos *DataStores*, por lo que debemos elegir cuál ejecutará la nueva máquina virtual y qué almacenamiento la contendrá. VER FIGURA 80.



Source: 192.168.166.204 [ubuntu] Destination: dhcp2.lcc.uma.es on vcsa2.lcc.uma.es (VMware vCenter)

Inventory for: vcsa2.lcc.uma.es Total source disks size: 465.76 GB

- CPD_338
 - bacall.lcc.uma.es
 - bogart.lcc.uma.es

Datastore:

Capacity: 7,537.5 GB
Free: 3,623.67 GB
Type: VMFS5
Block size: 1 MB

Figura 80. Host y DataStores en destino

Un servidor de DHCP tiene un consumo de recursos ínfimo, por lo que no le concederemos los mismos recursos que los de la máquina física de origen. Editamos las opciones previas a la conversión y bajamos el **procesamiento** a 1 core, la **memoria** a 1 GB y cambiamos el formato de disco para el **almacenamiento** de **Thick** a **Thin**. VER FIGURA 81.

Además, inhabilitamos IPv6 y cambiamos la vlan por defecto de la red IPv4 a 192.168.154.0/22.

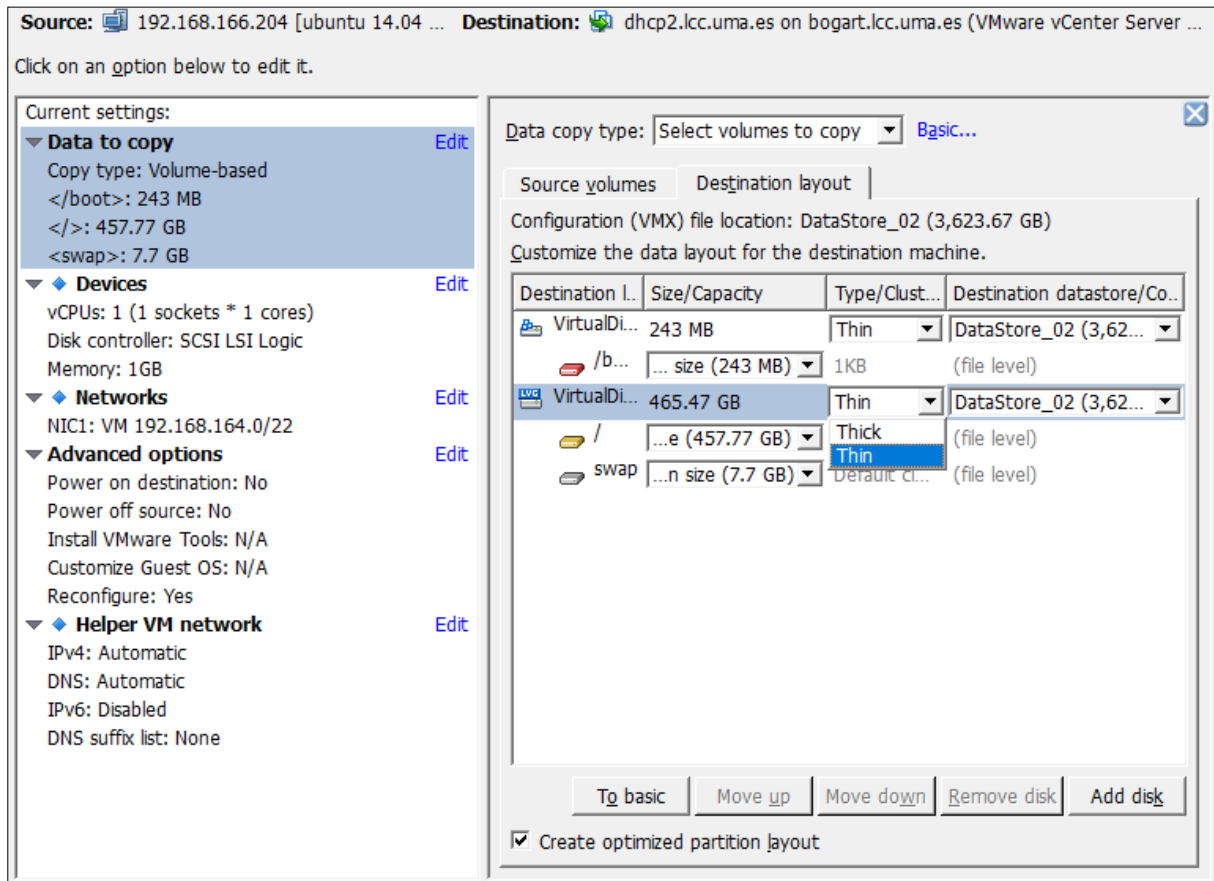


Figura 81. Opciones de conversión

Y comienza la conversión. VER FIGURA 82.

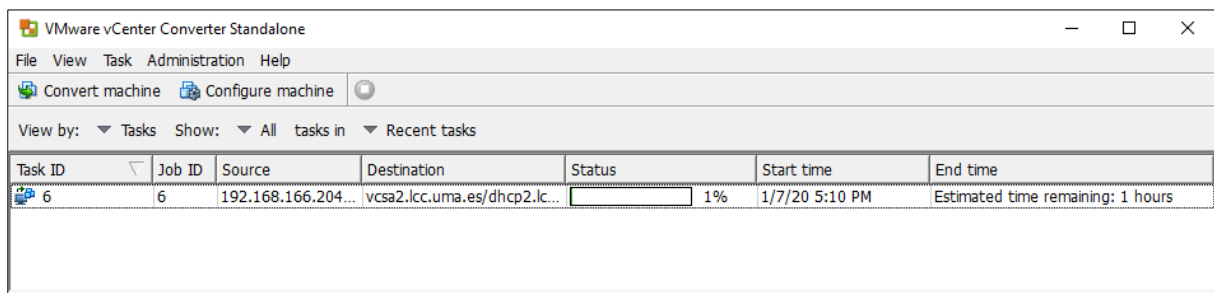


Figura 82. Conversión en curso

Una vez finalizada la conversión, accedemos a nuestro vCenter, seleccionamos la máquina virtual resultante y la encendemos (sin olvidar previamente apagar la máquina física) con el menú contextual del botón derecho del ratón. VER FIGURA 83.

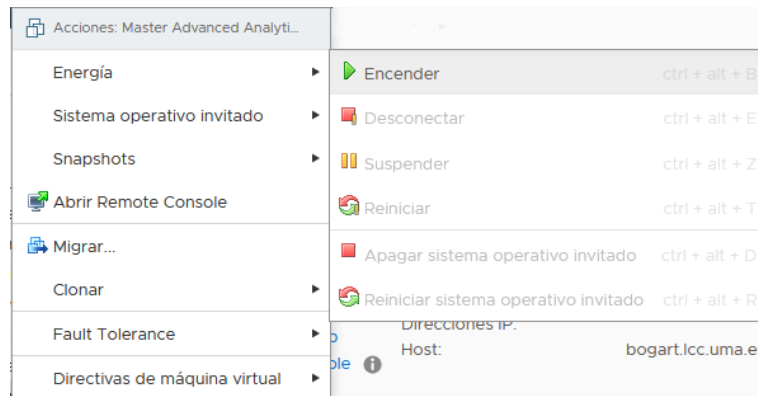


Figura 83. Encendido de máquina virtual de DHCP

Observamos que el cambio del proveedor del servicio de DHCP ha sido transparente para los equipos de los laboratorio - Aulas TIC dado que se trata de la misma VLAN por lo que, dichos equipos continúan obteniendo la configuración de red sin ninguna incidencia.

Además, constatamos que el consumo de recursos de la máquina virtual está muy por debajo de los que hemos asignado; 180 MB de memoria y gracias a aprovisionamiento *thin*, sólo 2,39 GB de espacio en disco. VER FIGURA 84 .

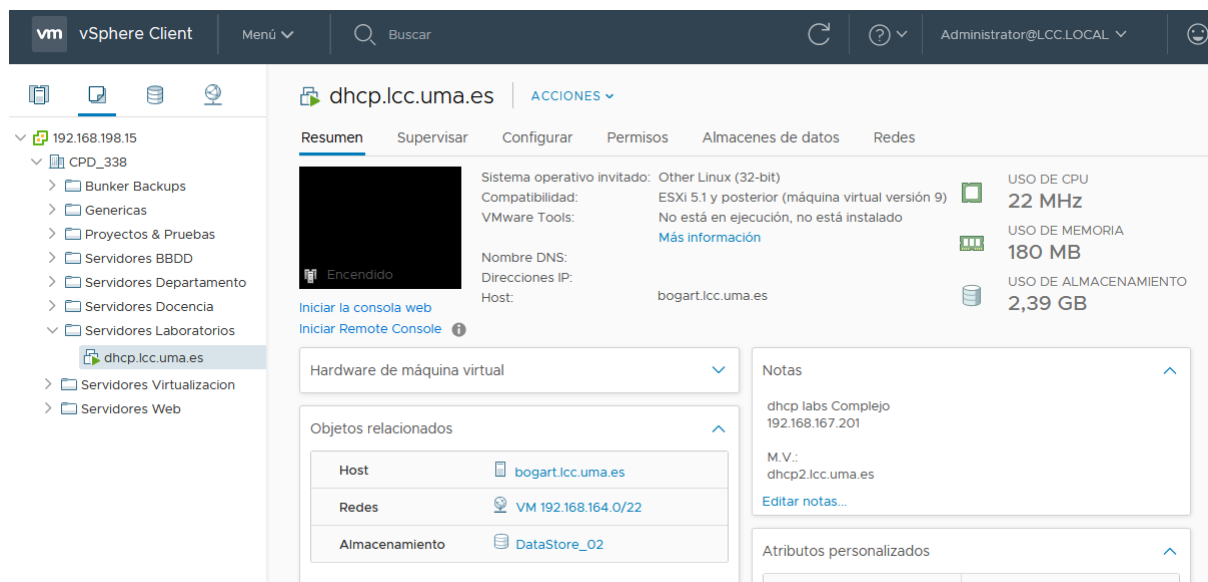


Figura 84. Características de la máquina virtual de DHCP

DHCP es un servicio suficientemente probado y documentado, por lo que no profundizaremos demasiado en ello salvo en las características necesarias para el funcionamiento de **OpenGnsys**. VER 3.4. DISEÑO DEL MODELO DE AULA TIC.

Añadimos las siguientes líneas al comienzo del archivo de configuración `/etc/dhcpd.conf` para permitir configuraciones de red en arranque PXE de los equipos de las Aulas TIC.

allow booting;
allow bootp;

A continuación, se muestra un ejemplo de configuración en `/etc/dhcpd.conf` para los dos primeros equipos del primero de los laboratorios:

```
# Laboratorio 3.1.1 -----
group {
# Gateway para los laboratorios:
  option routers 192.168.167.254;
#   servidor OpenGnSys og5.lcc.uma.es
  next-server 192.168.166.211;

  host pc0101 {
    option host-name "pc0101.docencia.lcc.uma.es";
    hardware ethernet 8C:DC:D4:35:9B:6C;
    fixed-address 192.168.164.1;
    filename "grldr";
  }

  host pc0102 {
    option host-name "pc0102.docencia.lcc.uma.es";
    hardware ethernet 8C:DC:D4:35:9A:3C;
    fixed-address 192.168.164.2;
    filename "grldr";
  }
}
```

Y no olvidar reiniciar el servicio: `service dhcpd restart`

4.2.2. Servidor de OpenGnsys

La implementación del servidor de OpenGnsys que vamos a realizar tendrá las siguientes características:

- Versión de OpenGnsys => v1.1.0 20180613081416
- Sistema Operativo => Ubuntu Server 14.04.5 LTS x64
- Nombre => og5.lcc.uma.es
- Localización => DataStore_02
- Almacenamiento => 750 GB en Thin
- Dirección IP => 192.168.166.211
- Página Web => og5.lcc.uma.es/opengnsys

Dividiremos la implementación de OpenGnsys en tres fases: 1) instalación de la máquina virtual con el sistema operativo; 2) instalación de la aplicación de OpenGnsys; y 3) configuración de OpenGnsys para adaptarlo a nuestro escenario docente.

4.2.2.1. Instalación del sistema para OpenGnsys

La instalación del sistema tiene dos partes: la creación del hardware virtual de la máquina virtual y la instalación del sistema operativo en la máquina virtual.

Accedemos a uno de los *hosts* mediante **VMware vSphere Client** y utilizamos el asistente para **Crear una nueva máquina virtual**. VER FIGURA 85.



Figura 85. Crear una nueva máquina virtual

Creamos la nueva máquina virtual con la configuración “Típica” de dispositivos y opciones de configuración comunes y la llamamos **og5.lcc.uma.es** para hacer coincidir el nombre de la máquina virtual con el que posteriormente tendrá el sistema operativo. VER FIGURA 86.

Nombre:

El nombre de una máquina virtual puede contener hasta 80 caracteres y debe ser único dentro de cada carpeta de máquina virtual de vCenter Server.

Las carpetas de máquina virtual no se pueden ver cuando la conexión a un host es directa. Para ver las carpetas de máquina virtual y especificar una ubicación para esta máquina virtual, conéctese a vCenter

Figura 86. Elección de nombre para la máquina virtual

Seleccionamos el **DataStore_02** como almacén de datos que contendrá la máquina virtual. VER FIGURA 87.

Seleccionar un almacenamiento de destino para los archivos de máquina virtual:

Nombre	Tipo de un...	Capacidad	Aprovision...	Libre	Tipo
Bogart_DAS1	No SSD	271,75 GB	6,03 GB	265,72 GB	VMFS5
Datastore_01	No SSD	10,63 TB	2,49 TB	8,20 TB	VMFS6
DataStore_02	No SSD	7,36 TB	4,74 TB	3,54 TB	VMFS5

Figura 87. Elección de almacén de datos contenedor de la máquina virtual

Identificamos el sistema operativo que contendrá la máquina virtual. Para la instalación de OpenGnsys será Linux Ubuntu Server 14.04 LTS. VER FIGURA 88.

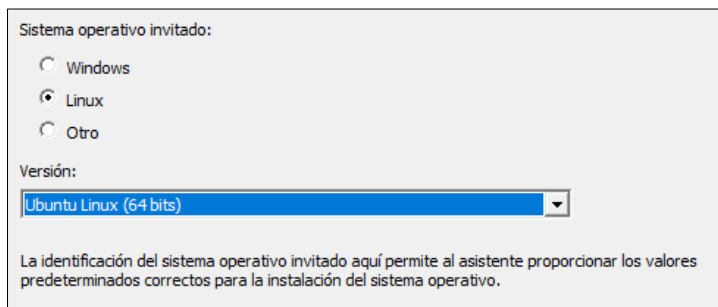


Figura 88. Sistema Operativo de la máquina virtual

Especificamos el número de adaptadores de red y redes a las que se conectarán cada uno de ellos. En nuestro caso un solo adaptador en la VLAN de la red 192.168.164.0/22 (VER FIGURA 89) que es la misma en la que se encuentran en producción el servidor de DHCP y los equipos de las Aulas TIC. VER 3.1.1. DIRECCIONAMIENTO DE LAS AULAS TIC.

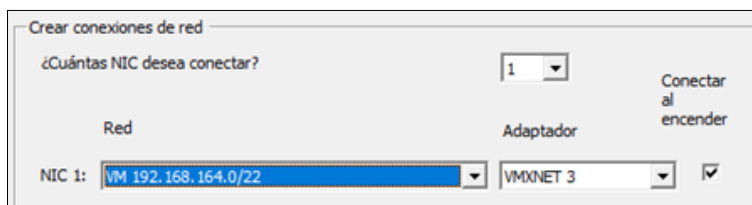


Figura 89. Adaptadores de red de la máquina virtual

Respecto al disco para la máquina virtual, optaremos por 750 GB con aprovisionamiento **Thin** (traducido por VMware al español como “fino”). A continuación, pulsamos *Aceptar* y se crea el contenedor hardware virtual para la nueva máquina virtual.

Para subir la imagen ISO del sistema operativo utilizamos el menú de contexto sobre el **DataStore_02** y seleccionamos **Examinar almacén de datos**. VER FIGURA 90.

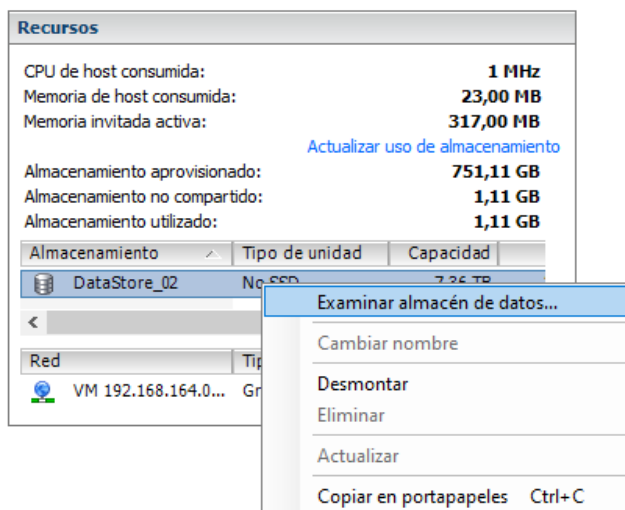


Figura 90. Examinar almacén de datos

El **Explorador de almacén de datos** proporciona herramientas que permiten **crear carpetas**, así como **cargar** y **descargar** archivos. Creamos una carpeta llamada **ISO** para contener la imagen **ISO** que vamos a cargar (también los que carguemos en instalaciones futuras) y finalmente, seleccionamos **Cargar** e indicamos el lugar de nuestro disco local donde se encuentra la imagen **ISO**. VER FIGURA 91.

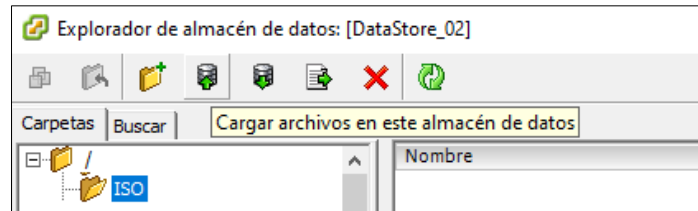


Figura 91. Explorador de almacén de datos

Seleccionamos la máquina virtual y la conectamos a la imagen **ISO** que hemos subido al **DataStore_02**. VER FIGURA 92.

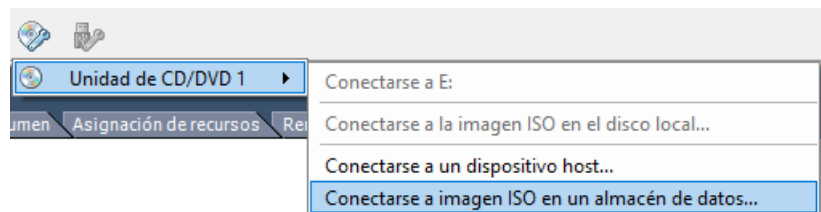


Figura 92. Conectar máquina virtual a imagen ISO

Encendemos la máquina virtual e iniciamos la instalación del sistema operativo siguiendo el asistente de instalación de Ubuntu Server, en el que sólo añadimos el **servidor de SSH**. Entendemos que la instalación de Ubuntu Server está más que documentada por lo que obviamos la documentación de dicha instalación.

4.2.2.2. Instalación de OpenGnsys

Habilitamos el **login** en el sistema para **root** para no tener que usar constantemente **sudo** mediante **sudo passwd root** y también para conexiones mediante **ssh** editando **/etc/ssh/sshd_config** y modificando el valor de la variable **PermitRootLogin yes**.

Nuestro Linux para OpenGnsys tiene una dirección IP privada por lo que necesitaremos exportar la dirección del servidor proxy web de la autoridad de red en línea de comandos.

```
export http_proxy=http://proxy.satd.uma.es:3128
```

Para la instalación de OpenGnsys necesitaremos los paquetes **“subversión”** y **“wget”**. Procedemos a la instalación:

```
apt-get update  
apt-get install subversión wget
```

A continuación, configuramos el proxy web de la autoridad de red en subversión editando el archivo `/etc/subversión/servers` y modificando las siguientes líneas:

```
[global]
http-proxy-host = proxy.satd.uma.es
http-proxy-port = 3128
```

Descargamos el instalador de OpenGnsys des web del proyecto:

```
wget http://www.opengnsys.es/svn/trunk/installer/opengnsys_installer.sh
```

Editamos el archivo que acabamos de descargar (`opengnsys_installer.sh`) y configuramos usuarios y contraseñas para OpenGnsys, con especial atención a `DB_USER` y `DB_PASSWD` que serán los que usaremos posteriormente para acceder a la consola web de OpenGnsys.

```
MYSQL_ROOT_PASSWORD="xxx"      # Clave root de MySQL
OPENGNSYS_DB_USER="xxx"        # Usuario de acceso a la base de datos
OPENGNSYS_DB_PASSWD="xxx"     # Clave de acceso a la base de datos
OPENGNSYS_CLIENT_PASSWD="xxx" # Clave de acceso del cliente
```

Damos permisos de ejecución al archivo de instalación y lo ejecutamos, lo que realizará la instalación de OpenGnsys en el sistema:

```
chmod 755 opengnsys_installer.sh
./opengnsys_installer.sh
```

4.2.2.3. Configuración de OpenGnsys

Ya tenemos instalado *OpenGnsys* en la máquina virtual, ahora queda adecuarlo a las aulas TIC. Hemos solicitado a la autoridad de red el alta en DNS por lo que accedemos a la consola web en la dirección ***og5.lcc.uma.es/opengnsys***. VER FIGURA 93.



Figura 93. Acceso para administradores de OpenGnsys

Para configurar la Unidad Organizativa la dejamos en blanco, accedemos con el usuario y contraseña que introdujimos *OPENGNSYS_DB_USER* y *OPENGNSYS_DB_PASSWD*.

A continuación, cambiamos el nombre de la *Unidad Organizativa default* (en inglés: *Unidad Organizativa por defecto*) por *LCC (default)*, creamos un usuario para los técnicos del departamento y lo hacemos administrador de *LCC (default)*.

En OpenGnsys la práctica totalidad de las acciones se realizan mediante los menús de contexto del botón derecho; seleccionamos *Usuarios* y la *Unidad Organizativa* respectivamente. VER FIGURA 94.

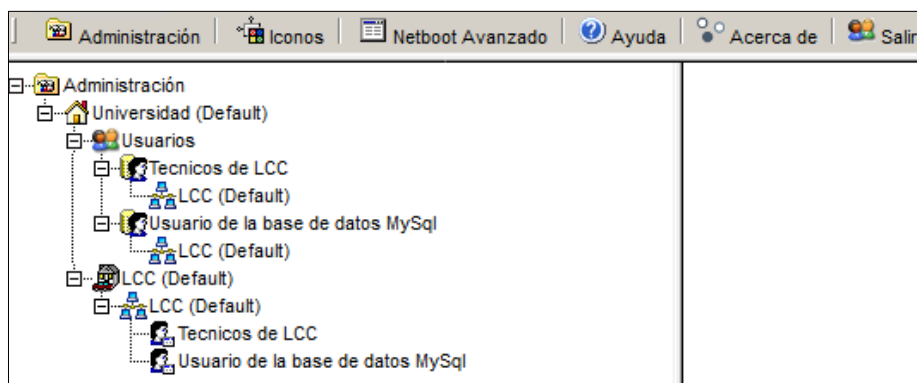


Figura 94. Usuarios y Unidad Organizativa de OpenGnsys

Para dar de alta las aulas TIC y los equipos, iniciamos sesión con el usuario que acabamos de crear en la Unidad Organizativa *LCC (default)* y a continuación, nuevamente con el menú de contexto creamos las aulas. VER FIGURA 96.

La planta del edificio donde se encuentran los laboratorios alberga dos armarios de datos. Estimamos más óptimo crear un aula en OpenGnsys por armario de datos e identificar los equipos de los diferentes laboratorios por grupos de ordenadores dentro de los armarios. VER FIGURA 95.

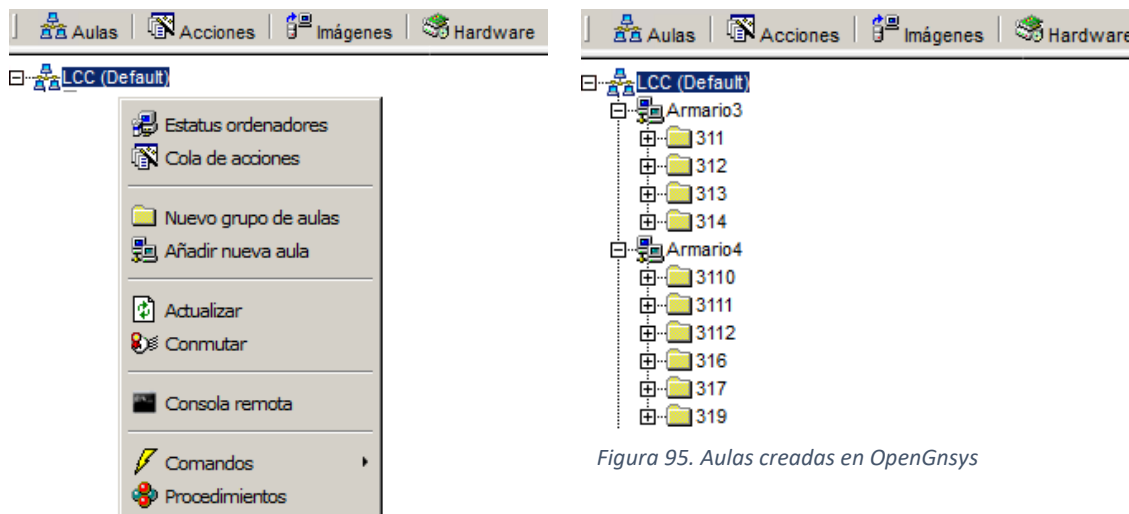


Figura 95. Aulas creadas en OpenGnsys

Figura 96. Creación de aulas en OpenGnsys

Es posible añadir los equipos de uno en uno mediante el menú de contexto sobre la agrupación donde deseamos añadirlo y seleccionando la acción **Añadir nuevo ordenador** que nos conduce a un completo formulario para tal fin. VER FIGURA 97.

Nombre *	<input type="text"/>	 (150X110)-(jpg - gif - png) ---- Insertar foto> Examinar... No se ha seleccionado ningún archivo.
Dirección IP	<input type="text"/>	
Dirección MAC	<input type="text"/>	
Nº de serie	<input type="text"/> (no detectado)	
Foto ordenador	fotoordenador.gif Ver fotos	
Perfil hardware	<input type="text"/>	
Repositorio	<input type="text"/>	
ogLive	Asignado por el administrador	
Menú	<input type="text"/>	
Autoexec	<input type="text"/>	
Interfaz de red	eth0	
Driver de red	generic	
Validación	No	
Página login	<input type="text"/>	
Página validación	<input type="text"/>	
* AVISO: El nombre de equipo no debe superar los 15 caracteres si se instalan sistemas Windows. ATENCIÓN: El equipo iniciará en local por defecto; usar NetBoot Avanzado para modificar su arranque.		

Figura 97. Añadir nuevo ordenador a OpenGnsys

Para un elevado número de equipos es una tarea muy engorrosa por lo que utilizamos una extraordinaria función llamada **Incorporar ordenadores** que permite hacerlo de una tacada mediante el archivo de configuración de DHCP (dhcpd.conf), aunque primero hay que depurarlo pues sólo debe contener las declaraciones de los equipos mediante la tripla: nombre de Host, dirección MAC y dirección IP. Después lo copiaremos en el cuadro "Código DHCP (declaraciones host)". VER FIGURA 98.

Código DHCP (declaraciones "host")	<input type="text"/>
* AVISO: El nombre de equipo no debe superar los 15 caracteres si se instalan sistemas Windows. ATENCIÓN: El equipo iniciará en local por defecto; usar NetBoot Avanzado para modificar su arranque.	

Figura 98. Incorporar ordenadores a OpenGnsys

Una vez creadas las aulas e incorporados los ordenadores tenemos la aplicación totalmente funcional para la gestión de nuestras aulas TIC.

Es mucho lo que podríamos extendernos con OpenGnsys: generación y despliegue de imágenes, protocolos (*unicast*, *multicast* o *bittorrent*) y modos de clonación (directo o con caché), inventario hardware y software de los equipos, repositorios de imágenes, tipos de arranque y un largo etcétera, pero entendemos que no es ese el propósito de este trabajo.

4.2.3. Servidor Proxy

El objetivo de este TFG es mostrar los extraordinarios beneficios que conlleva la virtualización de sistemas, por lo que en lugar de instalar nuevamente una máquina virtual siguiendo un procedimiento similar al del APARTADO 4.2.2.1, clonaremos la máquina virtual que contiene el servidor de DHCP (VER 4.2.1. SERVIDOR DE DHCP) para implementar el servidor Proxy.

4.2.3.1. Clonación de la máquina virtual

Iniciamos sesión en vCenter, seleccionamos la máquina virtual *dhcp.lcc.uma.es* con el botón derecho y seleccionamos **Clonar a máquina virtual** en el menú de contexto. VER FIGURA 99.

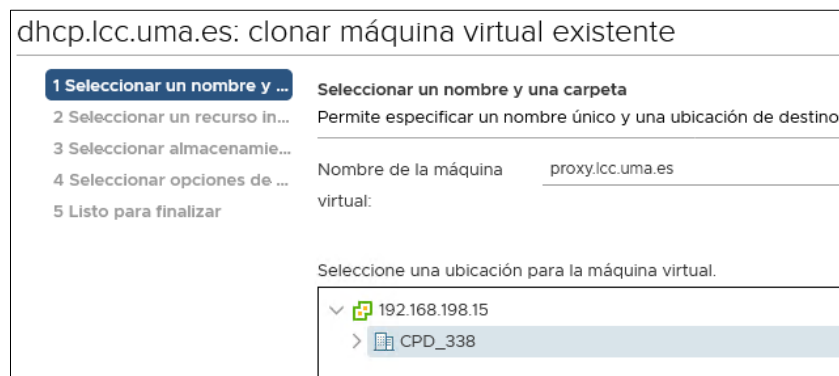


Figura 99. Nombre para la máquina virtual clonada

Seleccionamos el host que ejecutará la máquina virtual resultante. VER FIGURA 100.

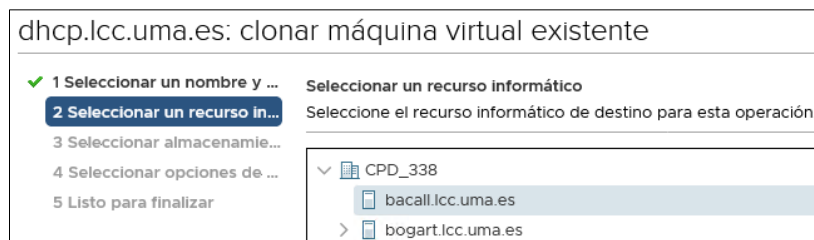


Figura 100. Host para la ejecución de la máquina virtual clonada

Seleccionamos el almacenamiento que contendrá la máquina virtual, de entre los almacenes de datos disponibles. VER FIGURA 101.

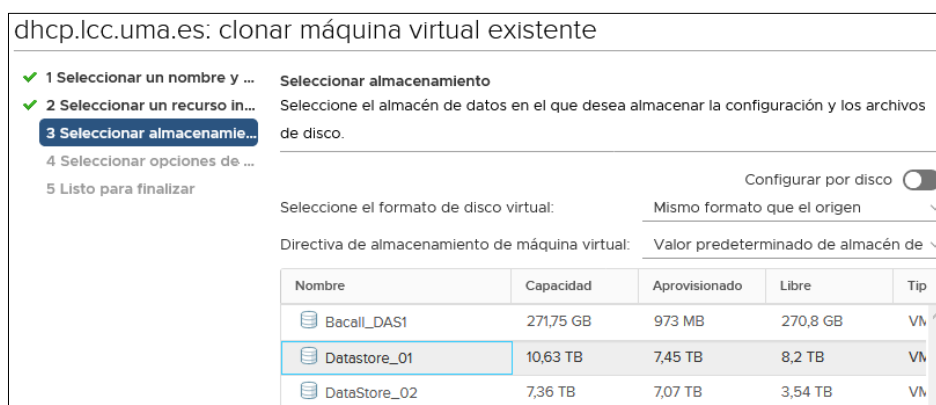


Figura 101. Almacén de datos que contendrá la máquina virtual clonada

Repasamos la configuración y aceptamos (VER FIGURA 102) .El procedimiento tarda muy poco puesto que se trata de una máquina virtual con aprovisionamiento **thin** cuyo tamaño en disco es sólo de 2,39 GB.

dhcp.lcc.uma.es: clonar máquina virtual existente

✓ 1 Seleccionar un nombre y ...
✓ 2 Seleccionar un recurso in...
✓ 3 Seleccionar almacenamie...
✓ 4 Seleccionar opciones de ...
5 Listo para finalizar

Listo para finalizar
Haga clic en Finalizar para iniciar la creación.

Tipo de aprovisionamiento	Clonar una máquina virtual existente
Máquina virtual de origen	dhcp.lcc.uma.es
Nombre de la máquina virtual	proxy.lcc.uma.es
Carpeta	CPD_338
Host	bacall.lcc.uma.es
Almacén de datos	Datastore_01
Almacenamiento en disco	Mismo formato que el origen

Figura 102. Máquina virtual lista para clonar

Ahora tenemos dos máquinas virtuales idénticas, por lo que ambas tienen la misma MAC. Antes de iniciar la configuración debemos generar una nueva MAC para la máquina clonada. Seleccionamos la máquina virtual proxy.lcc.uma.es con el botón derecho, ejecutamos **Editar configuración** en el menú de contexto y eliminamos el adaptador de red mediante el símbolo ⊗ de la parte derecha (VER FIGURA 103). A continuación, Agregar nuevo dispositivo => Adaptador de red y seleccionar la red VM 192.168.164.0/24.

AGREGAR NUEVO DISPOSITIVO

> CPU	1	▼	i	^
> Memoria	400	MB	▼	
> Disco duro 1	10	GB	▼	
> Controladora SCSI 0	LSI Logic Parallel			
▼ Adaptador de red 1	VM 192.168.164.0/22	▼	⊗	
Estado	<input checked="" type="checkbox"/> Conectar al encender			
Tipo de adaptador	Flexible ▼			
Dirección MAC	00:50:56:84:87:cf	Automático	▼	
> Unidad de CD/DVD 1	Dispositivo cliente	▼	<input type="checkbox"/> Conectar...	
> Tarjeta de vídeo	Especificar configuración personalizada ▼			
Dispositivo VMCI	Dispositivo del bus PCI de la máquina virtual que brinda compatibilidad con la interfaz de comunicación de la máquina virtual.			
> Otro	Hardware adicional			

Figura 103. Eliminar y Agregar nuevo dispositivo

Encendemos la máquina virtual, pero como el nuevo adaptador de red virtual no está configurado, accedemos mediante la consola web que proporciona vCenter. VER FIGURA 104.

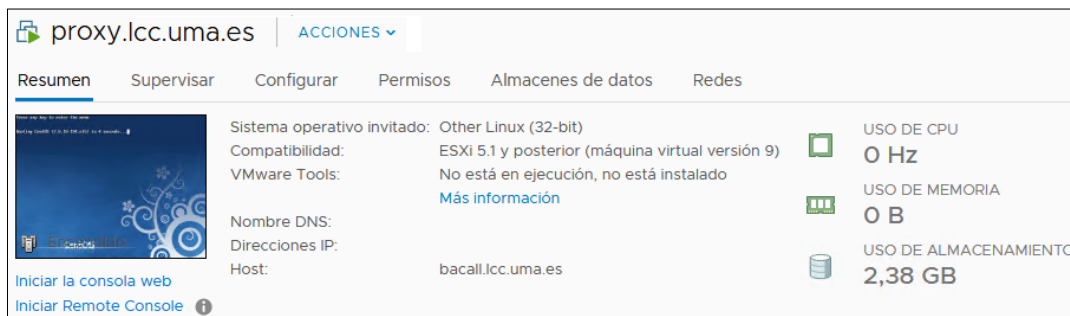


Figura 104. Resumen de máquina virtual

Iniciamos sesión con las credenciales del usuario *root* existente en la máquina virtual contenedora del servidor de DHCP (puesto que es un clon de la misma). VER FIGURA 105.

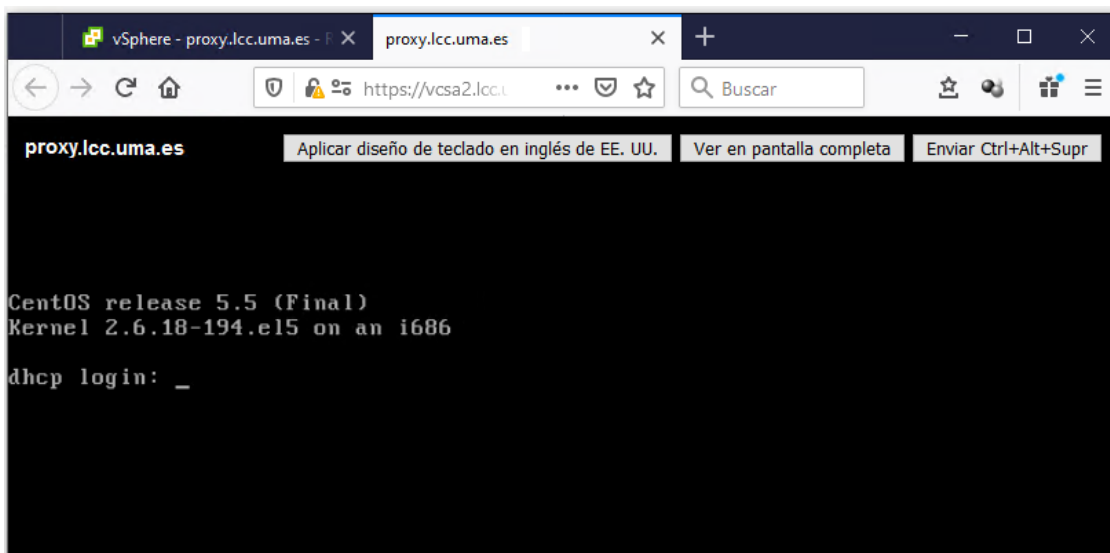


Figura 105. Consola web de máquina virtual

Editamos el archivo de configuración de red `/etc/sysconfig/network-scripts/ifcfg-eth0` y aplicamos la siguiente configuración:

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
BOOTPROTO=static
BROADCAST=192.168.167.255
#HWADDR=00:0C:29:80:D8:B3          <= dirección MAC anterior
HWADDR=00:50:56:9A:B3:8A       <= nueva dirección MAC
IPADDR=192.168.167.202         <= nueva dirección IP
NETMASK=255.255.252.0
NETWORK=192.168.164.0
ONBOOT=yes
```

No queremos que el demonio del servidor de *DHCP* se inicie automáticamente con el inicio del sistema (como está en la máquina virtual original de *DHCP*), así que ejecutamos:

```
chkconfig --level 35 dhcpd off
```

Reiniciamos el servicio de red `/etc/init.d/network restart` y comprobamos que la máquina se comunica con la red.

```
PING 192.168.167.254 (192.168.167.254) 56(84) bytes of data.  
64 bytes from 192.168.167.254: icmp_seq=1 ttl=255 time=0.399 ms
```

Cambiamos la identificación del sistema en `/etc/sysconfig/network`

```
NETWORKING=yes  
NETWORKING_IPV6=no  
HOSTNAME=proxy.lcc.uma.es
```

También en `/etc/hosts`

```
127.0.0.1    proxy.lcc.uma.es proxy localhost.localdomain localhost  
::1        localhost6.localdomain6 localhost6
```

Desinstalamos el paquete de *DHCP* e instalamos el paquete de servidor *Proxy squid*:

```
rpm -e dhcp  
yum install squid
```

Cambiamos la contraseña de *root* mediante el comando `passwd` y reiniciamos el sistema.

4.2.3.2. Configuración del servidor Proxy

Nos conectamos a la máquina virtual `proxy.lcc.uma.es` con un cliente de **ssh** (por ejemplo, *putty*) y editamos el archivo de configuración del proxy *squid* en `/etc/squid/squid.conf`

El archivo de configuración es muy extenso, por lo que nos ceñimos a los ítems fundamentales para la puesta en marcha en nuestro escenario.

Definición del proxy padre de la autoridad de red, dado que nuestro proxy tiene una dirección IP privada.

```
cache_peer 150.214.57.8 parent 3128 3130
```

Definición del tamaño en disco en el sistema operativo de la máquina virtual que ocupará la caché del servidor proxy.

```
cache_dir ufs /var/spool/squid 4000 16 256
```

Definición de etiquetas identificadoras de las aulas TIC, gracias a lo cual será posible permitir o denegar el acceso a internet de forma independiente a cada una, sustituyendo en la línea del laboratorio correspondiente **allow** (en inglés: permitir) por **deny** (en inglés: denegar) y reiniciando (o recargando) el servicio a continuación.

Agrupaciones de PCs por laboratorios – Planta 1

```
acl lab311 src 192.168.164.1-192.168.164.40/255.255.255.255
acl lab312 src 192.168.164.41-192.168.164.80/255.255.255.255
acl lab313 src 192.168.164.81-192.168.164.120/255.255.255.255
acl lab314 src 192.168.164.121-192.168.164.160/255.255.255.255
acl lab315 src 192.168.164.161-192.168.164.200/255.255.255.255
acl lab316 src 192.168.164.201-192.168.164.240/255.255.255.255
acl lab317 src 192.168.166.1-192.168.166.40/255.255.255.255
acl lab319 src 192.168.166.41-192.168.166.80/255.255.255.255
acl lab3110 src 192.168.166.81-192.168.166.120/255.255.255.255
acl lab3111 src 192.168.166.121-192.168.166.160/255.255.255.255
acl lab3112 src 192.168.166.161-192.168.166.200/255.255.255.255
```

Agrupaciones de PCs por laboratorios – Planta 3

```
acl lab331 src 192.168.167.227-192.168.167.249/255.255.255.255
```

Agrupaciones de máquinas virtuales de laboratorios – Planta 1

```
acl vmlab311 src 192.168.165.1-192.168.165.40/255.255.255.255
acl vmlab312 src 192.168.165.41-192.168.165.80/255.255.255.255
acl vmlab313 src 192.168.165.81-192.168.165.120/255.255.255.255
acl vmlab314 src 192.168.165.121-192.168.165.160/255.255.255.255
acl vmlab315 src 192.168.165.161-192.168.165.200/255.255.255.255
acl vmlab316 src 192.168.165.201-192.168.165.240/255.255.255.255
acl vmlab317 src 192.168.167.1-192.168.167.40/255.255.255.255
acl vmlab319 src 192.168.167.41-192.168.167.80/255.255.255.255
acl vmlab3110 src 192.168.167.81-192.168.167.120/255.255.255.255
acl vmlab3111 src 192.168.167.121-192.168.167.160/255.255.255.255
acl vmlab3112 src 192.168.167.161-192.168.167.200/255.255.255.255
```

Permisos o denegaciones de uso del Proxy para las Aulas TIC:

#Laboratorios docentes - Máquinas físicas – Planta 1

```
http_access allow lab311
http_access allow lab312
http_access allow lab313
http_access allow lab314
http_access allow lab315
http_access allow lab316
http_access allow lab317
http_access allow lab319
http_access allow lab3110
http_access allow lab3111
http_access allow lab3112
```

#Laboratorios docentes - Máquinas físicas – Planta 3

```
http_access allow lab331
```

#Laboratorios docentes - Máquinas virtuales

```
http_access allow vmlab311
http_access allow vmlab312
http_access allow vmlab313
http_access allow vmlab314
http_access allow vmlab315
http_access allow vmlab316
http_access allow vmlab317
http_access allow vmlab319
http_access allow vmlab3110
http_access allow vmlab3111
http_access allow vmlab3112
```

Una vez configurado, iniciamos el servicio:

```
/etc/init.d/squid start
```

Queremos que el demonio del servidor proxy *squid* se inicie automáticamente con el inicio del sistema, así que ejecutamos el siguiente comando:

```
chkconfig --level 35 squid on
```

Para comprobar el funcionamiento, configuramos el proxy en el navegador de un equipo de un aula TIC (VER FIGURA 106)

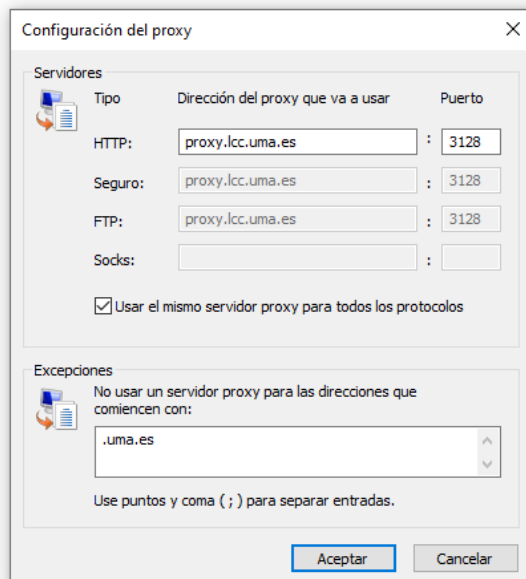


Figura 106. Configuración de proxy en un navegador

4.2.4. Servidor Samba

En base a nuestro **Análisis** (VER 2.2. DIMENSIONAMIENTO) y configuración de samba en base a nuestro **Diseño** (VER 3.5. SERVICIOS BÁSICOS PARA LA DOCENCIA) dividiremos la **Implementación** del servidor SAMBA en dos fases: 1) instalación de la máquina virtual con el sistema operativo, incluida selección del paquete *Samba*; y 2) configuración del paquete *Samba*.

4.2.4.1. Instalación del sistema para Samba

Realizamos los mismos pasos y operaciones que en el Apartado 4.2.2.1. INSTALACIÓN DEL SISTEMA PARA OPENGNYSYS, a partir de una imagen ISO de *Ubuntu Server 16.04.2 LTS x64*, obteniendo como resultado una máquina virtual con las siguientes características:

- Nombre => samba.lcc.uma.es
- Localización => DataStore_01
- Almacenamiento => 100 GB en *Thin*
- Dirección IP => 192.168.167.203

En el proceso de instalación hemos seleccionados los paquetes para el servidor de archivos de *samba* y para el servidor de *SSH*. VER FIGURA 107.



Figura 107. Elección de paquetes para Ubuntu Server 16.04

Una vez finalizada la instalación, arrancamos la máquina virtual e iniciamos sesión en el sistema con las credenciales del usuario creado en el proceso de instalación. Habilitamos el *login* en el sistema para *root* mediante *sudo passwd root* y también para conexiones mediante *ssh* editando */etc/ssh/sshd_config* y modificando el valor de la variable *PermitRootLogin* *yes*. A continuación, reiniciamos el demonio de SSH con *sudo systemctl restart sshd*.

Nos gustaría llamar la atención sobre el hecho de que la máquina virtual creada y puesta en producción sólo ocupa en disco (por ser *thin*) el espacio que ocupan sus datos, por lo que a pesar de haberla dimensionado con 100 GB de almacenamiento sólo consume 1,11 GB del almacén de datos. VER FIGURA 108.



Figura 108. Resumen de la máquina virtual para Samba

4.2.4.2. Configuración de Samba

Nos conectamos a la máquina virtual `samba.lcc.uma.es` con un cliente de `ssh` (por ejemplo, `putty`) y creamos los usuarios `alumno` y `profesor` en el sistema, sin permisos para iniciar sesión:

```
useradd alumno -s /sbin/nologin  
useradd profesor -s /sbin/nologin
```

Añadimos los usuarios `samba` y creamos las contraseñas (para `alumno`, sin contraseña):

```
smbpasswd -a técnicos  
smbpasswd -a profesor  
smbpasswd -a alumno
```

Creamos la estructura de directorios:

```
mkdir /DATOS  
mkdir /DATOS/practicas  
mkdir /DATOS/VM
```

Damos la posesión del directorio `practicas` y `VM` a los usuarios `profesor` y `técnicos` respectivamente:

```
chown -R profesor.profesor /DATOS/practicas/  
chown -R tecnicos.tecnicos /DATOS/VM/
```

No hemos cambiado permisos sobre los directorios, es decir que por defecto los propietarios tienen derechos de escritura y el resto de lectura, por lo que el `profesor` puede escribir en `prácticas` y los `técnicos` en `VM`, el resto de usuarios tienen lectura en ambos directorios.

```
drwxr-xr-x 2 profesor profesor 4096 ene 16 09:41 practicas  
drwxr-xr-x 2 tecnicos tecnicos 4096 ene 16 09:41 VM
```

Editamos el archivo de configuración de samba `/etc/samba/smb.conf` y añadimos las líneas correspondientes a los recursos compartidos prestando atención a las máscaras de creación de archivos o directorios que serán de sólo lectura (y ejecución en el caso de los directorios) para el resto de usuarios, es decir cualquiera que no sea el que está realizando la acción. Hay que tener en cuenta que el único que puede realizar la acción es el propietario del directorio:

```
[practicas]  
comment = Practicas en Laboratorios de LCC  
path = /DATOS/practicas  
guest ok = no  
browseable = yes  
writable = yes  
create mask = 0664  
directory mask = 0775  
valid users = tecnicos profesor alumno
```

[VM]

```
comment = Backup de maquinas virtuales en Laboratorios de LCC
path = /DATOS/VM
guest ok = no
browseable = yes
writable = yes
create mask = 0664
directory mask = 0775
valid users = tecnicos profesor alumno
```

Añadimos los demonios de samba al inicio del sistema:

```
systemctl enable nmbd.service
systemctl enable smb.service
```

Iniciamos el servicio:

```
service smb start
```

Finalmente comprobamos el funcionamiento (conexión y permisos de usuarios sobre los recursos compartidos) en un equipo de las Aulas TIC del departamento con la función *Conectar a unidad de red de Windows 10* (VER FIGURA 109). Para ello, especificamos en “*Carpeta*” cualquiera de los recursos compartidos implementados utilizando cualquiera de las credenciales de usuarios planificadas en nuestro diseño. VER 3.5. SERVICIOS BÁSICOS PARA LA DOCENCIA.

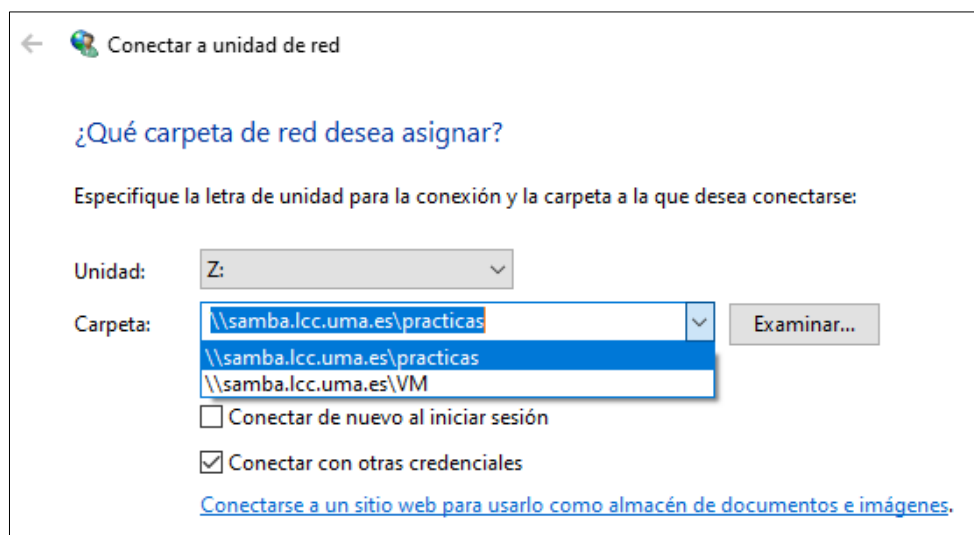


Figura 109. Conectar a unidad de red en Windows 10

5. CONCLUSIONES

Hemos empaquetado una solución de virtualización para entornos de docencia mediante el **análisis**, el **diseño** y la **implementación** en un espacio mucho mayor (VER FIGURA 110), pues el número de laboratorios y equipos informáticos supera de sobra la práctica totalidad de escenarios que pueden encontrarse en cualquier instituto, ya sea de la Bachiller o de Formación Profesional de Grado Medio o de Grado Superior.

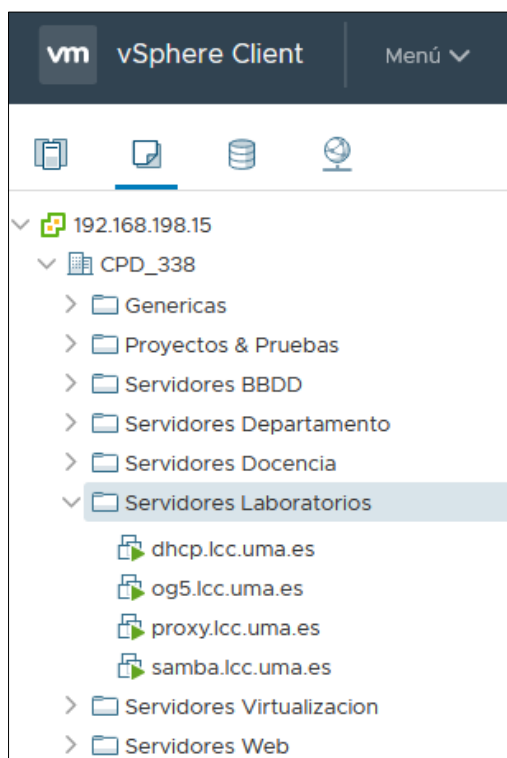


Figura 110. Servidores implementados respecto al total de la infraestructura de virtualización

Antes de construir la casa, había que fabricar los ladrillos. En otras palabras, antes de virtualizar los servicios y las aplicaciones, era necesario montar la infraestructura de virtualización y antes que esto, la interconexión de dispositivos.

Sin embargo, a pesar de la clara línea de trabajo, ha sido necesario un profundo estudio, pues el abanico de tecnologías era muy amplio, y los trabajos a realizar, considerables. Además, la virtualización tiene un profundo impacto sobre áreas como: sistemas, aplicaciones, almacenamiento, redes e incluso seguridad.

En nuestro caso, habíamos puesto el foco sobre los servicios y aplicaciones necesarios para alcanzar nuestros objetivos; el funcionamiento de los Laboratorios - Aulas TIC, por lo que ha sido imperativo un correcto dimensionamiento de la infraestructura de virtualización, esquematizar la interconexión de dispositivos, diseñar la asignación de direccionamiento de red y, finalmente, realizarlo todo de forma metodológicamente ordenada.

El trabajo se ha estructurado en **dos grandes apartados**, i) la creación de un sistema de virtualización y ii) la generación en el mismo de los servicios y aplicaciones necesarios para la puesta en marcha, el desempeño y la administración de Aulas TIC

Todo ello se ha llevado a cabo de forma muy estructurada y siguiendo una metodología clara: **Análisis, Diseño e Implementación del sistema de virtualización** (interconexión de dispositivos incluida) y nuevamente **Análisis, Diseño e Implementación de los servicios y aplicaciones**; en ambos casos, éstas emanan, de la tradicional **metodología en cascada**. VER 1.6. METODOLOGÍA.

Sin embargo, contábamos desde un principio con la complejidad añadida de trabajar en un escenario vivo, por lo que la ejecución y puesta en marcha del sistema no podía ser directa, si no que su acometida debía ser transparente para los usuarios y realizarse de forma gradual. Es por lo que para reducir los riesgos de paradas de servicio y sobre todo ante la compleja interconexión de dispositivos también nos hemos apoyado en la metodología en espiral (VER 1.6. METODOLOGÍA) mediante el fraccionamiento de tareas y las ejecuciones parciales y progresivas.

Por otro lado, como se ha podido comprobar a lo largo de este trabajo, la concentración de los recursos hardware y la virtualización servicios y aplicaciones, nos ha proporcionado un aprovechamiento sobresaliente de dichos recursos, lo que conlleva de forma implícita a un ahorro de espacio y de energía (disminuyendo la necesaria refrigeración).

En la FIGURA 111 se aprecia el bajo consumo de memoria y de almacenamiento antes de que los recursos compartidos del servidor *Samba* contengan datos y el servidor de *OpenGnsys* contenga imágenes de equipos (el consumo de CPU es prácticamente despreciable).

	<i>Memoria</i>	<i>Almacenamiento</i>
<i>Servidor de DHCP</i>	148 MB	2,39 GB
<i>Servidor Proxy web</i>	143 MB	2,39 GB
<i>Servidor Samba</i>	225 MB	1,11 GB
<i>Servidor OpenGnsys</i>	655 MB	2,15 GB
TOTAL	1171 MB	8,04 GB

Figura 111. Consumo de recursos

Además, la virtualización del sistema ha permitido que dichos servicios y aplicaciones sean extremadamente portables, lo que ha facilitado rápidos despliegues. Es precisamente, a través de la puesta en marcha de dichos servicios y aplicaciones que hemos mostrado la manera de generar máquinas virtuales a partir de sistemas físicos en producción, mediante la copia y adecuación de máquinas virtuales existentes o con una la instalación desde cero.

Por supuesto, hubiera sido posible acometer este trabajo con un solo hipervisor y con un solo conmutador pero, en tal caso, no hubiera tenido sentido la administración centralizada mediante vCenter, lo que habría impedido mostrar las virtudes de la virtualización, cosa que era uno de los objetivos de este trabajo.

5.1. Logros alcanzados

En definitiva, consideramos alcanzados los objetivos de este trabajo que se resumen a continuación:

- Por un lado, hemos demostrado los extraordinarios beneficios que conlleva la virtualización de sistemas, pues hemos reducido el número de servidores, verificado la facilidad en el despliegue de máquinas virtuales ya sean de nueva planta o a partir de otros modelos existentes (físicos o virtuales) y comprobado la sencillez de las tareas de administración.
- Por otro lado, hemos empaquetado una solución para entornos docentes con Aulas TIC mediante un método muy estructurado en el **análisis**, el **diseño** y la **implementación** que lo hace trasladable a la práctica totalidad de escenarios.

5.2. Futuras líneas de trabajo

El desarrollo de presente trabajo mediante un método estructurado nos ha permitido diseccionar cada tarea. Esto permitirá y facilitará futuras mejoras mediante la sustitución de cualquiera de sus partes. Tareas como la mejora, incremento o sustitución del sistema de virtualización, el sistema de almacenamiento, el dimensionamiento de red o los servicios y aplicaciones tienen cabida pues el esqueleto ya está servido; sólo habría que realizar la configuración pertinente.

5.2.1. Respecto al sistema de virtualización

Este trabajo se ha realizado utilizando los principales productos de virtualización de la empresa líder del sector; VMware, pero sería interesante reproducir esta experiencia en su totalidad o en parte con software libre en lugar de software de pago. Existen alternativas muy interesantes como **oVirt** (www.ovirt.org), **Citrix Xen** (www.citrix.com) u **OpenStack KVM** (www.openstack.org).

También sería deseable el desarrollo de alguna solución de Backups de máquinas virtuales al margen de soluciones de pago. Como hemos visto se pueden clonar máquinas virtuales, pero es necesario un sistema que permita una política de copias programadas.

Por último, sería posible virtualizar los propios equipos de las Aulas TIC, escalando nuestra infraestructura de virtualización hacia un sistema **VDI**³¹. Virtualizar el PC de los laboratorios mediante **VDI** añadiría una capa que independizaría el software del PC en el que se ejecuta. Esto prolongaría el tiempo de vida útil de los equipos de laboratorios con el consiguiente ahorro. Además, virtualizar los PCs facilitaría la creación de entornos de test que permitirían poner en marcha nuevas aplicaciones sin impactar a la producción.

³¹ **VDI** son las siglas en inglés de Virtual Desktop Infrastructure (en español: infraestructura de Escritorios Virtuales).

Para acometer **VDI** sería necesario incorporar a nuestra infraestructura un **BROKER**, que es un gestor de conexiones entre clientes y máquinas virtuales.

El **BROKER** se encarga de la creación y destrucción de pools de máquinas virtuales bajo demanda, aunque también puede asignarlas de forma persistente a usuarios o PCs físicos. VER FIGURA 112.

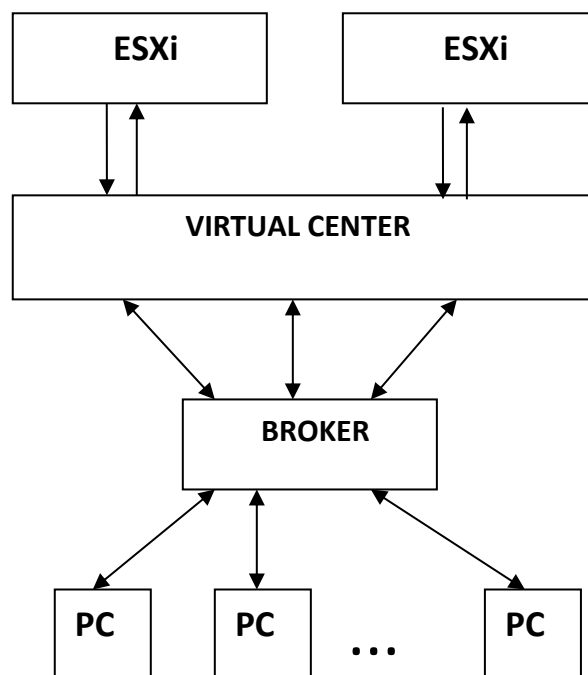


Figura 112. Esquema conceptual VDI

Algunos de los **BROKER** más interesantes a tener en cuenta son: *VMware Horizon* [20] o *VirtualCable UDS* [21]

Por supuesto, la virtualización de los PCs también requeriría de un nuevo dimensionamiento acorde con el número de equipos a virtualizar, lo que se traduciría en un crecimiento lineal de los recursos necesarios.

5.2.2. Respecto a los servicios y aplicaciones

DHCP, Samba y Squid son servicios y aplicaciones de probada eficacia que corren en millones de equipos del planeta. Respecto a **OpenGnsys** es mucho el partido que se le puede sacar en entornos docentes o empresariales, por lo sería muy interesante profundizar en el proyecto e incluso colaborar con esta interesante iniciativa de Software Libre.

6. BIBLIOGRAFÍA

- [1] Philippe Gillet. “Virtualización de sistemas de información con VMware”. Ediciones ENI. 2010.
- [2] Ryan Troy & Matthew Helmke. “VMware Cookbook”. O’Reilly. 2012.
- [3] VMware, Inc. “Virtualization Overview”. Recurso online accedido en noviembre de 2019. <https://www.vmware.com/pdf/virtualization.pdf>
- [4] Konstatin Kuminsky & Michael Bauer. “VMware vCenter cookbook”. O’Reilly. 2015.
- [5] VMware: Productos. Recurso online accedido en noviembre 2019. <https://www.vmware.com/products.html>
- [6] HPE: Productos y soluciones. Recurso online accedido en noviembre 2019. <https://www.hpe.com/es/es/home.html>
- [7] Tony Bautts, Terry Dawson y Gregor N. Purdy. “LINUX Guía para administradores de redes”. O’Reilly. 2005.
- [8] Squid. “Documentation”. Recurso online accedido en enero 2020. <http://www.squid-cache.org/Doc/>
- [9] Samba. “Documentation”. Recurso online accedido en diciembre 2019. <https://www.samba.org/samba/docs/>
- [10] OpenGnsys: Documentación. Recurso online accedido en noviembre 2019. <https://opengnsys.es/web/documentacion>
- [11] Sebastien Rohaut. “LINUX Preparación para la certificación LPIC-1”. Ediciones ENI. 2012.
- [12] VMware, Inc. “VMware Virtual Networking Concepts”. Recurso online accedido en noviembre de 2019. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/virtual_networking_concepts.pdf
- [13] VMware, Inc. “Redes de vSphere”. Recurso online accedido en diciembre de 2019. <https://docs.vmware.com/es/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-networking-guide.pdf>
- [14] VMware, Inc. “Understanding NAT”. Recurso online accedido en diciembre de 2019. https://www.vmware.com/support/ws3/doc/ws32_network21.html
- [15] VMware, Inc. “Configurar adaptadores y almacenamiento iSCSI”. Recurso online accedido en noviembre de 2019. <https://docs.vmware.com/es/VMware-vSphere/6.5/com.vmware.vsphere.storage.doc/GUID-C476065E-C02F-47FA-A5F7-3B3F2FD40EA8.html>
- [16] Oracle VM VirtualBox. “User Manual”. Recurso online accedido en enero de 2020. <http://download.virtualbox.org/virtualbox/UserManual.pdf>
- [17] VMware, Inc. “Instalar y configurar vCenter Server”. Recurso online accedido en diciembre de 2019. <https://docs.vmware.com/es/VMware-vSphere/6.7/vsphere-vcenter-server-67-installation-guide.pdf>

- [18] VMware, Inc. “Instalar y configurar VMware ESXi”. Recurso online accedido en diciembre de 2019. <https://docs.vmware.com/es/VMware-vSphere/6.7/vsphere-esxi-67-installation-setup-guide.pdf>
- [19] HPE, Inc. “HP P2000 G3 MSA SMU Reference Guide”. Recurso online accedido en diciembre de 2019. https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02558093
- [20] VMware, Inc. “Documentación de VMware Horizon 7”. Recurso online accedido en enero de 2020. <https://docs.vmware.com/es/VMware-Horizon-7/index.html>
- [21] VirtualCable, Inc. “Documentación de UDS Enterprise”. Recurso online accedido en enero de 2020. <https://www.udsenderprise.com/es/uds-enterprise/documentacion/>



UNIVERSIDAD
DE MÁLAGA

| uma.es

E.T.S. DE INGENIERÍA INFORMÁTICA

E.T.S de Ingeniería Informática
Bulevar Louis Pasteur, 35
Campus de Teatinos
29071 Málaga