ESCUELA TÉCNICA SUPERIOR DE INGENIEROS
INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Máster

IMPLEMENTACIÓN DE UN ENTORNO CLOUD EN LAS INFRAESTRUCTURAS DEL LABORATORIO DE APLICACIONES TELEMÁTICAS

(Implementing a Cloud Environment into the Laboratory of Telematics Applications Infrastructure)

Para acceder al Título de

Máster Universitario en Ingeniería de Telecomunicación

Autor: Martín Pereira Diéguez

Julio – 2017

E.T.S. DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACION

MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN

CALIFICACIÓN DEL TRABAJO FIN DE MÁSTER

Realizado por: Martín Pereira Diéguez
Directores del TFM: Alberto Eloy García Gutiérrez
José Ángel Irastorza Teja
Título: "Implementación de un Entorno Cloud en las infraestructuras del laboratorio de Aplicaciones Telemáticas"
Title: "Implementing a Cloud Environment into the Laboratory of Telematics Applications Infrastructure"

Presentado a examen el día: 18 de Julio de 2017

para acceder al Título de

MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN

Composición del Tribunal:

Presidente (Apellidos, Nombre):	Agüero Calvo, Ramón
Secretario (Apellidos, Nombre):	García Gutiérrez, Alberto Eloy
Vocal (Apellidos, Nombre):	Fanjul Vélez, Félix

Este Tribunal ha resuelto otorgar la calificación de: .....

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: El Vocal

Fdo.: El Director del TFM
(sólo si es distinto del Secretario)

Vº Bº del Subdirector

Trabajo Fin de Máster Nº
(a asignar por Secretaría)

AGRADECIMIENTOS

Me gustaría aprovechar estas líneas para agradecer a las personas que han contribuido a llegar a este momento, ya que sin su ayuda este documento no se habría hecho realidad.

A mi madre, porque madre sólo hay una.

A mi padre, que desde pequeño me enseñó que "*para poder recoger, hay que sembrar*".

A mi familia, que me brindó todo el apoyo que necesitaba.

A mi pareja, por estar tanto a las duras como a las maduras.

A mis amigos, porque ellos son El Ingrediente.

A mis tutores, por aconsejarme y guiarme por el buen camino.

A los profesores que me enseñaron y me educaron.

RESUMEN

En este trabajo se expone el procedimiento de despliegue de un entorno Cloud OpenStack utilizando dos soluciones de virtualización distintas. Citrix XenServer con Mirantis OpenStack y CentOS 7 con RDO PackStack ambas sobre servidores Huawei. Se integra dicha infraestructura en el Laboratorio de Aplicaciones de Telemáticas y se configuran los equipos de red para permitir el acceso desde el Laboratorio de Telemática. Además, se configuran el direccionamiento de los servidores para que la interfaz web de gestión de OpenStack sea accesible a través de las direcciones IP públicas de la Universidad de Cantabria. Con esta plataforma se pretende implementar un Cloud privado que permita la creación de laboratorios virtuales para facilitar el desarrollo de los conocimientos de los alumnos en un entorno aislado y seguro además de ser exportable a diferentes campos universitarios como la seguridad o actividades de cómputo en la Nube.

Palabras clave: Virtualización, Cloud, OpenStack, Citrix, XenServer, Mirantis, PackStack.

ABSTRACT

This work presents the deployment procedure of an OpenStack Cloud environment using two different virtualization solutions. Citrix XenServer with Mirantis OpenStack and CentOS 7 with RDO PackStack both on Huawei servers. That infrastructure is integrated into the Laboratory of Telematics Applications and network equipment is configured to allow access from the laboratory of Telematics. Networking is also configured in order to the OpenStack management web interface is accessible through the public IP addresses of the University of Cantabria. This platform aims to implement a private cloud that allows the creation of virtual laboratories to facilitate the development of students' knowledge in an isolated and secure environment as well as being exportable to different campus activities such as security or Cloud Computing.

Keywords: Virtualization, Cloud, OpenStack, Citrix, XenServer, Mirantis, PackStack.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Las soluciones de virtualización son una forma muy rentable de ofrecer servicios, de fácil gestión y despliegue. Es por eso que cada vez más empresas están optando por desplegar sus propias Nubes privadas en sus entornos virtualizados. Según un informe publicado en Forbes [1], es más barato desplegar un entorno Cloud privado que utilizar *Amazon Web Services* (AWS).

El despliegue de una Nube privada en una organización proporciona ventajas en la administración de recursos y ofrece un mejor control de la seguridad y la calidad de servicio. Un entorno de producción privado de este tipo facilita la integración con otros servicios o infraestructuras ya existentes, pero se necesita una mayor inversión inicial que se amortiza rápidamente.

La inversión en entornos Cloud crece cada año debido al aumento de la potencia de cómputo y la reducción del precio de los servidores físicos. La inversión en Nubes privadas locales representarán el 62,3% del gasto en infraestructura de TI de nube privada y crecerá un 13,1% en 2017 y así año tras año [2].

La tendencia de almacenamiento está cambiando y el medio más utilizado para este propósito es el Cloud. Además el *Cloud Computing* o Computación en la Nube se ha convertido en los últimos años en una de las tecnologías más populares y desplegadas a escala mundial como se refleja en la previsión de Salesforce [3].

OpenStack es un software de código abierto para construir Nubes públicas y privadas. Está desplegado en multitud de centros de datos a escala mundial y es respaldado por los principales jugadores en este campo. Además, es la infraestructura de Cloud privado por excelencia y ofrece a los usuarios un servicio para el despliegue de sistemas, aplicaciones o servicios.

Una de las ventajas de las que una institución como la Universidad puede beneficiarse es la virtualización de escritorio. Al utilizar equipos de tamaño reducido que se conectan por red a servicios de escritorio remoto (*thin-clients*) en vez de ordenadores de sobremesa físicos se consigue, a la hora de equipar un laboratorio docente, un gran ahorro tanto en hardware como en licencias y una reducción del consumo eléctrico. El sistema operativo y las aplicaciones del equipo se migrarían a una máquina virtual del servidor que permitiría al alumno acceder a su sesión de laboratorio para revisar prácticas ya realizadas, continuar donde se quedó o probar otras funciones sin necesidad de estar en horario docente.

Estos entornos son realmente necesarios para temas relacionados con la ciberseguridad, una máquina virtual podría monitorizar el tráfico de una red e identificar amenazas que pudiesen provocar perjuicios a los equipos de dicha red o robos de información. Como el servicio de red de OpenStack está basado en SDN (*Software Define Networks*) es posible definir un servicio de firewall (FWaaS) que filtre conexiones no autorizadas sin la necesidad de un firewall físico que se caracteriza por su elevado precio.

1.1. Motivación y objetivos

El presente trabajo tiene su origen en la necesidad de realizar un estudio de Técnicas Forenses en entornos Cloud. Con esta premisa se comenzó realizando un proceso de búsqueda de información del estado del arte en el que se concluyó que el despliegue de herramientas de este tipo en un entorno Cloud era, a priori, laborioso pero alcanzable.

De acuerdo con esta primera conclusión, la necesidad de tener un entorno de desarrollo basado en Cloud era un requisito fundamental para la continuación del trabajo. Las condiciones originales del proyecto se encontraban encuadradas en una secuencia de sendos trabajos desarrollados en el tiempo. En el

primero, realizado por Yassine Bouchdoug y titulado "Comparison of virtualization methods", se llegaba a la conclusión de que XenServer y OpenStack eran opciones ideales para el desarrollo de una nube privada en el entorno de la educación. Como resultado, otro alumno de intercambio, Henning Mende, dentro de su período de Erasmus, procedió colaborar en la instalación sugerida en el anterior trabajo dentro los Laboratorios Docentes del Grupo de Ingeniería Telemática, haciendo uso de los equipamientos para virtualización de equipos, que habían sido financiados por el Proyecto DECAMP. Precisamente este trabajo era el punto de partida de la propuesta original. Sin embargo, el despliegue del entorno OpenStack en los dos servidores bajo licencia Citrix XenServer daba continuos problemas, haciendo imposible su uso.

Llegados a este punto hubo de tomarse una decisión que afectó directamente al desarrollo del actual trabajo. El despliegue del entorno Cloud viene motivado por su aplicación en la formación de los alumnos en temas específicos relacionados con el Cloud y la seguridad, pero especialmente porque esta infraestructura es un complemento formativo de carácter práctico que puede ser utilizado en casi todas las asignaturas de la mención de Telemática de la titulación de Grado, así como las relacionadas que aparecen en el Master. Yendo más allá, podría ser incluso exportable como servicio de cálculos complejos para cualquier otra rama que trabaje con grandes tareas de cómputo como simulaciones electromagnéticas u optimizaciones de diseños electrónicos.

Como consecuencia, el principal objetivo del trabajo pasó a ser el de evaluar la viabilidad de la infraestructura de Cloud basada en XenServer y OpenStack existente.

De acuerdo con los problemas detectados antes del comienzo de esta tarea, el siguiente objetivo consistió en el análisis de soluciones alternativas a la existente sin dejar de lado las opciones de código abierto.

Como objetivo adicional, aunque directamente relacionado con las premisas anteriores, el resultado debe ser una infraestructura funcional, debidamente integrada en el Laboratorio de Aplicaciones Telemáticas (Laboratorio Docente 1), que permita el acceso desde el Laboratorio de Telemática (Laboratorio Docente 2) y ofrezca acceso al resto de la comunidad universitaria gracias al direccionamiento público perteneciente a la Universidad de Cantabria.

1.2. Estructura del documento

La estructura del trabajo se ha dividido en seis capítulos que se describen a continuación:

Capítulo 1: Introducción. Este capítulo, en el que se realiza una introducción que describe tanto las motivaciones que han propiciado la realización del trabajo, como los objetivos que se persiguen.

Capítulo 2: Conceptos Teóricos. Presenta el concepto de virtualización, cómo surge, qué objetivos persigue, su terminología y las arquitecturas existentes. Se exponen las características de la solución de virtualización de Citrix XenServer y se compara con otros existente. Además, se realiza un acercamiento al concepto de Cloud, sus tipos, y se detalla el funcionamiento de OpenStack y los módulos adicionales que lo componen.

Capítulo 3: Infraestructura del Laboratorio. El tercer capítulo muestra la infraestructura disponible, los equipos y conexiones del Laboratorio donde se encuentran los servidores, así como una descripción de las acciones que hay que llevar a cabo en ellos antes de la implementación.

Capítulo 4: Fase I: Instalación del hipervisor. Los primeros trabajos son expuestos aquí, incluyendo la instalación el hipervisor, los problemas encontrados y las soluciones propuestas para configurar la virtualización de Citrix. El capítulo incluye unas breves conclusiones asociadas a esta fase.

Capítulo 5. Fase II: Instalación de OpenStack. Una vez superados los problemas encontrados en el hipervisor, este capítulo expone las opciones propuestas para el despliegue del entorno OpenStack, así como su resultado, en forma de breves conclusiones.

Capítulo 6. Fase III: Instalación de CentOS 7 con PackStack. Como resultado de las anteriores fases, este capítulo recoge los procedimientos seguidos para instalar el sistema operativo CentOS en uno de los servidores y el despliegue del entorno OpenStack, utilizando la herramienta PackStack, de forma que se integre en la estructura del laboratorio. Esta es una alternativa que rompe con la idea original, por lo que al final del capítulo se incluyen sus correspondientes conclusiones.

Capítulo 7: Conclusiones y Líneas Futuras. Finalmente, en este capítulo, se hace balance global del trabajo, aportando ideas acerca de las posibles mejoras a realizar a corto y medio plazo.

2. CONCEPTOS TEÓRICOS

Este capítulo contiene un acercamiento general al concepto de virtualización, así como su historia, objetivos, la terminología utilizada en este campo y las ventajas y desventajas de dicha tecnología. Se exponen los tipos de hipervisores y el caso concreto de los componentes de la solución de virtualización Citrix XenServer, que además es comparada con otras soluciones existentes. Finalmente se hace una introducción al concepto de Cloud y se detalla el funcionamiento de OpenStack como infraestructura de Cloud Computing.

2.1. Virtualización

La virtualización es la emulación de una o más estaciones de trabajo o servidores en un único equipo físico. En otras palabras, es la emulación de hardware dentro de una plataforma software. Este tipo de virtualización se refiere a veces como virtualización total y permite a un equipo físico compartir sus recursos entre diferentes entornos. Esto significa que un solo equipo puede actuar como varios equipos diferentes. [4]

La tecnología de virtualización es una manera de hacer funcionar a un equipo físico como si se tratara de dos o más equipos, cada equipo no físico o "virtualizado" posee la misma arquitectura básica que un equipo físico genérico, existiendo varias formas de hacer esto [5], cada una con sus pros y sus contras, como se verá más adelante.

Aunque la tecnología de virtualización es un concepto que existe desde hace muchos años, recientemente ha tomado un papel muy relevante. Una de las razones de este hecho es el aumento de la potencia de cómputo y los avances en la tecnología hardware, posibilitando la compartimentación de los recursos hardware en forma de equipos virtualizados con funciones especializadas.

Para que un equipo físico pueda comportarse como varios equipos independientes, las características de cada hardware físico individual deben recrearse mediante el uso de software especializado, denominado abstracción., pero que en la literatura y especialmente en los productos comerciales suele confundirse con el hipervisor, el cual puede aparecer o no. Esta capa software proporciona un método de comunicación común para que los controladores (del hardware virtual) y el resto del software (sistema operativo) se comuniquen con el hardware real en un formato unificado. Esto hace que escribir el software y los controladores sea más sencillo dado que los desarrolladores no tienen que escribir software a medida para cada tipo de equipo en el que quieran ejecutar su código. La abstracción, en lo que se refiere a virtualización, es la representación de un conjunto de dispositivos hardware que son gestionados por software. Básicamente se trata de software que parece y actúa como hardware. La tecnología de virtualización permite la instalación de un sistema operativo en un hardware que realmente no existe.

Con todo ello, la virtualización permite que los recursos de un equipo se dividan o compartan entre múltiples entornos simultáneamente. Estos entornos pueden cooperar o ser totalmente independientes unos de otros, de forma que un único entorno puede ser consciente o no, de que está siendo ejecutado en un entorno virtual. Estos entornos son más conocidos como máquinas virtuales (*VMs*) y tienen su propio sistema operativo (Linux, Windows, etc.) instalado. Estas instalaciones del sistema operativo se conocen como sistemas operativos invitados (*Guest SOs*). Las instrucciones de una máquina virtual se pasan directamente al hardware físico que permite al entorno funcionar más rápido y de forma más eficiente que con la emulación. Las instrucciones más complejas deben ser capturadas e interpretadas con el fin de garantizar la adecuada compatibilidad con el hardware físico. [5]

2.1.1. Historia de la virtualización

La tecnología de virtualización existe desde hace más tiempo de lo que la mayoría de la gente piensa. Pero es ahora cuando está empezando a ser ampliamente utilizada debido al aumento masivo de los recursos de hardware. El concepto de la virtualización fue vislumbrado en la década de 1960. Posteriormente fue implementado por IBM para ayudar a dividir sus enormes máquinas *mainframe* en máquinas virtuales separadas. La motivación de este hecho era maximizar la eficiencia de las máquinas mainframe. Antes de que llegara la virtualización, un mainframe sólo podía trabajar en un proceso en cada momento y eso era desperdiciar recursos. La virtualización se introdujo para solucionar este problema, de forma que dividía los recursos hardware de las máquinas mainframe en entidades separadas. Con ello, una sola máquina mainframe física podría ejecutar múltiples aplicaciones y procesos al mismo tiempo.

Como la arquitectura x86 se convirtió en el conjunto de instrucciones dominante en la informática durante la década de 1980, y el modelo cliente-servidor se estableció para permitir la computación distribuida, la necesidad de la virtualización ya no era realmente necesaria. El principal motivo fue que el modelo cliente-servidor permitía a los administradores conectar entre sí muchas estaciones de trabajo de bajo coste. Los recursos se podrían distribuir entonces entre estas estaciones de trabajo usando menos servidores de gran potencia. El uso masivo de sistemas operativos basados en Windows y Linux durante la década de 1990 consolidó aún más la arquitectura x86 y el modelo cliente-servidor, como el modelo dominante en la informática. [4]

Sin embargo, nadie podría haber imaginado el crecimiento masivo en el uso de la tecnología informática y esto creó nuevas demandas de infraestructura TI y como es de esperar, nuevos problemas. Algunos de estos problemas incluyen: [4]

- Baja utilización de la infraestructura
- Incremento de los costes de la infraestructura física
- Incremento de los costes de gestión y administración
- Poca protección frente a desastres
- Coste elevado del mantenimiento y de los equipos del usuario final

La solución más viable para resolver los problemas mencionados fue la virtualización de hardware y así en 1999 VMware introdujo la primera aplicación de virtualización para sistemas basados en x86. Las máquinas de hoy en día pueden dividir sus recursos hardware al igual que hacían las máquinas mainframe durante la década de 1960, lo que permite un uso más eficiente de la potencia de cómputo y los recursos hardware.

2.1.2. Objetivos de la virtualización

Pese a la diferencia temporal entre los escenarios de aplicación de la virtualización original y actual, los objetivos sobre los cuales se fundamentan la mayor parte de soluciones se han mantenido en el tiempo, si bien es de lógica su adaptación a los avances tecnológicos sufridos. Cabe destacar:

- **Aumentar el uso de los recursos hardware**:

  Actualmente los servidores han mejorado tanto, que sólo se utiliza entre un 5-15% de los recursos hardware de los mismos. [6] Esto es un problema similar al que tenían originalmente las máquinas mainframe en la década de 1960, cuando se desperdiciaba la mayor parte de sus

recursos hardware. Al permitir que un servidor físico ejecute software de virtualización, los recursos del servidor se utilizan de forma más eficiente, lo que puede reducir en gran medida los costes de gestión y operación. Por ejemplo, si una organización utiliza 4 servidores para 4 servicios diferentes, esos 4 servicios podrían operar como servidores virtuales en un único servidor físico en lugar de tener 4 de ellos.

- **Reducir los costes de gestión y mantenimiento:**

Debido al uso de una gran cantidad de servidores físicos hoy en día, la mayoría de las organizaciones tienen que lidiar con cuestiones como el espacio, la energía y la refrigeración. Esto es algo que deja huella en el medio ambiente en forma de aumento de la demanda de energía o la construcción de nuevos edificios para albergar los equipos, algo que además es muy costoso para las empresas. Utilizando una infraestructura virtualizada, las empresas pueden ahorrar grandes cantidades de dinero y reducir así el impacto ambiental que generan. [6]

- **Mejorar la flexibilidad:**

El hecho de ampliar el número de servidores en una empresa es, a menudo, un proceso largo y costoso. La organización debe situar físicamente las máquinas, configurarlas, actualizarlas, etc. Este es un proceso que consume tiempo y desperdicia los recursos de las empresas tanto directa como indirectamente. Las máquinas virtuales se pueden configurar fácilmente sin coste de hardware adicional, sin necesidad de más espacio físico y sin esperas, ya que el software de gestión de máquinas virtuales facilita el trabajo de los administradores a la hora de configurarlas. [6]

- **Mejorar la seguridad y reducir la indisponibilidad:**

Generalmente cuando falla una máquina física, todo su software se vuelve inaccesible. El contenido de la máquina no está disponible y esto genera un tiempo de inactividad hasta que se soluciona el problema. Las máquinas virtuales son entidades separadas entre sí, por lo tanto, si una de ellas falla o tiene un virus, están completamente aisladas del resto de software en esa máquina física, incluyendo las otras máquinas virtuales. Esto aumenta la seguridad ya que es una forma de contener problemas.

Para finalizar, es especialmente destacable, el hecho que las máquinas virtuales no son dependientes del hardware. Esto significa que, si un servidor falla debido a un problema de hardware, las máquinas virtuales almacenadas en ese servidor se pueden migrar a otro. Su funcionamiento puede ser restaurado en instantes concretos anteriores al actual, como si nada hubiera pasado, independientemente del estado en el que se encuentre el servidor original. [6]

2.1.3. Terminología de virtualización

Puesto que la terminología utilizada en este tipo de soluciones, resulta en muchos casos muy especializada, la Tabla 1 recoge una lista de los términos más utilizados a lo largo de este documento, con el fin de facilitar la lectura y comprensión del mismo.

Tabla 1 – Terminología de la virtualización

Concepto	**Descripción**
Virtualización completa	Describe el proceso que permite a un sistema operativo ser instalado en un entorno virtual aislado, es decir, una máquina virtual. Se emulan todos los recursos hardware de una máquina virtual, mientras que los recursos físicos son compartidos entre una o más máquinas virtuales.
Virtualización parcial	Es un tipo de virtualización que simula parcialmente el hardware físico de una máquina. Debido a este hecho, las máquinas parcialmente virtualizadas no pueden ejecutar sistemas operativos completos. Sin embargo la virtualización parcial es más fácil de implementar que la virtualización total y muchas aplicaciones se pueden ejecutar en una máquina parcialmente virtualizada.
Virtualización asistida por hardware	Esto es similar a la virtualización completa, la única diferencia es que este tipo de virtualización no se basa únicamente en software y es asistida por hardware (generalmente por el procesador).
Emulación	Implica el uso de software para ejecutar sistemas operativos o aplicaciones en hardware que no fueron originalmente concebidos para ello.
Máquina virtual	Se trata de un entorno virtual aislado dentro de un sistema operativo anfitrión. Todo el hardware de las máquinas virtuales como procesador, memoria, discos, RAM, etcétera, son emulados y administrados mediante el uso de una aplicación de virtualización. Esta aplicación de virtualización está instalada en el SO anfitrión o en el hardware dependiendo del tipo de hipervisor, mientras que el sistema operativo invitado se instala dentro de máquinas virtuales.
Sistema operativo anfitrión	Este es el sistema operativo que está instalado en una máquina física y que alberga una o más máquinas virtuales.
Sistema operativo invitado	Este es el sistema operativo que está instalado en una máquina virtual o una partición. Al usar la virtualización, el sistema operativo invitado puede ser diferente del anfitrión.
Hipervisor o Monitor de Máquina Virtual (VMM)	Es una capa simulada entre un sistema operativo invitado y el hardware físico de un equipo. Atiende las peticiones hardware del sistema operativo invitado de una máquina virtual y las responde de la misma forma que lo haría el hardware físico.

Concepto	Descripción
Entorno *Bare Metal*	Describe el software de virtualización que se instala directamente sobre el hardware físico. Se instala en lugar de un sistema operativo. Ej.: VMWare ESXi, Xen o Microsoft Hyper-V Server
Entorno *Hosted*	Describe el software de virtualización que se instala sobre el sistema operativo del host. Ej.: VirtualBox, VMWare Server, Oracle VM
Grid Computing	Este es un modelo relativamente nuevo basado en la virtualización que implica el uso de la potencia de procesamiento de un gran número de máquinas geográficamente separadas pero conectadas en por red para realizar tareas complejas en paralelo. El Grid Computing es utilizado a menudo por instituciones científicas que aprovechan la potencia de cómputo no utilizada de las máquinas de los usuarios que ceden el uso de este recurso.
Copia de seguridad en caliente (Live Backup)	Se trata de copiar una máquina virtual completa con fines de respaldo mientras está funcionando.
Migración en caliente (Live Migration)	Se trata de copiar una máquina virtual completa a otra máquina en el mismo nivel que el SO anfitrión. Esto se realiza a menudo cuando un servidor físico necesita ser actualizado o apagado por mantenimiento.
Particionado	Esto implica crear múltiples "discos duros virtuales" de un disco duro físico, las particiones. Cada partición puede tener el mismo sistema operativo anfitrión instalado, pero a diferencia de las máquinas virtuales, no son independientes uno del otro. Esto significa que el contenido de las particiones, es accesible por un usuario que haya iniciado sesión en el sistema operativo anfitrión de una partición distinta.
Partición	Se trata de un disco duro virtual que ha sido creado desde un disco duro físico, que puede tener un sistema operativo anfitrión instalado en él.
RAID (Redundant Array of Independent Disks)	RAID es una forma de virtualización ya que utiliza varios discos, para simular un disco más grande.

Concepto	Descripción
Migración P2V (Físico a Virtual)	Describe el proceso de mover un sistema operativo completo junto con todas sus aplicaciones, de una máquina física a una máquina virtual (o partición). Este tipo de migración se lleva a cabo sin tener que reinstalar nada, por lo tanto, es bastante eficiente. P2V es lo contrario de migración V2P (Virtual a físico).
Migración V2P (Virtual a Físico)	Esto es exactamente lo contrario de una migración P2V. Se trata de mover todo un sistema operativo junto con todas sus aplicaciones de una máquina virtual a una o más máquinas físicas, sin tener que reinstalar nada.
Migración V2V (Virtual a Virtual)	Similar a una migración P2V y V2P, implica copiar el sistema operativo y aplicaciones de una máquina virtual a otra, sin tener que reinstalar nada.
Memoria virtual	Describe el proceso en el que los datos se almacenan de forma contigua a pesar de que pueden estar dispersos entre la RAM y el disco duro.

2.1.4. Ventajas y desventajas de la virtualización

Actualmente el uso de la virtualización está asociado a un conjunto de ventajas [7], más o menos relacionadas con los objetivos que dichas soluciones buscan, tal como observábamos en un apartado anterior:

- Minimiza los gastos en hardware y el espacio físico necesario, debido a la reducción del número de equipos físicos.
- Permite la recuperación frente a desastres y minimiza el MTTR (tiempo medio de recuperación) ya que se pueden crear copias exactas de las máquinas virtuales y restaurarlas en otro equipo físico.
- Reducción del consumo energético, tanto en la alimentación de los equipos como el empleado en su refrigeración.
- Permite balancear la carga de servicios entre máquinas virtuales.
- Mantenimiento de los servidores centralizado, la consola de gestión proporciona a los administradores una interfaz independiente del sistema operativo que les permite gestionar todas las máquinas virtuales.
- Permite realizar pruebas de software sin interrumpir el funcionamiento de otros servicios.
- Rápido despliegue de servidores, no es necesaria instalación física de un equipo ni cablear para tener un servicio funcionando.

Sin embargo, no todo son ventajas, ya que los inconvenientes [8] siempre aparecen cuando se particulariza en casos concretos:

- Pérdida de rendimiento. Dado que el hipervisor introduce una capa intermedia en la gestión del hardware para gestionar las peticiones de acceso y la concurrencia al mismo, el rendimiento de la máquina virtual se ve afectado
- Repartir recursos. El servidor es compartido por varios servidores virtuales, por eso es importante distribuir correctamente los recursos.
- Soporte del hardware. No es posible utilizar hardware que no esté gestionado o soportado por el hipervisor, ya que el software de virtualización impone una serie de dispositivos virtuales.
- Aceleración de video por hardware. No se disponen de efectos 3D si el equipo no tiene tarjeta gráfica y soporta la virtualización VT-d.
- Anfitrión como único punto de fallo. La avería del servidor anfitrión de virtualización afecta a todas las máquinas virtuales alojadas en él, por eso se recomienda utilizar sistemas de HA (Alta disponibilidad).
- La elección del sistema operativo anfitrión es crítica si se piensa migrar en el futuro.
- Desaprovechamiento de recursos. Crear máquinas virtuales innecesarias tiene un coste en ocupación de recursos, principalmente en espacio en disco, RAM y capacidad de proceso.

Como se observa, ambas listas nos llevan a la conclusión de que las soluciones de virtualización suelen estar adaptadas a entornos de aplicación específicos, de acuerdo con sus necesidades y requisitos, en las que se va a intentar balancear los pros y contras en modo adhoc.

2.2. Hipervisor

El hipervisor es la capa de abstracción que existe entre el sistema operativo invitado y el hardware físico de un equipo. Atiende a las peticiones hardware de una máquina virtual y las gestiona de la misma forma que lo haría el hardware físico. La arquitectura de Virtualización depende del tipo de hipervisor utilizado para conseguir la virtualización.

Existen tres tipos principales de hipervisores en el mercado: [9]

- **Hipervisores de tipo 1:** También llamados nativos, *unhosted* o *bare-metal*, en ellos el hipervisor se ejecuta directamente sobre el hardware físico. El hipervisor se carga antes que los sistemas operativos invitados y todos los accesos directos a hardware son controlados por él. La Figura 1 muestra la arquitectura de virtualización utilizando un hipervisor tipo 1.

  Aunque esta es la aproximación clásica y más antigua de la virtualización por hardware, en la actualidad las soluciones más potentes de la mayoría de fabricantes usan este enfoque. Es el caso de Microsoft Hyper-V, Citrix XenServer, VMWare ESXi-Server, KVM.

  Es muy frecuente que al resto de hipervisores, en general, se les aplique el término VMM (Monitores de máquina virtual), mientras que el término “hypervisor” se reserva para los hipervisores de este tipo.

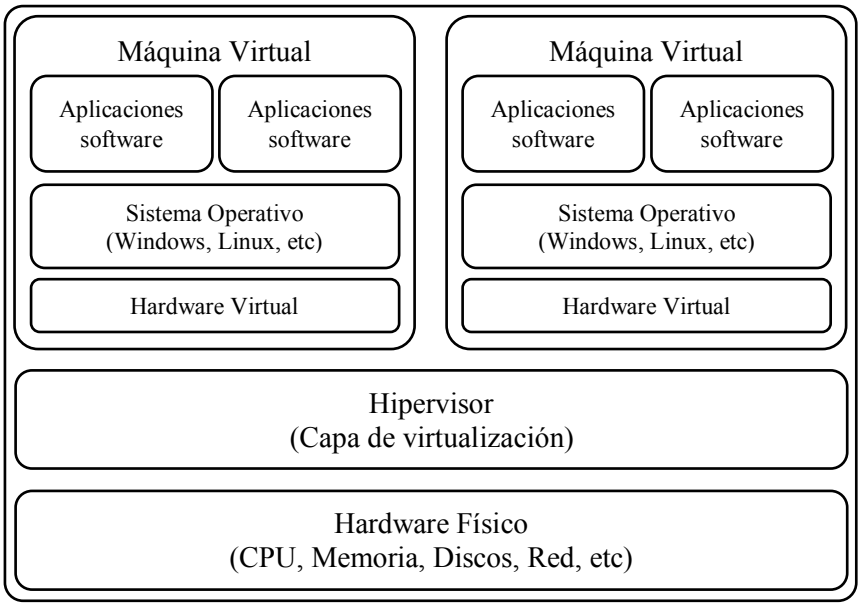


Figura 1 – Arquitectura de virtualización utilizando un hipervisor de tipo 1

- **Hipervisores de tipo 2:** También llamados *hosted*, en ellos el hipervisor se ejecuta en el contexto de un sistema operativo completo, el cual se carga antes que el hipervisor. Las máquinas virtuales se ejecutan en un tercer nivel, por encima del hipervisor. La Figura 2 muestra la arquitectura de virtualización utilizando un hipervisor tipo 2.

  Son típicos de escenarios de virtualización orientada a la ejecución multiplataforma de software, como en el caso de CLR de .NET o de las máquinas virtuales de Java.

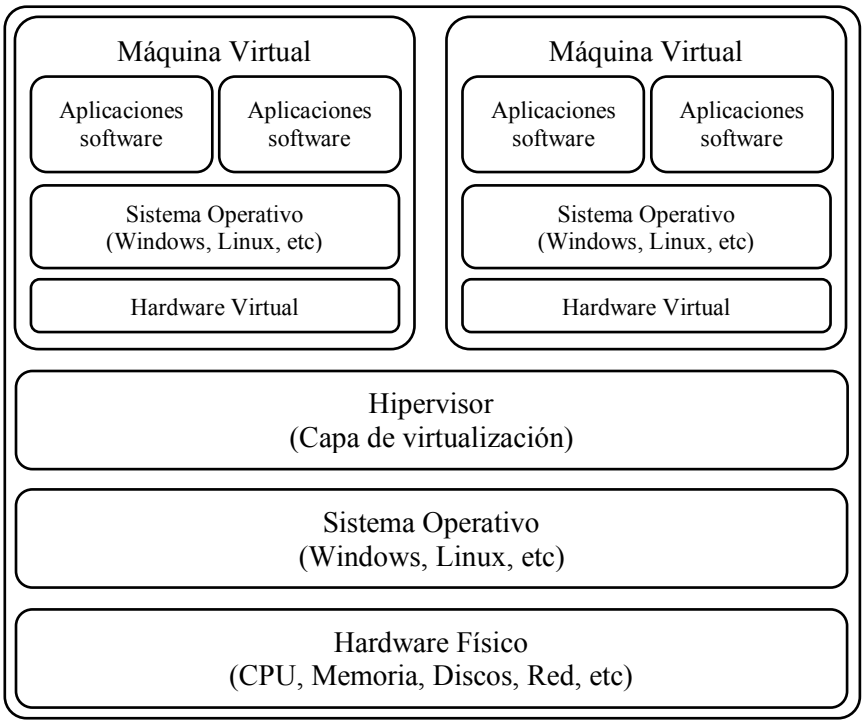


Figura 2 – Arquitectura de virtualización utilizando un hipervisor de tipo 2

- **Hipervisores híbridos:** en este modelo tanto el sistema operativo anfitrión como el hipervisor interactúan directamente con el hardware físico. La Figura 3 muestra la arquitectura de virtualización utilizando un hipervisor híbrido.

  Las máquinas virtuales se ejecutan en un tercer nivel con respecto al hardware, por encima del hipervisor, pero también interactúan directamente con el sistema operativo anfitrión.

  Es la aproximación usada en Microsoft Virtual PC, Microsoft Virtual Server, Parallels, VirtualBox, VMWare Server…

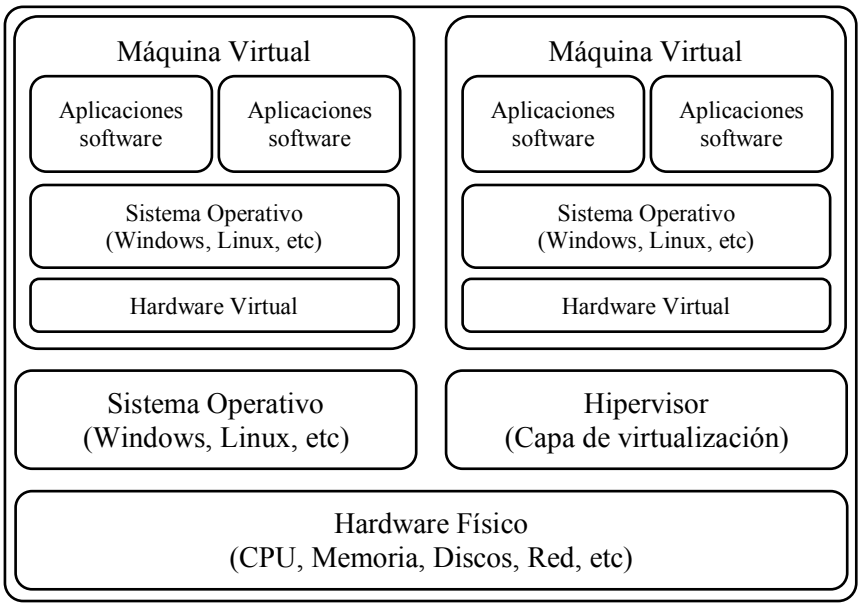


Figura 3 – Arquitectura de virtualización utilizando un hipervisor híbrido

2.2.1. Citrix XenServer y el hipervisor Xen

Dentro de las soluciones basadas en hipervisores de tipo 1, XenServer es una solución de virtualización preconfigurada por Citrix y basada en el hipervisor Xen. Es una solución gratuita que se puede instalar en un equipo con capacidad de virtualización para desplegar un entorno Cloud.

El hipervisor Xen es la base de todas las plataformas de virtualización basada en Xen y, como VMware ESXi y Microsoft Hyper-V, es un hipervisor *bare-metal*. Esto significa que el primer código que comienza en la máquina es el hipervisor y que no se requiere un sistema operativo de propósito general para administrar el sistema.

Xen fue originalmente diseñado en la Universidad de Cambridge y forma el núcleo del hipervisor de XenServer, pero también el de Oracle VM y puede utilizarse como un hipervisor opcional dentro de las principales distribuciones Linux como CentOS, Debian y SUSE Linux Enterprise Server. Además, Xen ha sido muy utilizado en el que es posiblemente el despliegue más famoso de Amazon, proporcionando la base de su oferta de productos Amazon Web Services (AWS). [10]

Xen se desarrolla activamente dentro del Xen Project, un proyecto colaborativo de la Linux Foundation donde se beneficia de las contribuciones y la participación activa de más de una docena de organizaciones. Esta amplitud de desarrollo asegura que la tecnología de hipervisor Xen se actualiza con el cambio de tendencias en las operaciones de los *datacenters* mientras se concentran en ofrecer servicios de hipervisor.

Es importante tener en cuenta que cada producto basado en Xen elige la versión del hipervisor que soporta y las características que integra dicha versión. Por ello, es normal que no se utilicen ciertas características presentes en Xen en otras soluciones.

2.2.1.1. XAPI Toolstack

El hipervisor Xen simplemente realiza la administración de máquinas virtuales y necesita algún tipo de herramientas para controlar su funcionamiento. Las herramientas modernas incluyen *libvirt*, una biblioteca para la gestión de la virtualización, y XAPI, la API de gestión de Xen. Al implementar una solución basada en Xen, es posible elegir las herramientas que mejor se adapten a las necesidades del producto. Sin embargo, debido a que XenServer es una solución de Citrix, la herramienta en cuestión ya viene incorporada como *XAPI Toolstack*. Ésta es parte integral de la solución de virtualización XenServer y no se puede cambiar por otra herramienta de gestión del hipervisor Xen.

XAPI proporciona interfaces y las implementaciones de todas las funciones esperadas para realizar operaciones de máquinas virtuales, administración de hosts, almacenamiento de información y configuración de red. Cuando dos o más hosts de XenServer se agrupan en un *pool*, XAPI proporciona controles adicionales sobre ellos y sus operaciones. XAPI es capaz de administrar varios hosts como un conjunto y es funcionalmente similar a libvirt. Por último, cabe resaltar que XAPI expone su API en algunos de los lenguajes más populares tales como Java, Java-Script, PowerShell, Python y C++. [11]

2.2.1.2. Dominio de control dom0

Es posible llegar a la idea errónea de que XenServer es Linux porque el proceso de instalación se parece a un entorno estándar de Linux. El gestor de arranque utilizado es *extlinux* y el instalador utiliza un diálogo amigable para una instalación interactiva. La instalación termina en una interfaz de un sistema operativo Linux con la sesión iniciada como el usuario con privilegios denominado *root*.

Tras la instalación arranca el hipervisor Xen. Éste crea la instancia de una máquina virtual con privilegios conocida como el dominio de control o, como se le conoce comúnmente, dom0. Este dominio de control es una máquina virtual Linux con un *kernel* personalizado y basada en un CentOS modificado con un diseño muy compacto. Desde un punto de vista administrativo, dom0 puede verse como una máquina virtual con altos privilegios responsable de las operaciones fundamentales en los sistemas de virtualización basados en Xen.

Dom0 es por tanto Linux, pero XenServer no, por eso no es un requisito ser un experto de Linux para configurar XenServer. No es habitual tener que realizar cambios en los archivos de configuración de Linux dentro de dom0. El control de dominio de XenServer tiene una interfaz de línea de comandos con una sintaxis propia que permite una alta versatilidad.

Hay que reseñar que XenServer tiene desactivado el gestor de paquetes de CentOS denominado *yum*. El dominio de control de XenServer se ha modificado para satisfacer las necesidades de una plataforma de virtualización, y como resultado, la instalación de paquetes que no hayan sido explícitamente diseñados o certificados para XenServer podrían desestabilizar o reducir la escalabilidad y el rendimiento del host.

2.2.1.3. Arquitectura

La arquitectura de XenServer se basa en tres elementos de hardware principales: Cómputo, Red y Almacenamiento como se muestra la Figura 4.

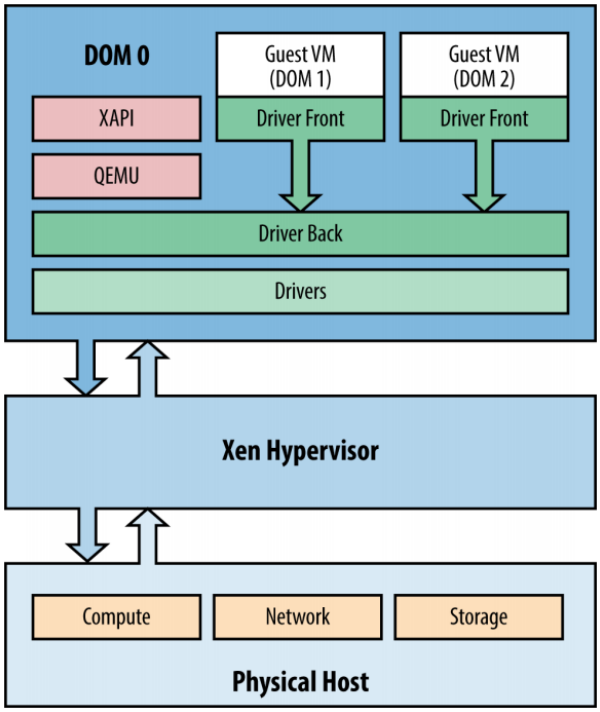


Figura 4 – Arquitectura XenServer [12]

Las flechas del diagrama reflejan cómo se realizan los accesos entre los diferentes elementos. El primer elemento de software es el hipervisor, el cual se carga desde el almacenamiento local y se comunica con el *Compute* para proveer los servicios de las máquinas virtuales.

La primera máquina virtual se corresponde con dom0, que como ya se señaló es el dominio con privilegios. Los dominios sin privilegios se conocen como domU, o más comúnmente, "máquinas virtuales invitadas o *guests VMs*", o simplemente máquinas virtuales. Todos los dominios son controlados por el hipervisor, que proporciona una interfaz para los servicios de cómputo. Las máquinas virtuales, necesitan algo más que cómputo, y es el dom0 quien proporciona acceso al hardware a través de controladores de dispositivo de Linux. El controlador de dispositivo se comunica con un proceso de XenServer, así proporciona un dispositivo virtual utilizando un modelo de *split-driver*. Esta interfaz se llama modelo de *split-driver* porque existe una porción del driver dentro de dom0 (*back-end*), mientras el resto del controlador se encuentra en el cliente (*front-end*) como refleja la Figura 5. [13]

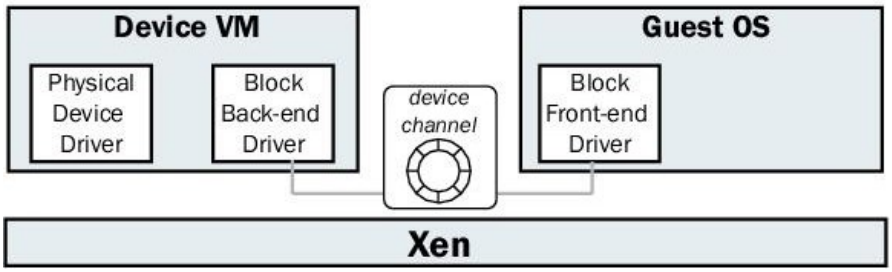


Figura 5 – Acceso a dispositivos en Xen [13]

Este modelo de dispositivo es soportado por diversos procesos incluyendo el proyecto de emulador rápido (QEMU, *Quick Emulator*) [14] (véase Figura 4). Dado que las máquinas HVM (*Hardware Virtual Machine*) y las PV (*Para-Virtualized*) invitadas no contienen controladores de para-virtualización, QEMU y QEMU-dm emulan aspectos de componentes de hardware como la BIOS, además de proporcionar acceso de red y disco. La unión de dichas tecnologías es PVHVM (*Para-*

Virtualized Hardware Virtual Machine) que permite ejecutar las nuevas versiones de las distribuciones más famosas de Linux (Ubuntu, Debian, CentOS, etc.) con controladores para-virtualizados sin necesidad de utilizar QEMU mejorando sustancialmente el rendimiento.

2.2.1.4. Tipos de máquinas virtuales soportadas

Existen tres tipos diferentes de máquinas virtuales en función del tipo de virtualización que el hipervisor es capaz de ofrecer al sistema operativo invitado:

- **Máquina Virtual Hardware (HVM)**

HVM requiere extensiones especializadas presentes en los procesadores modernos de Intel y AMD. Estas extensiones son conocidas como Intel VT-x o AMD-V y permiten que la CPU física capture ciertos conjuntos de instrucciones de CPU que los sistemas operativos usan normalmente para interactuar con un servidor bare-metal. Si fuese el sistema operativo quien ejecutase dichas instrucciones, estando virtualizado, podría afectar a otras máquinas virtuales.

HVM se utiliza comúnmente al virtualizar un sistema operativo, como Microsoft Windows, el cual no es posible modificar para que sea consciente de que está siendo virtualizado. Debido a que los huéspedes HVM no tienen conciencia de su virtualización, se utilizan normalmente controladores de dispositivo emulados. Con el fin de mejorar el rendimiento de las operaciones sensibles al hardware como el acceso disco o a la red, generalmente se instala en los huéspedes HVM las herramientas de XenServer (XenServer Tools). Estas herramientas proporcionan controladores específicos del sistema operativo que están optimizados para utilizan en un entorno XenServer y aumentan el rendimiento que ofrecería un controlador emulado.

Las XenServer Tools proporcionan controladores optimizados para la red de Windows, almacenamiento y hardware de vídeo virtual. Estos tres componentes son la clave para ejecutar una infraestructura de Windows de alto rendimiento, y como tal, es importante que las herramientas de XenServer en una máquina virtual de Windows coincidan con los del host XenServer. Las versiones antiguas de dichas herramientas pueden llegar a provocar la degradación del rendimiento y en ciertas circunstancias afectar a la estabilidad.

- **Máquina Virtual Para-Virtualizada (PV)**

A diferencia de los huéspedes HVM, las máquinas virtuales para-virtualizadas son conscientes que están siendo virtualizadas y cargan un kernel optimizado para el hipervisor de destino. Linux es un ejemplo perfecto de un sistema operativo que puede ser para-virtualizado. Las principales distribuciones de Linux generalmente detectan Xen, aunque ciertas distribuciones pueden requerir que se recompile el kernel para activar la detección de Xen. Históricamente, se consideró que la para-virtualización era la solución óptima para máquinas virtuales Linux, pero las versiones más recientes de Linux incluyen un kernel que detecta Xen y que opera en forma cooperativa con él, permitiendo un mayor rendimiento de las máquinas virtuales en modo HVM.

- **Máquina Virtual Para-Virtualizada en Hardware (PVHVM)**

Como se mencionó anteriormente, los cambios recientes en las distribuciones Linux se traducen en que el rendimiento óptimo se alcanza en el modo de HVM. Como el hipervisor Xen y XenServer continúan evolucionando, una de las características más interesantes es la de PVHVM, o en otras palabras, Linux corriendo con extensiones HVM. En general, esta es la forma más eficiente de virtualización y puede verse con Ubuntu, Debian, CentOS y muchas otras distribuciones con kernels preparados para soportar Xen.

2.2.1.5. XenCenter

Una vez instalado XenServer en un host, se puede administrar inmediatamente utilizando Secure Shell (SSH) a través de la interfaz de línea de comandos (CLI). Además, XenServer también puede gestionarse utilizando XenCenter, una interfaz gráfica basada en Windows para la visualización de la terminal y de video en uno o más hosts con XenServer (véase Figura 6).

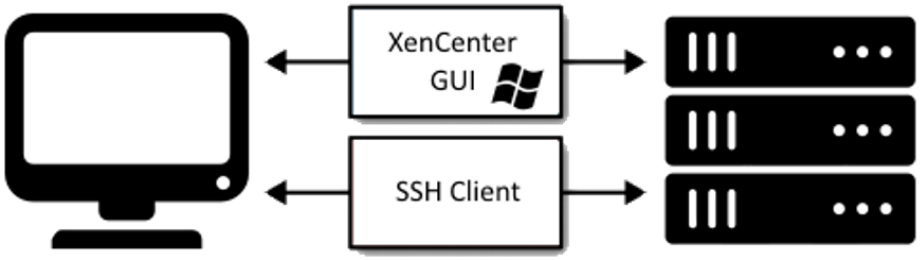


Figura 6 – Métodos de administración de equipos con XenServer

XenCenter proporciona una experiencia de usuario enriquecida para administrar varios servidores XenServer, agrupaciones de hosts en un *pool* y toda la infraestructura virtual asociada a ellos. Existen otras herramientas de código abierto y comerciales para gestionar XenServer, aunque XenCenter está diseñado en paralelo con cada versión de XenServer. XenCenter recoge las credenciales de usuario y luego interactúa con XenServer utilizando la XenAPI.

XenCenter está diseñado para ser retrocompatible con versiones anteriores de XenServer, aunque es recomendable utilizar siempre la versión más reciente disponible de XenCenter que se obtiene desde la web de XenServer. [15]

Para utilizar XenCenter es necesario obtener el ejecutable de Windows y proceder con la instalación del software. Una vez instalado será posible añadir el servidor con su IP y las credenciales. La Figura 7 muestra la pantalla principal de XenCenter y cómo añadir un nuevo equipo que tenga XenServer ya instalado y configurado.

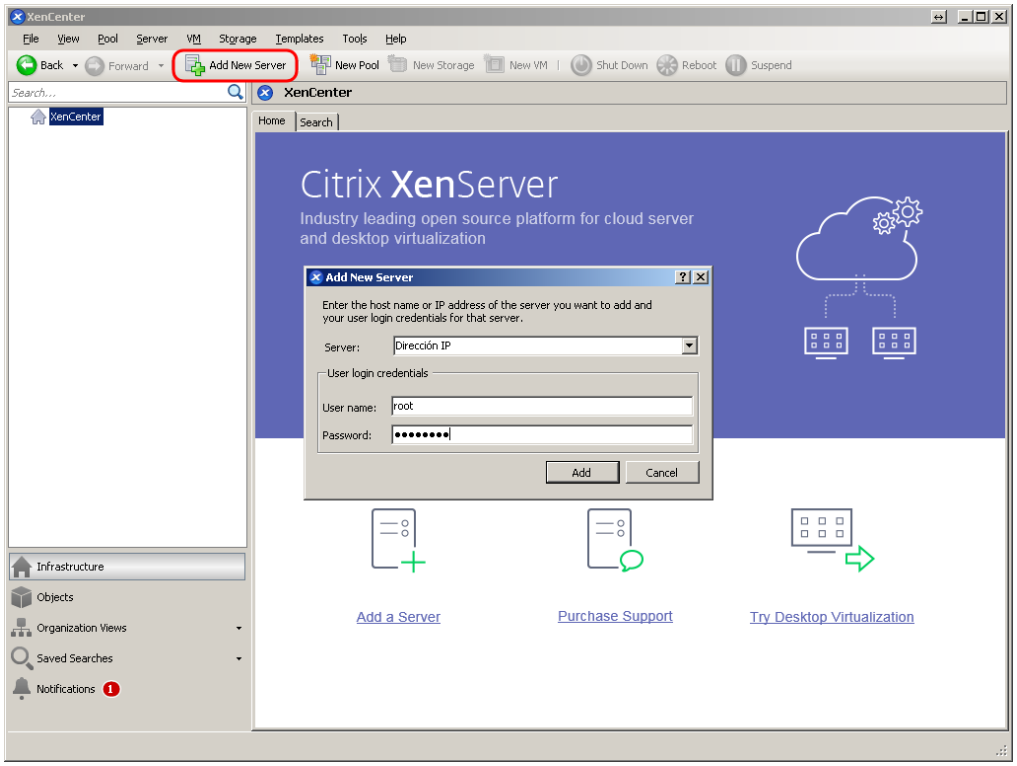


Figura 7 – Añadir un host en XenCenter

2.2.2. Comparativa de Citrix XenServer con otras soluciones

Puesto que existen múltiples soluciones de hipervisores de tipo 1, parece lógico hacer una breve comparación de las diferentes opciones existentes, comenzando con la que nos ocupa, Xen.

- Xen utiliza la técnica de para-virtualización, es decir, modifica el sistema operativo invitado. XenServer proporciona una buena infraestructura virtual que da la flexibilidad y las herramientas necesarias para mover escritorios, servidores y aplicaciones del plano físico a un entorno virtual. El hipervisor de XenServer prácticamente no genera *overhead* de virtualización acercándose al rendimiento de aplicaciones nativas. Existe una licencia gratuita que carece de algunas funcionalidades avanzadas, pero permite un uso estándar.
- VMware vSphere utiliza el hipervisor de virtualización completa VMware ESXi. ESXi ofrece avanzadas características de gestión y administración, como vMotion (migración en vivo), HA (alta disponibilidad) y tolerancia a fallos. VMware tiene una potente infraestructura debido a que múltiples proveedores desarrollan una gran variedad de herramientas. Sin embargo, es muy caro en comparación con otras plataformas de virtualización.
- Microsoft Hyper-V es la plataforma de virtualización desarrollada por Microsoft. Hyper-V, su hipervisor, gestiona y soporta sistemas operativos como Linux, Mac, Windows, etcétera. Sus licencias son incluso más caras que las VMware.
- KVM (Kernel Virtual Machine) es un hipervisor híbrido que soporta virtualización completa. KVM utiliza las ventajas del kernel estándar de Linux y es software gratuito y de código abierto. Existen soluciones comerciales que utilizan KVM como por ejemplo Proxmox, que ofrece licencias a precios muy bajos comparados con VMware o Hyper-V.

La elección del hipervisor es una elección controvertida y en la literatura cada autor expone sus argumentos a favor y en contra de un hipervisor u otro. Para tomar esta decisión deben tenerse en cuenta muchos factores, como qué sistemas operativos se van a instalar, cuál va a ser el objetivo final de esa

solución de virtualización, el precio de dicha herramienta y las funcionalidades adicionales que ofrece cada solución que se utilizarán de forma intensiva en el entorno. En cuanto al rendimiento existen diversas comparaciones de rendimiento entre los distintos hipervisores. En [16] se ha hecho un estudio del rendimiento utilizando CloudStack y comparando los hipervisores ESXi, Xen, KVM e Hyper-V.

2.3. Introducción al concepto de Cloud

En su sentido más básico, la Nube o Cloud se puede definir como una red. Según el National Institute of Standards and Technology (NIST), el Cloud Computing es "*un modelo que permite el acceso a un conjunto de recursos compartidos y configurables de forma eficiente y bajo demanda (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión o interacción por parte del proveedor del servicio*" [17].

Existen cuatro tipos de Nubes, en función de su propiedad:

- **Pública**, se refiere a la infraestructura que está abierta al público en general y su proveedor es una organización que vende sus servicios a terceros.
- **Privada**, se refiere a la infraestructura que sólo sirve a una única organización, aunque no necesariamente será dicha organización quien la gestione ni tampoco tendrá por qué estar en sus propias instalaciones.
- **Comunitaria**, es una infraestructura compartida por un conjunto limitado de organizaciones.
- **Híbrida**, en la que parte de las funcionalidades se ofrecen de manera privada (o en comunidad) y parte en un Cloud público.

Las organizaciones que utilizan la Nube Pública, acceden a través de Internet a los recursos informáticos que están alojados remotamente. Algunas organizaciones optan por Nubes Privadas, donde aprovechan la tecnología de Computación en la Nube manteniendo ellos mismos la infraestructura y el control de seguridad.

El Cloud Computing se basa en cinco características esenciales:

- *Autoservicio bajo demanda*, que permite que los usuarios obtengan acceso a los recursos sin interacción humana.
- *Acceso universal*, que permite acceder a los servicios con independencia del dispositivo o la plataforma.
- *Agrupación de recursos*, los recursos que ofrece el operador del servicio se sirven se simultáneamente a múltiples clientes asignándolos y liberándolos de forma dinámica.
- *Elasticidad*, permite que los recursos puedan ser asignados y liberados en función de la demanda de los servicios.
- *Monitorización*, que permita controlar y optimizar automáticamente el uso de recursos utilizados para su posterior tarificación.

Existen tres modelos de servicio del Cloud Computing, Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS). SaaS permite el acceso por parte del usuario a servicios que se ejecutan en la Nube del proveedor de servicio gracias a una aplicación cliente ligera (p.ej., correo web). PaaS permite que los usuarios desplieguen sus propias plataformas o aplicaciones en la Nube del proveedor (p.ej., Google App Engine). IaaS ofrece la capacidad de que sea el usuario quien controle el aprovisionamiento, los recursos de almacenamiento, de red e incluso de cómputo (p.ej., Rackspace). La Figura 8 muestra un resumen de las características de los modelos de servicio en función del tipo de Cloud.

El mayor atractivo de la Nube puede ser que al permitir que los proveedores de Cloud hagan lo que mejor saben hacer, construir infraestructuras y entornos de desarrollo a escala, el usuario final aprovecha esos conocimientos e inversión para centrarse en sus fortalezas, como escribir aplicaciones y servicios para sus clientes o proporcionar servicios a sus empleados. Y es por ello que las Nubes Públicas y Privadas se han vuelto tan populares.

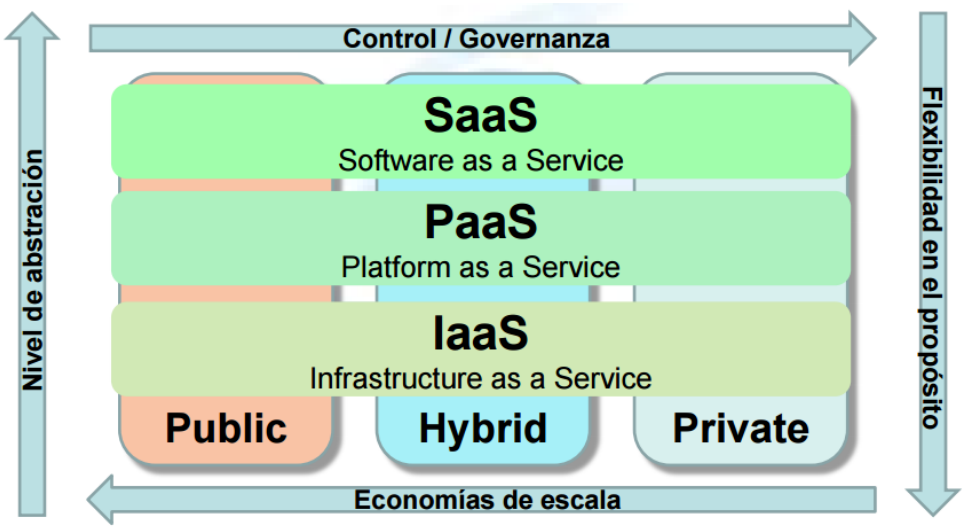


Figura 8 – Arquitecturas Cloud [18]

OpenStack se define como una Infraestructura como Servicio y permite al usuario crear un sistema de producción.

2.4. OpenStack

OpenStack es una plataforma de *Cloud Computing* (Computación en la Nube) distribuida como software libre y de código abierto formada por una variedad de servicios relacionados entre sí, que ofrecen una API que solventa los problemas de integración y permite gestionar y controlar los recursos disponibles de computación, almacenamiento y red. Los principales servicios de OpenStack y sus proyectos asociados se detallan brevemente en la Tabla 2.

Tabla 2 – Servicios y proyectos asociados de OpenStack [19]

Servicio	**Proyecto**	**Descripción**
Identidad	Keystone	Proporciona un servicio de autentificación para otros servicios de OpenStack así como la gestión de cuentas de usuarios y sus roles.
Imagen	Glance	Almacena y gestiona imágenes de los discos de las máquinas virtuales.
Computación	Nova	Gestiona las operaciones relacionadas con las máquinas virtuales incluyendo su creación, la selección del nodo de computación y su destrucción.

Servicio	Proyecto	Descripción
Red	Neutron	Proporciona conectividad de red como servicio a otros proyectos de OpenStack como por ejemplo Nova, el cual utiliza la API de Neutron para solicitar la conexión de las máquinas virtuales a un segmento de red determinado. Permite la creación de redes, subredes, enrutadores, cortafuegos, balanceadores de carga y redes privadas virtuales. Cuenta con una arquitectura modular que se integra con múltiples tecnologías de proveedores de red externos.
Interfaz de Gestión Web	Horizon	Portal de auto-servicio web que permite a administradores y clientes interactuar con los servicios subyacentes de OpenStack.
Almacenamiento de Bloques	Cinder	Proporciona almacenamiento permanente a las máquinas virtuales en ejecución. Presenta una arquitectura modular con una extensa variedad de drivers que permiten la creación de volúmenes de almacenamiento en bloques los cuales se acoplan a las máquinas virtuales
Almacenamiento de Objetos	Swift	Almacena y gestiona datos arbitrarios no estructurados en forma de objetos los cuales son accedidos mediante una API RESTful basada en HTTP. Es altamente tolerante a fallos a partir de la implementación de mecanismos de replicación de datos y arquitectura escalable. Su implementación no consiste en un servidor de ficheros compartidos con directorios montados, sino que escribe objetos y ficheros en múltiples dispositivos, garantizando que los datos estén replicados a lo largo del clúster de servidores.
Telemetría	Ceilometer	Supervisa y contabiliza los distintos servicios y el consumo de los recursos en OpenStack con fines de facturación, *benchmarking*, escalabilidad y reporte de estadísticas.
Orquestación	Heat	Orquesta múltiples aplicaciones de Cloud compuestas a partir del empleo del formato de plantilla nativa "HOT" o del formato de plantilla AWS CloudFormation, a través de ambas: una API REST nativa de OpenStack y una API Query compatible con CloudFormation
Base de Datos	Trove	Proporciona bases de datos como servicio de manera escalable y fiable. Las bases de datos ofertadas son tanto relacionales como no relacionales.
Procesamiento de Datos	Sahara	Proporciona las funcionalidades necesarias para desplegar y escalar un clúster Hadoop sobre OpenStack partiendo de la especificación de parámetros de configuración del clúster tales como la versión de Apache Hadoop, la topología del clúster y los detalles de hardware de los nodos que lo conforman.

La Figura 9 muestra el esquema conceptual del entorno OpenStack y cómo se relacionan todos sus servicios.

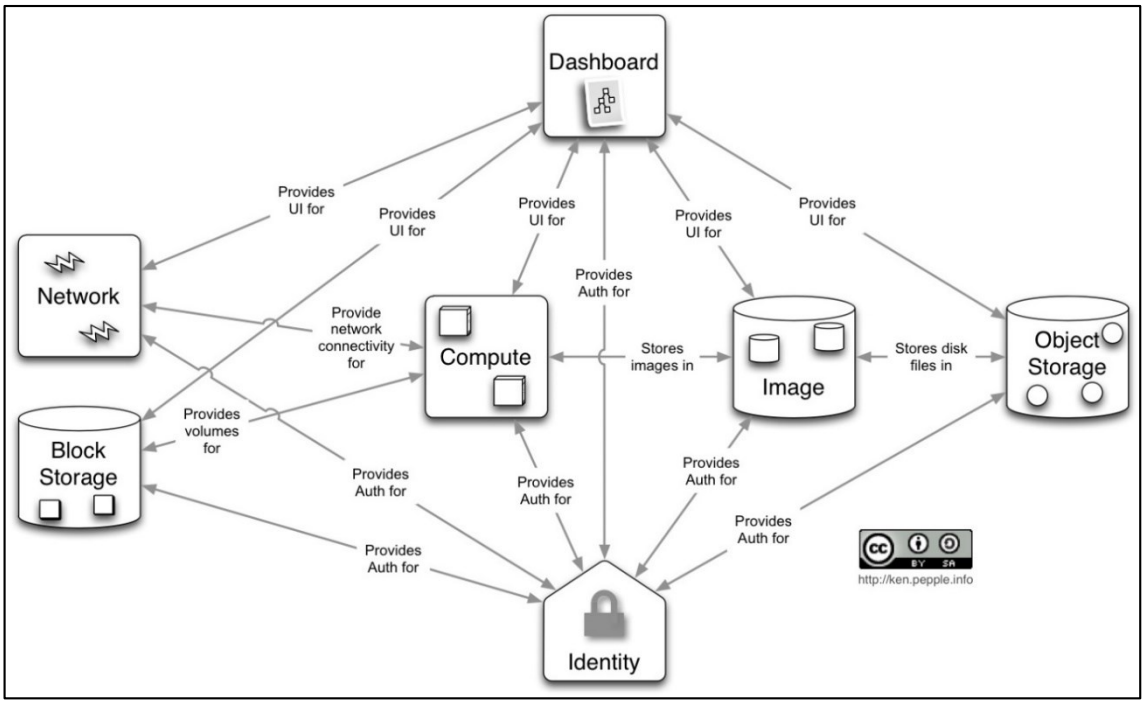


Figura 9 – Esquema conceptual de OpenStack [19]

2.4.1. Servicio de Identidad

El servicio de identidad de OpenStack, conocido como Keystone, proporciona servicios de autentificación y gestión de cuentas de usuario y del rol que éstos poseen en el entorno de OpenStack. Es un servicio fundamental que sustenta la autentificación y verificación entre todos los servicios de OpenStack y es el primer servicio que debe instalarse dentro de este entorno Cloud.

En Keystone, existen los conceptos de *tenants*, roles y usuarios. Un *tenant* se podría decir que es un proyecto y que cuenta con recursos como usuarios, imágenes e instancias, así como las redes que sólo pertenecen a ese proyecto en particular. Un usuario puede pertenecer a uno o más proyectos y puede cambiar entre estos proyectos para acceder a esos recursos. Los usuarios de un proyecto pueden tener varios roles asignados. En el escenario más básico, un usuario puede tener el papel de *admin* o simplemente ser un miembro. Cuando un usuario tiene privilegios de administrador dentro de un proyecto, puede utilizar funciones que pueden afectar el proyecto (como modificar redes externas). Un usuario normal con rol de miembro, puede realizar acciones más básicas relacionadas con el proyecto, como arrancar instancias, crear volúmenes y crear redes internas del proyecto.

Keystone autentifica usuarios frente a sus proyectos mediante el envío de un *token* de autorización validado entre todos los servicios de OpenStack. Esta información se utiliza para verificar si se tiene permiso para utilizar un servicio, como el almacenamiento o el cómputo. Por lo tanto, en primer lugar, se debe realizar la configuración de este servicio para crear los roles apropiados para los usuarios, servicios, proyectos y los *endpoints* de la API de servicio que conforman esta infraestructura Cloud.

2.4.2. Servicio de Imágenes

El servicio de imágenes de OpenStack, también conocido como Glance, es un servicio que le permite registrar, descubrir y recuperar imágenes de máquina virtual para su uso en el entorno de OpenStack. Las imágenes que se hayan hecho disponibles a través del servicio de imágenes pueden almacenarse en

una variedad de ubicaciones, desde el sistema de almacenamiento de archivos local a sistemas de ficheros distribuidos, como es el servicio de almacenamiento de objetos de OpenStack.

2.4.3. Servicio de Computación

El servicio de cómputo de OpenStack, también conocido como Nova, es el componente de cálculo del sistema operativo Cloud. Es el componente que permite ejecutar varias instancias de varios tipos en cualquier número de hosts que ejecuten el servicio de cómputo de OpenStack, lo que permite crear un entorno Cloud altamente escalable y redundante. Uno de los puntos fuertes de este proyecto de código abierto se el esfuerzo realizado por ser independiente del hardware e hipervisor. Este servicio se encarga de alojar y gestionar los sistemas de cómputo del entorno y es una parte importante de un sistema IaaS (Infrastructure-as-a-Service). OpenStack Compute impulsa algunas de las nubes computacionales más grandes como Rackspace Open Cloud.

2.4.4. Servicio de Red

OpenStack Networking es el componente SDN (*Software Define Networking* o Redes definidas por Software) de OpenStack y su nombre de proyecto es Neutron. Con SDN, se pueden describir redes complejas en un entorno multiusuario seguro que supere los problemas asociados a menudo con las redes planas (*flat*) y VLAN. En OpenStack, SDN es una arquitectura escalable, que significa que es capaz de conectar y controlar varios switches, firewalls, balanceadores de carga y conseguir implementar funciones como FWaaS (*Firewall-as-a-Service*). Todo esto se define en software para proporcionar un completo control sobre la infraestructura Cloud.

2.4.5. Servicio de Almacenamiento de Bloques

El servicio de Almacenamiento en Bloques de OpenStack llamado Cinder, gestiona la creación y eliminación de volúmenes de almacenamiento en bloque, así como su asignación a las máquinas virtuales creadas con el Servicio de Computación (Nova) y servidores físicos. Estos volúmenes de almacenamiento en bloque pueden gestionarse desde la interfaz web de OpenStack llamada Horizon, la cual permite a usuarios y administradores satisfacer de manera sencilla sus necesidades de almacenamiento.

2.4.6. Servicio de Almacenamiento de Objetos

OpenStack Object Storage, también conocido como Swift, es el servicio que permite el almacenamiento de información altamente redundante y escalable en un hardware modesto. Este servicio es utiliza por Rackspace como “archivos de la nube” y es análogo al servicio de almacenamiento S3 de Amazon. Con Swift, se pueden almacenar muchos objetos de cualquier tamaño, sólo limitado por el hardware. La naturaleza altamente redundante de OpenStack Object Storage, es ideal para almacenar información (como logs) además de proporcionar un sistema de almacenamiento que OpenStack Compute puede utilizar como plantilla para instancias de máquinas virtuales.

2.4.7. Interfaz Web de Gestión

Gestionar un entorno de OpenStack a través de una interfaz de línea de comandos permite tener un control completo del entorno Cloud, pero tener una interfaz web que los operadores y administradores pueden utilizar para manejar sus entornos e instancias facilita este proceso. *OpenStack Dashboard*, conocido como Horizon, proporciona esta interfaz web para el usuario desde la que se pueden gestionar

todos los componentes de OpenStack. Horizon es un servicio web que se ejecuta desde una instalación de Apache, utilizado la interfaz de puerta de enlace de servicio web (WSGI, *Web Service Gateway Interface*) de Python y Django, un *framework* web de rápido desarrollo.

Con OpenStack se pretende crear máquinas virtuales para que los alumnos sean capaces de desarrollar sus conocimientos en el área adecuada. Gracias a la flexibilidad y seguridad que proporciona, es posible desarrollar laboratorios virtuales a medida en función de las necesidades de formación de cada asignatura. Una de las características intrínsecas de OpenStack es que una máquina virtual es un entorno aislado cuya configuración no interfiere con la de otra y que si existe algún problema se puede volver a un estado anterior de la máquina utilizando instantáneas, o su término en inglés “snapshots”.

3. INFRAESTRUCTURA DEL LABORATORIO

En este capítulo se exponen el esquema del laboratorio donde se realizarán las implementaciones, las características de los servidores físicos utilizados, así como la configuración necesaria en los elementos de red que interconectan ambos laboratorios para permitir la comunicación entre ellos.

3.1. Esquema del laboratorio

Los servidores donde se llevarán a cabo las instalaciones de los diferentes sistemas se encuentran físicamente en el laboratorio docente de Aplicaciones Telemáticas de la escuela de Ingenieros Industriales y de Telecomunicación. Las características de dichos servidores se encuentran en el apartado 3.2. Para realizar dicha configuración, es necesario conocer y presentar dicha topología de red. A continuación se muestra en la Figura 10 el diagrama de conexión de los equipos.

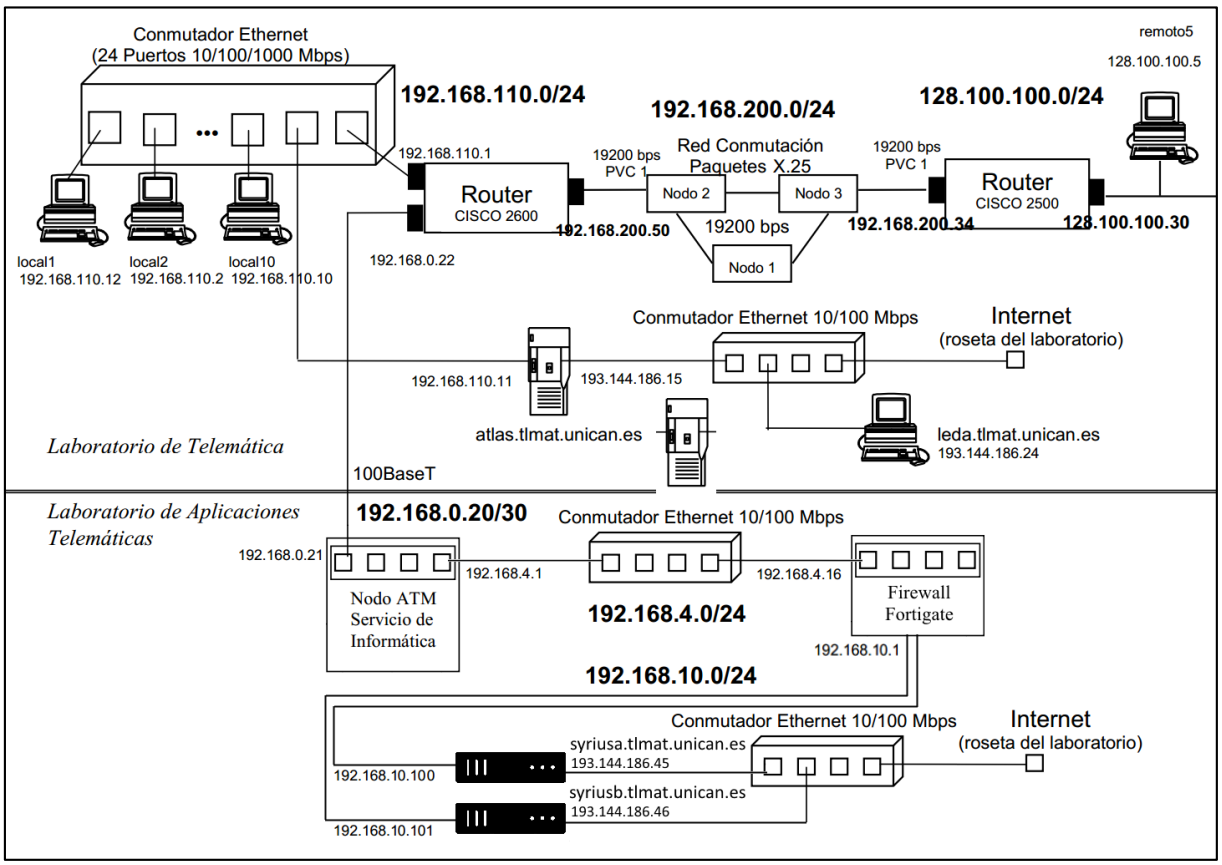


Figura 10 – Topología de red del laboratorio

En concreto, la infraestructura utilizada se corresponde con dos servidores Huawei FusionServer RH1288 v3 conectados al nodo ATM a través de un firewall FortiGate en la subred 192.168.10.0/24 y directamente a la red de la Universidad de Cantabria con las direcciones 193.144.186.45/24 y 193.144.186.46/24. Estas direcciones se encuentran detrás del firewall de la Universidad y solamente son accesibles desde equipos situados en la red de UNICAN.

3.2. Huawei FusionServer RH1288 v3

El hardware disponible sobre el que realizó la implementación de ambas soluciones es de dos racks gemelos de una U del fabricante Huawei. La Tabla 3 detalla las características soportadas por los equipos FusionServer RH1288 v3 con configuración de ocho discos.

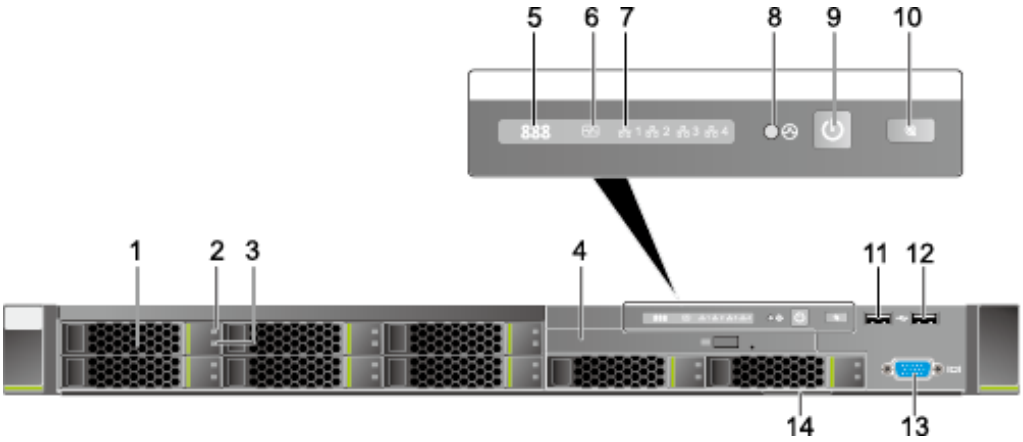
Tabla 3 – Características soportadas por el Huawei FusionServer RH1288 v3 de 8 discos duros [20]

RH1288 V3	
Factor de forma	Servidor rack de 1U
Número de procesadores	1 o 2
Modelo del procesador	Intel Xeon E5-2600 v3/v4
Memoria	16 slots de DDR4 RDIMMs o LRDIMMs
Almacenamiento local	Ocho SSDs, SAS o SATA de 2.5'' (El modelo NVMe soporta 4 discos NVMe SSD)
RAID	Soporta RAID 0, 1, 10, 5, 50, 6 y 60 Utiliza un supercondensador para proteger los datos de cache RAID de fallos de alimentación Soporta migración de estado RAID, configuración de memoria RAID, autodiagnóstico y configuración remota por web
Puertos de red	Soporta dos o cuatro puertos Gigabit Ethernet o dos puertos 10GE
Expansión PCIe	Admite hasta tres slots PCIe
Ventiladores	Cinco módulos de ventilador intercambiables en caliente con redundancia N+1 Cada módulo tiene dos ventiladores que giran en sentidos opuestos
Administración	El módulo iBMC module soporta *Intelligent Platform Management Interface* (IPMI), SOL, KVM sobre IP y medios virtuales Provee 1 Gbit/s en el puerto RJ45 de administración y soporta *Network Controller Sideband Interface* (NC-SI)
SOs soportados	CentOS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi
Módulo de alimentación	Soporta dos módulos redundantes intercambiables en caliente y soporta redundancia N+1 Soporta los siguientes módulos: • 460 W o 750 W AC o DC PSU • 800 W –48 V DC PSU • 1200 W alta tensión DC PSU
Tensión de alimentación	110 V-220 V AC 240 V-380 V DC –48 V DC
Temperatura de operación	5°C to 45°C
Certificaciones	CE, UL, FCC, CCC, y RoHS
Dimensiones	447 mm x 710 mm x 43.6 mm

A continuación se muestran, en la Tabla 4, la configuración disponible en ambos equipos del laboratorio, mientras que las Figuras 11 y 12, los principales componentes y puertos de acceso.

Tabla 4 – Características disponibles en los Huawei FusionServer RH1288 v3 del laboratorio

RH1288 V3	
Número de procesadores	2
Modelo del procesador	Intel Xeon E5-2603 v3
Memoria	128 GB (8 x16 GB)
Almacenamiento local	Un disco duro SAS de 1 TB
Puertos de red	Dos puertos GE (SM211)
Módulo de alimentación	Dos módulos redundantes intercambiables en caliente • 460 W o 750 W AC o DC PSU • 800 W –48 V DC PSU • 1200 W alta tensión DC PSU
Tensión de alimentación	110 V-220 V AC 240 V-380 V DC –48 V DC



1	Disco Duro	2	Indicador de fallo de disco duro
3	Indicador de actividad de disco duro	4	Lector DVD integrado
5	LED de diagnóstico de fallos	6	Indicador de estado
7	Indicador de estado de los puertos de red	8	Botón NMI
9	Botón de encendido	10	Indicador de identificación de unidad
11	Puerto USB 2.0	12	Puerto USB 2.0
13	Puerto de gráficos VGA	14	Etiqueta ESN

Figura 11 – Panel frontal del Huawei RH1288 v3 con leyenda [20]

Figura 12 – Panel posterior del Huawei RH1288 v3 [20]

3.2.1. iBMC y acceso a la Consola Virtual Remota

iBMC es el software de administración de los servidores Huawei descritos anteriormente. Este software está embebido en la memoria del equipo de forma que solo es accesible a través del puerto Ethernet preconfigurado para tal efecto. El acceso a este software de gestión se encuentra por defecto configurado en el puerto *eth2* y la IP de dicho puerto es la 192.168.2.100/24.

Es importante recordar que, aunque el equipo tiene un botón físico de encendido, este software de administración es independiente del estado del equipo, es decir, solo necesita tener una fuente de alimentación conectada a la red eléctrica para que sea accesible, da igual que el equipo esté apagado o reiniciándose.

Para acceder a dicho interfaz de gestión es necesario utilizar un cable Ethernet directo o cruzado, es indiferente ya que los nuevos equipos cruzan electrónicamente los pines correspondientes si es necesario, y configurar la interfaz de red del equipo desde el que se acceda con una IP de dicha subred de tipo C 192.168.2.0/24.

Al acceder a la IP del interfaz de administración del servidor se muestra la pantalla inicial (véase Figura 13) donde se piden las credenciales de acceso.

Por motivos de seguridad, se recomienda encarecidamente cambiar la contraseña preestablecida. Las credenciales por defecto son:

- Nombre de usuario: root
- Contraseña: Huawei12#$

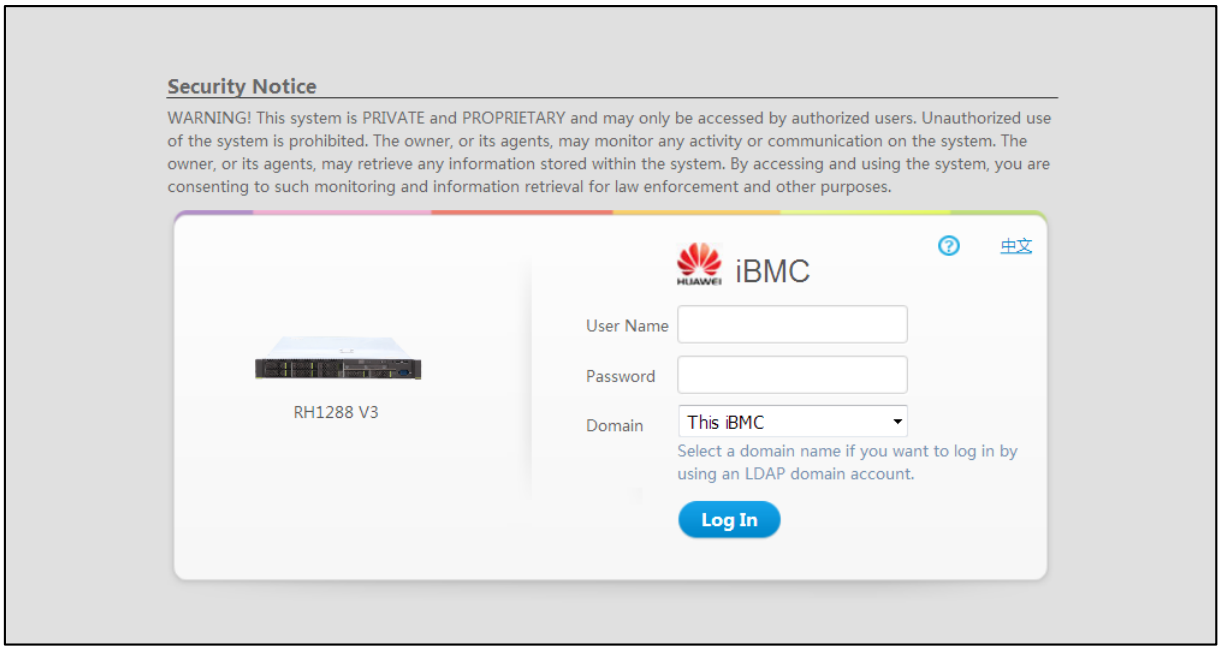


Figura 13 – Pantalla de identificación del software de administración iBMC

Tras identificarse con el nombre de usuario y la contraseña correctos se accede al panel de administración del dispositivo (véase Figura 14).

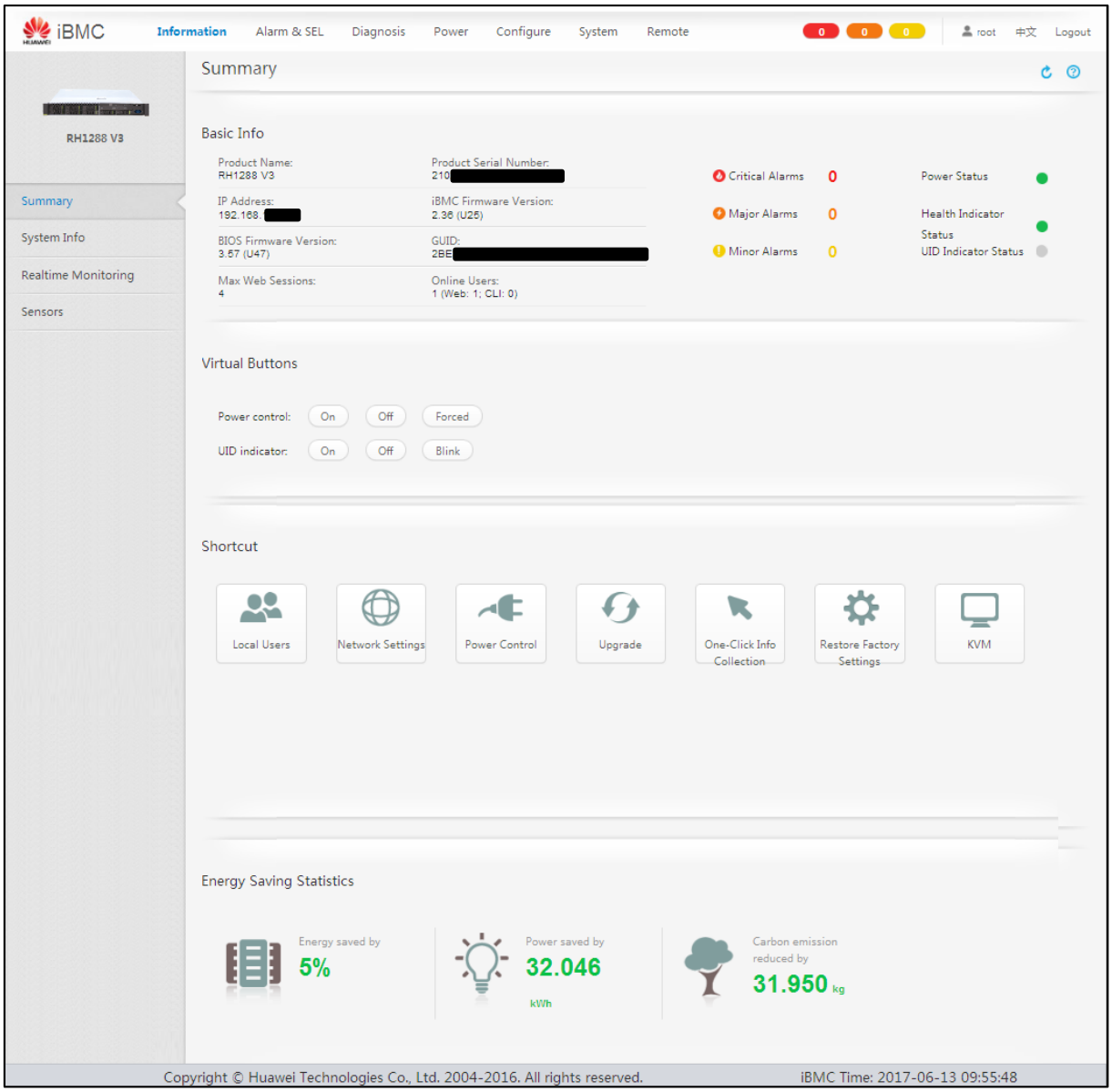


Figura 14 – Pantalla de inicio del software de administración iBMC

Este sistema de administración proporciona varias pestañas en las que se muestra información y opciones de configuración relativa al equipo.

El subapartado *Summary* de la pestaña *Information* muestra información básica del dispositivo, como la dirección IP del puerto de administración, el número de serie, la versión de la BIOS y del iBMC, etc. Se ha ocultado la información sensible por motivos de seguridad.

Permite a través de la interfaz web encender o apagar el equipo con un simple clic. Además, proporciona un acceso rápido a las funciones más utilizadas o de mayor interés como la configuración de usuarios, la configuración de red, el control de alimentación, la actualización del dispositivo y la consola virtual KVM.

La consola virtual remota permite al usuario realizar tareas de administración como la instalación de un sistema operativo, acceder a la BIOS o a la configuración de PXE o RAID. El acceso a la consola virtual se realiza a través del panel de control del iBMC.

Procedimiento

Paso 1 Acceder al software de administración iBMC a través del puerto de administración e identificarse con las credenciales correctas.

Paso 2 Seleccionar la pestaña *Remote,* véase Figura 15.

Paso 3 Elegir una de las opciones de *Remote Virtual Console*.

Existen dos opciones de conexión a la consola remote virtual:

- Remote Virtual Console (Shared Mode): permite a dos usuarios acceder y realizar operaciones simultáneamente. Un usuario puede ver las operaciones realizadas por el otro usuario.
- Remote Virtual Console (Private Mode): solo permite a un único usuario acceder y realizar operaciones en el servidor.

Es necesario tener el Java Runtime Enviroment (JRE) instalado para poder utilizar esta funcionalidad.

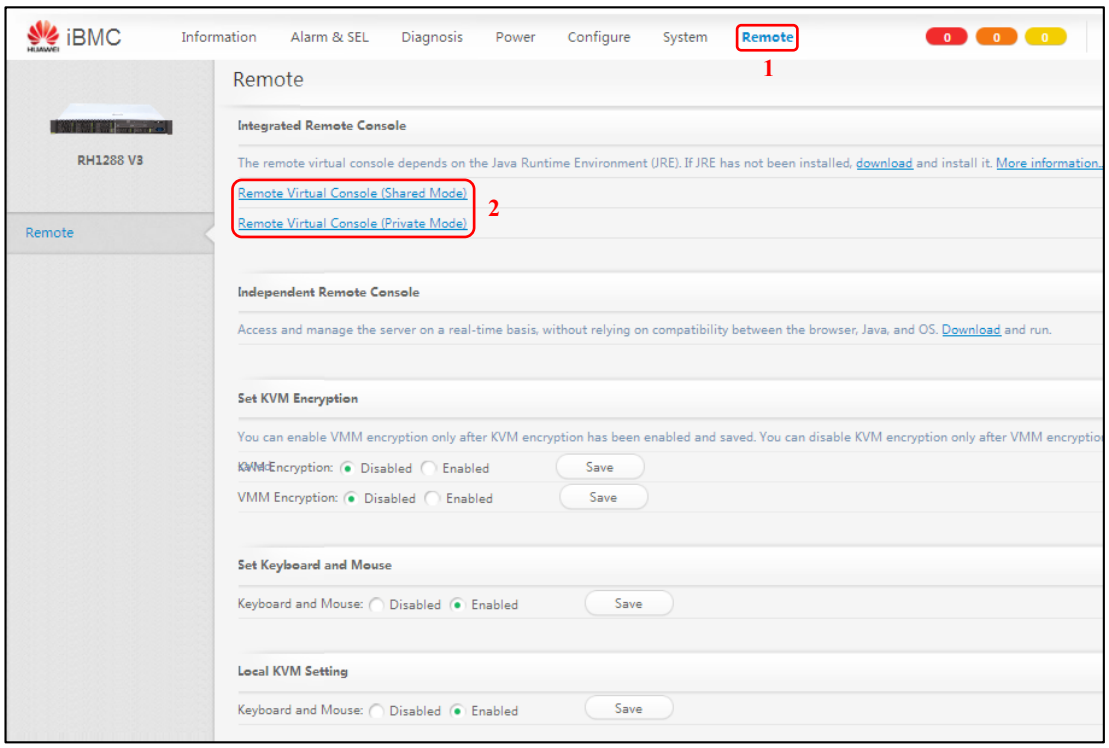


Figura 15 – Pestaña Remote del software de administración iBMC

Paso 4 Al seleccionar una de las opciones anteriores aparecerán mensajes para permitir la ejecución del applet "kvm.jnlp" de Java. Pulse en Abrir o Ejecutar en función del navegador.

Si se selecciona la opción *Shared Mode* aparecerá un aviso de que otra sesión KVM podrá visualizar sus acciones.

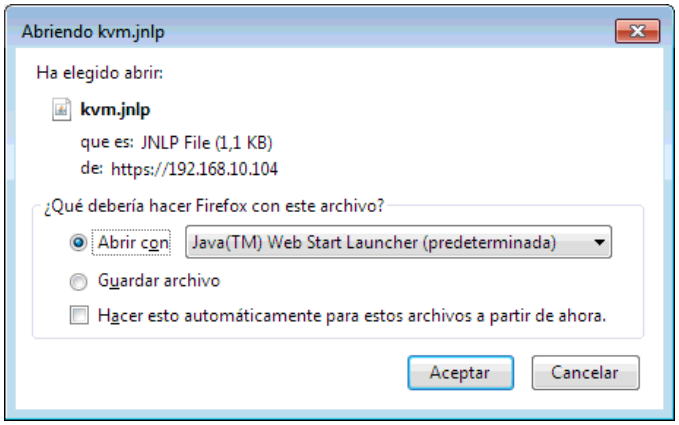


Figura 16 – Diálogo de descarga de Mozilla

Posteriormente arrancará la máquina virtual de Java y se mostrará una advertencia de seguridad si la dirección del host no se ha añadido a la lista de excepciones (véase Figura 17).

Paso 5 Pulsar en el botón Continuar en el cuadro de advertencia de seguridad

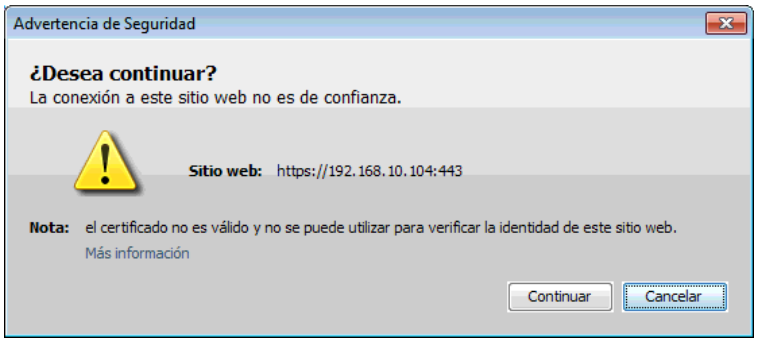


Figura 17 – Ventana de advertencia de seguridad de Java

Paso 6 Pinchar en el botón Ejecutar en el cuadro de diálogo que pregunta si se permite la ejecución dicha aplicación (véase Figura 17).

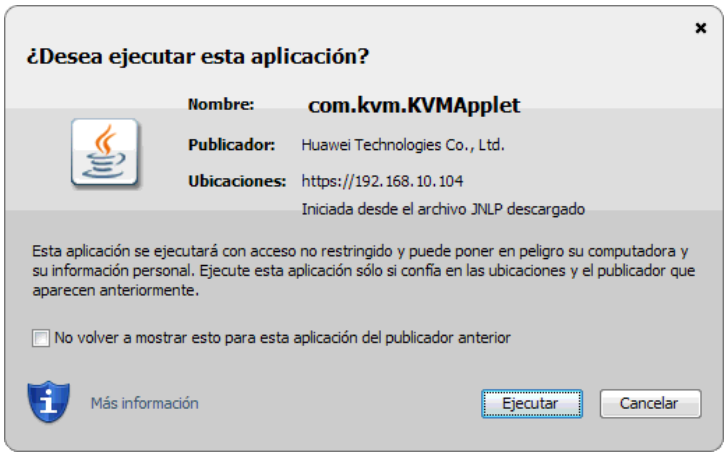


Figura 18 – Ventana de ejecución de aplicación Java

Por último, se abrirá una nueva ventana con la consola remota virtual en la que se podrán realizar diversas operaciones como apagar o encender el equipo, cargar medios virtuales como por ejemplo archivos de imagen ISO, capturar un video de la consola, etc.

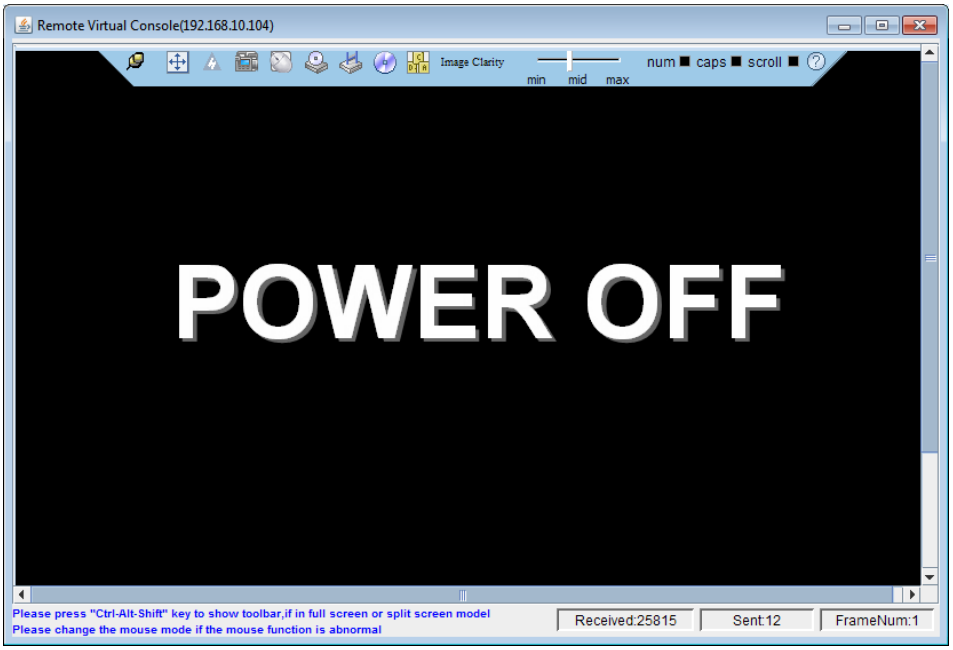


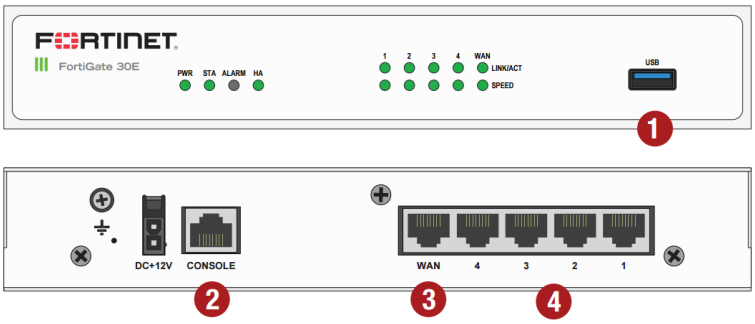
Figura 19 – Ventana de la consola remota virtual

3.3. Firewall FortiGate 30E

Este firewall interconecta los dos servidores Huawei con la red del Laboratorio de Aplicaciones Telemáticas. La Tabla 3 detalla las características soportadas por el firewall FortiGate 30E, y la Figura 20 el frontal y puertos disponibles.

Tabla 5 – Características del FortiGate 30E [21]

FortiGate 30E	
Factor de Forma	Escritorio
Almacenamiento	1 x Puerto USB 3.0
Puertos de red	4 x Puertos Switch Gigabit Ethernet RJ45 1 x Puerto WAN Gigabit Ethernet RJ45
Puertos de administración	1 x Puerto Consola RJ45
Throughput	950 Mbps
Latencia	130 µs
Sesiones concurrentes	900.000
Nuevas sesiones/segundo	15.000
Tensión de alimentación	110 V-240 V AC 60-50 Hz
Temperatura de operación	0°C to 40°C
Certificaciones	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN
Dimensiones	41 mm x 210 mm x 133 mm



1	Puerto USB 3.0	2	Puerto de Consola RJ45
3	1 x Puerto WAN GE RJ45	4	4 x Puertos Switch GE RJ45

Figura 20 – Panel frontal y trasero del FortiGate 30E con leyenda [21]

El firewall FortiGate dispone de una interfaz web de gestión accesible a través de la dirección IP configurada en la interfaz WAN o en la puerta de enlace de las interfaces LAN, pero por defecto sólo es accesible utilizando el protocolo HTTPS.

3.4. Preparación del entorno del laboratorio

Para que los servicios de la plataforma OpenStack sean accesibles desde ambos laboratorios docentes es necesario configurar los elementos de conexión de red existentes entre ellos. Otro requisito es permitir el acceso de las conexiones entrantes a los servidores y deshabilitar el servicio de DHCP en el firewall al que ambos están conectados.

3.4.1. Configurar enrutamiento entre los laboratorios

Para que desde el Laboratorio de Telemática (véase 3.1 Esquema del laboratorio) se pueda acceder a los servicios de las máquinas virtuales cuyas direcciones públicas pertenecerán a la red interna del firewall FortiGate (192.168.10.0/24) deben establecerse rutas estáticas, tanto en el router Cisco 2600 como en el Nodo ATM, que redirijan el tráfico hacia esta red por el camino adecuado.

Para configurar el router Cisco 2600 se debe iniciar una conexión al puerto serie con un cliente SSH (p. ej., PuTTY). La Tabla 6 lista las instrucciones para añadir una ruta estática en una interfaz Ethernet.

Tabla 6 – Instrucciones para añadir la ruta estática en el router Cisco 2600

Se entra en el modo configuración con los comandos *enable* y *configure terminal*:
`Router> enable`
`Router# configure terminal`
`Router(config)#.`
Para configurar las interfaces Ethernet se utiliza el comando interface:
`Router(config)#. interface Ethernet 0/1`
El "prompt" cambia al acceder al menú de configuración de una interfaz. Ahora se define una ruta estática que lleve el tráfico con destino la red del FortiGate, desde el router hacia el Nodo ATM:
`Router(config-if)# ip route 192.168.10.0 255.255.255.0 192.168.0.21`

Se sale del menú de configuración del interfaz:

```
Router(config-if)# exit
```

Por último se guarda la configuración:

```
Router(config)#. write memory
```

El Nodo ATM fue temporalmente sustituido por un router con la misma configuración que el Nodo y que por tanto realiza el mismo cometido. El router en cuestión es un Linksys WRT54G con el firmware DD-WRT v24. Desde la interfaz web, en el menú *Setup* > *Advanced Routing*, se configura la ruta estática del tráfico con destino la red 192.168.10.0 a través de la interfaz del FortiGate con la IP 192.168.4.16 como muestra la Figura 21.

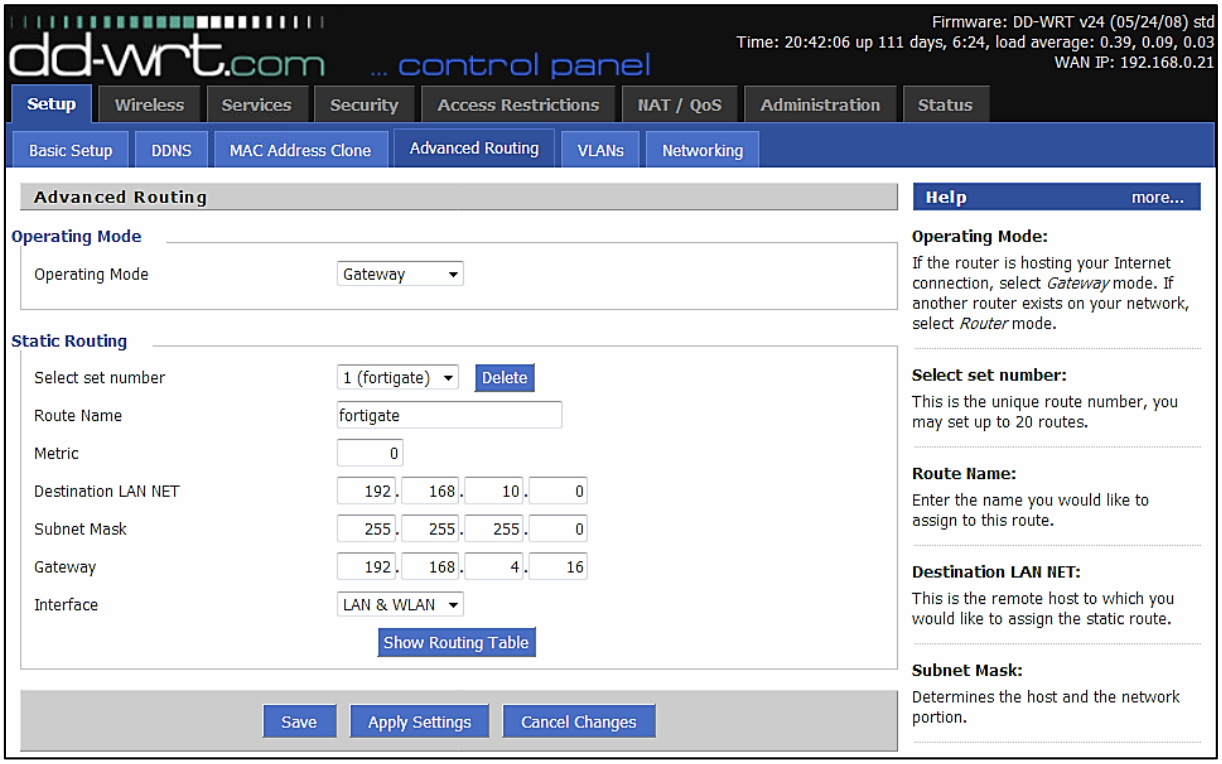


Figura 21 – Configuración de ruta estática en router Linksys WRT54G con firmware DD-WRT

3.4.2. Establecer listas de control de acceso y deshabilitar DHCP en el FortiGate

El objetivo de un firewall es bloquear el acceso desde su interfaz WAN a la interfaz LAN, pero permite configurar ciertas reglas que habiliten este acceso bajo determinadas circunstancias, por ejemplo, en función de la dirección de origen de la conexión.

Primero se selecciona el dominio virtual *root* y en el menú lateral se pincha en *Policy & Objects* > *IPv4 Policies* como muestra la Figura 22. Posteriormente se crea una nueva regla en la que se configura como interfaz de entrada el puerto WAN, como interfaz de salida el switch virtual (*Syrius*, véase Figura 23) donde están conectados los servidores y se define la subred desde la que se permitirá el acceso.

En el apartado origen se permite cualquiera porque sólo pueden ser accedidos desde los Laboratorios, en caso de no ser así, se recomienda definir los equipos o subredes que exclusivamente deban tener acceso.

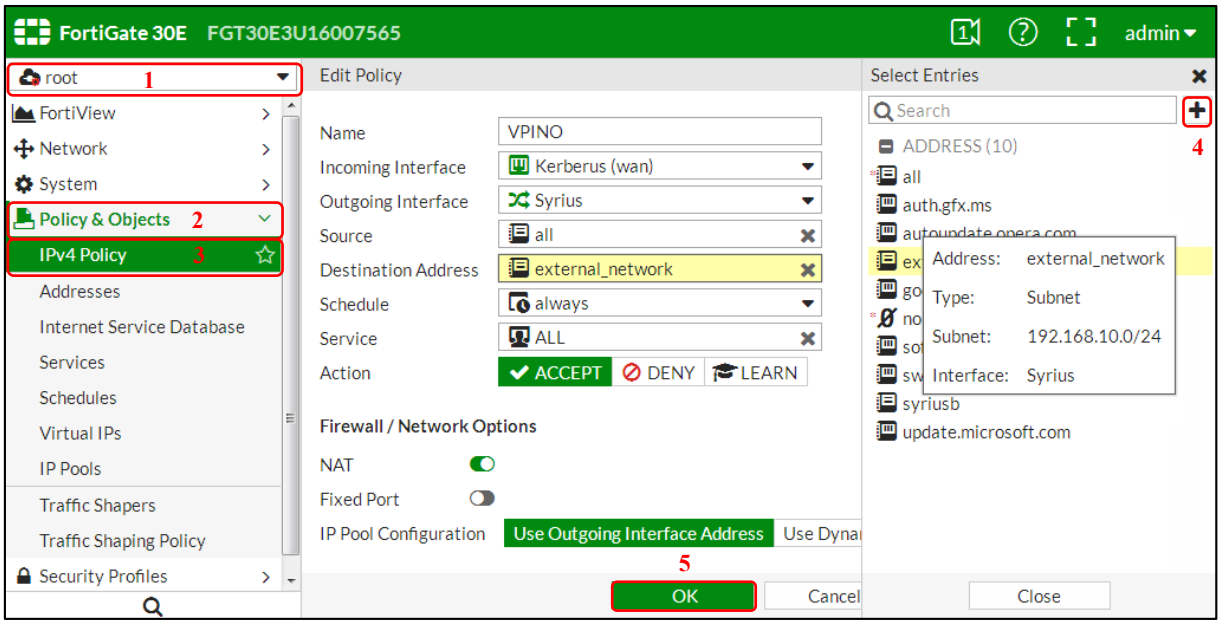


Figura 22 – Configuración de lista de control de acceso en el FortiGate 30E

Para permitir el correcto funcionamiento del posterior despliegue de OpenStack, es necesario deshabilitar todos los servidores de DHCP de las subredes en las que se trabaje. El FortiGate actúa como puerta de enlace y su dirección IP de la red interna es la 192.168.10.1. Debe accederse a ella utilizando el protocolo HTTPS para identificarse y gestionar su configuración.

Las Figuras 23 y 24 muestran cómo desactivar el servidor DHCP del firewall FortiGate 30E.

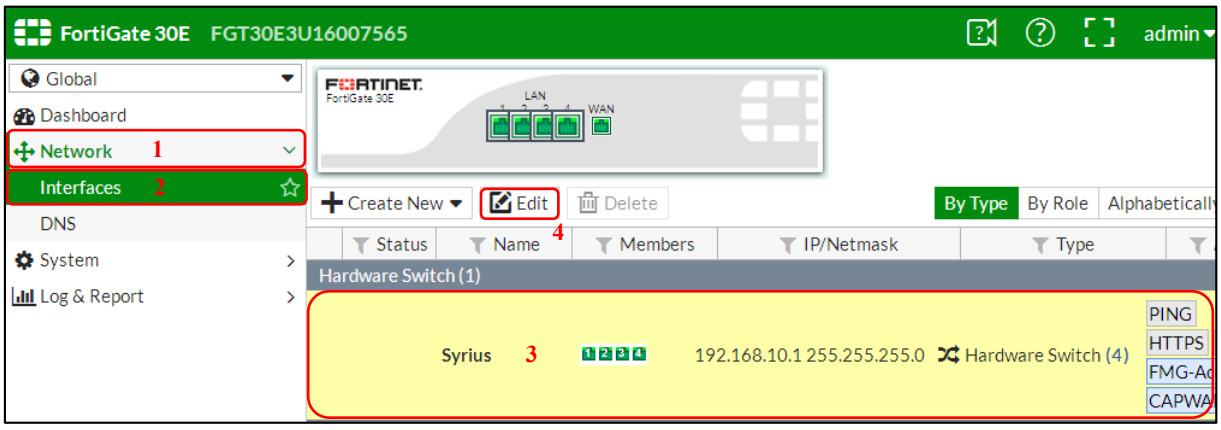


Figura 23 – Ventana Interfaces de la web de administración del FortiGate 30E

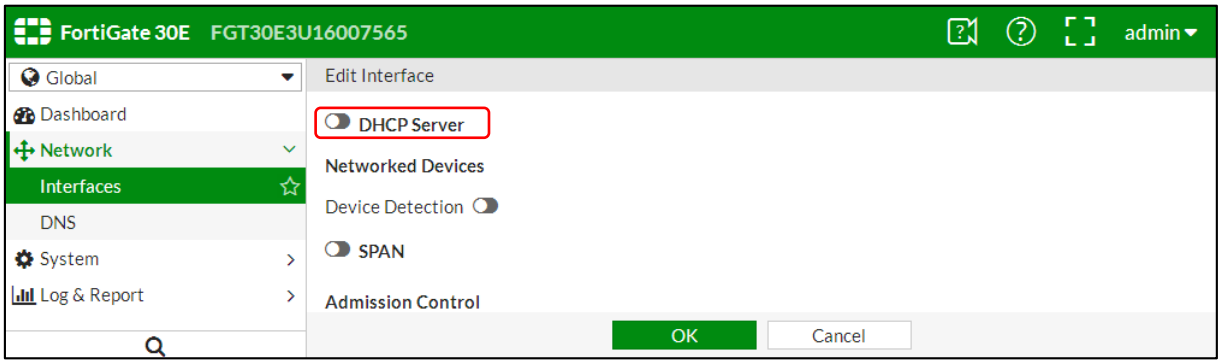


Figura 24 – Ventana de edición de interfaces de la web de administración del FortiGate 30E

4. FASE I: INSTALACIÓN DEL HIPERVISOR

En esta primera fase se procederá a detallar el flujo de trabajo realizado, mostrando las pruebas llevadas a cabo y los obstáculos que hubo que solventar en cuanto a tareas de instalación de Citrix XenServer se refiere. Se parte de los equipos físicos sin un sistema operativo instalado, con los discos duros formateados y con los parámetros de configuración de fábrica, estando ambos conectados al firewall. Tras este capítulo se espera disponer de un sistema de virtualización instalado en los servidores que permita el despliegue de la plataforma OpenStack.

4.1. Citrix XenServer 7.0

El primer paso realizado consistió en la instalación de la versión 7.0 de Citrix XenServer. El proceso de instalación de este sistema operativo es un proceso guiado y muy similar al de las versiones anteriores de este sistema operativo (véase 4.2 Citrix XenServer 6.5)

Tras la instalación, la primera prueba de funcionamiento que se realiza es crear una máquina virtual a través del asistente de creación de máquinas virtuales de XenCenter. Se eligió un Ubuntu en su versión 14.04 Desktop de 64 bits. Al iniciar el proceso de instalación el sistema se bloquea y el hardware no responde, XenCenter se cuelga sin permitir realizar acciones y pierde la conexión con XenServer.

Es en este momento cuando la única solución posible para recuperar el control del servidor es forzar su apagado y reiniciarlo.

Tras revisar que la tecnología de virtualización VT-x del procesador Intel está activada en la BIOS y contrastar el resto de opciones de configuración con el manual de referencia de la BIOS del equipo [22], se certifica que la configuración resulta correcta a pesar de que el sistema no funciona como debiera.

El siguiente paso que se realizó, fue la actualización de la BIOS del equipo y del sistema de administración de Huawei, iBMC, que aunque son procesos críticos que se detallarán a continuación, podrían albergar alguna incompatibilidad no detectada con Citrix XenServer 7.0. Dichos procedimientos se detallan en los apartados 4.1.1 Actualización de la BIOS y 4.1.2 Actualización del iBMC .

Tras realizar la actualización la prueba de funcionamiento continuó siendo infructuosa, el equipo continuaba bloqueándose al arrancar una máquina virtual con independencia del sistema operativo que se intentase instalar en ella.

Investigando posibles soluciones a este problema, se decidió actualizar XenServer aplicando los últimos parches de seguridad, publicados por Citrix, a través de XenCenter. Cabe reseñar que es un proceso lento y que consumió mucho tiempo debido a que muchas de estas actualizaciones requieren reiniciar el equipo tras su instalación si se instalan desde XenCenter. Más adelante se detalla el sistema de actualización automatizado que se desarrolló para que las pruebas realizadas desde cero no consumiesen tanto tiempo (véase 4.2.1 Actualización de XenServer a Service Pack 1 y parches de seguridad).

Tras instalar todas las actualizaciones y parches de seguridad que Citrix había publicado en su web, Citrix XenServer 7.0 seguía sin funcionar correctamente. La última opción que quedaba era verificar que el hardware del que se disponía era compatible con este sistema operativo. La web de Citrix [23], informa de que los equipos disponibles sí son compatibles con la versión 6.5 y 7.0 de XenServer.

Al final, contrastando esta información con la proporcionada por Huawei [24], resultó que no existe una certificación de compatibilidad por parte de Huawei para la configuración de hardware de los equipos

disponibles. Con todos los hechos presentados se deduce que no existe compatibilidad posible con la versión 7.0 de Citrix XenServer.

Por los motivos expuestos, se tomó la determinación de instalar la versión previa de este software, Citrix XenServer 6.5, que sí asegura la compatibilidad (véase 4.2 Citrix XenServer 6.5).

4.1.1. Actualización de la BIOS

La BIOS o *Basic Input/Output System* es el estándar de facto que define la interfaz de firmware para máquinas IBM o compatibles. Éste es el primer software que se ejecuta al arrancar el equipo, se utiliza para inicializar el hardware durante el proceso de arranque. Además, proporciona servicios en tiempo de ejecución para el sistema operativo y algunos programas.

Para comenzar el proceso de actualización de la BIOS es necesario descargar de la página de Huawei el fichero necesario que contiene la actualización. Hay que resaltar que éste es un proceso crítico, ya que si se realiza de forma incorrecta podría ocasionar graves daños en el equipo e incluso dejarlo inservible.

Durante la realización de este documento, la versión más reciente de la BIOS para este equipo publicada por el fabricante es la 3.63, la cual se puede obtener de la web de Huawei [25]. El archivo en cuestión se llama "RH1288 V3-BIOS-V363.zip", un archivo comprimido que contiene el fichero de actualización "biosimage.hpm". Este fichero debe extraerse del *Zip* en un lugar accesible para su posterior uso.

Una vez extraído, se accede al software de administración iBMC con las credenciales correctas.

Procedimiento

Paso 1 Seleccionar la pestaña *Power* > *Power Control*.

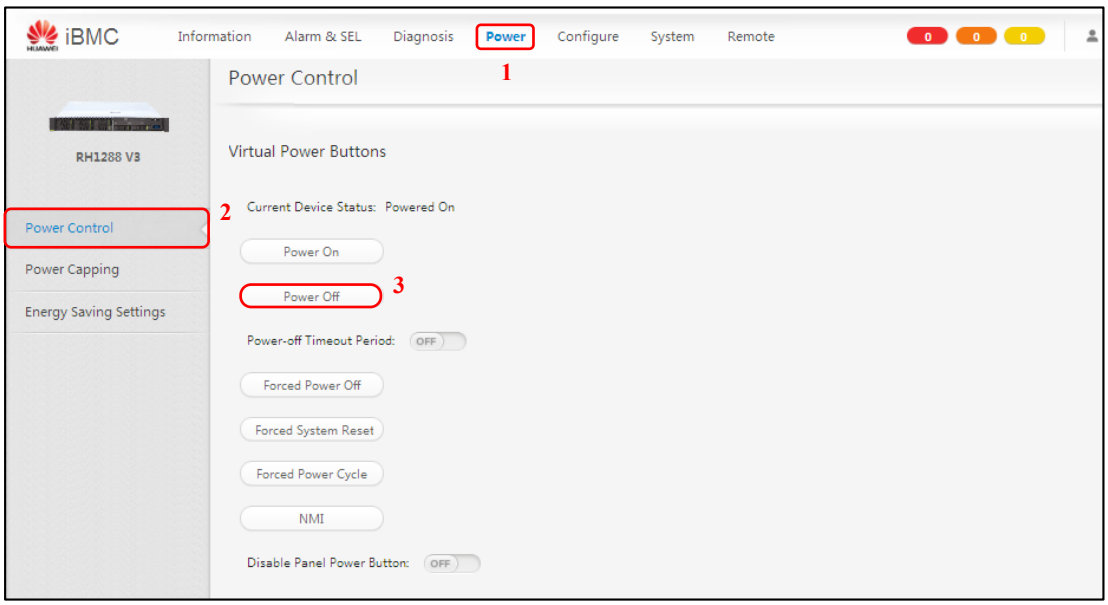


Figura 25 – Pestaña Power del software de administración iBMC

Paso 2 Clic en Power Off.

Paso 3 Seleccionar la pestaña *System* > *Firmware Upgrade*.

Paso 4 Clic en el botón *Browse*, se mostrará la ventana de búsqueda.

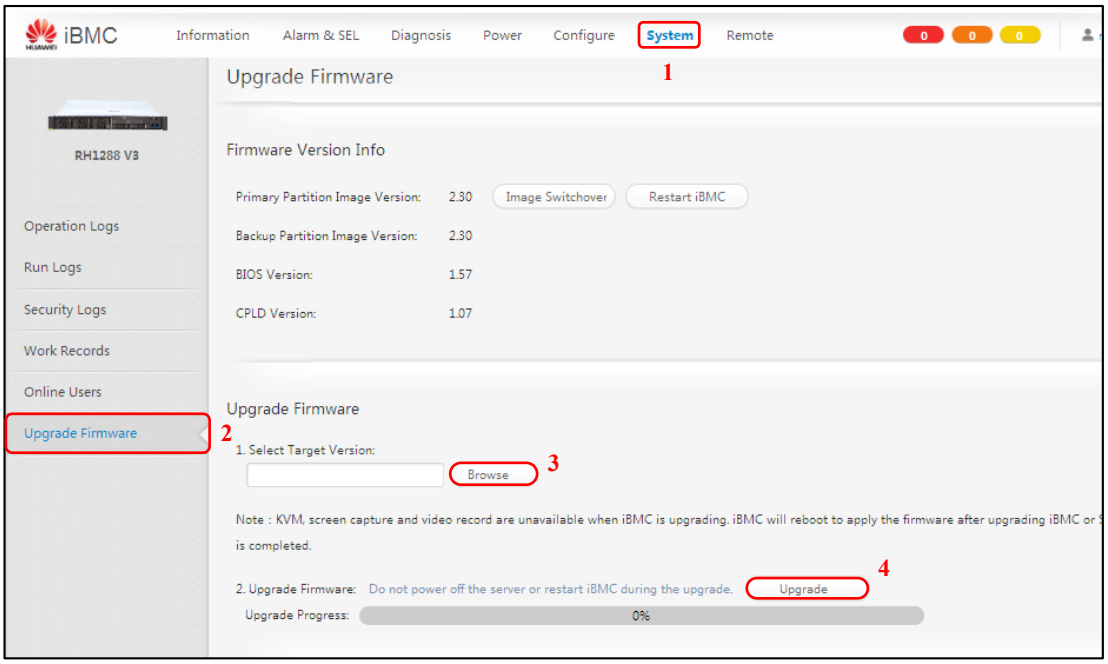


Figura 26 – Pestaña System del software de administración iBMC (I)

Paso 5 Seleccionar el fichero "biosimage.hpm" anteriormente extraído.

Paso 6 Clic en *Open*.

Paso 7 Clic en *Upgrade*.

Se muestra una ventana de confirmación de la acción a realizar.

Paso 8 Clic en *OK* para aceptar los cambios.

La preparación lleva unos dos minutos.

Tras la preparación, comienza la actualización del sistema. Durante el proceso, los ventiladores giran a máxima potencia generando mucho ruido.

Tras completar la actualización se muestra la siguiente información.

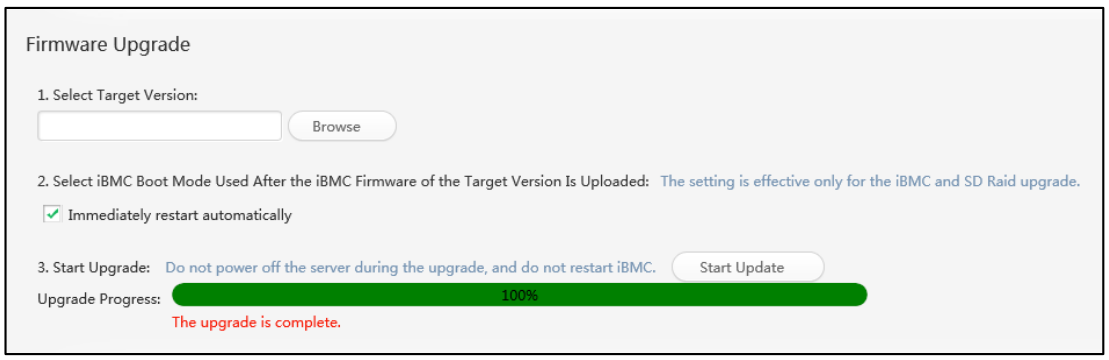


Figura 27 – Información de actualización completada del software de administración iBMC (I)

Paso 9 Seleccionar la pestaña *Power* > *Power Control*.

Paso 10 Clic en *Power On*.

La pestaña *Power Control* puede tener pequeñas diferencias en función de la versión de iBMC.

4.1.2. Actualización del iBMC

Para obtener el fichero de actualización del firmware iBMC hay que acudir a la web de Huawei. Durante la realización de este documento, la versión más reciente del iBMC disponible para este equipo publicada por el fabricante es la 2.42, la cual se puede obtener de la web de Huawei [26]. El archivo en cuestión se llama "RH1288 V3-iBMC-V242.zip", un archivo comprimido que contiene el fichero de actualización "image.hpm". Este fichero debe extraerse del *Zip* en un lugar accesible para su posterior uso. Una vez extraído, se accede al software de administración iBMC con las credenciales correctas.

El Huawei FusionServer RH1288 v3 posee dos imágenes del software iBMC, una partición primaria y otra de *backup*. El proceso de actualización debe realizarse dos veces para actualizar ambas particiones a la misma versión, primero la partición de *backup* y posteriormente la activa.

Procedimiento

Paso 1 Seleccionar la pestaña *System* > *Firmware Upgrade*.

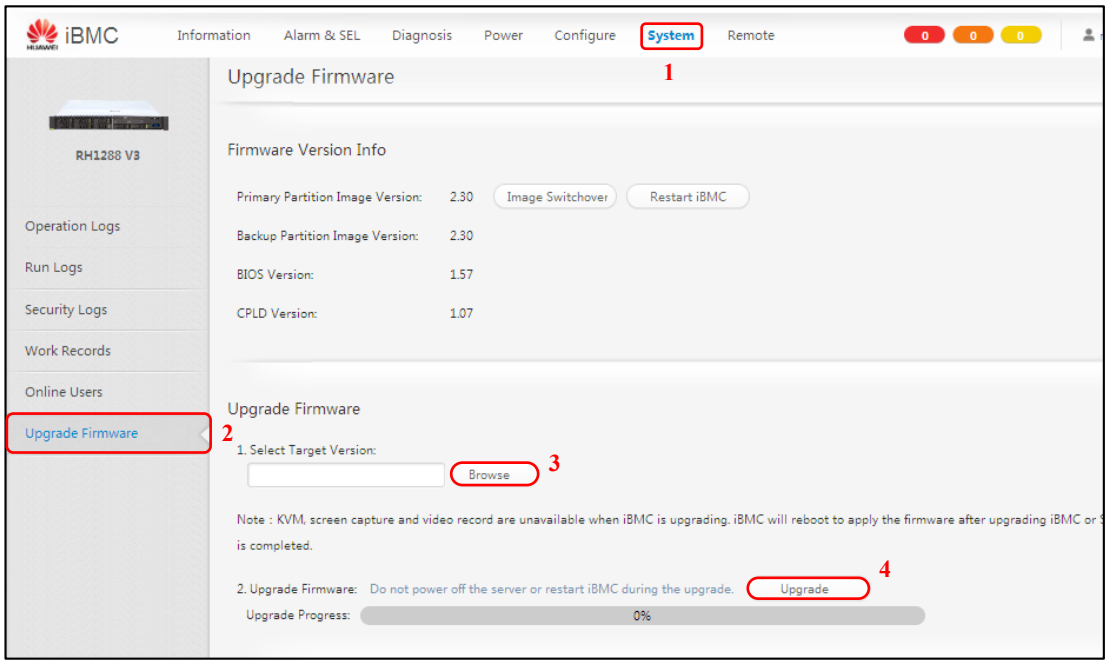


Figura 28 – Pestaña System del software de administración iBMC (II)

Paso 2 Seleccionar la pestaña *System* > *Firmware Upgrade*.

Paso 3 Clic en el botón *Browse*, se mostrará la ventana de búsqueda.

Paso 4 Seleccionar el fichero "image.hpm" anteriormente extraído.

Paso 5 Clic en *Open*.

Paso 6 Clic en *Upgrade*.

Se muestra una ventana de confirmación de la acción a realizar.

Paso 7 Clic en *OK* para aceptar los cambios.

La actualización del iBMC lleva alrededor de cinco minutos.

Tras completar la actualización se muestra la siguiente información.

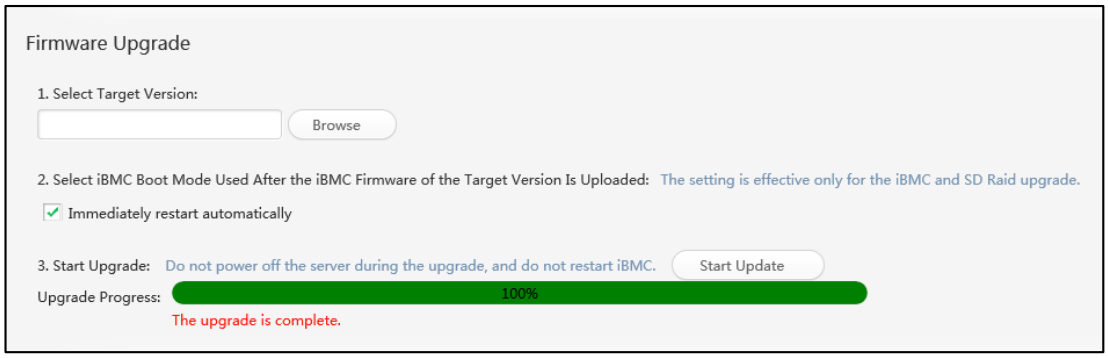


Figura 29 – Información de actualización completada del software de administración iBMC (II)

Tras la actualización el iBMC se reiniciará

Paso 8 Volver a acceder al iBMC con las credenciales.

La pestaña *Power Control* puede tener pequeñas diferencias en función de la versión de iBMC.

Paso 9 Repetir del Paso 1 al Paso 8 para actualizar la imagen activa del iBMC.

4.2. Citrix XenServer 6.5

Dado que la versión 7.0 se descartó por incompatibilidad con la configuración hardware de los servidores disponibles, se detalla a continuación el proceso de instalación de Citrix XenServer 6.5 SP1 y su configuración de acuerdo a lo establecido en el apartado 3.1 Esquema del laboratorio.

El primer paso es obtener la ISO de instalación del sistema operativo, la cual se puede obtener de la web de XenServer [27]. La tecnología de virtualización VT-x viene activada por defecto en la BIOS. En versiones anteriores del firmware de la BIOS era posible cambiar esta opción. Si se realiza el proceso de actualización de la BIOS (véase 4.1.1 Actualización de la BIOS) a una versión superior, es posible que dicha opción ya no aparezca quedando activada por defecto.

Procedimiento

Paso 1 Acceder al software de administración iBMC a través del puerto de administración e identificarse con las credenciales correctas.

Paso 2 Abrir la Consola Virtual Remota del software de administración iBMC.

Este procedimiento se detalla en el apartado 3.2.1 iBMC y acceso a la Consola Virtual Remota.

Paso 3 Apagar el equipo, *Power Management* > *Normal Power Off*, como se muestra en la Figura 30.

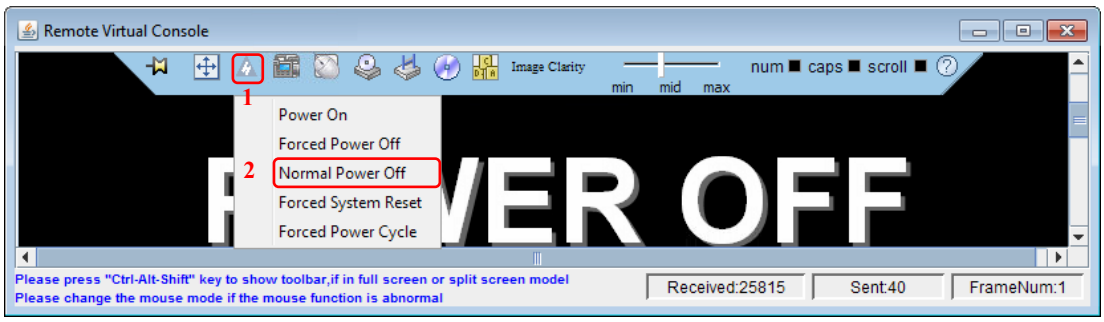


Figura 30 – Apagar el equipo desde la consola remota virtual

Paso 4 Volver a encenderlo, *Power Management* > *Power On*, para poder acceder a los parámetros de configuración de la BIOS.

Paso 5 Durante el proceso de arranque debe pulsarse la tecla *Supr* o *Del* o la tecla F4, cuando se muestre la pantalla de información como refleja la Figura 31.

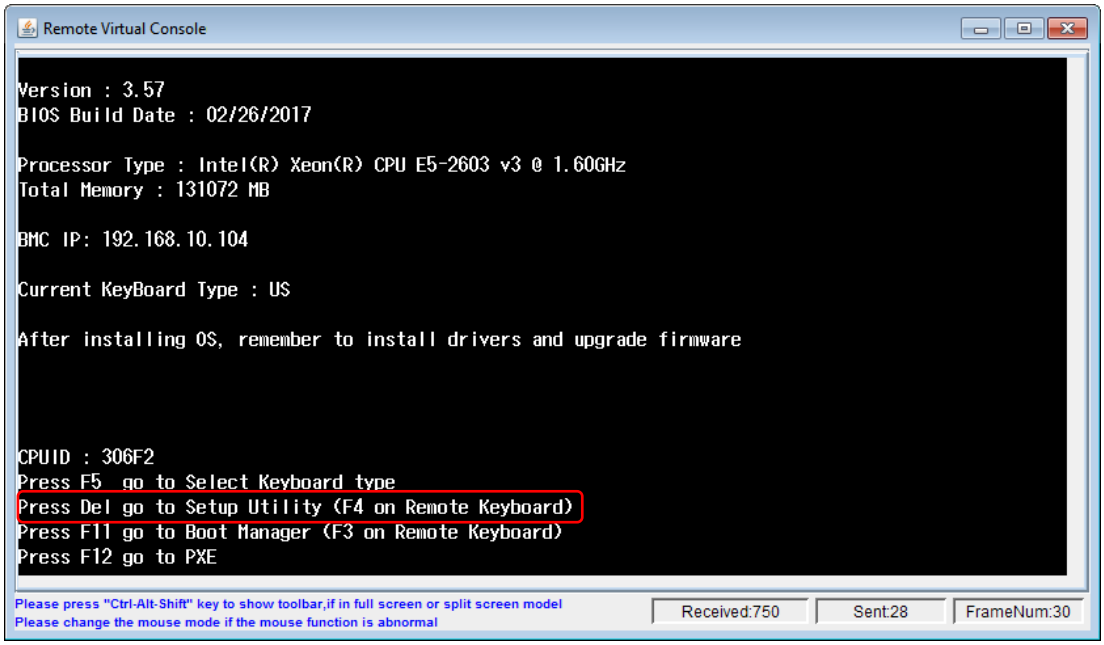


Figura 31 – Pantalla de información y acceso a la BIOS del Huawei FusionServer

Paso 6 Para acceder a la BIOS se pide la contraseña de acceso y es la misma que trae por defecto para el acceso al iBMC, Huawei12#$.

NOTA: Es de vital importancia tener en cuenta que el tipo de teclado por defecto es el inglés, por ello la combinación de teclas para introducir la contraseña difiere ligeramente que en el teclado español. La única diferencia es que el símbolo '#' debe introducirse con la combinación de teclas ⇧+3# (Mayúsculas+3) y no Ctrl+Alt+3# o Alt Gr+3# como en el teclado español. El símbolo '$' se introduce de la misma forma, ⇧+4$ (Maýusculas+4).

Paso 7 Al introducir la contraseña y pulsar la tecla *Intro* o *Enter*, aparece un mensaje de aviso que recomienda cambiar la contraseña por defecto como muestra la Figura 32, volver a pulsar la tecla Intro o Enter.

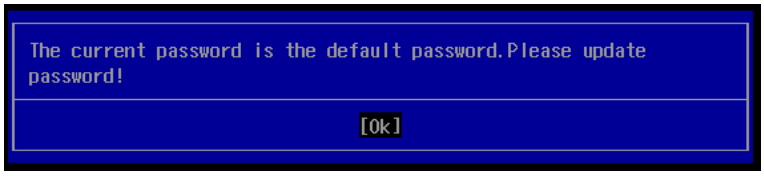


Figura 32 – Mensaje de recomendación de cambio de contraseña por defecto

Paso 8 Una vez en la BIOS, es recomendable actualizar la hora del sistema en la pestaña *Main* y en la sección *Boot*, seleccionar la opción *Boot Order Type* y con ayuda de las teclas F5 y F6 colocar como primera opción *CD/DVD-ROM Drive* como muestra la Figura 33.

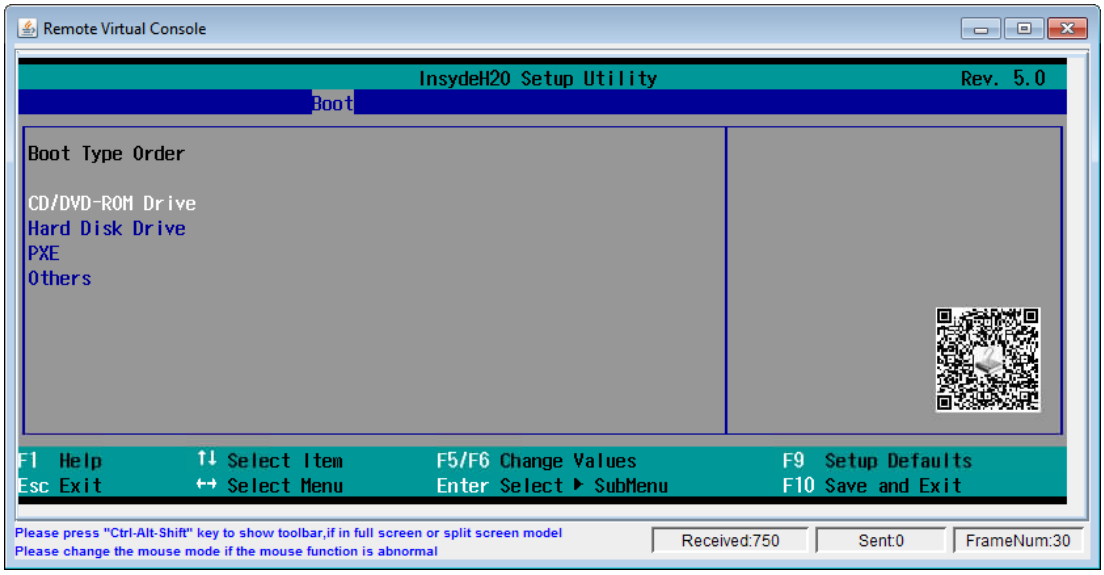


Figura 33 – Selección del orden de los medios de arranque

Paso 9 Pulsa la tecla F10 para guardar y salir.

Paso 10 Apagar el equipo, *Power Management* > *Normal Power Off*, como se muestra en la Figura 30.

Paso 11 Utilizar el icono *CD/DVD,* como se muestra en la Figura 34, para cargar la ISO de instalación de Citrix XenServer 6.5.

Paso 12 Seleccionar la opción *Image File*.

Paso 13 Hacer clic en *Browse* y seleccionar la ISO de instalación previamente descargada.

Paso 14 Pinchar el botón *Connect* para activar el lector de CD virtual.

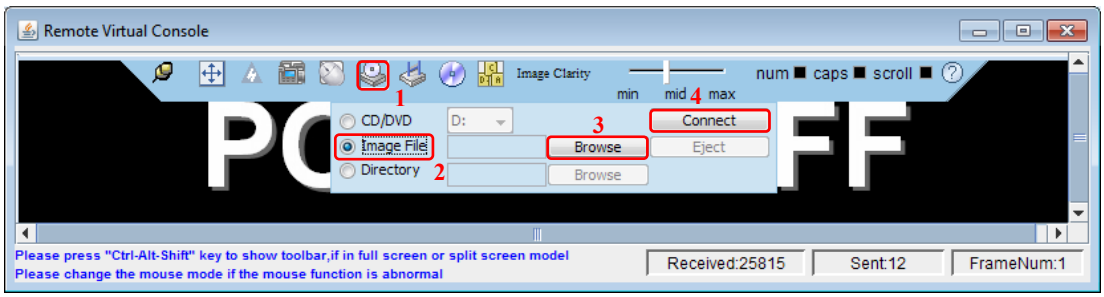


Figura 34 – Cargar medio virtual en consola remota virtual

Paso 15 Pinchar el botón *Power Management* > *Power On* para arrancar de nuevo el equipo y preceder con la instalación de XenServer.

Paso 16 Al arrancar de nuevo el equipo, se iniciará el proceso de instalación mostrando la pantalla principal. Pulsar la tecla *Intro* o *Enter* para continuar con el proceso de instalación estándar (véase Figura 35).

Figura 35 – Pantalla inicial del proceso de instalación de XenServer 6.5

Paso 17 El primer paso de la instalación consiste en seleccionar el tipo de teclado, para el teclado español seleccionar la opción '*[qwerty] es*'.

Paso 18 A continuación, se muestra un mensaje de advertencia de que la instalación de XenServer borrará el contenido del disco duro, seleccionar *Ok*.

Paso 19 La siguiente ventana del proceso detalla el acuerdo de licencia del usuario final, para continuar seleccionar *Accept EULA*.

Paso 20 A continuación, se pide seleccionar el disco duro de instalación, en este caso sólo hay uno de 1 TB. Además, es imprescindible marcar la opción *Enable thin provisioning*, como muestra la Figura 36, para que la partición de almacenamiento la cree en formato de Linux Ext3 y que posteriormente sea compatible con determinadas funcionalidad de OpenStack.

Figura 36 – Selección del disco duro de almacenamiento de la instalación

Paso 21 Se muestra una ventana de selección del medio de instalación, en este caso se debe selección *Local media*.

Paso 22 Es posible añadir *Supplemental Packs*, éstos añaden funcionalidades adicionales, no es un requisito indispensable pero se ha instalado el *Container management supplemental pack* para XenServer 6.5 SP1 disponible en la web de XenServer [28] para una posible futura integración con Docker [29].

Paso 23 Ahora se pide una contraseña para la cuenta del usuario privilegiado o *root*.

Paso 24 La Figura 37 muestra la configuración de red introducida de acuerdo a lo mostrado en el apartado 3.1 Esquema del laboratorio. El servidor de DNS será el mismo que la puerta de enlace o *Gateway*.

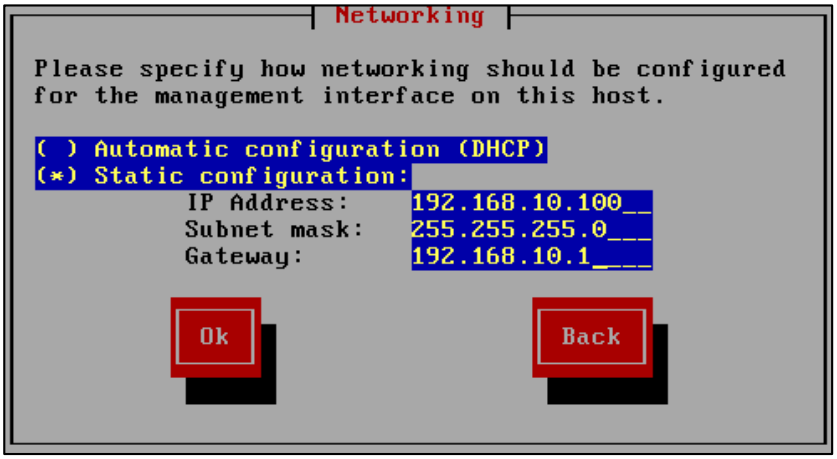


Figura 37 – Configuración de red de XenServer

Paso 25 Se fija la configuración regional para la hora del sistema en función del país, aunque se utilizarán servidores NTP para la sincronización de la hora, algo crucial a la hora de desplegar posteriormente OpenStack. Se pueden obtener los nombres de dominio de servidores NTP españoles en la web www.pool.ntp.org/zone/es, por ejemplo:

- 1.es.pool.ntp.org
- 0.europe.pool.ntp.org
- 3.europe.pool.ntp.org

Paso 26 Aceptar el comienzo del proceso de instalación como muestra la Figura 38.

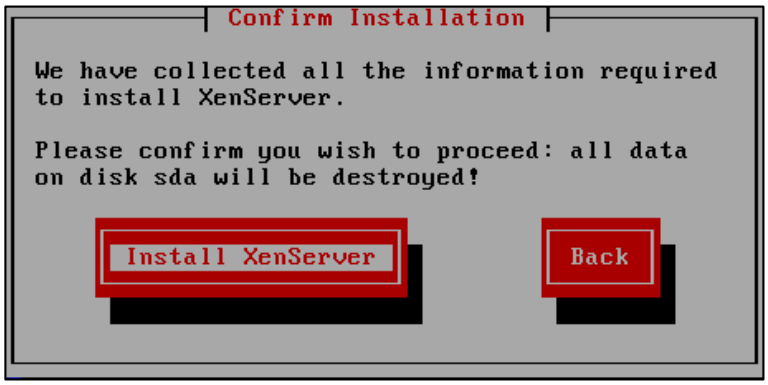


Figura 38 – Confirmación de Instalación de XenServer

Paso 27 Al finalizar se reiniciará el servidor y ya será posible administrarlo con XenCenter.

4.2.1. Actualización de XenServer a Service Pack 1 y parches de seguridad

Desde la presentación de la versión 6.5 de XenServer se han publicado muchos parches de seguridad para corregir problemas que presentaba este sistema operativo. El Service Pack 1 para esta versión contiene un pequeño número de actualizaciones y entre ellas, una de carácter crítico que corrige un problema de estabilidad del sistema.

Desde la aplicación XenCenter es posible actualizar XenServer pero es una labor lenta y tediosa, puede llevar horas dado que el proceso de actualización es manual, las actualizaciones deben descargarse e instalarse de una en una y hasta la fecha son más de cincuenta.

Como solución alternativa se propuso la descarga de las actualizaciones desde la web de Citrix para su posterior instalación mediante un script escrito en Shell, es necesario crear una cuenta gratuita en Citrix para su descarga.

El primer paso es instalar el Service Pack 1 a través de XenCenter, se puede descargar desde la propia aplicación o de la página de Citrix. Para actualizar XenServer desde XenCenter, hay que dirigirse a la pestaña *Tools* > *Install Update* y seleccionar posteriormente el fichero de actualización como muestra la Figura 39. Tras realizar unas comprobaciones previas comenzará la instalación, al finalizar el servidor se reiniciará con el Service Pack 1 ya instalado.

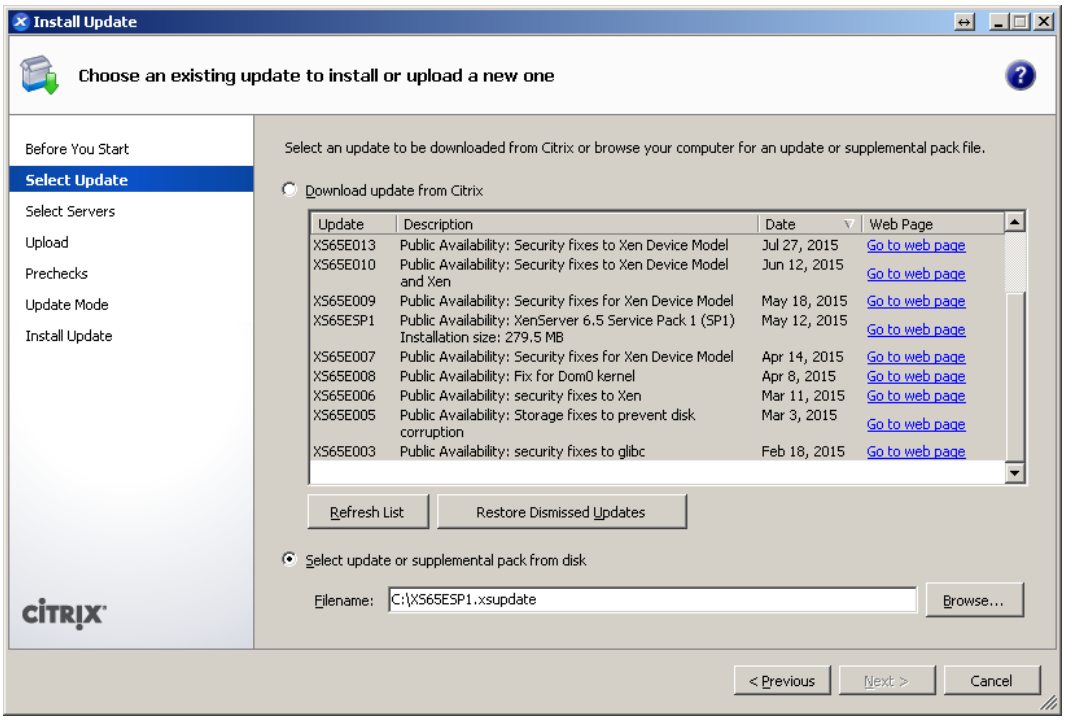


Figura 39 – Ventana de instalación de actualizaciones de XenCenter

Una vez obtenidas todas las actualizaciones en su formato de fichero con extensión "xsupdate", se colocarán en una carpeta y a través de SFTP deben copiarse en el servidor.

Este proceso se puede realizar con herramientas como Filezilla, gratuita y bajo la licencia GNU General Public License (GPL) versión 2. Para conectarse con el servidor es necesario crear un nuevo sitio, configurarlo como muestra la Figura 40 y pulsar el botón Conectar.

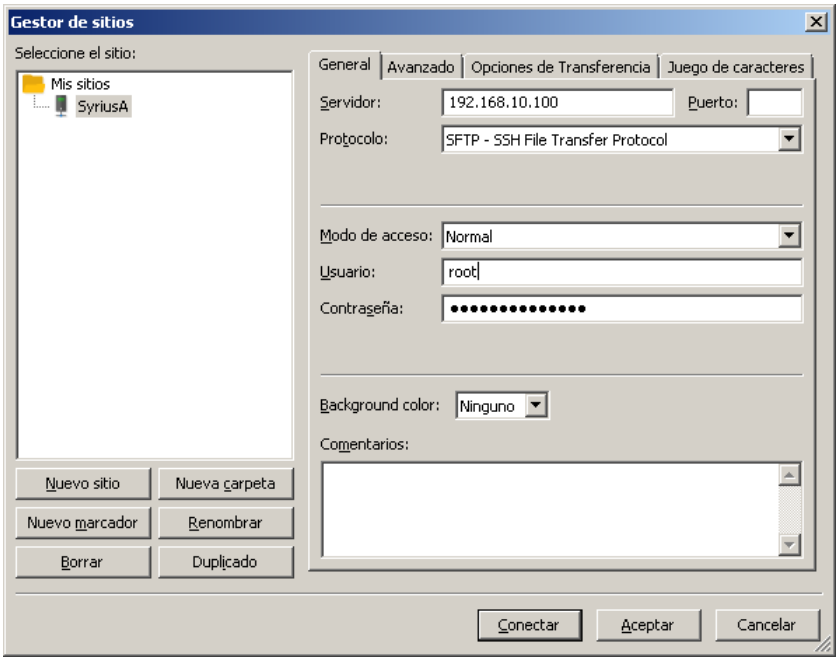


Figura 40 – Configurar conexión por SFTP a XenServer con Filezilla

Un lugar adecuado para subir la carpeta (p.ej. `updates`) con las actualizaciones es la carpeta `/tmp` del servidor, la carpeta de archivos temporales del sistema.

El script de actualización debe situarse en un fichero de texto con codificación UNIX, para que sea interpretado correctamente por el sistema, con extensión "sh", por ejemplo `updates.sh`.

El código propuesto para la instalación de las actualizaciones se muestra en la Tabla 7:

Tabla 7 – Script para instalar las actualizaciones de XenServer

```
#!/bin/bash
HOSTNAME=$(hostname)
HOSTUUID=$(xe host-list name-label=$HOSTNAME --minimal)

for PATCH in ./*
      do
            if [ -f $PATCH==updates.sh ]
            then
                  echo "Skiping $f file..."
                  continue
            fi
            if [ "$(echo "$PATCH" | head -c 1)" != '#' ]
            then
                  PATCHNAME=$(echo "$PATCH" | awk -F: '{
                    split($0,a,"/");split(a[2],b,"."); printf ("%s\n",
                    b[1]) }')
                  echo "Processing $PATCHNAME"
```

```
                    PATCHUUID=$(xe patch-list name-label=$PATCHNAME
                      hosts=$HOSTUUID --minimal)
                    if [ -z "$PATCHUUID" ]
                    then
                          echo "Patch not yet applied; applying .."
                          PATCHUUID=$(xe patch-upload file-name=$PATCH)
                          if [ -z "$PATCHUUID" ]
                          then
                                PATCHUUID=$(xe patch-list name-
                                  label=$PATCHNAME --minimal)
                          fi
                          xe patch-apply uuid=$PATCHUUID host-uuid=$HOSTUUID
                          xe patch-clean uuid=$PATCHUUID
                    else
                          echo "$PATCHNAME already applied"
                    fi
              fi
done
```

Este script comprueba uno por uno los ficheros en la carpeta en la que se encuentra, comprueba que realmente son ficheros de actualización de XenServer y a través de su identificador único (UUID) detecta si ya está instalado en el servidor, si es así, pasa al siguiente archivo, en caso contrario lo copia en la carpeta de actualizaciones de XenServer, lo instala y posteriormente lo borra de dicha carpeta.

El tamaño de la partición en la que XenServer copia los ficheros de actualización es limitado y por eso es necesario limpiar las actualizaciones completadas tras su instalación. El script muestra información durante el proceso de instalación que sirve para identificar el parche que está actualizando en ese momento y los paquetes que modifica dicha actualización.

Para lanzar este código, es necesario establecer una conexión de consola al servidor, ya sea a través de iBMC, de un cliente SSH o de la consola de XenCenter. Con cualquiera de estos métodos debe iniciarse sesión con el usuario *root* y aplicar las siguientes instrucciones:

Tabla 8 – Instrucciones para lanzar el script de actualizaciones

`[root@SyriusA ~]# cd /tmp`	# el directorio temporal
`[root@SyriusA tmp]# cd updates`	# la carpeta con los ".xsupdate"
`[root@SyriusA updates]# chmod +x updates.sh`	# dar permisos de ejecución al script
`[root@SyriusA updates]#./updates.sh`	# ejecución del script

Con dicho script el proceso de actualización que duraba horas, se ha reducido a 15 minutos obteniendo una mayor seguridad y estabilidad al mantener XenServer actualizado. El script permitirá instalar las mismas actualizaciones en otro servidor y con un pequeño cambio también servirá para actualizar *Pools* (agrupaciones) de servidores.

4.2.2. Crear una librería de imágenes ISO

Para instalar un sistema operativo en una máquina virtual en XenServer, es necesario definir una librería de imágenes ISO. Las opciones por defecto que permite XenServer son a través de *Windows File Sharing* (SMB/CIFS) o NFS ISO. Si no se dispone de estas posibilidades existe otra opción, crear una librería ISO en el disco duro de XenServer.

Este procedimiento se realiza a través de la consola de comandos desde XenCenter o a través de un cliente SSH. Las instrucciones se muestran en la Tabla 9.

Tabla 9 – Instrucciones para crear una librería de imágenes ISO

```
mkdir /var/run/sr-mount/UUID/ISOS

xe sr-create name-label=ISOS type=iso
     device-config:location=/var/run/sr-mount/UUID/ISOS
     device-config:legacy_mode=true content-type=iso
```

Se puede crear un enlace simbólico a una carpeta en la raíz del sistema para mayor comodidad:

```
ln -s /var/run/sr-mount/UUID/ISOS /ISOS
```

Sustituir UUID por el identificador de la partición (p. ej., b1c00e17-da19-6270-6ade-4ecbf34bc3e6).

A partir de este momento será posible subir las imágenes ISO al directorio `/ISOS` del sistema de archivos del XenServer y arrancar las máquinas virtuales desde ellas. Si las operaciones se realizaron correctamente, en XenCenter aparecerá un nuevo SR (Storage Repository) como muestra la Figura 41.

Figura 41 – Librería de ISOS creada

4.3. Conclusiones de la Fase I

Los procesos realizados durante la Fase I se resumen a continuación:

- Se comenzó instalando Citrix XenServer 7.0, el cual no funcionaba correctamente con los parámetros de fábrica. Para intentar subsanarlo, se actualizó la BIOS y el software de gestión del servidor, sin obtener un correcto funcionamiento.
- Con la ayuda del manual de referencia de Huawei sobre la configuración de la BIOS del equipo, se determinó que la configuración era correcta aún sin obtener el resultado esperado.
- Se instalaron las actualizaciones y parches de seguridad publicados por Citrix hasta que el equipo estuvo completamente actualizado, pero esto tampoco solucionó el problema.
- Por último, se contrastó la información disponible sobre compatibilidad de hardware y software en las webs de Citrix y Huawei. Mientras que Citrix afirma la compatibilidad de la versión 7.0, Huawei no la certifica.
- Por este motivo se tomó la determinación de instalar la versión 6.5 de XenServer que sí era compatible con el hardware del laboratorio.

5. FASE II: INSTALACIÓN DE OPENSTACK

Concluida la Fase I con un sistema operativo instalado, se detallan en este capítulo las pruebas y procedimientos realizados, así como los resultados obtenidos de los diferentes métodos de despliegue del entorno OpenStack sobre Citrix XenServer. Se persigue el objetivo de desplegar un Cloud privado utilizando soluciones en las que ya se tenía experiencia como DevStack y probando otras opciones compatibles con la versión de XenServer que soportan los servidores.

5.1. Instalación de DevStack

Las primeras pruebas de concepto que acercaban al concepto de Cloud vinieron de la mano de DevStack. DevStack fue una de las primeras plataformas que permitía al usuario hacerse una idea de qué era OpenStack con un despliegue rápido y sencillo en una máquina virtual. En un cliente de virtualización como VirtualBox, DevStack haría uso del hipervisor de tipo 2 o *hosted* de Oracle para correr las máquinas virtuales creadas con OpenStack. Lógicamente en un equipo con capacidades limitadas como puede ser un portátil, la creación de máquinas virtuales quedaba limitada a sistemas operativos ligeros que tu tuviese altos requisitos de hardware. Porque, aunque se hable de "memoria o almacenamiento virtual", la asignación de estos recursos nunca podrá ser superior a los recursos físicos de los que dispone el equipo.

Tras obtener una buena experiencia con estas pruebas, se decidió exportar la máquina virtual a XenServer de manera que se pudiese replicar este comportamiento en un sistema con muchos más recursos y capacidad de cómputo, algo que a priori parece sencillo y debiera funcionar.

Los problemas aparecieron por la falta de comunicación con el hipervisor Xen y por utilizar virtualización anidada. Se tuvo que buscar una herramienta que fuese compatible con XenServer y se encontró la solución Mirantis OpenStack para la que se había desarrollado un plugin que proporciona compatibilidad con la solución de Citrix.

5.2. Instalación de Mirantis con Fuel

Fuel es una aplicación software de código abierto que simplifica el despliegue de entornos Mirantis OpenStack y permite gestionar dichos entornos una vez desplegados [30]. Con esta herramienta es posible desplegar OpenStack tanto en entornos virtuales para realizar pruebas (VirtualBox o VMware), como en *bare-metal* (véase 2.1.3 Terminología de virtualización).

Fuel proporciona una interfaz de usuario de web, así como una interfaz de línea de comandos (CLI) y una API RESTful para provisión, configuración y administración de entornos de OpenStack. Tras el despliegue de OpenStack, Fuel muestra un enlace a la interfaz web de Horizon.

La arquitectura de Fuel incluye [30]:

- Nodo principal: Una máquina virtual con el software de Fuel instalado que realiza la configuración inicial, permite de arranque de los nodos auxiliares a través PXE, les provee de sistema operativo y les asigna las direcciones IP.
- Nodos auxiliares: son los servidores provistos por el nodo principal. Un nodo auxiliar de Fuel puede ser un nodo controlador (*controller*), de cómputo (*compute*) o de almacenamiento (*storage*) entre otros.

Para instalar OpenStack sobre Citrix XenServer de forma que utilice el hipervisor Xen, es necesario utilizar un *plugin* de Fuel que permita la comunicación entre OpenStack y el hipervisor. Este plugin se comunica utilizando la XAPI (véase 2.2.1.1 XAPI Toolstack) llamando a las funciones necesarias.

Existen requisitos previos al despliegue de Mirantis OpenStack como crear VLANs y el nodo maestro.

5.2.1. Crear VLANs de Fuel con XenCenter

El plugin de Fuel sólo es compatible con XenServer utilizando segmentación VLAN y necesita la arquitectura lógica que se muestra en la Figura 42 – Esquema de red para Mirantis OpenStack para funcionar:

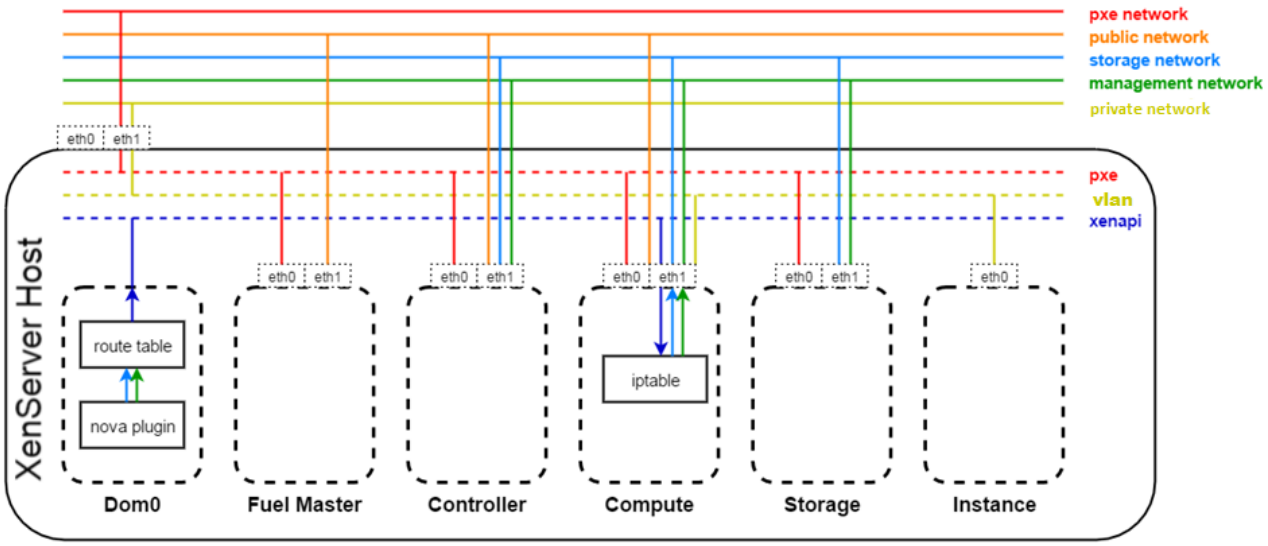


Figura 42 – Esquema de red para Mirantis OpenStack [31]

Para conseguir dicha topología lógica de red, es necesario crear las VLANs desde XenCenter. Cada VLAN debe asociarse a un interfaz de red físico y debe tener un identificador numérico.

Una vez añadido el servidor en XenCenter a través de su dirección IP y las credenciales, se añaden nuevas redes con los parámetros de la Tabla 10 como muestra la Figura 43.

Tabla 10 – Redes necesarias para Mirantis OpenStack a crear en XenServer

Tipo de Red	**Nombre**	**NIC**	**VLAN**
External Network	PXE	NIC1	99
External Network	Management	NIC1	101
External Network	Storage	NIC1	102

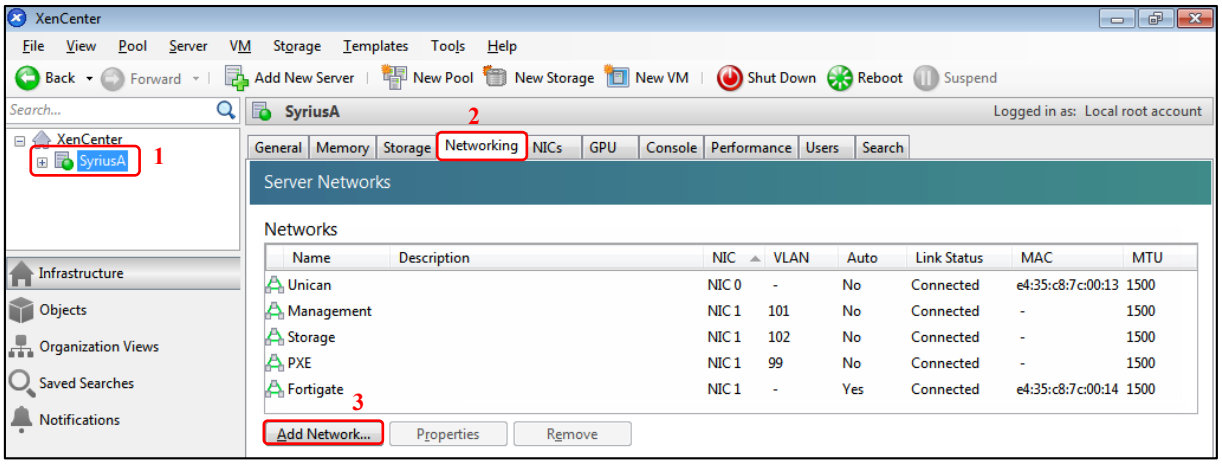


Figura 43 – Añadir redes en XenServer a través de XenCenter

5.2.2. Crear el nodo maestro de Fuel

La ISO de instalación de Mirantis se descarga desde su propia web oficial [32]. Es importante reseñar que no hay compatibilidad del plugin para XenServer 6.5 más allá de la versión 9.2 de Mirantis [33].

Una vez obtenida la imagen ISO, debe copiarse por SFTP o SCP a la librería de ISOS creada en XenServer (véase 4.2.2 Crear una librería de imágenes ISO). Una vez subida, se debe actualizar el repositorio para que detecte la nueva imagen y crear la nueva máquina virtual, para ello seguir los pasos que se muestran en la Figura 44.

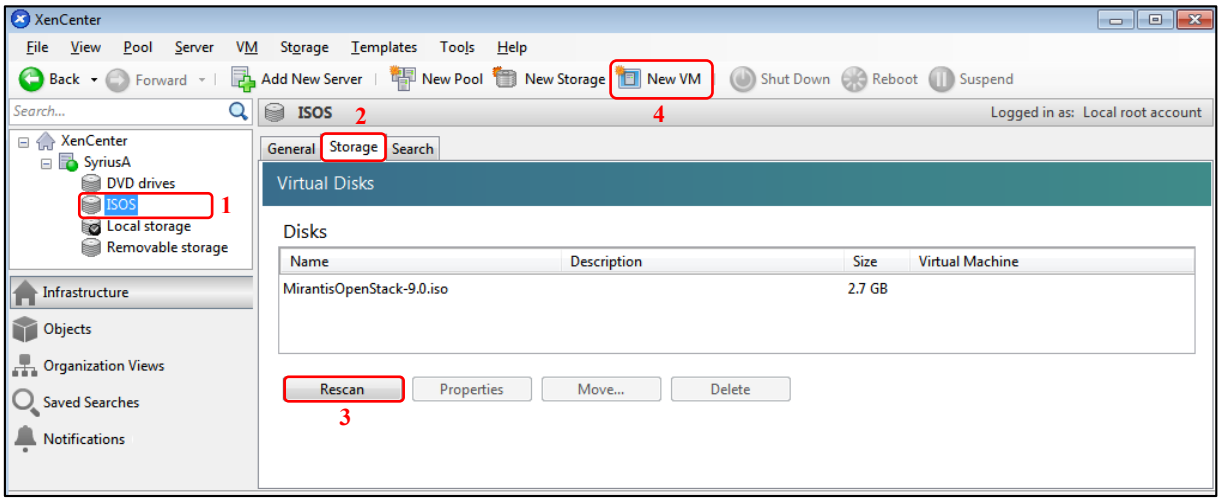


Figura 44 – Actualizar la librería de ISOS

Procedimiento

Paso 1 En el asistente de creación de máquinas virtuales, seleccionar la plantilla *Other Install Media* para forzar que la máquina virtual sea HVM (virtualizada en hardware).

Paso 2 Establecer el nombre de la máquina virtual (p. ej., Fuel Master).

Paso 3 El método de instalación del sistema operativo seleccionar *Install from ISO library* y elegir la imagen *MiratisOpenStack-9.0.iso*.

Paso 4 Elegir el servidor donde se alojará, en este caso SyriusA.

Paso 5 Asignar a la máquina 4 CPUs virtuales (vCPU) y 4 GB de memoria RAM.

Paso 6 Añadir un nuevo disco duro virtual de tamaño 50 GB.

Paso 7 Añadir las interfaces de red FortiGate (física) y PXE (VLAN).

Paso 8 Se muestra una pantalla resumen (véase Figura 45) y se termina haciendo clic en *Create Now*.

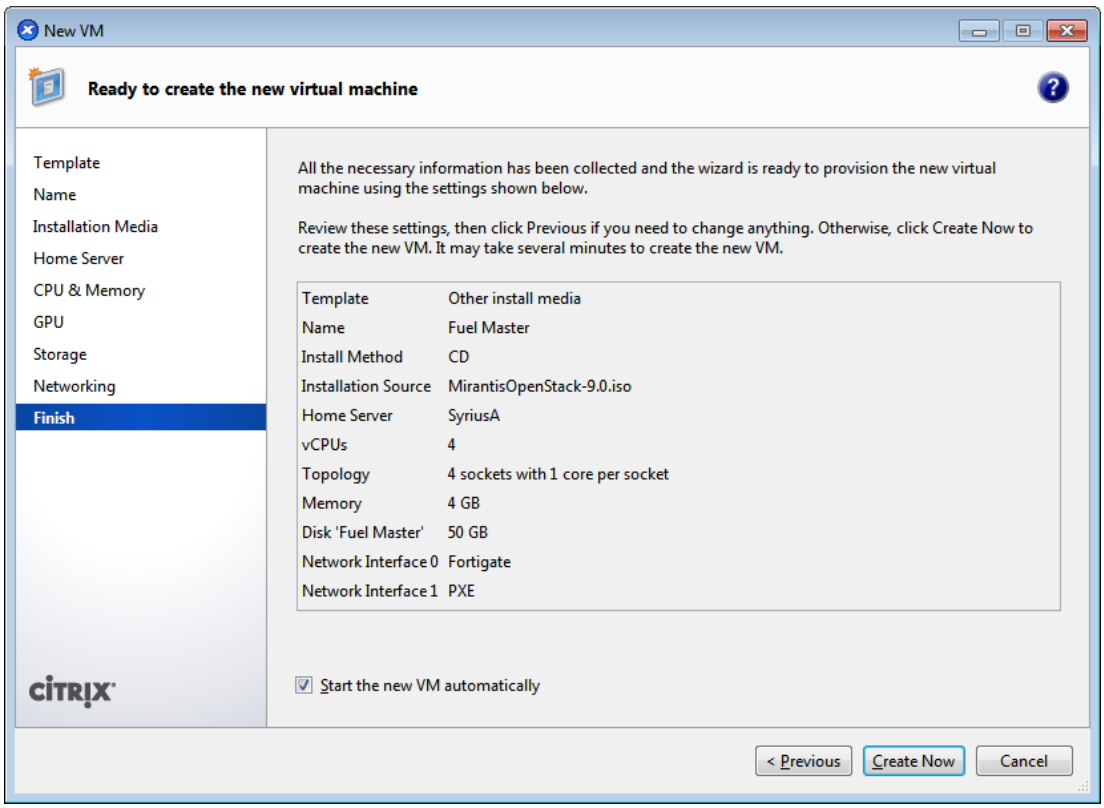


Figura 45 – Ventana resumen de creación de la máquina virtual Fuel Master

Paso 9 La máquina se iniciará y comenzará el proceso de instalación. Se reiniciará una vez, en ese momento debe desconectarse el medio virtual de instalación, para ello marcar la opción *<empty>* en la barra *DVD Drive 1* que se encuentra justo encima de la consola virtual en XenCenter.

Paso 10 Aparecerá la pantalla de configuración de Fuel. El primer aviso es cambiar la contraseña de administrador de Fuel.

Paso 11 Configurar las interfaces *eth0* (FortiGate) y *eth1* (PXE) como se muestra en la Figura 46. Es importante configurarlas de acuerdo al orden en el que se añadieron durante el proceso de creación de la máquina virtual.

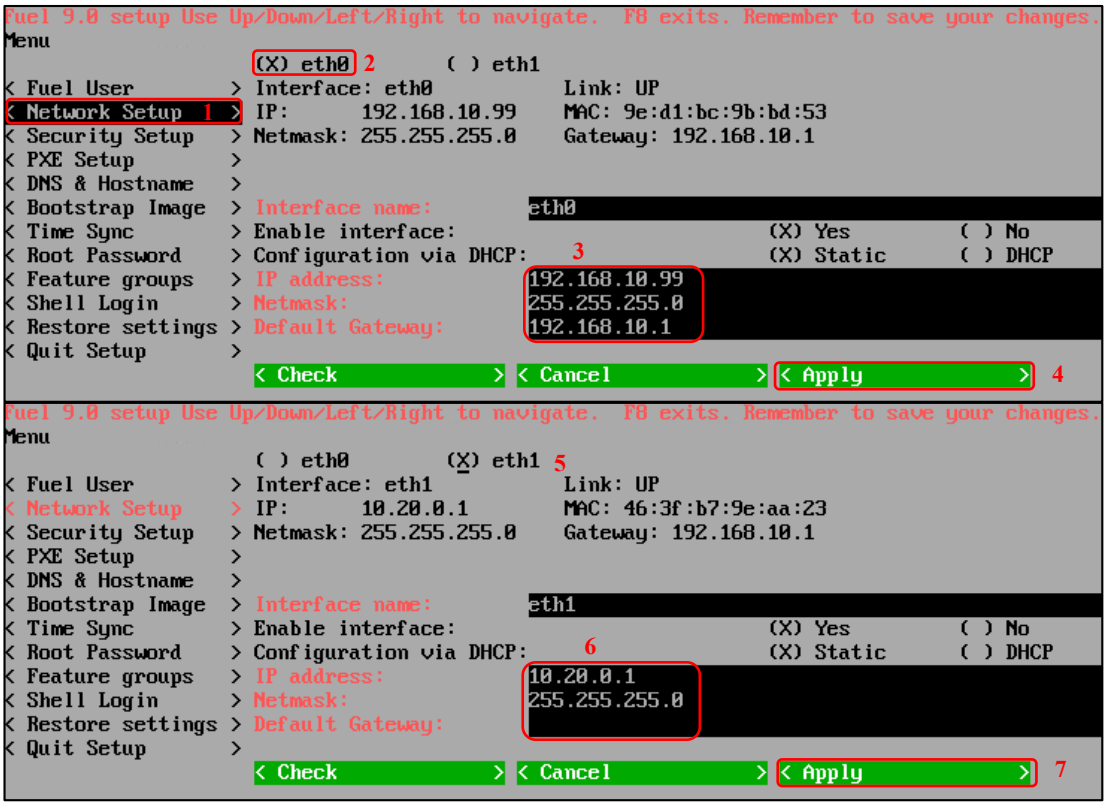


Figura 46 – Configuración de interfaces de red en Fuel Master

Paso 12 En el apartado *Security Setup* se puede limitar el acceso a esta máquina por SSH a partir de la IP de la red y la máscara de subred en formato CIDR. Si se desea que sea accesible desde cualquier dirección utilizar *0.0.0.0/0*.

Paso 13 En *PXE Setup* seleccionar el interfaz PXE de acuerdo a la Figura 47. Se establece el rango de direcciones de DHCP que Fuel asignará a los nodos auxiliares para su descubrimiento y aprovisionamiento.

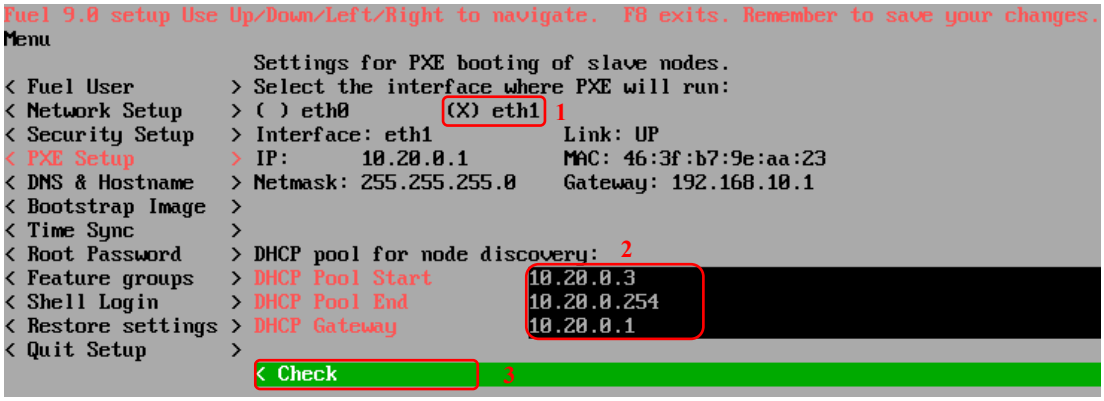


Figura 47 – Configuración de interfaz PXE Fuel Master

Paso 14 Establecer los DNS y el *Hostname*.

Paso 15 En el campo *Time Sync* fijar las direcciones de los servidores NTP.

Paso 16 Por último, dirigirse a *Quit Setup* y marcar *Save and Quit*. Realizará las comprobaciones pertinentes y finalizará la configuración mostrando la pantalla de inicio en el terminal como muestra la Figura 48.

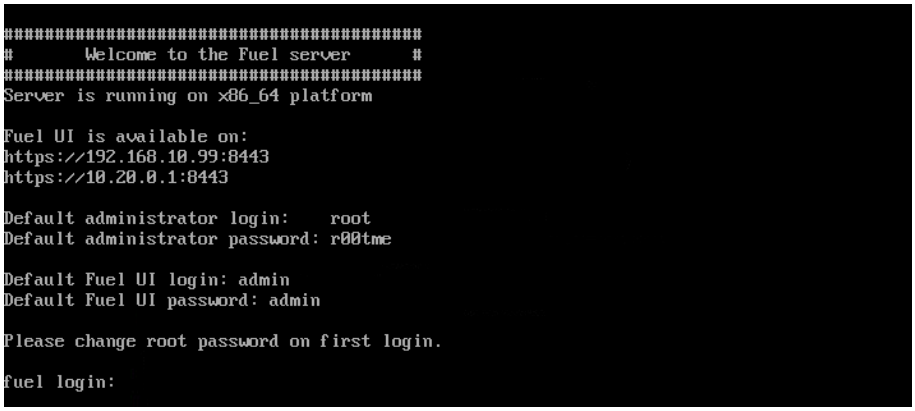


Figura 48 – Mensaje de inicio de Fuel

5.2.2.1. Actualizar a Fuel 9.2

Tras completar la instalación de la máquina virtual, hay que identificarse como usuario *root* en el nodo maestro de Fuel e introducir las instrucciones en el orden mostrado en la Tabla 11 para completar el proceso de actualización. Este proceso puede durar hasta una hora, en función de la velocidad de la conexión a internet.

Tabla 11 – Instrucciones para actualizar Fuel a la versión 9.2

```
[root@fuel ~]# yum install -y http://mirror.fuel-
     infra.org/mos-repos/centos/mos9.0-centos7/9.2-updates/x86_64/Package
     s/mos-release-9.2-1.el7.x86_64.rpm
[root@fuel ~]# yum clean all
[root@fuel ~]# yum install -y mos-updates
[root@fuel ~]# cd mos_playbooks/mos_mu/
[root@fuel mos_mu]# ansible-playbook playbooks/mos9_prepare_fuel.yml
[root@fuel mos_mu]# ansible-playbook playbooks/update_fuel.yml -e
     '{"rebuild_bootstrap":false}'
[root@fuel mos_mu]# ansible-playbook
     playbooks/mos9_fuel_upgrade_kernel_4.4.yml
```

Para comprobar que la actualización se completó correctamente:

```
[root@fuel mos_mu]# fuel2 fuel-version
  openstack_version: mitaka-9.0
  release: '9.2'
```

5.2.2.2. Instalar Plugin de Fuel para XenServer

El plugin de Fuel para XenServer se puede obtener descargándolo de la web http://ca.downloads.xensource.com/OpenStack/Plugins/Fuel-4.0.37/fuel-plugin-xenserver-4.0-4.0.37-1.noarch.rpm.

Para instalar el plugin es necesario subirlo a la máquina virtual de Fuel por SFTP o SCP a una carpeta temporal (p. ej., `/tmp`). Una vez subido utilizar las instrucciones de la Tabla 12 para instalarlo y comprobar que efectivamente ha sido registrado por Fuel.

Tabla 12 – Instrucción para instalar el plugin de XenServer para Fuel

```
[root@fuel ~]# fuel plugins --install
     /tmp/fuel-plugin-xenserver-4.0-4.0.37-1.noarch.rpm
```

Se puede comprobar su instalación con la instrucción:

```
[root@fuel ~]# fuel plugins
   id | name                   | version | package_version | releases
   ---+------------------------+---------+-----------------+--------------------
   1  | fuel-plugin-xenserver | 4.0.37  | 4.0.0           | ubuntu (mitaka-9.0)
```

La instrucción para eliminar el plugin es la siguiente:

```
[root@fuel ~]# fuel plugins --remove fuel-plugin-xenserver==4.0.37
```

5.2.3. Crear los nodos auxiliares Compute, Controller y Storage

Una vez configurado el nodo maestro de Fuel, se crean los nodos auxiliares. Para ello se hace uso del asistente de creación de máquinas virtuales de XenCenter. El siguiente procedimiento debe realizarse tres veces, una por cada nodo auxiliar, cambiando la configuración según se indica a continuación.

Procedimiento

Paso 1 En el asistente de creación de máquinas virtuales, seleccionar la plantilla *Other Install Media* para que las máquinas creadas sean HVM (virtualizadas en hardware).

Paso 2 Establecer el nombre de la máquina virtual (*Compute* | *Controller* | *Storage*).

Paso 3 Seleccionar *Boot from network* como el método de instalación del sistema operativo.

Paso 4 Elegir el servidor donde se alojará, en este caso SyriusA.

Paso 5 Para el *Compute*: 4 CPUs virtuales (vCPU) y 4 GB de memoria RAM.

Para el *Controller*: 4 CPUs virtuales (vCPU) y 6 GB de memoria RAM.

Para el *Storage*: 4 CPUs virtuales (vCPU) y 4 GB de memoria RAM.

Paso 6 Para el *Compute*: Disco duro virtual de 60 GB.

Para el *Controller*: Disco duro virtual de 80 GB.

Para el *Storage*: Disco duro virtual de 70 GB.

Paso 7 Añadir las interfaces de red FortiGate (física) y PXE (VLAN).

Antes de desplegar OpenStack es necesario añadir una interfaz de gestión interna en el nodo auxiliar *Compute* con un plugin de XenCenter, HIMN.

5.2.3.1. Configurar interfaz XAPI en el Compute con HIMN

El nodo Compute debe comunicarse con el Dom0 de XenServer a través de XAPI. Para ello utiliza una red especial que permite comunicar máquinas virtuales con el dominio de control. Dicha red se denomina *Host Internal Management Network* (HIMN) y existe un plugin para XenCenter, que permite añadir una interfaz XAPI a las máquinas virtuales de forma muy sencilla. [34]

Primero se descarga el plugin desde la misma web que donde se obtuvo el de XenServer para Fuel (http://ca.downloads.xensource.com/OpenStack/Plugins/SetupHIMN-1.0.2.zip).

XenCenter debe estar cerrado para proceder con la instalación, una vez terminada se arranca de nuevo. Con la máquina virtual Compute apagada se hace clic con el botón derecho del ratón sobre ella y se seleccionar la opción *Manage Internal Management Network*. Aparecerá una nueva ventana en la que se debe pulsar el botón *Add* para añadir la nueva interfaz de gestión interna como muestra la Figura 49.

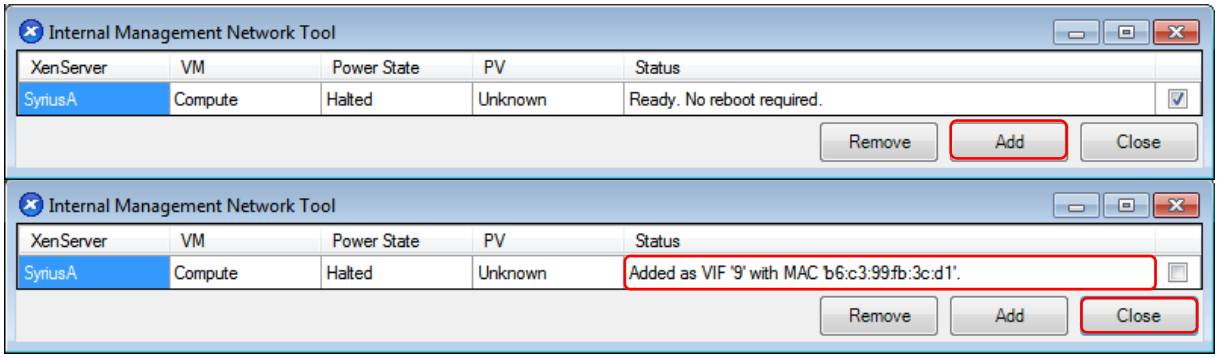


Figura 49 – Configurar la interfaz de gestión interna en el Compute con el plugin HIMN

5.2.4. Crear entorno OpenStack

Con los requisitos previos cumplidos, ya se puede desplegar Mirantis OpenStack. El primer paso es encender las máquinas virtuales Compute, Controller y Storage y que arranquen obteniendo una dirección IP proporcionada por el nodo Fuel a través de PXE.

Ahora se accede a la web de administración de Fuel configurada anteriormente (véase Figura 48) en la que hay que identificarse con el nombre de usuario *admin* y la contraseña establecida previamente en el apartado 5.2.2 Crear el nodo maestro de Fuel. En la siguiente pantalla pinchar en *New OpenStack Environment* (véase Figura 50).

Figura 50 – Crear nuevo entorno OpenStack en Mirantis

A continuación, se muestran los parámetros de configuración del entorno. Se establece un nombre al entorno (p. ej., Syrius). Se selecciona la opción XenServer como muestra la Figura 51, previa instalación del plugin de Fuel para XenServer.

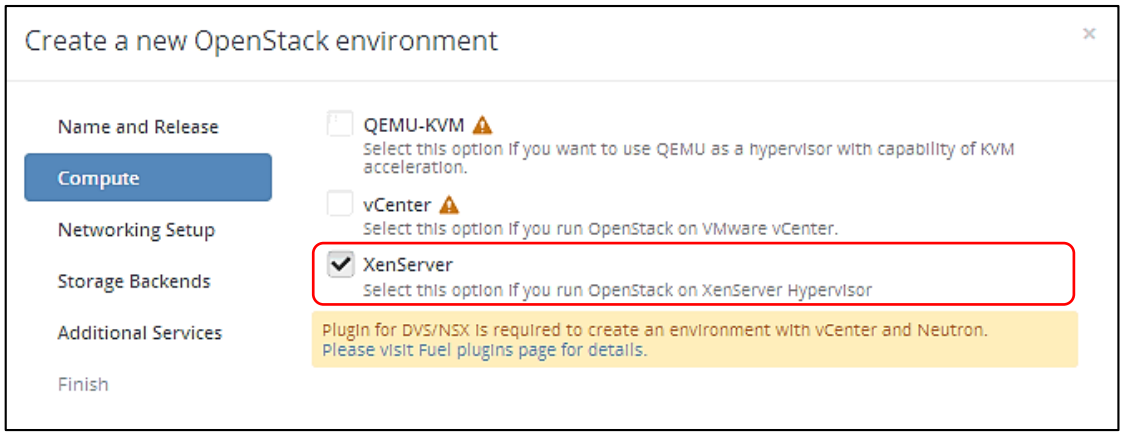


Figura 51 – Selección del hipervisor durante el despliegue de Mirantis OpenStack

Para el resto de parámetros se utiliza la configuración por defecto. La configuración de red que permite XenServer es segmentación VLAN y el almacenamiento de tipo LVM. Al terminar pulsar el botón *Create*. El siguiente paso es establecer la contraseña de *root* del XenServer en el apartado *Compute* de la sección *Settings*, para que el plugin se pueda comunicar con el hipervisor.

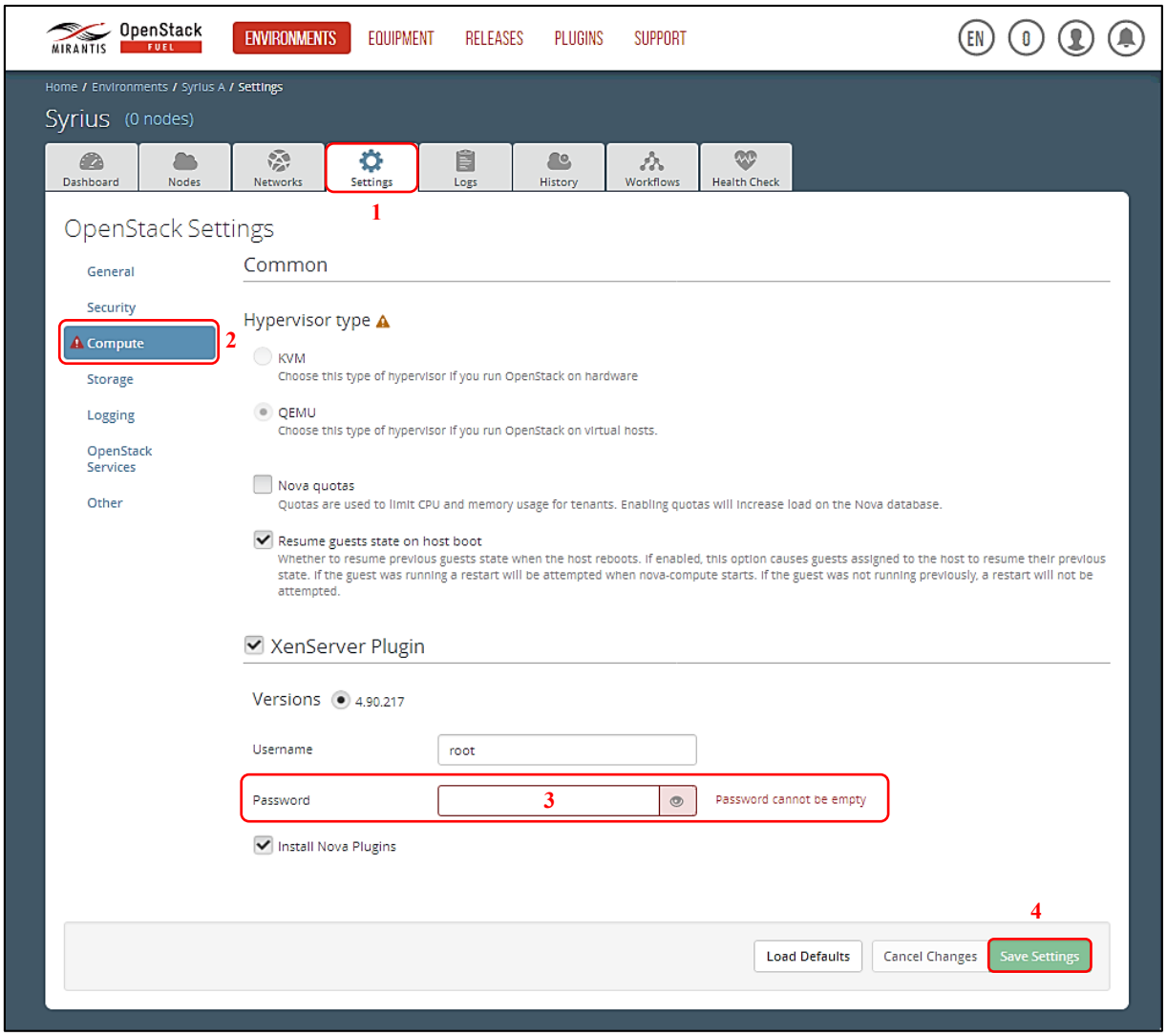


Figura 52 – Configurar la contraseña de administrador para el plugin de Fuel

El siguiente paso es añadir los nodos auxiliares detectados a través de PXE. En la sección *Nodes* agregar dichos nodos en función de su rol. Los nodos se pueden identificar por los últimos caracteres de la dirección MAC su interfaz de red PXE. Es recomendable cambiar su nombre identificativo y su nombre de dominio (*hostname*) para que posteriormente sea más sencillo identificar cualquier problema y conectarse a ellos por SSH. Con el botón *Add nodes* se añaden nodos una vez seleccionado su rol.

La configuración de red de los nodos se muestra en la Figura 53. El nodo Compute tiene un interfaz adicional, el de la red HIMN (véase 5.2.3.1 Configurar interfaz XAPI en el Compute con HIMN) que se muestra y debe quedar vacío.

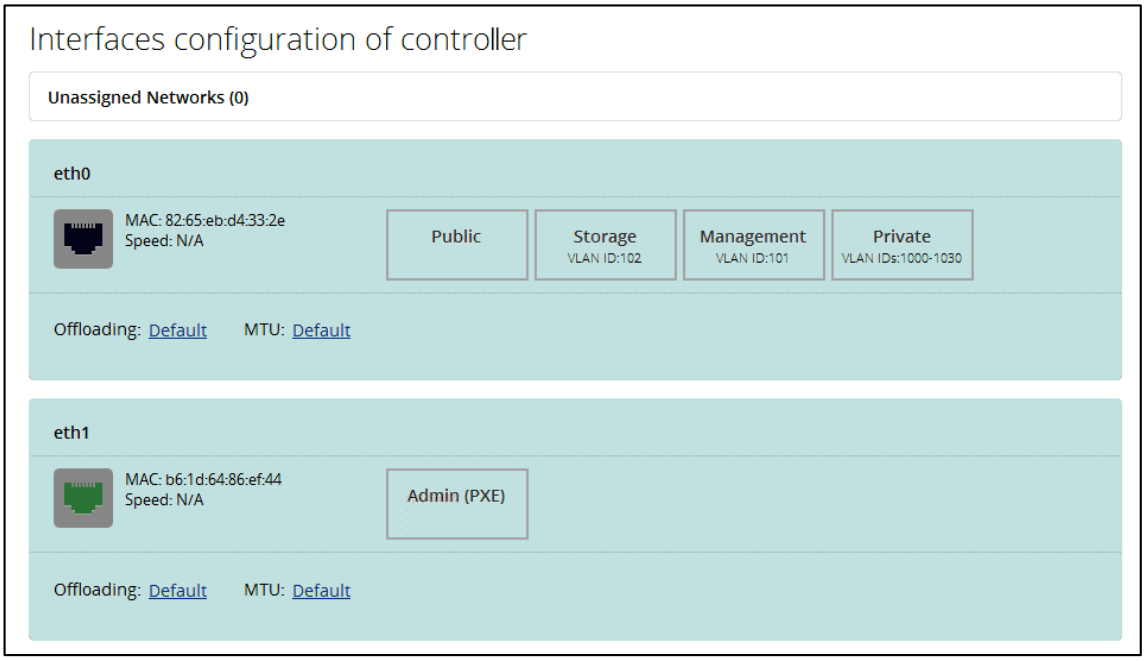


Figura 53 – Configuración de interfaces del nodo Compute

Tras añadir todos los nodos, es el momento de configurar las redes necesarias. En la sección *Networks* configurar, en el perfil por defecto (*default*), la red pública que corresponde a las direcciones IP que podrán tomar los nodos auxiliares del rango del FortiGate (véase 3.1 Esquema del laboratorio).

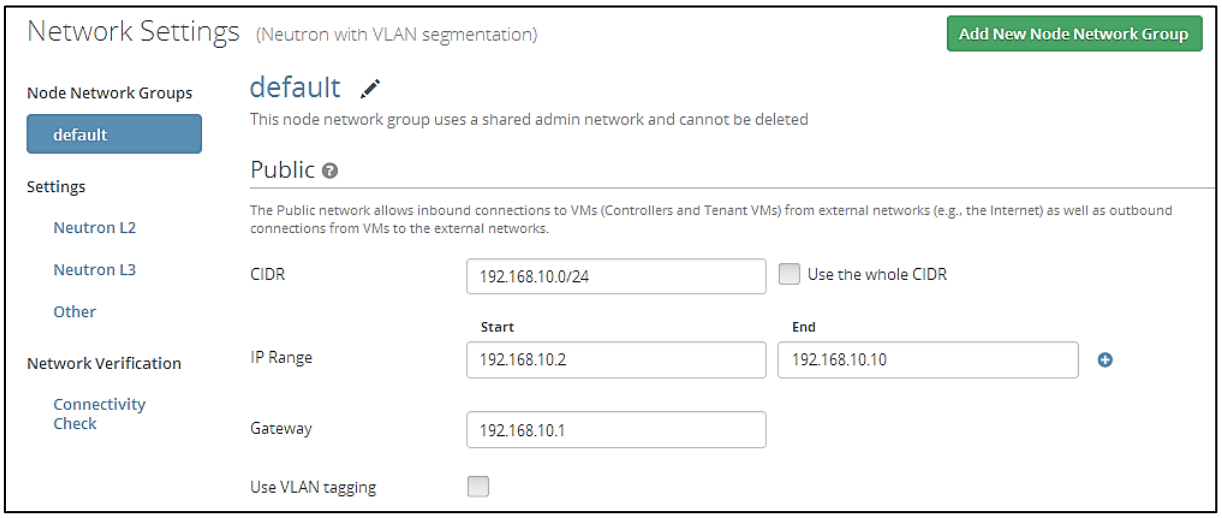


Figura 54 – Configuración de la red pública para los nodos auxiliares

Si se ha utilizado la misma configuración detallada en el apartado 5.2.1 Crear VLANs de Fuel con XenCenter, el resto de la configuración de esta pestaña se deja con las opciones por defecto.

En la pestaña *Neutron L3* se establecen las direcciones flotantes de la red pública y la red privada para las máquinas virtuales.

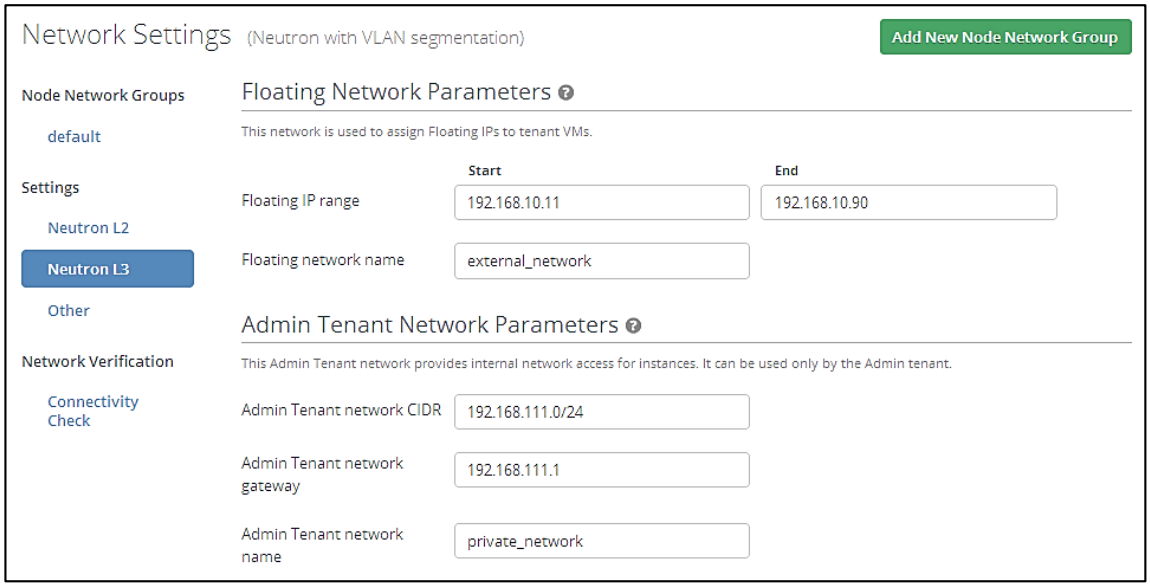


Figura 55 – Configuración de la red pública y privada para las máquinas virtuales

Tras guardar la configuración se suele realizar un test de conectividad (*Connectivity Check*) para comprobar el correcto funcionamiento de las redes. Si el resultado ha sido correcto se puede comenzar con el despliegue desde la pestaña *Dashboard* pulsando en el botón *Deploy Environment*. El proceso tarda cerca de una hora en la que se instalarán los sistemas operativos de los nodos auxiliares y se configurará el entorno OpenStack.

Al finalizar este proceso aparecerá un mensaje de éxito y un enlace a la interfaz web de Horizon como muestra la Figura 56.

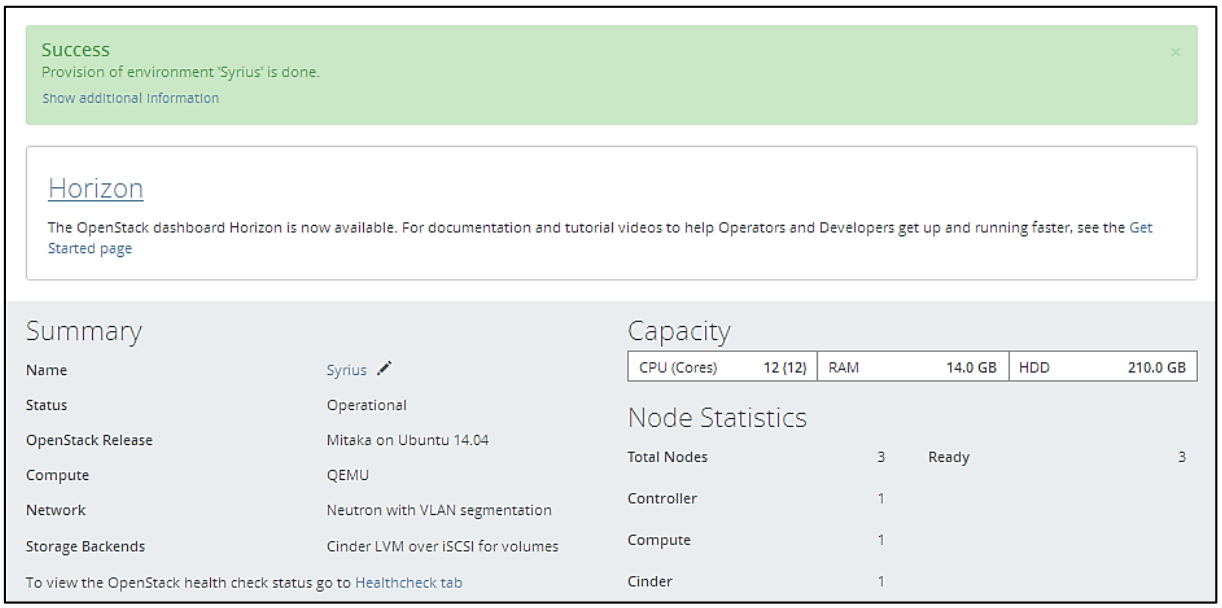


Figura 56 – Mensaje de éxito en el despliegue del entorno OpenStack

Desde la pestaña *Health Status* es posible realizar un conjunto de pruebas que confirman el correcto funcionamiento de todas las características del entorno.

Ya será posible acceder al entorno a través del enlace a Horizon. Fuel asigna una dirección IP virtual para esta interfaz web, en este caso ha sido la 192.168.10.3. Para que esta interfaz web sea accesible a través de la IP pública de la red de la Universidad de Cantabria, deben añadirse ciertas reglas a las `iptables` de XenServer como se muestra en la Tabla 13.

Tabla 13 – Instrucciones para redirigir el tráfico del puerto 80 de un interfaz físico a la IP de Horizon

```
iptables -t nat -A POSTROUTING --out-interface xenbr1 -j MASQUERADE
iptables -A FORWARD --in-interface xenbr0 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -i xenbr0 -m tcp --dport 80 -j DNAT
--to-destination 192.168.10.3:80
```

Estas instrucciones permiten que la interfaz física con la IP pública (*xenbr0*) pueda reenviar paquetes entrantes y traducir la dirección de destino de las peticiones que lleguen al puerto 80 por la dirección virtual de Horizon, utilizando como dirección de origen la dirección IP de la interfaz conectada a la red del FortiGate.

5.3. Conclusiones de la Fase II

Del proceso de instalación del entorno Cloud se recogen las siguientes impresiones:

- La migración de una máquina virtual donde el entorno DevStack ya estaba desplegado, al igual que un nuevo despliegue creando DevStack desde cero, fueron procesos realizados pero infructuosos.
- Por la incompatibilidad de ejecutar de DevStack sobre XenServer, se decidió probar otra solución diseñada para tal efecto, Mirantis OpenStack.
- Uno de los mayores problemas previos a la instalación de Mirantis fue comprender su arquitectura de red, que nada o poco tiene que ver con la de OpenStack e implementarla en XenServer para que el despliegue del entorno Cloud pudiese realizarse correctamente.
- Tras infinidad de pruebas de despliegue se consiguió un entorno Cloud OpenStack en el que algunas funcionalidades básicas no estaban disponibles, tales como el arranque de una máquina virtual desde una imagen ISO, la ejecución de sistemas operativos que tengan una interfaz gráfica o utilizar la consola de XenServer para gestionar OpenStack. Y todo ello a pesar de que el despliegue de OpenStack es correcto según el *Health Status* de Fuel, que prueba el correcto funcionamiento de todas las operaciones posibles a realizar en el entorno.
- Como punto negativo decir que cualquier operación se demora más de lo debido, tanto en la interfaz web como en la consola del Nodo Controller al que se le han asignado más recursos de los recomendados en la literatura. Sólo utilizar el comando `glance image-list`, para ver la lista de imágenes que tiene registradas Glance, tarda alrededor de 1 minuto.
- Por tanto, se tuvo que buscar otra solución que no presentase todos estos problemas recurriendo a las opciones de software libre de código abierto.

6. FASE III: INSTALACIÓN DE CENTOS 7 CON PACKSTACK

Debido a que las pruebas realizadas en la Fase II no fueron satisfactorias, este capítulo presenta otra alternativa al uso de Citrix XenServer de software libre y código abierto. Se hace uso del sistema operativo CentOS 7 y de su hipervisor KVM junto con la herramienta RDO PackStack para el despliegue del Cloud OpenStack, el cual permite utilizar la última versión existente en los repositorios oficiales.

6.1. Instalación de CentOS 7

CentOS (*Community ENTerprise Operating System*) es un sistema operativo Linux que proviene de la distribución Red Hat Enterprise Linux (RHEL). Red Hat se compone de software libre y código abierto, y publican parte del código fuente bajo la licencia GNU General Public License (GPL). A partir del código fuente, la comunidad de CentOS compila y distribuye el sistema operativo como software libre también bajo la licencia GPL o, de forma coloquial, Copyleft [35]. En 2014, CentOS unió fuerzas con Red Hat, quien pasaría a apadrinar dicho proyecto.

Se define como un sistema operativo robusto, estable, de fácil instalación y uso. Además, todas las versiones del operativo tienen soporte por parte de la comunidad durante los diez años siguientes a su lanzamiento.

Una de las ventajas de CentOS frente a otros sistemas operativos es que su proceso de instalación es personalizable, pudiendo decidir qué paquetes se instalarán con un sólo clic. Ofrece una gran variedad de configuraciones predefinidas de instalación para adaptarse a los requerimientos del usuario. A continuación, se muestra el proceso de instalación con las opciones elegidas para este entorno.

La versión utilizada es la 7 y la instalación se realiza a través de la ISO con la versión "*Everything*" [36] obtenida desde la web oficial. A continuación, se detalla el proceso de instalación y las opciones elegidas durante la instalación.

Procedimiento

Paso 1 Acceder al software de administración iBMC a través del puerto de administración e identificarse con las credenciales correctas.

Paso 1 Abrir la Consola Virtual Remota del software de administración iBMC.

Este procedimiento se detalla en el apartado 3.2.1 iBMC y acceso a la Consola Virtual Remota.

Paso 2 Apagar el equipo, *Power Management > Normal Power Off*, como se muestra en la Figura 30.

Paso 3 Utilizar el icono *CD/DVD,* como se muestra en la Figura 34, para cargar la ISO de instalación de CentOS 7.

Paso 4 Seleccionar la opción *Image File*.

Paso 5 Hacer clic en *Browse* y seleccionar la ISO de instalación de CentOS previamente descargada.

Paso 6 Pinchar el botón *Connect* para activar el lector de CD virtual.

Paso 7 Encender el quipo, *Power Management > Power On* y arrancar desde la ISO modificando la prioridad de arranque en la BIOS o con el *Boot Manager* (tecla F11).

Paso 8 Para comenzar el proceso de instalación se selecciona la opción *Install CentOS Linux 7*.

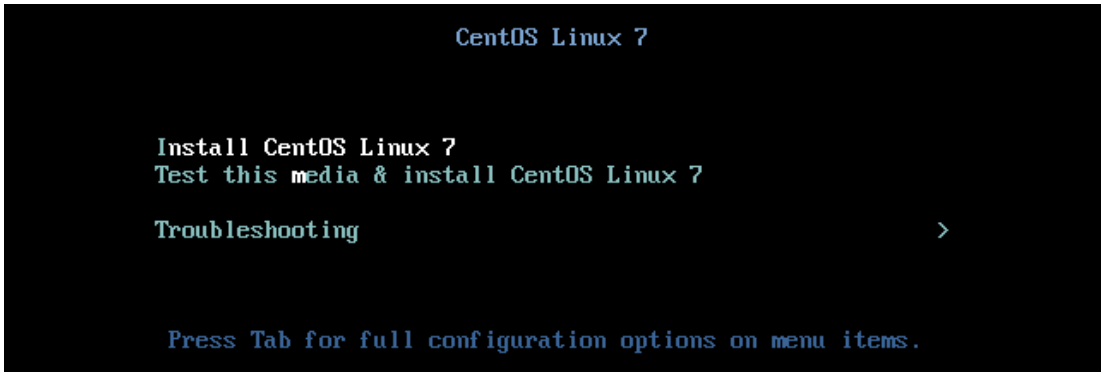


Figura 57 – Pantalla inicial de la instalación de CentOS 7

Paso 9 Seleccionar el idioma de la instalación.

Paso 10 Configurar los parámetros de localización como la zona horaria, el tipo de teclado y el soporte de idiomas para el sistema operativo.

Paso 11 Hacer clic en la pestaña *Software Selection* para elegir el software que se instalará con CentOS.

Nótese que la configuración elegida instala más características de las necesarias, pero se ha instalado alguna más por comodidad y pensando en futuros nuevos usos. La pre-configuración de *Virtualization Host*, sería suficiente para este cometido, pero se ha escogido la opción *Server with GUI* que proporciona además interfaz gráfica para una experiencia más cómoda.

Las opciones elegidas en dicha pre-configuración son las siguientes:

- **File and Storage Server**: Servidor de almacenamiento que soporta CIFS, SMB, NFS, iSCSI, etc.
- **Hardware Monitoring Tools**: Herramientas de monitorización de hardware.
- **Java Platform**: Java para CentOS.
- **Network File System Client**: Permite conectar almacenamientos de red.
- **Performance Tools**: Herramientas de rendimiento.
- **Remote Management for Linux**: Herramientas de monitorización como SNMP.
- **Virtualization Client**: Cliente de gestión de máquinas virtuales
- **Virtualization Hypervisor**: El hipervisor de virtualización.
- **Virtualization Tools**: Herramientas de gestión de imágenes virtuales.
- **Development Tools**: Herramientas de desarrollo como `make`, `gcc`, etc.
- **Security Tools**: Herramientas de seguridad.

Paso 12 En el apartado *Installation Destination* seccionar el disco duro existente.

En la sección *Other Storage Options* seleccionar *I will configure partitioning* y a continuación pulsar el botón *Done*, la configuración de particiones se muestra en la Figura 58.

Paso 13 En la nueva ventana seleccionar como esquema de particionado *LVM Thin Partitioning.*

Posteriormente pinchar en la opción *Click here to create them automatically*, para crear las particiones del sistema necesarias

Paso 14 Reducir el tamaño de la partición raíz "/" para poder crear la partición de usuario en `/home`.

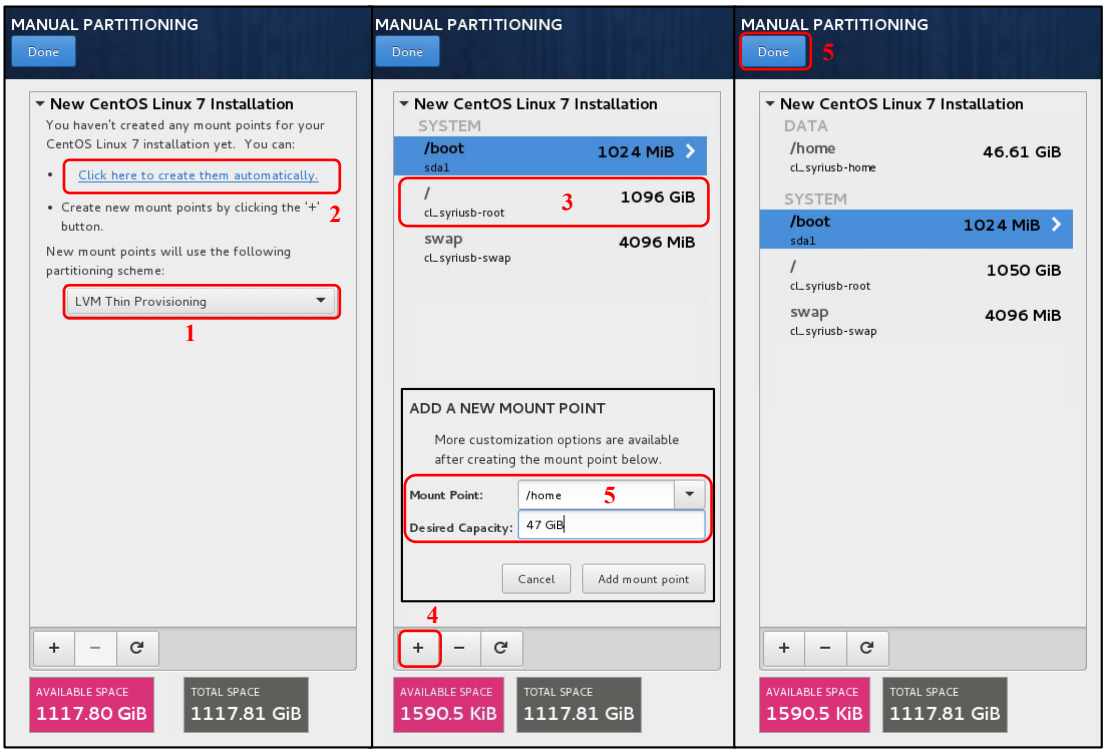


Figura 58 – Configuración de almacenamiento de CentOS 7

Paso 15 En el apartado *Network & Host Name* se configuran los interfaces de red, de momento se configura sólo el interfaz de la red interna.

Seleccionar el adaptador Ethernet *enp2s0f1*.

Hacer clic en el botón *Configure*

Dirigirse a la pestaña *IPv4 Settings*

En el campo *Method* seleccionar *Manual*

En la sección *Addresses* hacer clic en *Add* y establecer:

- *IP*: 192.168.10.101
- *Netmask*: 24
- *Gateway*: 192.168.10.1
- *DNS server*: 8.8.8.8

Hacer clic en el botón *Save*.

Establecer el *Host name* como *syriusb* y pulsar en *Apply*

Paso 16 En el apartado *Security Policy* seleccionar el perfil *Default*.

Paso 17 Con todo configurado pulsar el botón *Begin Installation*.

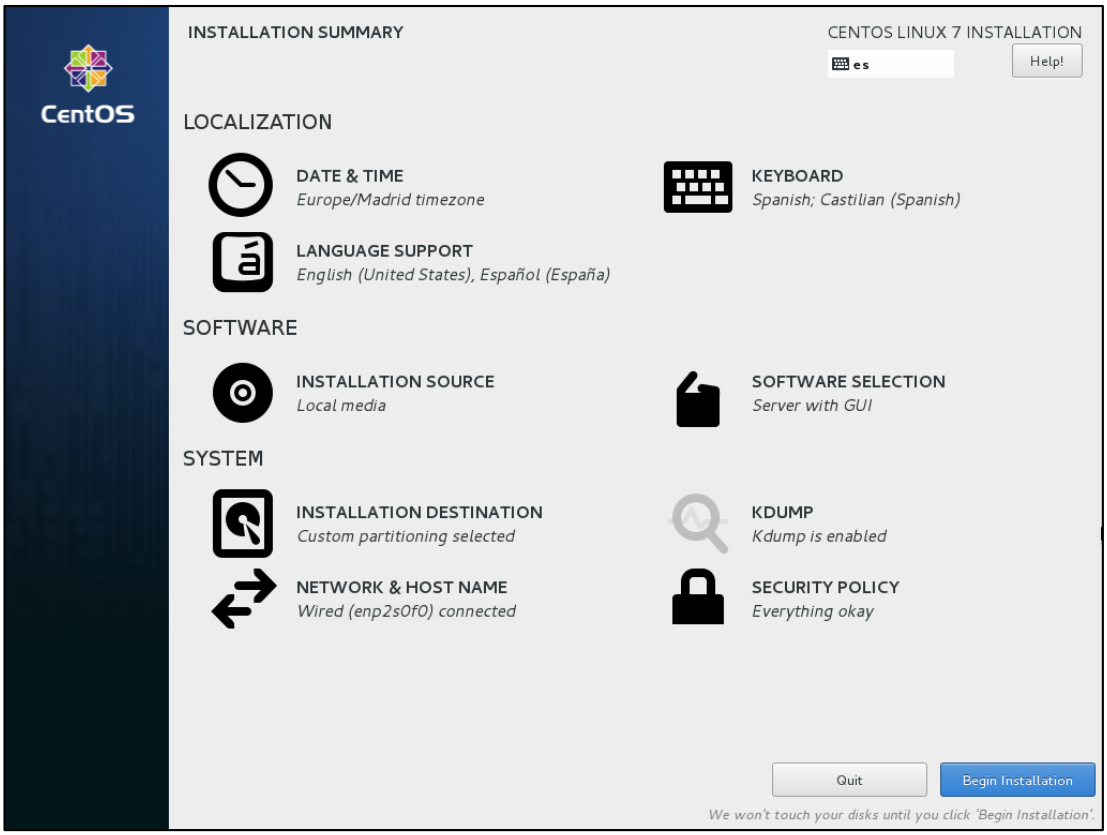


Figura 59 – Ventana resumen de la instalación de CentOS 7

Paso 18 Establecer la contraseña del usuario privilegiado *root* y crear un nuevo usuario.

Se recomiendo crear un usuario que tenga privilegios de administrador pero que no trabaje de forma permanente en modo privilegiado (como lo hace usuario *root*) por cuestiones de seguridad.

Figura 60 – Ventana de configuración de usuarios de CentOS 7

Paso 19 Tras reiniciar el equipo hay que aceptar la licencia y los términos de condiciones para poder utilizar CentOS.

Paso 20 Una vez completada la instalación se configura la interfaz Ethernet conectada a la red de la Universidad con una IP pública.

Nótese que no es recomendable asignar una dirección pública a la interfaz física de un equipo, es más seguro establecerla en la interfaz de una máquina virtual dado que es un entorno aislado y un acceso no autorizado no obtendría el control del equipo físico. En este caso la dirección pública se encuentra detrás de un firewall y sólo se puede acceder a esa ella desde la propia red de la Universidad de Cantabria, por esta razón se asignará a la interfaz física en vez de a una virtual.

La configuración de la interfaz se puede realizar a través de la interfaz gráfica o del *Terminal*. Aquí se muestra el proceso a través de *CLI*.

Paso 21 Abrir una ventana de *Terminal* desde *Applications* > *Utilities*.

Tabla 14 – Instrucciones para configurar y habilitar una interfaz de red en CentOS 7.

```
[admin@syriusb ~]$ sudo -s
[root@syriusb admin]# vi /etc/sysconfig/network-scripts/ifcfg-enp2s0f0
```

Establecer la siguiente configuración en el fichero:

```
TYPE=Ethernet
BOOTPROTO=yes
DEFROUTE=no
DEVICE=enp2s0f0
ONBOOT=yes
IPADDR=193.144.186.46
PREFIX=24
GATEWAY=193.144.186.1
DNS1=193.144.193.11
DNS2=193.144.193.22
```

Guardar el fichero pulsando las teclas *:wq* e Intro y habilitar la interfaz con la instrucción:

```
[root@syriusb admin]# ifup enp2s0f0
```

Una de las opciones de instalación de CentOS 7 fue el *Virtualization Client* y como resultado se instaló un software denominado Virtual Machine Monitor. Este software es muy similar a XenCenter ya que permite la conexión con las máquinas virtuales así como cambiar su estado de energía. Se puede accederé a él a través de *Applications* > *System Tools*.

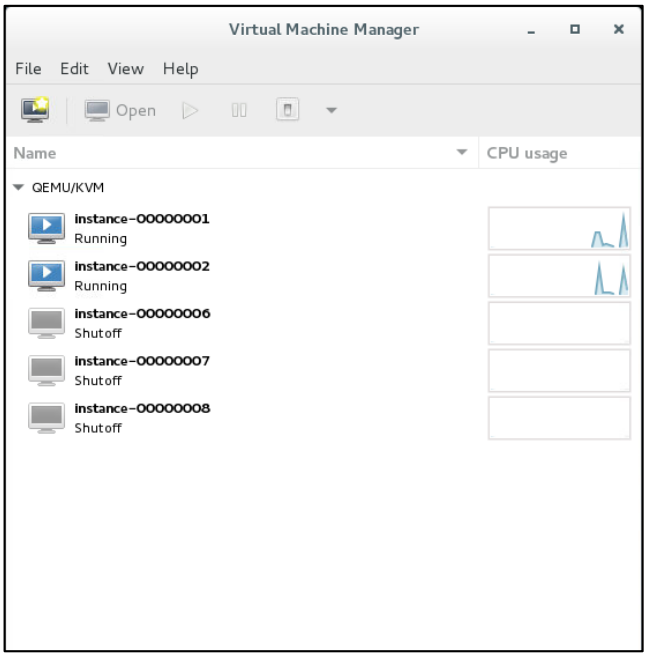


Figura 61 – Ventana del Virtual Machine Manager de CentOS 7

6.2. Instalación de PackStack

RDO PackStack es una utilidad de línea de comandos que utiliza los módulos Puppet [37] para soportar una rápida implementación de OpenStack a través de una conexión SSH con el servidor. PackStack se compone de un conjunto de scripts que sirven tanto para desplegar OpenStack en un solo nodo como para realizar instalaciones más complejas de múltiples nodos. [38]

El proceso de instalación de PackStack es sencillo y muy rápido comparado con un despliegue de OpenStack de forma manual.

A continuación se muestran los requisitos previos a la instalación [39]. Desde una terminal de CentOS e identificado como un usuario que tenga permisos de administrador, ejecutar las instrucciones de la Tabla 15.

Tabla 15 – Requisitos previos para la instalación y configuración de PackStack.

Se deshabilita el servicio de firewall, el gestor de red avanzado de CentOS y se vuelven a activar los servicios de red.

```
[admin@syriusb ~]$ sudo -s
[root@syriusb ~]# systemctl disable firewalld
[root@syriusb ~]# systemctl stop firewalld
[root@syriusb ~]# systemctl disable NetworkManager
[root@syriusb ~]# systemctl stop NetworkManager
[root@syriusb ~]# systemctl enable network
[root@syriusb ~]# systemctl start network
```

Se instalan los paquetes de OpenStack Ocata para Centos y los paquetes de PackStack más actualizados.

```
[root@syriusb ~]# yum update -y
[root@syriusb ~]# yum install -y centos-release-openstack-ocata
[root@syriusb ~]# yum install -y openstack-packstack
```

Una vez instalados los paquetes necesarios, se configura el despliegue de OpenStack con PackStack (véase Tabla 16)

La opción *allinone* establece que los nodos auxiliares (Compute, Controller, Storage, etc.) se encuentran todos en el mismo equipo físico [40].

La opción *provision-demo=n,* deshabilita la creación de las redes por defecto en OpenStack. Éstas se crearán posteriormente de forma manual.

Las opciones de *Neutron* se corresponden con configuración de red necesaria. Se crea una interfaz *bridge* para la red externa que esté puenteada con la interfaz física *enp2s0f1* (FortiGate).

Tabla 16 – Instrucción de instalación y configuración de PackStack

```
[root@syriusb ~]# packstack --allinone --provision-demo=n
      --os-neutron-ovs-bridge-mappings=external:br-ex
      --os-neutron-ovs-bridge-interfaces=br-ex:enp2s0f1
      --os-neutron-ml2-type-drivers=vxlan,flat
```

El instalador pide que se introduzca la contraseña de *root* para cada nodo de red que se esté instalando. Al ejecutar PackStack, se crea en el directorio `/root` un fichero con el formato de nombre `packstack-answers-YYYYMMDD-HHMMSS.txt`. Este fichero permite configurar PackStack con mayor detalle realizando un nuevo despliegue con la instrucción `packstack --answer-file`. También crea en el mismo directorio un fichero llamada `keystonerc_admin` que posee las credenciales necesarias para gestionar el entorno OpenStack ya desplegado.

El siguiente paso es configurar la red pública (FortiGate) y privada (máquinas virtuales) para este entorno OpenStack.

Tabla 17 – Instrucciones para crear las redes externa e interna en OpenStack

Se cargan en memoria las credenciales de OpenStack

```
source /root/keystonerc_admin
```

Se crea la red *external_network* (FortiGate) que es de tipo *flat* (No VLAN)

```
neutron net-create external_network --provider:network_type flat
        --provider:physical_network external --router:external
```

Se define el conjunto de direcciones IP que puede tomar, la puerta de enlace y la máscara de subred

```
neutron subnet-create --name public_subnet --enable_dhcp=True
        --allocation-pool=start=192.168.10.110,end=192.168.10.254
        --gateway=192.168.10.1 external_network 192.168.10.0/24
```

Se crea la red interna de OpenStack, la de las máquinas virtuales y se define su rango.

```
neutron net-create private_network
```

```
neutron subnet-create --name private_subnet private_network 10.0.0.0/24
```

Se crea un router virtual que conecte ambas redes, cuya puerta de enlace será la de la red externa

```
neutron router-create router1
```

```
neutron router-gateway-set router1 external_network
```

```
neutron router-interface-add router1 private_subnet
```

Para probar su funcionamiento, se descarga la imagen de un sistema operativo ligero como es CirrOS y se sube a OpenStack (véase Tabla 18) para crear posteriormente una máquina virtual.

Tabla 18 – Instrucciones para descargar una imagen de CirrOS y añadirla al servicio de imágenes

```
curl http://download.cirros-cloud.net/0.3.4/cirros-0.3.4-x86_64-disk.img
     | glance image-create --name='cirros image' --visibility=public --
     container-format=bare --disk-format=qcow2 --progress
```

Una vez concluido el proceso de despliegue de PackStack, el panel de control web de OpenStack, Horizon, es accesible a través de la dirección http://192.168.10.101. Se desea que dicho panel de control sea accesible a través de la IP pública del equipo, la Tabla 19 muestra cómo realizar este cambio.

Tabla 19 – Instrucciones para añadir un alias a Horizon

Editar con permisos de administrador el fichero de configuración de Horizon

```
nano /etc./httpd/conf.d/15-horizon_vhost.conf
```

Añadir la línea en la sección *Server Aliases*

```
ServerAlias 193.144.186.46
```

Guardar los cambios en el fichero

Tras realizar los cambios, Horizon ya es accesible a través de la IP pública del equipo. El nombre de usuario es `admin` y la contraseña se encuentra en el fichero `keystonerc_admin` en la carpeta `/root`

Una vez identificado correctamente en el panel web, es posible cambiar esta contraseña creada aleatoriamente. Para ello seguir las instrucciones de la Figura 62.

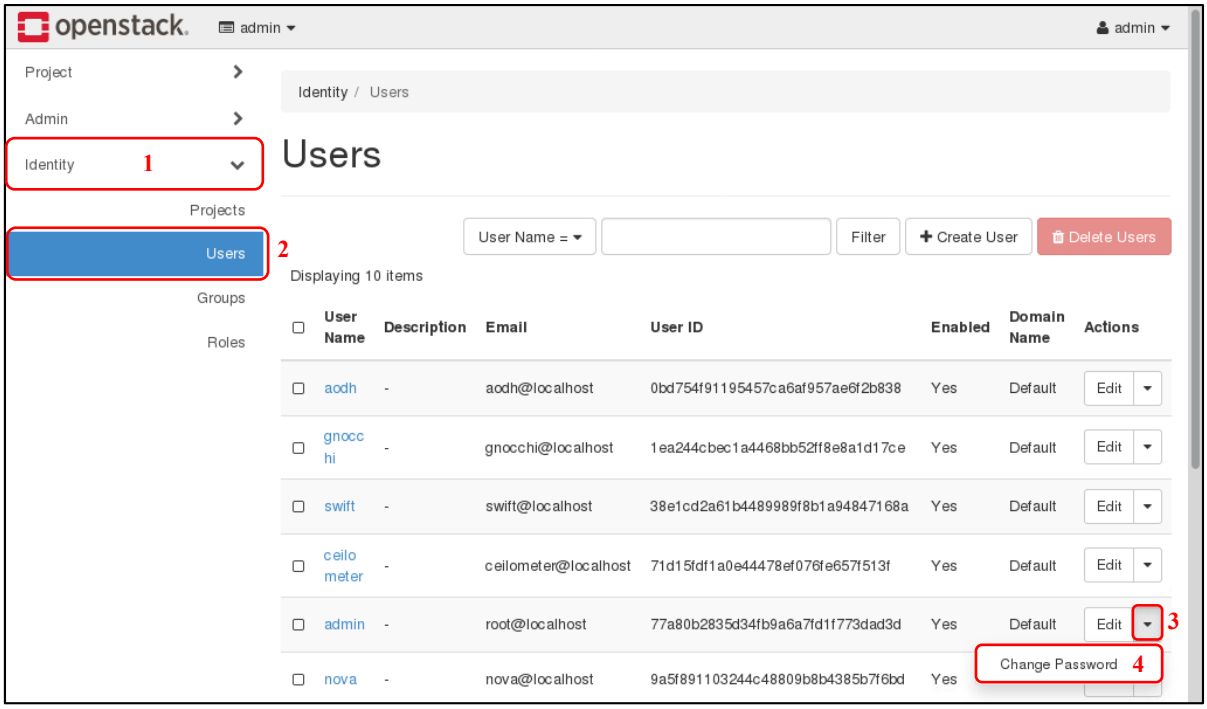


Figura 62 – Cambio de contraseña del usuario admin en OpenStack

Ahora se permite el acceso desde el exterior a las direcciones públicas que obtengan las máquinas virtuales. Por defecto si una máquina virtual adquiere una IP pública (FortiGate) no será accesible desde otras direcciones públicas del mismo rango. Para ello se debe permitir el acceso explícitamente para la red de los equipos origen hasta los servicios deseados de las máquinas virtuales.

En el menú lateral de navegación de Horizon dirigirse a *Project* > *Network Security Groups* y pulsar en el botón *Manage* del perfil de seguridad por defecto, *default*. En la nueva ventana pinchar en *Add Rule* y configurar las opciones como muestra la Figura 63 para permitir el acceso del protocolo ICMP desde cualquier equipo.

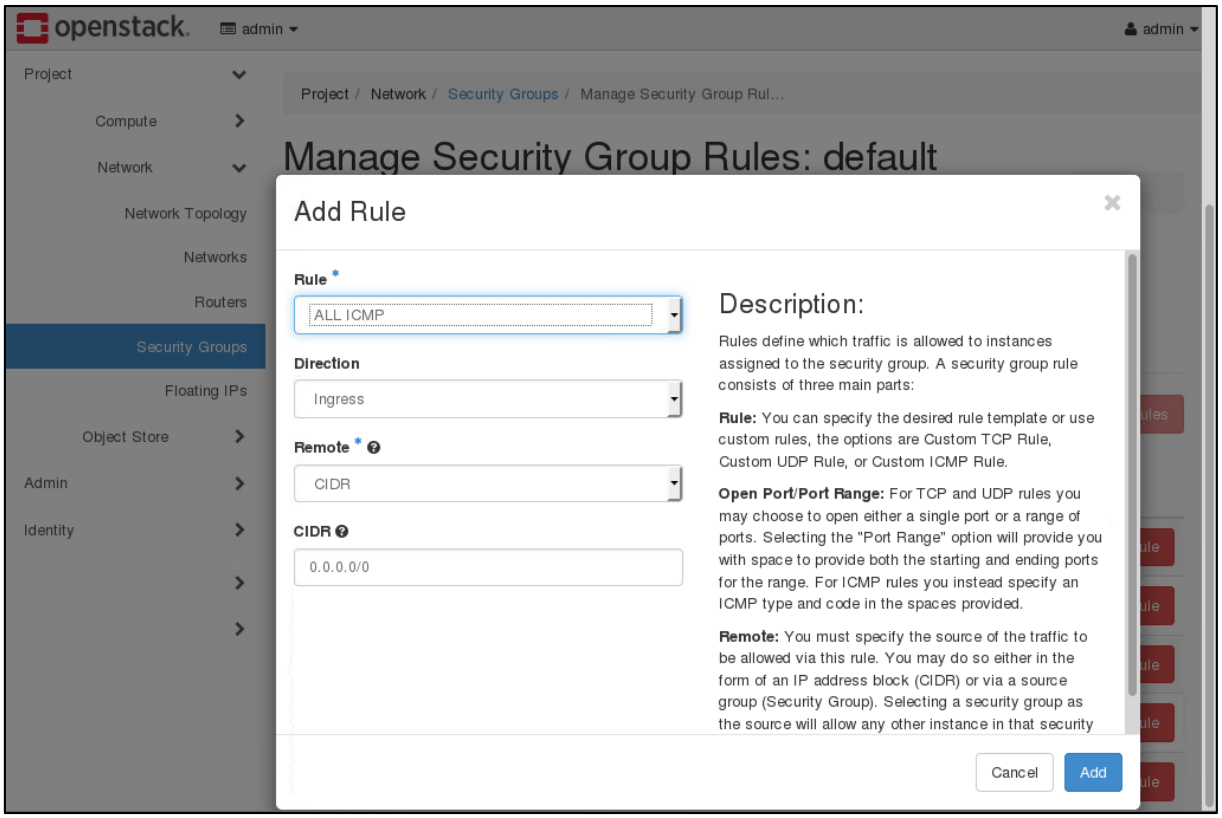


Figura 63 – Permitir mensajes ICMP desde cualquier origen a las máquinas virtuales

El siguiente paso es crear una máquina virtual de CirrOS para comprobar que todo funciona correctamente.

Desde la sección *Project* > *Network* > *Network Topology*, se puede visualizar la estructura lógica de las redes existentes, así como las máquinas virtuales conectadas a ellas. Para crear una nueva máquina virtual pulsar el botón *Launch Instance*.

El proceso de creación de una instancia comienza introduciendo su nombre identificativo. Seguidamente elegir el origen de arranque, en este caso *Image* y después seleccionar *cirros image*. En la sección *Flavors* seleccionar la opción con menores requisitos, *m1.tiny*. En la pestaña *Networks* se elige las redes a las que estará conectada la máquina, elegir ambas redes *private_network* y *external_network*

La nueva máquina virtual conectada a ambas redes y accesible desde el exterior se muestra en la Figura 64. Otra forma de conseguir el acceso desde el exterior a los servicios de una máquina es utilizando direcciones IP flotantes (*Floating IP*) que son asignadas de forma virtual por OpenStack.

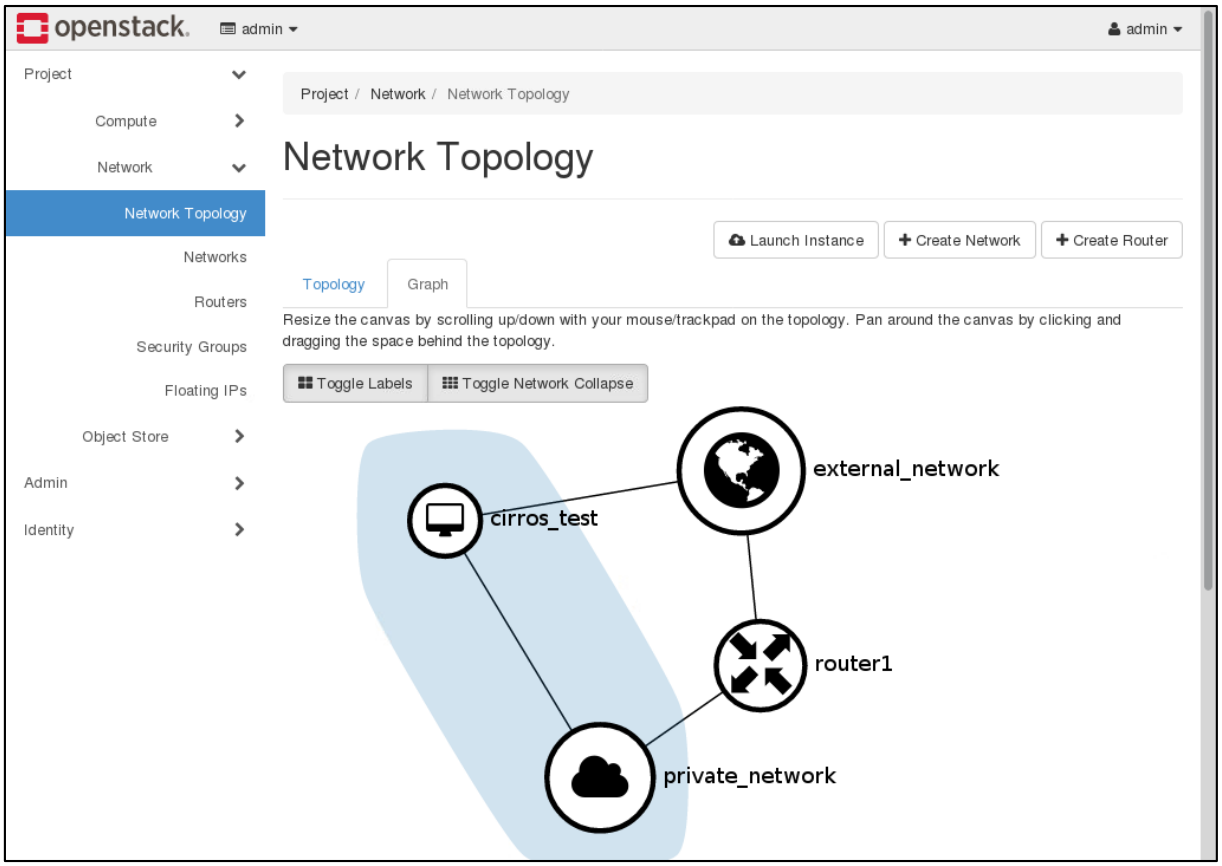


Figura 64 – Topología de red de OpenStack con una máquina conectada a las redes pública y privada

6.3. Conclusiones de la Fase III

De los procedimientos realizados en la Fase III, se puede concluir diciendo que:

- La instalación de CentOS en un proceso muy sencillo y guiado que permite una configuración a medida de manera muy cómoda.
- Con todo el software instalado, la instalación de PackStack es inmediata. Con muy pocas instrucciones se puede realizar el despliegue de OpenStack como la literatura promete, rápido, funcional y actualizado a la última versión ya que se instala desde los repositorios oficiales de OpenStack. Además, existe compatibilidad entre todas las características disponibles y no se limitan como en Mirantis.
- El proceso de configuración de OpenStack de forma manual es un proceso complejo y que requiere una gran cantidad de tiempo, pero esos problemas se solucionan con PackStack, con una simple instrucción se obtiene un Cloud completamente operativo.
- Una de las características más interesantes que añadieron desde RDO, es la creación de un fichero llamado *answer file* tras el primer despliegue del entorno. En él aparece la configuración y las opciones que se habilitaron en OpenStack, pero lo más relevante es que permite personalizarlo habilitando o deshabilitando cualquiera de la infinidad de características y paquetes de OpenStack y utilizar dicho fichero para modificar el entorno ya desplegado o para realizar un nuevo despliegue utilizando, de nuevo, una sola instrucción, `packstack --answer-file`.

7. CONCLUSIONES FINALES Y LÍNEAS FUTURAS

En este trabajo fin de Máster se han comparado métodos de implementación de una infraestructura Cloud virtualizada e integrada en el Laboratorio docente de Aplicaciones Telemáticas de la Escuela de Ingenieros Industriales y de Telecomunicación de la Universidad de Cantabria.

De acuerdo con las necesidades surgidas durante el desarrollo de esta implementación, los trabajos han ido encaminados a solucionar diferentes problemáticas sobre las que no se tenía constancia, por lo que la primera conclusión es que el desarrollo de implementaciones específicas mediante documentación genérica no puede considerarse nunca como un trámite.

Como trabajo previo se analizó el concepto de virtualización, una constante que se repite en todos los despliegues de grandes infraestructuras de los principales proveedores de servicios como Amazon, Google o Microsoft, y cómo ésta proporciona abundantes beneficios en cuanto a gestión y recursos se refiere. De esta manera, se han analizado las características de las soluciones de virtualización más populares tanto en las Nubes Públicas como Privadas utilizadas actualmente en entornos profesionales, del mismo modo que se estudió el funcionamiento de la infraestructura como servicio de software libre y código abierto denominada OpenStack.

Una vez seleccionada la solución Cloud a implementar, se procedió a la instalación de la misma en el entorno de red del Laboratorio de Aplicaciones Telemáticas. Para ello fue necesario completar la configuración de los servidores de virtualización, para lo cual se comenzó con el sistema Citrix XenServer 7.0. La principal conclusión obtenida durante este proceso fue la incompatibilidad de XenServer versión 7.0 con los servidores Huawei, ni siquiera tras actualizar dicho hardware con las últimas actualizaciones de la BIOS o del software de gestión proporcionadas por el fabricante.

Tras dar el paso atrás hacía la versión previa de XenServer (v. 6.5), y comprobar su funcionamiento a nivel de sistema operativo, se procedió a realizar unas primeras pruebas con el sistema DevStack (versión ligera de OpenStack), la cual cumplía su cometido utilizando un equipo más modesto, se intentó migrar la máquina virtual e incluso instalarlo desde cero en XenServer 6.5. Tras varios intentos se concluyó afirmando que DevStack no es compatible con el Sistema Operativo XenServer.

La alternativa para mantener XenServer pasa por utilizar una solución diseñada para tal sistema, denominada Mirantis OpenStack. Esta solución necesita una arquitectura de red específica que permite aprovisionar los nodos auxiliares que deben incluirse en XenServer para que el despliegue del entorno Cloud se realice correctamente. Tras completar el despliegue con Mirantis, se observó que algunas funcionalidades básicas no están disponibles, a pesar de que la herramienta de verificación del estado del entorno mostrase que todo funcionaba correctamente. Además, este entorno no resulta gestionable, al menos de forma sencilla y su lentitud al realizar cualquier operación no ofrece la comodidad que se esperaba.

Como resultado, fue necesario buscar otra solución que no presentase todos estos problemas, por lo que se ha recurrido a las opciones de software libre de código abierto utilizando CentOS y RDO PackStack.

La instalación del Sistema Operativo CentOS (v. 7.0) es un proceso muy sencillo y guiado que permite una configuración a medida de manera muy cómoda. Al combinarlo con PackStack, se soluciona la complejidad que conlleva el despliegue de OpenStack de manera manual, ya que permite su despliegue ad-hoc, añadiendo nuevas características con solo modificar un fichero de texto en el que se encuentran todas las opciones de configuración que OpenStack soporta. El tiempo de respuesta es rápido y todas las opciones básicas y avanzadas están operativas.

Con todo lo expuesto se puede concluir diciendo que la elección de la solución de virtualización es una decisión importante y que debe adecuarse y probarse previamente a su implementación en entornos de producción. Utilizando soluciones gratuitas se ha obtenido un resultado mejor que el obtenido con el software de Citrix, aunque si hubiese existido compatibilidad de hardware con las versiones más recientes de XenServer, esta infraestructura de Cloud que utiliza el hipervisor Xen, podría haber sido una solución satisfactoria.

A partir de los resultados obtenidos, queda patente todo el trabajo que queda por hacer, y que aquí se avanza en forma de **líneas futuras,** las cuales pasan por adoptar las últimas tecnologías en el despliegue de OpenStack, como es su integración con Docker para la gestión de contenedores que utilizan virtualización ligera a nivel de sistema operativo y el despliegue de clústeres para procesamiento de Big Data utilizando las tecnologías de Apache Hadoop. [41]

Además, una vez solucionados los problemas del entorno Cloud desplegado, el principal trabajo a realizar es la implementación de soluciones virtualizadas para el desarrollo de la docencia en el ámbito de los servicios y aplicaciones telemáticas, como primera aproximación, y su extensión al resto de temáticas relacionadas con la titulación de Grado y Master de Ingeniería de Telecomunicación.

Por último, al ser un tema de actualidad que parece estar contrapuesto con todo lo que se ha tratado hasta ahora, la adopción de arquitecturas *serverless* se está imponiendo, aunque actualmente se conozca más como el modelo *as a service*. Este modelo se basa en que los servidores físicos se vuelven invisibles para el desarrollador de aplicaciones y sin que tengan que preocuparse de la gestión de recursos. Los servicios serverless están diseñados para ejecutar fragmentos de código que llevan a cabo una única tarea de poco tiempo activadas mediante eventos. Según [42] "*Esta forma de computación resultará particularmente útil cuando se ejecuten aplicaciones sobre dispositivos conectados a Internet, ya que requerirán cantidades masivas de solicitudes de corta duración. Lo mismo sucederá para la próxima generación de servicios basados en inteligencia artificial y machine learning*.". El uso del entorno implementado puede hacerse extensivo hacia otro tipo de aplicaciones, como es el caso de las redes de sensores o el IoT (Internet of Things).

BIBLIOGRAFÍA

Durante desarrollo de este trabajo se ha utilizado la siguiente documentación:

[1] G. Longoria, «3 Reasons Why An OpenStack Private Cloud May Cost You Less Than Amazon Web Services (AWS),» 24 10 2016. [En línea]. Available: https://www.forbes.com/sites/moorinsights/2016/10/24/3-reasons-why-an-openstack-private-cloud-may-cost-you-less-than-amazon-web-services-aws/.

[2] IDC, «Worldwide Cloud IT Infrastructure Market Forecast,» 11 04 2011. [En línea]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS42454117.

[3] J. F. Gantz y P. Miller, «The Salesforce Economy: Enabling 1.9 Million New Jobs and $389 Billion in New Revenue Over the Next Five Years,» 09 2016. [En línea]. Available: http://www.salesforce.com/assets/pdf/misc/IDC-salesforce-economy-study-2016.pdf.

[4] G. Blokdijk y I. Menken, Virtualization - The Complete Cornerstone Guide to Virtualization Best Practices, 1 ed., The Art of Service, 2008.

[5] D. Marshall, W. A. Reynolds y D. McCrory, Advanced Server Virtualization, Auerbach Publications, 2006.

[6] CDW, «Server Virtualization: Decrease IT Cost and Data Center Space,» [En línea]. Available: https://biztechmagazine.com/sites/default/files/2_12_10%20Server%20Virt.pdf.

[7] K. Hess y A. Newman, Practical Virtualization Solutions, Crawfordsville, Indiana: Prentice Hall, 2009.

[8] J. M. Rodriguez, «Virtualizados - 10 Desventajas de la virtualización,» 04 01 2008. [En línea]. Available: http://www.jmarior.net/virtualizados/10-desventajas-de-la-virtualizacion/.

[9] datakeeper, «¿Qué son los Hipervisores?,» 23 12 2011. [En línea]. Available: http://www.datakeeper.es/?p=716.

[10] A. Maislos, «CloudTech,» 7 10 2016. [En línea]. Available: https://www.cloudcomputing-news.net/news/2016/oct/07/hypervisors-cloud-computing-what-out-there-you/.

[11] Linux Foundation Collaborative Projects, «XenProject,» [En línea]. Available: https://xenproject.org/developers/teams/xapi.html.

[12] T. Mackey y J. Benedict, XenServer Aministration Handbook, O'Reilly, 2016.

[13] A. Warfield, S. Hand, K. Fraser y T. Deegan, «Facilitating the Development of Soft Devices,» USENIX, 2005. [En línea]. Available: https://www.usenix.org/legacy/publications/library/proceedings/usenix05/tech/general/full_papers/short_papers/warfield/warfield_html/index.html.

[14] QEMU, «QEMU Wiki,» 31 03 2017. [En línea]. Available: http://wiki.qemu.org.

[15] XenServer, «XenServer Download,» 2017. [En línea]. Available: https://xenserver.org/open-source-virtualization-download.html.

[16] D. Bhatia y D. G. Bhattal, «A comparative study of Various Hypervisors Performance,» *International Journal of Scientific & Engineering Research,* vol. 7, nº 12, p. 65, 12 2016.

[17] National Institute of Standards and Technology, «The NIST Definition of Cloud Computing,» 09 2011. [En línea]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[18] L. Sánchez, «Apuntes de la asignatura Protocolos y Servicios para Redes de Nueva Generación del 2º Curso del Máster en Ingeniería de Telecomunicación 2016/2017. Tema 2 - Cloud Computing,» 09 12 2016. [En línea]. Available: https://www.tlmat.unican.es/index.php?l=es&p=teaching&s=postgraduate&ss=m_psrng&.

[19] K. Pepple, «Arquitectura de OpenStack,» 14 12 2012. [En línea]. Available: http://26a0ff8ca8ba32139f7d-db711c577a50b6bdc946ea71aaca027d.r97.cf1.rackcdn.com/openstack-conceptual-arch-folsom.jpg.

[20] Huawei, «RH1288 V3 Server V100R003 User Guide 16,» 22 05 2017. [En línea]. Available: http://support.huawei.com/enterprise/en/doc/DOC1000056730.

[21] FortiNet, «FortiGate/FortiWifi 30E Data Sheet,» 02 2017. [En línea]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_30E.pdf.

[22] Huawei, «HUAWEI Server Grantley Platform BIOS Parameter Reference 10,» 23 05 2017. [En línea]. Available: http://support.huawei.com/enterprise/en/doc/DOC1000053904.

[23] Citrix, «XenServer Hardware Compatibility List,» 2017. [En línea]. Available: http://hcl.xenserver.org/.

[24] Huawei , «Server Compatibility Checker,» 2016. [En línea]. Available: http://support.huawei.com/onlinetoolsweb/ftca/indexEn?serise=2.

[25] Huawei, «RH1288 V3 Server RH1288 V3-BIOS-V363.zip Download- Huawei,» 26 05 2017. [En línea]. Available: http://support.huawei.com/enterprise/en/software/22458206-SW1000239553.

[26] Huawei, «RH1288 V3 Server RH1288 V3-iBMC-V242.zip Download- Huawei,» 26 05 2017. [En línea]. Available: http://support.huawei.com/enterprise/en/software/22458206-SW1000239574.

[27] Citrix, «Xenserver 6.5 ISO Download,» [En línea]. Available: http://downloadns.citrix.com.edgesuite.net/10175/XenServer-6.5.0-xenserver.org-install-cd.iso.

[28] Citrix, «Container management supplemental pack Download,» [En línea]. Available: http://downloadns.citrix.com.edgesuite.net/10343/XenServer-6.5.0-SP1-xscontainer.iso.

[29] Citrix, «Docker,» [En línea]. Available: https://xenserver.org/partners/docker.html.

[30] OpenStack, «Introduction to Fuel,» 03 02 2017. [En línea]. Available: https://docs.openstack.org/developer/fuel-docs/userdocs/fuel-install-guide/intro/intro_fuel_intro.html.

[31] Citrix OpenStack Blogs, «XenServer and Neutron in MOS,» 31 08 2016. [En línea]. Available: http://citrix-openstack.siteleaf.net/posts/xenserver-and-neutron-in-mos/.

[32] Mirantis, «Mirantis OpenStack Download,» [En línea]. Available: https://www.mirantis.com/software/openstack/download/.

[33] H. Xie, «Deprecate XenServer 6.5 on MOS10,» 21 04 2017. [En línea]. Available: https://review.openstack.org/#/c/455562/.

[34] jianghuaw, «GitHub - citrix-openstack/xencenter-himn-plugin,» 20 12 2016. [En línea]. Available: https://github.com/citrix-openstack/xencenter-himn-plugin.

[35] GNU, «¿Qué es el copyleft? - Proyecto GNU - Free Software Foundation,» 17 04 2017. [En línea]. Available: https://www.gnu.org/licenses/copyleft.es.html.

[36] CentOS, «CentOS-7-x86_64-Everything-1611.iso Download,» 2017. [En línea]. Available: http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Everything-1611.iso.

[37] Puppet, «Puppet FAQ,» 2017. [En línea]. Available: https://puppet.com.

[38] Red Hat, «Part III. Deploying OpenStack using PackStack,» [En línea]. Available: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux_OpenStack_Platform/2/html/Getting_Started_Guide/part-Deploying_OS_using_PackStack.html.

[39] RDO, «Packstack: Create a proof of concept cloud,» [En línea]. Available: https://www.rdoproject.org/install/packstack/.

[40] RDO, «Neutron with existing external network,» [En línea]. Available: https://www.rdoproject.org/networking/neutron-with-existing-external-network/.

[41] OpenStack, «Docker - OpenStack,» [En línea]. Available: https://wiki.openstack.org/wiki/Docker.

[42] A. Piedrabuena, «Serverless, la computación sin servidores: la nueva tendencia cloud,» 16 12 2016. [En línea]. Available: http://aunclicdelastic.blogthinkbig.com/serverless-la-computacion-sin-servidores-la-nueva-tendencia-cloud/.