

***CAPÍTULO 2:***  
***Virtualización de Servidores***



**CAPÍTULO 2: VIRTUALIZACIÓN DE SERVIDORES (FIGURA 2.1)**

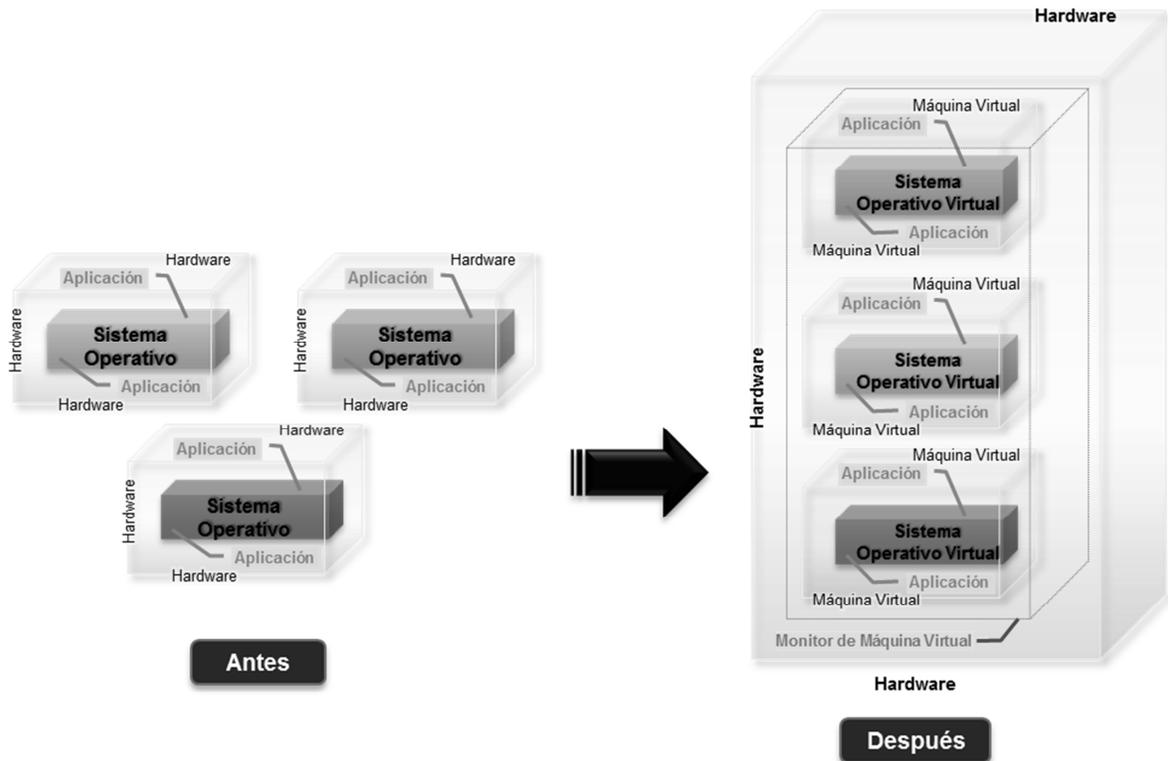


Figura 2.1 Representación visual de la virtualización de servidores

**2.1 HISTORIA DE LA VIRTUALIZACIÓN**

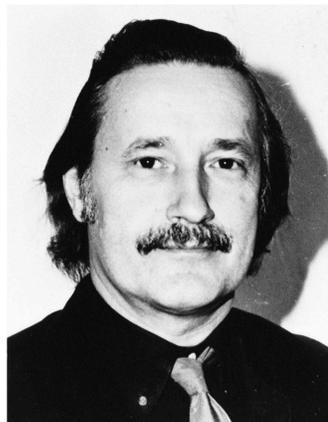


Figura 2.2 Christopher Strachey

El concepto de Virtualización no es nuevo en el mundo de la computación, de hecho es un término acuñado en la época de los grandes mainframes (años 60), cuando estas máquinas poderosas, principalmente fabricadas por IBM, eran muchas veces subutilizadas, por la restricción de operaciones de entrada y salida.

Christopher Strachey (Figura 2.2), primer profesor de computación en la Universidad de Oxford, publicó un trabajo de investigación llamado “*Time Sharing in Large Fast Computers*”<sup>7</sup> en el cual exponía la solución a la problemática de la espera de la liberación de un periférico cuando un programador estaba desarrollando un programa en su consola mientras otro programador depuraba su propio programa, tal solución fue llamada Multiprogramación (Multi-programming).

La técnica de Multiprogramación dio lugar a otras innovadoras ideas (los principios de la virtualización) que hicieron posible el desarrollo de la computadora Atlas y el proyecto M44/44X.

### 2.1.1 Computadora Atlas (Figura 2.3)

Fue la primera computadora que tomó ventaja de conceptos como tiempo compartido, multiprogramación y control compartido de periféricos. Este proyecto fue materializado en el Departamento de Ingeniería eléctrica de la Universidad de Manchester y financiado por Ferranti Limited una de las principales características de la computadora Atlas fue la rapidez de la misma – era la más rápida de la época- lograda por la separación de los procesos del sistema operativo (administrados por un componente llamado Supervisor) y los procesos ejecutados por el usuario.



Figura 2.3 Exhibición de la computadora Atlas en el Museo Nacional de Historia Americana<sup>8</sup>

<sup>7</sup> C. Strachey, "Time Sharing in Large Fast Computers", 1959.

<sup>8</sup> Imágenes históricas del Smithsonian, Computadora ATLAS en el Museo Nacional de Historia Americana, 1970s.

Este Supervisor otorgaba recursos clave del *hardware* a los programas de usuario; en esencia este fue el primer *Hypervisor* o Monitor de máquinas virtuales (*VMM*)<sup>9</sup>.

También la computadora Atlas incorporó el concepto de memoria compartida y técnicas de paginación de memoria que desembocaron en el desarrollo de la capa de abstracción de hardware que usan todas las tecnologías de virtualización actuales.

### 2.1.2 Proyecto M44/44X

A mitad de la década de 1960 el Centro de Investigación Thomas J. Watson de IBM puso en marcha el proyecto M44/44X<sup>10</sup> cuyo objetivo era evaluar los conceptos recién nacidos a partir de la técnica de tiempo compartido (*Time sharing*). La arquitectura del proyecto fue la primera en emplear el término máquina virtual; la computadora principal era una IBM 7044 (Figura 2.4) con varias máquinas virtuales 7044 (44X) simuladas mediante técnicas de memoria virtual y multiprogramación.

Una característica del proyecto M44/44X fue que no simulaba completamente la capa de hardware, lo cual dio lugar a una de las dos técnicas de virtualización bautizada más tarde como para-virtualización (*paravirtualization*).



Figura 2.4 IBM 7044<sup>11</sup>

<sup>9</sup> David Rule et al., *The Best Damn Server Virtualization Book Period*, Syngress. 2007, p. 3.

<sup>10</sup> *Ibid*

<sup>11</sup> IBM Corp., División de Procesamiento de Datos, IBM 7044, 1964.

### 2.1.2 El sistema operativo CP/CMS

Más tarde IBM completó el diseño de su modelo 7094 (Figura 2.5), el cual fue desarrollado por ingenieros de IBM e investigadores del MIT, esta computadora portaba un nuevo sistema operativo que integraba la tecnología CTSS (Sistema Compatible de Tiempo Compartido). El término compatible se refería a la compatibilidad con el sistema operativo por lotes de procesamiento usado en la computadora, conocido como FMS (Sistema Monitor Fortran).

El CTSS, no solo ejecutaba el FMS en la máquina 7094 como aplicación primaria para el flujo de lotes, sino que también ejecutaba una copia del FMS en cada máquina virtual como una aplicación en segundo plano. Las tareas en segundo plano tenían acceso a todos los periféricos, como impresoras, lectores de cintas y monitores, de la misma forma que una tarea del FMS en primer plano, siempre y cuando no interfiriera con los procesos – en primer plano– de tiempo compartido.



Figura 2.5 IBM 7094

Posteriormente el MIT desarrollo el proyecto MAC como un esfuerzo para la generación de nuevos avances en las tecnologías de tiempo compartido, presionando a los fabricantes de hardware a construir mejores plataformas en las cuales trabajar. La respuesta de IBM fue una nueva versión de su modelo System/360 que incluía la tecnología de tiempo compartido y memoria virtual. Esta propuesta de IBM fue rechazada por el MIT, haciendo áspera su relación, sin embargo, el CSC (Cambridge Scientific Center, enlace entre el MIT e IBM) liderado por Norm Rassmussen y Bob Creasey tomaron parte del proyecto MAC y para desarrollar CP/CMS<sup>12</sup> (uno de los productos más notables de IBM).

---

<sup>12</sup> David Rule et al., *The Best Damn Server Virtualization Book Period*, Syngress. 2007, p. 4.

En la década de los 60, el CSC concluyó con éxito el primer sistema operativo para una máquina virtual basado en hardware completamente virtualizado, conocido como CP-40. Más tarde el CP-67 fue liberado como una re implementación del CP-40 y después se convirtió en el S/370 (Figura 2.6). El éxito de esta plataforma recupero la credibilidad a IBM ante el MIT y mejoro su fuerza en el mercado. También dio paso a la evolución de las plataformas y sistemas operativos de máquinas virtuales siendo el más popular el sistema VM/370. El VM/370 fue capaz de correr varias máquinas virtuales con más memoria virtual de la que ofrecía el hardware, administrado por un componente llamado VMM (Monitor de Máquina Virtual) que se ejecutaba en el hardware real.

Cada máquina virtual era capaz de correr una única instalación del sistema operativo de IBM de forma estable y con gran rendimiento.

Sin embargo, no fue hasta la década de 1990 que las técnicas de virtualización se abrieron paso en el ambiente de centros de datos de mano de grandes compañías como Microsoft, Sun y VMware, en gran parte por los productos nivel empresarial que estos liberaron al mercado. Por parte de la comunidad se lanzaron otros proyectos como *Xen* y posteriormente KVM (Kernel-based Virtual Machine).

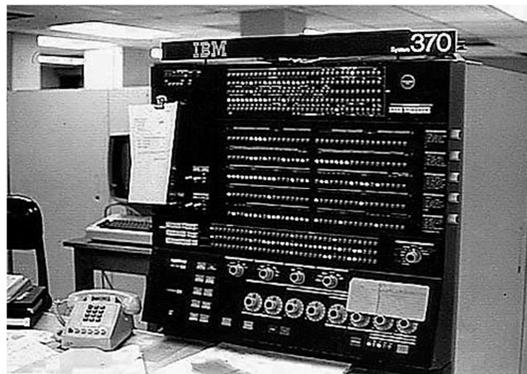


Figura 2.6 IBM S/370 [4]

La utilización de la virtualización para la consolidación de servidores no solo obedece al mejor aprovechamiento de los recursos de hardware sino que ha derivado también en las posibles soluciones a problemáticas actuales de seguridad de la información, acuerdos de nivel de servicio de los proveedores hacia sus clientes y motivaciones ambientalistas.

## 2.2 TECNOLOGÍAS DE VIRTUALIZACIÓN DE CÓDIGO ABIERTO

La presencia de proyectos de código abierto también se hizo evidente en las tecnologías de virtualización, el primero de ellos el proyecto Xen.

Xen es un VMM (Monitor de máquina virtual) o hypervisor de código abierto para arquitecturas de procesadores de 32 bits y 64 bits. Xen fue desarrollado como un proyecto de investigación por el grupo de sistemas del Laboratorio de computación de la Universidad de Cambridge. Este proyecto fue denominado Xenoserver<sup>13</sup> y fue patrocinado por el Consejo de Investigación de Ingeniería y Ciencias Físicas de Reino Unido.

El objetivo del proyecto es proporcionar una infraestructura pública accesible a todo el mundo para propósitos de cómputo distribuido, fue encabezado por Ian Pratt. Xen constituye el núcleo de cada nodo Xenoserver, administra los recursos, lleva a cabo tareas de auditoría.

Desde que Xen se liberó al público en 2003 ha crecido y madurado en variedad de implementaciones productivas. El desarrollo de Xen es gracias a la comunidad del código abierto y la organización XenSource. En Agosto de 2007 Citrix Systems compra a XenSource para darle un nuevo empuje a Xen, creando un producto para entornos empresariales llamado Xen Enterprise. En la actualidad Xen sigue como un proyecto de código abierto y Xen Enterprise como software comercial propiedad de Citrix Systems.

Un segundo icono de las tecnologías de virtualización de código abierto es el proyecto KVM, desarrollado inicialmente por Qumranet, una pequeña empresa israelita. Red Hat adquiere Qumranet en septiembre de 2008, Red Hat ve a KVM como la próxima generación de tecnología de virtualización. Hoy en día se utiliza como el VMM por defecto en Red Hat Enterprise Linux (RHEL) desde la versión 5.4 y en dos productos: Red Hat Enterprise Virtualization for Servers y Red Hat Enterprise Virtualization for Desktops.

---

<sup>13</sup> Citrix Systems Inc., Xen.org History, 2005.

Qumranet libero el código de KVM para la comunidad de código abierto. Hoy en día, empresas como IBM, Intel y AMD son parte de los colaboradores del proyecto. Desde la versión 2.6.20 KVM es parte del kernel de Linux y por lo tanto está disponible en todas las distribuciones de Linux con un kernel 2.6.20 o más reciente. KVM principalmente funciona en la arquitectura x86, pero el soporte para IA64 e IBM s390 ha sido añadido recientemente.

## 2.3 EL SISTEMA DE VIRTUALIZACIÓN

### 2.3.1 Definición

Desde de un enfoque simple, la virtualización es la tecnología que permite ejecutar varios sistemas operativos en una sola máquina física al mismo tiempo, siendo que cada sistema operativo se está ejecutando en una máquina virtual única.

Una definición formal sobre Virtualización se presenta a continuación:

Es la tecnología que combina y divide los recursos de hardware de una computadora para ejecutar uno o varios entornos de trabajo, mediante la aplicación de una o más tecnologías, como la partición de hardware y software, tiempo compartido, simulación parcial o completa de hardware, emulación, calidad del servicio y muchos otros<sup>14</sup>.

Esto significa, que la virtualización utiliza diversas tecnologías para abstraer el hardware real y proporciona ambientes aislados, llamados máquinas virtuales. Estos son capaces para ejecutar varias aplicaciones o incluso un sistema operativo completo. Uno de los objetivos es que el rendimiento de las máquinas virtuales debe ser cercano al nativo –el del hardware real–. Este es un punto muy importante, porque los usuarios siempre quieren sacar el máximo rendimiento del hardware.

---

<sup>14</sup> Susanta Nanda, et al., A Survey on Virtualization Technologies, Departamento de Ciencias de la Computación, Universidad Stony Brook, p. 2.

Dentro de un sistema de virtualización el servidor o la máquina física que contiene a las máquinas virtuales es denominado host (nodo de virtualización) y las máquinas virtuales comúnmente son llamadas guests (invitados)

### 2.3.2 Monitor de máquina virtual (Figura 2.7)

Un VMM (Monitor de máquina virtual) o Hypervisor, es una pieza de software o hardware que se ejecuta en el nodo de virtualización. Todas las máquinas virtuales son controladas y monitoreadas por el VMM, este proporciona herramientas al usuario para tales operaciones. Estas herramientas permiten realizar varias acciones como iniciar o apagar la máquina virtual, migrar máquinas virtuales entre nodos de virtualización. A la máquina virtual se le presentan elementos de hardware virtuales, por ejemplo un *CPU* virtual.

El VMM mapea el o los CPUs virtuales de las máquinas virtuales en ejecución hacia el o los CPUs físicos del nodo de virtualización o host. Por lo que, generalmente, entre mas CPUs físicos tenga el nodo de virtualización más máquinas virtuales podrá ejecutar. Esto se logra por algún tipo de mecanismo de *scheduling* (planificación) que asigna cierta parte de un CPU físico a cada CPU virtual.

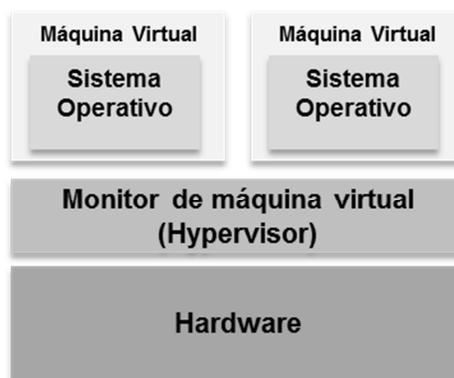


Figura 2.7 Arquitectura de un VMM

Un VMM también administra la memoria, es decir, mapea una cantidad de memoria física para el espacio de direcciones de las máquinas virtuales, otras funciones son el manejo de la fragmentación de la memoria y la técnica de *swapping* (intercambio de memoria). Generalmente las máquinas virtuales no tienen acceso directo al hardware físico,

al menos que así se desee, lo más común es que el VMM proporcione dispositivos de entrada y salida virtuales a las máquinas virtuales, ya sean tarjetas de red, discos duros o unidades ópticas; esto facilita la migración de máquinas virtuales a otros nodos de virtualización puesto que si se usa el mismo VMM se presentan los mismos dispositivos virtuales a las máquinas virtuales.

### 2.3.3 Criterio de Popek y Golberg

El criterio de Popek y Goldberg<sup>15</sup> define una serie de requerimientos que debe cumplir una computadora para poder soportar una tecnología de virtualización.

Las condiciones generales son:

- Equivalencia.- Un programa que se ejecuta bajo el VMM (en un ambiente virtual) debe tener un comportamiento predecible y además idéntico al que demostraría si se ejecutara directamente por el hardware. Este concepto también se conoce como Fidelidad (Fidelity).
- Control de recursos.- El VMM debe tener control total de los recursos de hardware virtuales que ocupan los sistemas operativos de las máquinas virtuales. También se conoce como seguridad (Safety).
- Eficiencia.- Un gran número de instrucciones de máquina se deben de ejecutar sin la intervención del VMM, es decir, directamente por el hardware físico. También se conoce como rendimiento (Performance).

Según Popek y Goldberg, el problema que los desarrolladores de monitores de máquinas virtuales deben enfrentar es la creación de un VMM que cumpla las condiciones anteriores cuando se opera con la *ISA* (arquitectura del conjunto de instrucciones) de un hardware específico.

Las instrucciones se puede clasificar en tres grupos: privilegiadas, de control sensible y de comportamiento.

---

<sup>15</sup> David Rule et al., *The Best Damn Server Virtualization Book Period*, Syngress. 2007, p. 19.

- Las instrucciones privilegiadas son las que se interceptan si el procesador está en modo de usuario y no se interceptan cuando está en Modo Supervisor.
- Las instrucciones de control sensible son aquellas que intentan cambiar la configuración de los recursos actuales de hardware.
- Las Instrucciones de comportamiento son aquellas cuyo comportamiento o resultado depende de la configuración de los recursos que el VMM debe operar en cada grupo de instrucciones mientras mantiene las condiciones de equivalencia, control de recursos y eficiencia.

Prácticamente cualquier VMM actual cumple los dos primeros requerimientos: el control de recursos y la equivalencia. Lo hacen mediante el manejo adecuado del sistema operativo de la máquina virtual y de la plataforma de hardware haciendo uso de técnicas de emulación, aislamiento, asignación y encapsulación, las cuales se describen a continuación (Tabla 2.1).

Tabla 2.1 Funciones de un VMM

Función	Descripción
Emulación	El VMM debe presentar un ambiente de hardware total (máquina virtual) para cada conjunto de software, ya sea una aplicación o un sistema operativo. Idealmente, el sistema operativo o la aplicación no deben tener conocimiento de estar compartiendo recursos de hardware con otros componentes de software. Esta técnica satisface la propiedad de equivalencia.
Aislamiento	El aislamiento aunque no es obligatorio es importante para mantener un ambiente seguro y confiable. A través de la abstracción del hardware, cada máquina virtual debe ser independiente y estar aislada de las operaciones y actividades de otra máquina virtual. Cualquier falla en una máquina virtual no debe afectar a otra, esto proporciona altos niveles de seguridad y disponibilidad.
Asignación	El VMM debe asignar los recursos de hardware a las máquinas virtuales que administra. Los recursos para procesamiento, memoria, dispositivos de red y almacenamiento deben estar balanceados para optimizar el rendimiento y alinear los niveles de servicio con los requerimientos del negocio. A través de la asignación el VMM satisface la propiedad de control de recursos en cierta medida también la propiedad de eficiencia.

Encapsulación	La técnica de encapsulación no es obligatoria según el criterio de Popek y Golderb, ésta permite que cada pila de software (sistema operativo y aplicaciones) sea altamente portátil y capaz de ser copiada o movida de un nodo de virtualización a otro. En algunos casos el nivel de portabilidad incluso permite que la migración de las máquinas virtuales sea <i>en vivo</i> (mientras la máquina virtual está encendida). La encapsulación debe incluir información del estado de cada máquina virtual transferida para mantener su integridad.
---------------	---

### 2.3.4 Asistencia del hardware

En la actualidad la arquitectura de CPU más usada es la x86, esta familia tiene dos principales métodos de direccionamiento de memoria: el modo real y el modo protegido. El modo real, el cual está limitado a solo un megabyte de memoria, rápidamente se volvió obsoleto. El modo protegido, permite nuevas características para proporcionar multitasking (técnicas multitarea); estas incluyen segmentación de procesos, por lo que ya no pueden escribir fuera de su espacio de direcciones, además del soporte de hardware para técnicas de memoria virtual y task switching (conmutación de tareas).

Para maximizar el rendimiento del hardware basado en la arquitectura x86 que está siendo usado como nodo de virtualización, se debe asegurar el uso de procesadores que soporten la tecnología hardware-assisted virtualization (virtualización asistida por hardware). Intel y AMD, dos de los grandes fabricantes de procesadores de la familia x86 ofrecen esta tecnología llamada Intel VT<sup>16</sup> y AMD-V<sup>17</sup>; tanto en sus servidores como en sus equipos de escritorio y portátiles. Los procesadores con esta tecnología le dan al sistema operativo de la máquina virtual la autoridad necesaria para tener acceso directo a los recursos de hardware sin compartir el control del mismo; anteriormente, el VMM tenía que emular el hardware virtual y presentarlo al sistema operativo virtual y a la vez mantener el control del hardware físico. Estos nuevos procesadores le dan la autoridad necesaria tanto al VMM como al sistema operativo virtual para poder ejecutarse sin emulación de hardware o modificación del sistema operativo; esto ayuda a los desarrolladores de monitores de máquinas virtuales a diseñar un VMM más simplificado.

---

<sup>16</sup> Se ofrece mayor información sobre esta tecnología en: <http://www.intel.com/technology/itj/2006/v10i3/1-hardware/6-vt-x-vt-i-solutions.htm>

<sup>17</sup> Se ofrece mayor información sobre esta tecnología en: <http://sites.amd.com/es/business/it-solutions/virtualization/Pages/amd-v.aspx>

Desde que se aplica esta tecnología el esfuerzo computacional que realiza el VMM se ha reducido. Además la información del estado del CPU y del sistema operativo virtual ahora reside en memoria protegida a la que solo tiene acceso el VMM. Finalmente los procesadores con la tecnología hardware-assisted virtualization que soporten procesamiento a 64 bits pueden proporcionar máquinas virtuales con mejor rendimiento.

Otras nuevas tecnologías en los procesadores han aumentado el rendimiento de las máquinas virtuales, tal es el caso de la tecnologías EPT (Extended Paging Tables) de Intel y NPT (Nested Paging Tables) de AMD<sup>18</sup>, éstas se usan para que el procesador realice la traducción entre la memoria virtual y la física, liberando al VMM de tales operaciones.

### 2.3.5 Niveles de privilegios

En la familia x86 el modo protegido usa cuatro niveles o anillos de privilegios (Figura 2.8), numerados del 0 al 3. El sistema de memoria se divide en segmentos, cada segmento es asignado a un anillo en particular<sup>19</sup>.

El procesador usa el nivel de privilegios para determinar que puede o no puede hacer con el código o los datos dentro de un segmento. El anillo 0 es considerado como el primer anillo (el interno) el cual tiene control total del procesador. El anillo 3 es el anillo externo solo se aprovisiona con acceso restringido.

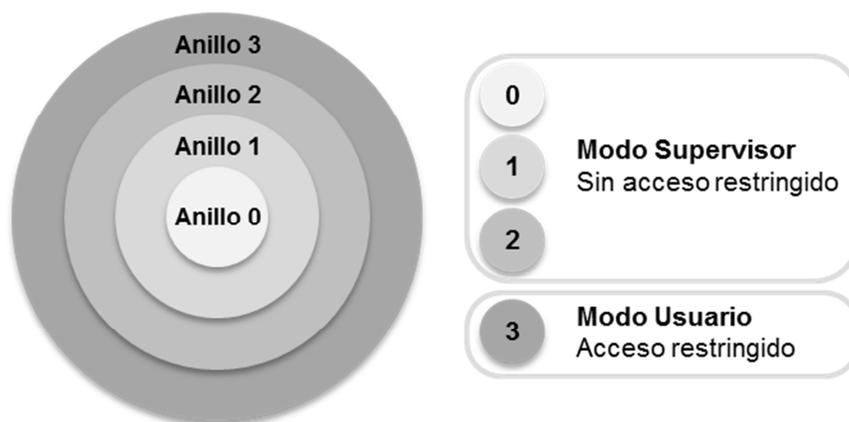


Figura 2.8 Anillos de privilegios de un procesador x86

<sup>18</sup> Se ofrece mayor información sobre las tecnologías Intel EPT y AMD NPT en: <http://www.anandtech.com/show/2480/10>

<sup>19</sup> El término “anillos” proviene del sistema usado por MULTICS, donde los niveles de privilegios se visualizan como un conjunto de anillos concéntricos.

El concepto de anillos de protección también existe en la arquitectura de los sistemas operativos actuales. Windows, Linux y la mayoría de las variantes de Unix usan anillos, con la diferencia que solo se ocupan dos anillos correspondientes a los niveles 0 y 3. El anillo 0 es comúnmente llamado Modo Supervisor, mientras que el anillo 3 es conocido como el Modo Usuario.

Los mecanismos de seguridad en el hardware restringen en el anillo 3 el acceso de código a los segmentos, páginas de memoria y de entrada y salida. Si un programa ejecutándose en modo usuario (anillo 3) intenta direccionar memoria fuera de su segmento, una interrupción de hardware detiene la ejecución del código. Algunas instrucciones de lenguaje ensamblador no están disponibles para su ejecución fuera del anillo 0, debido a su naturaleza –sensible– de bajo nivel.

### **2.3.6 Relación del VMM con los Niveles de privilegios**

El Modo Supervisor en un procesador de la familia x86 permite la ejecución de cualquier instrucción, incluyendo instrucciones privilegiadas como las operaciones de administración de memoria y entrada-salida. El sistema operativo normalmente se ejecuta en el Anillo 0 (Modo Supervisor). Si el Anillo 0 se compromete o es inestable impacta directamente al Anillo 3 (Modo Usuario).

El Anillo 0 de cada máquina virtual está aislado, de esta forma si hay alguna falla en el Anillo 0 de un *guest* no se afecta el de otro y en consecuencia tampoco su Anillo 3.

Estos Anillos 0 de los *guests* pueden residen en los Anillos 1, 2 o 3 del procesador x86. Entre más alejado este el Anillo 0 –de la máquina virtual– del Anillo 0 real, más tardarán las instrucciones en ser ejecutadas en el hardware, reduciendo el rendimiento de la máquina virtual.

El VMM se puede colocar en cualquiera de los anillos reales, existen dos tendencias en el software de virtualización; la primera coloca el VMM en el Anillo 0 real y la otra en el Anillo 3 real. En cualquiera de los casos el VMM representa el Anillo 0 para la máquina virtual siendo capaz de interactuar directamente con los dispositivos virtuales.

## 2.4 TÉCNICAS DE VIRTUALIZACIÓN

### 2.4.1 Para-virtualización

La Para-virtualización (Figura 2.9) le permite a cada máquina virtual ejecutar un sistema operativo completo, pero éstos no se ejecutan en el Anillo 0, dado que todas las instrucciones privilegiadas no pueden ser ejecutadas por una máquina virtual<sup>20</sup>. Por lo que se necesita modificar el sistema operativo virtual para implementar una interfaz. Entonces, el VMM toma el control y administra todas las instrucciones de la máquina virtual que son restringidas. La para-virtualización busca lograr un rendimiento nativo, pero no puede ser utilizada con sistemas operativos de código cerrado. El ejemplo más notable es con el sistema operativo Microsoft Windows, el cual no puede ser para-virtualizado.

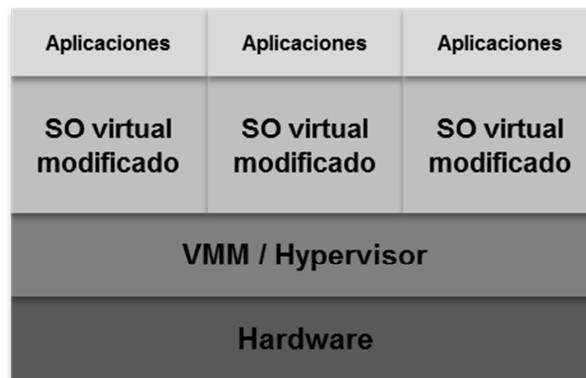


Figura 2.9 Ambiente de Para-virtualización(Para-virtualization)

#### Ventajas

- Es más sencillo de implementar que la virtualización total; dado que no requiere de tecnologías avanzadas de asistencia de hardware.
- Las máquinas virtuales para-virtualizadas ven mejorado su rendimiento, principalmente al procesar paquetes de red y operaciones de disco.

#### Desventajas

- Los sistemas operativos ejecutados en una máquina virtual para-virtualizada requieren de modificaciones.
- Las máquinas virtuales no se pueden exportar fácilmente y no hay una compatibilidad total entre versiones.

<sup>20</sup> Timo Hirt, KVM - The kernel-based virtual machine. Febrero 2010, p. 7.

### 2.4.2 Virtualización Total (Full-virtualization)

La técnica de Virtualización Total (Figura 2.10) permite operar varios sistemas operativos sobre un sistema anfitrión, cada uno ejecutándose en una máquina virtual aislada. El VMM se ayuda de las funcionalidades de asistencia del para operarlos, esto permite ejecutarlos sin que sea necesario modificarlos<sup>21</sup>. El VMM también proporciona dispositivos de entrada-salida para cada máquina virtual emulando hardware antiguo. Esto asegura que el sistema operativo virtual tiene suficientes controladores para dichos dispositivos. Esta técnica no es tan rápida como la para-virtualización, pero si se necesita virtualizar un sistema operativo de código cerrado es la una opción.

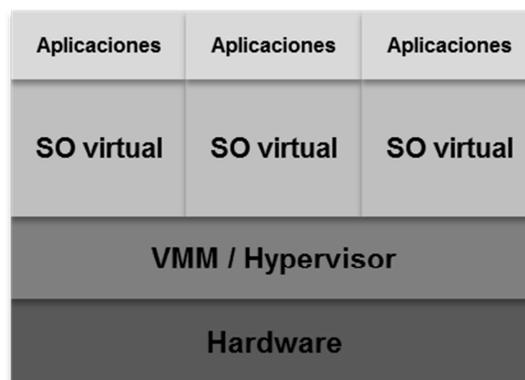


Figura 2.10 Ambiente de Virtualización Total (Full-virtualization)

#### Ventajas

- Proporciona un aislamiento total de las máquinas virtuales y el VMM.
- Ofrece un rendimiento de CPU y memoria casi nativo; usa sofisticadas técnicas para interceptar y emular las instrucciones en tiempo de ejecución.

#### Desventajas

- Requiere de una combinación adecuada de elementos de hardware y software, debido a que algunas instrucciones privilegiadas del procesador x86 no pueden ser emuladas.

<sup>21</sup> Timo Hirt, KVM - The kernel-based virtual machine. Febrero 2010, p. 7.

## 2.5 BENEFICIOS DE LA VIRTUALIZACIÓN

La virtualización no solo es una tecnología que permite la concentración de varios servidores independientes en una sola computadora física, sino que también involucra un nuevo paradigma en la administración de un centro de datos. Esta tecnología es la base de toda una plataforma de optimización, consolida la infraestructura de *TI* (tecnologías de la información), identificando y reduciendo el número de aplicaciones innecesarias y racionalizando los sistemas de información. La Figura 2.11 visualiza como la virtualización puede ayudar en la optimización de un centro de datos.

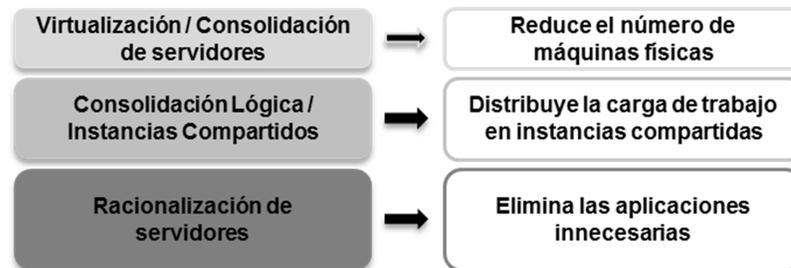


Figura 2.11 Beneficios de la virtualización<sup>22</sup>

En la Tabla 2.2 se enlistan y clasifican los principales beneficios logrados con la virtualización en un centro de datos, no obstante que cada organización tiene diferentes necesidades, estos puntos son lo suficientemente generales; pueden ayudar a elaborar una justificación completa en un proyecto de migración hacia un ambiente virtual.

Tabla 2.2 Beneficios de la virtualización

Clasificación	Beneficio
Consolidación	Incrementa el uso del servidor
	Facilita la migraciones desde <i>software legacy</i>
	Puede contener varios sistemas operativos
	Agiliza la creación de ambientes de desarrollo y de ambientes de pruebas
Confiabilidad	Aísla fallos de software
	Reasigna recursos existentes
Seguridad	Contiene ataques informáticos aislando los sistemas
	Aplica diferentes opciones de seguridad en cada partición

<sup>22</sup> David Rule et al., The Best Damn Server Virtualization Book Period, Syngress. 2007, p. 12.

### 2.5.1 Consolidación

El objetivo de la consolidación es el de combinar y unificar sistemas de información. En el caso de la virtualización, la carga de trabajo se combina en un menor número de máquinas físicas capaces cumplir con la demanda de recursos informáticos como CPU o memoria.

En los centros de datos modernos, las tareas realizadas muchas veces desperdician los recursos de hardware, a través de la consolidación, la virtualización permite combinar instancias de los sistemas operativos de una manera estratégica para colocarlos en un hardware compartido con capacidad suficiente para satisfacer la demanda de recursos. El resultado es una mayor utilización. Con el fin de maximizar la inversión, los servidores deben ocupar sus recursos lo más cerca posible de su límite, sin afectar a las tareas en ejecución o el rendimiento de los procesos de negocio.

Con una planeación adecuada y el conocimiento de las tareas a ejecutar, la virtualización ayudará a incrementar la utilización del servidor mientras que disminuye el número de máquinas físicas necesarias.

La virtualización ayuda a simplificar las migraciones de sistemas *legacy*, proporcionando una plataforma común y ampliamente compatible donde el sistema *legacy* se puede ejecutar. Esto aumenta las posibilidades de una migración de las aplicaciones sin mayor riesgo y con un impacto mínimo. Por último, la consolidación puede crear ambientes de desarrollo y pruebas. Teniendo en cuenta que las tareas de desarrollo y pruebas son menos demandantes que las tareas de producción, la consolidación de los entornos a través de la virtualización puede generar un ahorro mayor.

### 2.5.2 Confiabilidad

En la actualidad la confiabilidad se ha convertido una preocupación y una obligación para muchas organizaciones, ésta tiene una relación directa con la disponibilidad del sistema. Las empresas están dispuestas a hacer grandes inversiones en su infraestructura de servidores para asegurarse de que sus aplicaciones críticas permanecen en línea y sus

operaciones del negocio son ininterrumpidas. Al invertir en hardware y software adicionales ante el fallo de un sistema, se logra cierta preparación al ocurrir un incidente, sin embargo, esto es muy costoso. Las tecnologías de virtualización como solución a estos problemas, proporcionan un alto aislamiento entre máquinas virtuales.

Un error en el sistema operativo de la máquina virtual, no afectará a otras máquinas virtuales que se ejecutan en el mismo hardware. Este aislamiento lógico protege a las máquinas virtuales en el nivel más bajo; de hecho, las máquinas virtuales no saben que comparten los mismos recursos de hardware. Esta capa de abstracción, un componente clave en la virtualización, hace que cada máquina virtual se ejecute como si residiera en hardware dedicado. La flexibilidad de la virtualización permite a las organizaciones reasignar los recursos de hardware a diferentes máquinas virtuales según la carga de trabajo de éstas por un menor costo, manteniendo altos niveles de confiabilidad.

También se puede beneficiar del uso de la virtualización al crear ambientes en espera de algún fallo del sistema principal, como parte de un *BCP* (Plan de Continuidad del Negocio) o un *DRP* (Plan de Recuperación de Desastres).

### **2.5.3 Seguridad**

En caso de una máquina virtual sea comprometida, se encuentra aislada de las otras máquinas virtuales, impidiendo que se pueda extender la falla de seguridad. También gracias a la asignación y limitación de recursos de hardware a las máquinas virtuales, se puede asegurar la máquina física va a permanecer funcionando.

Estos incidentes de seguridad que comprometan un sistema pueden ser ataques cibernéticos, software malicioso o virus.

Como cualquier tecnología emergente, la virtualización también involucra algunas desventajas en su utilización, como: un decremento en el rendimiento, generado por la emulación de hardware que representa una capa adicional de software. Además de cierta incompatibilidad con dispositivos periféricos, al ser limitada la emulación de los puertos

serial, paralelo, *USB* y SCSI; esta limitación depende del software de virtualización usado<sup>23</sup>.

## 2.6 USOS COMUNES DE LA VIRTUALIZACIÓN

A continuación se enlistan algunos proyectos que se pueden llevar a cabo usando virtualización.

- Renovación tecnológica
- Continuidad del negocio y recuperación de desastres
- Pruebas de concepto
- Escritorios virtuales
- Laboratorio de pruebas

## 2.7 PLANEACIÓN DE UN PROYECTO DE VIRTUALIZACIÓN

Como cualquier proyecto en un área de tecnologías de la información, un proyecto de virtualización debe seguir ciertos procesos que eleven hasta que sea confiable, la probabilidad de éxito de ese proyecto.

Por otro lado, las tecnologías de virtualización para la plataforma x86 son relativamente recientes en el mundo de la computación, por lo que no existen estándares que indiquen como se debe desarrollar un proyecto de virtualización, además de que cada organización es única en cuanto a sistemas de información se refiere.

No obstante se pueden abstraer una serie de pasos para ajustar las necesidades del negocio a los requerimientos que debería de cubrir un proyecto de virtualización. A continuación se presentan algunos pasos clave (independientes de la tecnología a usar) para el desarrollo de un proyecto de virtualización.

---

<sup>23</sup> Alain Ribière, Using virtualization to improve durability and portability of industrial applications, 2008, p. 1546.

### 2.7.1 Descubrimiento

El primer paso dicta que se deben identificar los servidores candidatos a virtualizar, para lo cual es indispensable contar con un inventario del centro de datos, donde se indique con suficiente detalle las características de los equipos de cómputo y las aplicaciones que albergan, así como un informe histórico de demanda de recursos y rendimiento. Aunque esta tarea no sea tecnológicamente compleja a muchas veces elaborar o actualizar este tipo de documentos resulta tedioso y en muchas ocasiones una labor inconclusa. Aproximadamente solo el quince por ciento de los administradores de centros de cómputo tienen un inventario actualizado de la infraestructura de TI a la mano.

Generalmente, el mayor atractivo de los administradores de tecnologías de la información es la reducción de los centros de datos, es decir, menos servidores, menos utilización de fuentes de alimentación eléctrica, aparatos de aire acondicionado.

No obstante, la renovación tecnológica de un centro de datos puede ser muy costosa, por lo que surge la duda ante adoptar una tecnología nueva siendo que la infraestructura actual aún puede satisfacer las necesidades operativas; de ahí que los proyectos de virtualización o de consolidación de servidores deban ser justificados desde una perspectiva técnica y económica.

Existen herramientas que pueden elaborar inventarios de servidores por medio de escaneos en la red local y reportes que ayudan a identificar los servidores que se podrían virtualizar, de esta forma se hace más sencilla y dinámica la elaboración de estos documentos esenciales. Estas herramientas son: *MAP* (Microsoft Assessment and Planning, Figura 2.12), *VGC* (VMware Guided Consolidation), VMware Capacity Planner, CiRBA y PlateSpin Recon<sup>24</sup>. Para tener mayor fiabilidad de los datos se recomienda hacer el inventario de servidores y recursos de hardware utilizados de forma histórica para que la información recabada tome en cuenta la carga de trabajo máxima, mínima y promedio.

---

<sup>24</sup> Danielle Ruest, *Virtualization: A Beginner's Guide*. McGraw-Hill. 2009, p. 16.

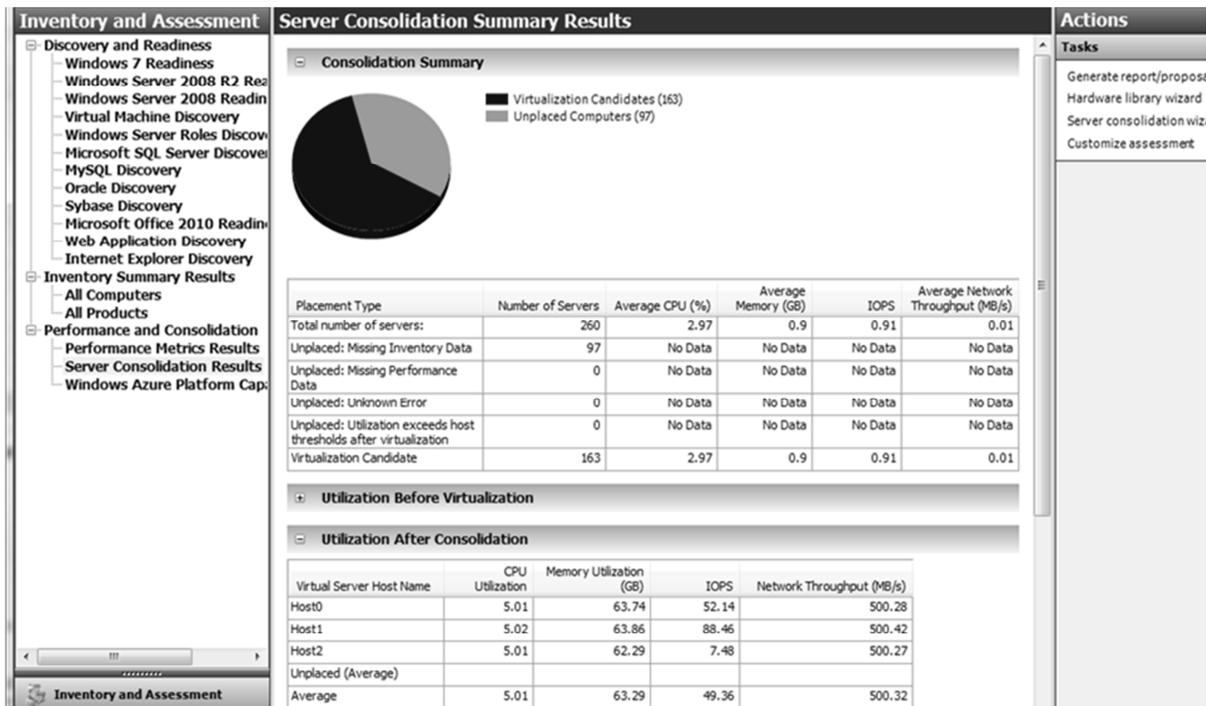


Figura 2.12 Resumen del análisis de consolidación de la herramienta MAP

En caso de que no se pueda contar con una herramienta como las mencionadas antes, se puede utilizar una herramienta de monitoreo que sea capaz de obtener datos de rendimiento, estas son más comunes en el mercado e incluso hay algunas que son software libre.

El inventario debe considerar los siguientes recursos de cómputo: CPU, memoria, almacenamiento, Consumo de energía eléctrica, Tráfico de entrada-salida, Tráfico de red y Carga de trabajo.

### 2.7.2 Análisis

En segundo lugar se debe analizar los servidores físicos de la infraestructura de TI para determinar si se requiere adquirir nuevo equipo de cómputo o mejorarse el actual antes de pasar a la virtualización.

Generalmente todos los servidores físicos más recientes incluyen los procesadores con capacidad de virtualización. En el caso de Intel, la funcionalidad VT (Virtual Technology) y con AMD AMD-V. Se debe tener especial cuidado al evaluar los servidores que serán nodos de virtualización, porque si no se incluyen estas tecnologías no se podrán

ejecutar algunos VMM, como los de Microsoft Hyper-V, Citrix XenServer o Red Hat Enterprise Virtualization.

Sin embargo, la validación de los nodos de virtualización no es la única actividad de la planeación del proyecto de virtualización. Además, se debe evaluar cada una de las capas de hardware que afectan a la virtualización, tales como:

#### *Almacenamiento*

Con base en el inventario realizado, se debe tomar en cuenta el espacio utilizado por los servidores actuales y qué tipo de almacenamiento es óptimo para el ambiente virtual: conectado directamente, conectado a través de la red o áreas de almacenamiento en red.

De esto dependerá en mucho el rendimiento de las máquinas virtuales, así como las opciones avanzadas de las tecnologías de virtualización como migración en vivo o alta disponibilidad.

#### *Ancho de banda*

Puesto que el *ancho de banda* de la interfaz de red física del nodo de virtualización va a ser ahora compartido entre múltiples máquinas virtuales, es necesario conocer cuánto tráfico de datos generan los servidores actuales, para ello se pueden utilizar herramientas que reporten el uso de la interfaz de red.

También este es un punto clave para tener redundancia en los elementos que conforman el ambiente virtual; en el caso de que se vea interrumpido el acceso a las unidades de almacenamiento donde residen las máquinas virtuales por la falla de una interfaz de red, este concepto se conoce como multipath.

Entonces, si el nodo de virtualización tiene más de una interfaz de red, se pueden asignar a diferentes máquinas virtuales, dependiendo de la demanda de tráfico de red de cada servicio o aplicación instalada.

### *Alimentación eléctrica y ambiente acondicionado*

Es importante cuantificar la alimentación eléctrica y ambiente acondicionado necesarios para pasar de un centro de datos convencional a uno virtual. Esta actividad también ayuda a identificar posibles defectos del sistema de alimentación eléctrica y ambiente acondicionado actuales. Este es uno de los cambios que se ven reflejados en una forma monetaria, al reducir el consumo de energía eléctrica.

#### **2.7.3 Elección del hardware a utilizar**

Desde la elaboración del inventario se puede saber si algún servidor físico existente puede ser útil en la construcción del ambiente virtual. Si no es así, se procede a la búsqueda de hardware para su adquisición, teniendo en cuenta el dimensionamiento del inventario y así poder asegurar que el hardware adquirido es suficiente para formar parte del entorno de virtualización.

Algo muy importante es que se debe tener un estudio de crecimiento de la demanda de recursos de cómputo para las aplicaciones del negocio y de esta forma hacer un buen balance entre el costo de los servidores físicos y la funcionalidad que puede alcanzar.

#### **2.7.4 Identificación de servidores complicados de consolidar en un ambiente virtual**

Un centro de datos puede contener infinidad de servidores de diferentes tipos y propósitos, de ahí que surja la interrogante de cuáles servidores pueden ser virtualizados o consolidados y cuáles no. A continuación se mencionan algunos casos específicos donde la virtualización puede ser una tecnología ineficaz e inviable.

- Virtualizar servidores que usan una cantidad de núcleos mayor a ocho (porque así lo demanda su carga de trabajo) puede ser un problema, esto depende de que el VMM pueda asignar más de ocho núcleos a una máquina virtual.
- Servidores que utilizan más del 85 por ciento de los recursos de hardware pueden ser excluidos del futuro ambiente virtual, siendo que podría acaparar todos los recursos del nodo de virtualización, siendo inviable que conviva con otra máquina virtual.
- Algunos servidores por la naturaleza de sus aplicaciones hacen uso de dispositivos de hardware atípicos, como el USB, dependiendo del VMM se puede cubrir o no esta necesidad, en la actualidad algunos VMM son capaces de virtualizar estos puertos. Sin embargo se pueden

utilizar aplicaciones de terceros para emular puertos USB a través del *protocolo IP*, como AnywhereUSB.

- Servidores de conmutación de voz, de fax o de acceso remoto que requieran acceso a módems, pueden presentar problemas al momento de ser virtualizados, por la falta de soporte del puerto serial.

## 2.8 ANTECEDENTES DEL PROYECTO

### 2.8.1 Funcionalidad y características de KVM

Como se mencionó en el capítulo uno, el producto que comercializa IPCom como solución de virtualización es Red Hat Enterprise Virtualization for Servers. Ahora se abordará de forma detallada esta tecnología, sus componentes básicos y su funcionamiento. Red Hat Enterprise Virtualization for Servers tiene como base la tecnología KVM (Máquina Virtual basada en el Kernel). KVM es una solución de virtualización que utiliza la técnica full-virtualization (virtualización total) para ejecutar las máquinas virtuales. Tiene una base de código pequeña y se apoya de las mejoras del sistema operativo Linux.

El sistema operativo Linux dispone de todos los mecanismos que un VMM necesita para ejecutar máquinas virtuales como un administrador de memoria, un planificador de procesos, una pila de operaciones de entrada-salida, controladores de dispositivos, un administrador de seguridad, implementación de una pila de protocolos de red, etc.; de modo que no es necesario construir todo un sistema de virtualización, basta con agregar algunos componentes para que pueda soportar la tecnología de virtualización. KVM está implementado como un *módulo* del núcleo (kernel) que puede ser cargado en el sistema para convertirlo en un VMM –o hypervisor–.

Como la tecnología KVM utiliza algunas las características que proporciona el hardware es requisito que este cuenta con la tecnología Intel VT-x o AMD-V, anteriormente descritas. KVM ha aprendido de otra tecnología de código abierto: Xen, en este sentido se ha beneficiado de su experiencia. Uno de los mayores retos de la arquitectura de Xen es que el VMM de Xen proporciona funcionalidades esenciales como un planificador de procesos o un administrador de memoria, a diferencia de KVM que

requiere estos componentes del sistema operativo; esto aumenta el rendimiento, siendo que estas tecnologías son mucho más maduras en el sistema operativo Linux que en el VMM de Xen.

Otra característica clave es que KVM forma parte del código fuente de Linux, está completamente disponible para mejoras y correcciones, y además es capaz de heredar las mejoras del kernel de Linux. Xen por otro lado depende de sus desarrolladores para crear mejoras y corregir errores. Cualquier mejora en el kernel de Linux debe ser adaptada al VMM de Xen, para asegurarse que trabaje correctamente, lo cual implica tiempo y esfuerzo.

Por último KVM aprovecha directamente la ayuda de los principales fabricantes de software incluyendo a Red Hat, HP, IBM, Intel, Novell y otros.

### 2.8.1 Arquitectura de KVM

En la arquitectura de KVM (Figura 2.13), cada máquina virtual se implementa como un proceso de Linux, siendo controlado por el planificador de procesos. De hecho cada CPU virtual también se ve como un proceso de Linux, esto le permite a KVM aprovechar todas las características del kernel de Linux.

La emulación de dispositivos –la presentación de dispositivos virtuales a las máquinas virtuales– es controlada por una versión modificada de *QEMU*<sup>25</sup> que proporciona una emulación de *BIOS*, bus de *PCI* y bus de *USB*, además de un conjunto estándar de dispositivos *IDE*, controladoras de disco *SCSI*, interfaces de red, etc.

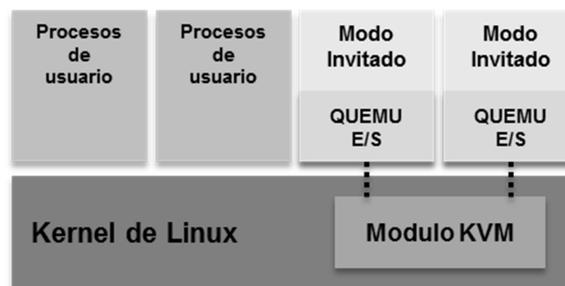


Figura 2.13 Arquitectura de KVM

<sup>25</sup> Timo Hirt, KVM - The kernel-based virtual machine, 2010, p. 10.

Un proceso de Linux tiene dos modos de ejecución: Modo Usuario y Modo Kernel. KVM agrega un tercer modo: Modo Invitado (Guest Mode)<sup>26</sup>; que a la vez tiene su propios Modo Usuario y Modo Kernel, pero estos no interactúan con el VMM.

Las tareas que llevan a cabo se describen en la siguiente tabla:

Tabla 2.3 Modos de ejecución y sus funciones

Modo de ejecución	Tareas que realiza
Modo Invitado	Ejecuta las instrucciones del sistema operativo virtual que no son de entrada-salida.
Modo Kernel	Cambia al Modo Invitado y controla cualquier instrucción del sistema operativo virtual que sea de entrada-salida o alguna instrucción especial.
Modo Usuario	Realiza las operaciones de entrada-salida en nombre del sistema operativo virtual.

Por la integración en el kernel, el VMM de KVM automáticamente adopta las últimas características provenientes del hardware sin mayor configuración.

#### *Administración de recursos*

KVM está diseñado para reusar tanto código como sea posible, se modificó el administrador de memoria de Linux para poder asignar memoria física en el espacio de direcciones de la máquina virtual. Se agregaron tablas de páginas *shadow* que eran necesarias cuando surgió la virtualización de la plataforma x86, cuando Intel y AMD aun no desarrollaban las tecnologías EPT y NPT (mencionadas anteriormente), respectivamente. Posteriormente el soporte para estas tecnologías fue incluido.

En los sistemas operativos modernos hay muchos más procesos que CPUs disponibles para ejecutarlos. El planificador de un sistema operativo calcula el orden en que cada proceso es asignado a un CPU disponible. De esta forma todos los procesos en ejecución comparten el tiempo de cómputo. Dado que KVM fue diseñado para utilizar la mayor parte de los mecanismos de Linux existentes, simplemente se ejecuta una máquina virtual como un proceso, delegándole la tarea al planificador de procesos de asignar poder de cómputo a las máquinas virtuales.

<sup>26</sup> Avi Kivity, et al., *kvm: the Linux Virtual Machine Monitor*, 2007, p. 225.

*Interfaz de control de KVM*

Una vez que el módulo KVM del kernel se ha cargado, se crea el nodo de dispositivo `/dev/kvm`. Este nodo de dispositivo especial representa la interfaz de KVM, la cual permite controlar al VMM a través de un conjunto de llamadas al sistema (`ioctl`). Éstas son comúnmente usadas en ciertos sistemas operativos como una interfaz de comunicación entre los controladores –y en consecuencia con los dispositivos– y los procesos ejecutados en Modo Usuario. Las llamadas al sistema `ioctl()` permiten ejecutar múltiples operaciones para crear nuevas máquinas virtuales, asignar memoria a una máquina virtual y asignar e iniciar los CPUs virtuales.

*Emulación de Hardware*

Para proporcionar dispositivos como discos duros, unidades ópticas, interfaces de red, etc. a las máquinas virtuales, KVM usa una versión de QEMU modificada y altamente optimizada. QEMU es una herramienta de virtualización de plataformas, que permite emular la plataforma completa de una computadora, incluyendo dispositivos de video, red y disco, así como algunos otros. Por cada máquina virtual se inicia un proceso de QEMU en Modo Usuario y los dispositivos emulados se agregan a la máquina virtual en cuestión. Cuando una máquina virtual realiza una operación de entrada-salida, estas son interceptadas por KVM y re-direccionadas al proceso de QEMU correspondiente.

**2.8.2 Modelo de ejecución**

El modelo de ejecución (Figura 2.14) de KVM es un ciclo de acciones para operar las máquinas virtuales. Estas acciones se separan en tres:

*Modo Usuario*

El módulo de KVM es llamado usando la función `ioctl()` para ejecutar código del sistema operativo virtual generado por operaciones de entrada-salida o un evento externo.

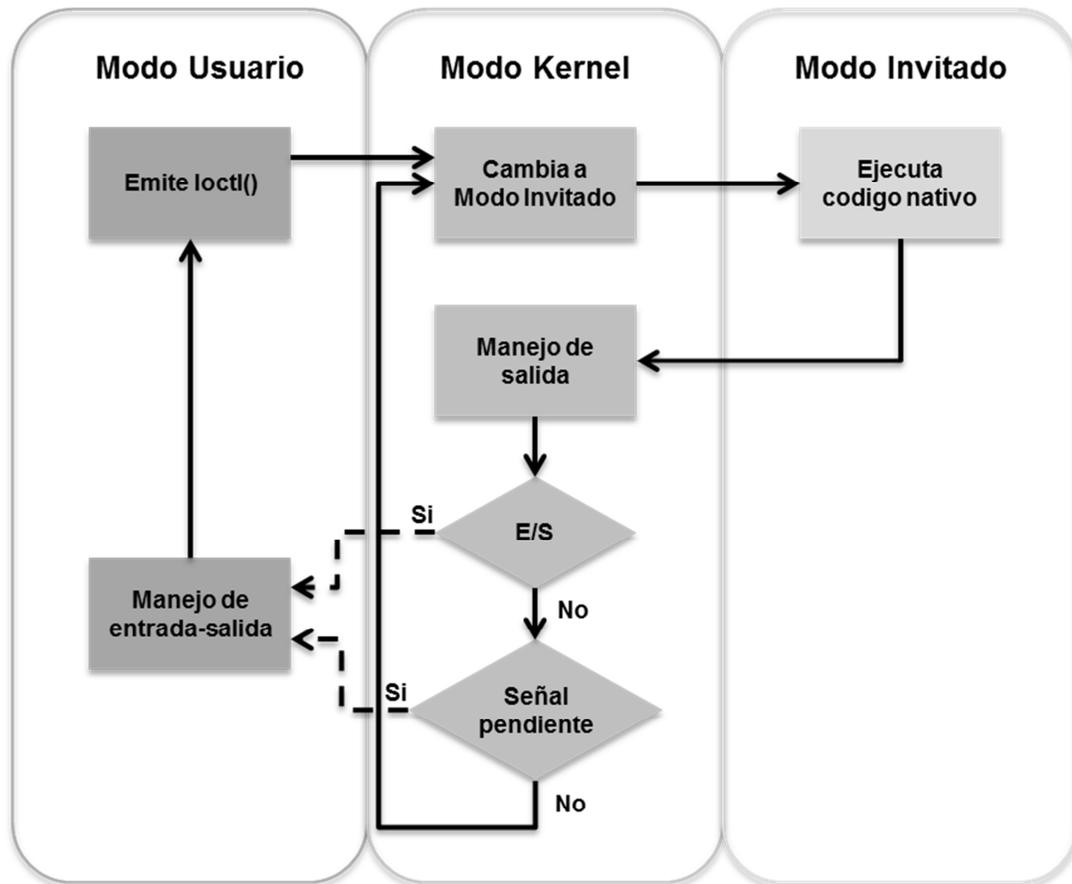
Un evento externo puede ser el arribo de un paquete de red, que podría ser la respuesta a una comunicación establecida por el sistema operativo virtual.

### *Modo Kernel*

El kernel hace que el hardware ejecute código del sistema operativo virtual de forma nativa. El kernel realiza las tareas necesarias para que el procesador de la máquina virtual reanude el flujo de ejecución cuando existen operaciones de memoria pendientes. Si un evento externo como una señal o una operación de entrada-salida iniciada por el sistema operativo virtual surgen, se cambia al modo usuario.

### *Modo Invitado*

Este es el nivel del hardware, donde un conjunto de instrucciones se utilizan para ejecutar código nativo en un CPU con capacidades de virtualización, hasta que una instrucción que necesita la asistencia de KVM, una falla o una interrupción externa se presenten.

Figura 2.14 Diagrama de flujo de los Modos de ejecución<sup>27</sup>

Mientras una máquina virtual se ejecuta, se cambia varias veces entre los modos de ejecución, desde el Modo Kernel hasta el Modo Invitado y viceversa, debido a que solo el código nativo es ejecutado en el hardware.

### 2.8.9 Controladores de dispositivos para-virtuales

Con el soporte del modelo de dispositivos para-virtuales *VirtIO*<sup>28</sup> (Figura 2.15), KVM supera las limitaciones de los dispositivos emulados por QEMU, *VirtIO* es un *framework* para escribir controladores independientes del VMM, acercando el rendimiento al de un dispositivo físico; desde que los dispositivos para-virtuales pueden ser agregados a una máquina virtual se puede prescindir de la emulación.

<sup>27</sup> Avi Kivity, et al., *kvm: the Linux Virtual Machine Monitor*, 2007, p. 226.

<sup>28</sup> Rusty Russell. *virtio: Towards a De-Facto Standard For Virtual I/O Devices*. IBM OzLabs, 2008, p. 2.

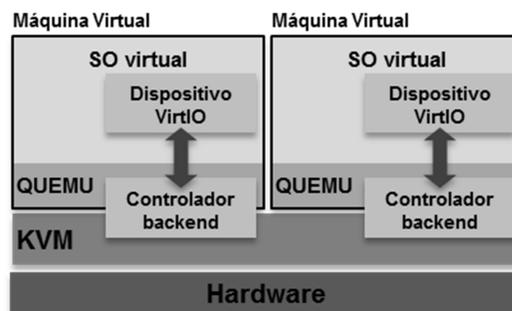


Figura 2.15 Dispositivos para-virtuales VirtIO

En cambio, se utiliza un controlador *backend* para realizar las operaciones de entrada-salida directamente o a través de un controlador backend en Modo Usuario. KVM usa QEMU como un controlador backend el cual maneja las operaciones de entrada-salida directamente, por lo tanto la carga de simular el comportamiento de un disco duro IDE se ve drásticamente reducida al simplemente usar los controladores del kernel para realizar ciertas operaciones.

### 2.8.10 Seguridad en KVM

Como la máquina virtual es ejecutada como un proceso de Linux, se aprovecha el modelo estándar de seguridad de Linux para proporcionar controles de aislamiento y recursos. El kernel de Linux incluye *SELinux*<sup>29</sup> (Seguridad Mejorada de Linux), un proyecto desarrollado en conjunto con la NSA (Agencia de Seguridad Nacional de Estados Unidos) que agrega el control de acceso obligatorio (Mandatory Access Control) al sistema.

Además SELinux proporciona un aislamiento riguroso de recursos y confinamiento para los procesos que están ejecutándose en el kernel.

El proyecto sVirt se basa en SELinux para proporcionar una infraestructura que permita al administrador definir políticas para el aislamiento de las máquinas virtuales, para asegurar que los recursos de una máquina virtual no pueden ser accedidos por otro proceso<sup>30</sup>.

<sup>29</sup> Se ofrece mayor información en: [http://selinuxproject.org/page/Main\\_Page](http://selinuxproject.org/page/Main_Page)

<sup>30</sup> Red Hat Inc., KVM – KERNEL BASED VIRTUAL MACHINE. 2009, p. 6.

Cualquier ambiente virtual es tan seguro como el propio VMM, es decir, si el VMM es comprometido todas las máquinas virtuales quedarían expuestas. SELinux y sVirt proporcionan un nivel de seguridad y aislamiento sin precedentes en la industria.

### 2.8.11 Administración de memoria

KVM hereda las funciones de administración de memoria del sistema operativo. La memoria de una máquina virtual es almacenada como la memoria de cualquier proceso de Linux y puede ser intercambiada a disco (técnica de swapping), almacenada en grandes páginas para incrementar el rendimiento o almacenada a un archivo en el disco. El diseño NUMA<sup>31</sup> (Acceso a memoria no uniforme) permite a las máquinas virtuales el acceso eficiente a grandes cantidades de memoria.

KVM soporta las funcionalidades de los CPU nuevos en el mercado, ya sea EPT (Tabla de páginas extendidas) de Intel o RVI<sup>32</sup> (Indexación rápida de virtualización) de AMD; estos mecanismos reducen la utilización de CPU y mejoran su capacidad de procesamiento.

La compartición de páginas de memoria es soportada mediante una funcionalidad del kernel llamada *KSM*<sup>33</sup> (Fusión de páginas similares del kernel). KSM escanea la memoria de cada máquina virtual y cuando las máquinas virtuales tienen páginas de memoria idénticas, KSM las fusiona en una sola página que comparten, almacenada como una sola página. Si una máquina virtual intenta cambiar la página compartida, se genera una copia para que la utilice. Cuando se consolidan varias máquinas virtuales en un nodo de virtualización, existen varias situaciones en las cuales las páginas de memoria se pueden compartir. Con KSM se pueden consolidar más máquinas virtuales en cada nodo de virtualización, reduciendo los costos de hardware y mejorando la utilización total del servidor.

---

<sup>31</sup> Se ofrece mayor información en: <http://cs.nyu.edu/~lerner/spring10/projects/NUMA.pdf>

<sup>32</sup> Se ofrece mayor información en: [http://www.vmware.com/pdf/RVI\\_performance.pdf](http://www.vmware.com/pdf/RVI_performance.pdf)

<sup>33</sup> Se ofrece mayor información en: <http://www.linux-kvm.com/content/using-ksm-kernel-samepage-merging-kvm>

### 2.8.12 Soporte de Hardware

Desde que KVM es parte de Linux aprovecha el ecosistema de hardware, por lo que cualquier dispositivo de hardware compatible con Linux puede ser utilizado por KVM. Linux tiene de uno de los mayores ecosistemas de proveedores de hardware y la naturaleza de la comunidad de código abierto, donde los fabricantes son capaces de participar en el desarrollo del kernel de Linux, esto asegura de que las últimas características del hardware son rápidamente adoptadas por el kernel de Linux, lo que permite KVM se utilice en una variedad de plataformas de hardware. Conforme las nuevas características se agregan al kernel de Linux, KVM las hereda sin necesidad de modificaciones, además la optimización hecha en Linux inmediatamente beneficia a KVM.

### 2.8.13 Almacenamiento

KVM es capaz de utilizar cualquier sistema de almacenamiento soportado por Linux para guardar las imágenes de las máquinas virtuales, incluidos los discos locales tipo IDE, SCSI y *SATA*, *NAS* (Almacenamiento vinculado en red), incluyendo *NFS* (Sistema de archivos en red), *SAMBA/CIFS* y *SAN* (Área de almacenamiento en red) con soporte de protocolos *iSCSI* y Canal de Fibra. Se puede utilizar técnicas de multi-acceso a dispositivos de almacenamiento (*Multipath I/O*) para mejorar el rendimiento y para proporcionar redundancia; todo esto porque son tecnologías implementadas en el kernel de Linux.

KVM también es soporta el almacenamiento de imágenes de máquinas virtuales en sistemas de archivos compartidos como GFS (Sistema de archivos global) para permitir que estas imágenes puedan ser compartidas entre varios nodos de virtualización o compartidas usando volúmenes lógicos. Las imágenes de disco soportan thin provisioning, lo cual permite que el disco de la máquina virtual crezca como sea requerido hasta el límite señalado.

El formato nativo para los discos en KVM es *qcow2* que incluye soporte para *snapshots* (copias instantáneas). Una imagen *qcow2* permite grabar las modificaciones en una imagen cruda sin sobrescribir los datos existentes. Cada imagen de disco, ya sea integra o *qcow2* puede tener una imagen *qcow2* apuntando a sí misma para escribir las

modificaciones, esto genera una cadena de imágenes compleja, de esta forma cuando se requiera acceso a las modificaciones para lectura o escritura se preserva la otra imagen que no ha sido modificada<sup>34</sup>.

#### **2.8.14 Red**

El controlador de la interfaz de red física transfiere los paquetes al puente Ethernet virtual, éste direcciona los paquetes al dispositivo *TAP* (controlador Ethernet virtual) apropiado, el cual implementa los dispositivos de red en software. Los paquetes son enviados por el nodo de virtualización a través del TAP hacia un programa de QEMU que se une al dispositivo físico. Una vez que los paquetes son transferidos, el TAP da una señal al módulo de KVM, esta señal es una interrupción virtual para que QEMU notifique a la máquina virtual sobre un nuevo paquete. Cuando se recibe la interrupción virtual, QEMU entrega el paquete a la pila de protocolos de red del sistema operativo virtual. Este esquema de trabajo tiene sus ventajas cuando se generan operaciones de E/S masivas<sup>35</sup>.

#### **2.8.15 Migración en vivo**

KVM soporta migración en vivo la cual ofrece la capacidad de mover una máquina virtual en ejecución entre nodos de virtualización sin interrupción de servicio. Esta técnica es transparente para el usuario final, la máquina virtual se mantiene encendida, las conexiones de red siguen activas y las aplicaciones del usuario siguen funcionando mientras la máquina virtual es reubicada a un nuevo nodo de virtualización. Además de la migración en vivo, KVM permite guardar el estado actual de una máquina virtual a disco para que pueda ser almacenado y posteriormente se reanude su ejecución.

#### **2.8.16 Soporte de sistemas operativos virtuales**

KVM es compatible con una amplia variedad de sistemas operativos virtuales, como Linux, Windows y otras plataformas como OpenBSD, FreeBSD, OpenSolaris, Solaris x86 y MS DOS<sup>36</sup>. En los productos de Red Hat, KVM ha sido certificado por el Programa de validación para la virtualización de Microsoft Windows Server (PVVS) para asegurar que

---

<sup>34</sup> Yu Su, et al., Data Hiding in Virtual Machine Disk Images. 2010, p. 2279.

<sup>35</sup> Qiang Li, et al., VM-based Architecture for Network Monitoring and Analysis. 2008, p. 1397.

<sup>36</sup> Red Hat Inc., KVM – KERNEL BASED VIRTUAL MACHINE. 2009, p. 8.

los usuarios que virtualizan Microsoft Windows Server reciban soporte comercial de Microsoft.

### **2.8.17 Rendimiento y escalabilidad**

KVM hereda el rendimiento y la escalabilidad de Linux, soportando para las máquinas virtuales hasta 16 CPUs virtuales con 256GB de memoria *RAM*, en los nodos de virtualización hasta 256 núcleos y 1TB o más de RAM.

El rendimiento general está entre 95% y 135% respecto al del hardware, esto en aplicaciones empresariales como SAP, Oracle, *LAMP* y Microsoft Exchange<sup>37</sup>.

## **2.9 RED HAT ENTERPRISE VIRTUALIZATION FOR SERVERS**

Red Hat Enterprise Virtualization for Servers es un producto de Red Hat Inc. lanzado al mercado en 2009 a partir de la compra de Qumranet. Red Hat Enterprise Virtualization for Servers es una solución completa de virtualización, que está diseñada para permitir la virtualización de centros de datos y maximizar la eficiencia de la operación y de la inversión en infraestructura.

Red Hat Enterprise Virtualization proporciona a los departamentos de TI las herramientas necesarias para afrontar los problemas de la administración de ambientes grandes y complejos. La tecnología de punta de Red Hat Enterprise Virtualization permite a los administradores reducir el costo y la complejidad de grandes implementaciones, así sean miles de máquinas virtuales. La plataforma Red Hat Enterprise Virtualization incluye:

- Alta disponibilidad para configurar las máquinas virtuales para tolerancia a fallos
- Migración en vivo para mover máquinas virtuales entre nodos de virtualización sin interrupción
- Planificador para crear políticas que equilibren dinámicamente los recursos de cómputo
- Sistema de ahorro de energía para crear políticas que reduzcan los costos de electricidad y aire acondicionado
- Administrador de imágenes para crear, administrar y aprovisionar máquinas virtuales

---

<sup>37</sup> Red Hat Inc., KVM – KERNEL BASED VIRTUAL MACHINE. 2009, p. 9.

- Implementación de un ambiente en Clúster para el acceso al almacenamiento desde cualquier nodo de virtualización.

### 2.9.1 Arquitectura de Red Hat Enterprise Virtualization

La plataforma Red Hat Enterprise Virtualization (Figura 2.16) principalmente consta de tres componentes:

- Red Hat Enterprise Virtualization Hypervisor (*RHEV-H*). Basado en KVM, es una capa de virtualización implementada a través de la infraestructura del servidor. Debido a que es un módulo del kernel de Linux, KVM es un medio muy eficaz para realizar la virtualización. Este componente tiene las tareas de VMM (Monitor de máquina virtual). Este componente puede ser uno o varios nodos de virtualización, basado en RHEL (Red Hat Enterprise Linux) la distribución de Linux soportada por Red Hat. De ahora en adelante se hará referencia a Red Hat Enterprise Virtualization Hypervisor como RHEV-H.
- Agentes y herramientas. Incluyen VDSM (Virtual Desktop Server Manager) que se ejecuta en el RHEV-H o nodo de virtualización y proporciona la administración local para las máquinas virtuales, redes y almacenamiento.
- Red Hat Enterprise Virtualization Manager (*RHEV-M*). Permite a los usuarios ver y administrar todos los componentes del sistema, las máquinas virtuales y las imágenes desde una interfaz gráfica. El sistema de administración de interfaz gráfica ofrece una amplia gama de características que incluyen capacidades de búsqueda, administración de recursos, migraciones en vivo y aprovisionamiento. De ahora en adelante se hará referencia a Red Hat Enterprise Virtualization Manager como RHEV-M.

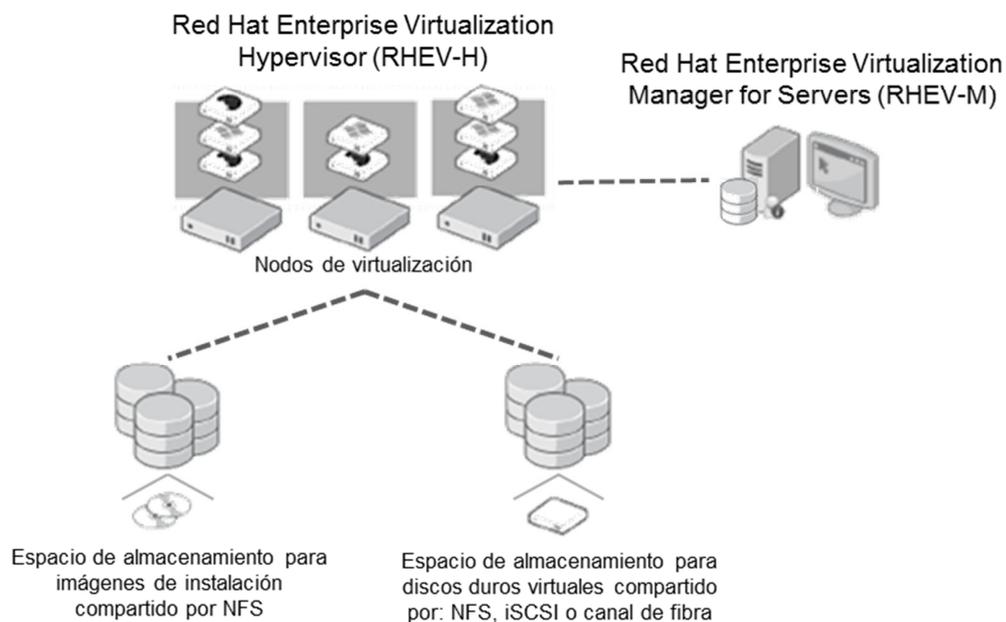


Figura 2.16 Arquitectura y componentes adicionales de Red Hat Enterprise Linux for Servers

Estos componentes funcionan en conjunto perfectamente para permitir al administrador del sistema la configuración y mantenimiento del ambiente virtual a través de una interfaz gráfica.

Adicionalmente, Red Hat Enterprise Virtualization requiere de otros componentes para su funcionamiento, éstos son dos medios de almacenamiento:

- Almacenamiento para las imágenes de los discos duros virtuales.- Este espacio puede ser de un dispositivo espacial como un NAS (Almacenamiento vinculado en red) NAS o una SAN, el requerimiento es que el protocolo a usar para compartir el espacio sea NFS, iSCSI o canal de fibra (*fibre channel*), estos son los protocolos soportados por la solución Red Hat Enterprise Virtualization.
- Almacenamiento para las imágenes de instalación.- Este espacio debe ser compartido a los nodos de virtualización por el protocolo NFS (sistemas de archivos en red), cualquier servicio o dispositivo que soporte este protocolo puede ser usado.

### **2.9.2 Terminología para los recursos de Red Hat Enterprise Virtualization**

#### *Centros de datos (Data Centers)*

Un centro de datos es una entidad lógica que define el conjunto de los recursos utilizados en un entorno específico. Se trata de una colección de una serie de clústeres, máquinas virtuales, dispositivos de almacenamiento y de redes. El centro de datos es el contenedor de más alto nivel para todos los recursos físicos y lógicos dentro del entorno virtual administrado.

#### *Dispositivos de almacenamiento (Storage)*

Un centro de datos depende de dispositivos de almacenamiento físico accesible y adecuado. La plataforma de administración RHEV-M proporciona una visión abstracta del almacenamiento físico asignado a un centro de datos, que permite a los administradores supervisar y gestionar fácilmente los requerimientos de almacenamiento.

Un conjunto de almacenamiento (Storage Pool) es una entidad lógica que contiene un depósito de almacenamiento de algún tipo, ya sea iSCSI, Canal de Fibra o NFS (Sistema de archivos en red). Cada conjunto de almacenamiento puede contener varios dominios de almacenamiento, para las imágenes de disco de las máquinas virtuales y para las imágenes

de instalación (*imágenes ISO 9660*). Los dominios de almacenamiento son un recurso en RHEV-M.

### *Clústeres (Clusters)*

Un clúster es un conjunto de nodos de virtualización –servidores físicos– que se manejan como un conjunto de recursos para una serie de máquinas virtuales. Los nodos de virtualización en el clúster comparten la misma infraestructura de red y los mismos dispositivos de almacenamiento. También es un dominio de migración en el que las máquinas virtuales se pueden mover de un nodo a otro.

### *Nodos de virtualización (Hosts)*

Un nodo de virtualización o host, es un servidor físico en el que se instala y ejecuta RHEV-H –el VMM– y que contiene las máquinas virtuales. Los nodos de virtualización se agrupan en clústeres. Las máquinas virtuales se pueden migrar desde un nodo a otro dentro de un clúster de servidores.

### *Máquinas Virtuales (Virtual Machines)*

Las máquinas virtuales pueden ser utilizadas como servidores virtuales y se pueden migrar desde un nodo de virtualización a otro dentro de un clúster.

### *Plantillas (Templates)*

Una plantilla es un modelo de una máquina virtual con cierta configuración y características. Una máquina virtual que se construye a partir de una plantilla determinada adquiere su configuración y características. Las plantillas se utilizan de manera conveniente y eficaz para crear un conjunto de máquinas virtuales idénticas, práctica conocida como aprovisionamiento rápido.

### *Copias instantáneas (Snapshots)*

Una copia instantánea es una imagen del sistema operativo virtual y todas las aplicaciones de una máquina virtual en un punto específico en el tiempo. Puede ser utilizada para guardar la configuración de una máquina virtual antes de una actualización o

antes instalar una nueva aplicación. En caso de algún problema, los parámetros de la copia instantánea se pueden utilizar para restaurar la máquina virtual al estado antes de la actualización o instalación.

### 2.9.3 Funcionalidades de Red Hat Enterprise Virtualization for Servers

#### *Alta disponibilidad*

Red Hat Enterprise Virtualization incluye prioridad en un ambiente de alta disponibilidad (Figura 2.17). RHEV-M supervisa continuamente los nodos de virtualización. Si ocurre una falla de hardware, cualquier máquina virtual configurada para estar en alta disponibilidad se reiniciará en otro nodo del clúster. Los tres niveles de prioridad; alto, medio y bajo, permiten a los administradores asegurar que las máquinas virtuales más críticas se reiniciarán primero.

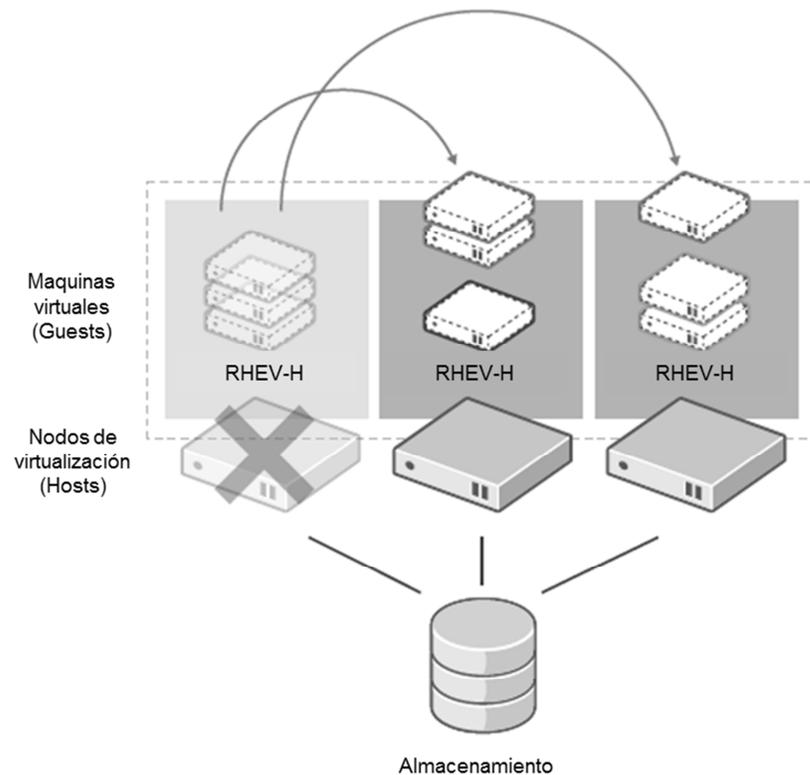


Figura 2.17 Funcionamiento de la característica de alta disponibilidad<sup>38</sup>

<sup>38</sup> Red Hat Inc., RED HAT ENTERPRISE VIRTUALIZATION: HIGH AVAILABILITY, 2009.

Así como el monitoreo de los nodos de virtualización, cada máquina virtual se monitorea. Si una falla de la máquina virtual se detecta, la máquina virtual se reiniciará automáticamente.

El reinicio de las máquinas virtuales es automático, sin intervención del usuario y el administrador recibe la notificación. Cuando el nodo de virtualización original se recupera, la migración en vivo se puede utilizar para regresar la máquina virtual a su nodo original, sin ninguna interrupción del servicio. El sistema de alta disponibilidad se integra con el sistema planificador para garantizar que la máquina virtual se reinicia en un nodo, en función de su utilización de los recursos actuales y en el cumplimiento de cualquier equilibrio de carga de trabajo o las políticas de ahorro de energía.

Con Red Hat Enterprise Virtualization la configuración de alta disponibilidad de una máquina virtual es simple como hacer clic en una casilla de verificación y seleccionar un nivel de prioridad. Las alertas se pueden configurar para notificar al administrador en caso de errores.

Además se pueden utilizar otras técnicas de *failover* para las conexiones de red con los dispositivos de almacenamiento, como Multipath I/O.

Un ambiente de alta disponibilidad en Red Hat Enterprise Virtualization requiere un sistema mediante una interfaz de administración, como IPMI, Dell DRAC, HP iLO, IBM RSA, BladeCenter<sup>39</sup>. Si surge una falla, estas interfaces se utilizan para comprobar el estado del hardware y controlar el apagado-encendido del equipo físico.

### *Migración en vivo*

Red Hat Enterprise Virtualization incluye un sistema de migración en vivo (Figura 2.18), que proporciona la capacidad de mover una máquina virtual en ejecución entre nodos de virtualización sin interrupción del servicio. La migración es transparente para el usuario final: la máquina virtual se mantiene encendida y las aplicaciones del usuario continúan

---

<sup>39</sup> Red Hat Inc., Red Hat Enterprise Virtualization for Servers 2.2: Administration Guide. 2010, p. 90

funcionando, mientras la máquina virtual se traslada a un nuevo nodo del clúster. Este sistema de migración conlleva beneficios como:

- Cambiar la ubicación de una máquina virtual a un nuevo nodo de virtualización para equilibrar dinámicamente los recursos dentro de un clúster.
- Migración de una máquina virtual desde un nodo que pueda estar experimentando una falla mínima.
- Mover una máquina virtual a un nuevo nodo para liberar recursos y así poder asignarlos a otras máquinas virtuales.

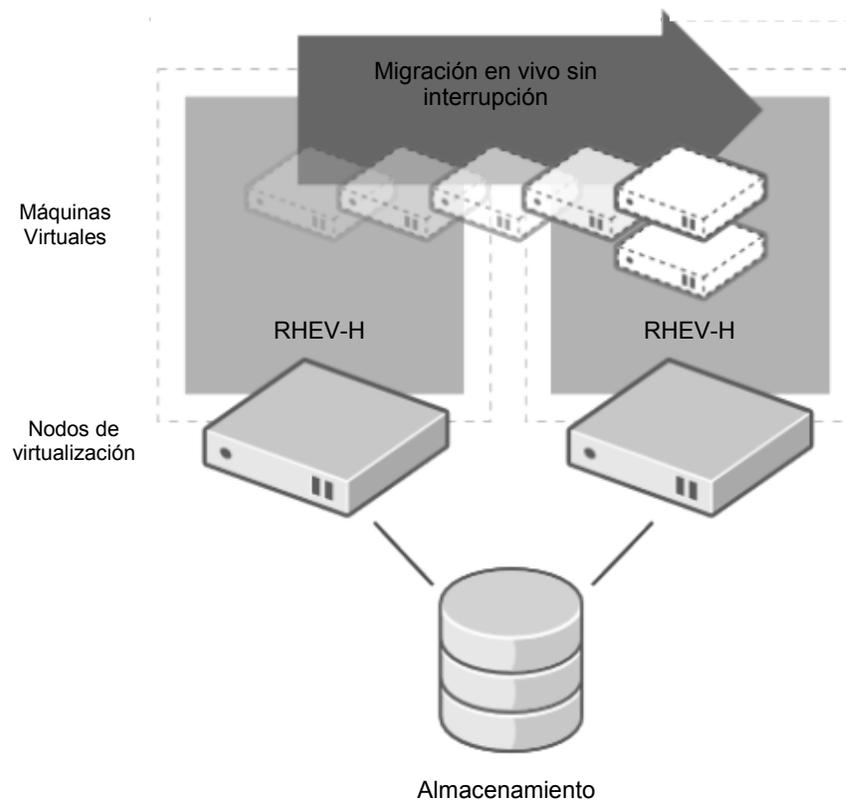


Figura 2.18 Funcionamiento de la característica de migración en vivo<sup>40</sup>

El sistema de migración en vivo es administrado desde RHEV-M. Desde esta interfaz web, el administrador puede definir un conjunto de nodos de virtualización en el que una máquina virtual puede ejecutarse, de esta forma RHEV-M se asegura que cada nodo de virtualización puede acceder a todos los recursos necesarios para ejecutar la máquina virtual. Los siguientes recursos son monitoreados para asegurar una migración exitosa:

<sup>40</sup> Red Hat Inc., RED HAT ENTERPRISE VIRTUALIZATION: LIVE MIGRATION, 2009.

- Almacenamiento. Para asegurar que cada nodo del clúster tiene acceso a los discos duros virtuales utilizados por las máquinas virtuales ya sea que el servidor de almacenamiento use el protocolo NFS, Fibre Channel o iSCSI.
- Red. Para comprobar que el nodo de virtualización tiene acceso a las redes virtuales o *VLAN* utilizadas por la máquina virtual. Durante la migración en vivo, las direcciones MAC de las interfaces de red asignadas a la máquina virtual se mantienen, lo que permite que las conexiones permanezcan activas durante y después de la migración.
- Utilización de CPU. Para asegurar que la migración de la máquina virtual no sobrepasará el umbral de utilización de CPU máximo definido en el nodo de virtualización.
- Memoria. Para comprobar que hay suficiente memoria disponible en el nodo de virtualización para ejecutar la máquina virtual.
- Compatibilidad de CPU. Para asegurar que cada nodo en el clúster tiene una familia de CPU compatible con la máquina a migrar. RHEV-M puede seleccionar automáticamente el nodo de virtualización al que se va a migrar la máquina virtual o el administrador puede anular la selección automática para elegir un nodo específico.

También se utiliza la migración en vivo por el sistema de ahorro de energía, que permite a los administradores definir reglas para equilibrar la carga de trabajo en el centro de datos de forma automática.

El almacenamiento compartido es necesario para la migración en vivo. Red Hat Enterprise Virtualization es compatible con NAS, NFS y modelos de almacenamiento SAN a través de Fibre Channel o iSCSI incluyendo soporte para Multipath I/O, lo que hace más confiable el acceso a los dispositivos de almacenamiento.

### *Planificador*

El planificador de Red Hat Enterprise Virtualization (Figura 2.19) administra la asignación de los recursos físicos basándose en políticas definidas por el administrador; y continuamente monitorea el uso de los recursos por los nodos de virtualización y las máquinas virtuales.

Los recursos físicos en el centro de datos virtual que maneja el planificador, como nodos de virtualización, almacenamiento y redes se pueden agrupar en depósitos lógicos (logical pools) para tener un control más flexible. Las áreas de almacenamiento se agregan al centro de datos virtual en forma de dominios de almacenamiento (storage domains), y son creados a partir de una conexión por canal de fibra, iSCSI o NFS. Los recursos de red

como redes físicas o VLANs se definen por centro de datos virtual y se pueden asignar a un clúster o a varios.

Los nodos de virtualización se agrupan en clústeres. El planificador es responsable de la asignación de una máquina virtual a un nodo del clúster.

Cuando una máquina virtual se inicia el planificador selecciona automáticamente el nodo de virtualización en el cual se ejecutará, basándose en la utilización del sistema y las políticas de recursos.

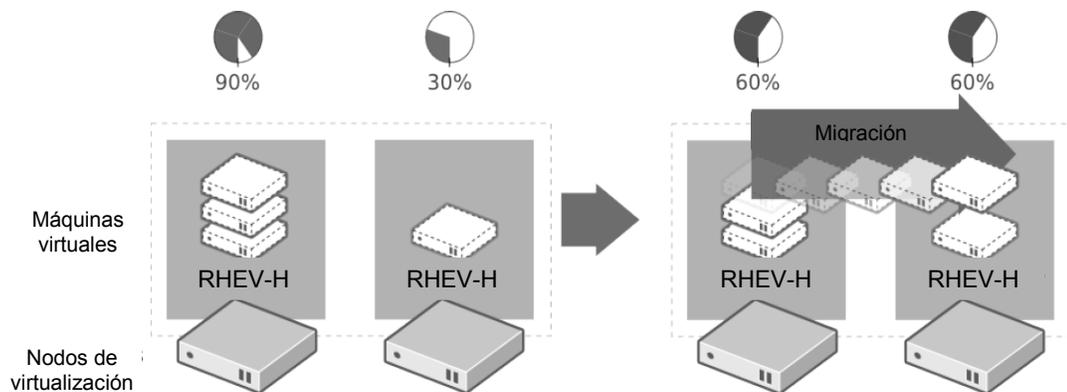


Figura 2.19 Funcionamiento del planificador para balancear la carga de trabajo<sup>41</sup>

El administrador puede definir umbrales de utilización de recursos en los que el planificador utilizará automáticamente la migración en vivo para trasladar las máquinas virtuales a un nodo específico, esto se usa para balancear la carga entre los nodos de virtualización, si ésta es grande; o para apagar nodos de virtualización si se están sub-utilizando, reduciendo así el consumo de energía eléctrica (Figura 2.20). El administrador configura el nivel de servicio mínimo en el cual se activa la política de ahorro de la energía. Por ejemplo, si la utilización de un nodo de virtualización es de 10% durante 20 minutos o más el planificador migra las máquinas virtuales que se ejecutan en este servidor a otros nodos del clúster.

<sup>41</sup> Red Hat Inc., RED HAT ENTERPRISE VIRTUALIZATION: SYSTEM SCHEDULER, 2009.

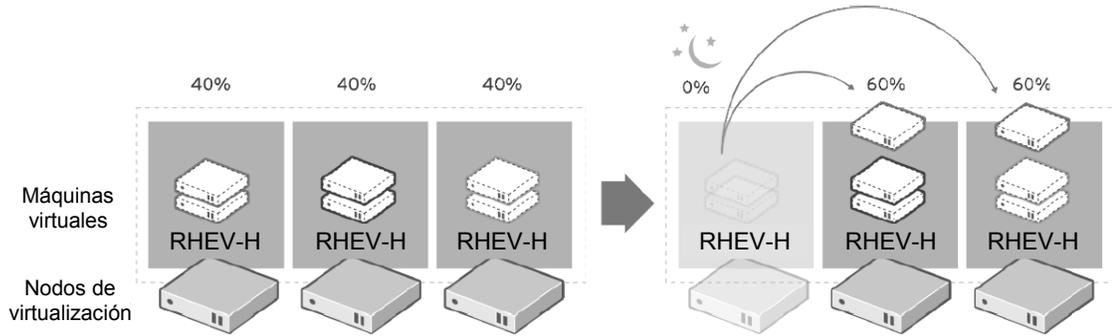


Figura 2.20 Funcionamiento del planificador para desocupar un nodo subutilizado<sup>42</sup>

### Administrador de imágenes (Figura 2.21)

RHEV-M incluye imágenes de un conjunto de características para crear y administrar imágenes de una máquina virtual, incluyendo:

- Aprovisionamiento ligero (Thin provisioning). Permitiendo a los administradores utilizar más eficazmente su almacenamiento
- Copias instantáneas. Una copia instantánea es la imagen de una máquina virtual en un punto en el tiempo. Las copias instantáneas permiten al usuario ejecutar una máquina virtual en un punto anterior en el tiempo, como si fueran puntos de restauración, por ejemplo, tomar una copia instantánea de una máquina virtual antes de que la actualización de una aplicación proporciona un punto de retorno en caso de problemas de compatibilidad con la nueva versión de la aplicación. Las copias instantáneas se pueden ver como respaldos en caso de una situación contingencia. La copia instantánea solo almacena las diferencias entre la imagen original y el estado actual, de forma que ahorra almacenamiento.
- Plantillas. Una plantilla es una imagen maestra de máquina virtual que se puede utilizar para crear rápidamente máquinas virtuales idénticas. Las plantillas pueden ser creadas a partir de una máquina virtual. El administrador puede generar múltiples plantillas que se almacenan en la biblioteca de imágenes.

<sup>42</sup> Red Hat Inc., RED HAT ENTERPRISE VIRTUALIZATION: SYSTEM SCHEDULER, 2009.



Figura 2.21 Funcionamiento del administrador de imágenes<sup>43</sup>

### 2.9.4 Esquema de suscripción de Red Hat Enterprise Virtualization for Servers

El costo de la suscripción de Red Hat Enterprise Virtualization for Servers (Figura 2.22) se calcula de acuerdo con el número de CPUs físicos de los nodos de virtualización, es decir, no hay límite de núcleos por nodo de virtualización. La suscripción incluye soporte técnico por un año con dos tipos de soporte: Standard y Premium, el primero con una cobertura en horario hábil de oficina y la segunda una cobertura total. Se debe tomar en cuenta las licencias o suscripciones de los sistemas operativos virtuales, tales no se incluyen en la suscripción Red Hat Enterprise for Servers

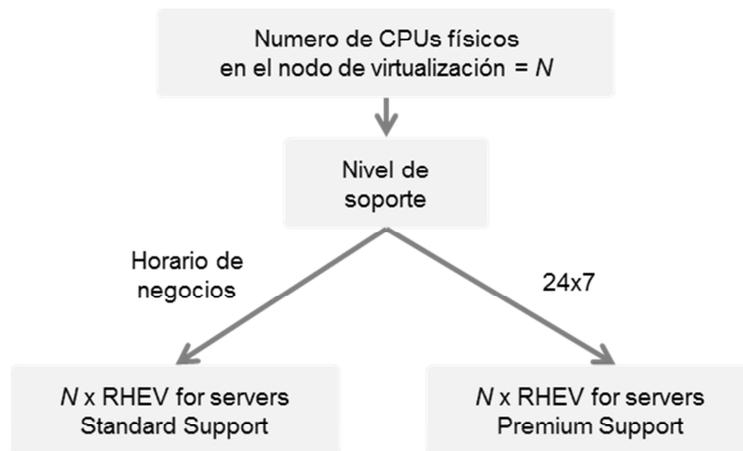


Figura 2.22 Tipos de suscripciones de Red Hat Enterprise Virtualization for Servers<sup>44</sup>

<sup>43</sup> Red Hat Inc., RED HAT ENTERPRISE VIRTUALIZATION: IMAGE MANAGER, 2009.

## 2.10 PRESENTACIÓN DEL PROYECTO

La empresa aseguradora se interesó en la solución de virtualización Red Hat Enterprise Virtualization for Servers para iniciar un proyecto interno que implicaba la consolidación de servidores físicos, la renovación tecnológica de una parte de su infraestructura de TI, optimización de la administración de los servidores y las bases para tener mecanismos de replicación y otros que le permitieran la continuación de las operaciones críticas en caso de una contingencia. La motivación fue su regulación interna y también cumplir con ciertos lineamientos de administración de infraestructura de TI al integrar junto con otras empresas un grupo asegurador a nivel nacional.

Así mismo internamente el área de sistemas realizó un estudio para determinar cuáles son los servidores que convenientemente podrían existir en un ambiente virtual. Como resultado de ese estudio se seleccionaron diez servidores candidatos a virtualizar, mostrados en la Tabla 2.4:

Tabla 2.4 Servidores candidatos a virtualizar

Núm.	Servidor	Sistema Operativo	Aplicación
1	Servidor Nómina	Microsoft Windows Server 2008	No conocida
2	Servidor Web	Microsoft Windows Server 2008	Microsoft IIS
3	Servidor Base de datos	Red Hat Enterprise Linux 5.4	Oracle
4	Servidor Archivos	SUSE Linux Enterprise Server 10	No aplica
5	Servidor VPN	Debian GNU/Linux 5.0	Vyatta
6	Servidor Sistema de negocio 1	Microsoft Windows Server 2008	SAP
7	Servidor Sistema de negocio 2	Microsoft Windows Server 2008	Microsoft IIS, .Net Framework
8	Servidor Intranet	Red Hat Enterprise Linux 5.3	LAMP
9	Servidor Propietario 1	Microsoft Windows Server 2008 R2	Software desarrollado en casa
10	Servidor Propietario 2	Microsoft Windows Server 2008 R2	Software desarrollado en casa

Algunas aplicaciones no se presentan como no conocidas y otras como desarrolladas en casa, esto con el fin de no dar demasiados detalles de la organización.

<sup>44</sup> Red Hat Inc., RED HAT ENTERPRISE VIRTUALIZATION FOR SERVERS: PRICING QUICK GUIDE, 2009.

La aseguradora ya cuenta con un medio de almacenamiento, una SAN (Área de almacenamiento en red) y se les va a sugerir cuántos servidores y de qué características serán necesarios para ser nodos de virtualización.

### **2.10.1 Plan de trabajo**

El inicio de un proyecto como este empieza cuando se elabora la propuesta de la solución con base en los requerimientos del cliente, una parte medular de la propuesta es el plan de trabajo, que incluye desde la planeación hasta la entrega del producto final y su memoria técnica. El plan de trabajo es resultado del análisis general del proyecto y especifica puntualmente tiempos y objetivos medios para el sano cumplimiento de cada una de las etapas.

Aunque la planeación y la implementación de un producto de software no es tan demandante como el desarrollo de software, sí involucra muchas tareas, tanto del cliente como del consultor, estas tareas deben estar bien planteadas para definir alcances, requerimientos y riesgos, por ejemplo, en un proyecto de virtualización se depende mucho de la infraestructura existente para determinar si se puede construir el ambiente virtual con el equipo actual o es necesario adquirir nuevos equipos y si es así, dimensionar sus características.

Este proyecto se dividió en cuatro grandes etapas: planeación, implementación, pruebas y entrega final; para cada una de estas etapas se estableció un tiempo estimado con base en las tareas a realizar y los riesgos que podrían retrasar o desviar el plan original. A continuación se describe cada una de estas etapas.

#### *Planeación.*

En esta etapa se calculan los recursos de cómputo necesarios para construir el ambiente virtual, para este proyecto se siguió una metodología general (antes mencionada), en donde se desarrollan las siguientes etapas:

- Descubrimiento
- Análisis
  - Almacenamiento

- Ancho de banda
- Memoria
- Elección del hardware a utilizar
- Identificación de servidores complicados de consolidar en un ambiente virtual  
Tiempo estimado de realización de esta etapa: 24h. Más tiempo adicional para el levantamiento de la información (depende de la operación del cliente).

#### *Riesgos en la planeación.*

Si la ejecución de esta tarea se hace de forma cuidadosa se pueden evitar muchos problemas en las subsecuentes etapas. Los riesgos identificados para esta etapa fueron los siguientes:

- No tener acceso a una herramienta adecuada para recabar la información necesaria de la infraestructura actual.
- Que no se cuente con otro medio para obtener la información mencionada.
- Que los datos sacados no consideren la carga de trabajo, en días o franjas horarias, cuando ésta es máxima.
- Que las aplicaciones actuales tengan algún tipo de conflicto interno que genere más carga de trabajo (por problemas de configuración o software defectuoso) que descarten al servidor como candidato a servidor virtual.
- Que el presupuesto del cliente no sea suficiente para adquirir nueva infraestructura si es necesario.
- Que un servidor clave para el desarrollo del proyecto no sea candidato a servidor virtual y por lo tanto genere la cancelación del proyecto.

#### *Implementación.*

En esta etapa considera toda la preparación e instalación de la solución de virtualización propuesta, para la cual es necesario contar con todo el equipo a utilizar, su instalación física y los ajustes en la infraestructura actual: red, dispositivos de almacenamiento, servidores existentes que se integren a la solución, etc. Los servicios para esta etapa son de instalación y configuración de software, en ningún momento se considera configuración de hardware salvo que los requerimientos de la solución así lo requieran. Esta etapa se divide en las siguientes tareas:

- Instalación de Red Hat Enterprise Virtualization Manager (RHEV-M)
- Configuración inicial de Red Hat Enterprise Virtualization Manager (RHEV-M)
- Instalación de Red Hat Enterprise Virtualization Hypervisor (RHEV-H)

- Configuración inicial de Red Hat Enterprise Virtualization Hypervisor (RHEV-H)
  - Integración de los sistemas RHEV-M y RHEV-H
  - Preparación de los dispositivos de almacenamiento
  - Construcción del ambiente virtual
- Tiempo estimado de realización de esta etapa: 40h

*Riesgos en la implementación.*

En esta etapa fueron considerados los siguientes riesgos:

- Que el equipo de cómputo designado para la implementación no sea el recomendado.
- Que la preparación previa de los equipos no se pueda llevar a cabo por conflictos con la política interna de la empresa.
- Que el equipo designado no esté debidamente instalado (físicamente).
- Que al equipo designado le fallen o le falten componentes necesarios para la implementación de la solución.
- Que el personal de la empresa no esté disponible para atender al consultor que ejecute la implementación.
- Que la infraestructura actual de la empresa no esté disponible por alguna contingencia fuera de control.
- Que no se cuenten con las suscripciones del software durante la implementación.

*Pruebas.*

Ya construido el ambiente virtual se realizarán pruebas para ejemplificar las funcionalidades de la solución y garantizar que el ambiente virtual es estable. En esta etapa se realizarán las siguientes tareas.

- Creación de máquina virtual de prueba.
  - Prueba de la funcionalidad migración en vivo.
  - Prueba de la funcionalidad alta disponibilidad.
  - Limpieza del ambiente virtual (Eliminación de la máquina virtual de prueba).
- Tiempo estimado de realización de esta etapa: 8h

*Riesgos en las pruebas.*

Los riesgos identificados para esta etapa fueron los siguientes:

- Que el ambiente virtual sea inestable.
- Que no se cuente con el tiempo contemplado para las pruebas.

- Que el personal de la empresa cliente no esté disponible para dar su visto bueno a las pruebas.

#### *Entrega final.*

En esta etapa se crearán las máquinas virtuales definidas en el objetivo, después de haber probado que el ambiente virtual es estable. Además de la entrega de la memoria técnica al cliente.

- Creación de las máquinas virtuales.
  - Entrega de documentación oficial de la solución implementada.
  - Entrega de la memoria técnica del proyecto (dos semanas después de concluido el proyecto).
  - Aprobación del cliente.
- Tiempo estimado de realización de esta etapa: 8h (y dos semanas para la entrega de la memoria técnica)

#### *Riesgos en la entrega final.*

Los riesgos identificados para esta etapa fueron los siguientes:

- Que surjan incidentes no previstos en las etapas de planeación y pruebas.
- Que el cliente no apruebe la finalización del proyecto.

## **2.11 OBJETIVO**

El objetivo del proyecto es proporcionar una plataforma de virtualización para la consolidación de diez servidores físicos de forma eficiente para el óptimo desempeño de aplicaciones críticas para el negocio del cliente, proporcionando técnicas de alta disponibilidad, recuperación rápida y sencilla en caso de una contingencia, así como un método de respaldo ágil y eficiente. Estos servidores físicos consolidados –o virtuales– contienen aplicaciones propietarias del cliente (desarrolladas en la misma empresa), gestores de bases de datos, servicios de páginas web y algunas otras aplicaciones generales.

De los diez servidores que se pasaron a un ambiente virtual, se encuentran tres que contienen aplicaciones críticas para el negocio de la empresa, para lograr el rendimiento documentado (por el fabricante del software de virtualización) de estas aplicaciones en el

ambiente virtual se crearán las máquinas virtuales de acuerdo con la demanda de los recursos del servicio y de acuerdo con las recomendaciones de los fabricantes, tanto del software de virtualización como de las aplicaciones a instalar.

Se hace énfasis en el hecho de que el cliente se encargará de la instalación de las aplicaciones y de la migración de los datos. El alcance del proyecto es la puesta a punto de la plataforma de virtualización y la creación de las máquinas virtuales de acuerdo con la documentación oficial y las recomendaciones del fabricante. No se considera la instalación de sistemas operativos y aplicaciones como parte de este proyecto.

## 2.12 PLANEACIÓN DEL PROYECTO DE CONSOLIDACIÓN

### 2.12.1 Descubrimiento

Dado que Red Hat no tiene una herramienta propia para realizar el estudio de planeación en un proyecto de consolidación se podría usar MAP, VGC (las otras mencionadas tienen un costo) o alguna otra de la que se disponga. Normalmente esta tarea la realizo usando una herramienta de monitoreo de software libre, pero eso depende del cliente, puesto que esta herramienta se debe ejecutar en su infraestructura.

En este caso el cliente ya cuenta con una herramienta de monitoreo y accedió a proporcionarnos los reportes necesarios. El primer reporte proporcionado fue el del inventario de los servidores candidatos, donde se presenta información como el tipo de CPU, la cantidad de memoria total, el tipo de interfaz de red y la capacidad total de disco duro.

El resumen del inventario correspondiente a los servidores virtuales se presenta en la Tabla 2.5:

Tabla 2.5 Inventario de los servidores candidatos a virtualizar

Servidor	Sistema Operativo	NIC	CPUs	Núcleos	Núcleos Totales	Tipo de CPU	Memoria física (MB)	Capacidad Disco (GB)
Servidor Nómima	MS Windows Server 2008 Enterprise	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon 3.06GHz	4096	80

Servidor Web	MS Windows Server 2008 Enterprise	2xBroadcom Gigabit Ethernet	1	4	4	Intel Xeon 3.06GHz	4096	80
Servidor Base de datos	Red Hat Enterprise Linux 5.4	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon E5405 2.00GHz	4096	80
Servidor Archivos	SUSE Linux Enterprise Server 10	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon E5405 2.00GHz	1024	60
Servidor VPN	Debian GNU/Linux 5.0	2xBroadcom Gigabit Ethernet	1	4	4	Intel Xeon E5405 2.00GHz	1024	40
Servidor Sistema de negocio 1	Red Hat Enterprise Linux 5.3	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon 3.00GHz	4096	80
Servidor Sistema de negocio 2	MS Windows Server 2008 Enterprise	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon 3.00GHz	4096	80
Servidor Intranet	Red Hat Enterprise Linux 5.3	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon E5405 2.00GHz	4048	40
Servidor Propietario 1	MS Windows Server 2008 R2 Standard	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon E5405 2.00GHz	4096	80
Servidor Propietario 2	MS Windows Server 2008 R2 Standard	Broadcom Gigabit Ethernet	1	4	4	Intel Xeon E5405 2.00GHz	4096	80
<b>Total</b>			<b>10</b>	<b>40</b>	<b>40</b>		<b>34768</b>	<b>700</b>

### 2.12.2 Análisis

Ya teniendo el inventario de los servidores candidatos a virtualizar, el cliente realizó un estudio de rendimiento, utilizando su herramienta de monitoreo, para obtener información adicional de los recursos de cómputo que ocupan las aplicaciones en los servidores candidatos. Estos datos son porcentaje de utilización de CPU, de memoria, de espacio de almacenamiento, y tráfico en la interfaz de red.

Los datos considerados son el promedio de la carga de trabajo de dos semanas convencionales, incluyendo los días operacionales de mayor trabajo, por lo que se presumen como válidos para definir las características de hardware necesarias para construir el ambiente virtual.

Además se toman las siguientes consideraciones:

- Capacidad suficiente ante un incremento en el número de servidores virtuales.
- Capacidad suficiente ante los recursos de cómputo utilizados eventos de mayor carga de trabajo (como fechas de cierre de operaciones, etc.).
- Capacidad de mantener en operación todas los servidores virtuales en un solo nodo de virtualización (para tener un mecanismo de alta disponibilidad)

Como el reporte del cliente ya tiene contemplado el uso de recursos de cómputo adicionales en eventos de mayor carga de trabajo, solo resta considerar los recursos adicionales para escalar la plataforma de virtualización, este porcentaje se determinó revisando el crecimiento histórico de la demanda de recursos, de acuerdo con el cliente y sus datos estadísticos ese incremento es de cuarenta por ciento desde la última renovación tecnológica; un porcentaje cerca del 50% como mínimo se considera adecuado, esto aplica para los recursos de memoria y espacio de almacenamiento, puesto que los recursos del CPU y capacidad de tráfico en la interfaz de red de un servidor se pueden usar con mayor eficiencia.

Además, se tiene el requerimiento de poder administrar fácilmente la plataforma de virtualización para lograr realizar respaldos eficientes y tener algún método para incrementar la disponibilidad de la aplicación. Dado este requerimiento, se deben considerar al menos dos servidores trabajando como nodos de virtualización, que estén en un ambiente clusterizado de tal forma que en caso de una falla de hardware de un nodo, el otro tenga la capacidad de mantener los servidores virtuales en operación. Sumando los porcentajes de crecimiento, carga de trabajo extra, operación de un solo nodo de virtualización tenemos los siguientes resultados, presentados en la tabla:

Se presenta el reporte resultado de las operaciones anteriores en la siguiente Tabla 2.6:

Tabla 2.6 Demanda de recursos de cómputo

Servidor	Núcleos Totales	Utilización de CPU (%)	Utilización de memoria (MB)	Utilización de disco (GB)	Trafico de red (MB/s)
Servidor Nómina	4	31.69	3528.44	96.92	228.77
Servidor Web	4	28.38	2743.80	48.39	1059.72
Servidor Base de datos	4	39.84	3618.58	87.06	651.27
Servidor Archivos	4	23.66	789.11	71.81	359.29
Servidor VPN	4	22.15	611.93	37.32	605.28
Servidor Sistema de negocio 1	4	34.69	3838.91	115.41	418.29
Servidor Sistema de negocio 2	4	37.91	3872.70	36.39	546.71
Servidor Intranet	4	34.04	3643.41	41.61	443.76
Servidor Propietario 1	4	23.85	2221.05	36.39	307.02
Servidor Propietario 2	4	24.42	2754.39	70.40	497.39
<b>Total</b>	<b>40</b>	<b>30.06</b>	<b>27622.32</b>	<b>641.70</b>	<b>5117.50</b>

Para obtener valores reales (los que pueden ser configurados) se redondearon las cifras, buscando no alterar demasiado el valor original. En el caso del espacio en disco requerido se redondeó la cifra, utilizando un factor de crecimiento del 55% en promedio (en lugar del 50%). Dado que el tráfico de datos no demanda más ancho de banda, todos los servidores virtuales necesitan una sola interfaz de red, excepto dos, el Servidor Web y el Servidor VPN, que tienen dos interfaces por razones operativas. Después de los ajustes resulta la Tabla 2.7:

Tabla 2.7 Demanda de recursos de cómputo

Servidor	Núcleos Totales requeridos	Memoria requerida (GB)	Espacio de disco requerido (GB)	Interfaces de red requeridas
Servidor Nómina	2	4	100	1
Servidor Web	2	3	50	2
Servidor Base de datos	2	4	90	1
Servidor Archivos	1	1	75	1
Servidor VPN	1	1	40	2
Servidor Sistema de negocio 1	2	4	120	1
Servidor Sistema de negocio 2	2	4	40	1
Servidor Intranet	2	4	45	1
Servidor Propietario 1	1	3	40	1
Servidor Propietario 2	1	3	75	1
<b>Total</b>	<b>16</b>	<b>31</b>	<b>675</b>	

### 2.12.3 Elección del hardware a utilizar

En esta etapa se determinó qué tipo de servidores y dispositivos adecuados para lograr un óptimo desempeño de los servidores virtuales.

Otro modificador importante es que para el almacenamiento de los discos duros virtuales, el cliente ya tiene un dispositivo funcional, por lo que este recurso no se tomó en cuenta para dimensionar los servidores nodos de virtualización. Tomando en cuenta los recursos de cómputo necesarios los servidores a utilizar deben cumplir con las siguientes características (Tabla 2.8):

Tabla 2.8 Características de los servidores que serán nodos de virtualización

Recurso de cómputo	Valor
Velocidad de CPU	2 GHz
Numero de CPUs	2
Núcleos por CPU	4
Velocidad de interfaz de red	4 Gbps
Numero de interfaces de red	3
Memoria física	32 GB

La plataforma de virtualización Red Hat Enterprise Linux necesita de cuatro componentes básicos:

- Red Hat Enterprise Virtualization Hypervisor (RHEV-H)
- Red Hat Enterprise Virtualization Manager (RHEV-M)
- Almacenamiento para las imágenes de los discos duros virtuales
- Almacenamiento para las imágenes de instalación

Así mismo, cada componente tiene sus propios requerimientos:

#### *Requerimientos de Red Hat Enterprise Virtualization Hypervisor (RHEV-H)*

- Un procesador con extensiones de virtualización de hardware si el fabricante es AMD debe contar con tecnología AMD-V si es Intel con tecnología Intel VT.
- La plataforma del procesador debe ser de 64 bits.
- Al menos una interfaz de red con un ancho de banda mínimo de 1 Gbps.
- 512 MB de memoria física RAM reservados.
- Capacidad de almacenamiento interno de mínimo de 1 GB más espacio adicional para memoria de intercambio.

*Límites de hardware para Red Hat Enterprise Virtualization Hypervisor (RHEV-H)*

- Máximo 64 CPUs físicos.
- Máximo 1 TB de memoria física RAM.
- Máximo 16 CPUs virtuales por máquina virtual.
- Máximo 256 GB de memoria virtual por máquina virtual de plataforma 64 bits.
- Máximo 4 GB de memoria virtual por máquina virtual de plataforma 32 bits.
- Máximo 8 dispositivos de almacenamiento virtuales por máquina virtual.
- Máximo 8 interfaces de red virtuales por máquina virtual.
- Máximo 32 dispositivos PCI virtuales por máquina virtual.
- Todos los nodos de virtualización de un mismo clúster deben tener el mismo tipo de CPU.

*Requerimientos de Red Hat Enterprise Virtualization Manager (RHEV-M)*

- Memoria física RAM mínima de 1 GB.
- Capacidad de almacenamiento libre mínima de 20 GB.
- Al menos una interfaz de red con un ancho de banda mínimo de 1 Gbps.
- Sistema operativo Microsoft Windows Server 2008 (R2)
- Paquete de software Microsoft .NET Framework 3.5.1.
- Paquete de software Internet Information Services (IIS).

*Requerimientos Almacenamiento para las imágenes de los discos duros virtuales*

- Capacidad de almacenamiento suficiente para guardar todas las imágenes de las máquinas virtuales (discos duros virtuales).
- Conexión al nodo de virtualización mediante el protocolo NFS, iSCSI o canal de fibra.
- Se debe configurar el dispositivo de almacenamiento para que el espacio a compartir sea visible desde los nodos de virtualización, este espacio debe ser suficiente para almacenar todos los discos virtuales.

*Requerimientos Almacenamiento para las imágenes de instalación*

- Capacidad de almacenamiento suficiente para guardar todas las imágenes ISO de instalación.
- Conexión al nodo de virtualización mediante el protocolo NFS.
- Se debe configurar el dispositivo de almacenamiento para que el espacio a compartir sea visible desde los nodos de virtualización, este espacio debe ser suficiente para almacenar las imágenes ISO de instalación de los sistemas operativos.

Con el conocimiento de todos los requerimientos de hardware el cliente decidió que los servidores que servirán como nodos de virtualización serian nuevos y los otros elementos se instalarían en servidores y dispositivos existentes, la configuración final es la siguiente (Figura 2.23):

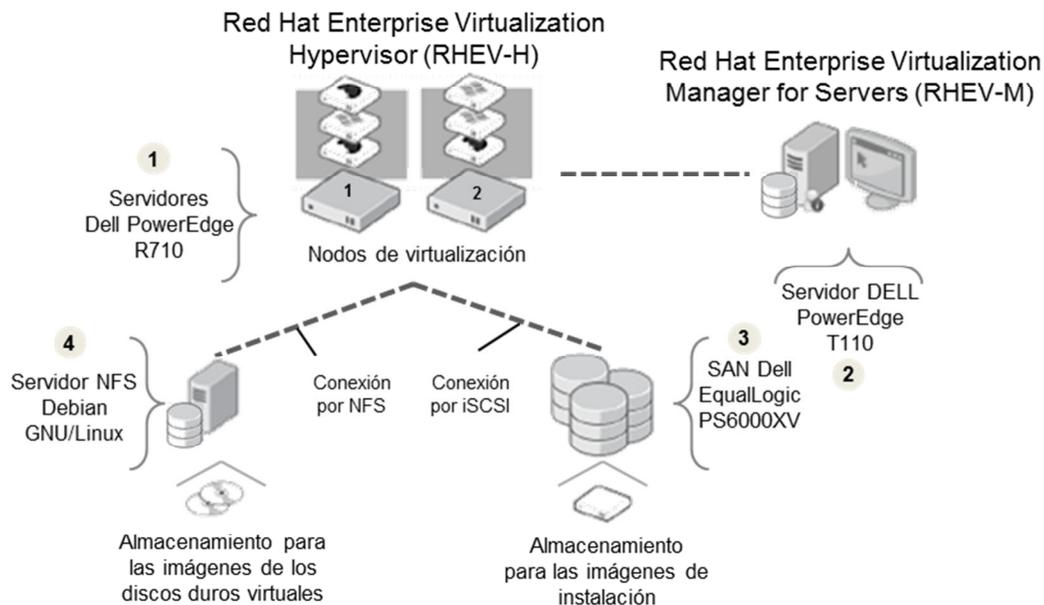


Figura 2.23 Diagrama conceptual de los elementos que integran la plataforma de virtualización

A continuación se describe cada elemento de acuerdo con la asignación del cliente, se hace mención especial de los servidores nuevos donde se instaló RHEV-H.

#### 1. Red Hat Enterprise Virtualization Hypervisor (RHEV-H)

El software de VMM se instaló en dos servidores Dell PowerEdge R710. Estos servidores tienen los recursos de cómputo suficientes para la eficiente virtualización de los servidores consolidados, como estos servidores son nuevos al cliente se le presentó una propuesta de servidor, que combinaba bien con su infraestructura existente y con sus políticas de adquisición por lo que fue aceptada.

Las características de estos servidores se presentan en la Tabla 2.9:

Tabla 2.9 Características de los nodos de virtualización adquiridos

Característica	Valor
Tipo de CPU	Intel Xeon E5640
Velocidad de CPU	2.66 GHz
Numero de CPUs	2
Núcleos por CPU	4
Memoria física	32 GB
Disco duro interno	146 GB 15K RPM SATA
Interfaz de red	3x <i>HBA</i> de canal de fibra Qlogic 4 Gbps
Administración remota	iDRAC6

## 2. Red Hat Enterprise Virtualization Manager (RHEV-M)

Para instalar la consola de administración de Red Hat Enterprise for Servers, se utilizó un servidor existente que cumple con las características requeridas. No se describe a detalle este servidor puesto que los recursos de cómputo no son tan exigentes, se utilizó un servidor Dell PowerEdge T110.

## 3. Almacenamiento para las imágenes de instalación.

Para este componente también se utilizó un servidor existente en el cual se configuró el servicio de NFS y se depositaron las imágenes de instalación en formato ISO.

## 4. Almacenamiento para las imágenes de los discos duros virtuales

Para almacenar los discos duros virtuales el cliente ya cuenta con un dispositivo, un dispositivo SAN (Área de almacenamiento en red). El modelo es Dell EqualLogic PS6510E, a este dispositivo se conectan los nodos de virtualización mediante el protocolo iSCSI.

### 2.12.4 Identificación de servidores complicados de consolidar en un ambiente virtual

Del estudio realizado por el cliente acerca de los servidores candidatos a virtualizar se hace notar que ninguno tuvo conflicto alguno para poder implementarse bajo la plataforma Red Hat Virtualization Enterprise for Servers; las aplicaciones usadas son convencionales y no requieren de algún dispositivo de hardware especial que tenga que interactuar con los servidores virtuales.

## 2.13 DESARROLLO

Nota importante: Con el fin de no exhibir detalles acerca de la configuración del cliente se van a cambiar algunos datos sensibles como los nombres de los servidores, direcciones IP, etc. En las imágenes utilizadas para describir los pasos de la instalación se va a ocultar la misma información.

### 2.13.1 Instalación de Red Hat Enterprise Virtualization Manager (RHEV-M)

Para la instalación de RHEV-M se necesita de una instalación fresca de Microsoft Windows Server 2008 R2, no hay requerimientos específicos de la instalación, excepto que el idioma del sistema operativo debe ser inglés. Los pasos para la instalación de RHEV-M se describen a continuación:

#### *Configuración del servicio DNS (Servicio de nombres de dominio)*

En el caso de un ambiente donde la mayoría de los servicios están en una plataforma Microsoft esta configuración requiere que el servidor sea un Controlador de Dominio, puesto que en la mayoría de las organizaciones existe un elemento que realiza esta tarea y así fue en la implementación de esta solución solo se mencionan las modificaciones que fueron necesarias. RHEV-M debe tener un nombre de dominio completo (Full Qualified Domain Name) que pueda ser resuelto por los nodos de virtualización, por el servidor donde se instale RHEV-M y por los clientes de RHEV-M, estos son servidores fuera de la plataforma de virtualización que tienen acceso a la consola de administración RHEV-M. Adicionalmente se agregaron los mismos registros para resolver los nombres que se van asignar a los nodos de virtualización que a su vez son componentes RHEV-H.

En el controlador de dominio existente que también tiene el rol de servidor DNS se agregaron los registros siguientes (Tabla 2.10):

Tabla 2.10 Registros configurados en el servidor DNS

Tipo de registro	Nombre de dominio	Dirección IP
A (resuelve nombre de dominio por dirección IP) y PTR (resuelve dirección IP por nombre de dominio)	rhevmanager.aseguradora.com	10.10.1.100/24
A (resuelve nombre de dominio por dirección IP) y PTR (resuelve dirección IP por nombre de dominio)	rhev1.aseguradora.com	10.10.1.101/24
A (resuelve nombre de dominio por dirección IP) y PTR (resuelve dirección IP por nombre de dominio)	rhev2.aseguradora.com	10.10.1.102/24

---

*Configuración de la interfaz de red del servidor rhevmanager (RHEV-M)*

Ya que creados los registros necesarios en el servidor DNS, se le asignó la dirección IP al servidor RHEV-M de manera estática, de la siguiente forma:

1. Ir al panel de control (*Control Panel*)
2. En la ventana del panel de control hacer clic en *Network and Sharing Center* (Centro de redes y recursos compartidos)
3. En la ventana que aparece, ir a la sección *Tasks* (tarefas), y hacer clic en *Manage Network Connections* (Administrar conexiones de red)
4. En la ventana *Network Connections* (Conexiones de red), hacer clic derecho en la conexión a configurar y seleccionar *Properties* (Propiedades). Aquí se modificó la correspondiente a *Local Area Connection*.
5. Seleccionar *Internet Protocol Version 4* (TCP/IPv4) y hacer clic en *Properties* (propiedades). Aparecerá entonces el cuadro de diálogo de las propiedades.
6. Ir a la pestaña *General*, hacer clic en *Use the following IP address* (Usar la siguiente dirección IP). En el cuadro de texto *IP address* se escribió la dirección IP 10.10.1.100
7. En el cuadro de texto correspondiente a *Subnet mask* (Máscara de red) se escribió la máscara de red 255.255.255.0 es decir de 24 bits.
8. En el cuadro de *Default Gateway* (Puerta de enlace), se configuró la dirección de la puerta de enlace correspondiente a la subred local, 10.10.1.254.
9. En el cuadro de *Preferred DNS server* (Servidor DNS primario), se configuró la dirección IP correspondiente al servidor DNS donde se agregó el nombre de dominio de RHEV-M, que es 10.10.1.253.
10. Para guardar y hacer efectivas las configuraciones hacer clic en *OK* (Aceptar),

En la Tabla 2.11 se presenta de forma resumida los valores configurados.

Tabla 2.11 Configuración de la interfaz de red del servidor RHEV-M

<b>Tipo</b>	<b>Configuración</b>	<b>Valor</b>
Casilla de verificación	Tipo de direccionamiento	<i>Use the following IP address</i>
Cuadro de texto	Dirección IP	10 . 10 . 1 . 100
Cuadro de texto	Máscara de red	255 . 255 . 255 . 255 . 0
Cuadro de texto	Dirección IP puerta de enlace	10 . 10 . 1 . 254
Casilla de verificación	Tipo de asignación de DNS	<i>Use the following DNS server addresses</i>
Cuadro de texto	Dirección IP del servidor DNS	10 . 10 . 1 . 253

*Conexión de RHEV-M al servidor controlador de dominio*

Para integrar el servidor RHEV-M al dominio de la organización y poder autenticar a los usuarios mediante un servicio de Directorio activo se realizaron las siguientes configuraciones:

1. Hacer clic en el botón start (inicio)
2. Hacer clic derecho en *Computer* (Equipo) y seleccionar *Properties* (Propiedades)
3. En la ventana que aparece, en la sección *Computer name, domain and group settings* (Nombre del equipo, dominio y grupo de trabajo del equipo) hacer clic en *Change settings* (Cambiar configuración).
4. Se abrirá la ventana *System Properties* (propiedades del sistema), hacer clic en el botón *Change* (Cambiar).
5. En la ventana que aparece se configuraron los siguientes datos en las opciones correspondientes (Tabla 2.12):

Tabla 2.12 Configuración del nombre del equipo y del dominio

Tipo	Configuración	Valor
Cuadro de texto	Nombre del equipo	rhevmanager.aseguradora.com
Casilla de verificación	Miembro de...	<i>Domain</i>
Cuadro de texto	Nombre del dominio	aseguradora.com

6. Para configurar los datos se deben escribir las credenciales de un administrador de dominio.
7. Hacer clic en el botón *OK* (Aceptar).
8. Para guardar las configuraciones se debe reiniciar el sistema.

*Instalación de software adicional requerido*

RHEV-M utiliza el servicio web IIS (Internet Information Services) que proporciona Microsoft para publicar su interfaz de administración web. Este servicio se instala agregando el rol Web Server (Servidor web). RHEV-M también requiere del *framework* Microsoft .NET 3.5.1, este componente se instala cuando se agrega el rol Application Server (Servidor de aplicaciones). El *framework* Microsoft .NET requiere del rol de Web Server (Servidor web).

A continuación se describen los pasos para instalar el *framework* Microsoft .NET 3.5.1.

1. Desde el menú inicio ir a *Administrative Tools* (Herramientas Administrativas) y seleccionar *Server Manager* (Administrador del servidor).
2. En la ventana que aparece se enlistan las funcionalidades actuales que tiene el servidor. Si no se muestra la funcionalidad *.NET Framework 3.5.1* desde la interfaz anterior seleccione *Add Features* (Agregar funcionalidades) para listar las funcionalidades posibles.
3. Expandiendo la funcionalidad *.Net Framework 3.5.1* se muestran las opciones disponibles, las siguientes fueron seleccionadas: *.NET Framework 3.5.1* y *WCF Activation*.
4. Hacer clic en el botón *Next* (siguiente).
5. A continuación aparecerá un cuadro de diálogo donde se muestran los requerimientos para la instalación del *framework*, el rol de *Web Server* y el rol de *Windows Process Activation Service*.
6. Hacer clic en el botón *Add required roles services* (Agregar los roles requeridos) y hacer clic en *Install* (Instalar, Figura 2.24).

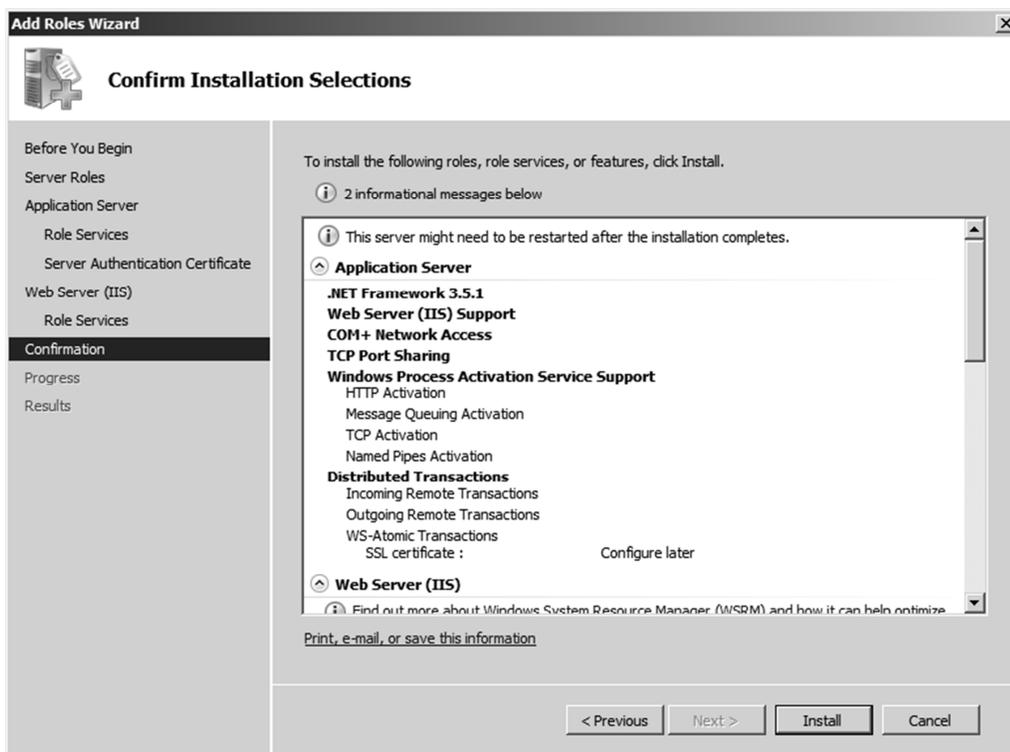


Figura 2.24 Ventana del Server Manager donde se agregan las funcionalidades requeridas

### *Instalación de la interfaz de administración RHEV-M*

La interfaz de administración RHEV-M se instala mediante un paquete ejecutable, que a su vez lanza un instalador gráfico donde se va describiendo paso a paso el proceso de instalación.

El paquete de instalación está disponible desde Red Hat Network (El portal de servicios para el usuario) cuando se adquiere la suscripción. La versión usada en esta implementación fue la 2.2.

Pasos para instalar la interfaz de administración RHEV-M:

1. Una vez descargado el paquete de instalación, se ejecutó el instalador haciendo doble clic en el mismo. Cuando el instalador termina los preparativos de la instalación presenta la ventana de bienvenida (Figura 2.25).



Figura 2.25 Ventana de bienvenida del instalador de Red Hat Enterprise Virtualization Manager

- 1.1. Se continuó con el proceso haciendo clic en *Next* (siguiente).

2. A continuación se pide que se lea la licencia y se acepten los términos establecidos (Figura 2.26). Se aceptaron los términos haciendo clic en el botón *Yes* (Sí).

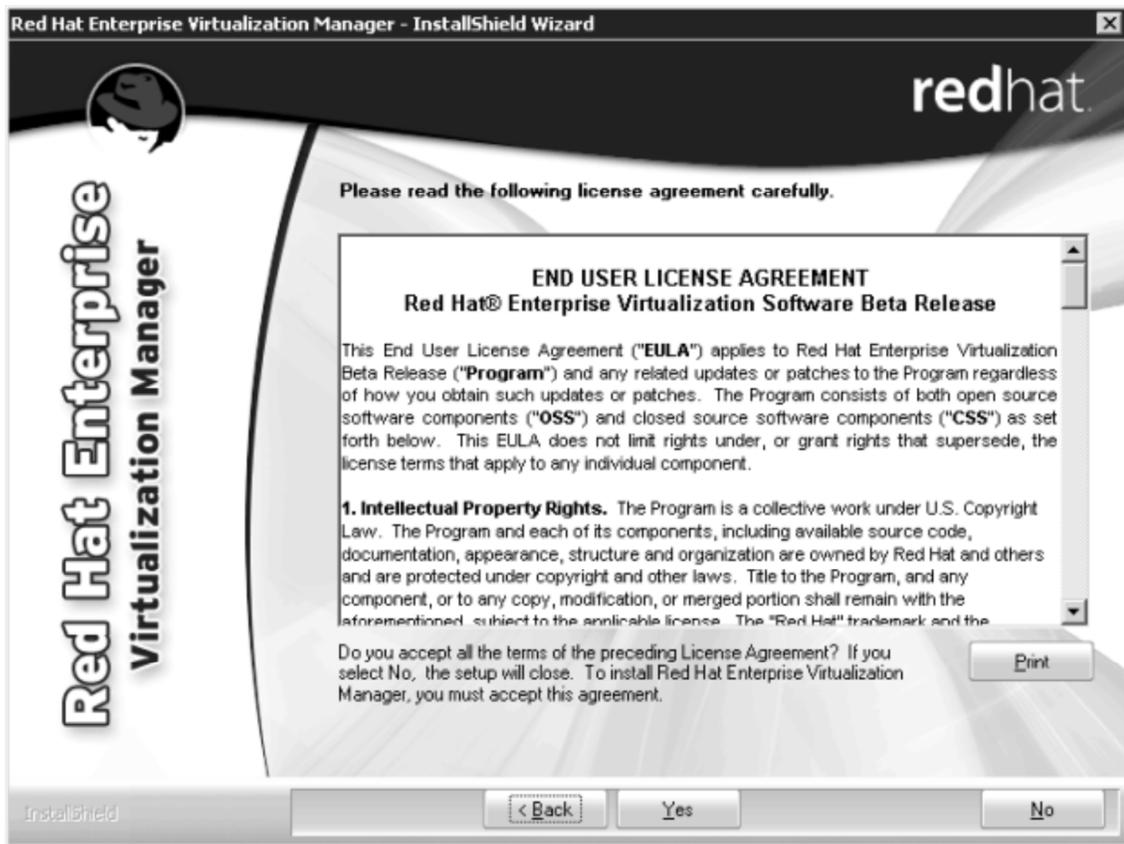


Figura 2.26 Presentación de los términos de la licencia

- 2.1. Si no se está de acuerdo con los términos de la licencia, se puede cancelar el proceso de instalación haciendo clic en No.

3. En este paso se seleccionan los módulos de RHEV-M (Figura 2.27). Una instalación típica incluye los siguientes módulos:
- RHEVM Web Admin: portal web de administración.
  - RHEVM Admin Portal: se utiliza para administrar el sistema RHEV y realizar las tareas asociadas.
  - RHEVM Database: *base de datos* que contiene información de la plataforma de virtualización en cuanto a los objetos creados, configuración y archivos de registros.
  - RHEVM Service: es el núcleo del interfaz de administración de la plataforma de virtualización.
  - RHEVM User Portal: portal web para los usuarios de escritorios.
  - RHEVM Scripting Library: Biblioteca de la aplicación PowerShell para RHEV y documentación.
  - RHEVM Net Console: servicio utilizado para la conexión con los nodos de virtualización.
- 3.1. Algunos módulos son obligatorios para la instalación, estos se presentan en color gris.
- 3.2. Se seleccionaron todos los módulos puesto que es una instalación típica, en el caso de la base de datos se puede usar una remota o una local, la recomendación es tener la base de datos local y que esta sea nueva, esta opción se seleccionó.

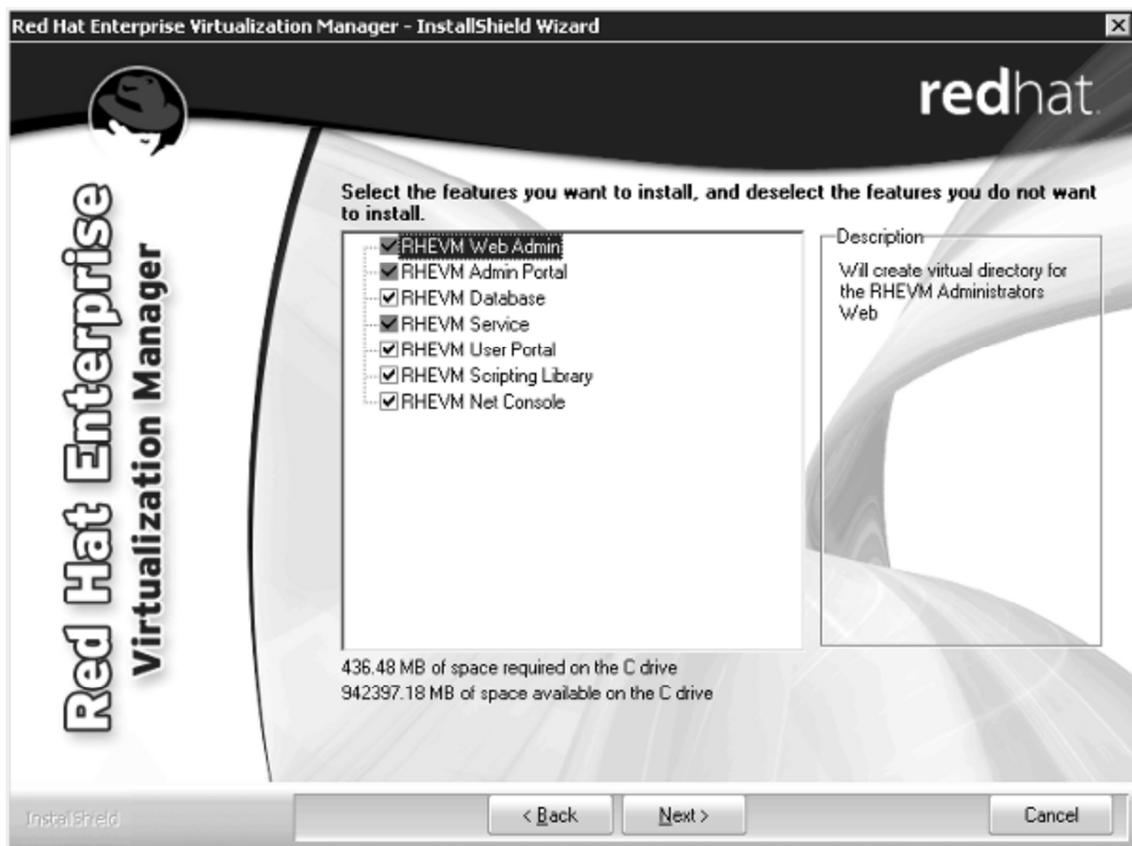


Figura 2.27 Módulos seleccionados para la instalación

- 3.3. Una vez que la selección esté completa, se continuó haciendo clic en Next.

4. Para la creación de la instancia de la base de datos (Figura 2.28), se seleccionó la opción: Instalación de SQL Server 2005 Express local



Figura 2.28 Configuración de la base de datos

- 4.1. Se configuró la contraseña del administrador de la base de datos, en SQLExpress.

5. A continuación se eligió la ubicación para la instalación (Figura 2.29), se dejó el valor default.

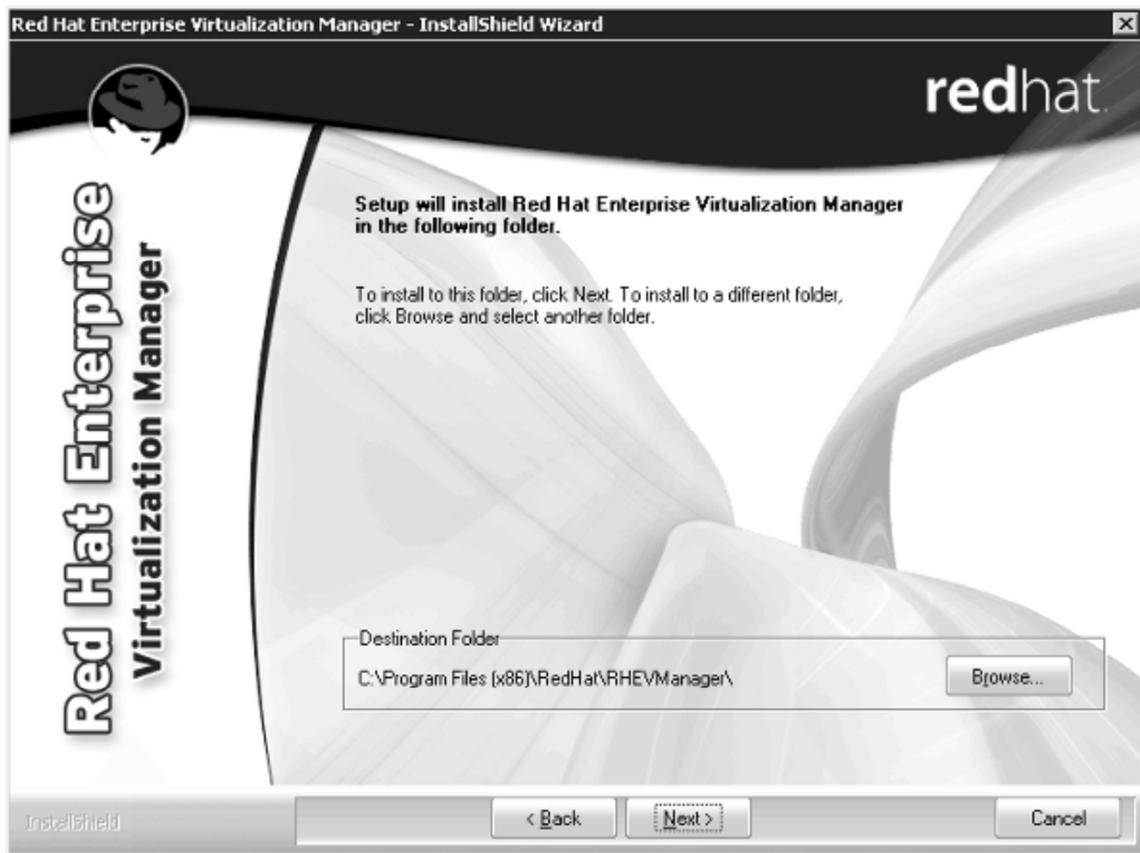


Figura 2.29 Configuración de la ruta de instalación

6. En el siguiente paso se configuró el sitio web para el acceso de los usuarios (Figura 2.30).
  - 6.1. Se eligió el sitio web default
  - 6.2. Se seleccionó la casilla de verificación Force SSL para cifrar las transacciones web de la interfaz de administración.



Figura 2.30 Configuración del sitio web

7. Se continuó haciendo clic en Next.

8. En este paso se establecen las credenciales del administrador de la plataforma de virtualización (Figura 2.31), como se conectó RHEV-M a un servidor controlador de dominio existente se seleccionó la autenticación por dominio y se configuró el dominio.
  - 8.1. Para esto se escribió el nombre del usuario de dominio creado para la administración y su contraseña configurada en el servidor controlador de dominio.

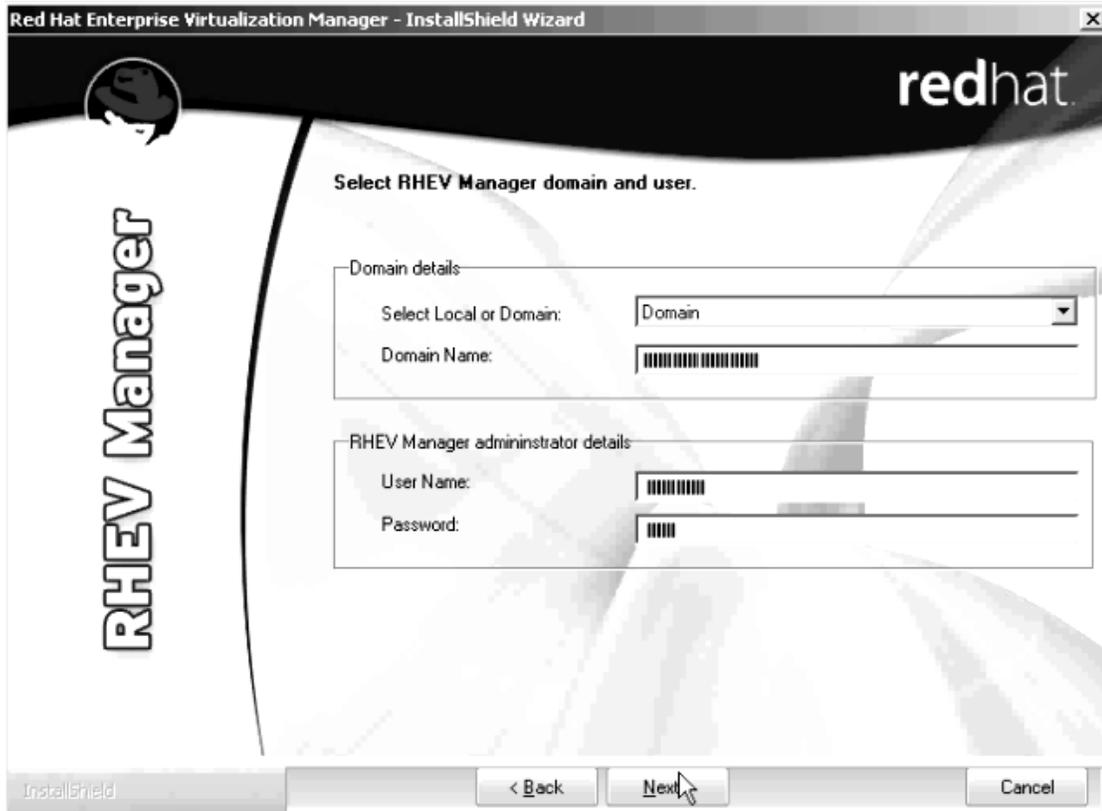


Figura 2.31 Configuración de la autenticación

9. Se continuo con el proceso haciendo clic en Next
10. En el siguiente paso se configuraron los parámetros para crear el certificado digital del portal de administración web (Figura 2.32).

- 10.1. Se escribió el nombre de la organización en el campo Organization Name.
- 10.2. Se escribió el nombre de dominio completo del servidor (*FQDN*) tal y como se configuró en el mismo equipo y en el servidor DNS, esto en el campo Fully qualified computer name.
- 10.3. Para validar si se está resolviendo bien el nombre de dominio se dejó en blanco la casilla de verificación Do not validate qualified computer name.
- 10.4. Se validó exitosamente la resolución del nombre de dominio.

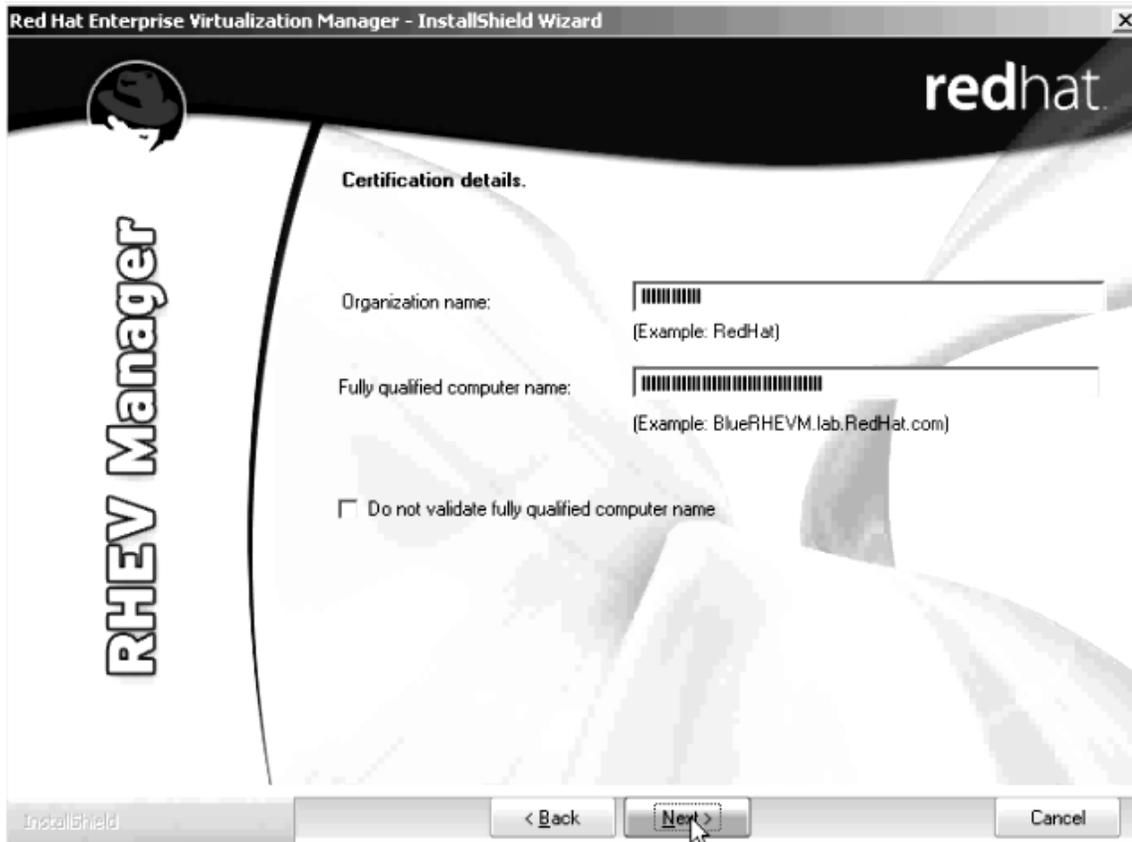


Figura 2.32 Configuración del certificado digital

11. En el siguiente paso se configuró el puerto utilizado para el servicio Net Console (Figura 2.33), se dejó el valor default que es 25285. Se validó con el cliente que este puerto no estuviera en

uso en la red local donde se implementó la plataforma de virtualización.

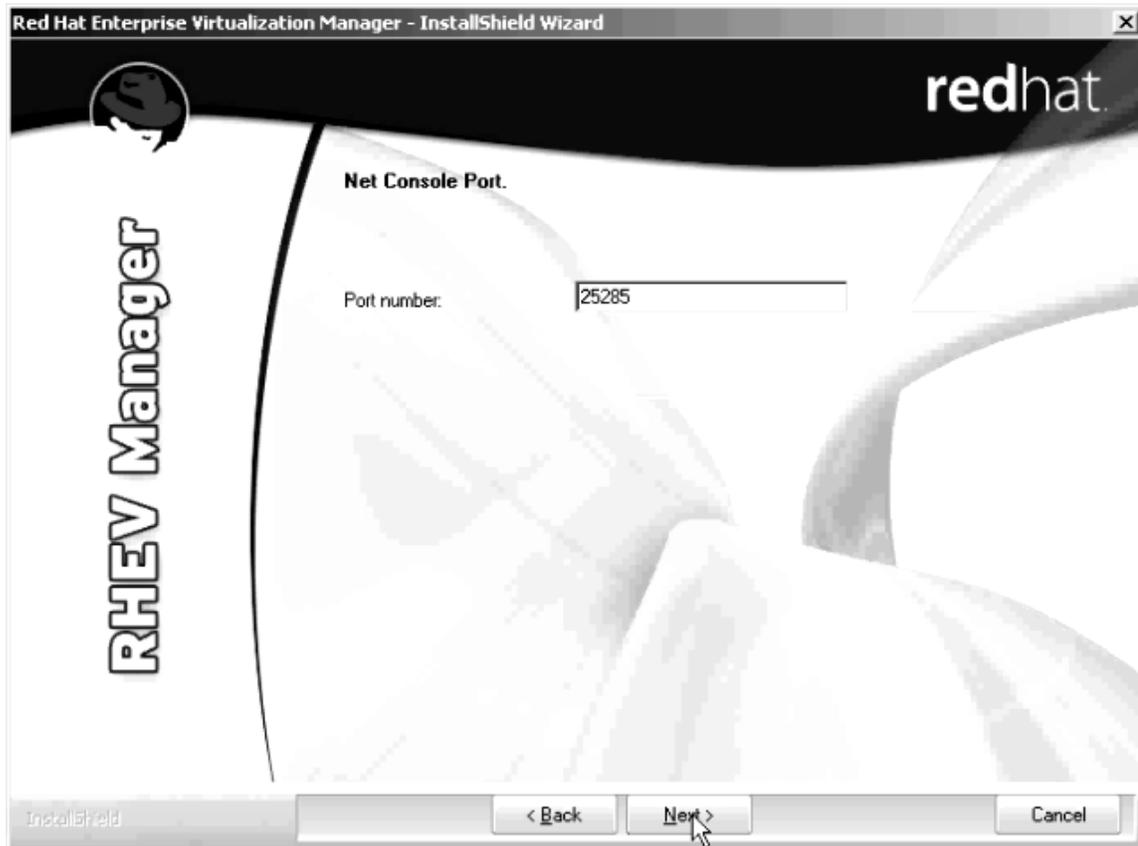


Figura 2.33 Configuración del puerto Net Console

12. A continuación se presenta un resumen con los datos configurados y se pide al usuario continuar para seguir con la instalación (Figura 2.34).

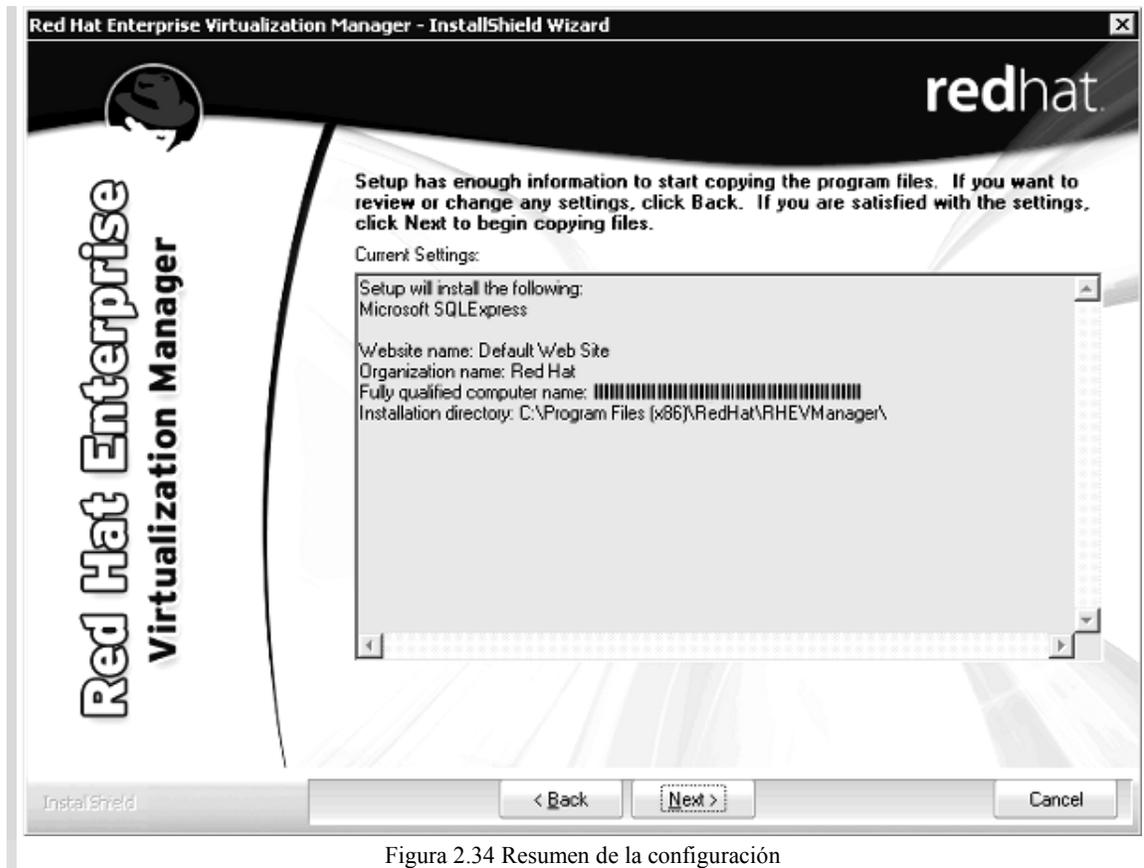


Figura 2.34 Resumen de la configuración

13. Se validaron los datos como correctos y el asistente de instalación continuó con la instalación.
14. Nota: Si hay cualquier aplicación que esté utilizando archivos que se requieren para la instalación, se le notificará para cerrarlos antes de proceder. Una vez hecho esto se puede continuar.
15. Cuando la instalación termina el instalador pide confirmación de la instalación.
16. Ahora la interfaz de administración de la plataforma de virtualización está lista para utilizarse.

### 2.13.2 Acceso a la interfaz de administración Red Hat Enterprise Virtualization Manager (RHEV-M)

Para acceder a la interfaz de administración RHEV-M, se ejecuta el acceso directo que existe en el menú de programas. Alternativamente se puede abrir un navegador web y escribir la *URL* `http://localhost/RHEVmanager` o `http://FQDN/RHEVmanager`.

Si se conecta a la interfaz de administración por primera vez, se pedirá que instale el certificado digital y se instalarán algunos componentes adicionales para visualizar la interfaz web (Figura 2.36).



Figura 2.35 Solicitud de instalación del certificado digital

Después se solicitara que escriba las credenciales de acceso tal cual se configuraron en la instalación (Figura 2.36), una vez procesadas se presentara la interfaz de administración.



Figura 2.36 Interfaz de administración RHEV-M

### 2.13.3 Instalación de Red Hat Enterprise Virtualization Hypervisor (RHEV-H)

El nodo de virtualización contiene el software para funcionar como monitor de máquina virtual (VMM). En la solución de Red Hat Enterprise Linux for Servers, este software se denomina RHEV-H y se distribuye mediante una imagen ISO instalable, al igual que el software RHEV-M se descarga desde el sitio de Red Hat Network teniendo activa la suscripción.

El software RHEV-H está basado en Red Hat Enterprise Linux (una distribución de Linux) y puede soportar reconocer el hardware que está certificado para RHEL, por esta razón la actualización del software RHEV-H tiene el mismo ciclo de vida que el sistema operativo RHEL y se beneficia de las mejoras de éste. La versión de RHEV-H instalada fue la 5.5-2.2, basada en RHEL 5.5.

Cuando se instala en el servidor que será nodo de virtualización se entiende que ese servidor será para uso exclusivo del sistema de virtualización y por lo tanto no se podrá ocupar como un sistema operativo normal.

La imagen ISO que se descarga se puede quemar en un disco compacto para la instalación o también se puede quemar en un dispositivo USB. El método utilizado para la

implementación fue el de instalar el software mediante un disco compacto, para lo cual se necesita que el servidor tenga un dispositivo óptico de lectura

Nota: La configuración de los dos nodos de virtualización es exactamente la misma haciendo las distinciones pertinentes en los parámetros únicos como las direcciones IP y los nombres de dominio.

### *Menú de configuración de RHEV-H*

Una vez que se inicia el sistema desde el disco compacto que contiene el software de RHEV-H, se presenta el siguiente menú (Figura 2.37):

```
Red Hat Enterprise Virtualization Hypervisor release 5.5-2.2

Hypervisor Configuration Menu

1) Configure storage partitions      6) Configure the host for RHEV
2) Configure authentication          7) View logs
3) Set the hostname                  8) Install locally and reboot
4) Networking setup                  9) Support Menu
5) Register Host to RHN
Choose an option to configure:
```

Figura 2.37 Menú de configuración de RHEV-H

- La opción *Configure storage partitions* (Configurar particiones de almacenamiento), prepara el dispositivo de almacenamiento interno para la instalación del software.
- La opción *Configure authentication* (Configurar autenticación), proporciona la posibilidad de configurar una contraseña para el usuario *root* (administrador local del sistema RHEV-H) para el acceso local o mediante una terminal remota por el protocolo SSH.
- La opción *Set the hostname* (Configurar nombre del servidor), configura el nombre del servidor.
- La opción *Networking setup* (Configuración de red), configura los parámetros de red incluyendo DHCP, IPv4, NTP y DNS.
- La opción *Register Host to RHN* (Registrar en RHN), registra el nodo de virtualización en el sistema de suscripciones Red Hat Network.
- La opción *Configure the host for RHEV* (Configurar el nodo para RHEV), configura la dirección IP del servidor RHEV-M para integrar el nodo de virtualización al centro de datos virtual.
- La opción *View logs* (Ver registros), visualiza los archivos de registros del proceso de instalación del sistema RHEV-H.
- La opción *Install locally and reboot* (Instalar localmente y reiniciar), instala el software de RHEV-H en el dispositivo de almacenamiento interno y reinicia el sistema.
- La opción *Support Menu* (Menú de soporte), muestra una terminal de comandos.

*Partición del disco*

La partición del disco se configura desde el menú *Configure storage partitions* (Configurar particiones de almacenamiento) y tiene las siguientes opciones (Figura 2.38):

```
Configure storage partitions
1) Configure
2) Review
3) Commit configuration
4) Return to the Hypervisor Configuration Menu
Choose an option:
```

Figura 2.38 Submenú de configuración particiones de almacenamiento

Para empezar el procedimiento se seleccionó la opción *Configure* (Configurar), esta opción presenta el o los dispositivos de almacenamiento interno del nodo de virtualización para elegir en cual se instalara el software RHEV-H. La información de los servidores utilizados se presenta a continuación (Figura 2.39).

```
/dev/mapper/SServerA_venh_076A0444 (sda) ( 149504 MB)
Disk Identifier: storage_serial_SServerA_venh_076A0444
1) /dev/mapper/SServerA_venh_076A0444 3) Manual selection
2) Abort
```

Figura 2.39 Selección del dispositivo de almacenamiento interno del nodo de virtualización

En esta implementación se eligió la primera opción que corresponde al disco duro del servidor. Después se debe configurar el espacio que utilizará cada partición, las particiones que requiere RHEV-H son: boot, swap, root, config, logging y data.

Por defecto se presenta una configuración de espacio predefinida la cual se puede utilizar en una implementación común.

Esta configuración se presenta en la Tabla 2.13:

Tabla 2.13 Tabla de tamaños por defecto de particiones de RHEV-H

Partición	Tamaño
root	512MB
boot	50MB
logging	2048MB
config	5MB
swap	5MB
data	254MB

Para optimizar la partición swap su tamaño se calcula en función de la capacidad de la memoria física, utilizando la siguiente fórmula:

$$\text{tamaño\_swap\_recomendado} + (\text{capacidad\_memoria\_física} * \text{overcommit}) = \text{tamaño\_particion\_swap}$$

Donde *overcommit* es un factor que representa el porcentaje de utilización de la memoria que hace el sistema operativo, en este caso el valor por defecto para los sistemas RHEL (Red Hat Enterprise Linux) es 0.5 y basados en la documentación oficial<sup>45</sup> se recomienda que para servidores con memoria física de 16GB a 64GB –nuestro caso– el mínimo de espacio reservado para la partición swap sea 8 GB (este es el valor tamaño\_swap\_recomendado). Por lo tanto el valor a utilizar para la partición swap es el siguiente:

$$8 + (32 * 0.5) = 24; 24GB$$

La partición *data* almacena los archivos de kvm los archivos de depuración de kernel y temporalmente almacena las imágenes ISO de instalación mientras se transfiere al medio de almacenamiento de imágenes de instalación.

El tamaño de los archivos de kvm depende de la memoria virtual asignada a las máquinas virtuales, para optimizar la partición *data* el tamaño mínimo recomendado es de 1.5 veces más que la memoria física del nodo de virtualización.

Entonces, para la instalación de los nodos de virtualización se asignaron 48GB a la partición *data*.

En resumen se usó la configuración de espacio para cada partición como se ve en la Figura 2.40, esta información se visualizó seleccionando la opción *review* (revisar) del menú anterior:

---

<sup>45</sup> Se ofrece esta información en: <https://access.redhat.com/kb/docs/DOC-15252>

```

The local disk will be repartitioned as follows:
=====
Physical Hard Disk: /dev/sda ( 149504 MB)
Disk Identifier: storage_serial_SServerA_venh_076A0444
Boot partition size: 50
Swap partition size: 24576 MB
Installation partition size: 256 * 2 MB
Configuration partition size: 5 MB
Logging partition size: 2048 MB
Data partition size: 49152 MB

```

Figura 2.40 Configuración del tamaño de cada partición de RHEV-H

Para finalizar con esta configuración y guardar los cambios hechos se seleccionó la opción *Commit configuration* (Guardar configuración), entonces se presentó el siguiente mensaje (Figura 2.41), donde advierte que se tiene que eliminar todo el contenido actual para dar formato al disco duro y crear las particiones necesarias.

```

!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!
!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!
!!WARNING!!                                     !!WARNING!!
!!WARNING!!                                     !!WARNING!!
!!WARNING!!      If you proceed, all data on your selected storage !!WARNING!!
!!WARNING!!      device will be destroyed and your hard disk      !!WARNING!!
!!WARNING!!      will be irreversibly reconfigured.                !!WARNING!!
!!WARNING!!                                     !!WARNING!!
!!WARNING!!                                     !!WARNING!!
!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!
!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!WARNING!!
Do you wish to proceed([Y]es or [N]o)?

```

Figura 2.41 Advertencia al realizar el formato del disco duro del nodo de virtualización

Para continuar se eligió la opción Yes (Sí).

#### *Asignación de una contraseña de administración*

Para tener acceso directo al sistema RHEV-H, se debe configurar una contraseña local para el administrador (root), esta contraseña se configura en la opción *Configure Authentication* (Configurar autenticación) del menú principal (Figura 2.42).

```
SSH remote access is currently disabled

1) Set administrator password
2) Toggle SSH password authentication
3) Return to the Hypervisor Configuration Menu
Choose an option to configure:
```

Figura 2.42 Submenú Configure authentication

Para configurar la contraseña se eligió la opción *Set administrator password* (Configurar la contraseña de del administrador) y se escribió la contraseña para este nodo de virtualización, además en el mismo menú se puede habilitar el acceso remoto a este nodo de virtualización por SSH, para hacerlo se habilito la opción *Toggle SSH password authentication* (Habilitar contraseña de autenticación SSH). Estas configuraciones nos permiten entrar al sistema RHEV-H directamente, para analizar archivos de registro (logs), verificar la conexión al dispositivo de almacenamiento central (donde se guardan las imágenes de los discos duros virtuales), etc.

#### *Asignación del nombre del servidor*

Para conectar exitosamente el componente RHEV-M con los nodos de virtualización (componentes RHEV-H) los nombres de dominio deben de ser resueltos por un servidor DNS en común, en la opción *Set the hostname* (Configurar nombre del servidor) del menú principal se configura el nombre asignado a cada nodo de virtualización, este nombre es el nombre completo (FQDN).

En el caso del primer nodo de virtualización instalado se configuró el nombre *rhev1.aseguradora.com* y en el caso del segundo nodo de virtualización instalado se configuró el nombre *rhev2.aseguradora.com*. Un mensaje afirmativo indicó que la configuración fue exitosa.

Nota: Este nombre de dominio se puede cambiar desde la misma opción del menú principal si es necesario.

#### *Configuración de la red*

En la opción *Networking setup* (Configuración de red) del menú principal se configuran todos los parámetros de la interfaz de red. Si el servidor nodo de virtualización tiene más de una interfaz de red se debe elegir una para la configuración.

Nota: Una vez que el sistema RHEV-M esté conectado con la interfaz de administración RHEV-M, se podrán configurar las interfaces de red restantes si así se desea.

Los parámetros de red configurados se presentan en la Tabla 2.14:

Tabla 2.14 Tabla de parámetros de red configurados

Parámetro de red	Nodo de virtualización rhev1.aseguradora.com	Nodo de virtualización rhev2.aseguradora.com
Dirección IP	10.10.1.101	10.10.1.102
Máscara de red	255.255.255.0	255.255.255.0
Dirección IP de la puerta de enlace	10.10.1.252	10.10.1.252
Dirección IP del servidor DNS	10.10.1.253	10.10.1.253
Dirección IP del servidor NTP	N/A	N/A

Al terminar de escribir los parámetros se guardó la configuración. Si la configuración se aplicó correctamente se ve la siguiente pantalla (Figura 2.43).

```
Configuring network
Network configured successfully
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]
Bringing up interface breth0:
Determining IP information for breth0... done. [ OK ]
```

Figura 2.43 Pantalla de configuración exitosa de los parámetros de red

### Registro en RHN

Para registrar cada sistema RHEV-H en Red Hat Network haciendo válida la suscripción se siguieron los siguientes pasos:

1. En el menú principal se eligió la opción *Register to RHN* (Registrar a RHN).
  - 1.1. En el campo *Enter RHN account username* se escribió el nombre de usuario vinculado con la suscripción.
  - 1.2. En el campo *Enter your RHN account password* se escribió la contraseña proporcionada por el cliente.
  - 1.3. El campo *Enter profile name for this system (optional)* se dejó en blanco al igual que el campo *Enter HTTP proxy*. El servidor no pasa a través de un proxy para tener acceso a la red externa.

### *Configuración del componente RHEV-H para la conexión con el sistema RHEV-M*

En este paso se configura la conexión con el sistema RHEV-M, para que se pueda llevar a cabo toda la administración desde esta interfaz de administración central.

Nota: Para que esta configuración sea exitosa se deben configurar los registros necesarios en el servidor DNS como se hizo en el punto 3.13.1.1.

Para esta configuración se eligió la opción *Configure the host for RHEV* (Configurar el nodo para RHEV) del menú principal

En el submenú que aparece para el campo Enter the RHEV Manager's hostname or IP address (Escribir el nombre del servidor RHEV-M o su dirección IP) se escribió la dirección IP de RHEV-M, 10.10.1.100.

Un mensaje afirmativo indicó que la configuración fue exitosa.

Adicionalmente se configuró el acceso tipo NetConsole, donde se especifican los mismos parámetros anteriores puesto que este componente está instalado en el mismo servidor.

### *Instalación*

Una vez que todos los pasos anteriores se completaron, se instaló el software RHEV-H en el servidor de forma definitiva, para esto se seleccionó la opción *Install locally and reboot* (Instalar localmente y reiniciar) del menú principal

Al reiniciar, el sistema RHEV-H se cargará de forma automática y el nodo de virtualización será visible desde la interfaz de administración RHEV-M.

#### **2.13.4 Aprobación del nodo de virtualización (host)**

Por defecto el sistema RHEV-M crea algunos elementos como un centro de datos virtual (Data Center) llamado *Default* y un clúster también llamado *Default*. Tanto el centro de datos virtual *Default* como el clúster *Default* tienen propiedades que se modificaron para configurar todos los demás elementos, almacenamiento, nodos, máquinas virtuales, etc.



### 2.13.6 Configuración del dispositivo de almacenamiento de los discos duros virtuales

Este es un dispositivo SAN marca Dell modelo EqualLogic PS6510E que soporta el protocolo iSCSI, en este dispositivo el cliente configuró la compartición del espacio requerido para almacenar los discos duros virtuales. Los datos que proporcionó y que son necesarios para la configuración desde el sistema RHEV-M son: la dirección IP del dispositivo SAN, el identificador del espacio compartido.

### 2.13.7 Configuración del almacenamiento de las imágenes de instalación en RHEV-M

Para configurar el almacenamiento de las imágenes de instalación, donde se depositan las imágenes ISO de instalación de los diferentes sistemas operativos<sup>46</sup>, se siguieron las instrucciones:

1. Entrar a la interfaz de administración RHEV-M.
2. En la pestaña Data Centers (Centros de datos) se seleccionó el centro de datos Default (el creado por defecto) y se hizo clic en el botón Guide Me (Guiarme) ubicado en la parte superior. Este botón lanza un asistente de configuración para los elementos del centro de datos virtual que aún no han sido configurados, como se puede ver en la Figura 2.45.

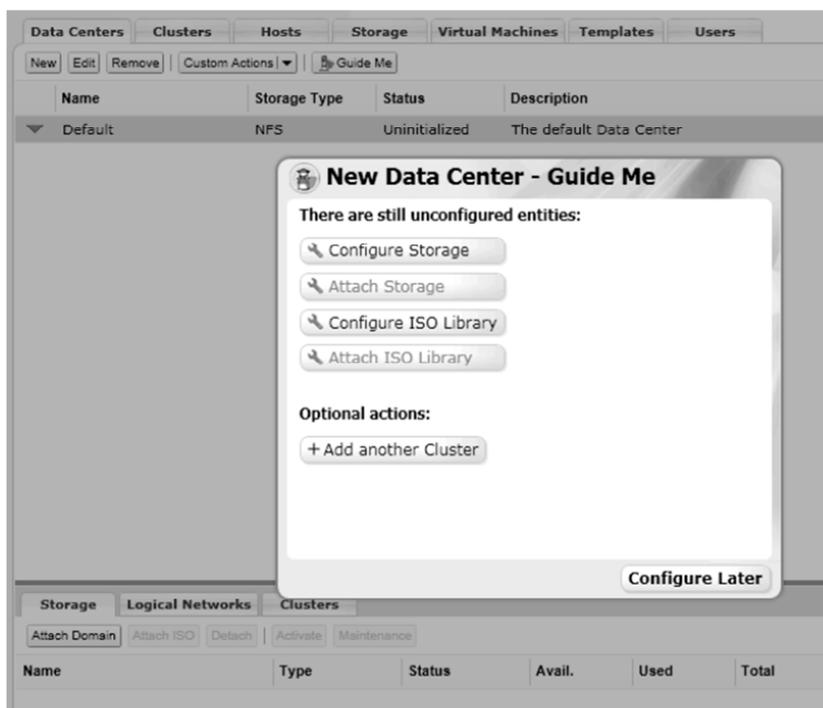


Figura 2.45 Asistente de configuración

<sup>46</sup> Red Hat Inc., Red Hat Enterprise Virtualization for Servers 2.2: Administration Guide. 2010, p. 46

3. Se hizo clic en el botón Configure ISO Library (Configurar biblioteca ISO).
4. En la siguiente ventana (Figura 2.46) se configuró el almacenamiento para las imágenes ISO, escribiendo los datos proporcionados por el cliente.
  - 4.1. En el campo Name (Nombre) se escribió un identificador para el dominio de almacenamiento.
  - 4.2. En la opción Domain function (Funcionalidad del dominio) se seleccionó ISO, correspondiente al almacenamiento de imágenes ISO.
  - 4.3. En la opción Storage type (Tipo de almacenamiento) se eligió la opción NFS, puesto que actualmente es el único protocolo soportado para configurar el dominio de almacenamiento para imágenes ISO.
  - 4.4. En la opción Use Host (Usar Host) se seleccionó el primer nodo, este nodo servirá para almacenar temporalmente las imágenes ISO que se suben a través de la interfaz de administración RHEV-M. Es importante mencionar que el servidor que contiene al sistema RHEV-M no tiene comunicación directa con los dispositivos de almacenamiento, sino que lo hace a través de los nodos de virtualización.
  - 4.5. En la campo Export path (Ruta de exportación) se escribió la ruta para montar el espacio compartido por el servidor NFS que se compone de la dirección IP del servidor y la ruta absoluta del directorio compartido. Ej. 10.10.1.252:/export/

**New Domain**

Name:

Domain function:  Data     ISO     Export

Storage type:  NFS     iSCSI     FCP

Use host:

Export path:

OK Cancel

Figura 2.46 Ventana de configuración de un dominio de almacenamiento

5. Para finalizar la configuración se hizo clic en OK (Aceptar). Esta acción regresa al menú principal del asistente de configuración.
6. A continuación se añadió el dominio de almacenamiento –para imágenes ISO– recién creado, al centro de datos haciendo clic en el botón Attach ISO Library (Añadir biblioteca ISO) del asistente de configuración. Esto activa este dominio de almacenamiento para que se pueda usar.

### 2.13.8 Almacenamiento de las imágenes de instalación ISO

Una vez realizada la configuración del almacenamiento para las imágenes de instalación ISO ya podemos llenar la biblioteca ISO, para esto se ocupa la aplicación *RHEV ISO uploader*<sup>47</sup>. Se hizo siguiendo las instrucciones:

1. Primero se hizo una copia en formato ISO del disco compacto de instalación y se almacenó temporalmente en el servidor RHEV-M.
2. Se ejecutó esta aplicación está en el servidor donde se instaló el software del sistema RHEV-M, en la ubicación: Start (Inicio) => All programs (Todos los programas) => Red Hat => RHEV Manager => ISO Uploader (Figura 2.47). El único usuario que puede usar esta herramienta es el administrador del sistema REHV-M.

---

<sup>47</sup> Red Hat Inc., Red Hat Enterprise Virtualization for Servers 2.2: Administration Guide. 2010, p. 67



### 2.13.9 Configuración del almacenamiento de los discos duros virtuales desde RHEV-M

Esta configuración requiere que previamente se haya configurado el dispositivo de almacenamiento central, como se hizo en el paso 3.13.6. Para la configuración desde la interfaz de administración RHEV-M se siguieron los siguientes pasos:

1. Entrar a la interfaz de administración RHEV-M.
2. En la pestaña Data Centers (Centros de datos) se seleccionó el centro de datos Default (el creado por defecto) y se hizo clic en el botón Guide Me (Guiarme) ubicado en la parte superior. Este botón lanza un asistente de configuración para los elementos del centro de datos virtual que aún no han sido configurados, como se puede ver en la Figura 2.52.
3. Para configurar el almacenamiento de los discos duros virtuales se dio clic en el botón Configure Storage (Configurar almacenamiento). Entonces, apareció de nuevo la ventana para la creación del dominio de almacenamiento como se ve en la Figura 2.53.
4. En esta ventana (Figura 2.48) se configuró el almacenamiento para los discos duros virtuales, escribiendo los datos proporcionados por el cliente.
  - 4.1. En el campo Name (Nombre) se escribió un identificador para el dominio de almacenamiento.
  - 4.2. En la opción Domain function (Funcionalidad del dominio) se seleccionó Data (Datos), correspondiente al almacenamiento de los discos duros virtuales.
  - 4.3. En la opción Storage type (Tipo de almacenamiento) se eligió la opción iSCSI, este es el protocolo usado para la conexión con el dispositivo SAN. Así como la opción Build New Domain, para crear un nuevo dominio de datos.
  - 4.4. En la opción Use Host (Usar Host) se seleccionó el segundo nodo, esta opción señala simplemente cómo se tendrá acceso al dispositivo de almacenamiento, puesto que no hay un acceso directo desde el servidor RHEV-M.
  - 4.5. A diferencia de la conexión por NFS, las opciones iSCSI y FCP (protocolo de canal de fibra) permiten la exploración de los recursos compartidos. Cuando termine el proceso de exploración se visualizarán los recursos de almacenamientos compartidos para el nodo de virtualización seleccionado.

**New Domain**

Name:

Domain function:  Data  ISO  Export

Storage type:  NFS  iSCSI  FCP

Build New Domain  Use Preconfigured Volume Group

Use host:

**Discovered LUNs**

LUN ID	UUID	Multipathing	Dev. Size
--------	------	--------------	-----------

**Selected LUNs**

LUN ID	UUID	Multipathing	Dev. Size
--------	------	--------------	-----------

Figura 2.48 Ventana de configuración de un dominio de almacenamiento

- 4.6. Se seleccionó el recurso de almacenamiento designado para almacenar las imágenes de los discos duros virtuales y que además es el único listado, haciendo clic en el botón Add (agregar).
5. Para finalizar la configuración se hizo clic en OK (Aceptar). Esta acción regresa al menú principal del asistente de configuración.
6. A continuación se añadió el dominio de almacenamiento –para discos duros virtuales– recién creado, al centro de datos haciendo clic en el botón Attach Storage (Añadir Almacenamiento) del asistente de configuración. Esto activa este dominio de almacenamiento para que se pueda usar.

### 2.13.10 Configuración de la administración de energía en los nodos de virtualización

Para poder implementar tecnologías como la alta disponibilidad es necesario que se realice una configuración adicional en los nodos de virtualización.

La administración de energía de un nodo se controla mediante la interfaz de administración remota del servidor, esta interfaz es independiente del sistema operativo. Los distintos fabricantes de hardware cuentan con su propia interfaz de administración remota, en esta implementación se cuenta con servidores marca Dell, con una interfaz de administración remota iDRAC6. La interfaz iDRAC6 es manejada por un sistema de administración, ese sistema recibe todos los comandos de administración remota y ejecuta las acciones correspondientes, aparte de proporcionar mecanismos de monitoreo y de cambio del estado del servidor (encendido o libre). Además este sistema de administración remota valida las órdenes recibidas según el emisor, es decir, para controlar el estado del servidor y otras funciones se debe contar con un usuario aceptado.

Para la configuración de la administración de energía de los nodos de virtualización es necesario contar con un usuario válido para controlar el servidor remotamente a través de la interfaz iDRAC6, además de su contraseña. Esta información fue proporcionada por el cliente, para ambos servidores.

Esta configuración se realizó desde la interfaz de administración RHEV-M para cada nodo de virtualización<sup>48</sup>, de la siguiente forma:

1. En la pestaña Hosts (Nodos) se seleccionó el nodo y se dio clic en el botón Edit (Editar).
2. En la ventana Edit Host (Editar nodo, Figura 2.49) se habilitó la administración de energía haciendo clic en la casilla de verificación Enable Power Management.

---

<sup>48</sup> Red Hat Inc., Red Hat Enterprise Virtualization for Servers 2.2: Administration Guide. 2010, p. 103

The image shows a 'Edit Host' dialog box with the following fields and controls:

- Name: [Text input field]
- Address: [Text input field]
- Port: [Text input field containing '25281']
- Host Cluster: [Dropdown menu showing 'Default']
- Enable Power Management
  - Address: [Text input field]
  - User Name: [Text input field]
  - Password: [Text input field]
  - Type: [Dropdown menu]
  - Port: [Text input field]
  - Slot: [Text input field]
  - Options: [Text input field]
  - Secure:
- Test: [Button]
- Save: [Button]
- Cancel: [Button]

Figura 2.49 Ventana de edición del nodo de virtualización

3. Los parámetros se llenaron de acuerdo con la información proporcionada por el cliente, donde:
  - 3.1. En el campo Address (Dirección IP) se escribió la dirección IP de la interfaz de administración remota iDRAC6. Es importante mencionar que esta dirección IP es diferente a la que se usa para la conexión con el sistema RHEV-M.
  - 3.2. En el campo User Name (Nombre de usuario) se escribió la contraseña del usuario proporcionado para realizar las tareas de administración de energía del nodo de virtualización.
  - 3.3. En el campo Password (Contraseña) se escribió la contraseña del usuario del sistema de administración remota.
  - 3.4. En el campo Type (Tipo) se escribió que tipo de agente se va a usar para la administración remota, en el caso de la interfaz iDRAC6 se utiliza el agente ipmilan.
  - 3.5. Los campos restantes se dejaron en blanco puesto que para la interfaz iDRAC6 no aplican.
4. Para probar si la conexión a la interfaz iDRAC6 era correcta se hizo clic en el botón Test (Prueba), el resultado fue satisfactorio.
5. Para guardar los cambios se hizo clic en Save (Guardar).

Con la configuración de estos parámetros se habilitan las técnicas de planificación y alta disponibilidad, además permite reducir el tiempo en el que los servicios están fuera de línea, por ejemplo, si se daña un nodo de virtualización automáticamente las máquinas virtuales que contiene se reiniciarán en el nodo funcional.

### 2.13.12 Configuración del planificador para balancear la carga de trabajo entre los nodos de virtualización

Una funcionalidad de la plataforma de virtualización Red Hat Virtualization for Server es la de balancear la carga de trabajo total entre los nodos de virtualización para mantener los niveles de servicio adecuados. Esta funcionalidad la proporciona el planificador, este componente puede trabajar bajo otro enfoque ofreciendo técnicas para el ahorro de energía, pero está limitado a solo una funcionalidad por clúster. Es decir, el planificador puede balancear la carga de trabajo entre los dos nodos o mover todas las máquinas virtuales a un solo nodo para dejar libre el segundo nodo y que este casi no gaste energía.

En esta implementación el cliente decidió que mantener los niveles de servicio era más relevante para la operación del negocio. Entonces se configuró el planificador para operar como un balanceador de carga.

Esta configuración se realizó con los siguientes pasos.

1. En la interfaz de administración RHEV-M, en la pestaña Clusters (Clústeres) se seleccionó el clúster activo (que además es el único enlistado) para tener acceso a sus propiedades, que aparecen en la parte inferior.
2. Se seleccionó la pestaña Policy (Política) y se dio clic en Edit (Editar).
3. En la ventana Edit Policy (Editar política, Figura 2.50) se seleccionó la opción Even Distribution (Distribución uniforme) y se configuraron los siguientes valores.
  - 3.1. La barra de porcentaje se colocó en 75% (Un porcentaje de nivel de servicio adecuado).
  - 3.2. En el campo tiempo se escribió 2 minutos.

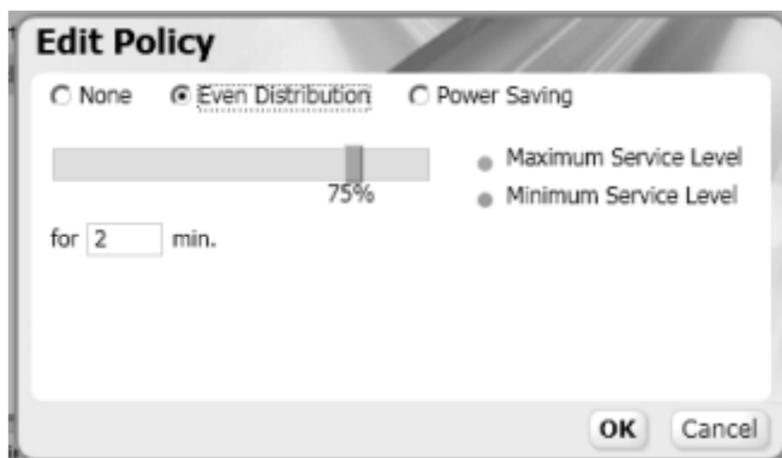


Figura 2.50 Ventana de edición de la política del planificador

4. Para hacer válida la configuración se hizo clic en OK (Aceptar).

La configuración se interpreta de la siguiente forma, la barra de porcentaje define el nivel de servicio máximo, este nivel indica la carga de trabajo que tienen los procesadores del nodo de virtualización, cuando un nodo supere el nivel de servicio máximo, se moverán las máquinas virtuales necesarias para lograr que no se rebase ese nivel. El tiempo configurado es la cantidad de minutos que esperará el planificador antes mover las máquinas virtuales una vez que se supere el límite, tiempo suficiente para descartar que la sobrecarga fue generada por un evento transitorio.

### **2.13.13 Configuración de las redes lógicas de los nodos de virtualización**

El diseño de las redes lógicas en una plataforma de virtualización es importante para ordenar de manera eficiente las comunicaciones. Una estrategia general y recomendada es crear las redes lógicas necesarias de acuerdo al tipo de comunicación, en cuanto a la solución se refiere. En los centros de datos virtuales se pueden observar dos grandes tipos de comunicación: la comunicación entre los componentes de la plataforma y la comunicación operacional de los servicios y aplicaciones instalados. La primera comunicación requiere de una protección mayor, puesto que es un punto medular, que de tener alguna falla, la plataforma entera se compromete.

El diseño de redes lógicas para este proyecto fue el siguiente (Figura 2.51):

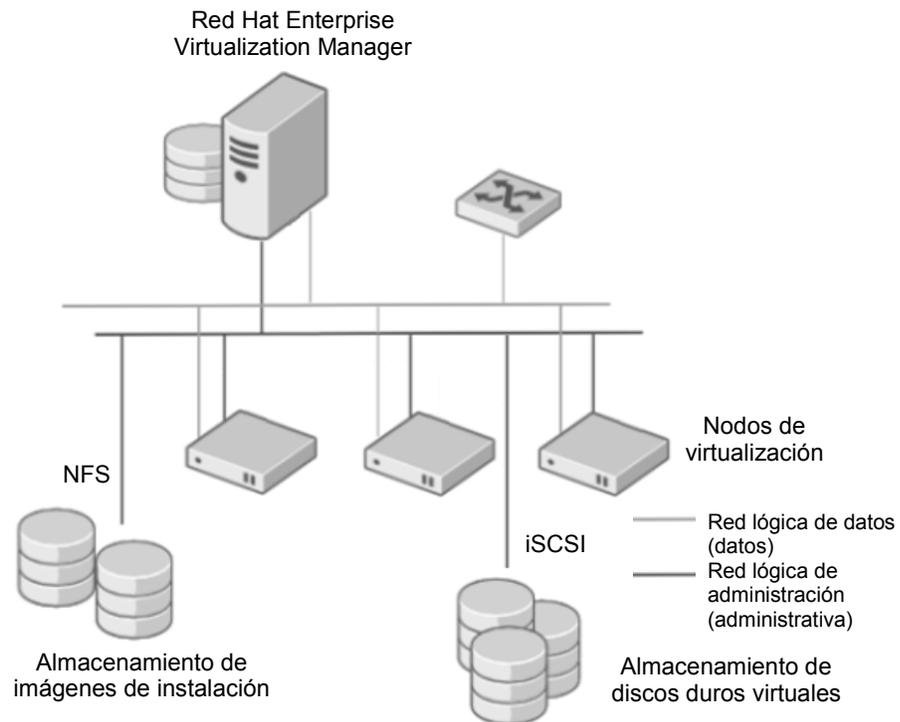


Figura 2.51 Esquema del diseño de las redes lógicas

Por defecto RHEV-M crea una red lógica llamada rhevm, esta red se utilizará como la red administrativa y se creará una segunda red lógica para el tráfico de datos operativos.

La creación de la red lógica<sup>49</sup> para tráfico de datos operativos se realizó siguiendo estos pasos:

1. En la interfaz de administración RHEV-M, en la pestaña Data Centers (Centros de datos) se seleccionó el centro de datos Default (que es el único listado) para tener acceso a sus propiedades, que aparecen en la parte inferior.
2. En la pestaña Logical Networks (Redes lógicas) se hizo clic en el botón New (Nueva) como se ve en la Figura 2.52.



Figura 2.52 Configuración de la nueva red lógica

3. En la ventana New Logical Network (Nueva red lógica) se llenaron los campos de la siguiente forma:
  - 3.1. En el campo Name se escribió el nombre de la nueva red lógica correspondiente a la red de datos operativos.
  - 3.2. En el campo Description se escribió una descripción como esta: “red de datos operativos”.
  - 3.3. Los campos Network address (Dirección de red), Subnet Mask (Máscara de red), Default Gateway (Puerta de enlace), STP Support (Soporte STP) y Enable VLAN tagging (Habilitar etiquetación para VLAN) se dejaron en blanco puesto que no se requieren configurar estos parámetros.
4. Para aplicar la configuración se hizo clic en OK (Aceptar).

<sup>49</sup> Red Hat Inc., Red Hat Enterprise Virtualization for Servers 2.2: Administration Guide. 2010, p. 38

La red de datos se puede implementar utilizando una sola interfaz de los nodos de virtualización y la administrativa debe tener un método de alta disponibilidad en la conexión de los nodos de virtualización con el dispositivo de almacenamiento de los discos duros virtuales (en esta implementación una SAN).

La disposición de las interfaces de red quedó de la siguiente forma (Tabla 2.15):

Tabla 2.15 Disposición del uso de las interfaces de red de los nodos de virtualización

Interfaz de red	Función	Configuración
HBA1	Conexión con dispositivo de almacenamiento	NIC Bonding
HBA2	Conexión con el sistema RHEV-M	
HBA3	Conexión a red de datos	

Las dos interfaces (HBA1 y HBA2) que servirán para la conexión con el dispositivo de almacenamiento además se configurarán de una forma especial para que se comporten como si fueran una sola interfaz pero combinando sus anchos de banda; además de proporcionar redundancia en la conexión.

Esta configuración se conoce como NIC Bonding y se configuró por cada nodo de virtualización, en esta implementación se llevó a cabo con los siguientes pasos:

1. En la interfaz de administración RHEV-M, en la pestaña Hosts (Nodos) se seleccionó el primer nodo (este procedimiento se realizó también para el segundo nodo) para tener acceso a sus propiedades, que aparecen en la parte inferior.
2. En la pestaña Network interfaces, donde se listan todas las interfaces de red, se seleccionaron las primeras dos (correspondientes a la HBA1 y a la HBA2) y se dio clic en el botón Bond.
3. En la ventana Bond Network Interfaces (Figura 2.53) se escribieron los siguientes valores:
  - 3.1. En la opción Bond se seleccionó bond0, que es el identificador que tendrá la interfaz.
  - 3.2. En la opción Network (Red lógica) se seleccionó rhevm que es el nombre de la red lógica creada por defecto.
  - 3.3. La opción Bonding options (Opciones de Bonding) se dejó en blanco puesto que no hay opciones adicionales que configurar.
  - 3.4. Se seleccionó la opción Static (Direccionamiento estático) para configurar cada valor de la interfaz de red.
  - 3.5. En el campo IP se escribió la dirección IP que tiene registrada el sistema RHEV-M para este nodo.
  - 3.6. En el campo Subnet Mask (Máscara de red) se escribió la máscara de red correspondiente.
  - 3.7. En el campo Default Gateway se escribió la dirección IP de la puerta de enlace.
  - 3.8. La casilla de verificación Check Connectivity (Verificar conexión) se seleccionó para validar si la nueva interfaz se puede activar.

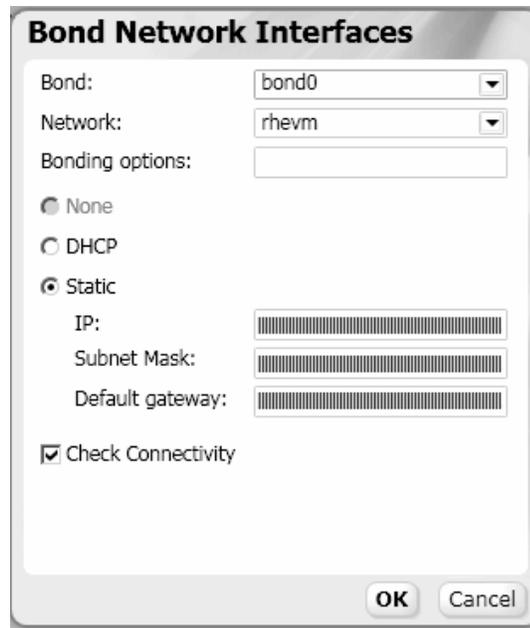


Figura 2.53 Ventana de edición de los parámetros de la interfaz bonding

4. Para aplicar la configuración se dio clic en OK (Aceptar).

La tercera interfaz de red se configuró<sup>50</sup> con un direccionamiento estático, asignándole una dirección IP diferente para la comunicación de datos operativos. Se realizó de la siguiente forma:

1. En la interfaz de administración RHEV-M, en la pestaña Hosts (Nodos) se seleccionó el primer nodo (este procedimiento se realizó también para el segundo nodo) para tener acceso a sus propiedades, que aparecen en la parte inferior.
2. En la pestaña Network interfaces, donde se listan todas las interfaces de red, se seleccionó la tercera interfaz (correspondientes a la HBA3) y se dio clic en el botón Edit (Figura 2.54).

---

<sup>50</sup> Red Hat Inc., Red Hat Enterprise Virtualization for Servers 2.2: Administration Guide. 2010, p. 92

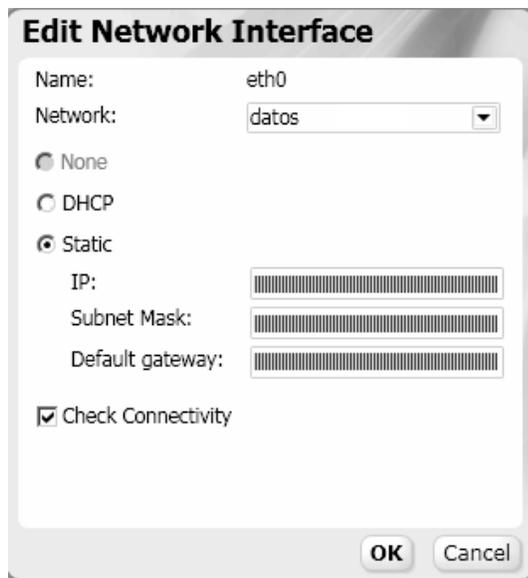


Figura 2.54 Ventana para la configuración de la interfaz de red

Todos los elementos de Red Hat Enterprise Linux configurados hasta ahora son indispensables para poner en funcionamiento óptimo las máquinas virtuales, cada componente desde la configuración del almacenamiento hasta la creación de redes lógicas es parte de una infraestructura de TI convencional en un centro de datos. El siguiente paso es la creación de las máquinas virtuales para la instalación de las aplicaciones de negocio, las máquinas virtuales están consideradas como el resultado del proyecto de virtualización, dado que el alcance así lo señala, por tal motivo, la creación y acondicionamiento de estas máquinas virtuales se detallará en el siguiente capítulo.

#### 2.13.14 Creación de una máquina virtual

Para la creación de las máquinas virtuales se hizo un análisis para saber que recursos necesarios de acuerdo con la aplicación que ejecutan.

##### *Configuración de los parámetros elementales*

A continuación se muestra el procedimiento general<sup>51</sup> para la creación de una máquina virtual.

<sup>51</sup> Red Hat Inc., Red Hat Enterprise Virtualization for Servers 2.2: Administration Guide. 2010, p. 113

1. En la interfaz de administración RHEV-M, en la pestaña Virtual Machines (Máquinas virtuales) se hace clic en el botón New Server (Nuevo servidor). En esta pestaña se enlistan las máquinas virtuales existentes.
2. En la ventana New Server Virtual Machine (Nuevo servidor en máquina virtual) se presentan cuatro pestañas de configuración, General, Console (Consola), High Availability (Alta disponibilidad) y Boot Sequence (Secuencia de inicio); con diferentes opciones cada una.
3. La pestaña General tiene los siguientes parámetros de configuración (Figura 2.55).

The image shows a screenshot of the 'New Server Virtual Machine' configuration window. The window has a title bar 'New Server Virtual Machine' and a sidebar with tabs: 'General' (selected), 'Console', 'High Availability', and 'Boot Sequence'. The main area contains the following fields: 'Data Center:' (Default), 'Host Cluster:' (Default), 'Default Host:' (Auto Assign), 'Name:' (empty text box), 'Description:' (empty text box), 'Based on Template:' (Blank), 'Memory Size:' (512 MB), 'Total Cores:' (1), 'CPU Sockets:' (1), and 'Operating System:' (Unassigned). Each of the last four fields has a slider control. At the bottom right are 'OK' and 'Cancel' buttons.

Figura 2.55 Ventana para la configuración de los parámetros generales de la nueva máquina virtual

- 3.1. En la lista desplegable Data Center (Centro de datos) se elige el centro de datos donde se va a colocar la nueva máquina virtual, en esta implementación solo existe el centro de datos virtual Default.
- 3.2. En la lista desplegable Host Cluster (Clúster) se elige el clúster donde se va a colocar la máquina virtual, en esta implementación solo existe el clúster Default.
- 3.3. En la lista desplegable Default Host (Nodo default) se elige en cual nodo de virtualización se va a colocar la nueva máquina virtual, en esta implementación existen dos: rhevh1.aseguradora.com y rhevh2.aseguradora.com. Además se puede elegir la opción Auto Assign (Auto-asignar), en este caso el planificador va a colocar la nueva máquina virtual en un nodo activo o con recursos suficientes. La distribución de las máquinas virtuales se va a definir más adelante.
- 3.4. En el campo Name (Nombre) se escribe el nombre deseado para la nueva máquina virtual, este es un sencillamente un identificador.
- 3.5. En el campo Description (Descripción) se escribe algún texto que detalle el uso o alguna característica de la nueva máquina virtual.

- 3.6. En la lista desplegable Based on template (Basada en una plantilla) se elige si la nueva máquina virtual se creará a partir de una plantilla previamente hecha, si no existe una plantilla se elige la opción Blank (en blanco).
  - 3.7. En el campo Memory Size (Tamaño de memoria) se especifica cuánta memoria virtual se le va a asignar a la nueva máquina virtual. En esta implementación esta asignación se hizo de acuerdo a la demanda de cada servidor consolidado, más adelante se definen estos valores.
  - 3.8. En la barra Total Cores (Núcleos totales) se define el número de núcleos virtuales que tendrá la nueva máquina virtual, el número máximo que puede tener es 16. En esta implementación esta asignación se hizo de acuerdo con la demanda de cada servidor consolidado, más adelante se definen estos valores.
  - 3.9. En la barra CPU Sockets (Número de CPUs) se define el número de CPUs virtuales que tendrá la nueva máquina virtual, el número máximo que puede tener es 16. En esta implementación esta asignación se hizo de acuerdo con la demanda de cada servidor consolidado, más adelante se definen estos valores.
4. En la pestaña Console (Consola), se pueden configurar los siguientes parámetros (Figura 2.56).

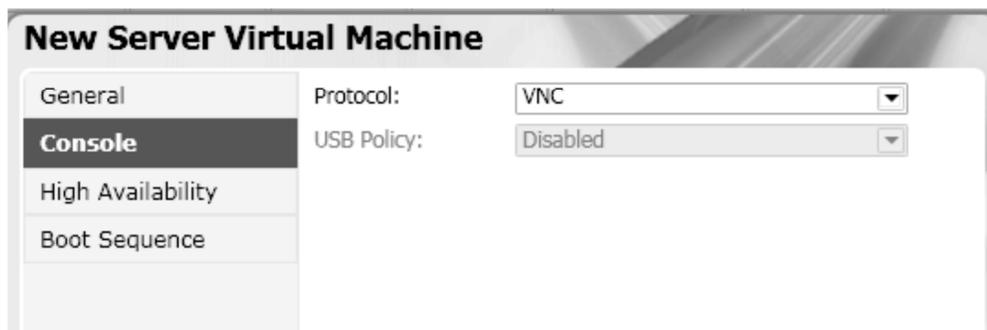


Figura 2.56 Ventana para la configuración del protocolo de visualización

- 4.1. En la lista desplegable Protocol (Protocolo), se elige el protocolo de visualización a usar, Red Hat Enterprise Virtualization maneja dos protocolos: *VNC*, que es un protocolo para escritorio remoto y *SPICE* que es un protocolo desarrollado por Red Hat para la visualización del escritorio virtual que proporciona una mejor experiencia de uso.
  - 4.2. La lista desplegable USB Policy (Política de USB), no está disponible para máquinas virtuales tipo servidor.
5. En la pestaña High Availability (Alta disponibilidad) se configura si la máquina virtual va a estar en un ambiente de alta disponibilidad y tiene los siguientes parámetros (Figura 2.57).

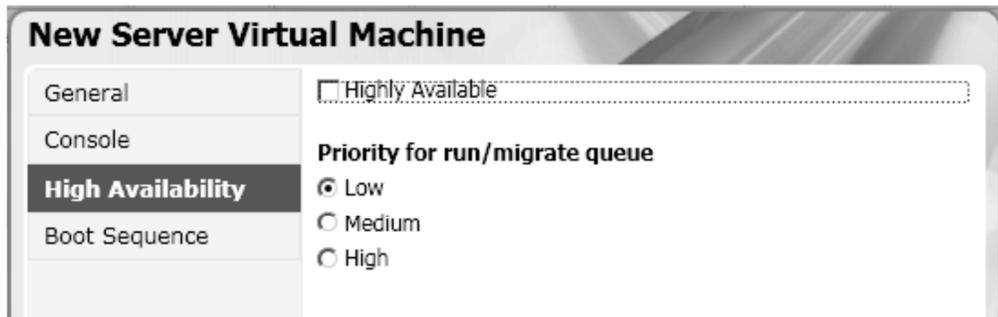


Figura 2.57 Ventana para la configuración de alta disponibilidad

- 5.1. La casilla de verificación Highly Available (en alta disponibilidad) se selecciona si la nueva máquina virtual va a estar en un ambiente de alta disponibilidad.
- 5.2. En las opciones del parámetro Priority for run/migrate queue (Prioridad para encender o poner en la cola de migración) se configura la prioridad de la nueva máquina virtual para encenderse (si está configurado el planificador en modo ahorro de energía) o para migrarse a un nodo de virtualización activo (en el caso de que el actual haya fallado). Existen tres prioridades: Low (Baja), Medium (Media) y High (Alta).  
En esta implementación si se manejó alta disponibilidad para las máquinas virtuales, la prioridad se define más adelante.
6. En la pestaña Boot Sequence (Secuencia de inicio, Figura 2.58) se definen la prioridad de elección para cada dispositivo de inicio, como pueden ser discos duros virtuales, interfaces de red virtuales o unidades ópticas virtuales.

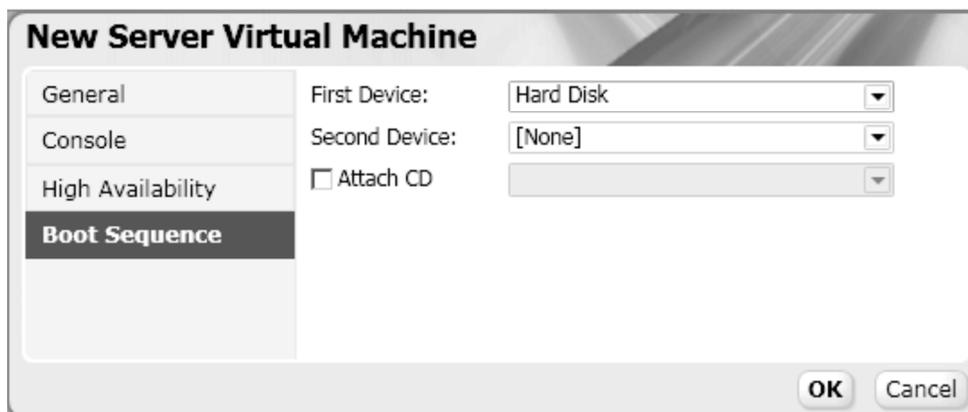


Figura 2.58 Ventana para la configuración de la secuencia de inicio

- 6.1. En la lista desplegable First Device (Primer dispositivo), se selecciona el primer dispositivo de inicio.
- 6.2. En la lista desplegable Second Device (Segundo dispositivo), se selecciona el segundo dispositivo de inicio.
- 6.3. En la opción Attach CD (Añadir CD) se elige si se va a cargar una imagen de instalación ISO.

Cuando los parámetros elementales han sido configurados el asistente de configuración para la máquina virtual aparece. En este asistente se pueden configurar las interfaces de red y los discos duros virtuales.

### *Configuración de la red*

El siguiente paso es la configuración de las interfaces de red, donde se definen los siguientes parámetros.

1. En la ventana New Network Interface (Nueva interfaz de red, Figura 2.59), se configura el tipo de interfaz de red, la dirección MAC y la red lógica a la que se conectará.
  - 1.1. En el campo Name (Nombre), se escribe el nombre de la interfaz de red, éste es un identificador solamente, dependiendo el sistema operativo la reconocerá con un nombre predefinido.
  - 1.2. En la opción Network (Red), se elige la red lógica donde estará conectada la interfaz de red, esta configuración debe ser congruente con la configuración de la interfaz de red dentro del sistema operativo. En esta implementación la red de datos operativos se llama *datos*.
  - 1.3. En la opción Type (Tipo) se especifica el tipo de interfaz virtual presentada al sistema operativo virtual, para sistemas Linux se recomienda la opción e1000 o Red Hat VirtIO, para sistemas Windows rtl8139 o Red Hat VirtIO. En el caso de elegir Red Hat VirtIO se deberán instalar controladores de dispositivos especiales para la optimización del desempeño de la interfaz de red, estos controladores están disponibles para Windows y para versiones de RHEL superiores a la 4.8.
  - 1.4. En el campo MAC Address (Dirección MAC) se especifica una dirección MAC, si así se requiere, en caso contrario se puede dejar en blanco la casilla de verificación.



Figura 2.59 Ventana para la configuración de las interfaces de red

### *Configuración del almacenamiento virtual*

Para completar la configuración de una nueva máquina virtual se requiere configurar el almacenamiento virtual, es decir, el o los discos duros virtuales.

1. En la ventana New Virtual Disk (Nuevo disco virtual, Figura 2.60), se configura el tipo de disco duro virtual, la capacidad y el formato, a continuación se presentan los parámetros:



Figura 2.60 Ventana para la configuración de las interfaces de red

2. En el campo Size (Tamaño), se especifica la capacidad de almacenamiento del disco duro virtual en unidades de GB (Giga Byte). En esta implementación esta asignación se hizo de acuerdo con la demanda de cada servidor consolidado, más adelante se definen estos valores.
3. En la opción Storage Domain (Dominio de almacenamiento), se elige el dominio de almacenamiento de donde se va a reservar el espacio para el disco duro virtual. En esta implementación solo existe un dominio de almacenamiento de datos.
4. En la opción Disk Type (Tipo de disco) se define el tipo de disco duro virtual.
  - 4.1. El tipo System (Sistema) si el disco duro virtual será para la instalación del sistema operativo.
  - 4.2. El tipo Data (Datos) si el disco duro virtual es para almacenamiento de datos. Solo el tipo System es *bootable* (Se puede iniciar la máquina virtual desde este dispositivo).
5. En la opción Interface (Interfaz) se define el tipo de disco duro virtual presentado al sistema operativo, existen dos opciones.
  - 5.1. La opción VirtIO es para presentar un dispositivo para-virtualizado al sistema operativo virtual, éste requiere de controladores especiales para su óptimo funcionamiento.
  - 5.2. La opción IDE presenta un disco duro virtual emulando el protocolo IDE, las máquinas virtuales con sistema operativo Windows 2008 requieren de este tipo de disco duro virtual.
6. La opción Format (Formato) puede ser Pre-allocated (Pre-asignado) o Thin provision (Provisión ligera).
  - 6.1. El formato Pre-allocated (Pre-asignado) o *RAW*, define que el espacio marcado por el campo Size (Tamaño) será reservado del dominio de almacenamiento, este formato es recomendable para máquinas virtuales tipo servidor.
  - 6.2. El formato Thin provision (Provisión ligera) o Qcow2 se define para usar el espacio de almacenamiento conforme la máquina virtual lo requiera. Si la máquina virtual se va a utilizar para crear una plantilla, se debe seleccionar este formato.
7. La opción Wipe after delete (Limpiar después de eliminar) se selecciona si el contenido del disco duro virtual será borrado cuando la máquina virtual se elimina.
8. La opción Is bootable, se selecciona si el disco duro virtual será un dispositivo de inicio para la máquina virtual.

Con estos pasos la máquina virtual esta lista para ser utilizada, para ejecutarla solo se selecciona y se hace clic en el botón run (ejecutar, Figura 2.61) situado en la parte superior.



Figura 2.61 Ejecución de una máquina virtual