UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Desarrollo de una infraestructura de virtualización de servidores y escritorios remotos con monitorización, para proporcionar servicios de TI en USECAD, Facultad de Ingeniería UNAM

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTAN:

ARGUETA CORTÉS JAIRO ISACAR
GUERRERO RAMÍREZ EDUARDO DANIEL

AVAL:
Filiberto Manzo González

Ciudad Universitaria, México, D.F. **Julio 2013**

Introducción

1. Antecedentes

2 Conceptos básicos

3 Planificación de carga (CapacityPlanning)

3.1. ¿Para qué realizar la planificación de carga?
3.2. ¿Cuándo hay que realizar una planificación de carga?
3.3. Planificación de carga en USECAD
3.4. Planificación de carga para RHEV
    3.4.1. Even distributión
    3.4.2. PowerSharing

4 Instalación de ambiente Red Hat Enterprise Virtualization

4.1 Instalación de RHEV-Manager (administrador de Red Hat Enterprise Virtualization)
4.2 Instalación de RHEV-Hypervisor
4.3 Configuración de bonding de tarjetas
4.4 Configuración de NFS en RHEL

5 Implementar servicios sobre esquema de virtualización

5.1 Creación de servidores virtuales
    5.1.1 Instalación de sistema operativo
    5.1.2 Configuración e instalación de servicios
    5.1.3 Migración de servidores fisicos a virtuales
5.2 Creación de escritorios remotos virtuales
    5.2.1 Creación de usuarios y asignación de escritorios virtuales
    5.2.2 Instalación de paquetes de VirtIO
    5.2.3 Instalación de cliente Spice

6 Instalación de Zenoss Core

6.1 Monitoreo de equipos en USECAD antes de la instalación de Zenoss
6.2 Lista de requerimientos para monitoreo de sistemas operativos en ambientes seguros
6.3 Configuración de Servidores
6.4 Monitoreo de servidores LINUX
6.5 Monitoreo de servidores Windows con WMI
6.6 Monitoreo de servidores Windows con SNMP
6.7 Monitoreo del tiempo de respuesta de páginas web
6.8 Monitoreo de Apache Web Server
6.9 Configuración de la herramienta de monitoreo
    6.9.1 Personalización de Alarmas
    6.9.2 Mensaje de las Alertas
    6.9.3 Integración con Google Maps

7 Análisis de resultados

7.1 Interpretación de los resultados del monitoreo
7.2 Análisis de desempeño en los servidores físicos
7.3 Análisis de desempeño en los escritorios virtuales
7.4 Análisis del estudio de consumo de energía anterior y actual

8 Conclusiones

Introducción

La ciencia de la computación ha tenido un desenvolvimiento enorme desde su aparición hace ya cinco décadas, los retos que afronta día a día son mayores y dentro de los cientos de problemas existentes que tratan de erradicarse o controlarse esta el máximo aprovechamiento de los equipos de cómputo destinados a ofrecer servicios dentro y fuera de una organización.

La búsqueda por lograr un mejor aprovechamiento de hardware en cada equipo y reducir el número de estos en cada centro de datos se volvió el punto de atención desde los años 60, cuando el concepto de virtualización lo dio a conocer por primera vez IBM sobre la plataforma de mainframe como una manera lógica de particionar ordenadores en máquinas virtuales independientes. Estas particiones permitían a los mainframe realizar varias tareas: ejecutar varias aplicaciones y procesos al mismo tiempo. Dado que en aquella época los mainframes eran recursos caros, se diseñaron para ser particionados para así aprovechar al máximo la inversión.

Hoy en día, los ordenadores basados en arquitectura x86 se enfrentan a los mismos problemas de rigidez e infrautilización a los que se enfrentaban los mainframes en la década de 1960. VMware inventó en la década de los 90 la virtualización de la plataforma x86 para solucionar dicha infrautilización, superando de paso muchos otros problemas.

El tema central de este trabajo tiene que ver con la virtualización o también conocido como la consolidación de servidores, es una tendencia la cual las empresas están considerando utilizar dado el análisis de especialistas y casos de éxito de empresas que ya cuentan con esta tecnología.

La virtualización permite que en un centro de datos existan servidores con muy buenas características de hardware que, a través de la virtualización se pueda aprovechar al máximo los recursos de hardware para consolidad diversos sistemas operativos de manera independientes unos de otros en un mismo equipo de cómputo y encapsulados en una máquina virtual sin afectar el rendimiento de las demás máquinas que ahí se alojen. La virtualización ayuda a reducir costos de adquisición y mantenimiento de equipo de cómputo, ahorro de energía eléctrica, ahorro de espacio físico, vida funcional de los componentes físicos y del sistema de enfriamiento o aire acondicionado, adicional a esto, se aíslan completamente ambientes de trabajo, permitiendo establecer políticas y herramientas de seguridad propias de la herramienta de virtualización o en cada uno de los servidores virtualizados, al final del día tenemos reducción en los costos de operación y mantenimiento.

El desarrollo e implementación de la infraestructura de virtualización descrita en este trabajo, tiene como objetivo proporcionar una plataforma de software de open source para consolidar servidores de manera eficiente para el óptimo desempeño de aplicaciones , proporcionando las herramientas necesarias para lograr una administración ágil y eficaz. Este proyecto está basado en el análisis de requerimientos del centro de datos de USEDCAD de la Facultad de Ingeniería, UNAM, y tiene como objetivo beneficiar a la institución en el ahorro de costos de adquisición de equipo de cómputo ya que este proyecto hace uso de los recursos disponibles para implementar dicha infraestructura.

Esta solución contempla la virtualización de escritorios, la cual consiste en tener sistemas operativos de escritorio virtualizados (Windows XP, Windows 7, Linux) con la finalidad de proveer un escritorio de acceso remoto consumiendo recursos mínimos de hardware por parte del cliente, de esta manera se mantiene la información del usuario dentro de la organización, disponible y segura.

También como parte de la solución, se integra una solución de monitoreo para la recolección de estadísticas de disponibilidad y rendimiento (CPU, RAM, RED I/O) de cada uno de los servidores virtualizados así como aquellos que formen parte de la solución de virtualización con

la finalidad de tener un histórico del comportamiento de todos los equipos involucrados en la solución.

A lo largo del documento, se dan a conocer los antecedentes históricos y técnicos para tener un mejor entendimiento de lo que es la tecnología de virtualización, los objetivos que hemos planteado, el análisis previo al diseño y desarrollo del proyecto con la debida explicación de los procedimientos técnicos ejecutados para el éxito del proyecto.

Al final de la implementación del proyecto se muestran los resultados obtenidos dando a conocer si se cumplieron o no los objetivos propuestos así como el análisis de las ventajas y desventajas de la solución planteada.

Se incluye también una sección de anexos, donde se detalla paso a paso cada una de las etapas de implementación. En dichos anexos se encuentran las instrucciones, salidas de comandos, con el fin de hacer más comprensible la implementación.

Para reforzar la comprensión del lector se incluye un glosario de términos utilizados en el presente trabajo.

Al final se enuncian las fuentes bibliográficas y electrónicas que dieron un marco referencial de inicio y desarrollo para la construcción de esta tesis.

1. Antecedentes

1.1 Situación actual de los centros de datos

Hoy en día las organizaciones gubernamentales, educativas y empresas, enfrentan nuevos retos y por consecuente la toma de decisiones para afrontar los mismos, que bien pueden favorecer a los objetivos de negocio y metas propuestas o bien afectar al éxito del negocio y operaciones con las áreas relacionadas. Las áreas de desarrollo, infraestructura y soporte tienen como objetivo mantener la disponibilidad de los servicios, recursos y equipo de cómputo los cuales soportan los objetivos de negocio tanto para usuarios internos o externos a la organización. Años atrás y hasta el día de hoy, la adquisición de equipo de cómputo va enfocada para soportar una o hasta dos aplicaciones por servidor físico, pero a través del análisis de utilización de recursos surge un gran interés por aprovechar estos al máximo, como CPU, memoria, espacio en disco y considerando también el consumo de energía de cada equipo de cómputo en un centro de datos, el espacio asignado que este mismo requiere con su adquisición, el soporte preventivo y correctivo para cada equipo de cómputo adquirido conlleva consigo un alto costo de adquisición y mantenimiento.

Derivado de un análisis de aprovechamiento de recursos y optimización de gastos podemos encontrar los siguientes problemas en los centros de datos actuales:

- Cuando se tiene un servidor físico en producción y de nivel crítico, en ocasiones es necesario ponerlo en clúster para contar con alta disponibilidad y balanceo de carga. El costo del mantenimiento de esta solución es elevado.
- El respaldo de la información también es una de las tareas difíciles a las que se enfrentan los administradores de TI, ya que necesitan de algún software capaz de brindar este servicio (ejemplo Veritas, CA, entre otros), el costo de las licencias también es grande.
- El consumo de energía eléctrica, un mal diseño de la instalación eléctrica y la variación de voltajes puede dañar los equipos y aumentar el costo de mantenimiento y/o reparación de los dispositivos.
- Cuando el número de servidores físicos es muy grande el número de personal también debe aumentar para poder administrar y brindar el mejor servicio posible.
- El mantenimiento preventivo de servidores físicos es costoso ya que se tiene que dar de baja temporal el servidor para poder dar dicho mantenimiento. Para servidores críticos es aún más costoso realizar esta tarea.
- El crecimiento de servidores también se vuelve un problema al ir reduciendo espacio en el centro de datos. Lo que provoca mayor calentamiento y la necesidad de un mejor sistema de enfriamiento. Este problema también se le conoce como “power&cooling”.
- La adquisición de un servidor por aplicación, esto implica tener un gran número de servidores físicos para soportar servicios como correo, CRM, web, base de datos, servidor de archivos, etc.

Todos estos problemas representan el 70% del presupuesto destinado al área de la infraestructura de la información, lo que significa que la inversión a la investigación a nuevas tecnologías se vuelve mínimo.

1.1.1 Situación actual de la infraestructura de USECAD

Actualmente USECAD cuenta con varios servidores que son creados para alguna tarea en específica como por ejemplo: Bases de datos (Sybase), correo electrónico, servidor web (LAMP), un servidor de compartición de archivos (SAMBA), servidores de prueba y de respaldos.

Toda esta infraestructura actual de USECAD origina la necesidad de reducir costos en energía eléctrica y evitar el crecimiento en número de servidores físicos por el espacio que se hace cada vez más angosto.
USECAD es una unidad de innovación donde está en constante investigación para fortalecer las tecnologías de información con nuevos proyectos, implementaciones y pruebas, por lo que requiere un cambio en su forma de ir incrementando el número de servidores, reducir el tiempo de instalación y mejorar la administración de los servidores.
Al realizar un Site-survey (levantamiento tecnológico) de la infraestructura encontramos las siguientes necesidades a erradicar en el centro de datos de USECAD

- Un gran número de servidores no está utilizando al máximo los recursos de hardware de los equipos físicos.
- No cuentan con una administración adecuada y tampoco centralizada para el número existente de servidores.
- No cuentan con herramientas de monitoreo apropiadas para la recolección de datos de rendimiento de los servidores.
- El espacio es cada vez más reducido para seguir agregando servidores.
- El consumo de energía eléctrica es muy alto por el número de servidores.
- Requiere de flexibilidad operativa para el rápido aprovisionamiento de servidores.
- Reducción de los costos directos, generados por: Servicios de soporte y mantenimiento al hardware, administración y atención de las necesidades de los usuarios.
- Reducir el número de PC's y equipos individuales que desperdician espacio útil del centro de datos y que consumen recursos tanto eléctricos, como de red y generan calor debido a su funcionamiento.

Los servidores existentes que forman parte del centro de datos de USECAD se muestran en la **Tabla 1** donde vemos las características y aplicaciones de cada servidor.

Servidor	SO	Aplicación	Procesador	Memoria RAM	Storage
bd1.fi-a.unam.mx	Solaris	Sybase	SPARC	4 GB	60 GB
bd2.fi-a.unam.mx	Solaris	Sybase	SPARC	16 GB	60 GB
Correo	Fedora 13	Postfix	Pentium 3	1 GB	100 GB
LAPM1	Fedora 8	LAMP	Pentium 4	2 GB	80 GB
web1.fi-a.unam.mx	RHEL 5	LAMP	Pentium 4	2GB	80 GB
web2.fi-a.unam.mx	RHEL 5	LAMP	Pentium 4	4 GB	80 GB
LAPM2	Fedora 8	LAMP	Pentium 4	2 GB	80 GB

Tabla 1. Servidores del centro de datos de USECAD

En la **Figura 1** se aprecia un diagrama de red de USECAD

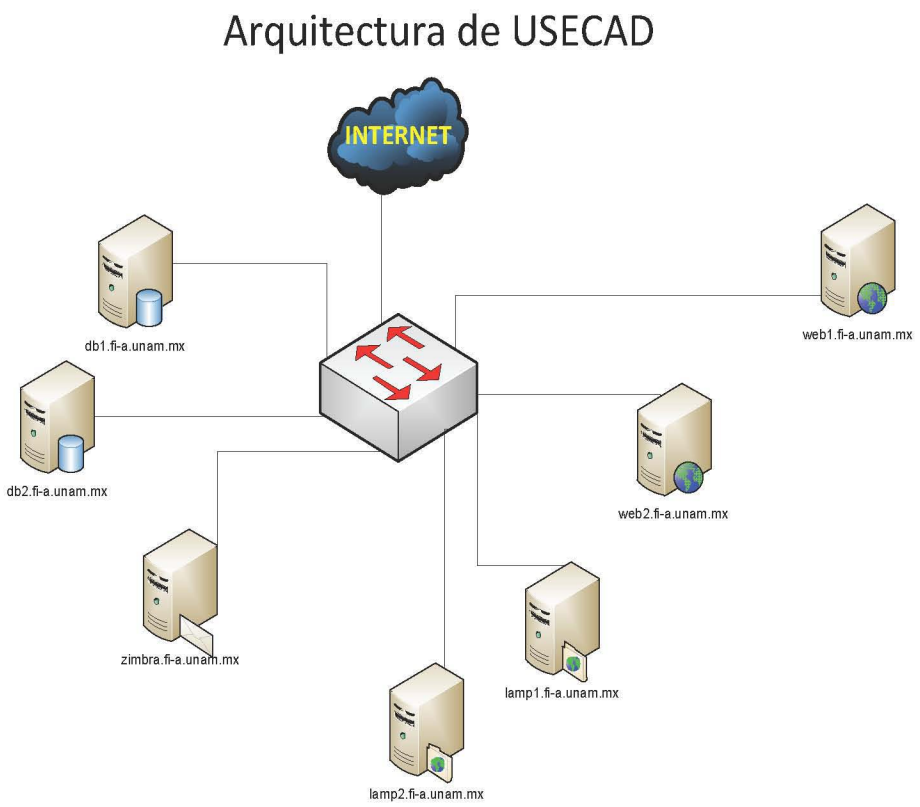


Figura 1. Diagrama de red de USECAD

Una vez detectadas las necesidades en el centro de datos, describimos a continuación una serie de objetivos a cumplir para mejorar las operaciones, mantenimiento y costos de los equipos de cómputo en USECAD.

1.2 Objetivo General

Desarrollar una infraestructura de virtualización con tecnología de Red Hat Enterprise Linux, así como, servicios de monitorización utilizando Zenoss Core en servidores disponibles con la finalidad de migrar la mayoría de aplicaciones de TI a un ambiente virtual para la Unidad de Servicios de Cómputo Administrativos (USECAD) de la Facultad de Ingeniería UNAM.

1.2.1 Objetivo de Virtualizar el centro de datos de USECAD

Lo siguiente son objetivos a alcanzar con la virtualización del centro de datos de USECAD:

- **Consolidar servidores y optimizar la infraestructura:** utilización de los recursos significativamente mayor mediante la agrupación de recursos de infraestructura comunes y la superación del modelo heredado de "una aplicación para un servidor".

- **Obtener recursos necesarios con los medios existentes**.- Poner en marcha aplicaciones y balanceo de cargas de trabajo entre los recursos que se tienen.

- **Centros de tolerancia a desastres**.- Tener una infraestructura virtual para poder replicar el centro de datos principal, replicando los servidores críticos en maquinas virtuales.

- **Virtualización de escritorios de trabajo**.- Proveer el escenario adecuado para crear entornos de trabajo en un futuro, creando escritorios remotos, para poder ser utilizados desde cualquier lugar de la red.

- **Flexibilidad operativa:** USECAD responderá rápidamente a los cambios de la tecnología informática con una gestión dinámica de los recursos, con un aprovisionamiento de servidores acelerado y con una mejora de la implementación de escritorios y aplicaciones.

- **Reducción de costos de infraestructura física:** se requiere reducir la cantidad de servidores y hardware inherente al centro de datos. Es necesario disminuir los requisitos inmobiliarios, de alimentación y refrigeración, con la consiguiente e importante disminución de los costos de TI.

- Asegurar que la tecnología de virtualización utilizada cubra el 100 % de los sistemas operativos utilizados en USECAD.

- Ampliar el uso de tecnologías de virtualización en USECAD

- Proveer un esquema de replicación y respaldos de información en tiempo real

- Contar con un esquema de alta disponibilidad de los servicios más importantes en los servidores virtualizados.

- Contar con un sistema de respaldo de la información, bases de datos, máquinas virtuales y datos.

1.2.2 Objetivo de monitorear los servidores de USECAD con Zenoss

La infraestructura de TI es el punto crítico para el éxito empresarial, hoy más que nunca. La responsabilidad del mantenimiento de la infraestructura, su disponibilidad y correcto funcionamiento recae en el equipo de operaciones.

Zenoss ayuda a lidiar con las empresas en constante evolución, con entornos dinámicos de TI, al proporcionar una solución integral que controla toda la infraestructura, física y virtual en un solo producto.

De acuerdo a las características más sobresalientes de Zenoss los objetivos planteados son los siguientes:

- Ofrecer una amplia cobertura de la pila de TI (redes, servidores, aplicaciones, servicios de virtualización).

- Dar un seguimiento profundo para un dispositivo gestionado.

- Tener una administración completa de funcionalidad y gestión de Operaciones de TI (inventario de servidores y dispositivos de red, monitoreo de disponibilidad de servicios, datos de rendimiento de hardware, generación de informes, y alertas).

- Tener una rápida adaptación al entorno administrado y sistemas de gestión.

- Ofrecer un control integrado de los recursos físicos, virtuales, internos y externos
  Menor costo total de propiedad (TCO), hasta en un 70%.

1.2.3 Objetivo de Virtualizar con RHEV (Red Hat Enterprise Virtualization)

- Contar con el mejor performance existente, proporcionado por esta solución de virtualización, el rendimiento de ciertas aplicaciones puede ser superior en entornos virtuales.
- Brindar una administración de servidores, hypervisores y storage centralizada mediante el uso de una administrador web de Red Hat (RHEV-M) sobre un sistema operativo Windows Server 2008.
- Reducción de costos de licenciamiento, esta es una solución más económica en comparación con otras soluciones (Vmware, Hyper-V, Citrix).

El mayor problema, consiste en buscar la mejor forma de consolidar parte de los servicios brindados por USECAD, utilizando la infraestructura física con la que se cuenta, que facilitara su orientación a servicios, con el menor costo posible y de manera transparente para los usuarios.

Con esta implementación tecnológica se pretende consolidar en un inicio, parte de los servidores y servicios que actualmente brinda USECAD en su centro de datos, la liberación de equipos de cómputo que podrían ser reutilizados para alguna otra aplicación con mayores requerimientos o dar paso a su utilización en nuevos proyectos, buscamos la reutilización productiva de la infraestructura actual, evitando tener la necesidad de adquirir infraestructura nueva.

También buscamos enérgicamente la reducción del impacto al ambiente, obteniendo menor perdida de energía, que resulta necesario en el uso de sistemas de enfriamiento y aire acondicionado del centro de datos.

Esperamos un gran ahorro en costos de operación, administración, mantenimiento, espacio, energía eléctrica y sistemas de enfriamiento, deseamos aprovechar al máximo la capacidad de los recursos físicos disponibles de la infraestructura, reorganizar de acuerdo a capacidad y utilización de las aplicaciones, de manera óptima, buscamos también una alta disponibilidad de los mismos y maximizar su desempeño.

2. Conceptos básicos

En este segundo capítulo vamos a ver información general sobre el término virtualización, sus diferentes aproximaciones teóricas y sus aplicaciones prácticas hoy en día, es necesario conocer el significado de diversos términos que engloba la virtualización para poder comprender el marco teórico que estamos trabajando.

2.1 Virtualización

Vladimir Posavac nos proporciona una definición más clara de virtualización:

> *"La Virtualización de Servidores es un concepto utilizado para definir el proceso de agrupar varios servidores en uno solo, manteniendo cada ambiente individual al mismo tiempo que se optimiza el uso de recursos tales como procesadores, memoria, redes y almacenamiento. El propósito es utilizar los recursos ociosos, balancear adecuadamente las cargas de trabajo en los momentos críticos y brindar una administración centralizada".*

2.2 ¿Qué es la virtualización?

La virtualización permite tener y administrar varias máquinas virtuales en una misma máquina física, donde cada una de las máquinas virtuales comparte los recursos de ese ordenador físico único entre varios entornos. Las distintas máquinas virtuales pueden ejecutar sistemas operativos diferentes y varias aplicaciones en el mismo ordenador físico.
La virtualización no es lo único importante. Se necesitan herramientas de administración para gestionar las máquinas y la capacidad de ejecutar todas las aplicaciones y los servicios de infraestructura de los que depende la organización. A continuación hablaremos de *Red Hat Enterprise Virtualization (RHEV)* permite que aumentar la disponibilidad de los servicios, porque elimina las tareas manuales en las que se cometen errores con mayor facilidad. Los centros de *Tecnologías de la Información (TI)* son más eficaces y efectivos con la virtualización en Red Hat. El personal gestionará una cantidad de servidores en gran número para proporcionar a los usuarios el acceso a los servicios que necesitan mientras conservan el control centralizado. Puede proporcionar disponibilidad, seguridad, integridad y rendimiento integrados directamente, desde el escritorio hasta el centro de datos.

2.3 Tipos de virtualización

La virtualización tiene múltiples usos y de acuerdo a estos podemos determinar qué tipo de virtualización estamos hablando. Los más comunes de forma muy general son la virtualización de servidores, virtualización de clientes y virtualización de almacenamiento de datos. Estos se dividen a su vez en sub tipos o especializaciones dentro de cada tipo de virtualización general.
Debido a la amplia gama a la que este concepto hace referencia, podemos definir tres tipos de virtualización más relevantes:

2.3.1 Emulador

Es la combinación de software y una extensión de hardware para simular el comportamiento de una máquina. Permite clonar un sistema y hacer uso de él en otro equipo distinto, y hacer pruebas en la simulación sin comprometer al sistema (previo guardado del estado del emulador).

Lo que se hace es primero tener un sistema operativo instalado en el cliente, luego se instala el software de emulación de hardware que una vez instalado y configurado queda listo para instalar otro sistema operativo invitado, esto se hace a través del software de virtualización en vez de instalarse directamente en el computador anfitrión quien configura el contenedor o lo que conocemos como la máquina virtual. Después de esto la instalación del nuevo sistema

operativo invitado se hace igual que como si lo estuviéramos haciendo en un equipo de cómputo nuevo como se muestra en la siguiente figura (Figura 1).

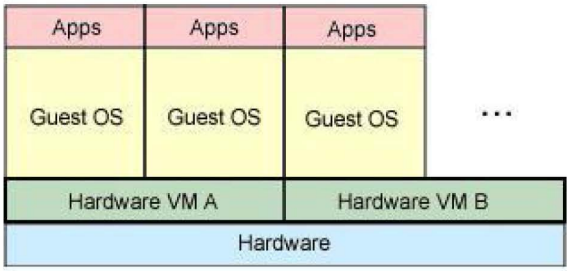


Figura 1. Emulación

2.3.2 Paravirtualización

Hace referencia a los sistemas operativos "hosts", que se encargan de administrar y monitorear el trabajo de las máquinas virtuales. De esta manera, todos los "guests" mandan sus peticiones al "host" a la hora de usar recursos. Para permitir esto, se necesita un interfaz estandarizado para uso de otros programas y sistemas. El esquema de paravirtualización se muestra en la siguiente figura (Figura 2).

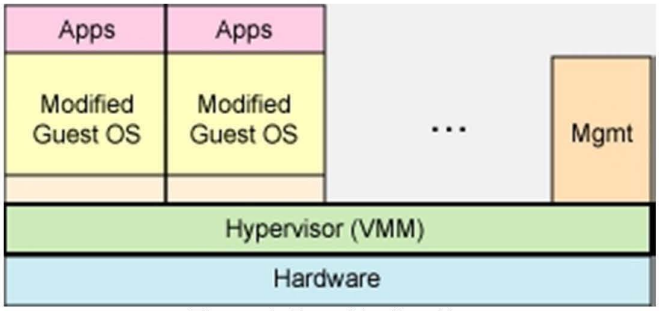


Figura 2. Paravirtualización

Las ventajas de este enfoque son un muy buen rendimiento y la posibilidad de ejecutar distintos sistemas operativos como guests. Se obtienen, además, todas las ventajas de la virtualización enunciadas anteriormente. Su desventaja es que los sistemas operativos guests deben ser modificados para funcionar en este esquema.

2.3.3 Virtualización completa

También llamado "full virtualization". Es la simulación de un hardware de tal forma que un sistema operativo "guest" pueda trabajar de forma aislada.

Este método tiene todas las ventajas de la paravirtualización, con la característica de que no es necesaria ninguna modificación a los guests. La única restricción es que estos últimos deben soportar la arquitectura de hardware utilizada. De esta forma es como trabajaremos para cumplir con los objetivos.

2.4 Red Hat Enterprise Virtualization

Es un sistema de gestión de virtualización de servidores con múltiples funciones que proporciona características avanzadas para hosts y guests, entre las que se incluyen, la migración en vivo, la gestión de almacenamiento, administrador de tareas entre otros. La Figura 3 muestra una arquitectra basada en RHEV.

Figura 3. Esquema de virtualización de RHEV

La virtualización permite a los usuarios aprovechar al máximo su entorno TI permitiendo que un servidor individual ejecute varios sistemas operativos de servidores o de escritorio.

Como líder de software basado en open source empresarial, Red Hat ha ampliado la oferta en el área de la virtualización con la distribución de una alternativa de virtualización abierta para empresas.

Al virtualizar con RHEV obtenemos una sofisticada gama de ventajas como las que se muestran a continuación:

- **Sin costes iníciales**: nuestro modelo de suscripción con pago según el uso acaba con los prohibitivos costes de licencia.
- **Mejor rendimiento que cualquier producto de la competencia**: Ahora es posible virtualizar incluso las mayores cargas de trabajo empresariales.
- **Seguridad**: Security-Enhanced Linux (SELinux) de Red Hat, desarrollado en colaboración con la Agencia de Seguridad Nacional (NSA) y el Gobierno federal de EE.UU., impide las vulnerabilidades de los productos de virtualización actuales.
- **Escalabilidad**: Las implantaciones de virtualización pueden ampliarse a decenas de millares de máquinas virtuales.
- **Gestión avanzada de la virtualización**: Facilita la administración de implantaciones enormes con funciones como migración directa, alta disponibilidad, ahorro de energía, gestión del mantenimiento, y supervisión e informes de infraestructura.

2.5 Arquitectura de Virtualización

Red Hat Enterprise Virtualization para servidores es una solución completa de virtualización diseñada para permitir una virtualización extendida del centro de datos y mejorar de manera importante la eficiencia de capital y operacional.

Enterprise Virtualization se basa en la plataforma Red Hat Enterprise Linux, en la que confían millones de organizaciones de todo el mundo para sus cargas de trabajo más importantes.

2.5.1 Red Hat Enterprise Virtualization Hypervisor

Es una tecnología que está compuesta por una capa de software que permite utilizar, al mismo tiempo, diferentes sistemas operativos en varias máquinas virtuales sobre una misma computadora central. Es decir es la parte principal de una máquina virtual que se encarga de manejar los recursos del sistema principal exportándolos a la máquina virtual.

Crea una capa de la abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (guest), de tal forma que maneja los recursos de las máquinas físicas subyacentes de una manera que el usuario pueda crear varias máquinas virtuales presentando a cada una de ellas una interfaz del hardware que sea compatible con el sistema operativo elegido. En la siguiente imagen (Figura 4) se define claramente los componentes de una arquitectura de virtualización de Red Hat Enterprise Linux.

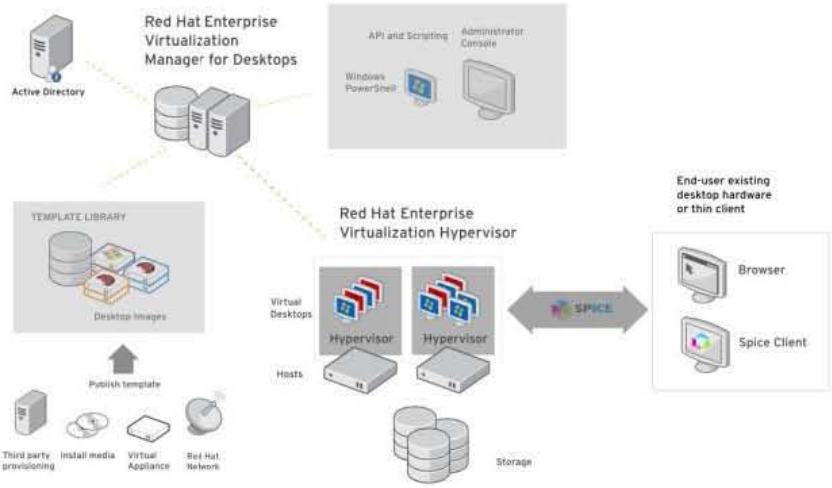


Figura 4. Arquitectura de una infraestructura RHEV

Los Hypervisores pueden clasificarse en dos tipos:

- **Hypervisor tipo 1**: También denominado nativo, unhosted o sobre el metal desnudo (bare-metal), es software que se ejecuta directamente sobre el hardware, para ofrecer la funcionalidad descrita.

- **Hypervisor tipo 2**: También denominado hosted, es software que se ejecuta sobre un sistema operativo para ofrecer la funcionalidad descrita.

En la siguiente tabla podemos observar la asignación de recursos para Hosts y guests:

Por Hypervisor

Número máximo de CPU física.	64
Máximos CPUś Lógicos	256
Máxima Memoria RAM	1TB

Por Máquina Virtual

Máximos vCPU/guest	16
Maxima RAM por Guest	64 GB
Guest soportados	RHEL3, RHEL4, RHEL5, Windows 2003, Windows 2008, Windows XP y Windows 7.
Características adicionales	Que comparten la memoria de página, la vinculación de la NIC, múltiples E / S, la administración de energía, etc.

2.5.2 Red Hat Enterprise Virtualization Manager (Consola de administración)

Es un sistema de gestión de virtualización de servidores con múltiples funciones que proporciona características avanzadas para hypervisor y máquinas virtuales, entre las que se incluyen, entre otras, la migración en vivo, la gestión de almacenamiento y el programador de sistemas.

Administrador de Máquinas virtuales RHEV-M

En un sistema de gestión de virtualización de servidores con múltiples características ofrece capacidades avanzadas para hosts y guest, incluidas las siguientes:

- Migración en vivo: Permite mover máquinas virtuales de un anfitrión al otro mientras están en funcionamiento sin afectar el rendimiento.

- Alta Disponibilidad Ante la falla de un host, garantiza que las máquinas virtuales críticas para el funcionamiento de la empresa sean reiniciadas en otro anfitrión.

- Administrador de mantenimiento: Permite actualizar y realizar el mantenimiento de anfitriones durante el funcionamiento de las máquinas virtuales.

- Administrador de imágenes: Permite el almacenamiento en disco según las necesidades actuales (thin provisioning) y el uso de plantillas para construir rápidamente nuevas máquinas virtuales a partir de configuraciones estándar.

- Planificador de Sistemas: Permite a Red Hat Enterprise Virtualization Manager migrar máquinas virtuales entre múltiples host para equilibrar las cargas de trabajo.

- Ahorro de energía: Permite a Red Hat Enterprise Virtualization Manager consolidar las máquinas virtuales en una cantidad menor de guest en horas de baja demanda y desactivar aquellos que no sean necesarios.

- Interfaz de Usuario de Búsqueda

- Entorno de Gestión Uniforme para Servidores y Escritorios

2.5.3 Almacenamiento

Un centro de datos se basa en el almacenamiento físico adecuado y accesible. La agrupación de almacenamiento proporciona una visión abstracta del almacenamiento físico asignado a un centro de datos, que permite a los planificadores y los administradores supervisar y gestionar fácilmente los requisitos de almacenamiento.

La agrupación de almacenamiento es una entidad lógica que contiene una imagen independiente depósito de un cierto tipo, ya sea iSCSI (Internet Small Computer System Interface) o FC (Canal de Fibra), o NFS (Network File System). Cada grupo de almacenamiento puede contener varios dominios de almacenamiento, para la máquina virtual de imágenes de disco y de imágenes ISO y para la importación y exportación de imágenes de máquinas virtuales.

Para muchas empresas pequeñas, el éxito radica en sus datos. Ya no se pueden permitir confiar su información a dispositivos cliente locales y copias de seguridad expresas. Por este motivo muchas pequeñas empresas están adoptando una estrategia de almacenamiento que se enfoca en dispositivos de almacenamiento en red centralizados que no sólo resultan robustos y escalables, sino que además se pueden gestionar por personal interno con conocimientos limitados de TI.

A continuación veamos algunas tecnologías dedicadas a compartir la capacidad de almacenamiento a través de una red.

2.5.3.1 SAN

Una red SAN (Storage Area Network) se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA, SATA y SCSI. En otros métodos de almacenamiento, (como SMB o NFS). La mayoría de las SAN actuales usa el protocolo SCSI para acceder a los datos de la SAN, aunque no usen interfaces físicas SCSI. Este tipo de redes de datos se han utilizado y se utilizan tradicionalmente en grandes main frames como en IBM, SUN o HP.

Una SAN es una red de almacenamiento dedicada que proporciona acceso de nivel de bloque a LUNs. Una LUN, o número de unidad lógica, es un disco virtual proporcionado por la SAN. El administrador del sistema tiene el mismo acceso y los derechos a la LUN como si fuera un disco directamente conectado a la misma. El administrador puede particionar y formatear el disco en cualquier modo que él elija.

Dos protocolos de red utilizados en una SAN son Fibre Channel e iSCSI. Una red de canal de fibra es muy rápida y no está agobiada por el tráfico de la red LAN de la empresa. Sin embargo, son bastante costosas También requieren switches especiales de canal de fibra. iSCSI es una nueva tecnología que envía comandos SCSI (Small Computer System Interface) sobre una red TCP / IP. Este método no es tan rápido como una red Fibre Channel, pero ahorra costos, ya que utiliza un hardware de red menos costoso.

2.5.3.2 NAS

Network Attached Storage es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un Servidor con ordenadores personales o servidores clientes a través de una red, haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar que un servidor Windows que comparte sus unidades por red es un sistema NAS, pero la definición suele aplicarse a sistemas específicos.

Los protocolos de comunicaciones NAS son basados en ficheros por lo que el cliente solicita el fichero completo al servidor y lo maneja localmente, están por ello orientados a información almacenada en ficheros de pequeño tamaño y gran cantidad. Los protocolos usados son protocolos de compartición de ficheros como NFS, Microsoft Common Internet File System (CIFS).

Muchos sistemas NAS cuentan con uno o más dispositivos de almacenamiento para incrementar su capacidad total. Normalmente, estos dispositivos están dispuestos en RAID (*Redundent Arrays of Independent Disks*) o contenedores de almacenamiento redundante mostrados en la figura 5.

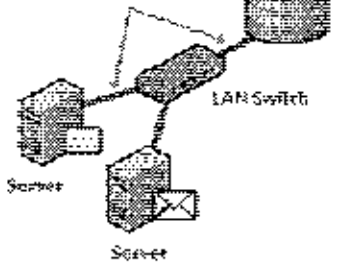


Figura 5. Red de almacenamiento compartido por NAS

2.5.3.3 iSCSI

Significa Internet SCSI (Small Computer System Interface), un protocolo de almacenamiento basado en el estándar IP, que permite el transporte de comandos SCSI sobre redes IP.
iSCSI es uno de los protocolos fundamentales que están dando más impulso a las redes de almacenamiento, ya que su costo es muy reducido y se puede optimizar mediante tarjetas aceleradoras en los servidores, estas permiten mejorar el rendimiento entre el servidor y la unidad de almacenamiento.

Una arquitectura de iSCSI se puede observar en la siguiente imagen (Figura 6).

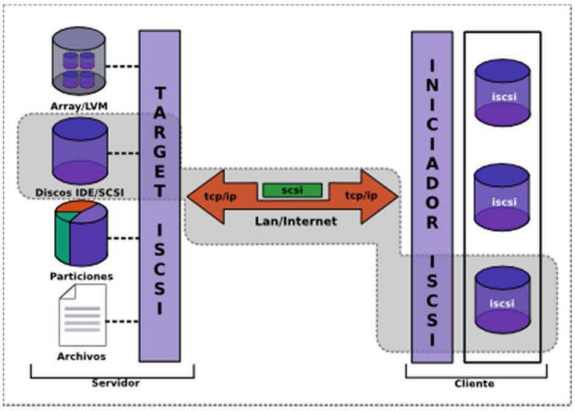


Figura 6. Diseño de almacenamiento compartido por iSCSI

¿Por qué usar iSCSI?

Actualmente iSCSI (internet Small Computer System Interface) es una seria competencia a FC (fiber Channel), podemos conseguir velocidades de acceso de hasta 10GB con iSCSI dependiendo de la velocidad de transferencia de la red Lan (switches y tarjetas de red de los servidores). Actualmente iSCSI es mucho más económica que FC por los costes de fibra óptica a comparación de sólo utilizar el cable UTP que se utiliza para la comunicación de la red con el servidor.

iSCSI es una extensión de SCSI, no es nada más que un protocolo de comunicaciones que puede ser utilizado en dispositivos físicos conectados a un host o servidor. En iSCSI los comandos que manejan el dispositivo se envían a través de la red trabajando en el sistema operativo como si los discos fueran SCSI, es decir, tramas y envío y recepción de paquetes.

iSCSI es una manera muy sencilla de poder compartir recursos de almacenamiento mediante un servidor iscsi, sólo con tener el suficiente espacio se pueden repartir los recursos en LUN (Logical Unit Number) por servidor.

En la siguiente imagen se muestra la trama del protocolo ISCSI:

Figura 7. Trama ISCSI

2.5.3.4. NFS

NFS (Network File System), este protocolo permite a las máquinas montar particiones en un sistema remoto en concreto y usarlas como si estuvieran en el sistema de archivos local. Esto permite centralizar archivos en una localización, mientras se permite su acceso continuo a los usuarios autorizados.

Hay dos versiones de NFS actualmente en uso. La versión 2 de NFS (NFSv2), que tiene varios años, es ampliamente soportada por muchos sistemas operativos. La versión 3 (NFSv3) tiene más características, incluyendo tamaño variable del manejador de archivos y una mejor información de errores. Red Hat Linux soporta tanto NFSv2 como NFSv3, y usa NFSv3 por defecto cuando se conecta a un servidor que lo soporta.

La versión 2 de NFS usa el *User Datagram Protocol (UDP)* para proporcionar una conexión de red sin estado entre el cliente y el servidor. La versión 3 de NFS puede usar UDP o TCP corriendo sobre una IP. La conexión UDP sin estado minimiza el tráfico de red, al mandar el servidor NFS una cookie al cliente, después de que el cliente sea autorizado a acceder al volumen compartido. Esta cookie es un valor aleatorio guardado en la parte del servidor y es pasado junto con las peticiones RPC desde el cliente. El servidor NFS puede ser reiniciado sin afectar a los clientes y las cookies permanecen intactas.

En la siguiente imagen (Figura 8) se muestra como se comparten los sistemas de archivo mediante el protocolo de NFS, donde se comparten mediante un servidor de NFS, en capítulos posteriores se mostrará cómo se debe realizar la configuración para poder compartir sistemas de archivos.

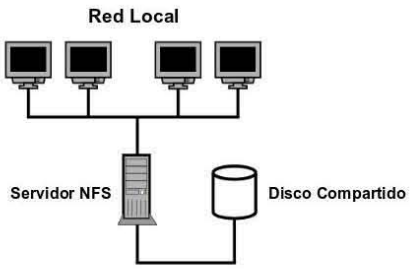


Figura 8. Diagrama de almacenamiento compartido por NFS

2.5.4 Tipos de conexión Fiber Channel

Existen dos tipos de conexión de Fiber Channel la de fibra pura que es mediante cables de fibra y la que se trabaja mediante las tramas de fiber Channel Over Ethernet. Estas se detallan en los siguientes subcapítulos:

2.5.4.1 Fiber Channel

Fiber Channel es un medio de comunicación de alta velocidad utilizado para tener acceso a la información de una manera más rápida. Comúnmente utilizada por SAN (Storage Area Network) por gran transferencia de la información qué van de 4Gb/seg y 8Gb/seg dando así resultados óptimos y números de transferencia de datos mucho más veloz que conexión SATA o por cable de red.

FC puede operar sobre cable y sobre fibra óptica a distancias de hasta 10 Kms sin uso de repetidores. Las Clases de Servicio incluyen servicios orientados a conexión (conmutación de circuitos) y orientados a no conexión (conmutación de paquetes), pudiendo elegir combinaciones con notificación y sin notificación de entrega, circuitos virtuales con reserva de ancho de banda y especificación de latencia máxima (QoS) y funciones de multicast, broadcast y hunt groups.

En la siguiente imagen (figura 9) se muestra cómo debe conectarse la fibra para tener alta disponibilidad de los sistemas de archivos, En la imagen se muestra que por cada servidor se conectan dos fibras para conectarlas en diferentes Switches de Fibra los cuales van conectados a los discos, donde se encuentran alojados los sistemas de archivos, LUN's.

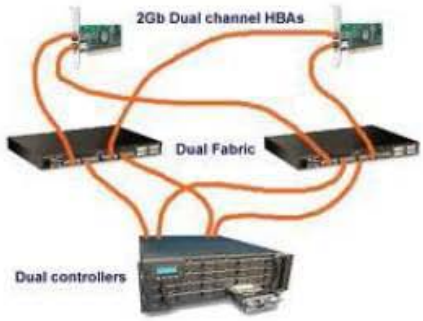


Figura 9. Diagrama de almacenamiento con FC

2.5.4.2 FCoE (Fiber Channel Over Ethernet)

Fiber Channel over Ethernet es el protocolo que encapsula los frames (etiquetas de Fiber Channel dentro de paquetes Ethernet que otorgan la capacidad de unificar la conectividad y el flujo de información en un servidor.

Con tecnología de FCoE, con un solo adaptador (CNA) que soporte el trafico de LAN y SAN.

La premisa subyacente de FCoE es consolidar los procesos de I/O permitiendo la coexistencia de distintos tipos de tráfico en la misma conexión, lo que reduce y simplifica el cableado, reduce el número de adaptadores necesarios en cada host y los requisitos de alimentación.

Ventajas de Fiber Channel over Ethernet

- Consolidación de I/O
- Mejor desempeño (lossless likes)
- Escalabilidad excepcional de las velocidades en Ethernet (1 y 10Gb)
- Reducción de adaptadores, dispositivos y cables
- Simplifica la administración de las operaciones de IT
- Protege la inversión de la actual infraestructura

La forma de una correcta interconexión de fiber cannel over Ethernet se muestra en el siguiente diagrama (Figura 10), donde se muestra la redundancia y configuración necesaria.

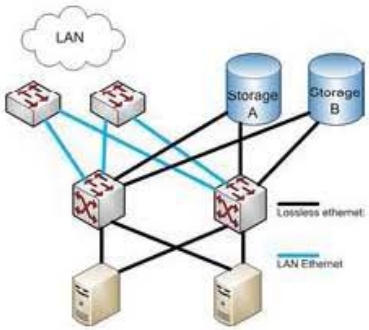


Figura 10. Diagrama de almacenamiento compartido por FCoE

2.6 Alta disponibilidad (High Availability)

Un Clúster de Alta disponibilidad, o de "Misión crítica", es un conjunto de dos o más servidores que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizados entre sí.

De un clúster se espera que presente combinaciones de los siguientes servicios:

1. Alto rendimiento
2. Alta disponibilidad
3. Equilibrio de carga
4. Escalabilidad

Es una solución accesible, confiable y fácil de utilizar que garantiza la alta disponibilidad de las aplicaciones que se ejecutan en las máquinas virtuales. En caso de fallo de un servidor físico, las máquinas virtuales afectadas se reinician automáticamente en otros servidores de producción con capacidad adicional. En caso de fallo del sistema operativo, en el caso de RHEV reinicia la máquina virtual afectada en el mismo servidor físico. Permitiendo a las organizaciones seleccionar y obtener fácilmente el nivel de disponibilidad requerido para todas las aplicaciones críticas.

Una correcta configuración para tener alta disponibilidad es necesario contar siempre con dos rutas para llegar al mismo destino, así como también para tener alta disponibilidad es contar con un mismo sistema de forma pasiva que trabajará al momento que falle el sistema Activo como lo muestra la siguiente figura (Figura 11).

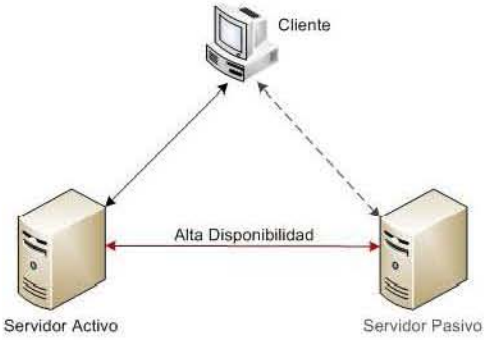


Figura 11. Diagrama de alta disponibilidad con cluster

2.6.1 Bonding de tarjetas

Permite a los administradores de red vincular múltiples interfaces juntas en un único canal usando el módulo del kernel bonding y una interfaz de red especial llamada la interfaz de unión de canales. Vinculación de canales permite dos o más interfaces de red para actuar como una, incrementando simultáneamente el ancho de banda y proporcionando redundancia.

El channel bonding o *unión de interfaces de red* consiste en simular un dispositivo de red con gran ancho de banda uniendo varias tarjetas de red independientes, de manera que las aplicaciones sólo verán una interfaz de red como se ve en la Figura 11.

Las ventajas de utilizar Channel Bonding

- **mayor ancho de banda**: el ancho de banda de la interfaz virtual será la suma de los anchos de banda de las interfaces reales.

- **balanceo de carga**: tendremos balanceo de carga del tráfico de red entre todas las interfaces reales (por defecto Round Robin).

- **redundancia**: si falla una tarjeta de red los datos irán sólo por las que estén en buen estado.

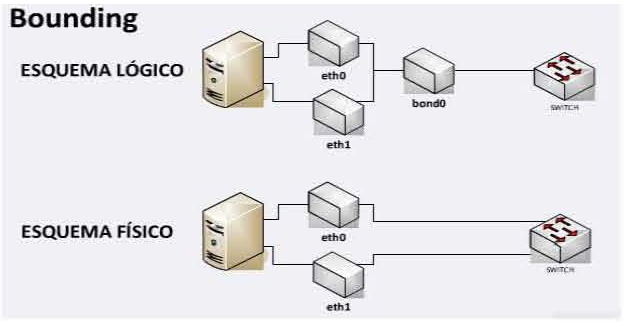


Figura 11. Bounding de tarjetas

2.6.2 Configuración de Taggeo

El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Esta tecnología es utilizada básicamente para el uso de diferentes Switches Virtuales y repartirlos sobre distintas VLAN y así poder distribuir el tráfico y máquinas virtuales, para tener una mejor administración y seguridad en la RED. Al poder separar los servicios de los usuarios cómo se hace normalmente con infraestructura física (figura 12).
Para poder utilizar dichos beneficios es necesario tener los cables de los hypervisores se encuentren trunkales para poder pasar el tráfico de cualquier VLAN sobre los cables sin problema, además de conocer la etiqueta de cada VLAN para poder crearlas en la administración de RHEV.

En la Figura 12 se muestra un diagrama del funcionamiento de tagging de tarjetas en una infraestructura virtualizada.

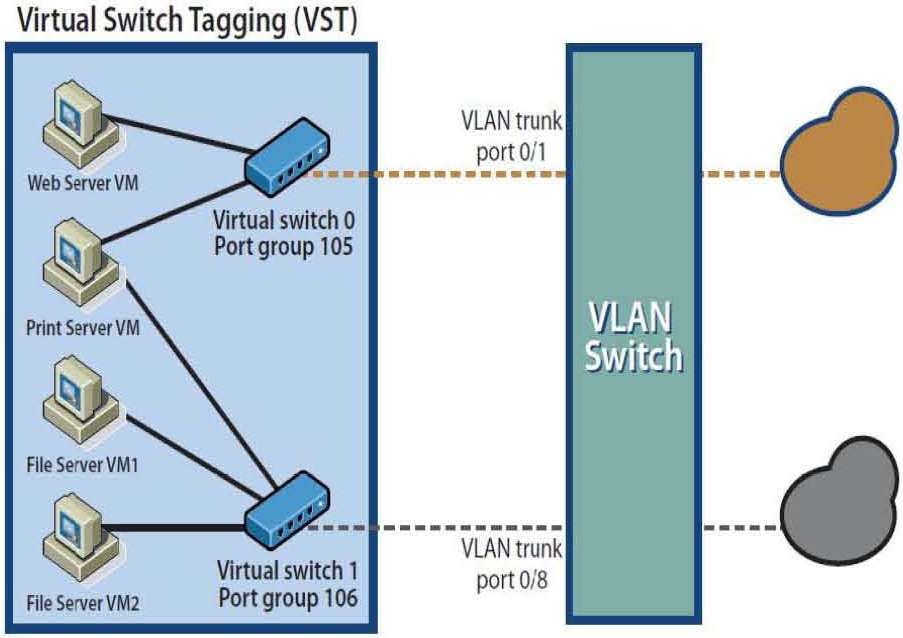


Figura 12. Taggeo de switchs virtuales

2.6.3 Multipath

Multipathing es el uso de componentes de red de almacenamiento responsables del proceso de transferencia de datos entre el servidor y el almacenamiento. Estos componentes incluyen cables, adaptadores, interruptores y el software que permite esta característica. Ello además permite el poder acceder a una serie de recursos de forma simultánea, para cierto tipo de dispositivos como iSCSI es necesaria la activación de este modo de acceso.

Multi-path es una técnica muy utilizada para conectar un servidor a un dispositivo de almacenamiento con dos conexiones en lugar de una. Esto proporciona una vía alternativa de conexión en caso de fracaso de este modo permite una mayor disponibilidad del almacenamiento ante un fallo y una alternativa de acceso a la misma. También proporciona hasta el doble de datos en entornos de gran acceso a los mismos y ofrece capacidad de balanceo de carga para maximizar el uso de cada una de las rutas asignadas.

En el uso de multipath es necesario contar con doble ruta para llegar a nuestra SAN como se muestra a continuación en la figura número 13.

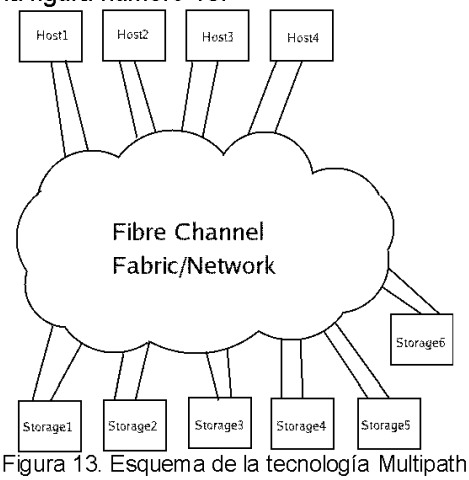


Figura 13. Esquema de la tecnología Multipath

2.7 Monitoreo

Dado que la tendencia natural de una red cualquiera es a crecer, conforme se añaden nuevas aplicaciones y cada vez más usuarios hacen uso de la misma, los sistemas de gestión empleados han de ser lo suficientemente flexibles para poder soportar los nuevos elementos que se van añadiendo, sin necesidad de realizar cambios drásticos en la misma.

Este punto, el de gestión de red, es uno de los más controvertidos en informática, ya que, prácticamente, no existe una solución única, aceptada por todos y que sea fácilmente implantable. Las soluciones existentes suelen ser propietarias: Netview de IBM, OpenView de HP, etc., lo que hace que en una red compleja, formada por equipos multifabricantes, no exista un único sistema capaz de realizar la gestión completa de la misma, necesitándose varias plataformas, una por cada fabricante, lo que dificulta y complica enormemente la labor del administrador de red de red.

Con la idea de presentar una solución única, válida para cualquier tipo de red, varios grupos de normalización están trabajando en ello y, aunque hay dos tendencias claras (SNMP (simple network management protocol) para redes de empresa y CMIS/CMIP para redes públicas), sólo SNMP es la que ha conseguido una aceptación e implantación amplia, a lo que ha contribuido su sencillez y rapidez de desarrollo.

Veamos a continuación que protocolos se utilizan actualmente para la gestión y monitorización de dispositivos de red.

2.7.1 Protocolos de gestión y control

Durante las primeras décadas las redes fueron usadas por investigadores para el envío de correo electrónico y por empleados corporativos para compartir recursos, en estas condiciones la seguridad no era un factor importante, no recibió mucha atención, hoy día aparece en el horizonte como un problema potencial de grandes proporciones; para atacar este problema las soluciones deben implementarse desde la capa de aplicación.

La capa de aplicación utilizará los servicios de la capa extremo – extremo, pasando datos y esta interfaz se repite entre las capas, la arquitectura TCP/IP no exige que se haga uso de todas las capas, sino que es posible desarrollar aplicaciones que invoquen directamente los servicios de cualquier capa, algunas de estas aplicaciones, como el protocolo sencillo de gestión de red(SNMP, Simple Network Management Protocol), utilizan un protocolo extremo-extremo alternativo denominado protocolo de datagrama de usuario (UDP).

Las redes son de una importancia crítica y creciente, una red no se puede instalar y gestionar sólo con el esfuerzo humano y en respuesta a ello se trata la gestión de redes que cubre los servicios, protocolo y la base de información de gestión

Un sistema de gestión de red es una herramienta para monitorear y controlar la red, diseñado para ver la red entera como una arquitectura unificada, con direcciones y etiquetas. Las estaciones de gestión y el agente (equipos) están enlazados por el protocolo de gestión de red, un protocolo SNMP, proyectado para redes basadas en OSI y en TCP/IP.

2.7.1.1 SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

Componentes básicos

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados
- Agentes
- Sistemas administradores de red (NMS's)

Un **dispositivo administrado** es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadoras, servidores o impresoras.

Un **agente** es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etc.), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un **NMS** ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

Comandos básicos

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: **lectura**, **escritura**, **notificación** y **operaciones transversales**.

El **comando de lectura** es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El **comando de escritura** es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

El **comando de notificación** es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

Base de información de administración SNMP (MIB)

Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red, como SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un identificador de objeto (*object ID*) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.

Los identificadores de los objetos ubicados en la parte superior del árbol pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas.

Los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama experimental.

Mensajes SNMP

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

2.7.1.2 SSH

SSH (Secure Shell) es un programa para conectarse a otros equipos a través de una red, para ejecutar comandos en una máquina remota y para mover archivos de una máquina a otra. Proporciona una exhaustiva autenticación y comunicaciones seguras en redes no seguras.

SSH provee fuerte autenticación y comunicación segura sobre un canal inseguro y nace como un reemplazo a los comandos telnet, ftp, rlogin, rsh, y rcp, los cuales proporcionan gran flexibilidad en la administración de una red, pero sin embargo, presenta grandes riesgos en la seguridad de un sistema. Adicionalmente, SSH provee seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP.

Para la autentificación, SSH se puede utilizar algoritmo de cifrado como RSA o DSA. Para el envío de datos a través de la red, usa 3DES, IDEA, Blowfish, etc.

Soporta ambas versiones del protocolo SSH, la 1 y la 2. Dependiendo de cuál usemos los métodos de autentificación, son distintos.

2.7.1.3 WMI

Otro protocolo de administración es el Instrumental de administración de Windows (WMI, *Windows Management Instrumentation*) es la implementación de Microsoft de WBEM, una iniciativa que pretende establecer normas estándar para tener acceso y compartir la información de administración a través de la red de una empresa. WMI cumple con WBEM y proporciona compatibilidad integrada para el Modelo de información común (CIM -Common Information Model), que describe los objetos existentes en un entorno de administración.

WMI incluye un repositorio de objetos compatible con CIM, que es la base de datos de definiciones de objetos, y el Administrador de objetos CIM, que controla la recopilación y manipulación de objetos en el repositorio y reúne información de los proveedores de WMI. Los proveedores de WMI actúan como intermediarios entre los componentes del sistema operativo, las aplicaciones y otros sistemas. Por ejemplo, el proveedor del Registro extrae su información, mientras que el proveedor de SNMP proporciona datos y sucesos de los dispositivos SNMP. Los proveedores proporcionan información acerca de sus componentes, y podrían proporcionar métodos para manipular los componentes, las propiedades que se pueden establecer, o los sucesos que le pueden alertar de las modificaciones efectuadas en los componentes.

Las herramientas de administración de equipos, como Microsoft Systems Management Server, WMI nos ayuda a administrar nuestros equipos. WMI también se utiliza en otras tecnologías y herramientas de Microsoft, como Microsoft Health Monitor y Microsoft Operations Manager, y también lo utilizan otros fabricantes de sistemas de administración de equipos. Podemos utilizar WMI con sistemas de programación o de secuencias de comandos (como Windows Script Host) para obtener información de configuración acerca de la mayor parte de los aspectos de los sistemas informáticos, incluidas las aplicaciones de servidor, o para realizar cambios en los mismos.

Se han habilitado varias herramientas administrativas WMI, incluidas Propiedades del sistema, Información del sistema y el componente Dependencias de Servicios. A continuación se incluimos una breve descripción de estos componentes:

- La herramienta Propiedades del sistema permite ver y cambiar las propiedades del sistema de un equipo local o remoto. Podemos reiniciar un equipo remoto para aplicar cambios de configuración o detectar hardware nuevo, ver el nombre del equipo e información del dominio de otros equipos de la red o cambiar la configuración del archivo de paginación de memoria virtual de un equipo que podría ejecutar programas que requieren mucha memoria.

- La herramienta Información del sistema recopila y muestra la información de configuración del sistema. Esto resulta especialmente útil a los técnicos de soporte para solucionar los problemas de los sistemas.

- La herramienta Servicios ayuda a administrar los servicios del equipo. Las dependencias de Servicios identifican los servicios de los que depende el servicio actual y los que dependen de éste.

2.7.2 Zenoss

Es una alternativa libre, un proyecto que permite una implementación sencilla de su sistema, y que aporta a la reducción de los costos empresariales, para estas tareas de monitoreo. Sus aracterísticas son escalabes, como veremos más adelante, esta es una suite muy completa que facilita el trabajo de los usuarios, y que trabaja nutriéndose de los aportes y sugerencias que estos puede brindar.

2.7.2.1 Componentes de la solución

2.7.2.2 Arquitectura Zenoss

Entender el diseño arquitectónico de un sistema es extremadamente útil para la comprensión de las necesidades funcionales y de diseño en un producto. Los dos elementos clave de la arquitectura son su diseño de cuatro niveles y la gestión basada en modelos. Juntos, estos dos elementos proporcionan escalabilidad que permite la gestión de decenas de miles de dispositivos.

2.7.2.3 Diseño de cuatro niveles

La arquitectura de Zenoss es un "sistema con diseño de cuatro niveles. Los elementos de cada nivel pueden ser desplegados en varias instancias de apoyo a escala, seguridad, y la separación de las necesidades que se encuentran distribuidas en el complejo de las organizaciones, a continuación se mencionan dichos niveles.

2.7.2.3.1 Global Dashboard

Global Dashboard ofrece vistas consolidadas a través de varias implementaciones independientes de Zenoss. Para entornos con un número muy elevado de dispositivos, o cuando las necesidades empresariales requieren un aislamiento completo de cada área de monitoreo.

El Global Dashboard es una aplicación web que colecta eventos y datos cada servidor Zenoss asociado. La información detallada permanece almacenada en cada Zenoss independiente, desde Global Dashboard, basta con hacer clic a través de Zenoss para investigar un conflicto.

2.7.2.3.2 Capa de presentación (Browsers)

La interfaz web de Zenoss combina funciones administrativas y de reportes en una sola aplicación web.

Varios operadores, de forma segura con vistas personalizadas, pueden:

• Supervisar el status por el sistema de negocios, ubicación geográfica o ver la lista de dispositivos.
• Trabajar con información precisa del dispositivo actual, incluyendo rendimiento, disponibilidad y la configuración del mismo.
• Monitorear, rastrear y responder a conflictos.
• Crear y ejecutar informes analíticos.
• Configurar, aplicar y personalizar las plantillas de monitoreo.

• Definir nuevos usuarios de Zenoss y definir el control de acceso.

2.7.2.3.3 Capa de lógica de negocio

La capa de lógica de negocio se puede considerar como una aplicación Web, un daemon de proceso y tres bases de datos. Estos pueden ser implementados en un solo servidor o distribuidos en varios servidores en ambientes de trabajo muy grandes.

Aplicación Web.
La aplicación Web se construye utilizando una colección de tecnologías de código abierto y se conoce como Zope. Zope fue elegido por su facilidad de administración, bases de datos de objetos y un modelo de seguridad excelente.

En general, Zope es compatible con la capa de usuario, está diseñado para manejar grandes bases de datos y un buen rendimiento incluso cuando se manipulan miles de objetos.

Process Daemon
Process Daemon administra la comunicación entre las capas de colección y de datos, y ejecuta las tareas de administración de los dispositivos iniciadas por los usuarios. Este demonio puede ser replicado en múltiples servidores para aumentar la escalabilidad o para responder a las necesidades particulares de la empresa según su diseño de red.

2.7.2.3.4 Capa de colección

Zenoss utiliza la función de administración nativa de cada dispositivo.
La capa de colección sin agentes de Zenoss comprende los servicios que recogen y alimentan de información a la capa de datos. Estos servicios se proporcionan por varios demonios que realizan el modelado, monitoreo y funciones colección de eventos. El sistema utiliza los protocolos **SNMP, SSH y WMI** para recopilar información de los servidores remotos.
El diseño multi-daemon proporciona flexibilidad para la distribución y la recopilación de datos.

2.7.2.4 Administración basada en modelado

Otro elemento clave de la arquitectura Zenoss es su diseño basado en modelado. El modelado permite un uso fácil y consistente de las políticas de monitoreo (figura 14).

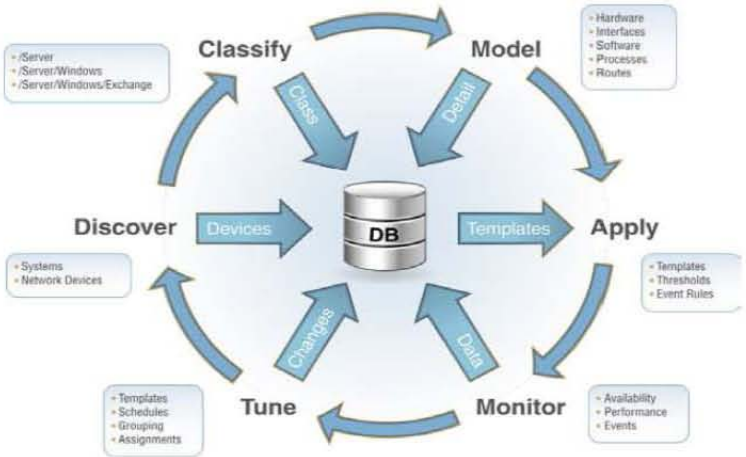


Figura 14. Arquitectura Zenoss

Descubrimiento

Zenoss llena su base de datos con dispositivos que descubre a través de un rango de direcciones IP dado. O puede optar por llenar la base de datos con las listas de sus propios dispositivos. Esto es útil cuando se optar por elegir dispositivos específicos para monitorear.

Clasificación

Podemos elegir una clasificación para cada dispositivo individual o por medio de selección múltiple. Al clasificar un dispositivo, Zenoss elije que tipo de monitoreo aplica al dispositivo. Por supuesto, se puede volver a clasificar a un dispositivo en cualquier momento.

Modelo

Una vez que Zenoss conoce la clasificación de un dispositivo, entiende cómo recoger la información detallada de ese dispositivo. La información se recoge de forma específica para cada clase de dispositivo. Por ejemplo, se utiliza SNMP para los dispositivos de redes, WMI para máquinas Windows y la API VI para servidores VMware ESX. Una vez recogidos los datos se almacenan en la base de datos de administración de la configuración.

Aplicación

Con una comprensión de la clasificación del dispositivo y su modelo, Zenoss asegura que cada dispositivo se controla adecuadamente dispositivos.

Monitoreo

Zenoss recibe, procesa y administra el almacenamiento de datos para todos los dispositivos monitoreados y los guarda en la correspondiente base de datos de Zenoss. Los datos recogidos se procesan mediante reglas de extracción de datos. Por ejemplo, los datos de rendimiento se normalizan de manera que los valores que deben estar representados en porcentajes son almacenados en forma de porcentajes, independientemente de la magnitud real de la métrica.

Afinación

Aunque Zenoss funciona muy bien sin ajustes especiales, sin duda, deseamos hacer las operaciones más parecidas a nuestras necesidades.
Podemos ajustar el modelado y por lo tanto el comportamiento de Zenoss, mediante la adición de grupos de dispositivos y configuración de propiedades. Podemos recoger diferentes datos de rendimiento o definir nuevas reglas de eventos, ya sea para una clase de dispositivo o sólo para un solo dispositivo.

Manejo de dispositivos

Zenoss actualmente administra redes tan grandes como 32 mil dispositivos.
Los componentes de la arquitectura Zenoss de cuatro capas se pueden implementar de varias maneras para satisfacer diferentes necesidades.
También se puede optar por distribuir la base de datos de eventos a un servidor independiente para cumplir con políticas de retención prolongada, manejo de volúmenes muy grandes de eventos, etc.

En la figura 15 y 16, se muestran los componentes y distribución de Zenoss Enterprise Server con relación del Distributed Collector

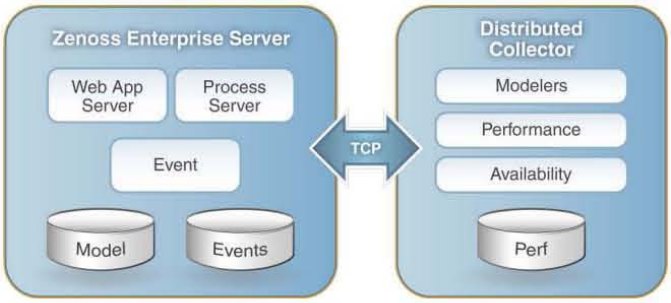


Figura 15. Distribución de Zenoss

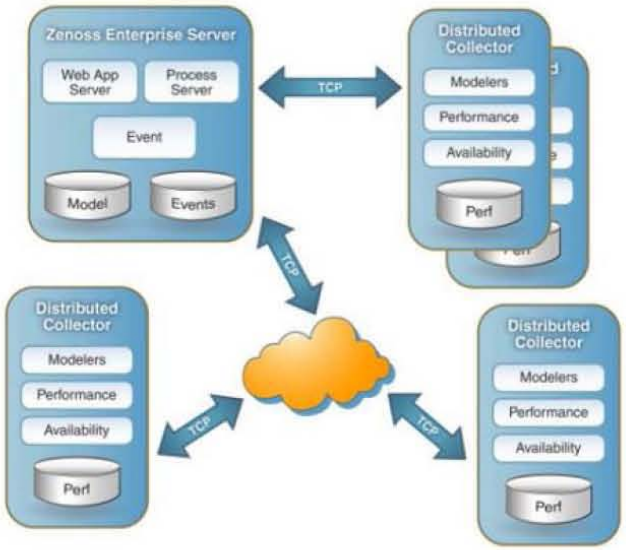


Figura 16. Distribución de Zenoss

En las redes más grandes con decenas de miles de dispositivos, Zenoss proporciona Global Dashboard para el monitoreo de múltiples servidores.

Completo conocimiento operacional

Zenoss incluye un conjunto de funcionalidades de administración de sistemas de TI:

- Descubrimiento de dispositivos e inventario
- Supervisión de disponibilidad y rendimiento
- Gestión de eventos y fallas
- Alertas y reparación
- Generación de informes
- Detección de cambios

Descubrimiento, modelado y detección de cambios

Zenoss automatiza la gestión de los procesos de detección de dispositivos, seguimiento y detección de cambios. Las características incluyen:

•Detección automática de componentes de TI

• Detección de cambios en la infraestructura (nuevos dispositivos, eliminar, mover dispositivos)
• Detección de cambios de configuración de dispositivos (drivers, versiones de software, software instalado, sistema operativo, etc.

• Muestra una topología de red con todos los dispositivos administrados y servidores
• Actualización automática de la configuración de la base de datos y el mapa de cambios.

Administración Modelo-Base

El descubrimiento es sólo el primer paso en Zenoss. Después, los dispositivos a través del motor de modelado se inicializa un seguimiento de información configuración, basado en el tipo de dispositivo (servidor de aplicaciones, correo electrónico, etc):
• Las plantillas de informes especifican y muestran las correctas métricas de rendimiento
• Despliegue rápido con descubrimiento automatizado, modelado, y supervisión de instalación
• Especificaciones de configuración y software instalado
• Ofrece una cobertura más completa en la misión crítica de la infraestructura

Monitoreo de Disponibilidad

Monitorizando proactivamente la disponibilidad y el rendimiento de los componentes de infraestructura, ayuda a minimizar las interrupciones y optimizar el rendimiento.

• Un "heartbeat" activo supervisa y comprueba regularmente cada dispositivo gestionado, servidor y servicios para asegurar que todo está funcionando como se esperaba.

• Múltiples protocolos se comprueban para cada dispositivo

- ICMP
- Procesos de Windows
- SNMP
- Servicios de Windows
- Linux / Unix procesos
- TCP / IP (HTTP, SMTP, etc)
- Puertos TCP / IP

• Los gráficos de rendimiento muestran el uso de recursos, rendimiento, y el rendimiento general de cualquier dispositivo, servicio o aplicación.

• Permite a los operadores realizar un análisis para determinar la causa de un problema directamente desde la pantalla de presentación de informes

Monitoreo de "Performance"

• Disponibilidad e información de estado de rendimiento se representa por: Rojo (Crítica), Orange (error), amarillo (advertencia), verde (OK)

• El tablero de instrumentos incluye un mapa de Google para ver geográficamente el estado de la toda la infraestructura de TI

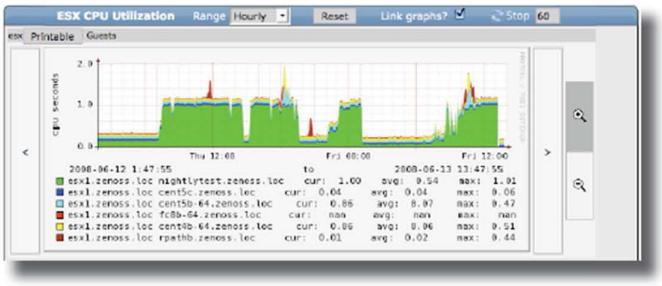
Los gráficos de rendimiento muestran el uso de recursos y el rendimiento general de cualquier dispositivo, servicio o aplicación.

• Los informes de rendimiento personalizados cuenta de todos los datos pertinentes a un dispositivo en una sola pantalla

• Permite a los operadores realizar análisis de la causa del problema, directamente en la pantalla de presentación de informes

• Los Umbrales definidos automáticamente dan alerta basados en el estándar de funcionamiento rendimiento

Un ejemplo de los umbrales y gráficas que muestra zenoss se muestra en la siguiente imagen (Figura 17).



Performance Graphs (live or historical) can include data from one device or as many as desired by the operations team

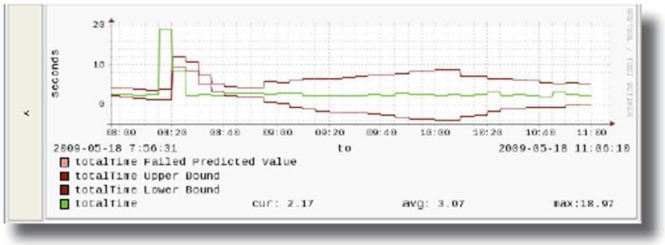


Figura 17. Umbrales de Zenoss

Los eventos ocurren la mayor parte del tiempo, incluso cuando se trata de la supervisión del rendimiento.
Una consola central integra eventos, fallas, errores, y alertas de todos los sistemas y todas las fuentes en una sola pantalla. La coordinación de eventos de consola ofrece una visibilidad completa de todos los eventos en todo el sistema, así como la funcionalidad clave para hacer frente a los errores, eventos y fallas más eficientemente durante el día.

Eventos y Gestión de Fallas

• Hora de inicio, contadores, y mucho más, en varios eventos permiten a Zenoss eliminar las descripciones múltiples para la misma causa.

• Cuando un asunto se trata o resuelve, un evento se convierte en “CLEAR" estado (verde), fundamental para la integración con soluciones de Help Desk

• Zenoss proporciona un informe de "Todos los dispositivos”, una visión instantánea del estado de cada dispositivo en la infraestructura.
• Los informes interactivos en tiempo real se pueden ordenar por atributo
• Informes de disponibilidad y rendimiento de todos los dispositivos

• El personal de operaciones puede hacer clic en el dispositivo específico y obtener información en pantalla para determinar el origen de la causa

¿Qué podemos monitorear con Zenoss Core?

- Dispositivos de Red
- Linux
- UNIX
- Windows
- Solaris
- Impresoras
- UPS
- Consultas HTTP, entre otros.

2.8 Escritorios Remotos Virtuales

Los escritorios remotos son una solución bastante atractiva para las empresas para poder controlar la información de cada escritorio de sus empleados y de esta manera poder centralizar la información en un centro de datos, con la finalidad de poder cumplir con las políticas de las tecnologías de la información, que solicitan tener la información en sitio y no tener problemas con auditorias.

A continuación se define cada concepto de escritorios remotos:

2.8.1 ¿Qué son los escritorios remotos Virtuales?

La Virtualización del escritorio ofrece oportunidades nuevas y llenas de potencial para que los TI puedan ofrecer y administrar escritorios corporativos y puedan responder a las diversas necesidades de los usuarios de una forma flexible. Los escritorios virtualizados pueden estar alojados en el cliente, o centralizados en servidores en el centro de datos; lo que a menudo se conoce como una Infraestructura de escritorio virtual (VDI).

La virtualización del escritorio alojada en cliente crea un entorno de sistema operativo independiente en el escritorio lo que hace posible que las aplicaciones de línea de negocio o aquellas que no son compatibles puedan funcionar dentro de su propio entorno sobre un sistema operativo más ligero o permitan que dos entornos TI (por ejemplo, uno personal y otro corporativo) se ejecuten de manera concurrente en el mismo dispositivo físico. La infraestructura de escritorio virtual (VDI) es un modelo que hace posible que las cargas de trabajo de escritorio del cliente (sistema operativo, aplicaciones, datos de usuario) se alojen y ejecuten en servidores del centro de datos. Los usuarios pueden comunicarte con sus escritorios virtuales a través de un dispositivo cliente que ofrece soporte para protocolos de escritorio remoto tales como el RDP.

En la siguiente figura (Figura 18), se muestra la arquitectura de virtualización de escritorios remotos virtuales.

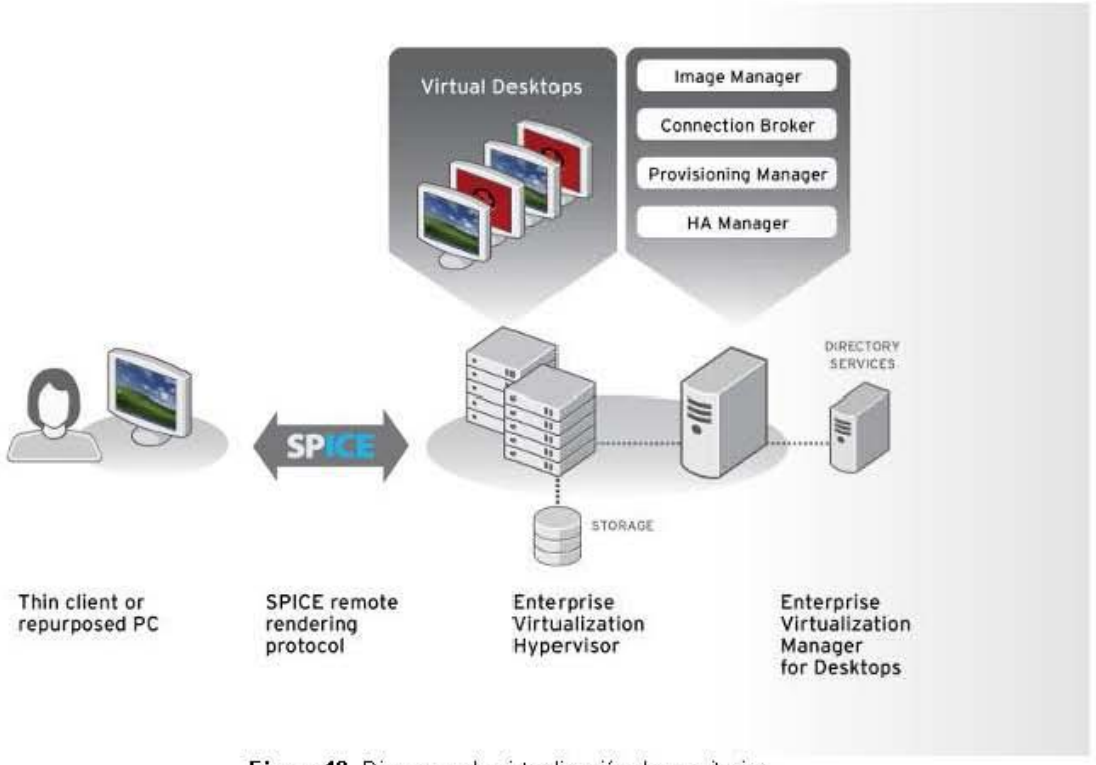


Figura 18. Diagrama de virtualización de escritorios.

Características

Este servicio posibilita acceder a la información y aplicaciones que requiere su negocio desde cualquier estación de trabajo, desde Thin Clients y computadores tradicionales así como a través de browser o dispositivos móviles.

Permite implementar de forma rápida varias estaciones de trabajo, sin tener que realizar una gran inversión en infraestructura y complicados procesos de capacity planning.

2.8.2 Beneficios de utilizar escritorios remotos Virtuales

- Simplifica la administración y soporte del parque de computadores instalados en la organización.
- Aumenta la vida útil de los dispositivos y equipos de escritorio ya existentes.
- Otorga movilidad a los usuarios.
- Costos predecibles de acuerdo a lo requerido por el negocio, ya que se paga por usuario del sistema.
- Mayor disponibilidad y seguridad de la información, ya que es almacenada en servidores cloud en un datacenter.

Ventajas de virtualizar escritorios sobre Red Hat

- Experiencia única para el usuario: Las capacidades multimedia brindan a los usuarios la experiencia que esperan obtener de sus escritorios.
- Soporte entre plataformas: El soporte para escritorios virtuales tanto de Windows como de Linux garantiza que los usuarios siempre cuenten con el escritorio adecuado para la tarea adecuada.
- Código abierto: Un cimiento construido sobre la base de tecnologías de código abierto significa que el mundo de la virtualización de escritorios está accediendo a un nuevo nivel de elección y libertad.

- Seguridad y conformidad de los datos: Una arquitectura alojada ayuda a las empresas a resguardar su información y mantenerse a la par del actual contexto de rápida transformación.
- Un socio confiable: Más de 15 años ofreciendo a las empresas el sistema operativo más seguro del mundo hace de Red Hat la mejor elección para las empresas que buscan implementar escritorios virtuales alojados.

Casos de Uso

- **Accesibilidad:** múltiples usuarios de su organización requieren viajar a distintas filiales de su empresa. Al virtualizar permitirá a estos usuarios poder acceder a su escritorio, aplicaciones e información, desde cualquier lugar o dispositivo de la misma forma como si estuvieran físicamente en sus oficinas.
- **Seguridad de información crítica:** los datos relevantes y estratégicos están almacenados en cada uno de los dispositivos de los usuarios, quienes constantemente están trasladándose y exponiendo la información ante eventuales pérdidas o robos de éstos. Al contar con una solución de escritorios virtuales su información está almacenada de forma segura y confiable dentro de datos.
- **Menor costo de Soporte:** cada vez que se realiza la actualización de una aplicación se debe intervenir manualmente todos los PC. Con la solución de escritorios remotos, el costo disminuye dramáticamente, ya que se hace el cambio una sola vez y se replica para todo el resto de los escritorios virtuales.

2.8.3 Protocolo SPICE (Simple Protocol for Independent Computing Environment)

SPICE es un protocolo de representación remota adaptable utilizado por Red Hat Enterprise Virtualization para Escritorios para conectar a los usuarios con sus escritorios virtuales. A diferencia de los protocolos de representación remota de primera generación como RDP e ICA, SPICE presenta una arquitectura de varias capas diseñada para soportar la experiencia de escritorio multimedia de hoy en día:

- **Controlador SPICE:** Componente que reside dentro de cada escritorio virtual.
- **Dispositivo SPICE:** Componente que reside dentro del Hipervisor de Red Hat Enterprise Virtualization.
- **Cliente SPICE:** Componente que reside en el dispositivo terminal, ya sea un cliente ligero o una PC rediseñada, que se utiliza para acceder a cada escritorio virtual.

En la siguiente figura se muestra la interacción entre el cliente final y SPICE (Figura 19).

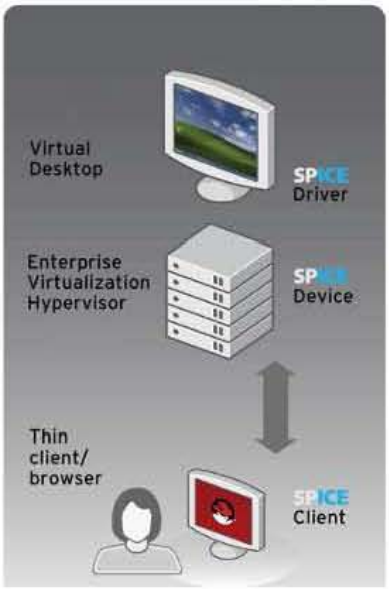


Figura 19. Componentes de Spice

Estos tres componentes funcionan simultáneamente, determinando cuál es el lugar más eficiente para procesar gráficos con el fin de maximizar la experiencia del usuario y minimizar la carga del sistema.

- Si el cliente es lo suficientemente poderoso, SPICE envía los comandos de los gráficos al cliente y los procesa al nivel de cliente, reduciendo considerablemente la carga del servidor.
- Por el contrario, si el cliente no es lo suficientemente poderoso, SPICE procesa los gráficos a nivel de host, donde el procesamiento de gráficos es mucho menos costoso desde la perspectiva de la UPC.

2.8.4 Protocolo RDP (Remote Desktop Protocol)

Es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón ó el teclado).

El modo de funcionamiento del protocolo es sencillo. La información gráfica que genera el servidor es convertida a un formato propio RDP y enviada a través de la red al terminal, que interpretará la información contenida en el paquete del protocolo para reconstruir la imagen a mostrar en la pantalla del terminal.

En cuanto a la introducción de órdenes en el terminal por parte del usuario, las teclas que pulse el usuario en el teclado del terminal así como los movimientos y pulsaciones de ratón son redirigidos al servidor, permitiendo el protocolo un cifrado de los mismos por motivos de seguridad. El protocolo también permite que toda la información que intercambien cliente y servidor sea comprimida para un mejor rendimiento en las redes menos veloces. Pues es la única de las soluciones de clientes ligeros analizadas que nos permite utilizar este protocolo para que los terminales puedan actuar como clientes de servidores Windows, lo que puede ser interesante en multitud de ambientes de trabajo en los que se utilizan servidores Microsoft.

Este servicio utiliza por defecto el puerto TCP 3389 en el servidor para recibir las peticiones. Una vez iniciada la sesión desde un punto remoto el ordenador servidor mostrará la pantalla de bienvenida de windows, no se verá lo que el usuario está realizando de forma remota.

Tabla comparativa entre SPICE y RDP (Tabla 1)

Comparison between SPICE and RDP:

FEATURES:	RDP WITH EXISTING VIRTUALIZATION SOLUTIONS	RED HAT ENTERPRISE VIRTUALIZATION
Bi-directional audio (capture)	No	Yes
Bi-directional video (capture)	No	Yes
Audio playback	Yes	Yes
Video playback	Poor quality	Good quality
USB support	No, needs external tools	Yes, fully integrated
Multimedia density on server	Poor	Maximizes density of virtual desktops on server by offloading graphics processing to clients or host

Tabla 1. Comparativa entre SPICE y RDP

Gestor de conexiones integrado

El gestor de conexiones integrado de Red Hat Enterprise Virtualization es responsable de permitir las conexiones entre los usuarios finales y las instancias específicas de los escritorios virtuales.

Al tratarse de un portal con base en la Web, los usuarios pueden acceder a sus escritorios virtuales a través de un cliente ligero o bien de una computadora personal rediseñada con un navegador de Internet. Una vez conectados al portal, los usuarios pueden elegir de entre los diversos escritorios virtuales para los cuales se les otorgaron derechos de acceso.
En la figura número 20, se muestra como aparecen los escritorios remotos que tenemos compartidos en un browser para poder abrir desde cualquier lado.

Figura 20. Cliente ligero web

IPA Server

Basado en tecnologías y estándares abiertos, incluyendo LDAP y Kerberos (Figura 21), Red Hat Enterprise IPA ofrece servicios de administración centralizada de identidades, servicios de inicio de sesión único, servicios de directorios de alta disponibilidad y una infraestructura de control de acceso en un paquete fácil de instalar y administrar.

Nos sirve para ofrecer servicios de inicio de sesión único que permiten a los usuarios acceder a las aplicaciones y a los datos identificándose una sola vez. También permite administrar de forma centralizada a usuarios y grupos (creación, edición, eliminaciones) mediante una sencilla interfaz gráfica de usuario

Red Hat Enterprise IPA es una solución de código abierto para la administración de identidades, directrices, auditorías y accesos de usuarios, máquinas y servicios en entornos Linux y UNIX. Mejora la productividad, reduce los riesgos y simplifica las iniciativas para cumplir con las normativas legales. La hemos desarrollado pensando en la interoperatividad, es decir, para que sea fácil de integrar con las herramientas existentes y no tener que depender de un proveedor.

- Inicio de sesión único mediante Kerberos y LDAP Replicación de directorios de patrones múltiples Sincronización con los directorios existentes para simplificar la administración.
- Los servicios se autentican y cifran mutuamente utilizando Kerberos
- Compatibilidad con estándares abiertos, una infraestructura de control de acceso

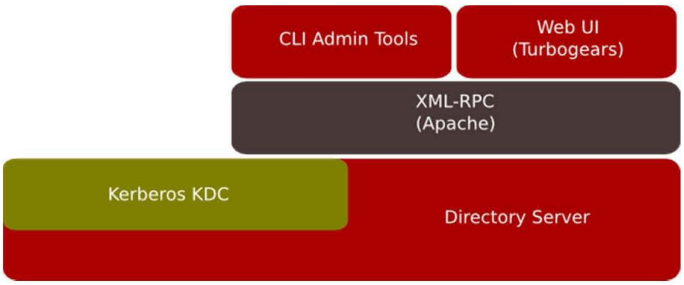


Figura 21. Esquema de administración IPA

3. Planificación de Carga (CAPACITY PLANNING)

Es el proceso de determinar los recursos de hardware y red requeridos para prevenir un impacto en el rendimiento de los negocios o aplicaciones críticas. La administración del rendimiento es la práctica de administrar el tiempo de respuesta de los servicios de la red, administración del hardware, su consistencia y su calidad.
Este proceso permite predecir y planificar los tipos y cantidades de recursos claves de IT (tecnologías de la información) que se necesitan para alcanzar los requerimientos de negocio más importantes, a través del planteamiento de posibles escenarios, que sirvan para lograr mejores costos, mayor rendimiento y una mayor utilidad de los elementos.

3.1 ¿Para qué realizar la planificación de carga?

En la planificación de carga uno debe considerar cualquier factor que pueda dañar el sistema de un ambiente controlado en una infraestructura de IT, pero para llevar acabo este proceso hay que conocer dos conceptos totalmente diferentes la gestión de riesgo y la percepción del riesgo.

- La gestión del riesgo.- conocer en profundidad cuales son los riesgos reales a los que se puede enfrentar nuestra plataforma y realizar actividades que puedan a la medida posible eliminar o reducir el riesgo en lo más mínimo el impacto de dichos riesgos.
- Percepción del riesgo.- es tener el conocimiento de la existencia de ciertos riesgos, pero no analizar el impacto de los riesgos. Es una idea errónea o un cálculo incorrecto que en realidad puede causar un impacto enorme.

Con estos dos conceptos nos damos cuenta la necesidad de realizar una planificación de carga que nos permite saber cuáles son los riesgos reales de la plataforma.
La planificación de carga no sólo sirve para medir el rendimiento de nuestro sistema desde el punto de vista de IT, también nos permite observar el dinero que pierde la compañía cada vez que hay un problema de rendimiento en la BD.

3.2 ¿Cuándo hay que realizar una planificación de carga?

En una infraestructura de las tecnologías de la información existen tres momentos importantes donde se debería realizar una planeación de carga:

- Durante el periodo de desarrollo del proyecto, para identificar posible carencia en la definición de las especificaciones de un proyecto, así como el impacto que tendrá el proyecto en la infraestructura.
- Una vez que la infraestructura de IT, periódicamente se debe realizar un capacity planning, para identificar posibles cuellos de botella y gestionar los riesgos para el negocio que se puedan encontrar.
- Cada que se piense en realizar más proyectos, debería realizar un capacity planning para comprobar que dicho proyecto no impactara de forma negativa la infraestructura actual.

3.3 Planificación de carga en USECAD.

Para realizar una correcta planificación de carga en USECAD es necesario seguir un procedimiento recomendado por varias plataformas de virtualización. Para nuestro proyecto nos basaremos en el estudio de vmware para saber cuántos recursos se necesitan para tener la arquitectura mínima para virtualizar.
Es muy importante realizar un excelente cappacity planning para poder quedar con un 20% libre para cualquier eventualidad que pueda requerir nuestra arquitectura, así como para no quedar limitados en recursos y tampoco se exageren para no exceder el presupuesto que se tiene destinado a la infraestructura.
Donde primero se realizará un análisis de los recursos que se utilizan con arquitectura física y descubrir cuanto se está ocupando actualmente antes de iniciar la virtualización.

1.- *El análisis de los recursos de la infraestructura*.- En este punto se realiza un análisis donde se identificaran todas las unidades de trabajo de cada uno de los componentes de la

infraestructura como son el CPU, memoria, discos duros, red. Donde se señalará cada unidad de trabajo con la información de su rendimiento.
La siguiente tabla (tabla 1) se realizó revisando cada servidor físico que se encuentra dentro de la arquitectura del centro de USECAD, para revisar si podrían ser candidatos a virtualizar, así como también realizar el estudio de cuantos recursos son necesarios para poder realizar el requerimiento mínimo para crear nuestra estructura de virtualización.

Servidor	*Sistema Operativo*	*Aplicación*	*Procesador*	*RAM*	*Storage*	**Concurrencia en la red ***
bd1.fi-a.unam.mx	RHEL 5	Sybase	Intel Pentium 4	4 GB	60 GB	60-70 peticiones/min.
bd2.fi-a.unam.mx	RHEL 5	Sybase	Intel Pentium 4	16 GB	60 GB	60-70 peticiones/min.
Correo	Fedora 13	Postfix	Pentium 3	1 GB	100 GB	10-15 peticiones/min.
LAMP1	Fedora 8	Respaldo BD	Pentium 4	2 GB	80 GB	60-70 peticiones/min.
Web1.fi-a.unam.mx	RHEL 5	LAMP	Pentium 4	2 GB		70-90 peticiones/min.
Web2.fi-a.unam.mx	RHEL 5	LAMP	Pentium 4	4 GB		70-90 peticiones/min.
LAMP2	Fedora 8	Respaldo BD	Pentium 4	2GB	80 GB	60-70 peticiones/min.

Tabla 1. La información fue extraída en temporada de inscripción de alumnos.

En la Tabla 1 se puede observar las características de cada unidad de trabajo, en ella se puede hacer un análisis más detallado de cada componente.

2.- Creación de un esquema de las unidades de trabajo críticas para USECAD. En este punto uno tiene que definir claramente cuáles son las unidades de trabajo que tienen mayor criticidad y que necesitaran mayores privilegios por RHEV-Manager. En la gráfica anterior debemos seleccionar a base del conocimiento de la carga del trabajo y la importancia de cada servidor.

- **bd1.fi-a.unam.mx**

  Base de datos número 1 para el sistema de inscripciones de la facultad de ingeniería
- **bd2.fi-a.unam.mx**

  Base de datos número 2 para el sistema de inscripciones de la facultad de ingeniería.
- **Correo**

  Es el servidor de correo open-source utilizado internamente en el departamento de USECAD
- **LAMP1**

  Respaldo de Sybase
- **Web1.fi-a.unam.mx**

  Es el servidor de la página electrónica de USECAD.

- **web2.fi-a.unam.mx**

  Es el servidor de respaldo de la página electrónica de USECAD.
- **LAMP2**

  Respaldo 2 de sybase y pruebas

3.4 Planificación de carga para RHEV

Con esta información podemos darnos cuenta de la importancia de cada servidor. Podremos ir definiendo prioridades.

Una de las características de RHEV es que se pueden definir algunas políticas de cluster para la alta disponibilidad (high availability). Los puntos que considera son los siguientes:

3.4.1 Even Distributión.

Es una característica similar a DRS (distribution resource service) de vmware que sirve básicamente para distribuir la carga de los hosts en otras palabras significa que si un servidor está ocupando bastantes recursos y rebasa le porcentaje designado en la política realiza una tarea de distribuir la carga hacia otros hosts dejando sólo el servidor con mayor carga de trabajo aislado en el host.
En la administración de RHEV-Manager se muestra una ventana similar si se quisiera realizar una distribución de la carga en ambos servidores como se muestra en la siguiente figura (Figura 1).

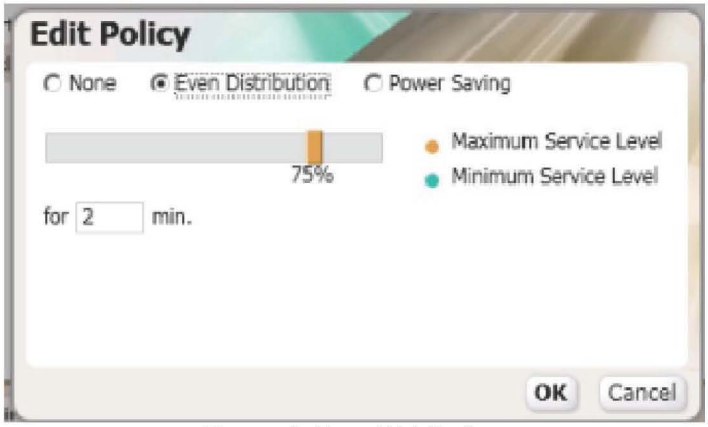


Figura 1. Even Distribution

Ejemplo:
Se tiene un esquema de virtualización RHEV en el host1 se encuentra una máquina virtual Windows, y en el host2 se encuentran tres máquinas virtuales corriendo 1 con Red Hat y 2 Windows (véase en figura2).

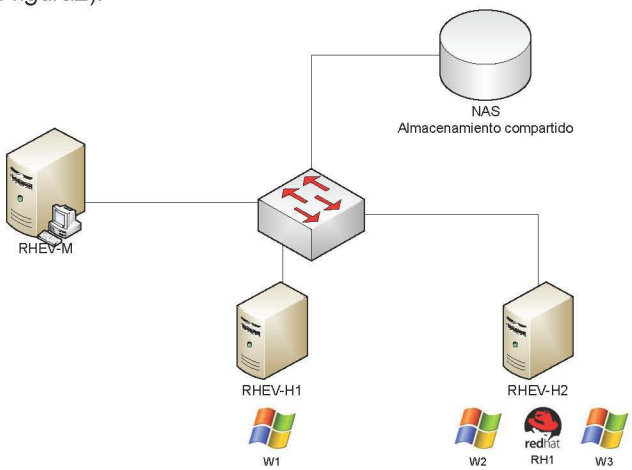


Figura 2. Esquema de virtualización RHEV

Suponiendo que el servidor RH se configuro su política de even Distribution a un 75% y precisamente está ocupando un 80% de su capacidad durante 2 minutos, entonces RHEV empieza a desalojar a los demás servidores al otro servidor para dejar trabajar aislado al servidor con mayor carga de trabajo (véase en la figura 3).

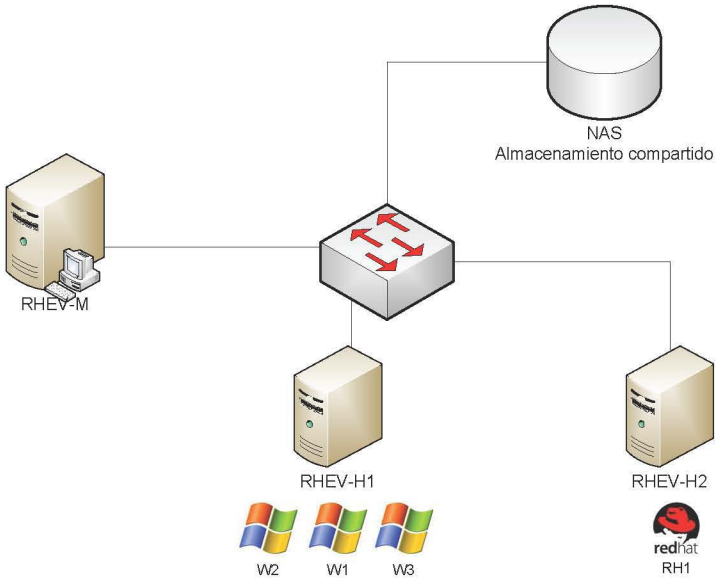


Figura 3. Esquema de virtualización RHEV con ever Distribution

Esta característica nos da como resultado mayor performance en nuestros resultados, evitando cargas de trabajo que puedan provocar alguna perdida de desempeño.

3.4.2 Power Sharing

Otra de las características que se pueden aprovechar claramente al hacer un correcto capacity planning es la de Power Sharing, esta característica es parecida a la de Even distribution. Aquí si un servidor se encuentra consumiendo muy pocos recursos y después de un tiempo designado sigue consumiendo el mínimo de recursos RHEV duerme el equipo para ahorrar energía.

Ejemplo.
En el mismo esquema de la Figura 1, suponiendo que el servidor de Windows 2 y Windows 3 están ocupando el mínimo de recursos RHEV mandara a dormir dichos servidores y así estará ahorrando energía (véase en la figura 4).

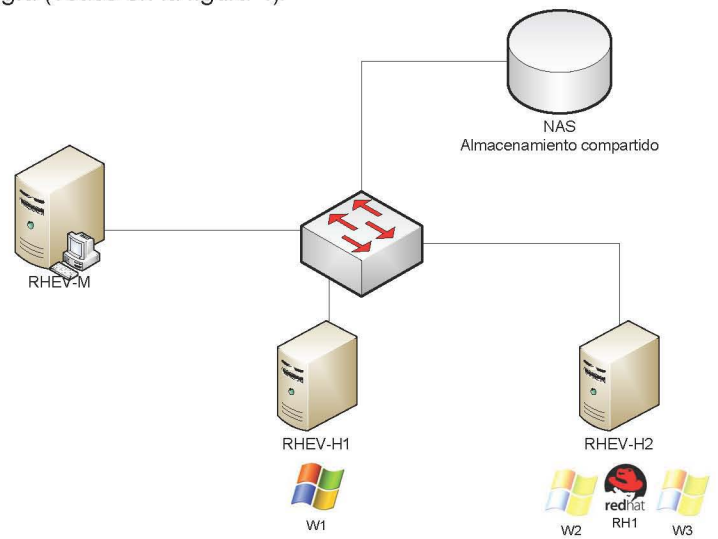


Figura 4. Esquema de virtualización RHEV con power Sharing

Y otra característica que se puede aprovechar al realizar un correcto capacity planning es el dar la prioridad de arranque a los equipos cuando algún host llegue a fallar y se hayan apagado algunas máquinas virtuales.

Esta característica con ayuda de high availability que su función se basa en que si un host se apaga las máquinas virtuales que se encontraban en dicho host se apagaran con el host pero automáticamente reiniciara en el otro host. Pero al configurar las políticas se puede decidir el orden en que encenderán los equipos para perder el menor tiempo posible con el servidor abajo.

NOTA.
Cada característica se define según el tipo de servidor y nivel de criticidad del mismo.

4. Instalación de ambiente Red Hat Enterprise Virtualization

Para poder iniciar una instalación de un ambiente de RHEV es necesario considerar todos sus componentes y así poder tener una infraestructura completa y sobretodo tener la opción a manejar todas sus tecnologías. Los componentes mínimos son los siguientes:

- Servidor RHEV manager
- Dos hosts (hypervisor) para poder brindar alta disponibilidad entre otras características.
- Un almacenamiento compartido para alojar máquinas virtuales
- Un almacenamiento para imágenes de sistemas operativos (ISOS)

Actualmente en la versión 2.2 de Red Hat Enterprise Virtualization es necesario que la instalación del administrador de RHEV sea sobre un Windows.

4.1 Instalación de Red Hat Enterprise Virtualization-Manager (Administrador de RHEV)

Los requisitos mínimos de hardware para la instalación son los siguientes:

- Al menos 1 GB de memoria RAM
- 20 GB de espacio local en disco
- Al menos una tarjeta de red con ancho de banda de 1 Gbps.

Requisitos de Software.

Red Hat Enterprise virtualization Manager puede trabajar con un Windows Server 2003 R2 a 64 bits o superior, pero por recomendaciones de Red Hat

- Sistema operativo Windows Server 2008 Server R2
- Con el rol de web server (IIS) y aplicaciones de servidor.
- Microsoft .NET Framework 3.5.1

Para instalar RHEV-M tenemos que instalar algunos roles en Windows server 2008 como son el rol de web server (IIS), así como también aplicaciones de servidor y Microsoft .NET Framework 3.5.1, al estar instalados en resumen deberá mostrar los siguientes componentes. Al agregar los roles nos mostrará un resumen de las características para iniciar la instalación (figura 1)

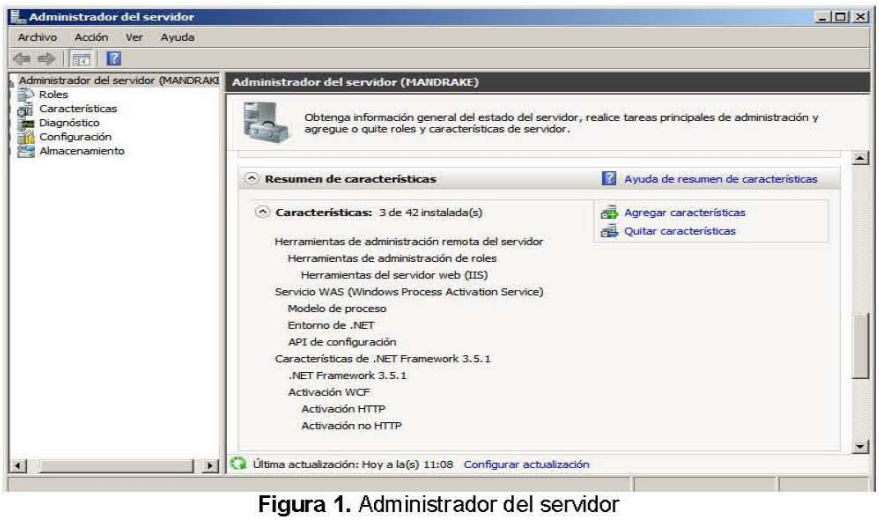


Figura 1. Administrador del servidor

Después de que tenemos la certeza de tener todos los componentes solicitados y asegurarnos que tenga un nombre de de dominio y dirección IP fija podremos comenzar con la instalación del manager de RHEV.

En la siguiente figura (Figura 2), si tenemos los componentes y roles ya instalados podemos iniciar la instalación.

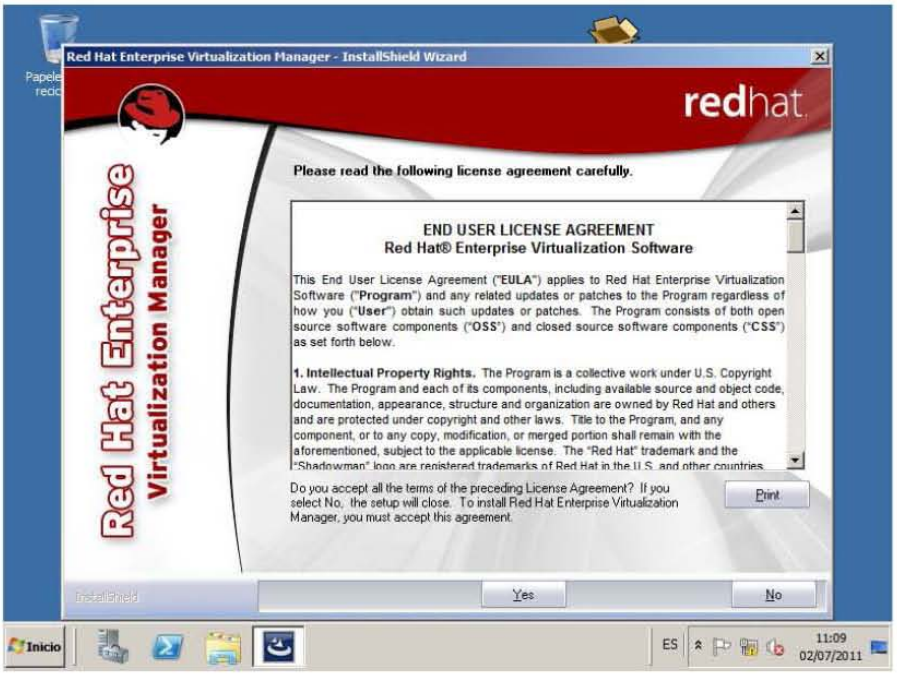


Figura 2. InstallShield Wizard

Al iniciar la instalación tendremos que seleccionar todos los paquetes que aparecen para elegir (véase Figura 3).

Figura 3. Instalación de Características de RHEVM

Continuando con la instalación ahora tendremos que escoger la instalación del motor de la base de datos, para esta instalación el motor más recomendado es el SQL Server 2005 Express por la pequeña infraestructura, la recomendación de utilizar un motor más grande es directamente proporcional al tamaño de infraestructura (Figura 4).

Figura 4. Instalación de la Base de Datos

Ingresaremos un password para el motor de la base de datos. El password deberá contener mayúsculas, minúsculas, números y signos especiales (figura 5).

Figura 5. Asignación del password para la Base de Datos de SQL

Después nos mostrara unas opciones para crear un sitio web o seleccionar el que crea por default así como dejaremos las características de ***Force SSL*** (Figura 6).

Figura 6. Selección del Web Server

Ahora saldrán las opciones de detalles del administrador y del dominio (Figura 7). En la primera seleccionaremos el dominio al cual pertenece el *RHEV-Manager* en este caso nuestro dominio es local y nuestro nombre de dominio es ***SHUN***. En la segunda sección definiremos el nombre de usuario de Windows y el password para la sincronización.

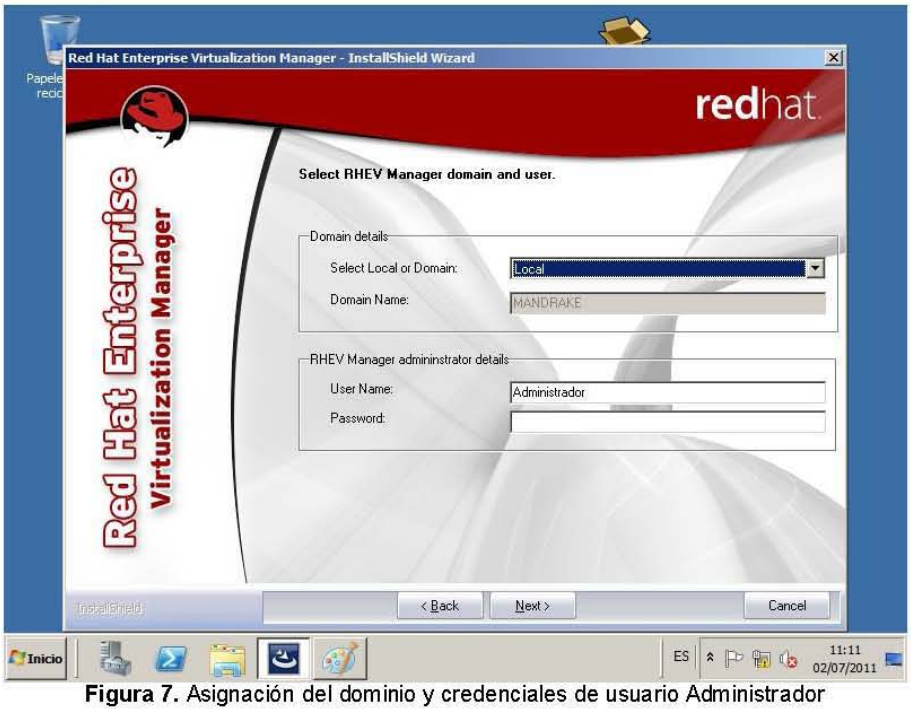


Figura 7. Asignación del dominio y credenciales de usuario Administrador

Ya en los últimos datos sirven específicamente sí uno cuenta con un directorio activo. El nombre de la organización y el nombre completo del equipo. Si contáramos con un directorio activo podríamos seleccionar la opción de validar si el nombre se encuentra dentro del dominio (Figura 8).

Figura 8. Asignación del FQDN

Al final seleccionaremos el puerto que propone *RHEV-Manager* por default y continuaremos con la instalación (Figura 9).

Figura 9. Asignación del puerto de la Consola

Mostrará un resumen de la configuración realizada para la instalación del administrador (Figura 10).

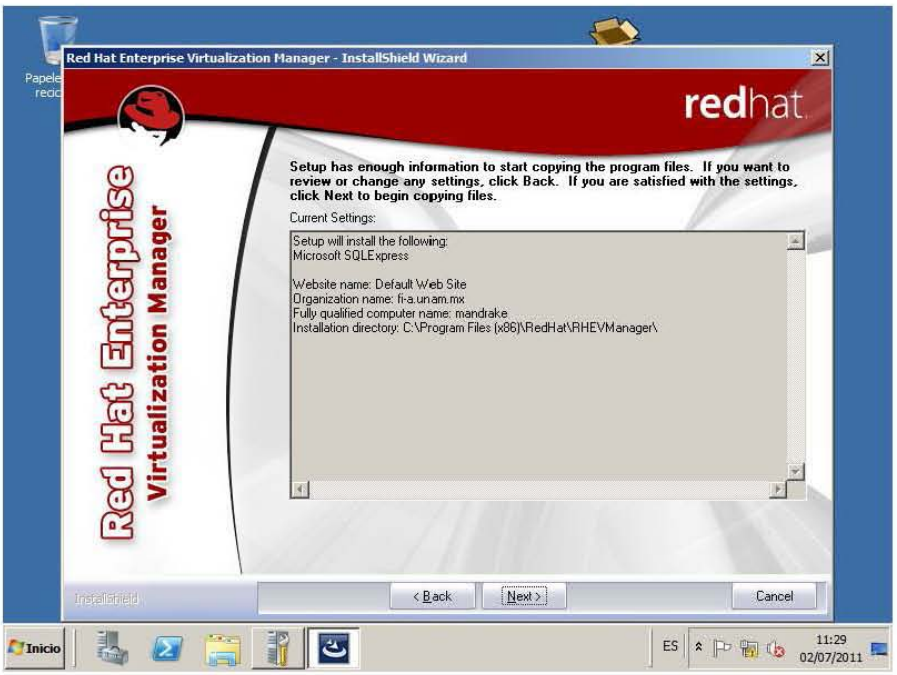


Figura 10. Resumen de instalación

Finalizando la instalación copiaremos el certificado ***SHA1*** (Figura11).

Figura 11. CA SHA1 Fingerprint

Después de la instalación de RHEV-Manager será necesario reiniciar el equipo para que trabaje correctamente el equipo. Al iniciar la instalación iremos a inicio e iremos a la parte y escribiremos RHEVM y nos dará la opción, y nos abrirá un Internet Explorer.

Para empezar a trabajar se ocupará un certificado que al conectarse a la página nos pedirá que lo descarguemos y lo instalemos como nos muestra a continuación (Figura 12 y Figura 13)

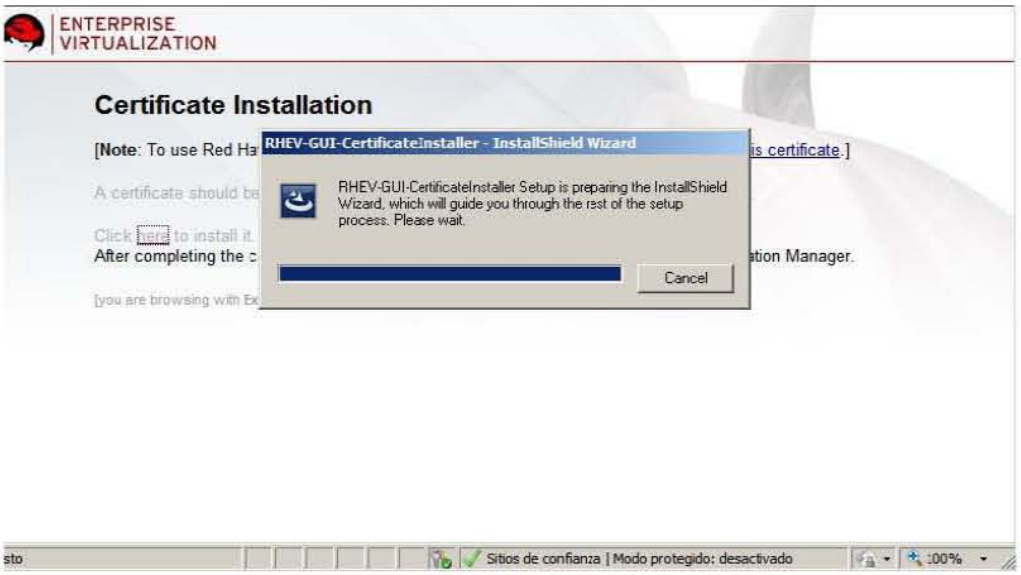


Figura 12. Descarga del certificado

Figura 13. Instalación del cliente

Al haber terminado de instalar el certificado nos pedirá la autenticación para poder entrar a la administración web del manager. Dentro del administrador Web ya podremos agregar hypervisores, servidores de almacenamiento, crear máquinas virtuales y escritorios remotos.

4.2 Instalación de RHEV-Hypervisor

El Red Hat Enterprise Virtualization (RHEV) Hypervisor es una plataforma compacta y completa virtualización destacado de forma rápida y fácil implementación y administración de invitados virtualizados. El RHEV Hypervisor está diseñado para integrarse con el Administrador de Red Hat Enterprise Virtualization para servidores y de Red Hat Enterprise Virtualization Manager for Desktops.

El RHEV Hypervisor se puede instalar desde dispositivos de almacenamiento USB, CD-ROMs, DVDs, pre-instalado por un OEM o provisionado con PXE.

El RHEV Hypervisor se basa en la Máquina Virtual basada en el Kernel (KVM). KVM es una virtualización avanzada y eficiente hypervisor implementado como un módulo del kernel de Linux. Como KVM es un módulo del kernel, que aprovecha la existente Red Hat Enterprise Linux kernel y se beneficia de numerosas pruebas el kernel por defecto, el soporte de dispositivos y la flexibilidad.
Limitaciones

Las siguientes limitaciones se aplican a los hipervisores y son compatibles y los clientes virtualizados:

- Un máximo de 64 CPUs físicas en el host.
- Un máximo de 1 TB de RAM.
- Un máximo de 16 CPUs virtuales por invitado.
- Un máximo de 256 GB de memoria RAM virtual por invitado de 64 bits.
- Un máximo de 8 dispositivos de almacenamiento virtuales por invitado.
- Un máximo de 8 controladores de interfaz de red virtualizados por invitado.
- Un máximo de 32 dispositivos virtuales PCI por invitado

Los clientes de RHEV pueden soportar los siguientes sistemas operativos:

- Red Hat Enterprise Linux 3 (32 bits y 64 bits)
- Red Hat Enterprise Linux 4 (32 bits y 64 bits)
- Red Hat Enterprise Linux 5 (32 bits y 64 bits)
- Windows XP Service Pack 3 y posteriores (32 bits)
- Windows Server 2003 Service Pack 2 y posteriores (32 bits y 64 bits)
- Windows Server 2008 (32 bits y 64 bits)
- Windows Server 2008 R2 (64 bits)
- Windows 7 (32 bits y 64 bits)

Para la instalación del Hypervisor como se comentó anteriormente no necesita bastante almacenamiento para poder hacer la instalación, hasta se puede realizar desde una USB, ya que es un sistema operativo recortado únicamente con las características y paquetes necesarios para poder fungir como hypervisor.

Al iniciar la instalación muestra un menú dinámico para hacerlo más sencillo (Figura 14).

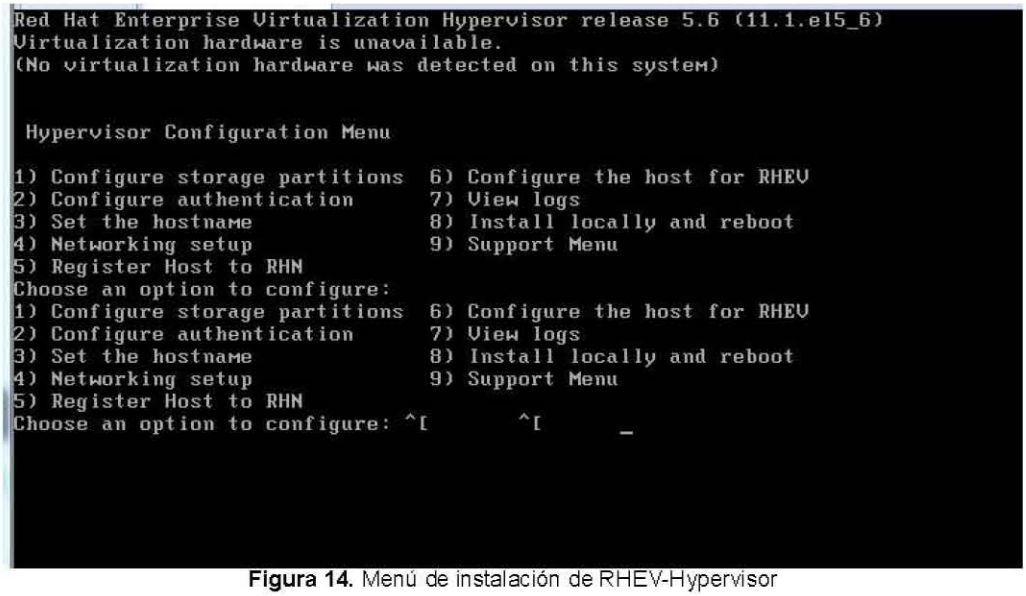


Figura 14. Menú de instalación de RHEV-Hypervisor

El primer paso es hacer las particiones donde se instalará el RHEV-Hypervisor, seleccionaremos la opción 1 para iniciar con el particionamiento.

Seguiremos paso a paso el menú de instalación. Las particiones quedarán de la siguiente manera:

```
The local disk will be repartitioned as follows:
================================================

Physical Hard Disk: /dev/hdb (10000 MB)
Disk Identifier: storage_serial_QM00002
Boot partition size: 50 MB
Swap partition size: 2233 MB
Installation partition size: 256 * 2 MB
Configuration partition size: 5 MB
Logging partition size: 2048 MB
Data partition size: 5152 MB
```

Aceptaremos la configuración y hará el particionado de forma automática, después seleccionaremos el número dos donde configuraremos la autenticación del ssh para la conexión con el hypervisor (Figura 15).

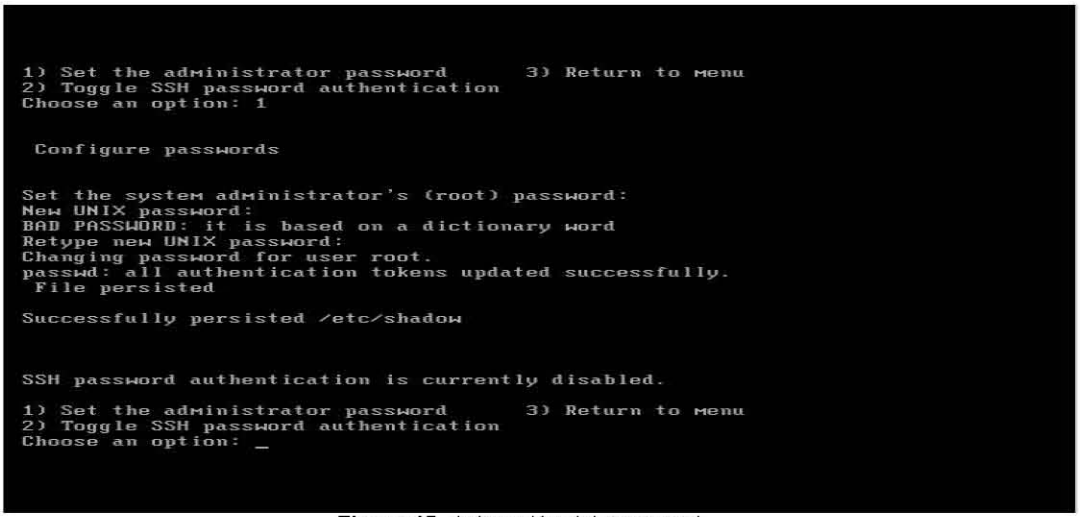


Figura 15. Asignación del password

Y seleccionaremos la opción dos para habilitar el ssh y al final regresaremos al menú principal. En el menú principal ahora seleccionaremos la opción 3 para configurar nuestro *hostname* cómo lo muestra la Figura 16.

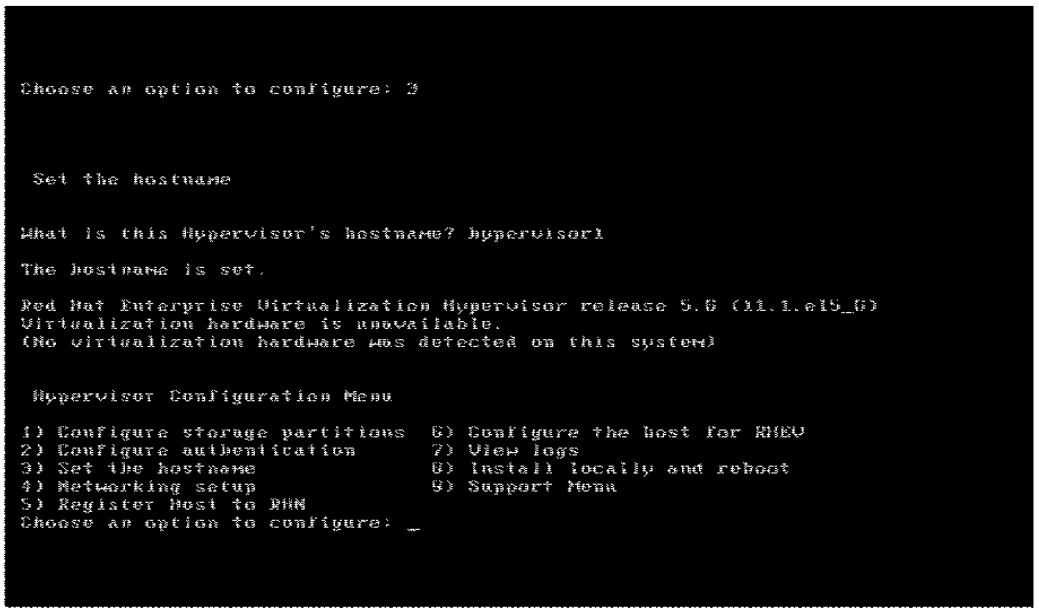


Figura 16. Asignación del Hostname

En la Opción 4 se podrá configurar la red y todos los nodos de red que tenga nuestro equipo.

Al iniciar la configuración de los nodos, primero da la opción de hacer que encienda el puerto para identificarlo físicamente, después si es que pertenece a alguna VLAN y para finalizar poner la IP, NETMASK y GATEWAY, ya sea con IPv4 o IPv6.

En los pasos siguientes de ese sub-menú también se puede configurar el NTP (Network Time protocol) y el DNS (Domain Name Server).

Al terminar dicha configuración del sub-menú se iniciará el servicio de la red y podremos continuar con el menú principal (Figura 17).

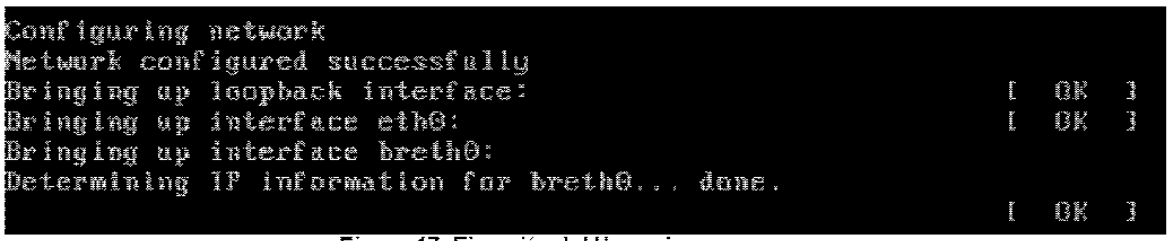


Figura 17. Ejecución del Hypervisor

Dentro de la opción 5 se tiene la oportunidad para poder registrar nuestros equipos dentro de Red Hat Network y así poder recibir las ventajas de tener una suscripción de Red Hat, tener todo el soporte vía telefónica por gente certificada, además de poder contar con parches de algún bug de error, o mejoras dentro de algún servicio o aplicación que se esté ejecutando dentro del hypervisor.

Para registrar el equipo nos dará dos opciones una será para registrarlo a Red Hat Network (RHN) y otro será para poder registrarlo en algún Proxy de RHN mejor conocido como RHN Satellite.

En esta opción nos pedirá datos del usuario que previamente se tuvo que haber creado en la página de Red Hat Network y también nos pedirá el password.

Nota. Para poder realizar dicha tarea es necesario contar con una suscripción de RHEV y además de tener salida a Internet para que se pueda autenticar con RHN a menos que se cuente con el Proxy RHN satellite.

El paso 6 consiste en registrar el hypervisor al RHEV-Manager, en la comunicación con el Manager trabajan mediante 2 puertos 443 y el puerto 25285, esto con la finalidad de que se este trabajando con algún firewall de seguridad.

Lo primero que se pide en esta opción es ingresar la dirección IP de nuestro RHEV-Manager:

```
Enter the RHEV Manager's hostname or IP address.
Optionally: append a port after the hostname or IP address
For example, 10.0.0.1:443 or rhev.example.com:443
```

Si la comunicación fue un éxito nos mandará la siguiente leyenda

```
The RHEV Manager's address is set
The RHEV Manager's port is set.
```

Después nos pedirá de nuevo que ingresemos los datos del RHEV-Manager pero ahora mediante el puerto 25285 de la misma manera que la vez anterior:

```
Enter the RHEV Manager's hostname or IP address.
Optionally: append a port after the hostname or IP address
For example, 10.0.0.1:25285 or rhev.example.com:25285
```

Si la comunicación fue un éxito nos mandará la siguiente leyenda:

```
The NetConsole manager address is set.
The NetConsole manager port is set.
```

Una vez terminado el registro del hypervisor en el Manager los últimos pasos son para configurar los directorios y archivos de log, que en eso consiste el siguiente paso. Por último guardaremos los cambios de configuración y realizará la instalación de nuestro hypervisor.

Una vez reiniciado el equipo y con la instalación terminada, tendremos que aprobar la administración del hypervisor dentro del manager.

Seleccionaremos la pestaña de **Hosts**. En este punto observaremos que el hypervisor que registramos ya aparece pero falta aceptarlo, si le damos clic al hypervisor observaremos un botón que dice **Pending approval,** le damos clic y con eso es más que suficiente para haber aprobado el hypervisor para una administración.

4.3 Configuración de bonding de tarjetas

Al realizar el capacity planning de la parte de almacenamiento, será necesario repartir la carga de las tarjetas de red con la finalidad de no saturar y poder balancear la carga de trabajo, además de construir un bonding de tarjetas para poder tener la redundancia en la red, para realizar todo esto de manera exitosa al menos necesitaremos 4 nodos de red en nuestro servidor.

Iniciaremos la configuración de la red creando dos bonding de tarjetas considerando que tendremos dos IP's para configurar. El primer paso es crear el archivo /etc/sysconfig/network-script/ifcfg-bond0 con el siguiente contenido:

```
DEVICE=bond0
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.100.163
NETMASK=255.255.255.0
GATEWAY=192.168.100.254
PEERDNS=no
IPV6INIT=no
USERCTL=no
```

Y para la siguiente tarjeta será crear el archivo /etc/sysconfig/network-script/ifcfg-bond1 con el siguiente contenido:

```
DEVICE=bond1
BOOTPROTO=static
ONBOOT=yes
IPADDR=192.168.100.164
NETMASK=255.255.255.0
GATEWAY=192.168.100.254
PEERDNS=no
IPV6INIT=no
USERCTL=no
```

El siguiente punto será editar las interfaces de red, para que puedan ser administradas por los bonding creados.

Editaremos los siguientes archivos:

/etc/sysconfig/network-script/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-script/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-script/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=none
ONBOOT=yes
MASTER=bond1
SLAVE=yes
```

/etc/sysconfig/network-script/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=none
ONBOOT=yes
MASTER=bond1
SLAVE=yes
```

Al haber configurado las tarjetas procederemos a configurar el archivo de /etc/modprobe.conf para asignarle los parámetros que más nos convengan en nuestro caso lo configuraremos para que cada 100ms este validando la conexión y para evitar fallos utilizaremos round-robbin con las siguientes líneas al final del archivo:

```
alias bond0     bonding
options bond0 miimon=100 mode=0
alias bond1     bonding
options bond1 miimon=100 mode=0
```

Para finalizar sólo queda reiniciar el servicio de red con el comando `service network restart`
Y después hacer una validación de qué tarjeta es la principal y cual se encuentra de respaldo con el comando:

```
cat /proc/net/bonding/bond0
cat /proc/net/bonding/bond1
```

Básicamente nuestra configuración quedará como el siguiente diagrama mostrado en la Figura 18, donde muestra claramente el funcionamiento de la configuración y beneficios de tolerancia de fallos. Aunque cabe destacar que la alta disponibilidad quedaría de una mejor manera si cada interfaz se conectará a diferentes switches, para de esta manera también contar con tolerancia de fallo en capa 2.

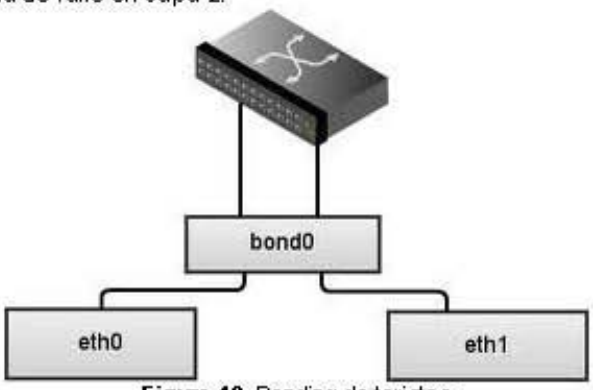


Figura 18. Bonding de tarjetas

4.4 Configuración de NFS en RHEL

Una vez que se han registrado los Host (hipervisores) a nuestro administrador, el paso a seguir es configurar un servidor con la finalidad que nos proporcione un servicio de NFS (Network File System) que nos proveerá de un sistema de archivos para poder compartirlo a través de nuestra red LAN, a nuestros hipervisores y administrador.

Para que la arquitectura de RHEV pueda trabajar y se puedan utilizar todas sus funciones es indispensable contar con tres sistemas de archivos compartidos, como se ha tratado anteriormente, se pueden compartir estos sistemas de archivos mediante varios protocolos, pero por nuestra corta infraestructura que contamos utilizaremos NFS.

Los tres sistemas de archivos que se necesitan tienen las siguientes funciones.

- Almacenamiento principal (storage master).- Dentro de este sistema de archivos se encontrará la información actualizada de la distribución de las máquinas virtualizadas. Además de poder contener el almacenamiento asignado a las máquinas (Disco Duro Virtual).
- Almacenamiento de isos (isos).- El sistema de archivos de isos tiene la tarea de contener las imágenes de los sistemas operativos que se quieran instalar virtualmente, dentro de la infraestructura.
- Almacenamiento de exportación (Export).- En este sistema de archivos, no es indispensable contar con él para utilizar la infraestructura de RHEV. Pero es necesario cuando se quiere hacer una migración de un equipo físico a virtual, para este proceso es necesario contar con este almacenamiento ya qué su función es validar que la máquina que esté recibiendo cuente con todas las características para poder trabajar dentro de la infraestructura.

La finalidad de tener dos IP's sobre el mismo servidor es para brindar mayor desempeño a las máquinas virtuales, por qué la interfaz de red será como su cable SATA para comunicar el disco duro con los demás elementos como procesador, red y memoria RAM. Una de las IP será sólo para utilizar el almacenamiento Master, y las otra IP sera utilizada para utilizar el almacenamiento de **isos** y **export**.

Los requerimientos de instalación del nuestro servidor de NFS es la siguiente:

- Contar con espacio suficiente en disco duro, para poder compartir lo necesario para poder crear discos duros virtuales para cada máquina virtual
- Crear las políticas de seguridad necesarias para qué sólo se compartan los recursos a los hipervisores y administrador.
- Tener al menos dos tarjetas de red para poder hacer un balanceo de carga en la red, y tenerlas configuradas con diferente IP, pero que se encuentre dentro del mismo segmento.
- Tener previamente instalado, el servicio portmap y nfs-utils.

Instalación

Toda la instalación del servicio del NFS se realizará en el servidor de almacenamiento, con un sistema operativo Red Hat Enterprise Linux.
Para poder levantar el servicio de NFS es necesario instalar los paquetes de portmap y nfs-utils.

```
yum -y install portmap
yum -y install nfs-utils
```

Una vez instalados procederemos a habilitarlos para qué arranque cada que se reinicien los equipos

```
chkconfig portmap on
chkconfig nfs on
```

Iniciaremos creando las particiones para poder montarlas en sus directorios correspondientes, cuando se instaló el sistema operativo se crearon las particiones con la tecnología de LVM para poder tener las ventajas de expandir o reducir el tamaño de nuestros sistemas de archivos.
Crearemos tres particiones lógicas:

```
lvcreate -L 1000G -n /dev/VolGroup00/master
lvcreate  -L 50G -n /dev/VolGroup00/isos
lvcreate -L 200G -n /dev/VolGroup00/export
```

Después le asignamos un tipo de sistema de archivos, en nuestro caso utilizaremos ext3:

```
mkfs.ext3 /dev/VolGroup00/master
mkfs.ext3 /dev/VolGroup00/isos
mkfs.ext3 /dev/VolGroup00/export
```

Crearemos los directorios:

```
mkdir /master
mkdir /isos
mkdir /export
chmod 777 /master /isos /export
```

Para finalizar esta tarea asociaremos en el archivo de fstab los volúmenes lógicos creados con el directorio así como también montarlo en caliente para poder iniciar a trabajar.

En el archivo `/etc/fstab` agregaremos al final del archivo las siguientes líneas:

```
/dev/VolGroup00/master   /master       ext3            default        0 0
/dev/VolGroup00/isos     /isos        ext3            default        0 0
/dev/VolGroup00/expo     /export       ext3            default        0 0
```

Al finalizar de agregar las líneas pondremos el siguiente comando:

```
mount -a
```

Al poner el comando validaremos que están correctas las líneas que acabamos de montar en su defecto nos arrojara un error y en las líneas que están erróneas. Además de dicha validación también montará en caliente los volúmenes lógicos y particiones que se encuentren asociadas a un directorio dentro del archivo.

El siguiente paso será editar el archivo de configuración de `/etc/exports` en donde se tendrá que poner las políticas que seguirá cada almacenamiento para poder ser utilizado.

```
/master   192.168.100.161(rw,sync) 192.168.100.162(rw,sync) 192.168.100.160(rw,sync)
/isos     192.168.100.161(rw,sync) 192.168.100.162(rw,sync) 192.168.100.160(rw,sync)
/export   192.168.100.161(rw,sync) 192.168.100.162(rw,sync) 192.168.100.160(rw,sync)
```

Estas políticas hacen referencia a que sólo los miembros que se encuentren en el segmento 192.168.100 pueden acceder al sistema de archivos.

Una vez agregadas las líneas reiniciaremos el servicio de nfs:

```
service nfs restart
```

Con este último paso habremos terminado de configurar el servidor de almacenamiento para para poder iniciar con agregar los respectivos sistemas de archivos en el administrador.

El primer sistema de archivos que se debe agregar a nuestro administrador, es el almacenamiento donde vivirán alojadas las máquinas virtuales, en este caso el /master, le damos clic en el pestaña **storage** y nos mostrará una ventana de opciones de storage. En las cuales seleccionaremos la opción de NFS y datos como lo muestra la siguiente figura (Figura 19).

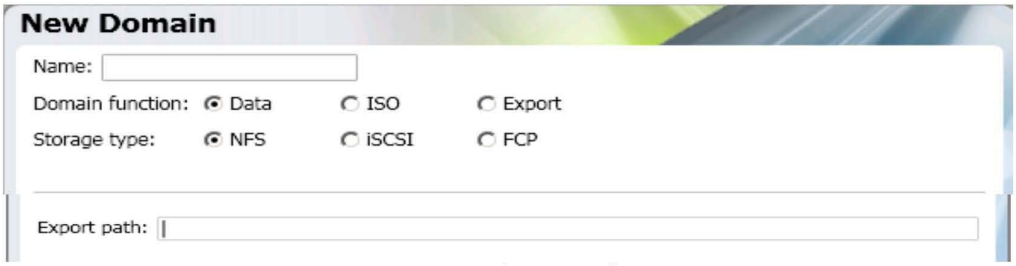


Figura 19. Asignacion de Storage al Hypervisor

Dentro del campo *export path* ingresaremos la ubicación del servidor de NFS y carpeta compartida:

```
192.168.100.163:/master
192.168.100.164:/isos
192.168.100.164:/export
```

Una vez terminada la tarea realizada en el primer sistema de archivos compartidos, seguiremos con el sistema de archivos de **isos**, y al final agregaremos la parte de exportación. En ese orden para no tener problemas con agregar los sistemas de archivos.

5. Implementar servicios sobre esquema de virtualización

Los escritorios remotos virtuales son de gran impacto en las empresas por las nuevas políticas de las tecnologías de la información que van cambiando haciendo de ellas, políticas más rigurosas y estrictas proponiendo y obligando a las empresas a centralizar la información en el centro de datos. Dando como resultado una administración más sencilla así como la implementación de los mismos. También la ventaja de tener la información centralizada y no tener que estar transportando la información a donde se mueva el escritorio remoto.

A diferencia de los servidores virtuales, los escritorios remotos virtuales tienen otros beneficios adicionales para su uso con el usuario final. Uno de varios beneficios es el poder conectar dispositivos al escritorio virtual, sin necesidad de estar frente al equipo. Alta disponibilidad al poder trabajar directamente en tu equipo desde cualquier dispositivo o cualquier PC, sin tener que estar cargando con el equipo.

Todas las ventajas mencionadas anteriormente van de la mano a contar con mayor seguridad de los escritorios, al tenerlos en sitio. Facilidad de realizar respaldos y poder trabajar con terminales tontas, eliminando la relación entre hardware robusto para poder trabajar.
Dentro de Red Hat Enterprise Virtualization, ofrece el servicio de virtualización de escritorios remotos al adquirir la suscripción de Virtualización de servidores. Es por eso que al realizar la instalación, adicionalmente se implementó el servicio para ofrecer más ventajas y beneficios de la solución.

5.1 Creación de servidores virtuales

Una vez que se tiene la infraestructura de RHEV, se pueden iniciar a crear servidores y escritorios remotos virtuales. El procedimiento para crear servidores virtuales es el siguiente:

Lo primero que tenemos que hacer es posicionarnos dentro de la pestaña de "máquinas virtuales". Dentro de la ventana encontraremos un botón que dice "Nuevo Servidor" (ver Figura 1), lo seleccionamos y empezamos a realizar la configuración, el primer paso es seleccionar el hypervisor o hosts donde se va a crear la máquina virtual y dentro de que centro de datos se alojará el servidor.

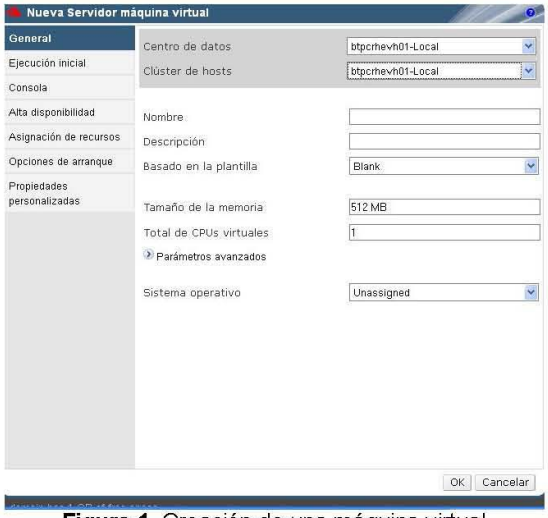


Figura 1. Creación de una máquina virtual

Dentro de esta pestaña también debemos añadir el nombre del equipo, su descripción, elegir si va a crearse en base en una plantilla (template, se explicará más adelante). Adicionalmente también seleccionaremos el hardware que pertenecerá a el servidor virtual, tanto el tamaño de la memoria como el número de CPU's virtuales y si se sabe el sistema operativo que se instalará, esto es para mejorar los parámetros de hardware desde el bios virtual y así poder darle mejor rendimiento a el servidor dentro de su sistema operativo (Figura 1).

Después de seleccionar los parámetros base de un servidor Virtual o escritorio, el siguiente paso es seleccionar las opciones de arranque, cómo crear un Storage para el servidor y un iso que anteriormente montamos varios para poder instalar cualquier sistema operativo. Y el nivel de arranque en nuestro caso como será instalación de un sistema operativo desde una media de instalación, por lo que tendremos que elegir como primer medio de arranque el ISO (ver Figura 2).

Figura 2. Opciones de arranque

Para terminar con la configuración de la máquina virtual añadiremos las interfaces de red y su disco duro virtual, ya sea por thin provisioning o completo (figura 3).

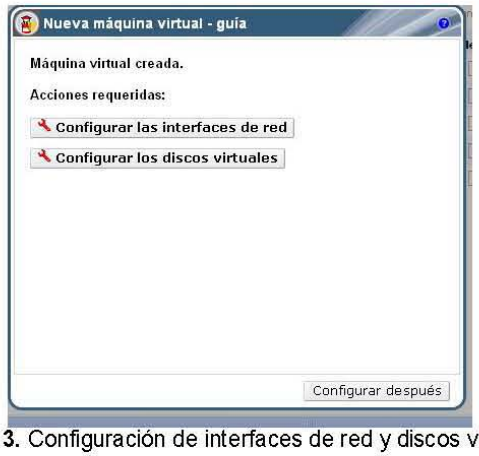


Figura 3. Configuración de interfaces de red y discos virtuales

Dentro de la configuración de interfaces de red seleccionaremos primero porque interfaz de red vamos a salir a la red LAN. Adicionalmente podremos especificar una MAC personalizada o dejar que la misma plataforma asigne una aleatoria (ver Figura 4).

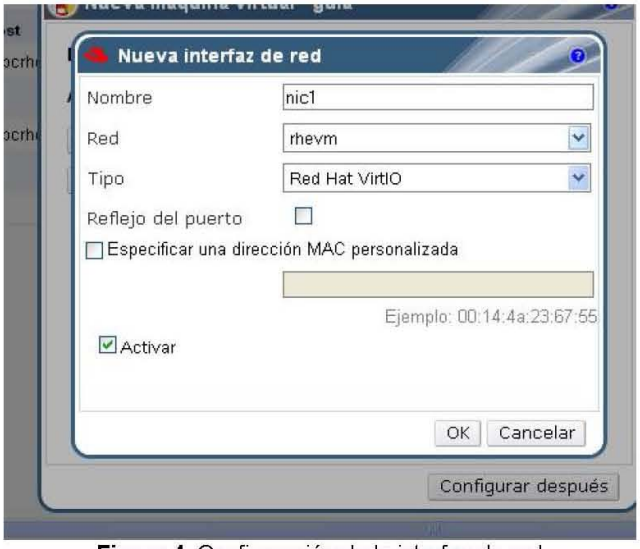


Figura 4. Configuración de la interfaz de red

5.1.1 Instalación de sistema operativo

Al haber creado la máquina virtual lo siguiente será realizar una instalación normal, cómo si tuviéramos el equipo físico, ya que añadimos la unidad de CD-rom que será el disco de instalación y tenemos todo lo que una máquina física contiene, se puede realizar el inicio de la instalación como se muestra en la siguiente figura (ver Figura 5).

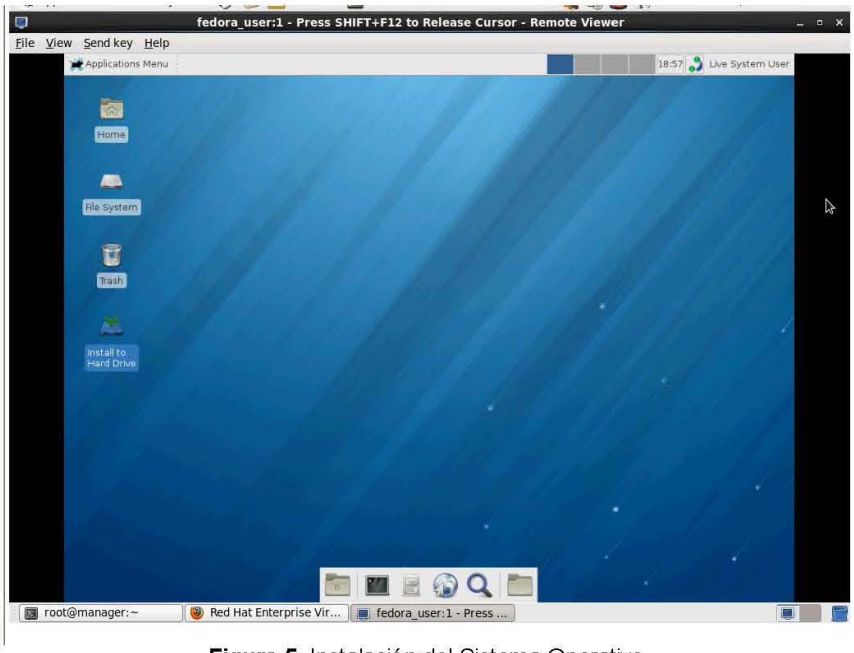


Figura 5. Instalación del Sistema Operativo

5.1.2 Configuración e instalación de servicios

Una vez configurada la máquina virtual podemos instalar cualquier servicio y utilizarla como si fuera una máquina física, al tener los servidores de esta manera, como se mencionó anteriormente se puede tener una administración centralizada, generando ahorro de gastos de energía, de enfriamiento.

Para esta parte se instalaron algunos servicios entre ellos se encuentra un Zimbra es un servidor de correo electrónico gratuito, casi con las mismas funciones de Outlook y otros servidores de correo electrónico. Es uno de los mejores por sus características y funcionalidad de administración y costos de licenciamiento y mantenimiento que son mucho menores a los proporcionados por Microsoft.

El servidor fue instalado con la finalidad de poder demostrar la funcionalidad, desempeño y disponibilidad de los servidores virtuales sobre la plataforma de RHEV.

5.1.3 Migración de servidores Físicos a virtuales

Además se migraron los servicios de físico-virtual mencionados en el capítulo 1. Cumpliendo todas las expectativas, se realizaron las migraciones de físico a virtuales con el único inconveniente de no poder migrar servidores con un kernel menor, es decir no se pudieron migrar servidores con Red Hat Enterprise 3 y con un kernel menor a 2.6.X.

Dentro de la migración se realizaron varios procedimientos y enfrentando varios problemas como el anterior mencionado. Los pasos a seguir para realizar este interesante procedimiento fueron los siguientes:

Se creó un servidor que sirvió como pivote para poder ser el encargado de realizar el intercambio y conversión de imágenes de máquinas virtuales (pivote), dicho servidor tuvo que tener características suficientes para poder soportar la máquina física a virtualizar y almacenamiento suficiente.

Dentro del servidor que utilizaremos como pivote para realizar la migración se instalaron paquetes como el p2v de RHEL, se configuro para poder virtualizar de forma paravirtualizada con KVM (kernel Virtual machine).

En la máquina pivote se pasará bit a bit el disco duro de la máquina física que estamos migrando con una extensión *.img* para que pueda ser compatible con el sistema de paravirtualización. Una vez terminada la copia del disco duro se procede a correr la máquina para comprobar y corroborar que no sufrió problemas o pérdida de algún bit en la copia.

Si se puede arrancar la máquina se procede a correr el comando de p2v, dicha máquina se empezará a migrar a un almacenamiento compartido de Red Hat Enterprise Virtualization conocido como almacenamiento de exportación.

Al terminar la migración al almacenamiento de exportación, el último paso será importar la máquina virtual y con ese paso terminaremos la migración de físico a virtual (Todas las configuraciones y procedimiento de los comandos a seguir se encuentran en las bitácoras de instalación.

En la siguiente imagen (Figura 6) se describe mediante un esquema como es el circulo que sigue el procedimiento de físico a virtual.

Figura 6. Esquema de Migración físico-virtual

6.2 Creación de escritorios remotos virtuales

En la creación de escritorios remotos virtuales se realiza casi de la misma manera que los servidores Virtuales, con la diferencia que una vez creada la plantilla podremos crear un conjunto de escritorios dentro de un mismo almacenamiento compartido.

Para iniciar la instalación el primer paso es posicionarnos en la pestaña de máquinas virtuales y después seleccionar el botón de nuevo escritorio como se muestra en la siguiente imagen (Figura 7).

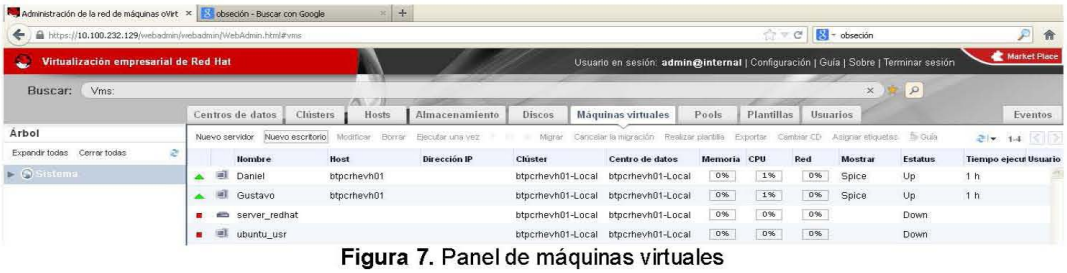


Figura 7. Panel de máquinas virtuales

Nos aparecerá una imagen muy similar a la de servidores virtuales con la diferencia que cuenta con más características que tendremos que agregar. Iniciamos con las básicas que son la ubicación del hypervisor donde se alojará para su creación y después el centro de datos a la cual pertenecerá nuestro escritorio virtual. Entre las opciones siguientes daremos nombre y una descripción al escritorio, así como también la plantilla o si se creará desde cero cómo será la primera máquina lo dejaremos en blanco y finalizaremos la primera parte señalando cuanto de memoria RAM y número de CPU's virtuales va a tener cada escritorio y el sistema operativo para mejorar los parámetros a nivel del bios para mejorar el rendimiento de los sistemas operativos (Ver Figura 8).

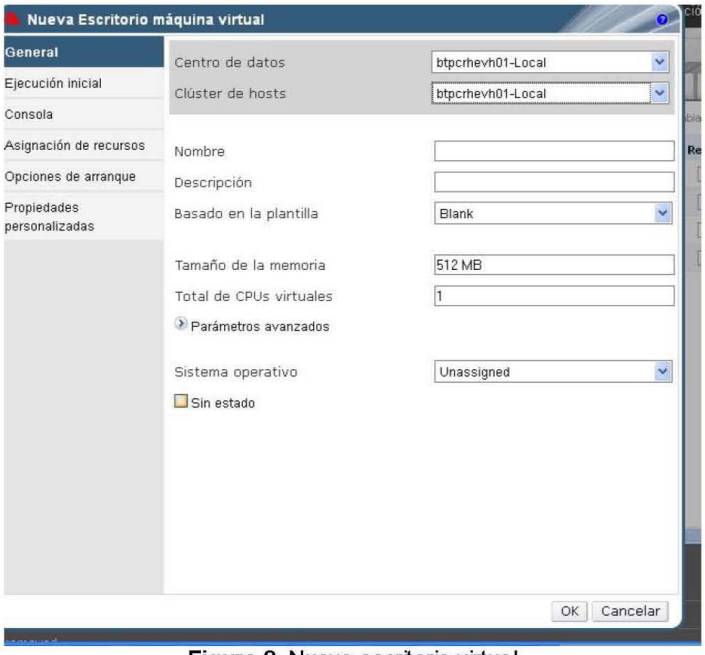


Figura 8. Nuevo escritorio virtual

La siguiente pestaña hace referencia a si el escritorio remoto virtual pertenecerá a algún dominio del centro de datos y así poder tomar las credenciales de nuestro active directory y/o IPA (Ver figura 9).

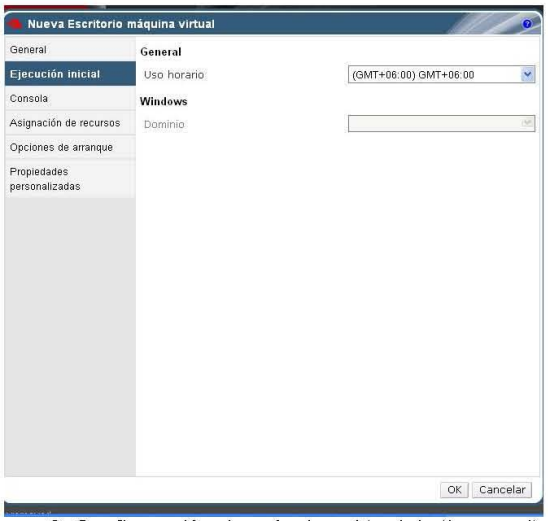


Figura 9. Configuración de máquina virtual de tipo escritorio

Una de las grandes diferencias de un servidor y un escritorio remoto es que el escritorio está pensado para ser utilizado por el usuario final simulando una máquina física de escritorio en la cual pueda realizar todas sus tareas del trabajo o de uso personal en cualquier equipo únicamente conectándose mediante un navegador "internet Explorer", la manejabilidad de conectar cualquier dispositivo USB en el escritorio remoto.

En los siguientes campos tenemos que definir qué tipo de protocolo va a utilizar si será VNC o SPICE (las diferencias se definieron en el capítulo de conceptos de tesis). Por mejor desempeño en cada máquina utilizaremos el protocolo de SPICE y de esta manera podremos ocupar el soporte a USB de forma legacy para que cada que se habrá un escritorio virtual en cualquier máquina o dispositivo pueda tomar la USB que se conecte físicamente desde el equipo o terminal tonta de la cual se esté trabajando con el escritorio virtual.

Y por último, definir cuantos monitores se pone por escritorio, cabe mencionar que con el protocolo SPICE automáticamente define quien proporciona el Hardware de Video de mejor calidad, ya sea el hypervisor o la máquina o terminal tonta con la cual se esté trabajando (ver Figura 10).

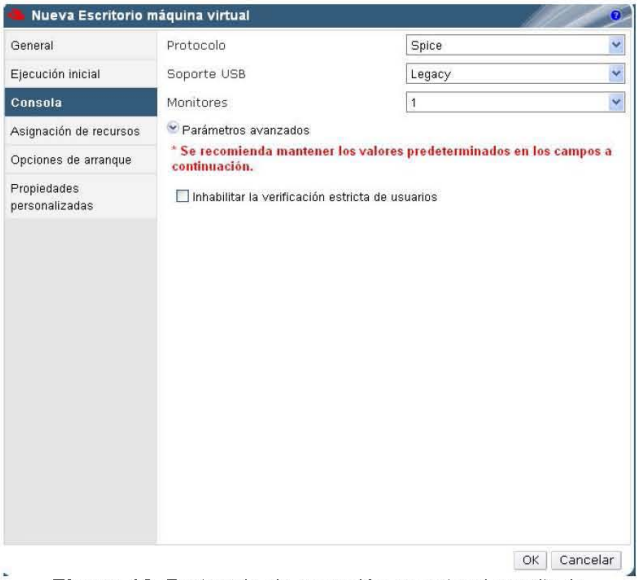


Figura 10. Protocolo de conexión remota al escritorio

En el siguiente apartado tendremos que definir el tamaño de la memoria RAM minima para poder funcionar el escritorio Virtual (ver Figura 11).

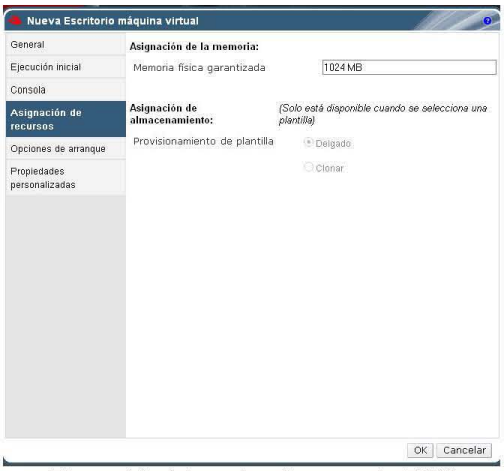


Figura 11. Asignacion de memoria RAM

En el siguiente apartado que se trata de ejecución inicial haremos lo mismo que con los servidores virtuales el cual será señalar los niveles de arranque de nuestra máquina virtual, como se configura originalmente a nivel del BIOS las máquinas físicas.

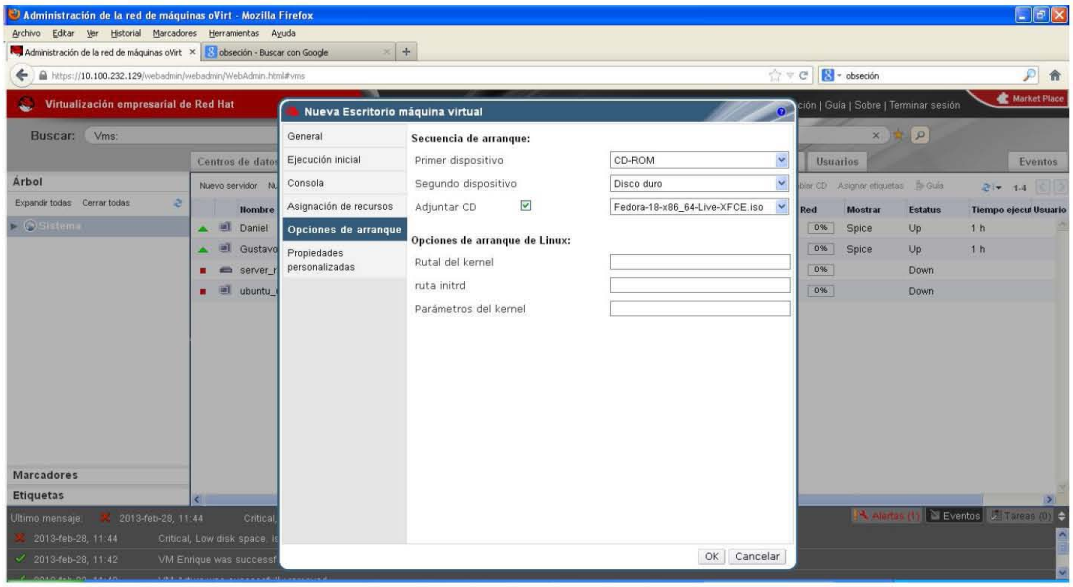


Figura 12. Orden de secuencia de arranque

Al final sólo será necesario configurar las interfaces virtuales de red y configurar los discos que tendrá el escritorio Virtual que acabamos de crear (figura 13).

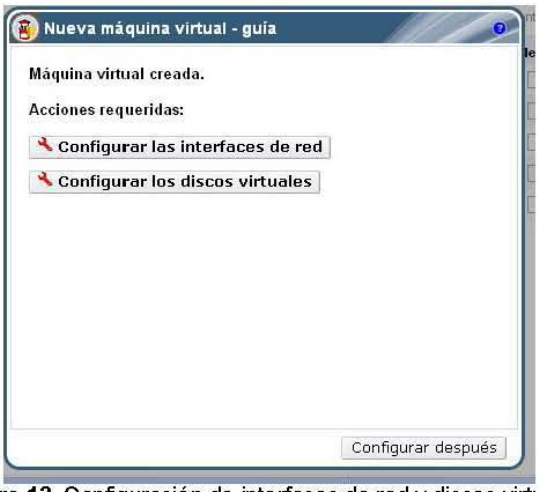


Figura 13. Configuración de interfaces de red y discos virtuales

Dentro de la configuración de interfaces de red seleccionaremos primero porque interfaz de red vamos a salir a la red LAN. Adicionalmente podremos especificar una MAC personalizada o dejar que la misma plataforma asigne una aleatoria (ver Figura 14).

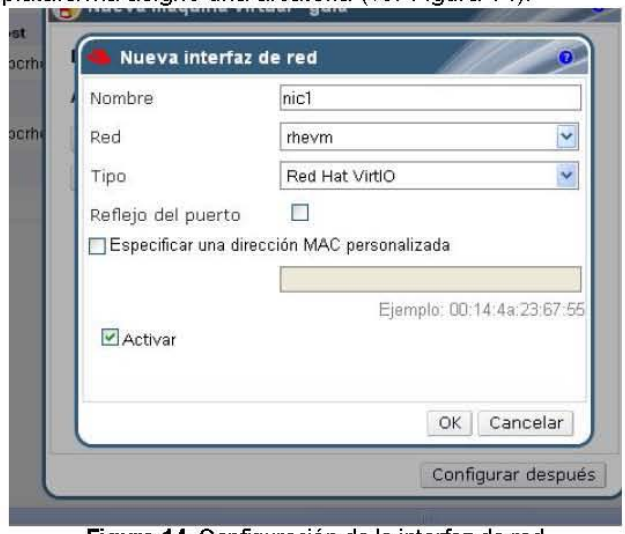


Figura 14. Configuración de la interfaz de red

Iniciamos el escritorio virtual creado e iniciamos con la media de instalación montada para poder iniciar con la instalación del sistema operativo. Paso 1 seleccionar el escritorio remoto virtual, el paso 2 para encender la máquina es dar clic en el botón de “play” y el paso 3 será dar clic en icono de pantallita para que nos muestre el escritorio remoto, cómo se muestra en la siguiente imagen (Figura 15).

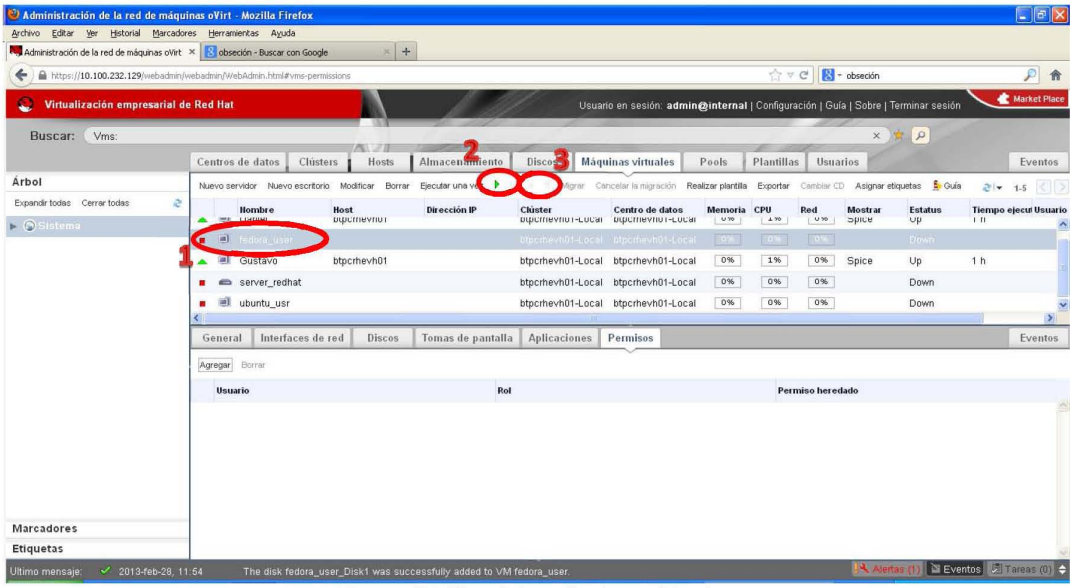


Figura 15. Panel de máquinas virtuales

Una vez iniciado el escritorio Virtual podremos instalarlo de la misma forma en la que se instalan los equipos físicos. Sólo que por ser la primera instalación evitaremos poner parámetros que hagan la autenticación o diferencia entre un equipo y otro, con la finalidad de poder realizar una plantilla y no tener que instalar el mismo sistema operativo y escritorio. Con la plantilla ahorrara tiempo a la hora de crear futuros escritorios bajo el mismo sistema operativo y con las mismas características de Hardware (figura 16).

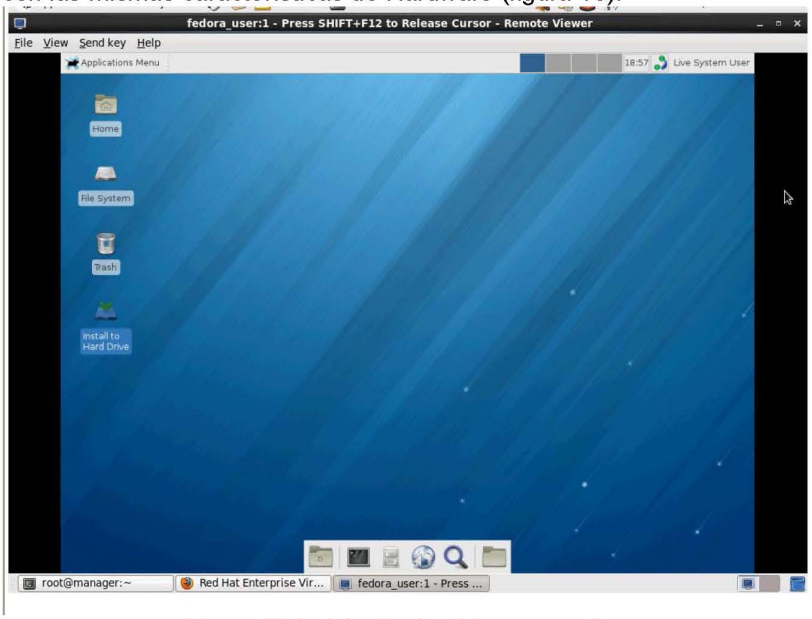


Figura 16. Instalación del sistema operativo

En la siguiente figura (Figura 17), nos muestra una pantalla pidiendo la contraseña que será usada para el usuario Root.

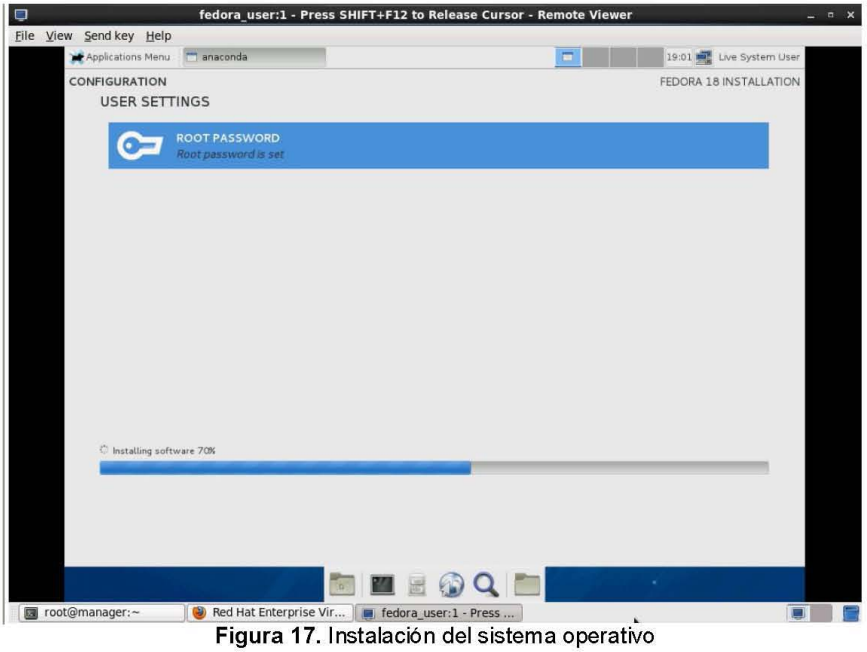


Figura 17. Instalación del sistema operativo

6.2.1 Creación de usuarios y asignación de escritorios virtuales

Al haber creado una plantilla y algunos escritorios virtuales será necesario asociar el escritorio al personal que utilizará dicho equipo.

Parar realizar dicha actividad nos posicionaremos en la parte de creación de Usuarios y agregaremos usuarios. Previamente en la instalación se mencionó el agregar o conectar a un active directory o IPA para poder utilizar su base de usuarios y credenciales (Figura 18).

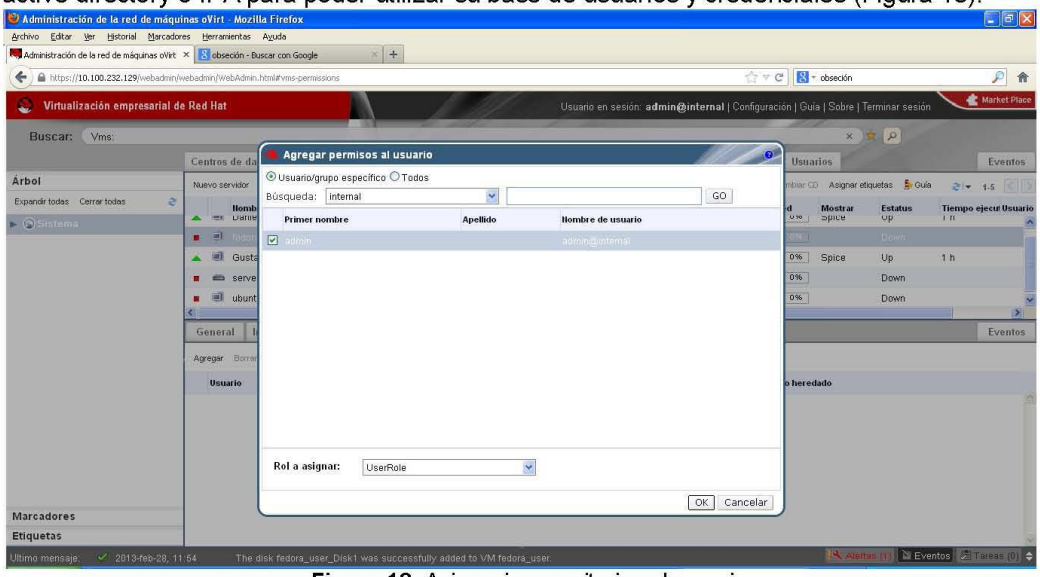


Figura 18. Asignacion escritorios al usuarios

La administración de usuarios y escritorios es a criterio del administrador de la infraestructura de virtualización, sólo cabe señalar que varios usuarios pueden tener varias máquinas o escritorios Virtuales. Y las máquinas virtuales pueden tener varios usuarios, esta relación es de muchos a muchos.

Para terminar la parte de creación de usuarios también tenemos que tener en cuenta que tendremos que solicitar apoyo para que nos proporcionen las credenciales de conectividad a la base de active directory y/o IPA.

IPA es un similar a LDAP o active directory de Microsoft sólo que una solución creada por los desarroladores de Red Hat. Basada en el sistema operativo red hat Enterprise Linux versión 6.

5.2.2 Instalación de paquetes de VirtIO

Los paquetes de VirtIO son drivers que se cargan en la máquina y escritorios virtuales para poder tener toda la compatibilidad de las máquinas virtuales con la terminal a la cual estemos accediendo a ellas. Los paquetes se descargan de la página oficial de Red Hat y antes de crear la plantilla de algún sistema operativo habrá que instalar los paquetes para evitar instarlos en otra ocasión. Los drivers son compatibles directamente con el protocolo del cliente de virtualización SPICE.

Antes de abrir cualquier máquina virtual de la infraestructura de Red Hat Enterprise Virtualization es recomendable instalar una paquetería que viene en una ISO para clientes en Windows y clientes en red hat.

Esta paquetería se llama RHEV-tools", que nos ayudará a poder utilizar los recursos de Hardware de nuestra terminal tonta y así poder conectar la USB y/o cualquier dispositivo a el escritorio Virtual (ver Figura 19).

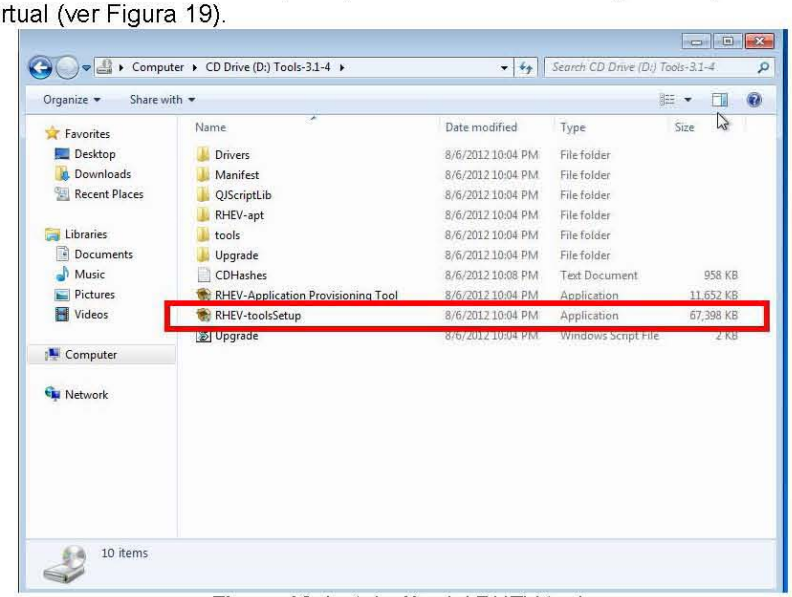


Figura 19. Instalación del RHEV-tools

Cabe mencionar que al virtualizar el Hardware con VirtIO daremos el mismo desempeño que lo daría el Hardware físico, como se muestra en la siguiente gráfica de performance haciendo una comparación contra una emulación, con drivers de vmware, citrix, los de VirtIO de red hat y los nativos (equipo físico) (ver figura 20).

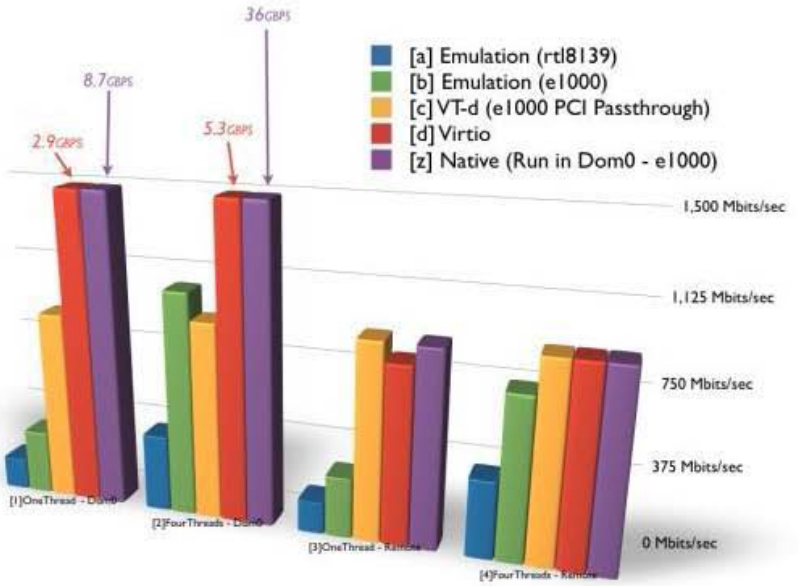


Figura 20. Comparativa de Drivers para la optimización de uso de hardware

5.2.3 Instalación de cliente Spice

La instalación del cliente de Spice es para poder compartir los recursos de Hardware de nuestra terminal tonta o equipo donde nos conectemos a la máquina virtual.

Cabe mencionar que en equipos Windows únicamente se puede trabajar directamente con el explorador nativo de Windows, el cual con el Active-X hará la instalación del cliente de SPICE de forma automática con solo evitar el bloqueo de ventanas emergentes.
Y la instalación la realiza de forma automática.

También se puede correr el cliente sobre un Linux sólo que hay que instalar paquetes adicionales como lo es el **Spice-client.** Este paquete es un pluggin realizado para Mozilla Firefox. Actualmente se siguen trabajando en el desarrollo de generalizar el uso de la herramienta de SPICE sobre cualquier navegador.

Para finalizar esta parte, se agrega que se sigue trabajando en aplicaciones y desarrollos para mejorar el uso del cliente de SPICE, según fuentes de Red Hat en agosto lanzarán una aplicación para poder tener el escritorio virtual sobre cualquier Android. Lo cual mejorará la portabilidad y disponibilidad de nuestros escritorios.

6. Instalación de Zenoss Core

6.1 Monitoreo de equipos en USECAD antes de la instalación de Zenoss

Los dispositivos de red y servidores de USECAD no cuentan con un software dedicado para el monitoreo de rendimiento y disponibilidad de cada uno de estos equipos, en un ambiente de TI es buena práctica utilizar alguna herramienta de monitoreo que nos permita extraer información relevante sobre las caracterísitas y funcionalidad de los equipos, ésta nos permite tener un control de inventario, saber sobre la disponibilidad del equipo, configuración, desempeño y eventos. Los administradores de TI de USECAD utilizan algunos comandos propios del sistema operativo Linux los cuales ejecutan manualmente cuando requieren observar el comportamiento del equipo o resolver problemas que ocurran en el sistema, la información que muestran los comandos tiene que ser visualizada en varias pantallas o bien almacenada en archivos. Algunos ejemplos de comando utilizados son los siguientes:

`uptime`: permite ver la carga promedio del sistema para los últimos 1, 5 y 15 minutos

```
# uptime
10:21:06 up 5 days, 19:11,  2 users,  load average: 0.08, 0.03, 0.00
```

`top`: Este comando permite una visión dinámica del sistema en tiempo real. El comando muestra un listado de los procesos que se están ejecutando. Proporciona además un gran número de datos como el uso de la memoria y procesador.

```
# top
top - 14:21:10 up 6 days,  3:01,  2 users,  load average: 0.00, 0.00, 0.00
Tasks: 125 total,   2 running, 123 sleeping,   0 stopped,   0 zombie Cpu(s):
0.7%us,  0.7%sy,  0.0%ni, 98.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st Mem:
1293232k total,  1268956k used,    24276k free,   100388k buffers Swap:
1020116k total,      380k used,  1019736k free,   969436k cached

PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
2106 nobody    18   0 90464 1728 1004 S  1.0  0.1  12:20.85 gmetad
4175 root      18   0  4332  828  684 S  0.3  0.1   0:07.61 watch
19382 root      15   0 10232 2972 2400 R  0.3  0.2   0:00.03 sshd
19569 root      15   0  2428 1040  804 R  0.3  0.1   0:00.01 top
1 root      15   0  2160  640  552 S  0.0  0.0   0:00.63 init
2 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 migration/0
3 root      34  19     0    0    0 S  0.0  0.0   0:00.19 ksoftirqd/0
4 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
5 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 events/0
```

`free`: este comando muestra información relativa al uso de la memoria. Sin embargo, el resultado mostrado por este comando es estático, para poder visualizar el uso de la memoria de manera dinámica, se le puede agregar el comando `watch`:

```
# watch free -m
Every 2.0s: free -m
Thu Apr 25 12:57:01 2013               total       used       free
shared    buffers     cached Mem:          1262       1239         23
0          92        953 -/+ buffers/cache:        193       1069 Swap:
996          0        995
```

Cabe mencionar algunos otros comandos utilizados manualmente por los administradores como: `vmstat`, `iostat`, `du`, `df`, `ps`. Al no contar con una herramienta específica para esta tarea que permita centralizar, procesar y analizar la información, propusimos la utilización de la herramienta de monitoreo llamada Zenoss, misma que utiliza los comandos ya mencionados, estos son utilizados por la herramienta de monitoreo para la extracción de datos de cada uno de los servidores, conectándose a ellos mediante SSH, SNMP o WMI. Zenoss centraliza la información, la procesa y la muestra en pantalla, de esta manera los administradores pueden tener una consola vía web para observar eventos y gráficas del comportamiento de cada uno de estos equipos, de tal manera que permita tener un

historial de cada uno de ellos. A continuación veamos el proceso de instalación de esta herramienta sobre Linux.

Requerimientos

Para la instalación del software de monitoreo de Zenos debemos considerar los siguientes requerimientos de hardware para un servidor virtual aunque también aplican para la instalación de Zenoss en un servidor físico. La tabla siguiente esta basada en la documentación de Zenoss Core.

Ambiente	Memoria RAM	CPU	Disco
1-50 Dispositivos a monitorear	4GB	2 Core	80 GB

Tabla 1. Requerimientos de Hardware

En cuanto a los requerimientos de software utilizamos la versión de RedHat Enterprise 6 a 64 bits con la siguiente tabla de particionamiento de acuerdo a los requerimientos de Zenoss Core:

Partición	Punto de Montaje	Sistema de Archivos	Tamaño
Boot	`/boot`	Ext4	200 MB
Raiz	`/`	Ext4	10 GB
Zenoss	`/opt`	Ext4	Espacio Restante del disco Duro
Swap	`swap`	swap	8GB

Tabla 2.

Este es el esquema de particionamiento del sistema operativo asignado a Zenoss, posteriormente verificamos los siguientes puntos:

- Deshabilitamos Selinux para no tner problemas con contextos.
- `/opt/zenoss` debe ser un directorio y no un enlace simbólico
- El directorio `/home/zenoss` debe existir como parte del usuario zenoss y debe ser escribible por root

Tareas

Antes de instalar Zenoss realizamos las siguientes tareas:

- Configurar el Firewall
- Instalar y configurar repositorios, prerrequisitos de sotware y paquetes adicionales

La siguiente tabla es una lista de prerrequisitos de software para instalar Zenoss Core

Prerequisite	Version
Oracle Java	1.6 Update 31 or later. (1.7 is not supported.)
RRDtool	1.4.7 or later
MySQL Community Server	5.5.25 or later
RabbitMQ	2.8.4 or later
Nagios Plugins	1.4.15 or later
Erlang	R12B

Tabla 3. Prerrequisitos de Software

Configuración del Firewall

Zenoss Core requiere que los siguientes puertos estén abiertos en el Firewall si es que estamos trabajando en un ambiente seguro, por tanto los dimos de alta en `iptables`, si no estamos utilizando el firewall podemos omitir la siguiente tabla.

Puerto	Protocolo	Dirección a Zenoss Core	Descripción
11211	TCP/UDP	Entrante	Memcached
8080	TCP	Entrante	Web Interface

514	UDP	Entrante	Syslog
162	UDP	Entrante	SNMP Traps

Tabla 4. Puertos utilizados por Zenoss Core para el monitoreo de equipos.

Instalacion de Oracle Java

OpenJDK no esta soportado por Zenoss Core, por tanto es necesario desinstalarlo en caso de que esta instalado en el servidor de RedHat y posteriormente instalar Oracle Java.

El entorno de ejecución JAVA (JRE) (64 bits) ofrece las bibliotecas, la máquina virtual Java y otros componentes para ejecutar applets y aplicaciones escritas en el lenguaje de programación Java, las cuales Zenoss contiene dentro de su solución de monitoreo. Además, hay dos tecnologías de implementación clave que forman parte de JRE: el plug-in Java, que permite que las applets se ejecuten en navegadores populares del cual hace uso el Dashboard o consola principal de Zenoss, y Java Web Start, que implementa aplicaciones autónomas en una red.

Para identificar que versión de java tenemos, ejecutamos el siguiente comando en la terminal:

```
[root@zenosscore ~]# java -version
java version "1.6.0 24" OpenJDK Runtime Environment (IcedTea6 1.11.1)
(rhel-1.45.1.11.1.el6-x86 64) OpenJDK 64-Bit Server VM (build 20.0-b12,
mixed mode)
```

Eliminamos la vesion OpenJDK de java.

```
[root@zenosscore ~]# yum remove java
```

1.- Descargamos Oracle JRE, pesa alrededor de 20 MB:

```
[root@zenosscore ~]# wget -O jre-6u31-linux-x64-rpm.bin
http://javadl.sun.com/webapps/download/AutoDL?BundleId=59622
```

2.- Cambiamos Permisos:

```
[root@zenosscore ~]# chmod +x ./jre-6u31-linux-x64-rpm.bin
```

3.- Instalamos Oracle JRE:

```
[root@zenosscore ~]#./jre-6u31-linux-x64-rpm.bin
```

4.- Actualizamos JAVA_HOME. Agregamos la siguiente línea al final del archivo `/etc/profile`

```
export JAVA_HOME=/usr/java/default
```

5.- Verificamos la versión de java que acabamos de instalar:

```
[root@zenosscore ~]# java -version
```

Instalacion y configuracion de RRDtool

RRDtool es el acrónimo de *Round Robin Database Tool* . Se trata de una herramienta que trabaja con una base de datos que maneja planificación según Round-Robin. Esta técnica trabaja con una cantidad de datos fija, definida en el momento de crear la base de datos, y un puntero al elemento actual.

El funcionamiento es el siguiente: se trata la base de datos como si fuese un círculo, sobrescribiendo los datos almacenados con anterioridad una vez alcanzada la capacidad máxima de la misma. Esta capacidad máxima dependerá de la cantidad de información que se quiera conservar como historial.

Su finalidad principal es el tratamiento de datos temporales y datos seriales como temperaturas, transferencias en redes, cargas del procesador, etc. Algunos proyectos que utilizan RRDtool son: Cacti, Ganglia, JFFNMS, Lighttpd, MRTG,Munin, Smokeping, Zenoss, etc.

1.- Descargamos e instalamos los prerrequisitos de RDDtool y dependencias:

```
[root@zenosscore ~]# wget http://pkgs.repoforge.org/rpmforge-
release/rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm
```

```
[root@zenosscore ~]# yum -y --nogpgcheck localinstall rpmforge-
release-0.5.2-2.el6.rf.x86_64.rpm
```

2.- Instalamos RRDtool

```
[root@zenosscore]# yum -y --enablerepo=rpmforge-extras --nogpgcheck
install rrdtool-1.4.7
```

Instalación y configuración de MySQL Community Server

En esta tarea instalamos MySQL, aunque también es posible utilizar por separado MySQL Server en el caso de que monitoriemos mas de 1000 dispositivos, esta base de datos almacenara toda y cada una e la información que extraera Zenoss de cada uno de los dispositivos monitoreados, esta base de datos puede ser respaldada para tener un backup de los datos de Zenoss y en caso de contingencia poder restaurar la base de datos en otro servidor.

1.- Descargamos los archivos de instalación de MySQL:

Buscamos los archivos en: http://dev.mysql.com/downloads/mysql/#downloads

Seleccionamos los paquetes *MySQL Client Utilities, MySQL Sever y MySQL Shared* para la plataforma de Oracle & RedHat Linux 6.

```
[root@zenosscore ~]# http://mysql.ntu.edu.tw/Downloads/MySQL-5.5/MySQL-
shared-5.5.27-1.el6.x86_64.rpm
```

```
[root@zenosscore ~]# wget http://mysql.ntu.edu.tw/Downloads/MySQL-
5.5/MySQL-server-5.5.27-1.el6.x86_64.rpm
```

```
[root@zenosscore ~]# wget http://mysql.ntu.edu.tw/Downloads/MySQL-
5.5/MySQL-client-5.5.27-1.el6.x86_64.rpm
```

2.- Instalacion de los RPM de MySQL

Eliminamos cualquier paquete relacionado con MySQL para evitar conflictos

```
[root@zenosscore ~]# rpm -qa | grep -i mysql
mysql-libs-5.1.61-4.el6.x86_64
[root@zenosscore ~]# rpm -e --nodeps mysql-libs
```

Instalamos los rpm de MySQL

```
[root@zenosscore ~]# rpm -ivh MySQL-client-5.5.27-1.el6.x86_64.rpm
Preparing...                ########################################### [100%]
1:MySQL-client              ########################################### [100%]
[root@zenosscore ~]# rpm -ivh MySQL-shared-5.5.27-1.el6.x86_64.rpm
Preparing...                ########################################### [100%]
1:MySQL-shared              ########################################### [100%]
[root@zenosscore ~]# rpm -ivh MySQL-server-5.5.27-1.el6.x86_64.rpm
Preparing...                ########################################### [100%]
1:MySQL-server              ########################################### [100%]
```

3.- Creamos el archivo `/etc/my.cnf` y agregamos las siguientes líneas

```
[mysqld]
max_allowed_packet=16M
innodb_buffer_pool_size=256M
innodb_additional_mem_pool_size=20M
```

4.- Ejecutamos los siguientes comandos para iniciar el demonio de `mysql` y configurar su inicio en automático en un `reboot`:

```
[root@zenosscore ~]# service mysql start
[root@zenosscore ~]# chkconfig --add mysql
[root@zenosscore ~]# chkconfig --level 2345 mysql on
```

5.- Configuramos MySQL para la instalación de Zenoss Core:

```
[root@zenosscore ~]# mysqladmin -u root password ''
[root@zenosscore ~]# mysqladmin -u root -h localhost password ''
```

Habilitar el acceso al repositorio de EPEL

Los siguientes pasos fueron necesarios para habilitar el acceso a *Extra Packages for Enterprise Linux (EPEL)*, estos paquetes son desarrollados para distribuciones como Fedora, RedHat y CentOS los cuales no estan disponibles en la pagina donde se distribuye cada sistema operativo, Zenoss requiere de paquetes adicionales para su funcionamiento.

1.- Descargamos el RPM que creara los repositorios de EPELx

```
[root@zenosscore ~]# wget -r -l1 --no-parent -A 'epel*.rpm'
http://dl.fedoraproject.org/pub/epel/6/x86_64/
```

2.- Instalamos el RPM

```
[root@zenosscore ~]# yum -y --nogpgcheck localinstall
dl.fedoraproject.org/pub/epel/6/x86_64/epel-*.rpm
```

Instalación de RabbitMQ

RabbitMQ es un software de negociación de mensajes de código abierto, y entra dentro de la categoría de middleware de mensajería. Implementa el estándar Advanced Message Queuing Protocol (AMQP). El servidor RabbitMQ está escrito en Erlang y utiliza el *framework* Open Telecom Platform (OTP) para construir sus capacidades de ejecución distribuida y conmutación ante errores.

1.- Descargamos el RPM

```
[root@zenosscore ~]# wget http://www.rabbitmq.com/releases/rabbitmq-
server/v2.8.4/rabbitmq-server-2.8.4-1.noarch.rpm
```

2.- Instalamos el RPM

```
[root@zenosscore ~]# yum -y --nogpgcheck localinstall rabbitmq-server-
2.8.4-1.noarch.rpm
```

Nota: debemos validar que las versiones de cada uno de los paquetes instalados sean las correspondientes a las mencionadas en la **Tabla 1** de este capitulo. En la mayoría de los casos los repositorios son actualizados y las versiones de los paquetes son mas recientes que las requeridas por Zenoss, si esto sucede tendremos que buscar en otros repositorios los paquetes según los requerimientos, también puede existir el caso de resolver las dependencias de forma manual.

3.- Ejecutamos los siguientes comandos para iniciar el demonio de `rabbitmq-server` y configurar su inicio en automático en un `reboot`:

```
[root@zenosscore ~]# service rabbitmq-server start
[root@zenosscore ~]# chkconfig rabbitmq-server on
```

Instalacion de Zenoss Core

Los siguientes pasos fueron ejecutados para la instalación de Zenos Core y los ZenPacks, todos los comandos se ejecutaron como usuario `root`.

Los paquetes de instalación se descargaron de:

http://community.zenoss.org/community/download

1.- Instalación de Zenoss Core

```
[root@zenosscore ~]# yum -y --nogpgcheck localinstall zenoss-
4.2.0.el6.x86_64.rpm
```

Inicialización y configuración de `memcached` y `snmp`

Los siguientes comandos fueron utilizados para inicializar y configurar los demonios de `memcached` y `snmp`. `memcache` es un servicio de Linux, diseñado para aliviar la carga de la base de datos en aplicaciones web dinámicas mediante el almacenamiento de objetos en memoria mismo que utiliza Zenoss en su Dashboard.

Configuración de los demonios para su inicio automático después de un reboot.

```
[root@zenosscore ~]# service memcached start
[root@zenosscore ~]# chkconfig memcached on
[root@zenosscore ~]# service snmpd start
[root@zenosscore ~]# chkconfig snmpd on
```

Inicialización de Zenoss Core e instalación de los Core Zenpacks.

1.- Primero iniciamos el servicio de Zenoss para poder instalar los ZenPacks:

```
[root@zenosscore ~]# service zenoss start
```

2.- Instalamos los Core ZenPacks

```
[root@zenosscore ~]# yum -y --nogpgcheck localinstall zenoss-core-
zenpacks-4.2.0.el6.x86_64.rpm
```

Primeras configuraciones en Zenoss Core

Después de la instalación, realizamos algunas configuraciones iniciales como el password del usuario **admin**, dar de alta un segundo usuario con menos privilegios de admin para la gestión de Zenoss Core y poder agregar algunos servidores para monitorear.

Abrimos un navegador y tecleamos la IP o Hostname del servidor: http://zenosscore:8080 y veremos la página inicial (Figura 1) de las primeras configuraciones de Zenoss.

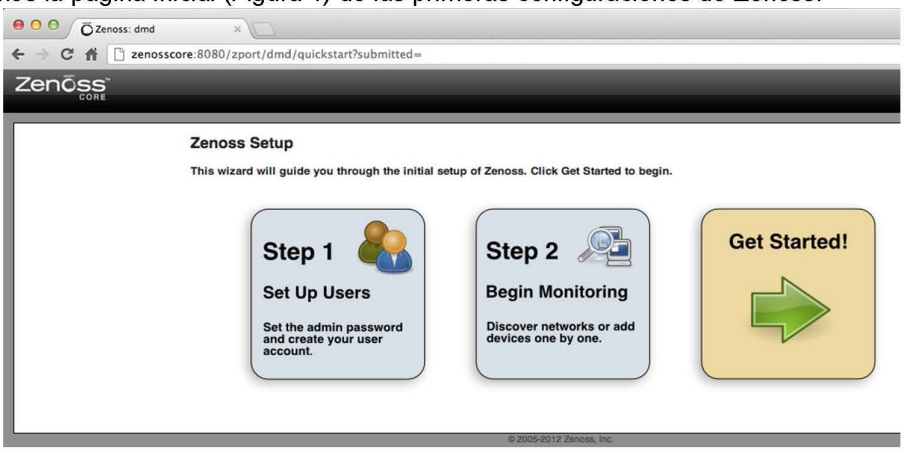


Figura 1. Portal de inicio de Zenoss Core

1.- Damos clic en “Get Started”, asignamos un password al usuario root y definimos un segundo usuario para la gestion de tareas en Zenoss Core (Figura 2):

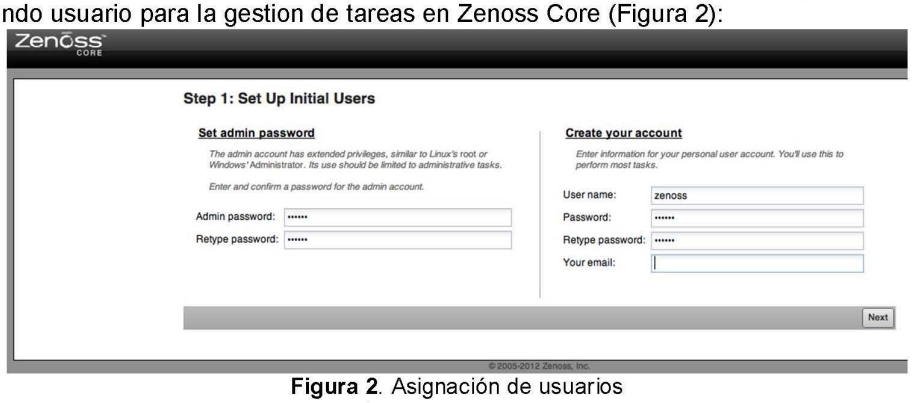


Figura 2. Asignación de usuarios

2.- Damos clic en Next y a continuación veremos el Dashborad de Zenoss Core, a partir de este momento podemos comenzar a añadir dispositivos para monitorear, este apartado lo veremos en el subcapítulo 6.3 de configuración de servidores.

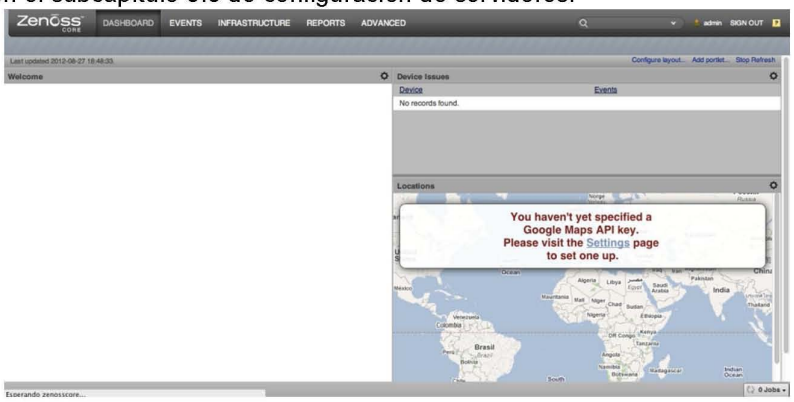


Figura 3. Dashboard de Zenoss Core

6.2 Lista de requerimientos para monitoreo de sistemas operativos en ambientes seguros

En un ambiente de red con esquema de seguridad es necesario considerar un número de puertos para implementar reglas de entrada y salida en firewalls para la comunicación de Zenoss a los servidores a monitorear y viceversa.

Monitoreo de servidores con plataforma Windows

Requisitos

Habilitar ping

- Se tiene que permitir el tráfico del protocolo ICMP entre el servidor Microsoft Windows y el servidor Zenoss.

Configuración del servidor Windows

- Se requiere la cuenta de administrador local o administrador de dominio.
- Se requiere habilitar el servicio WMI para extraer datos adicionales referentes al sistema operativo Windows, mismos que no se pueden obtener con SNMP y poder tener un monitoreo mas compleot del sistema.

Configuración de comunidad de SNMP

- Se requiere una comunidad de SNMP de sólo lectura.
- El firewall de Windows debe estar deshabilitado o en su defecto incluir las llaves de registro necesarias.
- Para probar la conectividad hacia el servicio de WMI podemos usar el comando `wmic` desde el servidor Zenoss junto con el usuario de administración del equipo Windows:

```
[root@zenosscore ~]# wmic -U 'user' //dirIPServerWin 'select * from
Win32_computerSystem'
```

Configuración de comunidad SNMP

- Se requiere de una comunidad de SNMP de solo lectura
- Si trabajamos con un firewall entre el servidor Windows y el servidor Zenoss, se tiene que permitir el tráfico en el puerto 161 de SNMP

Nota: La siguiente sección es para forzar a los servicios de WMI y DCOM a usar puertos fijos

Sección A. Configuración *de registros en Windows*

Nota: Este procedimiento aplica cuando existe un firewall entre el servidor de monitoreo Zenoss y el servidor monitoreado MS Windows Server, ya sea un firewall por software o por hardware.

DCOM asigna dinámicamente un puerto por proceso. Necesitamos decidir cuántos puertos deseamos asignar a los procesos DCOM, lo que equivale al número de procesos DCOM simultáneos a través del firewall.

Debemos abrir todos los puertos UDP y TCP correspondientes a los números de puerto que se van a usar. También es necesario abrir el puerto TCP/UDP 135, que se utiliza para el punto

final de mapeo RPC, entre otras cosas. Debe permitirse el tráfico para el puerto 135 ya que este es necesario para el monitoreo con WMI, por seguridad debemos utilizar este puerto de ser posible solo en la red interna, ya que es objetivo de constantes ataques para hacer vulnerable Windows.

Además, debemos editar el registro donde se especifica que puertos se han reservado para DCOM. Esto es en la llave de registro :

`HKEY_LOCAL_MACHINES\Software\Microsoft\Rpc\Internet`

En la siguiente tabla se muestra la configuración de la llave de registro para restringir el rango de puertos DCOMs a 10 puertos.

Registro	Tipo	Configuración
Ports	REG_MULTI_SZ	Rango de puertos. 3001-3010 y 135
PortsInternetAvailable	REG_SZ	Y
UseInternetPorts	REG_SZ	Y

Tabla 3. Configuración de Puertos en el registro de Windows

Donde 3001-3010 son los puertos fijos que usara DCOM. Veamos la Figura 4, donde se nos muestran los puertos que deben ser permitidos en el firewall para la comunicación de Zenoss con los servidores a monitorear.

Nota. Este procedimiento se tiene que hacer en cada sistema MS Windows Server

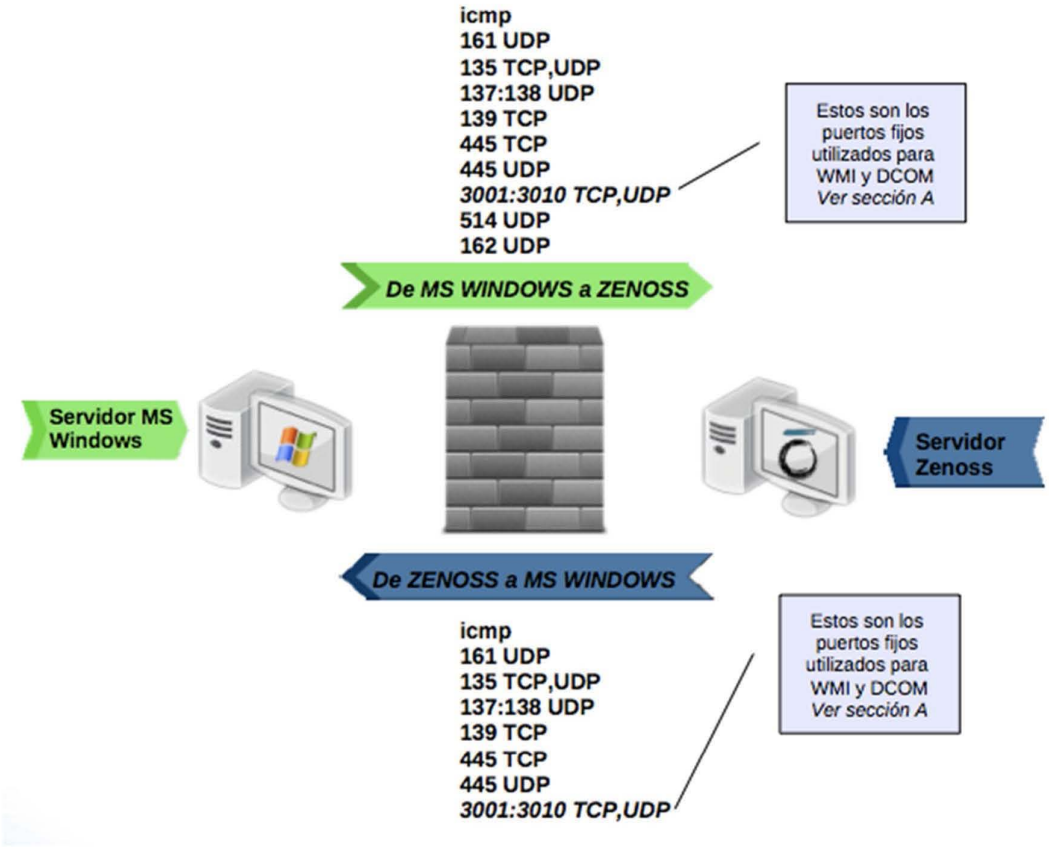


Figura 4. Listado de puertos que deben considerarse en la reglas de filtro de un Firewall

En cuanto a la configuración de servidores Windows para su monitoreo con Zenoss, no profundizamos en como realizar esta actividad ya que USECAD no cuenta con sistemas operativos de este tipo pero consideramos conveniente mecionar los requerimeintos si llegara a presentarse el caso en un ambiente mixto.

Monitoreo de servidores con plataforma Unix/Linux

Requisitos

Habilitar ping

- Se tiene que permitir el tráfico del protocolo ICMP entre el servidor Unix / Linux y el servidor Zenoss.

Configuración del servidor Unix / Linux

5. Se requiere la cuenta del usuario root
6. El servidor Unix / Linux debe tener deshabilitado el firewall, en su defecto se debe permitir el tráfico de ICMP, abrir el puerto 161 de SNMP y el puerto 22 de SSH.

Configuración de comunidad de SNMP y del servicio SSH

1. Se requiere una comunidad de SNMP de sólo lectura.
2. Se debe permitir el acceso vía SSH con la cuenta de root y se debe permitir la

autenticación basada en password.

3. Si se esta trabajando con un firewall entre el servidor Unix / Linux y el servidor Zenoss, se tiene que permitir el tráfico en el puerto 161 de SNMP y el puerto 22 de SSH

Veamos a continuacion como configurar el servicio de SNMP y una comunidad del mismo en Linux, para esto en el servidor **BD1** el cual esta ejecutandose sobre la plataforma virtual de RHEV configuraremos SNMP para que Zenoss pueda extraer datos.

`snmpd` es un servicio que regularmente se instala de modo predefinido en la mayoría de las distribuciones Linux, aunque no está habilitado en los servicios de arranque del sistema. El paquete `net-snmp-utils` no suele instalarse de modo predefinido, por tanto se puede ejecutar lo siguiente en una terminal para realizar la instalación del software necesario:

1. Instalamos los siguientes paquetes:

```
[root@bd1 ~]# yum install net-snmp net-snmp-utils
```

Se deben crear las listas de control de acceso (ACL) correspondientes en el fichero `/etc/snmp/snmpd.conf` y que servirán para definir quien tendrá acceso al servicio de `snmpd`. A una de estas listas se le otorgará permiso de acceso de lectura y escritura para lo que sea necesario y a la otra de solo lectura. Por razones de seguridad solo la interfaz 127.0.0.1 será la de lectura y escritura. Se otorgará permiso de acceso de solo lectura a una red o bien a una IP en la otra lista de control de acceso (ACL).

2. Encontramos la siguiente línea:

```
com2sec notConfigUser  default       public
```

La remplazamos con la siguientes líneas asegurándonos de poner la ip del servidor Zenoss el cual será el único con acceso a SNMP de este equipo así como localhost, también asignamos nombres a nuestras ACLs.

```
com2sec local  localhost       public
com2sec mynetwork 192.168.1.112 public
```

3. Buscamos la líneas:

```
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c           notConfigUser
```

Las remplazamos asignando permisos de lectura y escritura para localhost y únicamente lectura para la IP del servidor Zenoss.

```
group MyRWGroup v1         local
group MyRWGroup v2c        local
group MyRWGroup usm        local
group MyROGroup v1         mynetwork
group MyROGroup v2c        mynetwork
group MyROGroup usm        mynetwork
```

4. Buscamos la línea

```
view    systemview     included      system
```

La sustituimos por la siguiente linea que esecifica las ramas de MIB que se van a permitir ver a través del servicio:

```
view all    included  .1                                80
```

5. Buscamos la línea

```
access  notConfigGroup ""      any       noauth    exact  systemview
none none
```

La sustituimos por la siguientes lineas que especifican que permisos tendrán los dos grupos, MyROGroup y MyRWGroup. Son de especial interés las últimas columnas.

```
access MyROGroup ""      any       noauth    exact  all    none   none
access MyRWGroup ""      any       noauth    exact  all    all    none
```

6. Se definen dos parámetros de carácter informativo para que cuando utilicen aplicaciones cliente se incluya algo de información acerca de que sistema se está accediendo.

```
syslocation BD1 Server USECAD.
syscontact Administrador support@mail.com
```

7. Nos aseguramos que el servicio de snmpd siempre se iniciara tras reiniciar o encender el servidor.

```
[root@bd1 ~]# chkconfig snmpd on
```

8. Iniciamos el servicio

```
[root@bd1 ~]# service snmpd start
```

9. Finalmente desde la terminal del servidor de **Zenoss** ejecutamos el siguiente comando para verificar la funcionalidad de SNMP, `snmpwalk` permite obtener toda la información almacenada en el grupo `system` del MIB del servidor que tenga correctamente configurado SNMP, para este caso el servidor **DB1**.

```
[root@zenoss ~]# snmpwalk -v2c -cpublic ip_bd1_server:161 system
```

Este procedimiento de configuración de SNMP se realizó en los servidores virtuales llamados **BD1**, **BD2**, **LAMP1**, **LAMP2,** los servidores físicos **Hypervisor1** quien contiene estas maquinas virtuales y **BD1-físico**, en el siguiente subtema mostraremos como monitorearlos con Zenoss.

6.3 Configuración de Servidores

Los ZenPacks son el mecanismo de extensión proporcionada por Zenoss para construir nuevas funciones y también la personalización de manera sencilla de los servidores o dispositivos a monitorear con Zenoss. A continuación se muestra como aplicar los

ZenPacks en cada clase según sea el tipo de servidor a monitorear, recordemos que existen ZenPacks para monitorear switches, routers, sistemas operativos, bases de datos, y por consiguiente es necesario aplicar los ZenPacks correspondientes.

6.4 Monitoreo de servidores LINUX/UNIX

Información del monitoreo

El ZenPack LinuxMonitor incluye la funcionalidad de modelar y monitorear varios tipos de componentes de un servidor a través del servicio Secure Shell (SSH).

Activación del monitoreo

Los servidores UNIX/LINUX deben estar bajo la clase correspondiente al sistema operativo dentro de la herramienta de Zenoss, esto es necesario pata que se aplique el correcto template de monitoreo según el servidor designado, veamos la siguiente tabla para mayor referencia.

Sistema operativo	Clase
Linux	/Server/SSH/Linux
Solaris	/Server/SSH/Solaris
AIX	/Server/SSH/AIX
HP-UX	/Server/SSH/HP-UX

Tabla 4. Clasificación de servidores Unix/Linux en Zenoss

A continuación veremos el procedimiento utilizado para dar de alta el servidor Linux **BD1** para monitorearlo por SSH, posteriormente al finalizar esta tarea, lo hicimos también para los servidores **BD2**, **LAMP1** y **LAMP2**.

1. En la interfaz web de Zenoss vamos a **Infrastructure ► Devices**
2. Damos clic en el botón  y seleccionamos **Add a single Device**
3. En la ventana **Add a single Device**(Figura 5) damos clic en **More** para ver todas las opciones

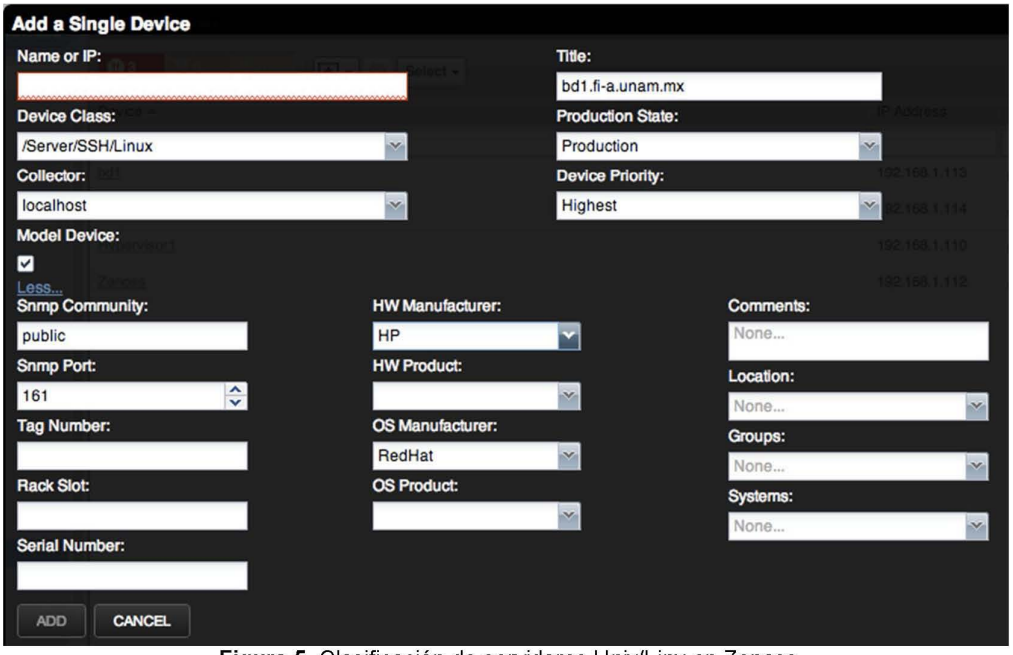


Figura 5. Clasificación de servidores Unix/Linx en Zenoss

4. Llenamos los siguientes campos con la información correspondiente:
   4.1. **Name or IP** - Escribimos la dirección IP o el FQDN del servidor UNIX/LINUX
   4.2. **Device Class** - Seleccionamos la clase correspondiente (ver ***tabla 4***)
   4.3. **SNMP Community** – Escribimos el nombre de la comunidad SNMP de este servidor, según nuestra configuración es la comunidad llamada `public`

5. Damos clic en **Add**

6. En la interfaz web de Zenoss vamos a **Infrastructure ► Devices** y seleccionamos el dispositivo UNIX/LINUX recién agregado

7. Seleccionamos **Configuration Properties**

8. Escribimos las credenciales del servidor UNIX/LINUX
   8.1. **zCommandUsername** - Usuario del sistema
   8.2. **zCommandPassword** - Password del usuario

9. Damos clic en **Save** para guardar los cambios

10. Después de aproximadamente quince minutos las gráficas de rendimiento en la sección **Graphs** empezaran a reflejar los datos recabados mediante su representación en gráficas.

6.5 Monitoreo de servidores Windows con WMI

Información del monitoreo

ZenWinPerf es el ZenPack que permite el monitoreo de rendimiento de servidores Microsoft Windows sin necesidad de instalar un agente. ZenWinPerf recaba los datos del servidor Microsoft Windows conectándose a su servicio WMI. Veamos a continuación como se configuraría un servidor Windows en caso de que llegue a

utilizarse un servidor de este tipo en USECAD, recordemos actualmente no son parte de esta infraestructura.

Requisitos

Activación del monitoreo

Los servidores Microsoft Windows deben estar bajo la clase:

`/Devices/Server/Windows/WMI.`

1. En la interfaz web de Zenoss vamos a **Infrastructure ► Devices**
2. Damos clic en el botón  y seleccionamos **Add a single Device**
3. En la ventana **Add a single Device** (Figura 6) damos clic en **More** para ver todas las opciones

Figura 6. Clasificación de servidores Windows en Zenoss

4. Llenamos los siguientes campos con la información correspondiente:
   - 4.1. **Name or IP** - Escribimos la dirección IP o el FQDN del servidor Microsoft Windows a monitorear
   - 4.2. **Device Class** - Seleccionamos la clase **/Devices/Server/Windows/WMI**
   - 4.3. **SNMP Community** - Escribimos el nombre de la comunidad SNMP de este servidor
5. Damos clic en **Add**
6. En la interfaz web de Zenoss vamos a **Infrastructure ► Devices** y seleccionamos el dispositivo Microsoft Windows recién agregado
7. Seleccionamos **Configuration Properties**
8. Escribimos las credenciales del servidor Microsoft Windows
   - 8.1. **zWinUser** - Usuario del sistema, si el usuario esta en dominio se debe especificar el dominio, ej. \dominio\user. Si es un usuario local se especifica así .\usuario
   - 8.2. **zWinPassword** - Password del usuario

9. Damos clic en **Save** para guardar los cambios

10. Después de aproximadamente quince minutos las gráficas de rendimiento en la sección **Graphs** empezaran a reflejar los datos recabados

6.6 Monitoreo de servidores Windows con SNMP

Requisitos

Activación del monitoreo

Los servidores Microsoft Windows deben estar bajo la clase /Devices/Server/Windows/SNMP

Para verificar la disponibilidad de la comunidad de cada servidor se utilizó el siguiente comando:

```
[root@zenosscore ~]# snmpwalk -c nombre_comunidad -vc2 <IP> system
```

1. En la interfaz web de Zenoss vamos a **Infrastructure ► Devices**
2. Damos clic en el botón  y seleccionamos **Add a single Device**
3. En la ventana **Add a single Device** (Figura 7)damos clic en **More** para ver todas las opciones

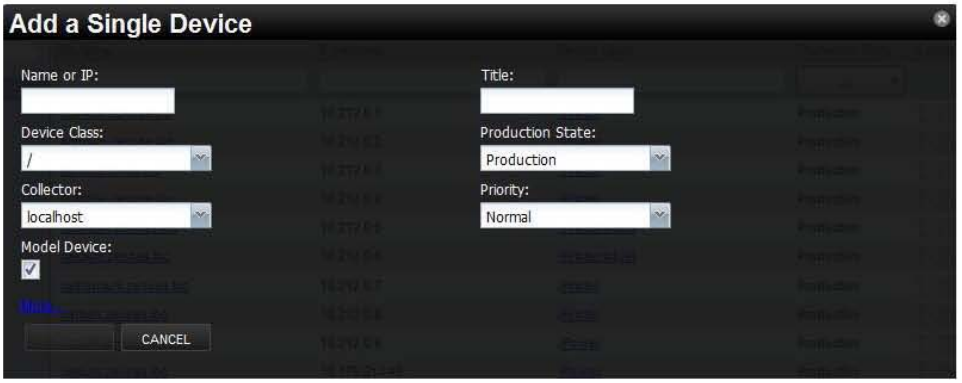


Figura 7. Clasificación de servidores Windows en Zenoss

4. Llenamos los siguientes campos con la información correspondiente:
   4.1. **Name or IP** - Escribimos la dirección IP o el FQDN del servidor Microsoft Windows a monitorear
   4.2. **Device Class** - Seleccionamos la clase **/Devices/Server/Windows**
   4.3. **SNMP Community** - Escribimos el nombre de la comunidad SNMP de este servidor
5. Damos clic en **Add**
6. En la interfaz web de Zenoss vamos a **Infrastructure ► Devices** y seleccionamos el dispositivo Microsoft Windows recién agregado
7. Seleccionamos **Configuration Properties**
8. Escribimos la comunidad de SNMP en las siguientes áreas de texto:
   8.1. **zSnmpCommunity**
   8.2. **zSnmpAuthPassword** - Password de la comunidad en case de ser necesario
9. Damos clic en **Save** para guardar los cambios

10. Después de aproximadamente quince minutos las gráficas de rendimiento en la sección **Graphs** empezaran a reflejar los datos recabados mediante su representación mediante gráficas.

6.7 Monitoreo del tiempo de respuesta de páginas web

El **ZenPacks.zenoss.HttpMonitor** monitorea el tiempo de respuesta de conexión a un servidor HTTP y determina si existe o no el contenido específico de una página Web.

Activación del Monitoreo

1. En la interfaz de Zenoss seleccionamos **Infraestructure**
2. Damos clic en el nombre del servidor que posee el servicio de http.
3. En el panel izquierdo expandimos la opción **Monitoring Templates** y damos clic en el botón  y seleccionamos la opción **Bind Templates**
4. Agregamos el template **HttpMonitor** y damos guardar
5. El template de **HttpMonitor** esta agregado a la lista de templates de monitoreo, ahora podremos recolectar métricas para el servicio de http del servidor

6.8 Monitoreo de Apache Web Server.

El ZenPack **ApacheMonitor** proporciona un método para extraer parámetros de rendimiento del servidor Apache directamente con Zenoss Core, sin requerir el uso de un agente. Esto se logra mediante el uso del módulo `mod_status` que viene con Apache versión 1 y 2.

Las siguientes métricas son recolectadas y graficadas para el servidor HTTP Apache:

- Solicitudes por segundo
- Rendimiento Bytes/sec y Bytes/Solicitud
- Uso de CPU por parte del servidor http (Procesos)
- Conexiones (Open, Waiting, Reading Request, Sending Reply, Keep-Alive DNS Lookup y Logging)

Para poder monitorear el servidor de Apache necesitamos realizar modificaciones previas al archivo de Apache, para nuestro caso estamos utilizando la versión 2.x.

```
[root@bd1 ~]# apachectl -version
 Server version: Apache/2.2.15 (Unix)
 Server built:   Apr  9 2011 08:58:28
```

Configuración de Apache Web Server

1. Editamos el archivo de configuración `/etc/httpd/conf/httpd.conf`, y habilitamos la opción de **ExtendedStatus**, esta nos permitirá obtener información del servidor Apache, debemos descomentar la línea siguiente:

```
ExtendedStatus On
```

2. En este mismo archivo de configuración habilitamos la opción `/server-status`, de igual manera descomentamos las siguientes líneas, quedando da siguiente manera:

```
<Location /server-status>
   SetHandler server-status
   Order deny,allow
   Deny from all
   Allow from zenoss.fi-a.unam.mx
</Location>
```

En la línea de `Allow from` debemos indicar que servidores o segmento de red podrá realizar conexiones al servidor de Apache, si solo indicamos la IP o hostname de los servidores deberemos separarlos por espacios.

3. Guardamos los cambios en el archivo y reiniciamos el servicio de `httpd`
4. Para verificar que la configuración de Apache Web Server trabaja correctamente, abrimos un navegador y escribimos la URL:

   `http://lamp1.fi-a.unam.nx/server-status?auto`

   Si las configuraciones son correctas se desplegara en pantalla un estado del servidor similar al siguiente texto:

```
Total Accesses: 1
Total kBytes: 2
Uptime: 43
ReqPerSec: .0232558
BytesPerSec: 47.6279 B
ytesPerReq: 2048
BusyWorkers: 1
IdleWorkers: 5
Scoreboard: _W___.............................
```

Activación del Monitoreo

1. En la interfaz de Zenoss seleccionamos **Infraestructure**
2. Damos clic en el nombre del servidor que posee el servicio de http.
3. En el panel izquierdo expandimos la opción **Monitoring Templates** y damos clic en el botón  y seleccionamos la opción **Bind Templates**
4. Agregamos el template **Apache** y damos guardar
5. El template de **Apache** esta agregado a la lista de templates de monitoreo, ahora podremos recolectar métricas para el servicio de http del servidor

Para finalizar este capítulo recordemos que tenemos actualmente monitoreando 5 servidores para su análisis de resultados en el capitulo 7 del presente trabajo, los cuales son:

- bd1.fi-a.unam.mx (Virtual)
- bd2.fi-a.unam.mx (Virtual)
- lamp1.fi-a.unam.mx (Virtual)
- lamp2.fi-b.unam.mx (Virtual)
- hypervisor1.fi-a.unam.mx (Físico)
- bd1-fisico.fi-a.unam.mx (Físico)
-

En el capítulo de resultados veremos en comportamiento de los datos extraídos en Zenoss mediante su representación en graficas.

6.9 Configuración de la herramienta de monitoreo

6.9.1 Personalización de alarmas

En este apartado se muestra la configuración de alarmas referentes a los incidentes detectados por zenoss, se configuró una dirección de correo al cual se envían las alertas en caso de que ocurra algún incidente con alguno de los servidores monitoreados.
En la sección **Advanced->Edit** en el campo Email se introdujo la dirección: *monitorsistemas@gmail.com*

Configuración de alarmas por usuario

En **advanced->Users->Users->Alerting Rules** se definieron las alertas por usuario, para cuestiones de permisos se configuraron las alertas para el usuario *admin*.

Las alarmas configuradas son las siguientes:

-Alerta de CPU
-Alerta de Memoria
-Alerta servicios
-Conexión perdida
-Alerta Espacio

Conexión perdida

Estatus de configuración

```
Delay (secs)                0
Action                      email
Plain Text                  true
Send clear messages         true
Enabled                     True
Event State           =     new
Messages                    contain is down
Event Class                 Begins with /Status/ping
```

Alerta CPU

Estatus de configuración

```
Delay (secs)                0
Action                      email
Plain Text                  true
Send clear messages         true
Enabled                     True
Event State           =     new
Severity              >=    warning
Messages                    contain is down
Event Class                 Begins with /Perf/CPU
```

Alerta CPU

Estatus de configuración

```
Delay (secs)                0
Action                      email
Plain Text                  true
Send clear messages         true
Enabled                     True
Event State           =     new
Severity              >=    warning
Messages                    contain is down
Event Class                 Begins with /Perf/Memory
```

Alerta Servicios

Estatus de configuración

```
Delay (secs)                0
Action                      email
Plain Text                  true
Send clear messages         true
Enabled                     True
Event State           =     new
Severity              >=    warning
Event Class           begins with /Status/WinService
```

Alerta de espacio

Estatus de configuración

```
Delay (secs)                    0
Action                          email
Plain Text                      true
Send clear messages             true
Enabled                         True
Event State              =      new
Production State         =      Produccion
Severity                 >=     warning
Event Class               begins with /Perf/Filesystem
```

6.9.2 Mensaje de las Alertas

Cada Alerta dada de alta en Zenoss lleva un mensaje personalizado en código HTML donde podemos asignar colores, imágenes, ligas se puede personalizar para que este acorde al departamento, se define de la siguiente manera :

ADVENCED->Users->Admin->Alerting Rules-> <Regla_Definida>

Tiene la siguiente estructura:

```
<table style="height: 186px;" border="0" cellpadding="5" cellspacing="1"
width="600px"><!
  <tbody><!
    <tr><!
      <td colspan="2" bgcolor="#d35f62"><font face="verdana"
size="2"><b>Message</b></font></td><!
    </tr><!
    <tr><!
      <td style="height: 20px;" colspan="2" bgcolor="#d1ddf5">
%(message)s</td><!
    </tr><!
    <tr><!
      <td style="height: 20px;" colspan="2" bgcolor="#d1ddf5"><font
face="verdana" size="2"><b>Alarm Details</b></font></td><!
    </tr><!
    <tr><!
      <td style="height: 24px;" bgcolor="#ebf4f7" width="120"><font
face="verdana" size="2">Event Details</font></td><!
      <td style="height: 24px;" bgcolor="#d1ddf5" width="580"><font
face="verdana, helvetica, arial" size="2"><!
      <p><a href="%(eventUrl)s">Event Detail</a></p><!
      </font></td><!
    </tr><!
    <tr><!
      <td style="height: 28px;" bgcolor="#ebf4f7" width="120"><font
face="verdana" size="2">Device Name</font></td><!
      <td style="height: 28px;" bgcolor="#d1ddf5" width="580"><font
face="verdana, helvetica, arial" size="2">%(device)s</font></td><!
    </tr><!
    <tr><!
      <td style="height: 29px;" bgcolor="#ebf4f7" width="120"><font
face="verdana" size="2">Components</font></td><!
      <td style="height: 29px;" bgcolor="#d1ddf5" width="580"><font
face="verdana, helvetica, arial" size="2">%(component)s</font></td><!
    </tr><!
    <tr><!
      <td style="height: 25px;" bgcolor="#ebf4f7" width="120"><font
face="verdana" size="2">Severity</font></td><!
      <td style="height: 25px;" bgcolor="#d1ddf5" width="580"><font
face="verdana, helvetica, arial" size="2">%(severityString)s</font></td><!
    </tr><!
    <tr><!
      <td style="height: 28px;" bgcolor="#ebf4f7" width="120"><font
face="verdana" size="2">Actions</font></td><!
      <td style="height: 28px;" bgcolor="#d1ddf5" width="580"><font
face="verdana, helvetica, arial" size="2"> <a
```

```
href="%(ackUrl)s">Acknowledge</a>      <a
href="%(deleteUrl)s">Delete</a>      <a
href="%(eventsUrl)s">Device Events</a> </font></td><!
    </tr><!
  </tbody><!
</table><!
<table border="0" cellpadding="5" cellspacing="1" width="600px"><!
  <tbody><!
    <tr><!
      <td style="height: 56px;" align="right" bgcolor="#d1ddf5"><font
face="verdana, helvetica, arial" size="2">Generated at
%(firstTime)s</font></td><!
    </tr><!
    <tr><!
      <td style="height: 0px;"><!
      <p align="right"><font color="#999999" face="verdana"
size="2"><b>Reported by : <span style="text-decoration:
underline;">Zenoss</span>     </b></font></p><!
      </td><!
    </tr><!
  </tbody><!
</table>
```

6.9.3 Integración con Google Maps

La integración con Google Maps nos permite ubicar geográficamente nuestros centros de datos en caso de que exista mas de uno, de tal manera que podemos recorrer cada uno de ellos de una forma fácil e intuitiva.

Se generó una API key de google maps, esta clave la proporcionó Zenoss a partir del Zenoss Server Key, para introducirla se siguen los siguientes pasos:

Abrir la interfaz web de Zenoss Enterprise. **Advanced -> Settings** y en la parte inferior, en el campo **Google Maps API Key** introducimos la key: ***fi-a.unam.mx***

Ubicación de sedes de USECAD en Google Maps

Para definir una ubicación geográfica dentro de google maps en **INFRASTRUCTURE->Locations**, seleccionamos **Locations** y damos clic en el icono de [+] para agregar un punto geográfico, introducimos **Name, Description y Address.**
Las localidades definidas fueron:

USECAD: Coyoacán, Ciudad de México, Distrito Federal

La Anterior Ubicación aparecerá automáticamente en el mapa de Google Maps.
La importancia de contar con un mapa de ubicación de nuestros servidores básicamente consiste en que si nosotros contáramos con más centros de datos, por ejemplo, un centro de datos en la facultad de ingeniería de ciudad universitaria (véase figura 8), pero además tenemos otros dos centros de datos en provincia, podemos tener un mapa que nos muestre las alertas dependiendo la criticidad de cada servidor. Nos sirve para ubicarnos donde se encuentra el problema.

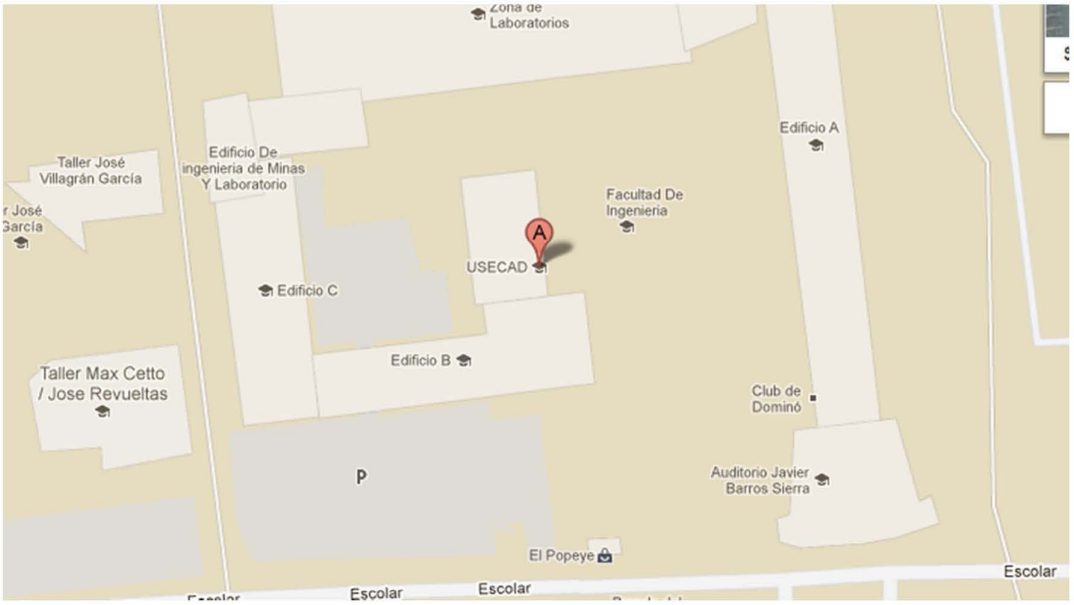


Figura 8. Ubicación del centro de datos USECAD en GoogleMaps

7. Análisis de resultados

7.1 Interpretación de los resultados del monitoreo

La metodología que hemos venido siguiendo (análisis, diseño, implementación y evaluación) nos ayudará a concluir, si cumplimos con las metas esperadas, tales como la maximización de recursos, ahorro en el consumo de energía, ahorro en espacio, entre otros. Con la finalidad de evaluar el trabajo de implementación de virtualización que se usó en el presente trabajo de Tesis, se partió de una base, es decir, algo que sirve como referencia para confirmar al final, si la técnica cumplió con los resultados esperados o bien, si no cumplió y poder hacer una comparación antes y después de virtualizar.

Los datos comparados están basados en parámetros de evaluación definidos además con criterios de aceptación, es decir una breve explicación sobre qué tipo de cambio antes y después de virtualizar es el conveniente.

Como resultado, se espera obtener datos que demuestren que la técnica de virtualización de servidores usando RedHat Linux Enterprise Virtualization es óptima y que en efecto, los consumos de energía disminuyen, así como el ahorro en espacio, la administración se simplifica y los recursos del servidor se aprovechan en un mejor porcentaje.

A continuación se describen cuales son los parámetros de evaluación utilizados los cuales son métricas que ayudan a tener información útil y tomar acciones sobre el sistema informático, optimizando con ello aspectos como los comentados en este proyecto de Tesis, tales como utilización de recursos de memoria RAM, CPU, espacio en disco, tarjetas de red, etc.

- **Porcentaje de utilización de recursos**

Se define como recursos de un servidor al CPU, interfaz de red y a la memoria disponible.

Unidades de Medida: El procesador o CPU se mide en % de ciclos de reloj usados en procesos y % de ciclos de reloj ociosos. La memoria se mide en % de uso en referencia al 100% que es la memoria instalada físicamente, mientras que una interfaz de red se mide en bits/segundo que entran y salen por este medio, así como el número de paquetes/segundo que se transmiten mediante su interfaz. Los sistemas operativos

modernos, cuentan con procesos que monitorean los recursos del servidor, facilitan la medición de estos y proveen información extra, como el uso de recursos por cada proceso en el sistema.

Criterio de evaluación: Como parte de los activos de una organización, los recursos de un servidor deben ser optimizados, con el fin de obtener un mejor retorno de Inversión, a mayor % de utilización sin disminuir el nivel de servicio, mejor se aprovechan dichos recursos.

Resultados esperados: Un servidor virtualizado, al consolidar diversos servicios, utiliza mayor cantidad de recursos de cómputo, se espera que, a diferencia de los servidores no virtualizados, la propuesta hecha en este trabajo alcance mas de un 30% de uso de recursos en promedio.

El monitoreo de la utilización de recursos en el servidor se realiza con comandos nativos del sistema Linux que proporcionan información para la determinación del estado del servidor en cuanto al aprovechamiento recursos. Estos comandos suelen ser complicados de interpretar si se desconoce su sintaxis. Existen herramientas de monitoreo de recursos más amigables en su uso y que hacen una mejor presentación de resultados para facilitar la interpretación, en nuestro caso utilizamos Zenoss el cual hace uso de comandos del sistema Linux para extraer datos y obtener graficas y hacer un histórico de datos. Los principales comandos utilizados para el monitoreo de los recursos del servidor se describen a continuación:

- ***vmstat :***(Virtual Memory Statistic)
  Reporta estadísticas que mantiene el kernel sobre los procesos, la memoria y otros recursos del sistema.

- ***iostat :*** (Input/Output statistics)
  Este comando funciona para obtener estadísticas sobre la actividad en los dispositivos de entrada y salida, así como reportar también información de CPU. Sin embargo, lo utilizamos principalmente para obtener datos sobre la utilización de los discos.

- ***top:*** El comando **top** permite una visión dinámica del sistema en tiempo real. El comando muestra un listado de los procesos que se están ejecutando. Proporciona además un gran número de datos como el uso de la memoria y procesador.

- ***free:*** El comando **free** muestra información relativa al uso de la memoria. Sin embargo, el resultado mostrado por este comando es estático.

Obtención y Análisis de Resultados

Monitoreo del servidor *lamp1-fisico.fi-a.unam.mx*

En esta primera prueba para la obtención de resultados, trabajamos con el servidor ***lamp1-fisico.fi-a.unam.mx***, éste servidor inicialmente era un equipo físico, sus características de hardware se muestran en la **Tabla 1**.

Servidor	Sistema Operativo	Aplicación	Procesador	Memoria RAM	Storage
lamp1-físico	Fedora 8	BD y web	Pentium 4	2 GB	80 GB

Tabla 1. Servidor físico LAMP1

El sistema operativo de este servidor ocupa los recursos físicos del equipo como CPU, memoria RAM, tarjeta de red y disco duro, por tanto podemos ver el típico esquema existente en algunos centros de datos: una aplicación para un servidor. Nuestro siguiente paso es poner cargas de trabajo a este equipo y monitorear el uso de recursos físicos mediante Zenoss.

La siguiente figura ilustra los componentes físicos este equipo, observamos también que el sistema operativo es quien administra todos los recursos de hardware única y exclusivamente

para una o varias aplicaciones contenidas en este.

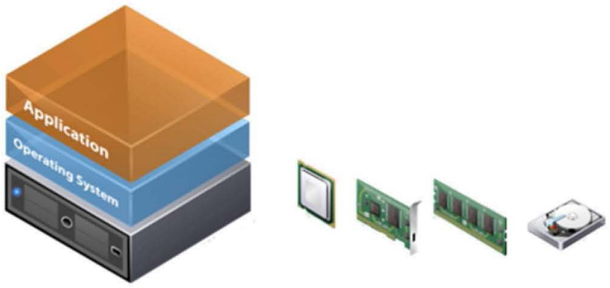


Figura 1. Representación gráfica de los componentes físicos y lógicos de equipo físico **lamp1-fisico.fi-a.unam.mx**

Antes de realizar alguna prueba, veamos las gráficas de rendimiento del servidor **lamp1-fisico.fi-a.unam.mx** proporcionadas por Zenoss, este servidor actualmente provee servicio web y base de datos, inicialmente no tenía un a carga de trabajo especifica, estas pruebas se aplicarón mas adelante.

La **Figura 2** muestra que el sistema utiliza solamente del .8% al 1.4% de la capacidad total del CPU, esto indica que el sistema base no atiende solicitudes de procesos de CPU ya que inicialmente no existe carga de trabajo en este.

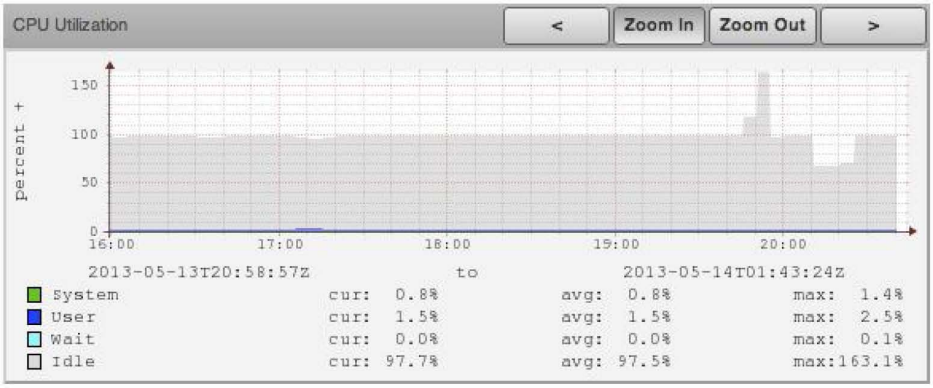


Figura 2. Utilización en porcentaje de CPU de **lamp1-fisico.fi-a.unam.mx**

La **Figura 3** muestra la utilización de memoria RAM utilizada por el servidor **lamp1-fisico.fi-a.unam.mx,** este muestra una disponibilidad de 598.77MB de RAM en promedio, el resto es utilizado por el sistema operativo y procesos que se ejecutan en el, es decir el 70.76% de la memoria RAM esta en utilización.

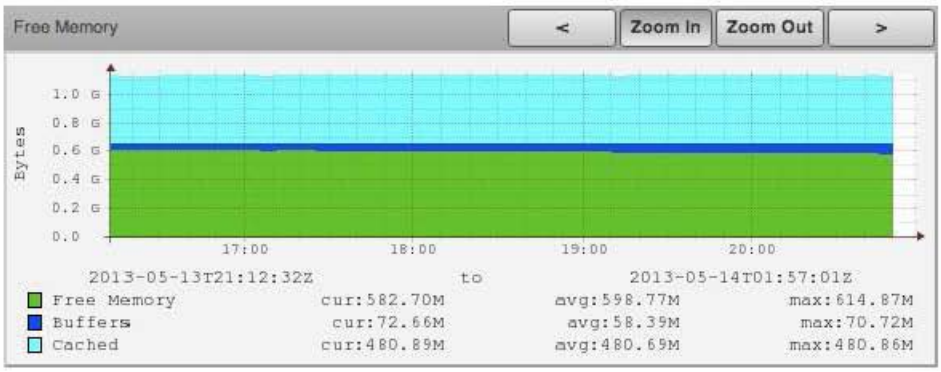


Figura 3. Utilización de memoria RAM de **lamp1-fisico.fi-a.unam.mx**

Hemos observado el comportamiento de utilización de recursos del servidor **lamp1-fisico.fi-a.unam.mx** sin cargas de trabajo o procesos en ejecución que demanden gran cantidad de procesamiento y memoria, veamos a continuación los resultados obtenidos tras realizar pruebas de estrés de este servidor para el análisis de utilización de recursos y la demanda de ejecución de tareas.

Prueba 1: Ejecutar la herramienta `stress`

Objetivo: Validar que el servidor físico con base de datos es capaz de ejecutar los procesos esperados en tiempo y de forma exitosa, así como evaluar el uso de recursos de CPU y Memoria RAM en el servidor sin virtualización.

Realización de pruebas y resultados

El comando `stress` utilizado en Linux para la realización de estas prueba se describe a continuación:

Sinopsis

stress [*OPCIONES* [*ARG*]] ...

Parámetros

-c, --cpu N genera N trabajos de CPU con `sqrt()`

-i, --io N genera N trabajos de I/O con `sync()`

-m, --vm N genera N trabajos con `malloc()/free()`

--vm-bytes B B bytes malloc por trabajo de tipo vm `(default 256MB)`

-t, --timeout N tiempo de duración en ejecución

En la terminal del servidor **lamp1-fisico.fi-a.unam.mx** introducimos el siguiente comando el cual genera 10 procesos de ejecución de la función `sqrt()`, asigna 1024 localidades de memoria con `malloc()` cada una de ellas de 1MB en tamaño y 5 procesos para el flujo de datos a disco de tipo I/O con `sync()` durante 1 hora.

```
[root@lamp1-fisico ~]# stress --cpu 10 --io 5 --vm 1024 --vm-bytes
1MB --timeout 1h --verbose

...[Salida truncada]
stress: dbug: [9034] <-- worker 10074 signalled normally
stress: dbug: [9034] <-- worker 10075 signalled normally
stress: info: [9034] successful run completed in 3600s
```

Una vez concluida la ejecución se observa que todos los procesos indicados terminaron en el tiempo indicado, por lo que se demuestra que el servidor es capaz de soportar los procesos esperados en tiempo y forma exitosa.

Análisis de las graficas obtenidas mediante Zenoss después de generar cargas de trabajo al servidor.

La **Figura 4** muestra un incremento de utilización de CPU del 1.4% a un máximo de utilización de 38.4% de la capacidad total de CPU durante un tiempo aproximado de 30 minutos, al observar el Dashboard de Zenoss donde muestra las gráficas del monitoreo del servidor **lamp1-fisico.fi-a.unam.mx**, nos damos cuenta que el servidor comenzó a rechazar conexiones, en este caso la conexión de SSH de Zenoss a este servidor comenzaron a ser rechazadas, las alertas las podemos ver en la **Figura 5** donde vemos un error de tipo **time out** para la ejecución de comandos en este servidor, el comando `stress` ejecutado para generar carga de trabajo en este equipo físico demando gran cantidad de recursos lo que mantuvo al servidor imposibilitado de ejecutar o atender tareas como las que enviaba Zenoss para su monitoreo, esto mismo ocasionó que Zenoss no pudiera graficar a partir de la hora 22:00, para corroborar este comportamiento ejecutamos conexiones de SSH al servidor **lamp1-fisico.fi-a.unam.mx** tales conexiones demoraron bastante tiempo en ser atendidas o en algunas ocasiones fueron rechazadas.

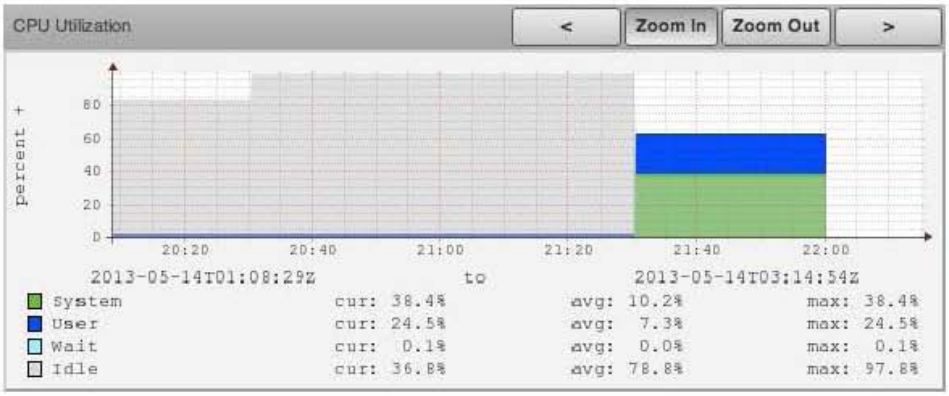


Figura 4. Utilización en porcentaje de CPU del servidor **lamp1-fisico.fi-a.unam.mx** con cargas de trabajo.

⚠	/	Datasource FileSystem/disk command timed out
⚠	/Perf/CPU	Datasource Device/cpu command timed out
⚠	/Perf/CPU	Datasource Device/uptime command timed out
⚠	/Perf/Memory	Datasource Device/mem command timed out
⚠	/Cmd/Fail	Datasource FileSystem/idisk command timed out

Figura 5. Error de tipo **time out** al intentar monitorear el servidor **lamp1-fisico.fi-a.unam.mx**

Monitoreo del hypervisor y servidor *lamp1.fi-a.unam.mx* virtualizado

Hasta este punto nosotros ya tenemos implementada la arquitectura de *Red Hat Enterprise Virtualization* y contamos con un equipo que funciona como hypervisor (***hypervisor1.fi-a.unam.mx***), este contiene las siguientes máquinas virtuales, las cuales hacen uso de los recursos compartidos de memoria RAM, CPU, tarjetas de red y espacio en disco del hypervisor.

Tabla 2. Servidores virtualizados contenidos en el **hypervisor1**

Servidor	Sistema Operativo	Aplicación	Procesador	Memoria RAM	Storage	NIC
bd1.fi-a.unam.mx	Fedora 8	LAMP	2 vCPU	2 GB vRAM	80 GB	1 vNIC
lamp1.fi-a.unam.mx	RHEL 5	LAMP	1 vCPU	2 GB vRAM	80 GB	1 vNIC
lamp2.fi-a.unam.mx	RHEL 5	LAMP	1 VCPU	2 GB vRAM	80 GB	1 vNIC
bd2.fi-a.unam.mx	Fedora 8	LAMP	2 vCPU	2 GB vRAM	80 GB	1 vNIC

Las características de hardware del **hypervisor1** son las siguientes:

- Intel(R) Xeon(R) CPU X3470 2.93GHz 4 Núcleos
- 10 GB en Memoria RAM
- 500 GB en disco duro

La **Figura 6** ilustra los componentes físicos del **hypervisor1** los cuales comparte con las máquinas virtuales como se muestra en la **Tabla 2** donde se define la utilización de recursos. Aquí las máquinas virtuales hacen uso de los recursos físicos del hypervisor que las contiene, tales como CPU, memoria RAM, espacio en disco y tarjetas de red.

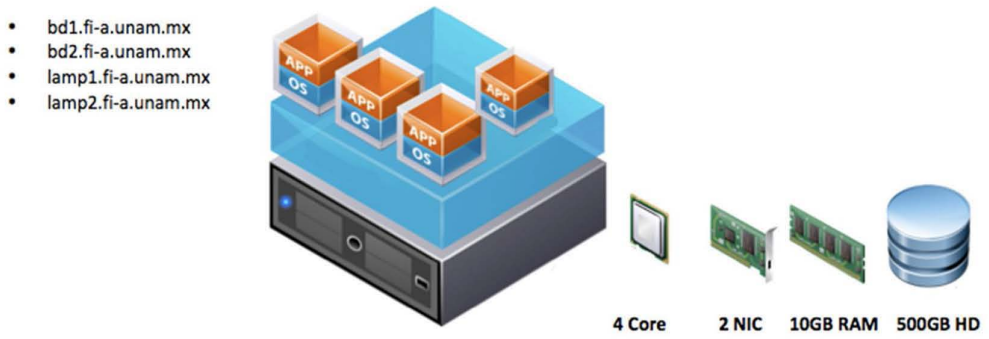


Figura 6. Hypervisor1 compartiendo recursos de hardware con las máquinas virtuales

Gráficas de rendimiento del servidor hypervisor1.fi-a.unam.mx

Antes de realizar alguna prueba, analizamos las gráficas de rendimiento del servidor **hypervisor1.fi-a.unam.mx** proporcionadas por Zenoss, las cuatro máquinas virtuales alojadas en el hypervisor no contienen tareas específicas en ejecución, podríamos decir que están es un estado ocioso (idle).

La **Figura 3** muestra que el sistema utiliza solamente del 12.6% al 14.18% de la capacidad total del CPU, esto indica que el sistema base del hypervisor no tiene solicitudes de procesos de CPU que atender de las máquinas virtuales, dado que no existe carga de trabajo en ellas.

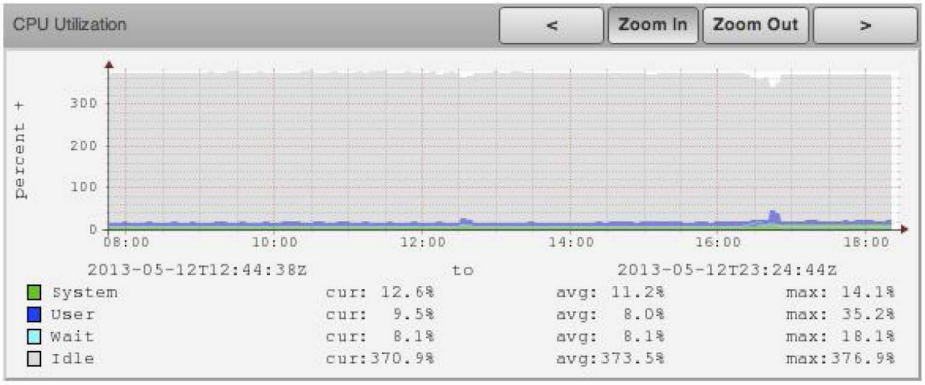


Figura 7. Utilización en porcentaje de CPU del servidor **hypervisor1.fi-a.unam.mx**

La **Figura 4** muestra la utilización de memoria RAM utilizada por el hypervisor y las máquinas virtuales, muestra una disponibilidad de 1.34. GB de RAM en promedio, el resto es compartido entre las máquinas virtuales según los requerimientos de sus sistemas, es decir el 86.6% de la memoria RAM esta en utilización.

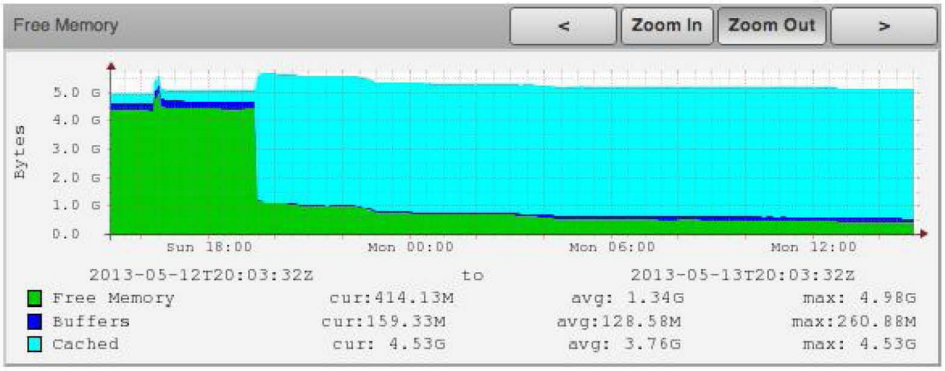


Figura 8. Utilización de memoria RAM del servidor **hypervisor1.fi-a.unam.mx**

La **Figura 9** muestra la utilización de ancho de banda en bits/sec o bps de una de las interfaces de red del hypervisor con un promedio de salida de 10.86kbits/seg. y de entrada 2.27kbit/seg., un cantidad muy mínima de utilización considerando que las interfaces de red del hypervisor tienen una capacidad de 1Gbps, es decir el 0.00103% esta siendo utilizado.

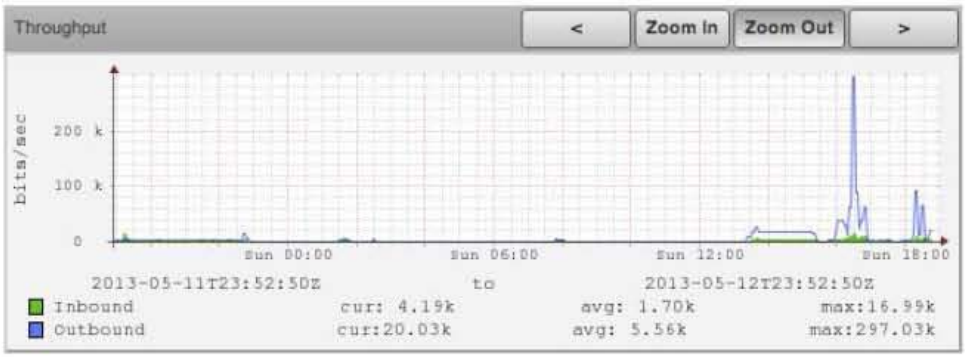


Figura 9. Volumen de flujo de datos a través de la interfaz de red del servidor **hypervisor1.fi-a.unam.mx**

Ahora veamos el comportamiento de la maquina virtual **lamp1.fi-a.unam.mx**

La **Figura 10** muestra que el sistema de la maquina virtual utiliza solamente del .1% al .4% de la capacidad total del CPU, esto indica que el sistema operativo no tiene solicitudes de procesos de CPU que atender, dado que no existe aun carga de trabajo en este.

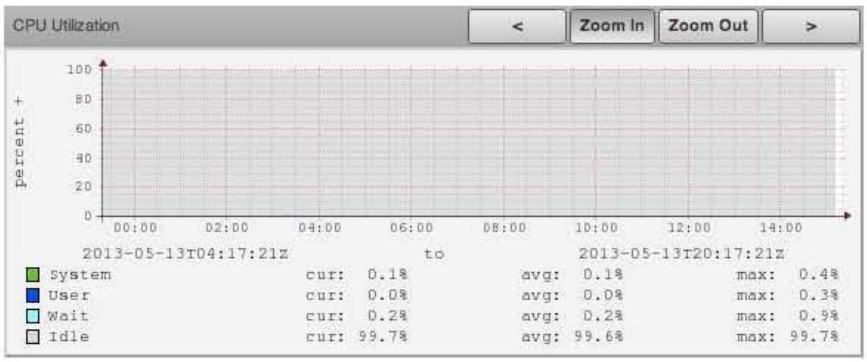


Figura 10. Utilización en porcentaje de CPU del servidor **lamp1.fi-a.unam.mx**

La **Figura 11** muestra la utilización de memoria RAM utilizada por el servidor **lamp1.fi-a.unam.mx**, muestra una disponibilidad de 1.7 GB de RAM en promedio, el resto es utilizado por los procesos del sistema operativo, es decir el 15% de la memoria RAM esta en utilización.

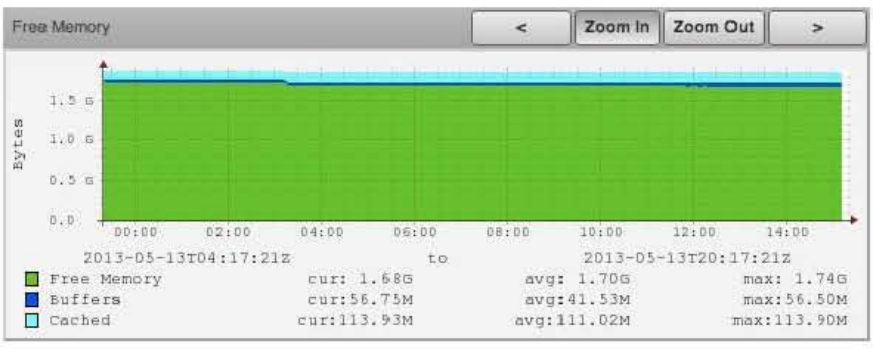


Figura 11. Utilización de memoria RAM del servidor **lamp1.fi-a.unam.mx**

La **Figura 12** muestra la utilización de ancho de banda en bits/sec o bps de la interfaz de red del servidor **lamp1.fi-a.unam.mx** con un promedio de salida de 859,85bps. y de entrada 696.55bps, un cantidad muy mínima de utilización considerando que las interfaces de red del hypervisor tienen una capacidad de 1Gbps.

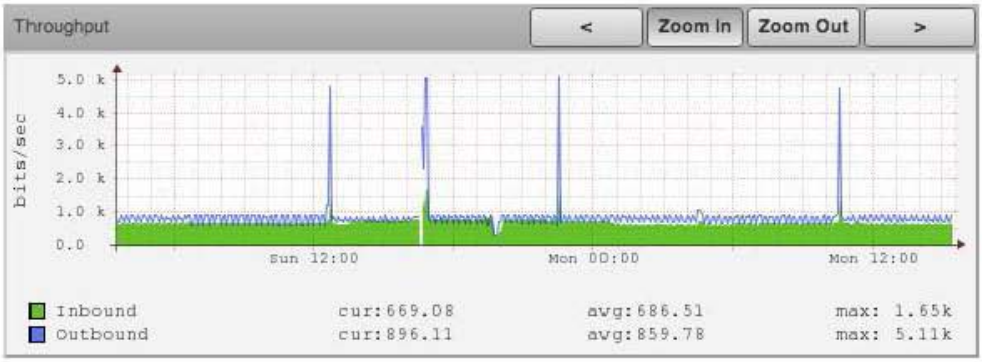


Figura 12. Volumen de flujo de datos a través de la interfaz de red del servidor **lamp1.fi-a.unam.mx**

Hemos observado el comportamiento de utilización de recursos del **hypervisor1** y el servidor virtual **lamp1.fi-a.unam.mx** sin cargas de trabajo o procesos en ejecución que demanden gran cantidad de procesamiento y memoria, veamos a continuación los resultados obtenidos tras realizar pruebas de estrés en los servidores virtuales para el análisis de utilización de recursos y la demanda de tareas que le es solicitado al hypervisor.

Prueba 1: Ejecutar la herramienta `stress` en el servidor *lamp1.fi-a.unam.mx*

Objetivo: Validar que cada servidor virtualizado con su aplicación correspondiente es capaz de ejecutar los procesos esperados en tiempo y de forma exitosa.

Realización de la Prueba y Resultados

El comando `stress` utilizado en Linux para la realización de estas prueba se describe a continuación:

Sinopsis

stress [*OPCIONES* [*ARG*]] ...

Parámetros

`-c, --cpu N` genera N trabajos de CPU con `sqrt()`

`-i, --io N` genera N trabajos de I/O con `sync()`

`-m, --vm N` genera N trabajos con `malloc()/free()`

`--vm-bytes B` B bytes malloc por trabajo de tipo vm `(default 256MB)`

`-t, --timeout N` tiempo de duración en ejecución

En la terminal del servidor **lamp1.fi-a.unam.mx** introducimos el siguiente comando el cual genera 10 procesos de ejecución de la función `sqrt()`, asigna 1024 localidades de memoria

con `malloc()` cada una de ellas de 1MB en tamaño y 5 procesos para el flujo de datos a disco de tipo I/O con `sync()` durante 1 hora.

```
[root@lamp1 ~]# stress --cpu 10 --io 5 --vm 1024 --vm-bytes 1MB --
timeout 1h --verbose

...[Salida truncada]
stress: dbug: [3530] <-- worker 4568 signalled normally
stress: dbug: [3530] <-- worker 4569 signalled normally
stress: info: [3530] successful run completed in 3601s
```

Análisis:

Para el servidor **lamp1.fi-a.unam.mx** se aplicó una carga de trabajo por lapso de tiempo de una hora. Este servidor virtualizado sobre RHEL Virtualization cumplió de forma eficaz los requerimientos para soportar la carga generada.

Al iniciar la prueba el consumo de CPU y Memoria RAM se elevan considerablemente a comparación de los resultados obtenidos antes de aplicar una carga de trabajo.

Para el servidor **lamp1.fi-a.unam.mx**, se obtuvieron muestras mediante el software de monitoreo Zenoss para observar el consumo de los recursos del servidor. Los resultados del monitoreo se muestran en las siguientes gráficas tras aplicar el comando `stress`:

La **Figura 13** muestra la utilización de CPU durante la ejecución de las tareas creadas por el comando `stress`, vemos claramente sobre la línea de tiempo que en la hora 23:40 el uso de CPU por parte del sistema pasa de .4% a un máximo de 44.8% de la capacidad total de CPU y un promedio de uso de 20.44% de utilización de recursos de CPU por parte del sistema. El uso de CPU por parte del usuario es de suma importancia, este indica la utilización de recursos al ejecutar el comando `stress` donde observamos un máximo de uso de 160% de la capacidad total del CPU de esta maquina virtual y un promedio de uso de 85.3% de uso de procesador. Vemos claramente que el procesador esta trabajando mas allá de su capacidad de procesamiento en determinado espacio de tiempo.

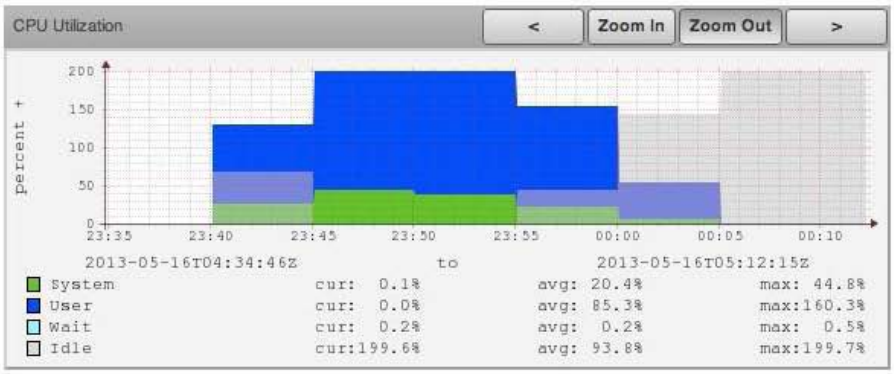


Figura 13. Utilización en porcentaje de CPU del servidor **lamp1.fi-a.unam.mx** con carga de trabajo.

La **Figura 14** muestra la utilización de memoria RAM tras la ejecución del comando `stress`, observamos como de 1.7 GB de RAM promedio que teníamos disponible para el sistema, ahora durante la ejecución del comando solo disponemos de 746.52 MB de RAM disponible en promedio, al termino de la ejecución de comando después de la hora 00:00 se libera memoria RAM disponible para el sistema. Como no es utilizada toda la memoria RAM del la maquina virtual, su memoria de intercambio o mejor conocida como memoria SWAP se mantiene intacta.

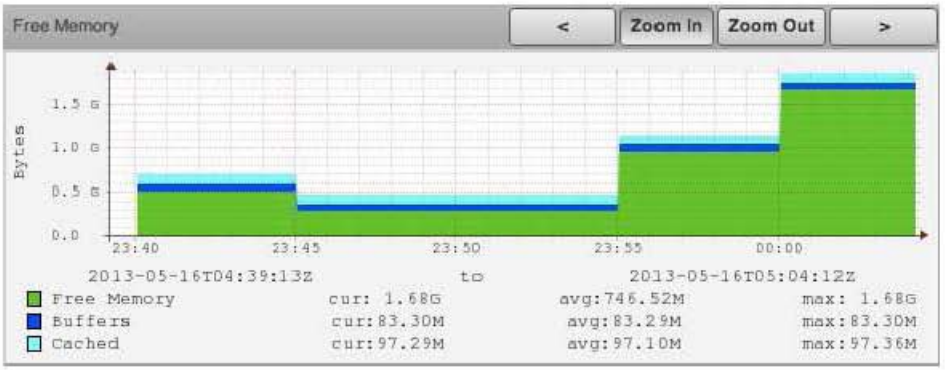


Figura 14. Utilización de memoria RAM del servidor **lamp1.fi-a.unam.mx** con carga de trabajo.

Estas mismas pruebas fueron realizadas para los servidores virtuales **BD2**, **LAMP1** y **LAMP2**, donde se obtuvieron resultados similares puesto que se ejecutó en mismo comando y sintaxis al mismo tiempo en los 4 servidores, ahora bien veamos la utilización de recursos del hypervisor mientras estos comandos eran ejecutados por igual y al mismo tiempo en sus maquinas virtuales.

Las siguientes gráficas nos mostraran la utilización de recursos de CPU y memoria RAM del hypervisor los cuales son solicitados por parte de los servidores virtuales para el procesamiento de tareas. La **Figura 15** muestra la utilización de recursos de CPU, las cuatro máquinas virtuales están ateniendo las tareas generadas por el comando `stress` y vemos notablemente como los recursos de CPU por parte del usuario (gráfica azul) aumentan considerablemente a un máximo de utilización de 305% de uso de CPU y un promedio de 40.4% de uso, vemos como la utilización de CPU del Hypervisor se aprovecha a un buen porcentaje, recordemos que en este intervalo de tiempo los cuatro servidores están demandando recursos de procesamiento en paralelo y por unidad de segundo en tiempo.

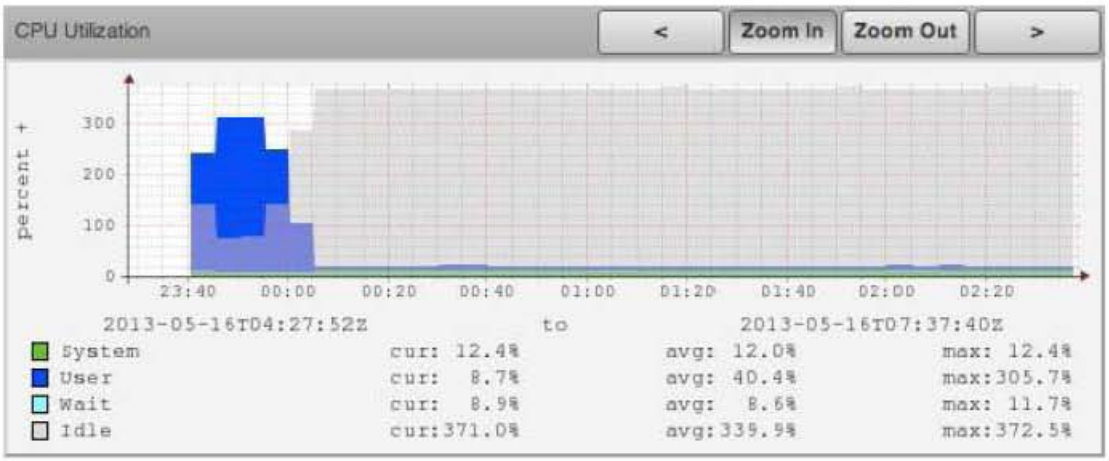


Figura 15. Utilización en porcentaje de CPU del servidor **hypervisor1.fi-a.unam.mx** con carga de trabajo.

La **Figura 16** muestra la utilización de menoría RAM por parte del hypervisor y las máquinas virtuales, si observamos a detalle podemos deducir que la menoría RAM se mantiene casi constante, con una variación de 570 MB que fueron utilizados por el hypervisor para la ejecución de las tareas demandadas por cada una de las máquinas virtuales. Recordemos que cada máquina virtual tiene asignada una cantidad fija de memoria RAM para la utilización de su sistema operativo, por ende se limita a utilizar la memoria que le es asignada cuando es creada la máquina virtual, en caso de que esta demandara mas uso de memoria RAM, el sistema operativo haría uso de la memoria de intercambio o memoria SWAP para optimizar sus tareas

más no haría uso de la memoria RAM disponible que tenga el hypervisor, por tanto deducimos que esa pequeña variación de memoria utilizada fue requerida por el propio hypervisor.

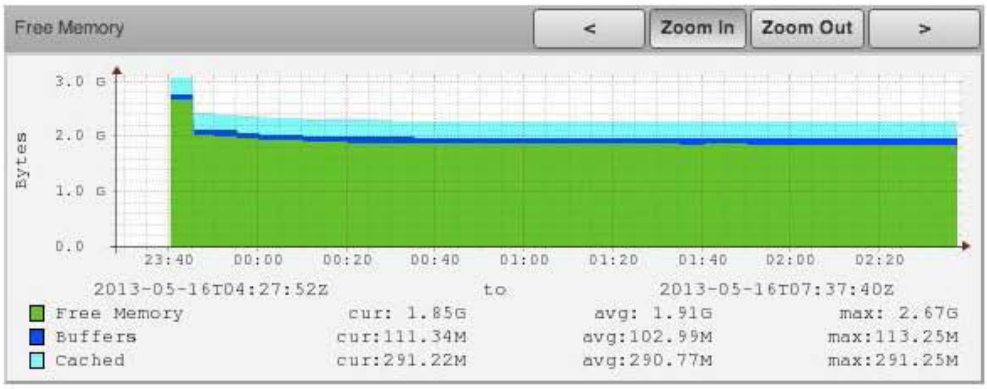


Figura 16. Utilización de memoria RAM del servidor **hypervisor1.fi-a.unam.mx** con cargas de trabajo.

Las gráficas de rendimiento obtenidas antes y después de aplicar cargas de trabajo a los servidores, nos muestran la utilización de recursos por cada sistema en entornos físicos o virtuales, es evidente que la utilización de recursos es diferente en porcentaje según el entorno donde se ejecuta cada sistema operativo. Las cargas aplicadas al servidor **lamp1-fisico.fi-a.unam.mx** demandaron bastantes recursos de procesamiento lo que originó que Zenoss no pudiera realizar la conexión de SSH para extraer los datos de rendimiento y poder generar las gráficas correspondientes, cualquier intento de conexión era cerrado y clasificado como un evento de tipo **time out** lo que nos lleva a concluir que cualquier petición enviada a este servidor físico tenia una demora de tiempo en ser atendida, dado que este servidor tenia como prioridad atender las tareas asignadas mediante el comando `stress`.

Las máquinas virtuales fueron creadas con las mismas características de hardware que los servidores físicos y de igual manera se aplicaron los mismos comandos de `stress` en estos servidores virtuales, las gráficas muestran un mejor desempeño de utilización de recursos y disponibilidad para atender peticiones independientemente de las cargas de trabajo que procesaban con `stress`. Las características de hardware del hypervsor son superiores a los equipos físicos que pusimos a prueba, pero recordemos que el hypervisor comparte esos recursos de CPU y memoria RAM entre las máquinas virtuales que fueron creadas en el, estas contienen las mismas características de hardware que los equipos físicos y aun así fueron capaces de procesar las tareas asignadas, con esto vemos un mejor aprovechamiento del hypervisor como servidor físico, el cual aloja las máquinas virtuales funcionando de manera independiente cada una.

Monitoreo del servicio de Apache Web Server

Los servidores virtualizados **bd1**, **bd2**, **lamp1**, **lamp2** cuentan con servicio de http para proveer portal web y conexión a base de datos de MySQL, por tanto aplicamos pruebas de estrés para analizar rendimiento del servicio, peticiones por segundo, tráfico de datos y tiempo de respuesta mediante las gráficas de Zenoss. La siguiente herramienta permitió realizar las pruebas de estrés a nuestros servidores web.

Apache Benchmark es una gran utilidad para probar la capacidad de nuestro servidor web, de forma general nos sirve para ver la cantidad de peticiones por segundo que es capas de

realizar, obviamente esto dependerá en gran medida del hardware que tengamos, y de la pagina ya que no es igual lanzar peticiones a una pagina HTML de 10 lineas que a una de 2000, su uso aunque a primera vista puede parecer complicado en realidad no lo es tanto, de hecho generalmente solo se usan 2 flags u opciones, que son `-n` para la cantidad de consultas y `-c` para la cantidad de concurrencia (numero de consultas al mismo tiempo).

La sintaxis del comando es la siguiente:

```
ab [options] [http://]hostname[:port]/path
```

Las opciones a utilizar son:

```
-n requests     Numero de peticiones a ejecutar
-c concurrency  Numero conexiones concurrentes
```

El comando `ab` contiene mas opciones, esencialmente solo necesitamos los parámetros anteriores para nuestras pruebas.

`ab` permite simular una solicitud de conexión a una página web, pero también simular la conexión de cientos de clientes, así como la concurrencia de varios thread's simultáneamente. De esta forma podemos comprobar, más o menos, el rendimiento que tendría nuestra web con una carga de trabajo real. Para este caso simulamos 800 conexiones concurrentes (800 Usuarios) en una temporada de inscripciones de USECAD en un estimado por hora, en una primera etapa cada conexión concurrente hace 5 solicitudes del portal web de USECAD, después 10, 15 y por ultimo 20 por cada conexión(Usuario), que ya es un número un poco elevado de solicitudes que podría hacer cada usuario. La **Figura 17** muestra la página principal de USECAD en donde cada usuario que realiza una inscripción cada semestre hace uso de este portal para realizar sus trámites, es una pagina programada con código HTML, PHP, CSS, javascript y con imágenes de contenido.

Figura 17. Portal web de USECAD utilizado en la generación de solicitudes concurrentes

Las siguientes líneas ilustran las peticiones indicadas, la ejecución de `ab` se realizo desde un servidor Linux el cual puede realizar peticiones a lamp1.fi-a.unam.mx:

```
[root@host ~]# ab -kc 800 -n 4000 http://lamp1.fi-a.unam.mx/index.php
```

```
[root@host ~]# ab -kc 800 -n 8000 http://lamp1.fi-a.unam.mx/index.php
```

```
[root@host ~]# ab -kc 800 -n 12000 http://lamp1.fi-
a.unam.mx/index.php
```

```
[root@host ~]# ab -kc 800 -n 16000 http://lamp1.fi-
a.unam.mx/index.php
```

Las líneas anteriores se ejecutaron con un intervalo de tiempo de 1 a 2 minutos y solamente mostramos la salida en pantalla del último comando:

```
[root@hypervisor1 ~]# ab -kc 800 -n 16000  http://lamp1.fi-
a.unam.mx/index.php
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking lamp1.fi-a.unam.mx (be patient)
Completed 1600 requests
Completed 3200 requests
Completed 4800 requests
Completed 6400 requests
Completed 8000 requests
Completed 9600 requests
Completed 11200 requests
Completed 12800 requests
Completed 14400 requests
Completed 16000 requests
Finished 16000 requests


Server Software:        Apache/2.2.15
Server Hostname:        lamp1.fi-a.unam.mx
Server Port:            80

Document Path:          /index.php
Document Length:        502 bytes

Concurrency Level:      800
Time taken for tests:   3.059 seconds
Complete requests:      16000
Failed requests:        0
Write errors:           0
Keep-Alive requests:    0
Total transferred:      11136000 bytes
HTML transferred:       8032000 bytes
Requests per second:    5229.69 [#/sec] (mean)
Time per request:       152.973 [ms] (mean)
Time per request:       0.191 [ms] (mean, across all concurrent requests)
Transfer rate:          3554.56 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0   29 290.1      1    3002
Processing:     1   45 255.6     17    3044
Waiting:        1   45 255.6     17    3043
Total:         15   75 385.0     18    3057

Percentage of the requests served within a certain time (ms)
  50%     18
  66%     19
  75%     26
  80%     28
  90%     29
  95%     46
  98%    627
  99%   3016
 100%   3057 (longest request)
```

De acuerdo a este último reporte generado por el comando **ab** y las gráficas obtenidas por Zenoss realizamos el siguiente análisis.

Primeramente debemos tomar en cuenta que el portal web o la página principal (index) tiene un tamaño de 502 bytes igual a 0.490234 kylobytes, una pagina realmente muy ligera. El número de conexiones concurrentes fue de 800, las cuales generaron 16000 peticiones del portal web, esto es como si 800 usuarios realizara cada uno de ellos 20 solicitudes del sitio web de USECAD, el tiempo que llevo atender estas 16000 peticiones (Request) fue de 3.059 segundos. El número de peticiones por segundo fue de 5229.69/sec según el reporte de **ab** y mismo que se puede ver en la Figura 18.

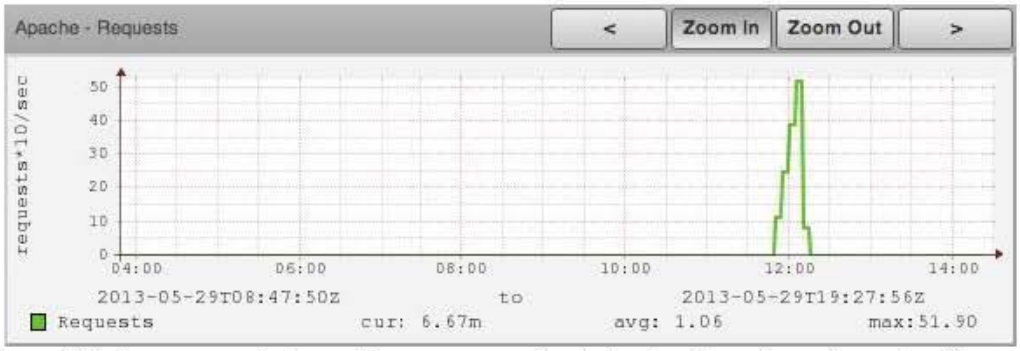


Figura 18. La imagen muestra las peticiones por segundo al ejecutar **ab**, cada escalón en la gráfica es el fin e inicio de ejecución de cada comando.

El reporte de **ab** indica el la cantidad de bytes totales que fueron transmitidos del servidor al cliente, este fue de 11136000 bytes equivalente a 10.62012 Megabytes. La transferencia de bytes por segundo fue de 3554.56 [Kbytes/sec] como se muestra en la Figura 19.

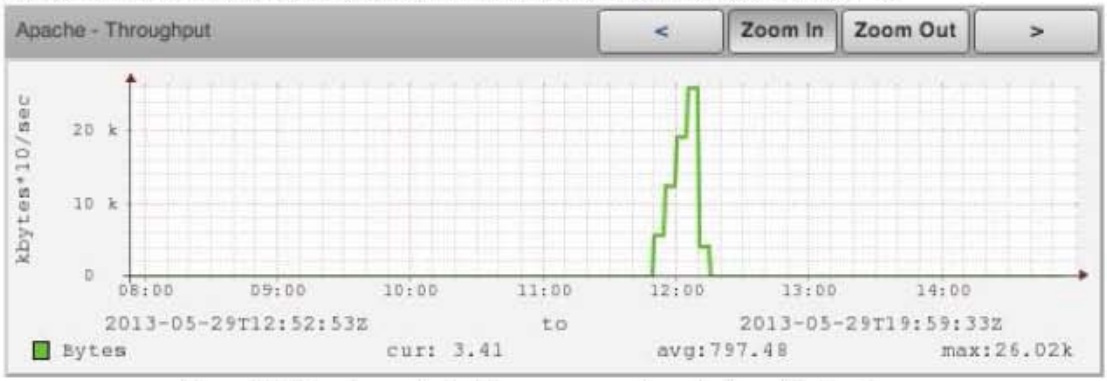


Figura 19. Transferencia de bytes por segundo en la ejecución de **ab**.

Cada petición del portal web realizada por **ab** tardo 152.973 [ms] en ser atendida por el servidor Apache, vemos que el numero de solicitudes concurrentes son atendidas sin ningún problema por el servidor web, esta prueba nos ejemplifica que este servicio proporcionado sobre una infraestructura virtual es apto para proveer una alta concurrencia de usuarios para el uso del portal web de USECAD.

7.2 Análisis de desempeño en los servidores físicos

Para poder realizar un análisis de desempeño en los servidores con infraestructura virtual se tuvo que realizar un estudio de concurrencia por aplicaciones así como también carga de trabajo en cada servidor físico, para eso fue instalado el servidor de monitoreo Zennoss y así tener un estudio más detallado de cada servidor

Al tener los detalles de monitoreo y análisis de desempeño, pudimos realizar la migración de los servidores a la infraestructura de virtualización para poder hacer una comparación de resultado del desempeño, concurrencia y carga de trabajo en el hardware (RAM, red y procesamiento).
Se dividió el análisis de resultados, mostrando cuales son los efectos, ventajas y desventajas de ambas infraestructuras y los resultados del análisis físico fue el siguiente:

Hardware

El comportamiento de los servidores del consumo de recursos de la RAM y de Procesamiento fueron muy similares y el motivo fue el siguiente:
En un servidor físico toma toda la RAM con la que cuenta físicamente. Por lo tanto si sólo tiene 16 Gb en RAM, serán 16Gb que utilice dependiendo si el sistema operativo lo soporta. Trabaja de la misma manera para el procesamiento; si el procesador es sólo uno y trabaja con 4 nucleos, será con los que trabaje el sistema operativo, cabe mencionar que en BIOS se puede manipular para utilizar el servidor de manera ahorradora, o para dar el mayor performance posible en base al procesador.
Ahora bien, en la parte del servidor físico cuenta con una interfaz de red dedicada únicamente para el servicio que solicite el equipo. Por lo que si trabaja el servidor con una interfaz de 1G/s por puerto, será lo máximo que pueda soportar.

Sostware

El manejo de las aplicaciones sobre un servidor físico si sólo corriera la aplicación sobre un servidor se tiene el riesgo de perder la disponibilidad si algo del hardware fallará. Para evitar dicho problema se tiene la solución de crear cluster de aplicaciones en donde se corra la misma aplicación sobre al menos dos equipos y así contar con la disponibilidad de la aplicación en ambos servidores.
En USECAD se tenía un servidor para cada servicio y un equipo adicional que se utilizaba hasta que llegará a fallar el servidor, mientras nuestra no fallará no existía algún problema, pero si fallará el servidor la disponibilidad del servicio se veía afectado mientras se hacía el cambio de equipo de equipo y se validará que todo se levantaría sin inconvenientes.
Se comenta que la alta disponibilidad mínima de horas fuera de servicio al año es tener más del 99.9 % de disponibilidad. Lo que nos permite tener fuera de servicio 8.7 horas fuera de servicio en tiempo productivo. Y así evitamos pérdidas de hasta un día en nuestro sistema de inscripción. En un esquema de virtualización se pudieron realizar mantenimientos de soporte de hardware y software sin provocar algún inconveniente en la perdida de servicio.

Espacio

Con el esquema de tener los servidores en equipos físicos, adicionalmente al perder la disponibilidad de los mismos, consume más espacio en el centro de datos, lo que provocará a la larga no tener espacio para futuras adquisiciones.
Adicionalmente a este problema se le genera otro al tener que adquirir más cableado de red y de red eléctrica lo que genera más costos de instalación de cableado y el mantenimiento de las mismas en el mejor de los casos.
En USECAD se cuentan con los servidores pero no una infraestructura de cableado adecuada, por qué se encuentran cableados con adaptadores para tener más conexiones, el cableado estructurado no era el ideal, cada que se requería un nuevo equipo el cableado de la red no cumplía todas los ISO's de cableado estructurado.

Energía

Otro de los problemas de seguir manejando servidores físicos, es el problema de energización, el uso de la energía se incrementa cada que se adquiera un equipo, contemplando que sólo se tiene una fuente por equipo, aunque el equipo esté ocupando recursos mínimos el equipo demandará energía suficiente para mantenerlo encendido, así como también generando más perdidas de corriente.
Todo esto derivará gastos más fuertes en los recibos de luz (Comisión Federal de Electricidad) y dependiendo el sistema de pago y plan que se tenga contratado, se corre el riego de rebasar límites y pagar arriba de lo estimado.
En USECAD el consumo de la energía era fuerte por tener prendidos los equipos que se encontraban en producción y los de respaldo, además de no tener un cableado adecuado para repartir el voltaje y las cargas de corriente, al realizar cableado eléctrico improvisado con adaptadores sobre alguna toma de corriente.

Enfriamiento

Y por último los problemas fue el enfriamiento de servidores, como se sabe los equipos deben de encontrarse a una temperatura, pero al tener más demanda de energía mayor será la

potencia que tengan los sistemas de enfriamiento. Esto nos limita mucho en los recursos económicos ya que los gastos bastante pesados para una pequeña y mediana empresa. Para el caso de USECAD si es una gran limitante.
Recordando los gastos de pagos de Luz al tener que generar más enfriamiento en el centro de datos, generará más consumo de energía eléctrica y los costes del recibo de luz serán mayores al sobrepasar.
USECAD sólo cuenta con un pequeño rack en su centro de datos, mismo donde se encuentra un ventilador para proveer el enfriamiento necesario para todos los equipos físicos. Dando como resultado una temperatura que no es la ideal disminuyendo el tiempo de vida de la infraestructura. En un futuro si se quieren agregar más servidores será necesario mejorar toda su infraestructura de enfriamiento para no dañar los equipos y brindar una mejor temperatura y evitar disminuir el tiempo de vida de los servidores.

7.3 Análisis de desempeño en los escritorios virtuales

Una vez realizada la migración de físico a virtual en los servidores donde se pudo realizar tal actividad, el análisis tanto de la RAM como el procesamiento fue el mismo en cada máquina, sólo hay que mencionar que el servidor donde se encuentra actualmente (en el Hypervisor) tiene mejores características físicas de hardware. Por lo tanto si el servidor virtual requiere hardware y lo que necesita es menos del que puede ofrecer el servidor físico podrá ofrecer los recursos sin ningún problema, brindando el mismo performance y desempeño.
El problema donde nos encontramos son las conexiones de red ya que sólo contamos con 2 interfaces de red para el servidor de virtualización (RHEV-Hypervisor) sobre tarjetas de 1Gb/s. y el problema radica que el servidor virtual va a requerir trabajar con la misma velocidad como si estuviera físico, pero cabe mencionar que no sólo está compartiendo la red a un solo equipo virtual sino a todos los que se tengan alojados sobre el Hypervisor.
Suponiendo que en un solo hypervisor trabajan más de 4 equipos (Donde se encuentran dos servidores Web y dos servidores de bases de datos) el tráfico de la red sería únicamente por las dos tarjetas de red, lo que provocaría un poco de lentitud, dependiendo la demanda y la concurrencia de los servidores.
En el periodo de inscripción se realizó el monitoreo de ambos equipos y el desempeño si disminuyo un poco en recurso de la red, por el motivo antes mencionado ya que cada servidor empezó a tener más peticiones sobre minuto tanto a la página web como en las bases de datos, la ventaja fue que al adquirir un switch de capa dos con los puertos de 1Gb, se inició a repartir el tráfico de la red sobre las dos tarjetas, aun así no pudimos mejorar los tiempos.
Cabe mencionar que aparte de la redundancia de red que se colocó en los servidores virtuales, la alta disponibilidad que ofrece tener los equipos virtuales también USECAD cuenta con redundancia en sus servicios al tener dos equipos para brindar también los servicios de respaldo.

Software

En la comparación de servidor Físico a Virtual se pudo comprobar que el rendimiento de las aplicaciones y del sistema operativo sigue siendo el mismo, cumpliendo con las expectativas esperadas al momento de realizar la migración.
Lo que sí se pudo mejorar fue la alta disponibilidad de los servidores y tener más confianza en que los servidores no tendrán caída de la aplicación.

Comparación físico-virtual

También se pudo realizar mantenimiento sobre de hardware mientras la aplicación y máquina virtual se encontrará en producción. Donde se le añadió más RAM a un hypervisor para poder soportar las cargas de los servidores.

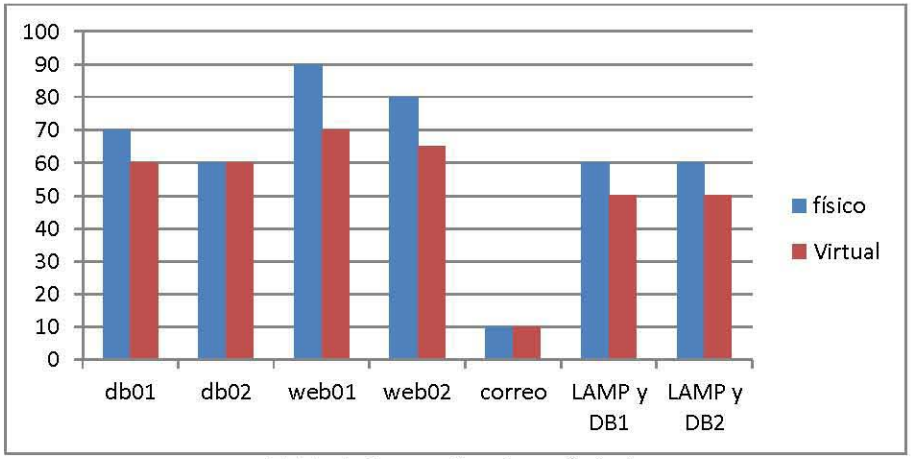


Tabla 1. Comparativa de rendimiento

En la tabla se comprueba que las peticiones sobre minuto fueron mejores en el servidor físico a comparación del servidor Virtual.

7.3 Análisis del estudio de consumo de energía anterior y actual

Análisis de consumo de energía en una infraestructura física.

Haciendo un análisis de la infraestructura física se recabaron datos muy básicos para medir el rendimiento y el consumo energético de los servidores.
Se puede observar en la siguiente tabla el consumo mensual en seis servidores físicos con fuente de energía de 600W de potencia en la fuente de poder.

	Potencia debida a la carga [W]	Potencia de pérdidas magnéticas [W]	Tiempo de uso [Hr]	Consumo diario [KWHr)	Consumo mensual [KWHr]	Costo Energía mensual [$]
Equipo #1	600	10	8	4.88	146.4	204.96
Equipo #2	600	10	8	4.88	146.4	204.96
Equipo #3	600	10	8	4.88	146.4	204.96
Equipo #4	600	10	8	4.88	146.4	204.96
Equipo #5	600	10	8	4.88	146.4	204.96
Equipo #6	600	10	8	4.88	146.4	204.96
					Total:	1229.76

Tabla. Consumo de energía en servidores físicos.

Con la siguiente tabla podemos demostrar que debido a las pérdidas magnéticas nos afectan a los seis servidores, también se observa que se realizó únicamente el estudio durante horarios laborables, sin contemplar tiempos fuera de horario laboral con el fin de no afectar las pruebas por las diferencias de tecnologías entre una infraestructura física y una infraestructura virtualizada.

En un mes de estudios se está consumiendo 1229.76 pesos mexicanos.

Análisis de consumo de energía en una infraestructura virtual

El estudio del consumo energético de una infraestructura virtual se trató de hacer de una forma que se puedan comparar los resultados y contemos con las mismas condiciones. Para el estudio de la infraestructura virtual se tuvo que adquirir equipo más robusto o incrementar piezas a algún servidor para poder utilizarlo de hypervisor (donde vivirán las máquinas virtuales). Únicamente los hypervisores trabajaron con los seis equipos que se compararon cuando estaban en la infraestructura física (stand alone).

Los resultados se muestran en la siguiente tabla:

	Potencia debida a la carga [W]	Potencia de pérdidas magnéticas [W]	Tiempo de uso [Hr]	Consumo diario [KWHr]	Consumo mensual [KWHr]	Costo Energía [$]
Hypervisor 1	900	15	8	7.32	219.6	307.44
Hypervisor 2	900	15	8	7.32	219.6	307.44
Servidor de administración RHEVM	600	10	8	4.88	146.4	204.96
Storage compartido	600	10	8	4.88	146.4	204.96
					Total:	1024.8

Tabla. Consumo de energía en servidores virtuales.

En la infraestructura virtual como se muestro en la tabla los dos hypervisores repartieron la carga de las máquinas virtuales de manera que se pudiera comparar y realizar el ejercicio del consumo de energía. Considerando el punto anterior que los hypervisores son servidores más robustos, requieren mayor potencia para su utilización.

Por definición y análisis de resultados los dos hypervisores cuentan con mucha más capacidad para poder alojar al menos otros diez servidores virtuales y/o escritorios remotos virtuales, que al ir agregando más equipos virtuales mayor será la potencia que necesitará el hypervisor para poder trabajar. Y por ende la comparativa del consumo de energía entre seis equipos físico a virtuales no tendría un buen enfoque.

Recordando un poco cuales son los requerimientos minimos para que una infraestructura virtual funcione es necesario contar con al menos un hypervisor y dos si se quiere contar con las tecnologías de alta disponibilidad. También es necesario tener un servidor externo que se encarga de la administración de máquinas virtuales y por último el servidor o centro de almacenamiento. De tal motivo se consideran equipos que necesitan estar encendidos y consumiendo energía.

Cómo sabemos los hypervisores serán los encargados de proveer los recursos físicos a las máquinas virtuales por eso el consumo de energía es mucho mayor a comparación a los equipos físicos stand alone.

El costo del consumo de energía en una infraestructura virtualizada nos arrojó como resultado durante un mes de horario laborable un total de 1024.8 pesos mexicanos.

Considerando únicamente seis equipos los resultados favorecieron a la infraestructura virtualizada por un menor costo de energía aún sin comparar los niveles de potencia del sistema de enfriamiento para el centro de datos, que al aumentar el número de equipos aumentaría el número de fuentes conectadas y menor sería el espacio del centro de datos requiriendo mucho más potencia en una infraestructura física.

Con respecto a la infraestructura virtualizada podemos observar que si se quieren agregar más servidores únicamente adquiriendo un servidor más robusto nos podrá ofrecer no sólo una

máquina virtual sino las soportadas por las características de hardware del hypervisor y requerimientos de la máquina virtual.

Al mes en seis equipos donde se realizó el ejercicio, se tiene un retorno de la inversión de 200 pesos aproximadamente al mes, recalcando que es únicamente para seis equipos, se tienen más consideraciones a la hora de crear y explotar la solución de virtualización. Con más máquinas virtuales, la creación de escritorios remotos virtuales que no se consideraron para la prueba.

Conclusiones

En base a los estudios realizados de los equipos físicos y virtuales, existe una gran diferencia entre ambos, ya que cuentan con diferentes factores que afectan directamente al rendimiento de cada uno de los equipos.

Por ejemplo los equipos físicos que se virtualizaron, cuentan con tecnología de hardware más vieja tanto en procesador (ciclos de reloj), la memoria RAM cambio de tecnologías y todas estas mejoras de hardware se le ofrecieron a los equipos virtualizados que reemplazarán a los equipos físicos. Es decir, se pueden comparar dos equipos un físico y otro virtual, aunque cuenten con la misma arquitectura y características, el rendimiento en los equipos virtuales tendrá un poco de mayor ventaja a los equipos físicos.

La inversión de adquirir equipos robustos con nuevas tecnologías puede ser un gasto mayúsculo a las empresas, pero en base a todas las pruebas que se realizaron durante nuestro proyecto de tesis, se puede comprobar que es totalmente rentable y sobresaliente los resultados obtenidos, basados en rendimiento por máquina virtual, así como también en base a la disponibilidad del servicio, la reducción del consumo de energía tanto eléctrico como del consumo de energía requerida para el sistema de enfriamiento.

También se puede destacar la facilidad de administración de los equipos virtuales a comparación a los equipos físicos, para realizar cualquier migración, mantenimiento, actualización, adquisición de nuevos equipos y soporte a cada uno de ellos. El ahorro de tiempo de realizar este tipo de tareas es considerablemente menor con respecto a los equipos físicos que es más difícil conseguir ventanas de mantenimiento para realizar cualquier actividad, ya que se requiere contar con mayor tiempo para realizar cualquier actividad.

Ante todas las mejoras de contar con un ambiente virtualizado, se puede complementar otras ventajas como son la creación de varios grupos de equipos con un solo clic, realizar snapshots (impresión del estado actual de un equipo) para poder regresar al mismo estado después de realizar algunas pruebas, la creación de ambientes de prueba basados en snapshots, sobre la infraestructura virtualizada, adicional a esto es más fácil poder adquirir un equipo virtual a realizar todos los trámites para la adquisición de un equipo de prueba y aprobación de la misma (sí toda la infraestructura fuera física).

Uno de los principales focos del proyecto de tesis realizado, es la creación de escritorios remotos virtuales, que tienen como actividad principal proveer a los usuarios y administradores de sistemas escritorios que físicamente se encuentren en el centro de datos, pero que puedan ser utilizados en cualquier lugar, considerando las mejores prácticas de la red para evitar cualquier ataque o perpetración a algún equipo. Es decir la flexibilidad de poder conectarse únicamente mediante un navegador y contar con toda la información de nuestro escritorio remoto virtual.

El poder contar con una infraestructura más robusta nos favorece también en el ámbito energético y de ahorro de la energía, demostrado en los análisis de un

menor consumo y ahorro energético, así como también demandar menos potencia en el sistema de enfriamiento y de esta manera poder reducir costos en el consumo energético de CFE. Con esto podrá generarse el ROI o mejor conocido como recuperación de la inversión.

El contar con un servidor de monitoreo no sólo te da las ventajas de poder estar revisando el estado en tiempo real del servidor, sino también se va creando un inventario que facilita el aprendizaje y comprensión de los sistemas y relación con la que cuenta el centro de datos.

Otro de los puntos a destacar que le dan un valor agregado a nuestro proyecto de tesis es el complemento de una solución de virtualización con una herramienta de monitoreo apoyando de forma automática la prevención de fallos y tener reportes del comportamiento de los equipos, que al final no sólo sirven como evidencia de parte del administrador de servidores, sino también como parte de una pequeña auditoria, que facilitará y proporcionará la información requerida por las empresas.

De esta manera se cumplen todos los objetivos planteados durante el proyecto de tesis, se alcanzaron resultados muy positivos y demostramos las grandes ventajas de virtualizar los centros de datos, de ante mano se conoce la gran inversión que se requiere para poder contar con tal solución, pero a la larga las mejoras, características y soluciones que ofrece tener una infraestructura de virtualización son mucho mejores a contar con equipos únicos de uso específico.

Para terminar todas las herramientas y soluciones utilizadas en este proyecto de tesis son de código abierto, y también se puede adquirir un soporte que ya cuenta con un costo, para nuestro proyecto y reducir los costos de inversión se maneja un soporte personal, ya que nosotros los integrantes del proyecto contamos con la experiencia en el área que se está realizando el proyecto, así como también se está muy familiarizado con las solución.

Por la importancia que tiene las tecnologías de la información en las empresas, nos hemos dado cuenta que también es necesario mejorar un poco nuestros planes de estudios agregando más talleres o algunas materias más especializadas con el fin de poder salir y conocer más soluciones y aplicaciones que se utilizan en el mundo laboral.

Para poder ser un buen administrador de servidores es necesario perder el miedo a los cambios tecnológicos, muchas veces por miedo a perder la estabilidad en los servicios, aplicaciones y sistemas operativos se pierde la oportunidad de conocer las mejoras tecnológicas que van cambiando con respecto al tiempo.

Es difícil aceptar el cambio, pero a la larga los beneficios de aceptar los retos te hacen un excelente administrador, perfeccionando los sistemas con los que se cuentan, se le puede ofrecer mayor satisfacción al usuario de aplicación, base de datos entre otros y sobre todo y uno mismo. También más satisfacción de siempre estar en busca de nuevos retos que aporten a las empresas excelsos

resultados, de esta manera creando nuevas oportunidades a crecer profesionalmente.

"Para llegar a la excelencia nunca hay que detenerse, los éxitos, la grandeza y la superación personal requieren de vencer retos, brincar obstáculos y sobre todo nunca conformarse ni rendirse."

Bibliografía

Capítulo 2

[1]Vladimir Posavac, ***Virtualización de Servidores***
Revista de Tecnologías de Información para la Gerencia
http://www.emb.cl/gerencia/articulo.mvc?sec=1&num=112&mag=1&wmag=46
Marzo 2005

Aspectos básicos de la virtualización
http://www.vmware.com/es/virtualization/what-is-virtualization.html
Red Hat rompe las barreras para la adopción de la virtualización
http://www.es.redhat.com/solutions/virtualization/

Tipos de Virtualización
http://www.vmlogia.com/tiposdev.aspx
Antonio Pérez, *Tipos de Virtulización*
http://blog.pucp.edu.pe/item/52077/tipos-de-virtualizacion
Abril 2009

Hypervisor
http://www.virtualizacion.com/?page_id=8

¿Qué es un Hypervisor?
http://khan1.blogspot.com/2008/09/qu-es-un-hypervisor.html
Septiembre 2008

Red Hat Enterprise Virtualization Hypervisor
http://www.redhat.com/virtualization/rhev/desktop/hypervisor/

Red Hat Enterprise Virtualization Manager para Escritorios
http://www.latam.redhat.com/virtualization/rhev/desktop/components/rhevm/

Red Hat Enterprise Virtualization for Desktops 2.2
http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Virtualization_for_Desktops/2.2/html-single/Administration_Guide/index.html#storage_over

NFS
http://www.linux-cd.com.ar/manuales/rh9.0/rhl-rg-es-9/ch-nfs.html

Nick Triantos, *FCoE: ¿el futuro de Fibre Channel?*
http://www.netapp.com/es/communities/tech-ontap/tot-fcoe-es.html

iSCSI vs Fibre Channel: combate por el storage
http://www.revistatcn.com/id10727/iscsi-vs-fibre-channel-combate-por-el-reinado-del-storage/
Noviembre 2010

Linux Networkin Bounding
http://www.slideshare.net/jsancheznav/bounding-en-linux

Alta Disponibilidad
http://www.neovalia.es/imagenes/ficheros/vmware/Datasheets/high_availability_es.pdf

J. Case, M. Fedor, M. Schofftall, J. Davin
A Simple Network Management Protocol (SNMP)
Request for Comments: 1157
http://tools.ietf.org/html/rfc1157
May 1990

Introducción a Instrumental de administración de Windows
http://technet.microsoft.com/es-es/library/cc736575%28WS.10%29.aspx

WMI
http://msdn.microsoft.com/en-us/library/aa384642%28v=vs.85%29.aspx

T. Ylonen, C. Lonvick, **The Secure Shell (SSH) Protocol Architecture**
http://www.ietf.org/rfc/rfc4251.txt
January 2006

Zenoss
Zenoss Core - Open Source IT Management
Shuckins
http://community.zenoss.org/docs/DOC-2614

Zenoss Enterprise Architecture Overview
White Paper
http://www.zenoss.com/in/White_Paper_Zenoss_Enterprise_Architecture_Overview.html

Escritorios Remotos
http://www.qumulos.com/escritorios-virtuales/
http://www.tuexpertoit.com/2009/12/15/red-hat-libera-el-codigo-del-protocolo-de-virtualizacion-spice/
http://www.latam.redhat.com/virtualization/rhev/desktop/components/spice/
http://www.articuloz.com/redes-articulos/que-es-el-protocolo-rdp-4830509.html

Capítulo 3

http://jjmora.es/capacity_planning_introduccion_i/
http://www.impulseit.com/cmsimple/?Servicios:Capacity_Planning

Iscsi,the Universal Storage Connection
john l. hufferd
Editorial: addison-wesley

Vmware vsphere
Install, configure, manage
Student manual-volume 1
ESX 5.0and vCenter Server 5.0

Vmware vsphere
Install, configure, manage
Student manual-volume 2
ESX 5.0and vCenter Server 5.0

Red hat training and certification RH318
Redhat enterprise Virtualization 3
Release en 1-20120210

Red Hat training and certification RH100
Red Hat enterprise Linux 6.0
Release en 1-20120210

Red Hat training and certification RH200
Red Hat enterprise Linux 6.0
Release en 1-20120210

9.-Red Hat training and certification RH300

Red Hat enterprise Linux 6.0
Release en 1-20110729

10.- RED HAT LINUX: MANUAL DEL ADMINISTRADOR

Richard Petersen, mcgraw-hill

interamericana de españa, s.a., 2004