



Instituto Tecnológico de Morelia
División de Estudios Profesionales
Departamento de Sistemas y Computación

Opción X

Informe de Residencia Profesional

“Implementación de servidores virtualizados que mejoren la eficiencia del uso de energía y servicios de red en centros de investigaciones”

Que para obtener el título de:

Ingeniero en Sistemas Computacionales

Presenta:

Fernando Villaseñor Béjar

Asesor:

M.T.I. Heberto Ferreira Medina

Morelia, Michoacán, Junio de 2011



Instituto Tecnológico de Morelia
División de Estudios Profesionales
Departamento de Sistemas y Computación

Opción X

Informe de Residencia Profesional

“Implementación de servidores virtualizados que mejoren la eficiencia del uso de energía y servicios de red en centros de investigaciones”

Que para obtener el título de:

Ingeniero en Sistemas Computacionales

Presenta:

Fernando Villaseñor Béjar

Asesores:

M.T.I. Heberto Ferreira Medina

Ing. Alberto Valencia García

Morelia, Michoacán, Junio de 2011

Dedicatoria

A mis padres Fernando y Susana y a mi hermano Rodrigo, por su apoyo y estímulo para poder continuar con mis estudios. A mis primos Carlos y Liz por siempre estar ahí y ser unos guías en mi vida.

Agradecimientos

Agradezco a mi familia, en especial a mis papas y hermano por creer en mí y apoyarme en cada paso que di durante el transcurso de mi carrera.

Expreso mis más sinceros agradecimientos al Centro de Investigaciones en Ecosistemas (CIEco) por haberme dado la oportunidad de desarrollar éste proyecto.

A mis asesores M.T.I Heberto Ferreira Medina y al I.S.C Alberto Valencia García por apoyarme en el desarrollo de éste proyecto.

A mis amigos José Luis Rivera Magallón, Sergio Luis Guzmán y al I.S.C Armando Galindo por sus consejos y colaboración en éste proyecto.

Índice

Introducción	i
Justificación	ii
Objetivo general del proyecto:	iii
Objetivos Específicos	iii
Caracterización del área donde se participó	iii
Problemas a resolver	iv
Alcances y limitaciones	iv
Capítulo 1: Virtualización de servidores	6
1.1.- Virtualización	7
1.2.- Software para virtualización	9
1.2.1.- Microsoft Virtual PC	9
1.2.2.- Kernel Virtual Machine (KVM)	9
1.2.3.- Microsoft Virtual Server	9
1.2.4.- VMware	9
1.2.5.- Xen	10
1.2.6.- VirtualBox	10
1.2.7.- Citrix XenServer	10
1.3.- XenCenter	11
1.4.- Alta Disponibilidad	12
1.4.1. Clúster de Alta Disponibilidad	12
1.5. Herramientas de Alta disponibilidad	13
1.5.1. Heartbeat	13
1.5.2. Idirectord y LVS (linux virtual server)	13
1.5.3. Pirahna	14

1.5.4. UltraMonkey	14
1.5.5. Kimberlite	14
1.6. Aplicaciones para servicios en red	15
1.6.1. Postfix (administrador de correo electrónico)	15
1.6.2. ClamAV	17
1.6.3. SpamAssassin	18
1.6.4.- Mailscanner	19
1.7.- Sistema Operativo CentOS	21
Capítulo 2: Instalación y configuración de servicios de red virtualizados	24
2.1. Actividades con XenServer	25
2.2. Administración del servidor con XenCenter	27
2.3. Alta disponibilidad en máquinas virtuales	29
2.4. Aplicaciones de Seguridad	32
2.5. Herramientas de gestión de información y servicios web (servidores web virtualizados).	33
2.5.1. Servidor Web	33
2.5.2. Servidor Web Apache	34
2.5.3 MySQL	35
2.5.4. PHP5	36
2.5.5. Joomla	38
2.6. Implementación de clientes ligeros (curso de XenServer de Citrix)	40
2.6.1. XenDesktop	42
2.6.2. XenApp	43
2.6.3. XenClient	44
2.7. Servidor Untangle	50

2.7.1. Firewall (Cortafuegos)	53
2.7.2. Configuración del Servidor Firewall Untangle	54
Capítulo 3: Pruebas y Resultados de la Virtualización	61
3.1. Ahorro de Energía	62
3.2. Uso de servicios virtualizados	63
3.3. Pruebas de rendimiento de los servicios virtualizados	66
Capítulo 4: Conclusiones y Recomendaciones	69
Referencias y Bibliografía	72
Anexos	75
Anexo A : Instalación y configuración de XenServer	75
Anexo B : Instalación y configuración de Heartbeat	79
Configuración del Nodo 1	84
Configuración del Nodo 2	90
Verificando el agrupamiento (cluster).	94
Mantener sincronizados los directorios.	94
Anexo C : Instalación de Postfix	96
Anexo D : Instalación de ClamAv	96
Anexo E : Instalación de SpamAssassin	98
Anexo F : Instalación de Mailscanner	100
Anexo G : Instalación de Mailwatch	102
Anexo H: Instalación de MySql	107
Anexo I: Instalación de PHP	108
Anexo J: Instalación de Joomla!	109

Índice de Figuras y Tablas

<i>Figura 1.1: Virtualización de servidores</i>	7
<i>Figura 1.2: XenCenter 5.0</i>	12
<i>Figura 1.3: Postfix</i>	15
<i>Figura 1.4: ClamAV</i>	17
<i>Figura 1.5: SpamAssassin</i>	18
<i>Figura 1.6: MailScanner</i>	19
<i>Figura 2.2: Ventana principal de XenCenter</i>	28
<i>Figura 2.3: Configuración del servidor</i>	28
<i>Figura 2.4: Heartbeat; cliente 1 activo</i>	31
<i>Figura 2.5: Heartbeat; cliente 2 activo</i>	32
<i>Figura 2.6: Herramientas para ofrecer servicios de red</i>	33
<i>Figura 2.7: Apache</i>	34
<i>Figura 2.8: PHP 5</i>	37
<i>Figura 2.9: Joomla!</i>	38
<i>Figura 2.10: Virtualización del puesto de trabajo</i>	41
<i>Figura 2.12: Citrix Receiver</i>	43
<i>Figura 2.11: XenDesktop 5</i>	42
<i>Figura 2.13: XenApp</i>	44
<i>Figura 2.15: Servidor virtualizado con 3 clientes ligeros</i>	46
<i>Figura 2.16: Servidor con componentes instalados</i>	47
<i>Figura 2.17: Untangle</i>	50
<i>Figura 2.18: Rack de Untangle; Características de Untangle !</i>	52
<i>Figura 2.19: Firewall!</i>	54
<i>Figura 2.20: Rack de Untangle</i>	56
<i>Figura 2.21: Firewall con sus reglas</i>	59
<i>Figura 3.1: Máquinas virtuales instaladas</i>	63
<i>Figura 3.2: Alta disponibilidad</i>	64
<i>Figura 3.3 Máquina virtual con herramientas de seguridad en linux</i>	65
<i>Figura 3.4: Máquina virtual con servidores</i>	65
<i>Figura 3.5: Servidor Virtualizado para los clientes ligeros</i>	66
<i>Figura A1: Contraseña root.</i>	75
<i>Figura A2: Selección de DHCP</i>	76
<i>Figura A3: Nombre del servidor</i>	76
<i>Figura A4: Localización de XenServer</i>	77
<i>Figura A5: Se instala XenServer</i>	77
<i>Figura A6: Instalación del segundo CD</i>	78
<i>Figura A7: Figura 27. XenServer</i>	78

<i>Figura H1: LocalHost Apache en navegador</i>	107
<i>Figura I2: Servidor PHP com MySql</i>	109
<i>Figura I1: LocalHost del servidor PHP</i>	108
<i>Figura J1: LocalHost de Xampp</i>	110
<i>Figura J6: Localhost de Joomla! configurado</i>	114
<i>Figura J5: Paso 3 del asistente de configuración de Joomla!</i>	113
<i>Figura J4: Paso 1 del asistente de configuración de Joomla!</i>	112
<i>Figura J3: LocalHost de Joomla!</i>	112
<i>Figura J2: phpMyadmin</i>	111
<i>Tabla 1. Actividades Realizadas</i>	v
<i>Tabla 1.1: Características de Clamav</i>	18
<i>Tabla 1.3: Características de CentOS</i>	23
<i>Tabla 2.1: Comparativa entre virtualizadores</i>	26
<i>Tabla 2.2: Requisitos de Untangle</i>	55
<i>Tabla 2.3: Aplicaciones de Untangle</i>	57
<i>Tabla 2.4: Reglas para el firewall del ciego (ref)</i>	58
<i>Tabla 2.6: Configuración de la red en untangle</i>	60

Introducción

La virtualización de servidores se sitúa, en la actualidad, como una de las facetas más importantes dentro de la tendencia de modernización e implantación de las nuevas tecnologías en el mundo de las Tecnologías de la Información (TI).

El Centro de Investigación en Ecosistemas de la UNAM campus Morelia (Unam, 2011) ha tenido la necesidad de implementar servidores virtuales con el propósito de hacer más eficiente el uso de los recursos, mejorar su disponibilidad, ahorro de energía, recuperación de datos y además de ofrecer redundancia en servicios de red.

Las actividades que se realizaron en el proyecto abarcan temas relacionados con servidores, tal es el caso de la virtualización, así como también alta disponibilidad y redundancia. Se realizaron actividades de instalación servidores web y de correo en las máquinas virtuales, como Joomla (Joomla, 2011) y Apache (Linux para todos, 2009). Mientras tanto, también se instalaron herramientas de seguridad en Linux, con la finalidad de proteger la información contenida en las máquinas virtuales.

Además de un curso impartido por Citrix acerca de la plataforma XenServer (Citrix, 2011) para la creación de clientes ligeros, mediante las distintas herramientas que Citrix ofrece. Así como la implementación de un servidor Untangle que permite dar seguridad a la red mediante firewalls.

Se tiene una breve justificación del porqué se desarrolló el proyecto, además de sus objetivos primordiales y específicos, una descripción de cómo y dónde se desarrolló y cuáles eran los problemas al inicio del mismo.

Posteriormente se describen los alcances del proyecto, sus limitaciones, los aspectos teóricos, el procedimiento de cómo se realizaron todas las actividades y los resultados, finalmente se tienen las conclusiones del proyecto en general.

Justificación

La UNAM ha destacado entre otras universidades por sus investigaciones y avances tecnológicos, además de tener dentro de sus centros de investigación tecnología que le permite realizar su trabajo de una mejor manera.

La UNAM campus Morelia (Unam, 2011) no es la excepción, ésta tiene áreas y centros de investigación con tecnología de punta que le permiten poder realizar sus proyectos.

El Centro de Investigación en Ecosistemas debido al crecimiento de las tecnologías de la información y comunicaciones ha tenido la necesidad de establecer el sistema de red con una infraestructura altamente competitiva, además de virtualizar servidores físicos para su mejor aprovechamiento, mejora de energía, alta disponibilidad y redundancia de máquinas virtuales.

Este centro de investigación cuenta con información que debe estar almacenada en servidores para el fácil acceso de los usuarios; por tal motivo éste proyecto busca migrar esa información a máquinas virtuales que se encuentran en el servidor físico, con la finalidad de tener un mejor control utilizando alta disponibilidad.

Además de facilitar un laboratorio con clientes ligeros para lograr mejores costos administrativos, utilizando un servidor virtualizado con XenServer.

Otro de los motivos para desarrollar éste proyecto fue la seguridad de la red, es decir la implementación de cortafuegos, para controlar el filtrado de información.

Objetivo general del proyecto:

Mejorar la eficiencia de energía y alta disponibilidad de los servidores del CIEco, utilizando la virtualización de servicios de red.

Objetivos Específicos

- Virtualización de servidores.
- Crear servidores virtuales con alta disponibilidad, redundancia y mejora de energía.
- Implementar servicios de red mediante la configuración de servidores ftp, correo y web.
- Establecer filtrado y bloqueo a la red mediante firewalls.
- Implementar herramientas de seguridad para las maquinas virtualizadas
- Cubrir áreas de la universidad con red inalámbrica con HotSpot.
- Implementar clientes ligeros en los laboratorios de cómputo en la plataforma XenServer.
- Documentar cada proceso y actividad que se realice.

Caracterización del área donde se participó

Este proyecto fue realizado en el Centro de Investigaciones en Ecosistemas, en la Universidad Autónoma de México (UNAM) Campus Morelia. En el área de telecomunicaciones y cómputo del centro.

Para desarrollar el proyecto, el departamento asignó una oficina, la cual cuenta con escritorio, impresora, escáner, un switch y el servidor con el cual se llevó a cabo el proyecto.

La UNAM Campus Morelia se encuentra localizada al sur de la ciudad de Morelia en la antigua carretera a Pátzcuaro #8701 Col. ex-hacienda de San José de la Huerta C.P 58190 Morelia, Michoacán, México.

Problemas a resolver

- Mejoras en la red LAN, utilizando conceptos de CISCO.
- Mejorar el acceso y denegación de servicios a la red mediante cortafuegos con servidor Untangle.
- Virtualización de servidores físicos con la finalidad de:
 - Mejora en el uso de energía.
 - Alta disponibilidad
 - Facilitar la administración
- Configuración de servidores Web, para mejorar los servicios de red de la UNAM, Web y correo electrónico en máquinas virtuales.
- Activación de servicios red en las máquinas virtuales; servidor web, servidor de correo electrónico, servidor de aplicaciones, redundancia de máquinas virtuales mediante heartbeat, etc.
- Implementar herramientas de seguridad para las maquinas virtualizadas.
- Implementar clientes ligeros en los laboratorios de cómputo en la plataforma XenServer, propuesta.

Alcances y limitaciones

El proyecto que se desarrolló en residencias profesionales, resolvió los problemas que se plantearon en el apartado de *Problemas a Resolver*, sin embargo, el proyecto no ha finalizado aún. Todavía se encuentra en fase de desarrollo debido al tiempo de entrega de éste documento.

Cabe destacar, que estas actividades serán realizadas en un periodo posterior a la entrega del proyecto. En la tabla 1 se muestran las actividades realizadas:

No. Actividad	Nombre de la Actividad
1	Virtualización de servidores físicos
2	Alta Disponibilidad en máquinas virtuales
3	Configuración de servidores web y correo
4	Implementación de herramientas de seguridad para las máquinas virtualizadas
5	Implementación de clientes ligeros con XenServer (curso de Citrix)
6	Implementación de firewalls con la herramienta Untangle

Tabla 1. Actividades Realizadas

En el primer capítulo se describe los conceptos fundamentales de la virtualización de servidores, características, ventajas y desventajas, las diferencias entre las herramientas de virtualización.

Además de los conceptos de alta disponibilidad, las diferentes herramientas que existen para implementarla. Algunas aplicaciones que dan seguridad al sistema operativo Linux y finalmente las cualidades que éste presenta.

Capítulo 1: Virtualización de servidores

1.1.- Virtualización

La virtualización de servidores se puede aplicar para muchos propósitos, tales como para mantener entornos múltiples de software dentro de una misma máquina para realizar pruebas o simplemente para que un usuario de escritorio pueda ejecutar distintos sistemas operativos. En la actualidad se pueden encontrar tres modelos de Virtualización (Eugenio Villas, 2010).

- Modelo de Máquina Virtual.
- Modelo de Máquina Paravirtual.
- Modelo de virtualización a nivel de Sistema Operativo.

Para el caso de los servidores físicos que se tiene en el CIEco, el modelo a implementar es el Modelo de Máquina Virtual, ya que este modelo está basado en la arquitectura cliente/servidor, donde cada cliente funciona como una imagen virtual de la capa hardware. Este modelo permite que el sistema operativo cliente funcione sin modificaciones. Además permite al administrador crear diferentes sistemas clientes con sistemas operativos independientes entre sí, ver figura 1.1.

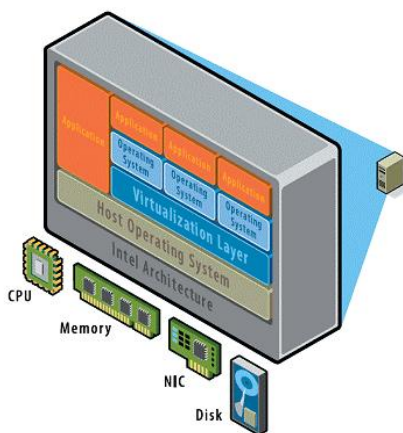


Figura 1.1: Virtualización de servidores

La virtualización de servidores tiene varias ventajas, una de ellas es que permite crear en una máquina física varias máquinas virtuales que se comportan como

una real con sistemas operativos y aplicaciones instaladas en ellas, es decir que el software no distingue ninguna diferencia entre una máquina física y una virtual (Eugenio Villas, 2010).

Todas las máquinas virtuales pueden configurarse de forma aislada e independiente de las demás, sin influir en el hardware o en el resto de máquinas virtuales.

La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución. Cada máquina virtual permanece completamente aislada de las otras, y se separa del host subyacente mediante una fina capa de software denominada hipervisor. Ello permite que cada máquina virtual ejecute diferentes sistemas operativos y aplicaciones. Al estar las máquinas desvinculadas del host que las aloja, el huésped también puede ser trasladado de un servidor físico a otro mientras está funcionando; a esto se le denomina migración en vivo

También se pueden enlistar varias desventajas de la virtualización de servidores (Jmarrior, 2008):

- ⊕ Rendimiento Inferior
- ⊕ No es posible utilizar hardware que no esté gestionado o soportado por el *hipervisor* tecnología de virtualización (VT-X).
- ⊕ El sistema operativo anfitrión se vuelve de rol crítico
- ⊕ No se dispone de aceleración de video por hardware.
- ⊕ Desaprovechamiento de recursos
- ⊕ Disminuye las ventas de hardware.

1.2.- Software para virtualización

1.2.1.- Microsoft Virtual PC

Es un software gestor de virtualización desarrollado por Connectix y comprado por Microsoft para crear equipos virtuales. Su función es emular mediante virtualización, un hardware sobre el que funcione un determinado sistema operativo. Con esto se puede conseguir ejecutar varios sistemas operativos en la misma máquina a la vez y hacer que se comuniquen entre ellos (Montenegro, 2009).

1.2.2.- Kernel Virtual Machine (KVM)

Es una solución para implementar virtualización completa con Linux sobre hardware x86. Está formada por un módulo del núcleo (con el nombre kvm.ko) y herramientas en el espacio de usuario, siendo en su totalidad software libre. El componente KVM para el núcleo está incluido en Linux desde la versión 2.6.20 (Montenegro, 2009).

1.2.3.- Microsoft Virtual Server

Es una aplicación que facilita la creación de máquinas virtuales en los sistemas operativos Windows XP y Windows Server 2003. Originalmente fue desarrollado por Connectix, siendo adquirido posteriormente por Microsoft. Virtual PC es el paquete de Microsoft para escritorios virtuales (Montenegro, 2009).

1.2.4.- VMware

Filial de EMC Corporation (Montenegro, 2009). que proporciona la mayor parte del software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player. El software de VMware puede funcionar en Windows, Linux, y en la plataforma Mac OS X compatible con INTEL, bajo el nombre de VMware Fusion. El nombre corporativo de la compañía es un juego de palabras usando la interpretación tradicional de las siglas VM en los ambientes de computación, como máquinas virtuales (Virtual Machines) (Montenegro, 2009).

1.2.5.- Xen

Es un monitor de máquina virtual de código abierto desarrollado por la Universidad de Cambridge (Montenegro, 2009).

Su objetivo es ofrecer virtualización de sistemas operativos con todas sus características, de forma completamente funcional en un equipo sencillo. Xen proporciona aislamiento seguro, control de recursos, garantías de calidad de servicio y migración de máquinas virtuales.

Los sistemas operativos pueden ser modificados explícitamente para correr Xen (aunque manteniendo la compatibilidad con aplicaciones de usuario). Esto permite a Xen alcanzar virtualización de alto rendimiento sin un soporte especial de hardware. Intel ha realizado diversas contribuciones a Xen que han permitido añadir soporte para sus extensiones de arquitectura *VT-X Vanderpool* (Montenegro, 2009). Esta tecnología permite que sistemas operativos sin modificar actúen como hosts dentro de las máquinas virtuales de Xen.

1.2.6.- VirtualBox

Es un software de virtualización para arquitecturas x86, creado originalmente por la empresa alemana Innotek GmbH (Montenegro, 2009). Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como sistemas invitados, dentro de otro sistema operativo llamado anfitrión, cada uno con su propio ambiente virtual.

1.2.7.- Citrix XenServer

Citrix XenServer es una solución empresarial abierta y potente para virtualización de servidores, capaz de reducir radicalmente los costos del centro de datos, transformando entornos estáticos y complejos en centros de distribución más dinámicos y fáciles de administrar (Citrix, 2011)

XenServer es una solución para infraestructuras de virtualización en entornos de *cloud computing*, integra gratuitamente funcionalidades críticas, como la migración

en tiempo real y la gestión centralizada multinodo. Además incluye: alta disponibilidad automatizada, automatización del ciclo vital, aprovisionamiento dinámico para máquinas físicas y virtuales, e integración con las principales plataformas de almacenamiento de datos.

Con plataformas de virtualización de servidores más avanzadas, se puede incluso migrar activamente las cargas de trabajo a distintos servidores físicos. Con este sistema se distribuye la carga flotante de trabajo entre todo el *pool* * de recursos físicos, permitiendo a las Tecnologías de la información maximizar su utilización, reducir costes y entregar aplicaciones a los usuarios de forma fiable y eficaz.

- Infraestructura de Servidores y Almacenamiento

XenServer es una herramienta gratuita que incluye ciertas funcionalidades tales como la migración en tiempo real, soporte compartido para almacenamiento, gestión centralizada multinodo y pooling de recursos.

Al unificar cargas de trabajo de varios equipos de hardware subutilizados, se puede lograr un ahorro inmediato en energía, enfriamiento y administración, optimizar el uso del hardware existente y mejorar la gestión y confiabilidad.

- Distribución de las Cargas de Trabajo de los Servidores

La administración centralizada multiservidor y la migración en tiempo real de XenServer permite a los administradores de Tecnologías de la Información optimizar la utilización de los recursos, reduciendo a cero los tiempos de inactividad de los usuarios.

1.3.- XenCenter

XenCenter es una herramienta de administración para los servidores, ver figura 1.2, con ella se puede acceder al servidor, manipularlo, llevar a cabo la creación

Pool = Suma de recursos de todos los servidores físicos. Se pueden añadir y compartir.*

de las máquinas virtuales, además de controlar otros aspectos del servidor. Es la consola para acceder al servidor, visualizar lo que el servidor contiene, sus características y propiedades.



Figura 1.2: XenCenter 5.0

1.4.- Alta Disponibilidad

Es la implementación mediante dos o más máquinas de asegurar, mediante mecanismos de monitorización, que el trabajo no se interrumpa en caso de fallo, es decir asegura un cierto grado de continuidad operacional durante un período de medición dado. Se refiere también a la habilidad de los usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema se dice que está no disponible. El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible (Paredes, 2010)

1.4.1. Clúster de Alta Disponibilidad

Es un sistema capaz de ocultar los fallos que se producen en él para mantener una prestación de servicio continua.

Los conceptos de alta disponibilidad y de *clustering* están profundamente relacionados, ya que el concepto de alta disponibilidad de servicios implica directamente una solución mediante un clúster de computadoras.

El funcionamiento de un clúster muy importante: se trata de un conjunto de piezas, por ejemplo, de varios microprocesadores a través de una red de alta velocidad que los vincula de forma tal que funcionan como un único ordenador pero de una potencia mayor al convencional.

Un clúster se implementa básicamente con varias computadoras, deben conectarse en una LAN compartida dedicada sólo para el clúster. El clúster de alto rendimiento opera bajo circunstancias en que las tareas a procesar se reparten paralelamente a las computadoras.

1.5. Herramientas de Alta disponibilidad

Existen diversas herramientas de alta disponibilidad, algunas gratuitas mientras que para otras se debe pagar una licencia. Se hizo una investigación previa de estas herramientas para poder determinar cuál de ellas era viable para el proyecto, enseguida se describen las herramientas de alta disponibilidad más comunes:

1.5.1. Heartbeat

Es una de las herramientas fuertes de alta disponibilidad para Linux, permite crear un clúster de alta disponibilidad (Scribd, 2011). Heartbeat como cluster, soporta como mínimo dos nodos, permite intercambiar recursos entre nodos, sin embargo carece de herramientas de monitorización.

1.5.2. Idirectord y LVS (linux virtual server)

LVS permite crear un clúster de balanceo de carga, en el cual hay un nodo que se encarga de gestionar y repartir las conexiones (nodo máster LVS) entre todos los

nodos esclavos del clúster (López, 2011). *ldirectord* es un demonio que se ejecuta en el máster LVS, que se encarga de probar el servicio de datos de los nodos esclavos y eliminarlos e insertarlos en el clúster dinámicamente, si surge algún problema o si el servicio se restablece según sea el caso.

1.5.3. Pirahna

Red Hat ofrece una solución basada en LVS (Scribd, 2011), agrega una interfaz Web para configurarlo. Es una solución sencilla de implementar, es una compilación de herramientas para el cluster Linux LVS, a las que se ha agregado una interfaz amigable que facilita al usuario la instalación y configuración de esta aplicación.

1.5.4. UltraMonkey

Es una solución creada por VA Linux que se basa en LVS y Heartbeat para ofrecer clústers de alta disponibilidad y balanceo de carga (Scribd, 2011).

Ultra Monkey es un proyecto destinado a crear una red de servicios de alta disponibilidad con balanceo de carga. Por ejemplo, un cluster de servidores web que se hace ver al mundo real como un solo servidor web.

Ultra Monkey permite al sistema GNU/Linux proporcionar una solución flexible que puede ser adaptada a una amplia gama de necesidades, desde pequeños clustes con dos nodos hasta enormes sistemas sirviendo miles de conexiones por segundo.

1.5.5. Kimberlite

Creada por Mission Critical Linux (Paredes, 2010), está especializada en almacenamiento compartido de datos y mantenimiento de la integridad de los mismos.

1.6. Aplicaciones para servicios en red

1.6.1. Postfix (administrador de correo electrónico)

Postfix es un servidor de correo de software libre o código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura (Venema, 2008). Ver figura 1.3

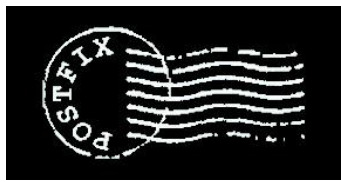


Figura 1.3: Postfix

Sus características son las siguientes:

- **Diseño modular (no es un programa monolítico):** Postfix está compuesto de varios procesos que se comunican entre sí, con las ventajas e inconvenientes que ello conlleva. Esta característica repercute positivamente en otras.
- **Gran Seguridad:** Desde el comienzo de su diseño ésta ha sido una de sus premisas fundamentales. De este modo, provee de:
 - Seguridad frente a ataques contra el servidor
 - Seguridad contra el uso inadecuado (spam, relay, etc.), debido a que soporta directamente listas negras. Además, se puede instalar Postfix de forma que corra en modo *chroot*, lo que le conlleva a su operativa más seguridad.
 - Filtrado de cabeceras y cuerpos de mensajes por expresiones regulares.
 - Cada proceso corre con los mínimos permisos necesarios para realizar su tarea.

- **Gran Rendimiento:** Postfix puede procesar una gran cantidad de mensajes al día sin problemas. Esta potencia se debe en parte a su modularidad, que además viene con el añadido de que se pueden definir ciertos parámetros para cada uno de los procesos, como el número máximo de procesos simultáneos de un tipo, activar o desactivar un proceso innecesario, etc., que permiten optimizar aún más su funcionamiento. Además, el sistema de gestión de colas de mensajes es también modular, consistiendo en cuatro colas distintas que está procesadas muy eficientemente.
- **Soporte para las tecnologías más actuales:** Al estar actualizado, emplea técnicas desarrolladas para aprovechar mejor y dar soporte a los servidores Web más modernos.
- **Muy buen soporte para administrar dominios virtuales**
- **Facilidad de configuración:**
- **Compatibilidad hacia/desde fuera con Sendmail**
- **Fácil integración con programas antivirus:** Se pueden insertar procesos externos entre ciertas partes del sistema Postfix, lo cual es muy útil para integrar un antivirus. Un ejemplo de ello es Clamav.
- **Facilidad para detectar errores:** Postfix tiene múltiples formas de obtener información de los errores ocurridos y explicarlos. Además, gracias a su modularidad es más sencillo saber qué proceso es el que falla, también se puede activar la emisión de más información de depuración de forma independiente para cada programa.
- **Posibilidad de lanzar varias instancias de Postfix en la misma máquina con distintas configuraciones:** Se puede usar cada una de estas instancias con distintas direcciones IP, distintos puertos, etc. De esta forma se puede tener más de un servidor para cada necesidad.

- **Código Fuente abierto y bien estructurado:** Se considera el código fuente de Postfix como un ejemplo de *diseño, claridad y documentación*, por lo que facilita su mantenimiento por parte de desarrolladores así como la incorporación de nuevas capacidades, corrección de errores, adaptaciones, etc.

1.6.2. ClamAV

El proyecto ClamAv Antivirus fue fundado en el año 2001 por Tomasz Kojm (Linux para todos, 2010). Actualmente tiene una amplia aceptación como antivirus para servidores. ClamAV nació como un proyecto Open Source que pretende identificar y bloquear virus en el sistema. Ver figura 1.4.



Figura 1.4: ClamAV

Gracias a la colaboración de varias compañías, universidades y otras organizaciones ha posibilitado al proyecto ClamAV poseer una red extensa de distribución rápida y fiable en todo el mundo.

Algunas de las características de ClamAV son las siguientes:

1	Licenciado bajo GNU General Public License 2
2	Detecta alrededor de 320,000 virus, gusanos, troyanos, incluyendo virus programados como macros de Microsoft Office
3	Escaneo de archivos y ficheros

	comprimidos
4	Soporta plataformas de 32/64 bit..
5	Soporta la mayoría de formatos de correo electrónico

Tabla 1.1: Características de Clamav

1.6.3. SpamAssassin

SpamAssassin, es una herramienta para inspeccionar correos electrónicos, que permite determinar si se trata de un mensaje basura (SPAM) (Linux para todos, 2010). Ver figura 1.5.



Figura 1.5: SpamAssassin

En este sentido SpamAssassin es considerado un pre-procesador de correos, ya que la inspección es llevada a cabo en el servidor de correos previo a que el usuario descargue su correo, permitiendo así una pre-clasificación de mensajes antes de utilizar un cliente de correo (Outlook, Eudora o Mozilla, entre otros).

SpamAssassin utiliza varios criterios para determinar si un mensaje es SPAM :

- Inspección de *Headers* : Los *Headers* o cabeceras de mensaje contienen información importante acerca del mensaje, como lo son procedencia y rutas de servidor, SpamAssassin inspecciona esta información para fines de detección.

- **Análisis del Mensaje:** El cuerpo y título del mensaje también son leídos por SpamAssassin, realizando búsquedas por palabras claves o estructuras que conforman un correo basura.
- **Listas Negras:** Actualmente, existen listas que enumeran servidores de correo conocidos como generadores de SPAM ("Open-Relays").
- **Análisis probabilístico:** Una vez definidas las reglas iniciales para detección, SpamAssassin utiliza análisis probabilístico para determinar similitudes entre mensajes entrantes y aquellos ya detectados como SPAM.
- **Listas Hash o Firmas de Correo :** Debido a que un correo SPAM suele ser enviado a miles de personas a la vez, la estructura de cada mensaje es idéntica en todas sus instancias, así produciendo un Hash inequívoco. SpamAssassin consulta listas de Hashes sobre mensajes conocidos.

1.6.4.- Mailscanner

MailScanner es una herramienta que permite agregar una mayor seguridad y filtrado de e-mail, contiene un paquete anti-spam para servidores de MTA (Agente de Transferencia de Correo (Linux para todos, 2011)). Está diseñado para ejecutarse en los servidores de correo operados por algún servidor de correo como sendmail o postfix. Ver figura 1.6.



Figura 1.6: MailScanner

El software funciona con cualquier sistema basado en Unix y el sistema es compatible con una amplia gama de MTA. Viene con soporte para cualquier combinación paquetes antivirus, incluida la de distribución libre ClamAV escáner, y su diseño permite el uso de escáneres de virus múltiples en paralelo para aumentar el nivel de seguridad.

La protección contra el SPAM se basa en el ampliamente aclamado paquete de SpamAssassin, sin embargo tiene la característica de efectuar búsquedas rápidas rechazar de una gran porción de mensajes.

Para proteger la información contra el MALWARE (Linux para todos, 2011), se realiza una serie de pruebas para poder detectarlo, éstas se basan en ciertas normas para analizar el contenido de los archivos. También incorpora uno de los más sofisticados detectores de *phishing*.

MailScanner es altamente configurable mediante un sistema de reglas muy intuitivo. Prácticamente cada opción de configuración, por ejemplo, puede ser controlado en un esquema por usuario, por dominio o por IP.

MailScanner no requiere modificación de las configuración de sendmail, además es fácil de integrar en su sistema de transporte de correo.

MailScanner es totalmente gratuito, no requiere licencia, la instalación o de cuotas de suscripción. Es utilizado actualmente por una gran selección de organizaciones de todo el mundo, desde las pequeñas empresas y proveedores de servicios de Internet en los EE.UU. y el Gobierno Militar.

*Phising** = término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas

Algunas de sus características son las siguientes:

1	Distribuido bajo los términos de la Licencia Publica General GNU versión 2.
2	Revisa el correo electrónico en busca de virus utilizando cualquier combinación de entre más de una docena de distintos programas anti-virus
3	Automáticamente actualiza todo los anti-virus instalados cada hora
4	Puede eliminar el contenido gráfico de correo masivo no solicitado (Spam) de tipo pornográfico protegiendo a los usuarios de contenido obsceno.
5	Es altamente escalable. Un servidor puede procesar más de millón y medio de mensajes de correo por día.

Tabla 1.2: Características de MailScanner

1.7.- Sistema Operativo CentOS

CentOS (Community ENTERprise Operating System) (Red Hat, Inc, 2005), es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible

para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat. Existen otras distribuciones también derivadas de los fuentes de Red Hat. El escritorio de CentOS se muestra en la figura 1.7.

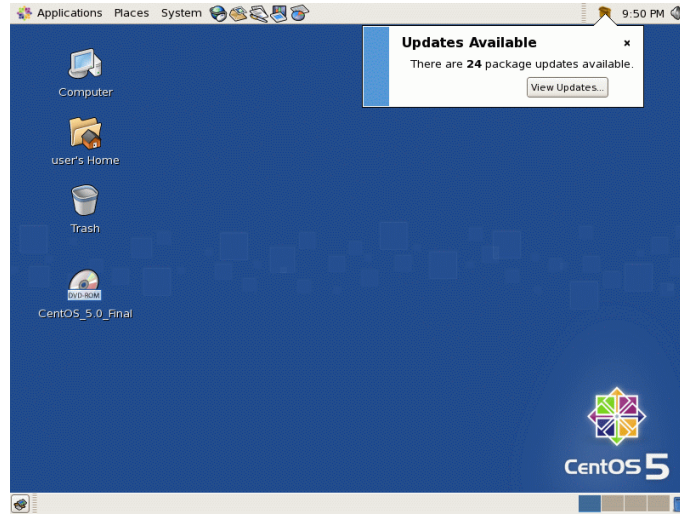


Figura 1.7: CentOS 5

1.7.1.- Características de CentOS

1	CentOS soporta (casi) todas las mismas arquitecturas que el original Red Hat Enterprise Linux.
2	Intel x86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/II/III, AMD Duron, Athlon/XP/MP).
3	Intel Itanium (64 bit).

4	Advanced Micro Devices AMD64(Athlon 64, etc) e Intel EM64T (64 bit).
5	PowerPC/32 (Apple Macintosh PowerMac corriendo sobre procesadores G3 o G4 PowerPC).
6	IBM Mainframe (eServer zSeries y S/390).

Tabla 1.3: Características de CentOS

Capítulo 2: Instalación y configuración de servicios de red virtualizados

2.1. Actividades con XenServer

El CIEco necesita virtualizar ciertos servidores que se encuentran en el área de telecomunicaciones, con la finalidad de que las máquinas virtuales creadas en dicho servidor tengan la capacidad de guardar información referente a varios sistemas informáticos y sitios web del CIEco.

Para continuar con el proceso de virtualización se hizo un análisis detallado sobre la herramienta de virtualización o el virtualizador con el que se debía contar para seguir este proceso, en capítulo 1 se muestra una lista de ellos, cabe destacar que algunos son gratuitos mientras que para otros se necesita comprar la licencia para poder utilizarlos.

Herramienta virtualización	Conocimiento del usuario	Ventajas	Desventajas	Costo	Indicado para
VMware	Solución más popular y extendida.	Solidez, estabilidad, seguridad, soporte del fabricante propietario.	Dificultad de puesta en marcha usuarios sin mucha noción, su código es propietario.	Variable en función del producto. Posee VMware Server como gratuito.	Desarrollo, investigación técnica, entorno de pruebas, consolidación de servidores.
Virtuozzo	No goza de mucha popularidad como el primero, pero es un producto muy en línea de VMware.	Seguridad, escalabilidad y disponibilidad interesantes.	Soporte difícil de encontrar. No es GPL, no admite drivers del entorno emulado.	Variable en función del producto. Posee Open Virtuozzo como gratuito.	Entornos con necesidad rápida de recuperación, consolidación de servidores.
QEMU	Bastante conocido sobre todo entre los usuarios de soluciones Linux	Código libre, ligero en ejecución. Fácil de desplegar y configurar.	Soporte escaso, velocidad de CPU muy baja en entornos emulados.	Gratuito, es GPL (General Public License).	Desarrollo, entorno de pruebas no profesional
Microsoft Virtual PC	Sigue siendo una de las soluciones más vendidas, por su popularidad en la comunidad de usuarios Microsoft.	Integración con plataformas Microsoft correcta, soporte y documentación abundantes.	Consumo excesivo de recursos, despliegue y ejecución lentos, virtualización dificultosa en algunos entornos derivados de UNIX	Su código es propietario, se comercializa bajo modelo de licencias.	Uso doméstico (Virtual PC), consolidación de servidores.

Xen	Cada vez más presente en las distribuciones	Potente y escalable. Muy seguro. Sistema de para virtualización innovador y efectivo.	Curva de aprendizaje costosa, documentación no excesivamente abundante, tiempos de despliegue mayores.	Gratuito, es GPL. (General Public License).	Entornos de prueba, consolidación de servidores, sistemas de recuperación rápidos.
Virtual Box	Está dándose a conocer muy rápidamente.	Comportamiento estable y sencillo, puede correr aplicaciones en Windows y linux.	La lentitud del sistema anfitrión es aceptable, falta de reconocimiento dispositivos USB.	Gratuito, es GPL. (General Public License).	Uso personal como empresarial.
Microsoft Virtual Server	Popularidad en la comunidad de usuarios Microsoft.	Familiar para usuarios Windows, Admiten drivers de los sistemas a emular.	Consumo excesivo de recursos, inestabilidad bajo ciertas condiciones de contorno, despliegue y ejecución lentos	Virtual Server GR2 es Gratuito	Consolidación de servidores y granjas de servidores.

Tabla 2.1: Comparativa entre virtualizadores

Una vez obtenida la información acerca de los virtualizadores, se decidió con cuál de estas herramientas se trabajaría para realizar la virtualización.

Se tomó la decisión de utilizar la herramienta XenServer ver tabla anterior, puesto que es la única plataforma de virtualización utilizada en muchas empresas y probada para *clouds* que brinda las características fundamentales de administración centralizada de servidores múltiples sin cargo (Montenegro, 2009).

Es importante mostrar el proceso de instalación y la configuración de XenServer en el servidor, ya que una de las finalidades de este proyecto es documentar de la mejor manera el desarrollo del mismo para posteriores usos.

Para iniciar la instalación de XenServer, es necesario checar las características del hardware, ya que sólo es compatible con aquellos servidores que posean la tecnología de virtualización por Hardware Intel VT-x y AMD-V (Citrix, 2011), una

vez *verificada* esta característica es necesario acceder al BIOS del servidor y habilitar la opción de virtualizar que se encuentra, si no es así XenServer no podrá servir como virtualizador.

Una vez que se ha verificado que se contiene dicha tecnología, se puede proseguir con la instalación de XenServer, este no necesita de un sistema operativo intermedio ya que está hecho para trabajar directamente sobre el hardware. Dicha instalación de XenServer se muestra en el *Anexo A*.

Una vez instalado el XenServer en el servidor, si éste se encuentra conectado a cualquier red de internet se recomienda utilizar direcciones IP dinámicas basadas en un servidor DHCP, para mantener a las máquinas virtuales con acceso a internet.

En los temas siguientes se describe cómo funciona la consola de administración para el servidor virtualizado, utilizando la herramienta XenCenter descrita en el capítulo anterior.

2.2. Administración del servidor con XenCenter

Esta consola como comúnmente se denomina, se instala como una aplicación cliente en una máquina remota al servidor (generalmente instalada en la red local para mejores resultados) y soporta diferentes SO, en este proyecto se montó en el sistema operativo Windows 7, cabe señalar que se instaló en este con la finalidad de tener una mayor facilidad de instalación y administración, ya que es uno de los SO más utilizados en máquinas personales.

Esta herramienta se descarga desde el sitio Citrix (Citrix, 2011), una vez descargado_ se prosigue a la instalación, para lo cual se ejecuta el instalador y es necesario seguir el asistente de instalación como se muestra en la figura siguiente:

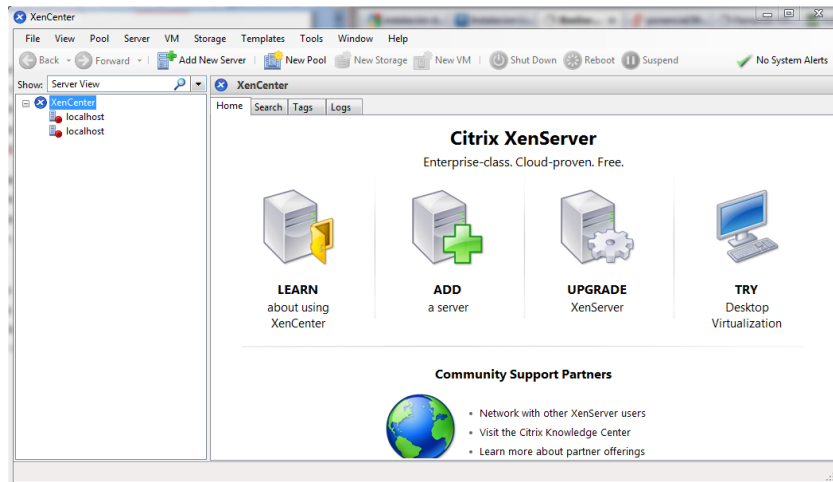


Figura 2.2: Ventana principal de XenCenter

Como se observa en la figura 2.2 se muestra la pantalla de inicio de XenCenter, es aquí en donde se agrega el un nuevo servidor por medio de su nombre (localhost) o dirección IP, una vez agregado el asistente pedirá el nombre de usuario y clave de acceso para su posterior administración, los cuales se definieron durante la instalación del XenServer, ver *Apéndice A* para más detalles. En la figura siguiente 2.3 se muestra la ventana de diálogo.

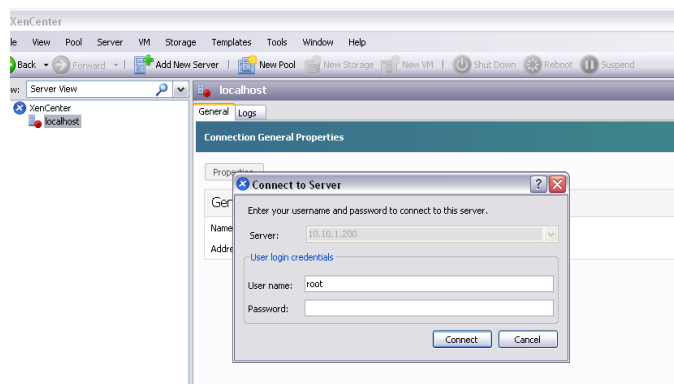


Figura 2.3: Configuración del servidor

Una vez establecida la conexión al servidor, se crearon las máquinas virtuales, dando click derecho sobre el nombre del servidor; a continuación se describe el proceso de creación de cada una:

- ⊕ Se eligió la nueva máquina virtual a crear; apareció una ventana donde se escoge que sistema operativo se quiere instalar, en este caso CentOS 5.5, en la lista no se encuentra pero se puede seleccionar la opción “others”, ahí se escoge y escribe la dirección de la cual va a tomar la imagen del sistema operativo,
- ⊕ Se definió el número de procesadores que se desean en la MV y el tamaño de memoria RAM requerida, se selecciona el tamaño en disco que va a ocupar la máquina virtual, en este caso de 120 Gb (esto se calculó por la capacidad en disco que tiene el servidor y el número de MV que se instalaron) ya que serán 3 máquinas virtuales las que se crearon en el servidor, después se selecciona la red y se finaliza el proceso.

Por cuestiones técnicas de instalación de herramienta de alta disponibilidad y pro requerimiento de la unidad de telecomunicaciones del Centro se decidió instalar CentOS 5.5 en las tres máquinas virtuales y eliminar el antiguo SO Fedora 13 que se tenía en otros servidores.

2.3. Alta disponibilidad en máquinas virtuales

Para lograr la alta disponibilidad se investigó y se analizó que la herramienta **Heartbeat** cumplía con las características deseadas (estable y licencia GPL), en los servidores antiguos se contaba con dos máquinas virtuales con la distribución de Fedora 13, sin embargo las versiones de Heartbeat estaban caducas, por lo tanto se decidió instalar la nueva versión en servidores CentOS de nueva generación.

La distribución CentOS 5.5, está enfocada a servidores y es de las más estables, además de que el software Heartbeat se encuentra ampliamente utilizado y

documentado para esta distribución. Además de que éste trae ciertos componentes que Heartbeat necesita para poder trabajar de manera correcta.

Como se ha mencionado en los capítulos anteriores el CIEco utiliza servidores Linux, de aquí la necesidad de buscar herramientas compatibles y estables basadas en licencia GPL de software libre.

Una vez analizado las herramientas de alta disponibilidad se tomó la decisión de utilizar Heartbeat, ya que ofrece disponibilidad a los servidores, además de mejorar su rendimiento y el bajo costo de implementación. Se tomó en consideración el punto de vista de los encargados del área de telecomunicaciones para tomar la decisión de utilizar ésta herramienta, ya que en proyectos pasados donde se utilizaban máquinas virtuales, probaron ésta herramienta y resultó que era fácil de instalar y utilizar. Además de que existe documentación en línea sobre su instalación y funcionamiento.

XenServer proporciona alta disponibilidad a las máquinas virtuales, sin embargo se debe contar con una licencia del mismo para poder utilizarla, por tal motivo se buscó como herramienta alternativa a Heartbeat y evaluar su desempeño.

La consola de XenCenter tiene la opción de realizar la alta disponibilidad entre las máquinas virtuales, al inicio se pensaba que esta opción se podría habilitar descargando o actualizando su nueva versión, pero después de una previa investigación se pudo observar que se necesita pagar una licencia para poder tener esta herramienta disponible en XenCenter, así que se descarto esta opción por completo (por los costos que esto representaría al centro).

En el *Anexo B* se muestra el avance detallado de instalación y configuración de **Heartbeat**, además de hacer una prueba para determinar si esta herramienta queda operativa.

Durante la pruebas de las herramientas para alta disponibilidad se pudo llegar a una solución de implementación utilizando Heartbeat. Estas consistieron en construir la alta disponibilidad entre dos máquinas virtuales instaladas en una computadora para primero decidir si este proceso era el correcto para implementarlo en este proyecto.

En la investigación sobre el software para alta disponibilidad, se han encontrados artículos que mencionan que la alta disponibilidad solo se puede aplicar a nivel hardware, sin embargo en este proyecto se tenía pensado llevarlos a cabo a nivel software, es por eso que se investigó y se hicieron pruebas para garantizar un funcionamiento adecuado, por el momento se tiene la ventaja haber hecho pruebas de alta disponibilidad en las dos máquinas virtuales instaladas en una PC y funcionó correctamente.

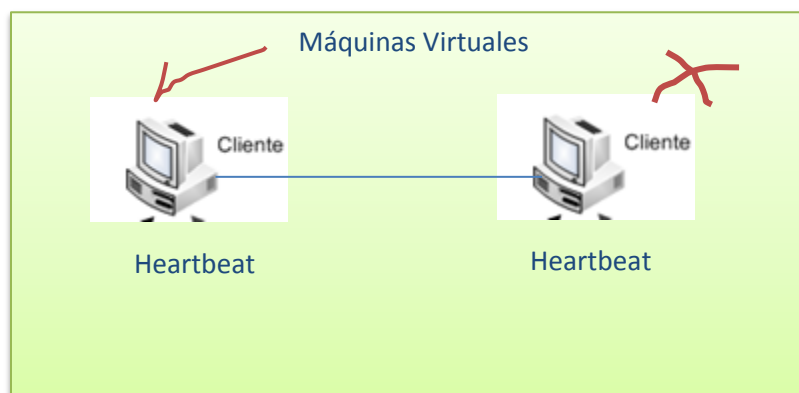


Figura 2.4: Heartbeat; cliente 1 activo

En la figura 2.4 se puede observar que ambos clientes tienen instalado el servicio de Heartbeat, solo uno de ellos se encuentra procesando información, sin embargo llegó un momento en que se desactivo el servicio de heartbeat en el primer nodo, entonces el segundo nodo activa su heartbeat para seguir con el proceso que el otro nodo hacía, ver figura 2.5.

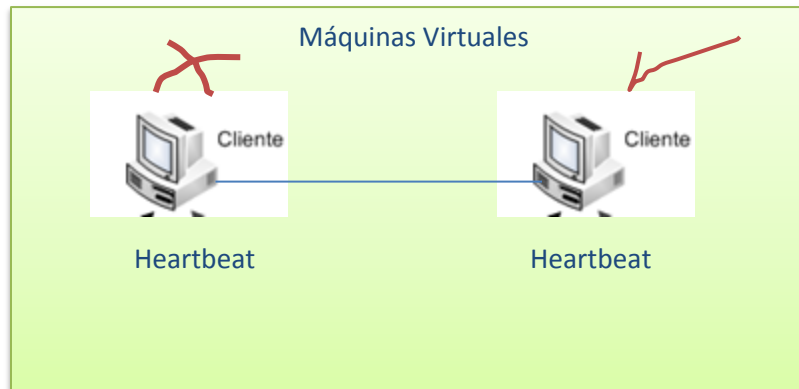


Figura 2.5: Heartbeat; cliente 2 activo

2.4. Aplicaciones de Seguridad

Una de los objetivos más importante en este proyecto, era buscar herramientas de seguridad dentro de las máquinas virtuales del servidor físico, con la finalidad de garantizar servicios estables y proteger la información que se almacena en éstas.

Para lograr esto, se creó una máquina virtual para instalar los servicios que desean ofrecer con la finalidad de tener una mejor facilidad de administración y redundancia de aplicaciones en los servidores virtualizados.

Cabe mencionar que estos servicios fueron instalados para que en un futuro cuando se requieran, se utilicen como servidores reales y cuya información contenida dentro de las máquinas virtuales serán datos reales del departamento de telecomunicaciones, el cual es el encargado de decidir si se utilizaran estas máquinas virtuales.

En el capítulo anteriore se describieron estas herramientas que ofrecen servicios vitales para el CIEco, se hizo una breve explicación de estas, mientras que en el apartado de Apéndices se muestran la instalación de cada una de ellas.

En los temas siguientes se describe la utilidad de estas herramientas y los servicios de red que ofrecen a través de la plataforma de virtualización.

2.5. Herramientas de gestión de información y servicios web (servidores web virtualizados).

Otro de los de los objetivos de virtualizar servidores en el CIEco es de instalar servicios de red dentro de las máquinas virtuales, servicios que son configurados en el SO CentOS 5.5, y que permiten gestionar información de diferente índole.

En el centro de investigaciones se utilizan varias herramientas que estan instaladas en sus servidores, estas ofrecen diferentes servicios de red que se muestran en la figura 2.6 siguiente:

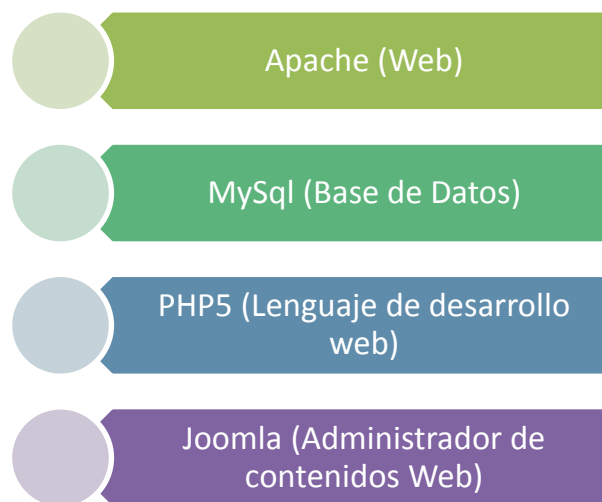


Figura 2.6: Herramientas para ofrecer servicios de red

2.5.1. Servidor Web

Un servidor web es un programa que sirve para atender y responder a las diferentes peticiones de los navegadores, proporcionando los recursos que soliciten usando el protocolo HTTP o el protocolo HTTPS.

Los servidores del CIEco se encuentran virtualizados con la herramienta XenServer, cuentan con máquinas virtuales que tienen instalado como servidor “web” a Apache. Éste se encuentra instalado en dos de las máquinas virtuales con

sistema operativo Linux, Apache se encuentra configurado de tal forma que siempre permanezca activo y estable.

El CIEco decidió trabajar con Apache ya que presenta ventajas favorables para el centro de investigación; Apache es uno de los servidores web más flexibles dentro de éste ámbito, es multi-plataforma, gratuito y proporciona ayuda y soporte.

2.5.2. Servidor Web Apache

Apache es el servidor web más común, su fácil configuración, robustez y estabilidad hacen que cada vez millones de servidores reiteren su confianza en este programa (Cibernetina, 2010).

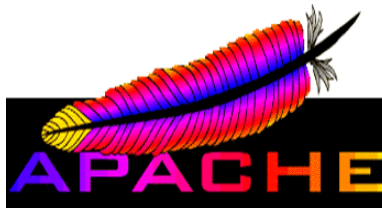


Figura 2.7: Apache

Apache es un servidor web de código abierto para S.O. Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras que implementan el protocolo HTTP/1.1, permite la construcción de sitios virtuales basados en un solo servidor.

Algunas de las ventajas son: modular, de código abierto, multi-plataforma, extensible, popular (fácil conseguir ayuda/soporte), entre otras.

Cabe mencionar, que apache es el servidor web número uno a nivel mundial (TechnoBlog; Blog de tecnología, 2010), el cual abarca cerca de un 52.26 % del

mercado total de Internet desbancando a servidores web como el IIS (Internet Information Server) de Microsoft.

Existe también una fundación dedicada a dar soporte legal y financiero al desarrollo de los proyectos relacionados con Apache (**Apache Software Foundation**), la cual actualmente está conformada por una comunidad de desarrolladores que día a día contribuyen a la expansión y mejora de proyectos.

2.5.3 MySql

Es un sistema de gestión de bases de datos relacional, fue creada por la empresa sueca MySQL AB (Cruz-Chávez, 2011) ahora adquirido por Oracle. MySQL es un software de código abierto, esto significa que es posible para cualquier persona usarlo y modificarlo.

Cualquier persona puede bajar el código fuente de MySQL y usarlo sin pagar. MySQL usa el GPL (GNU General Public License) para definir qué puede hacer y que no puede hacer con el software en diferentes situaciones.

MySQL es un sistema de administración relacional de bases de datos. Una base de datos relacional archiva datos en tablas separadas en vez de colocar todos los datos en un gran archivo. Esto permite velocidad y flexibilidad. Las tablas están conectadas por relaciones definidas que hacen posible combinar datos de diferentes tablas en demanda (Wikipedia, Inc, 2011). Su principal objetivo es velocidad y robustez.

- ⊕ Soporta gran cantidad de tipos de datos para las columnas.
- ⊕ Gran portabilidad entre sistemas, puede trabajar en distintas plataformas y sistemas operativos.
- ⊕ Cada base de datos cuenta con 3 archivos: Uno de estructura, uno de datos y uno de índice y soporta hasta 32 índices por tabla.

- ⊕ Aprovecha la potencia de sistemas multiproceso, gracias a su implementación multihilo.
- ⊕ Flexible sistema de contraseñas y gestión de usuarios, con un muy buen nivel de seguridad en los datos.
- ⊕ El servidor soporta mensajes de error en distintas lenguas

El CIEco por las características y ventajas que MySQL presenta se decidió utilizar ésta herramienta para la creación de las bases de datos que estarán en las máquinas virtuales.

Algunas ventajas se describen enseguida:

- ⊕ Velocidad al realizar las operaciones, lo que le hace uno de los gestores con mejor rendimiento.
- ⊕ Bajo costo en requerimientos para la elaboración de bases de datos, ya que debido a su bajo consumo puede ser ejecutado en una máquina con escasos recursos sin ningún problema.
- ⊕ Facilidad de configuración e instalación.
- ⊕ Soporta gran variedad de Sistemas Operativos
- ⊕ Baja probabilidad de corromper datos, incluso si los errores no se producen en el propio gestor, sino en el sistema en el que está.
- ⊕ Conectividad y seguridad

Algunas desventajas se muestran a continuación:

- ⊕ Un gran porcentaje de las utilidades de MySQL no están documentadas.
- ⊕ No es intuitivo, como otros programas.

2.5.4. PHP5

PHP (**Hypertext Preprocessor**) es un lenguaje script, para el desarrollo de páginas web dinámicas, cuyos fragmentos de código se intercalan fácilmente en

páginas HTML, debido a esto, y a que es de Open Source (código abierto), es el más popular y extendido en la web (Cruz-Chávez, 2011). Ver figura 2.8.



Figura 2.8: PHP 5

PHP es capaz de realizar determinadas acciones de una forma fácil y eficaz sin tener que generar programas programados en un lenguaje distinto al HTML. Esto se debe a que PHP ofrece un extenso conjunto de funciones para la explotación de bases de datos sin complicaciones.

La última versión es PHP5, que utiliza el motor Zend-2 y presenta mejoras significativas y un entorno de programación orientado a objetos mucho más completo, que permite que el PHP proporcione un alto rendimiento a las aplicaciones Web empresariales a nivel de las plataformas J2EE y .NET.

Una diferencia sensible es que PHP ha sido desarrollado inicialmente para entornos UNIX y es en este sistema operativo donde se aprovechan mejor sus prestaciones y consigue un mayor rendimiento.

2.5.5. Joomla!

Joomla! es un sistema de gestión de contenidos, y entre sus principales virtudes está la de permitir editar el contenido de un sitio web de manera sencilla. Es una aplicación de código abierto bajo una licencia GPL. Este administrador de contenidos puede trabajar en Internet o intranets y requiere de una base de datos MySQL, preferiblemente, de un servidor HTTP Apache. Ver figura 2.9.



Figura 2.9: Joomla!

En Joomla! se incluyen características como:

- ⊕ Mejorar el rendimiento web
- ⊕ Versiones imprimibles de páginas
- ⊕ Flash con noticias, blogs
- ⊕ Foros, polls (encuestas)
- ⊕ Calendarios, búsqueda en el sitio web e internacionalización del lenguaje.

Tiene varios módulos o plug-in que hacen de Joomla! un sistema modular y fácil de extender y que puede implementarse incluso para multisitios.

Enseguida se describe el procedimiento que se hizo para la creación de la máquina virtual y la instalación de las herramientas anteriores:

Para crear la máquina virtual se construye un *template* (plantilla) de una máquina virtual que facilita la gestión e instalación de máquinas en servidor XenServer.

Para el servicio Web del centro se utilizó el servidor Apache/CentOS 5.5, y además se instaló el servicio de base de datos MySQL/CentOS y como lenguaje de programación para las páginas se instaló el PHP5/CentOS.

La instalación se hizo desde la consola (*shell*) de la máquina virtual, la utilización del entorno gráfico en servidores no es recomendable ya que se gastan recursos valiosos para otros servicios (tiempo de procesador y memoria), la instalación generalmente se hace desde conexión remota utilizando el protocolo SSH/SSL (Joomla, 2011).

Para la instalación de los servicios en el servidor CentOS se utilizó el comando **yum** que obtiene de los repositorios (bibliotecas de código) los paquetes y los instala.

Los detalles de las instalaciones y configuraciones de estos servicios se encuentran en los apéndices siguientes:

- ❖ *Anexo I: Instalación del MySQL*
- ❖ *Anexo J: Instalación de PHP*

Siguiendo los pasos de los apéndices *I* y *J*, se procede a hacer una serie de pruebas de funcionamiento y con estas se asegura que los servicios instalados funciona correctamente. Después se procedió con la instalación del servicio de administración de contenido **Joomla** dentro de las máquinas virtuales, esta herramienta requiere de PHP5, MySQL y Apache server para funcionar adecuadamente, además de una serie de bibliotecas que es necesario configurar con anticipación, en el *Apéndice K se muestra con detalle la Instalación de este servicio; Joomla* (Joomla, 2011).

De esta manera se concluye con la instalación de los servicios que ofrece la red del CIEco mediante máquinas virtuales, y están listas para su uso posterior y ahora queda el único paso de migrar la información de los servidores en funcionamiento y con esto ofrecer redundancia.

Una de las actividades más importantes dentro de las máquinas virtuales, fue la implementación del “Sistema Curricula” del CIEco, el cual fue diseñado y programado en el área de telecomunicaciones, que mantiene una gran base de datos de toda la información de los académicos del CIEco. Proyecto que requiere de varios recursos y software extra, este sistema quedó funcionando en forma adecuada y parte vital de la información que el centro comparte.

2.6. Implementación de clientes ligeros (curso de XenServer de Citrix)

Dentro de las actividades que se desarrollaron en el Centro fue la de asistir a un curso de instalación y configuración de XenServer de Citrix (Citrix, 2011). La tarea principal fue instalar y configurar clientes ligeros en los laboratorios de cómputo mediante la virtualización de un servidor utilizando XenServer, el cual consistió en hacer que las PCs solo mostraran las aplicaciones contenidas en el servidor, para que los usuarios pudieran trabajar con éstos como si de una computadora normal se tratara; algunas de estas aplicaciones instaladas en el servidor fueron Microsoft Office y ArcGis.

Cabe destacar que el curso de Citrix fue impartido por personal capacitado y certificado del mismo, el cual tuvo una duración de 12 horas divididas en dos días en uno de los laboratorios de cómputo del CIEco.

Citrix XenServer es una plataforma completa de virtualización de servidores, basada en el potente *hipervisor* Xen. La tecnología Xen está reconocida ampliamente como el software de virtualización más rápido y más seguro de toda la industria (Citrix, 2011). XenServer está diseñado para una gestión eficiente

de servidores virtuales que utilizan los SO Windows® o Linux® o MacOSX y ofrece rentabilidad en la consolidación de servidores y en la continuidad de la actividad de la organización.

El proceso de instalación de XenServer se describe en el Apéndice A.

Al inicio del curso de Citrix se explicó acerca de las propuestas que esta compañía maneja, de las ventajas de implementarlas y cuáles son las mejores opciones acorde a las necesidades del CIEco. Estas opciones son herramientas que tienen diferente funcionamiento, pero que al final llegan a una misma utilidad se les llama “Virtualización de puestos de trabajo”, en la siguiente imagen se muestra un pequeño esquema de estas herramientas:



Figura 2.10: Virtualización del puesto de trabajo

Dentro de la demostración del curso de Citrix, se describió la virtualización del puesto del trabajo, esto quiere decir que hay diferentes herramientas que XenServer tiene para poder administrar o crear los clientes ligeros. Como se muestra en la figura 2.10, se tiene a XenDesktop, XenApp y XenClient, estos muestran las aplicaciones de diferentes maneras en los host o clientes, es importante señalar que éstas son máquinas virtuales que funcionan como servidor y proporcionan aplicaciones desde el servidor físico a los clientes.

En los temas siguientes se describen las herramientas de la virtualización del “puesto de trabajo” que ofrece XenServer.

2.6.1. XenDesktop

Citrix XenDesktop (Citrix, 2011), transforma los “puestos de trabajo” de aplicaciones Windows en servicios bajo demanda, a los que puede acceder cualquier usuario, con cualquier dispositivo, desde cualquier lugar, con una sencillez y una buena escalabilidad. Sean cuales sean los equipos utilizados por los usuarios; desde *tablets*, *smartphones*, portátiles, clientes ligeros, etc. XenDesktop es capaz de entregar “puestos de trabajo” y aplicaciones virtuales de manera rápida y segura.



Figura 2.11: XenDesktop 5

XenDesktop, ver figura 2.11, distribuye los puestos de trabajo en forma de servicio, es decir en lugar de instalar Sistemas Operativos además de cientos de aplicaciones en todas las computadoras de manera individual, estos se empaquetan como imágenes únicas en el centro de datos, después se enlazan de forma dinámica los escritorios para cada uno de los usuarios. Una imagen única significa que solamente se hacen parches y actualizaciones una vez. Se necesita mucho menos espacio de almacenamiento para manejar el mismo número de escritorios, y mayor centralizado de datos implica tener mayor control y seguridad de los datos.

Ofrece tres beneficios:

- 1.- Reduce el costo total de propiedad
- 2.- Aumenta la agilidad en el área de trabajo
- 3.- Mejora la seguridad de las redes

La entrega rápida y flexible de “puestos de trabajo” ayuda al departamento de TI a adaptarse con rapidez a los cambios de la organización y contempla el trabajo por turnos, la ampliación de sucursales, las fusiones y adquisiciones y otras iniciativas.

Citrix Receiver (Citrix, 2011), ver figura 2.12, es un cliente ligero universal, permite que cualquier PC, Mac, *Smartphone*, *tablets* o cliente ligero acceda a las aplicaciones y los puestos de trabajo corporativos, de manera fácil y segura.



Figura 2.12: Citrix Receiver

Es una herramienta que se instala en los clientes ligeros (computadoras o host) para poder tener comunicación con la máquina virtual que contiene las aplicaciones que serán suministradas a los diferentes usuarios o escritorios. En este caso ayudaría en la comunicación con XenDesktop.

2.6.2. XenApp

Citrix XenApp (Citrix, 2011), figura 2.13, es una solución para entregar aplicaciones bajo demanda que permite virtualizar, centralizar y administrar

cualquier aplicación en el centro de datos y distribuirla instantáneamente en forma de servicio a los usuarios en donde se encuentren y con cualquier dispositivo.



Figura 2.13: XenApp

Respecto a la tecnología tradicional de despliegue de aplicaciones, la distribución de aplicaciones virtuales con XenApp permite la gestión de sus aplicaciones mediante:

- La centralización de las aplicaciones en el centro de datos, a fin de reducir costes
- El control y el cifrado del acceso a los datos y a las aplicaciones, para mejorar la seguridad
- La entrega instantánea de las aplicaciones a los usuarios, estén donde estén

La entrega de aplicaciones virtuales permite que el departamento de TI administre una única instancia de cada aplicación del centro de datos. Las aplicaciones se distribuyen mediante *streaming* a los PC con Windows para ser utilizadas fuera de línea, o bien se ejecutan en los potentes servidores del centro de datos para que sean utilizadas en línea desde cualquier dispositivo o sistema operativo.

2.6.3. XenClient

La virtualización de puestos de trabajo está siendo adoptada rápidamente como la mejor manera de poner los “puestos de trabajo” de aplicaciones del SO a

Implementación de servidores virtualizados que mejoren la eficiencia del uso de energía y servicios de red en centros de investigaciones.

disposición de los usuarios de empresa. Con Citrix XenClient (Citrix, 2011), figura 2.14, las organizaciones pueden extender las ventajas de la virtualización de puestos de trabajo a los usuarios de ordenadores portátiles, alcanzando nuevos niveles de flexibilidad, seguridad y control.



Figura 2.14: XenClient

XenClient es un *hipervisor* que funciona en el lado del cliente y permite ejecutar los puestos de trabajo virtuales directamente en los dispositivos cliente. Al separar el sistema operativo del hardware subyacente, las imágenes de los puestos de trabajo se pueden crear, proteger, desplegar y trasladar de un equipo soportado a cualquier otro, reduciendo considerablemente la carga de mantenimiento del departamento de TI y simplificando la recuperación de los usuarios de portátiles en caso de desastre.

Las distintas funciones de Citrix XenApp permiten a los usuarios acceder a sus aplicaciones fácilmente y aumentar su productividad (Citrix, 2011).

El departamento de telecomunicaciones del CIEco había decidido implementar clientes ligeros en los laboratorios de cómputo para facilitar su administración y control, sin embargo el costo de las licencias de la herramientas de Citrix los orilló a tomar la decisión de dejar éste proyecto por un tiempo hasta analizar bien las ventajas y desventajas que trae consigo esta propuesta, sin embargo el laboratorio en este momento cuenta con los clientes ligeros y sus máquinas virtuales en su respectivo servidor físico, ver figura 2.15.

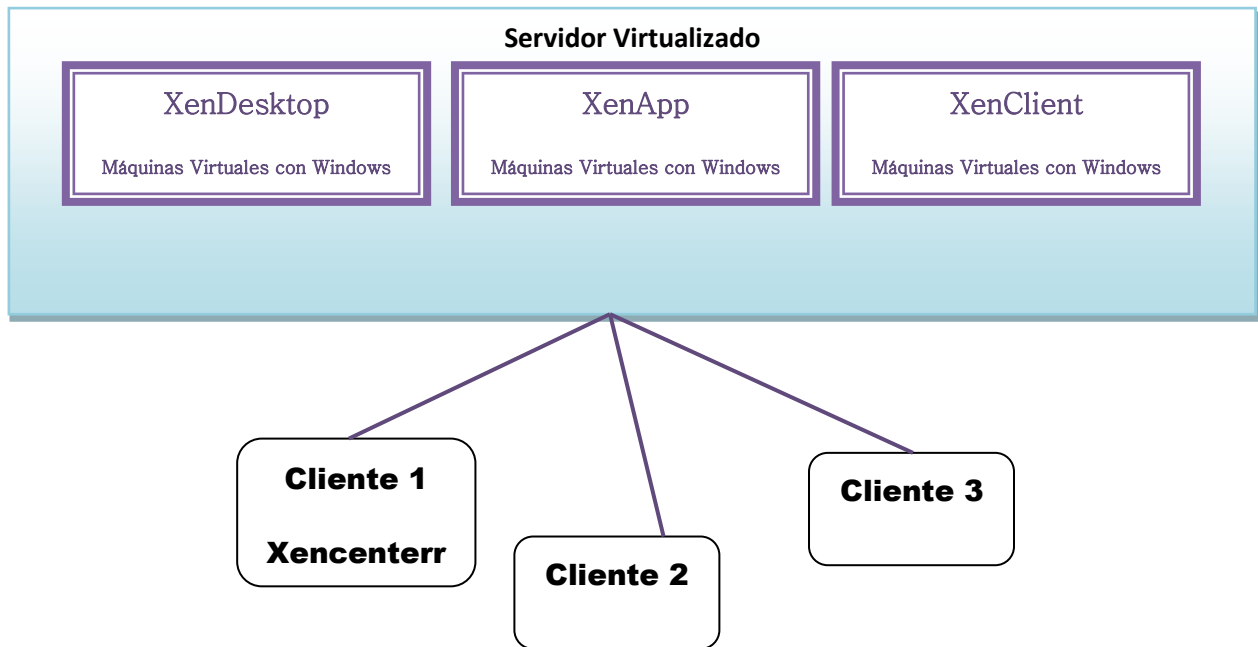


Figura 2.15: Servidor virtualizado con 3 clientes ligeros

A continuación se muestran los pasos realizados durante la creación de clientes ligeros, ver diagrama anterior:

1. El primer paso que realizó, fue instalar XenServer en el servidor físico con el que se ha estado trabajado desde el inicio del proyecto.
Este paso ya se había realizado con anterioridad y se encuentran en el *Apéndice A los detalles de instalación*.
2. Se creó una red VLAN que segmenta la red para asegurar el funcionamiento adecuado de los clientes ligeros y evitar saturación de la red.
3. Una vez instalado XenServer en el servidor, se instaló XenCenter en dos o tres máquinas virtuales para construir el laboratorio basado en las herramientas de XenServer.
4. Durante el primer día se hizo la instalación de todos los componentes que se ocuparon para la creación de los clientes ligeros tales como las máquinas virtuales necesarias para ello, ver figura 2.16 en donde se explica cada componente, además se muestra la configuración de la máquinas

virtuales en el servidor una vez instalados todos los componentes necesarios:

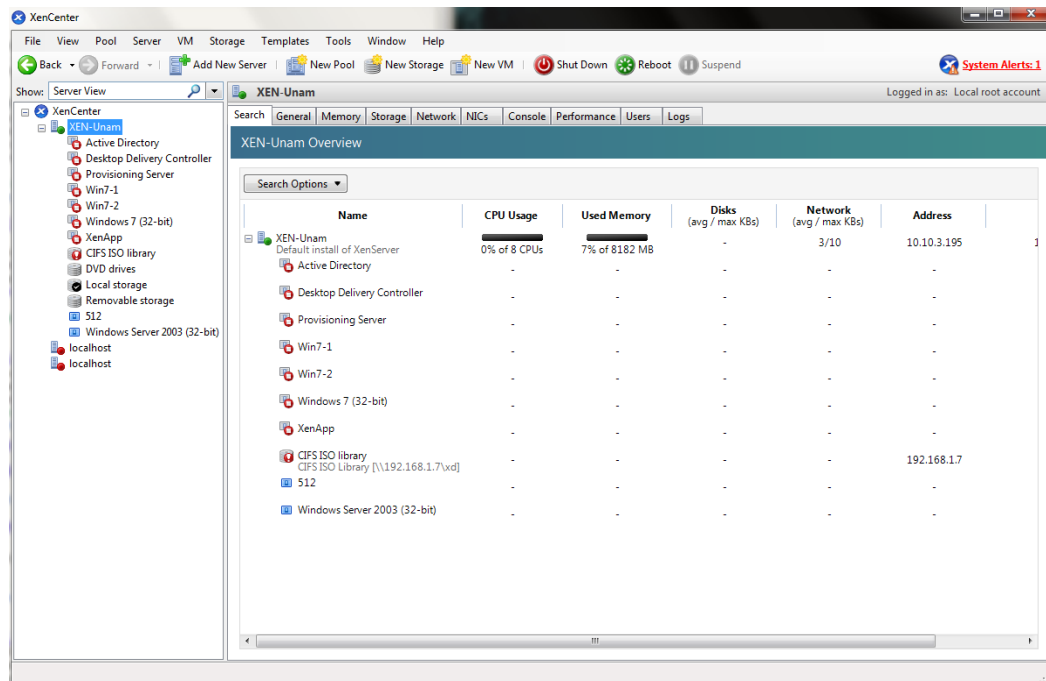


Figura 2.16: Servidor con componentes instalados

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores (Wikipedia, Inc, 2011). Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

Desktop Delivery Controller utiliza los servicios proporcionados por Active Directory. Requiere que todos los equipos de una comunidad sean miembros de un dominio, con relaciones de confianza mutua entre el dominio utilizado por Desktop Delivery Controller y los dominios utilizados por los escritorios virtuales (Citrix, 2011) .

Citrix Provisioning Services puede distribuir servidores o escritorios por la red, esto permitirá generar de una forma dinámica y acelerada escritorios virtuales. Junto con XenDesktop se puede gestionar escritorios virtuales y distribución de imágenes que se obtienen desde un escritorio virtual maestro (Hermida, 2011).

Win 7-1, Win 7-2, Windows 7(32 bits) son máquinas virtuales que tienen instalado el sistema operativo Windows 7.

XenApp, es una máquina virtual que tiene xenapp y que es una forma de distribución de clientes ligeros, el cual se describió en el capítulo anterior

Máquina virtual **Windows Server 2003** es un sistema operativo de la familia Windows de la marca Microsoft para servidores que salió al mercado en el año 2003. Está basada en tecnología NT y su versión del núcleo NT es la 5.2.

En términos generales, Windows Server 2003 se podría considerar como un Windows XP modificado para labores empresariales, no con menos funciones, sino que estas están deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor (Wikipedia, Inc, 2011).

5. Posteriormente se instalaron dos aplicaciones en el servidor, las cuales fueron distribuidas a los clientes ligeros mediante las diferentes maneras: XenDesktop, XenClient y XenApp. Es importante que para poder utilizar

estas herramientas ya se tengan instaladas previamente en las máquinas virtuales y también los componentes necesarios mencionados en el paso 4. Las aplicaciones sobre Win7 que se instalaron en el servidor para ser distribuidas fueron Arcgis (Sistema de Información Geográfica) y Microsoft Office 2010.

6. No obstante, para poder visualizar estas aplicaciones en los clientes, fue necesario instalar herramientas para clientes ligeros en las demás computadoras que se encontraban en la red Lan creada anteriormente con un DHCP que se había proporcionado al servidor. Cada máquina cliente tenía una manera distinta para demostrar las herramientas XenDesktop, XenClient y XenApp, ya que este era el objetivo del curso, demostrar las diferentes maneras de hacer clientes ligeros con XenServer.

Algunos clientes podían acceder a las aplicaciones del servidor desde un entorno Web con una IP, otras desde un entorno web pero con la aplicación de un cliente ligero, mientras que la otra forma era mostrar en el escritorio directamente en el cliente las aplicaciones que el administrador del servidor quería para el cliente ligero.

Con esto se concluyó el curso de Citrix, observando que es muy buena opción para los administradores de los centros de cómputo o laboratorios. Sin embargo es bastante caro comprar las licencias para configurar los laboratorios con clientes ligeros, por lo tanto el laboratorio donde se hizo el curso se encuentra con clientes ligeros desde ese día, el personal de Citrix dejó instalado todo el proceso para que los encargados del área de telecomunicaciones probaran esta solución y posteriormente decidieran si es viable para el CIEco.

Además se probó que los laboratorios del CIEco con o sin clientes ligeros son efectivos, con la diferencia de que se ahorra bastante tiempo en hacer las instalaciones en una máquina virtual y después aplicar el proceso de cliente ligero en todas las pc's, que hacer instalaciones y configuraciones de aplicaciones en cada computadora por individual.

El CIEco tiene las posibilidades de adquirir hardware y software de alta calidad, sin embargo da preferencia a proyectos que son sumamente importantes, por tal motivo, existen proyectos que necesitan de una inversión más alta que el que se está desarrollando.

Las licencias de Citrix son caras, así que los encargados del área de telecomunicaciones y soporte técnico decidieron dejar los demás laboratorios sin clientes ligeros y ver cómo funciona el proceso de virtualización de éstos en el laboratorio de computo 1.

2.7. Servidor Untangle

El servidor Untangle, figura 2.17, es una herramienta sencilla de controlar y muy útil para monitorear la red, además de que proporciona la tecnología necesaria para proteger la red contra las diferentes amenazas o ataques, virus entre otros. Por otro lado, protege controlando las páginas que son ilegales además de dar una vista de la actividad de la red (Cestero, 2009).



Figura 2.17: Untangle

El software de firewall de Untangle simplifica y consolida los productos de red y seguridad que las organizaciones necesitan en la puerta de enlace hacia Internet, protegiendo y filtrando de manera fácil y confiable la información.

La puerta de enlace (**Gateway**) de Untangle integra en un solo aparato todas sus funcionalidades (UTM) , lo que significa que no deberá aumentar la complejidad de su red mediante el uso de servidores dedicados para las distintas funciones. UTM (Unified Threat Management o de gestión unificada de amenazas) es un aplicativo todo en uno con funcionalidades para seguridad Web, seguridad email, *firewalls* entre otros (Buenas Tareas, 2011). El **Gateway** Untangle proporciona los siguientes servicios: Ver figura 2.18.

- ⊕ Antivirus
- ⊕ Antispam
- ⊕ Antispyware
- ⊕ Filtrado de contenidos web por temas o dirección
- ⊕ Firewall
- ⊕ Redes Privadas Virtuales (VPN)
- ⊕ Generación de Informes



Figura 2.18: Rack de Untangle; Características de Untangle !

Puede funcionar como Bridge o Router, su funcionamiento en modo de Proxy Transparente, significa que no se tendrá que configurar ningún ordenador ni modificar la red. Simplemente se debe ensamblar el Gateway Untangle a la conexión de Internet, y todas las configuraciones se harán a través de la interface Web.

Algunos beneficios que tiene el servidor Untangle son:

- ⊕ Evitar amenazas que provienen de Internet como virus o intentos de conexiones no autorizados, etc.
- ⊕ Aumentar la productividad de los usuarios evitando el uso de páginas web no autorizadas, por ejemplo redes sociales, juego online, compras, pornografía, etc.
- ⊕ Evitar el uso de programas de que consumen un ancho de banda mayor, como programas de intercambio de archivos, descargas de videos, etc.
- ⊕ Favorecer la movilidad de los usuarios permitiéndoles acceder de forma remota mediante Redes Privadas Virtuales a los recursos de su red.

Untangle es en realidad una recopilación de programas de seguridad unificados bajo una interfaz común UTM que nos permite configurar y manejar la suite de forma sencilla. Se puede instalar en un equipo que actúe como servidor independiente que únicamente ejecuta esta solución o utilizarlo como un programa en una computadora de escritorio con Windows XP.

En Untangle se categorizan las funciones en tres apartados, productividad, seguridad y acceso remoto:

- ⊕ Productividad: filtrado web que permite bloquear el acceso a ciertas páginas, bloqueo de SPAM y control de protocolos, para impedir el uso de aplicaciones tipo P2P o aquellas que hacen uso de determinados puertos que no se quiere dejar al descubierto.

- ⊕ Seguridad: bloqueo de virus, spyware y phishing. No elimina ningún virus, simplemente impide su entrada en la red local.
- ⊕ Acceso remoto: acceso mediante una red privada virtual, utilizando OpenVPN, que permite una conexión remota al escritorio de los equipos dentro de la red local y una alternativa de acceso vía web a servicios internos de la red.

2.7.1. Firewall (Cortafuegos)

Un *firewall* es un dispositivo que funciona como router entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial [referencia], Controla todas las comunicaciones que pasan de una red a la otra y en función de una serie de reglas (definidas por el usuario) permite o deniega su paso. Para permitir o denegar una comunicación, el firewall examina el tipo de servicio al que corresponde, como puede ser el web, el correo o el IRC (por sus siglas en inglés Internet *Relay Chat*) el cual es un protocolo de comunicación en tiempo real basado en texto (Alvarez, 2009). Dependiendo del servicio, el firewall decide si lo permite o no.

El objetivo de un firewall es prevenir ataques a las redes (sea Internet o la intranet de una empresa) empleando distintos medios.

Los firewalls tradicionales son de hardware, es decir, un dispositivo específico instalado en una red. Son los utilizados en entorno profesionales: el administrador de red define una serie de reglas para permitir el acceso y detiene los intentos de conexión no permitidos.

Los firewalls personales, figura 2.19, son programas que filtran el tráfico que entra y sale de una computadora. Una vez instalados, el usuario debe definir el nivel de

seguridad: permite o deniega el acceso de determinados programas a Internet (de forma temporal o definitiva) y autoriza o no los accesos desde el exterior.

Algunas ventajas pueden ser:

- ⊕ Protege intrusiones
- ⊕ Optimización de acceso
- ⊕ Protección de información privada
- ⊕ Protección contra virus

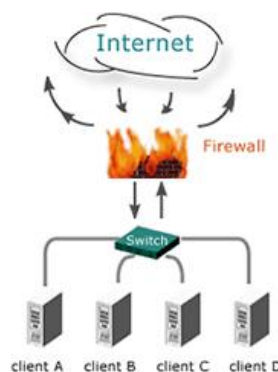


Figura 2.19: Firewall!

Se manejan por zonas (seguras o no) o bien por niveles de seguridad, los que establece el usuario según el grado de permisividad que le imponga al equipo.

2.7.2. Configuración del Servidor Firewall Untangle

El servidor Firewall de Untangle, es un servidor de seguridad multifunción. La interfaz administrativa tiene un panel de navegación, que contiene dos fichas: aplicaciones y configuración. Las aplicaciones se han descargado desde el almacenamiento de Untangle (por lo cual es importante tener activo el Internet), aparecerá en la ficha aplicaciones y se puede instalar en un rack virtual. La ficha de configuración contiene ajustes administrativos para el servidor Untangle.

Durante el proceso de instalación, se selecciona la partición en la que se instalará en el disco o discos duros, idioma, país, etc. El proceso de instalación es fácil y si la computadora donde se instala cuenta con suficiente memoria RAM y un procesador rápido la instalación se lleva poco tiempo.

El servidor Untangle requiere una PC dedicado instalado en la puerta de enlace a la red. El hardware no necesita un sistema operativo, el servidor Untangle instala su propio sistema operativo, además se necesitan ciertos requerimientos para que éste funcione. Los requisitos de Untangle se muestran en la tabla 2.2.

Recursos	Procesador	Memoria	Disco Duro	NIC	Notas
Mínimos 1-50 Usuarios	Intel/AMD (800+MHz)	512 MB	20 GB	2	
	Pentium 4 o equivalente AMD	1 Gb	80 GB	2 o más	
51-150 Usuarios	Dual Core	2 GB	80 GB	2 o más	
	2 o más Cores	2 GB	80 GB	2 o más	
151-500 Usuarios	4 Cores	4 GB	80 GB	2 o más	64-bit
501-1500 Usuarios		4 GB	80 GB	2 o más	64-bit
1501-5000 Usuarios	4 o más Cores	4GB	80 GB	2 o más	64-bit

Tabla 2.2: Requisitos de Untangle

Se instalan dos tarjetas de red (NIC) esto es para poder utilizarlo como enrutador y así utilizarlo como servidor DHCP que es uno de los servicios con los que cuenta el servidor. Durante el proceso de instalación se escribe un usuario y una contraseña para poder ingresar al sistema que es el administrador.

El sistema cuenta con una barra de administración en la cual se muestra las opciones de ingreso al explorador, resolución de la pantalla, herramientas, terminal, entre otras. Una vez que se ingresa a la pantalla principal ésta pide el usuario y la contraseña del administrador para ingresar al rack de administración de aplicaciones y configuraciones. Del lado izquierdo de la pantalla se muestra una barra donde se encuentran las aplicaciones que se utilizan para ser instaladas

y configurarlas. Existen muchas aplicaciones, la mayoría son gratuitas y otras son con costo. Sin embargo no se ocupan más que las herramientas gratuitas para configurar el firewall, ya que con ellas se logra un desempeño óptimo de la red en la que formara parte. Ver figura 2.10.

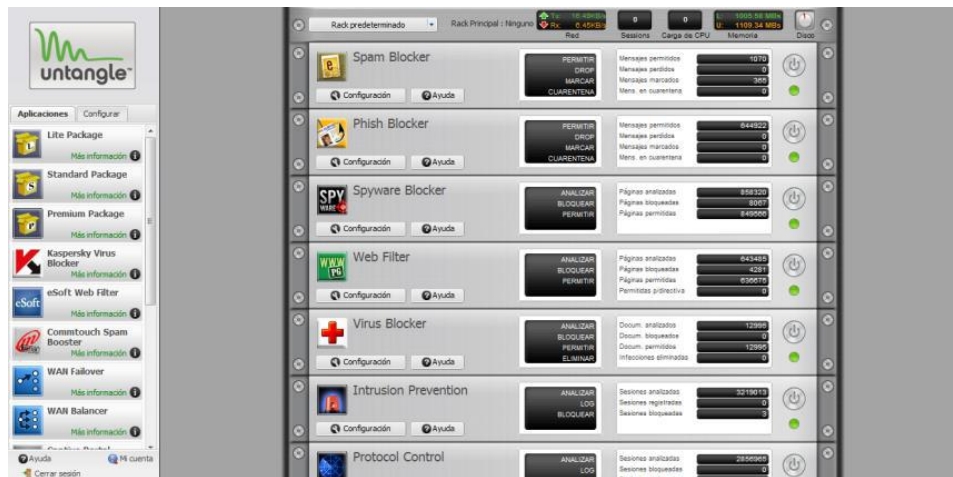


Figura 2.20: Rack de Untangle

Una vez que la instalación de Untangle ha finalizado, para poder acceder al sistema, se le tiene que dar una contraseña para iniciar con el explorador de las aplicaciones de untangle.

Algunas de las aplicaciones de esta versión de Untangle se enlistan en la tabla 2.3:

Spam Blocker	Contiene el análisis a SMTP, POP3 e IMPA con modo de resistencia a los mail y su tipo de medida a utilizar. Así como su Log de eventos
Phish Blocker	Analiza SMTP, POP3, IMPA, web y filtración de <i>phishing</i> , contiene su Log de eventos de mail y de web
Spyware Blocker	Bloqueará todas las URL de software espía, publicidad, cookies, instalaciones Active X no deseadas, así mismo creando su Log de eventos

Web Filter	Edita categorías de restricción y acceso a los usuarios dentro de la red, así mismo añade URL's a restringir. Extensiones de archivos.
Virus Blocker	Bloqueador de virus se basa en una fuente de virus de escáner abierto, Clam Antivirus
Intrusion Prevention	Detecta toda actividad no deseada en la red basándose en las firmas de las bases de datos de patrones de ataques conocidos
Protocol Control	Controla registros de todo lo que entra y sale de la red, y verificando los puertos que se utilizan para el acceso de las páginas web, mensajería instantánea, protocolos peer to peer
Firewall	Aplicación basada en reglas y protocolos de puertos., donde todas las sesiones entrantes están bloqueadas, excepto los expresamente autorizados con puerto. Para cada nueva conexión las normas se evalúan en orden hasta que la primera regla que coincida se encuentra. Las reglas pueden ser combinadas para algunas direcciones IP asignadas o pueden ser reglas de puertos permitidos de esta manera para crear políticas de firewall
Add Blocker	Servicio que permite bloquear la mayoría de contenido publicitario que se entrega en las páginas web. Se utiliza para descargar las suscripciones de filtro. La configuración se compone de una larga lista de sitios web y sus extensiones de sitios web que son conocidas por ser utilizadas con fines publicitarios
Reports	Generación de informes y los pone a disposición a través de correo electrónico, archivo CSV. Si bien el informe enviado por correo electrónico proporciona una cantidad significativa de información sobre el tráfico de red

Tabla 2.3: Aplicaciones de Untangle

La aplicación de firewall (cortafuegos) necesita que ciertos puertos estén abiertos para permitir el tráfico fino que circula por la red, de este modo se utilizarán los puertos TCP estándar, dichos puertos son 80,8080, 53, 20, 21, 110, 25, 443.

Mientras que los puertos por donde se pueden enviar mensajes a otros hosts son los UDP, sin tener una comunicación previa. Así pues para realizar la transmisión de canales especiales o rutas de datos se utilizara el puerto UDP 53 DNS.

Por otro lado los protocolos que se utilizan para la transferencia de archivos entre sistemas interconectados a una red cliente-servidor son los puertos FTP, de los cuales se usarán el puerto SFTP 1022, 22 y 21, que quedarán como protocolos libres en el firewall.

También se abrirá el puerto IMAP 143, ya que es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.

Por último se da una regla que se le nombra “Drop All”, que significa que bloqueará todos los puertos y reglas que no hayan sido añadidas en las excepciones de la configuración cuando se abrieron los puertos. Así que de esta manera este servidor firewall será el protector de la red del centro de investigación en ecosistemas (CIEco).

En la tabla 2.4 se muestran las reglas principales que se definieron en el firewall del CIEco, que normalmente para áreas administrativas son las que se implementan, sin embargo no se muestran las reglas como tal por simple seguridad de la red del centro de investigación:

Aplicación	Reglas
Spam Blocker	Analizar SMTP, POP3 e IMAP a nivel medio
Phish Blocker	Analizar SMTP, POP3 e IMAP con cuarentena a nivel medio
Spyware Blocker	Bloquear toda URL de software espía, publicidad y malware
Web Filter	Bloquear paginas no convenientes a actividades educativas
Virus Blocker	Analizar todo HTTP
Firewall	Bloquear puertos no habilitados

Tabla 2.4: Reglas para el firewall del cieco (ref)

En la figura 2.21 se muestra el firewall con sus reglas ya establecidas. De igual forma es necesario configurar las conexiones de red, para esto se debe acceder a esta opción en la pestaña “configurar” y en la primera ficha “configuración de red”:

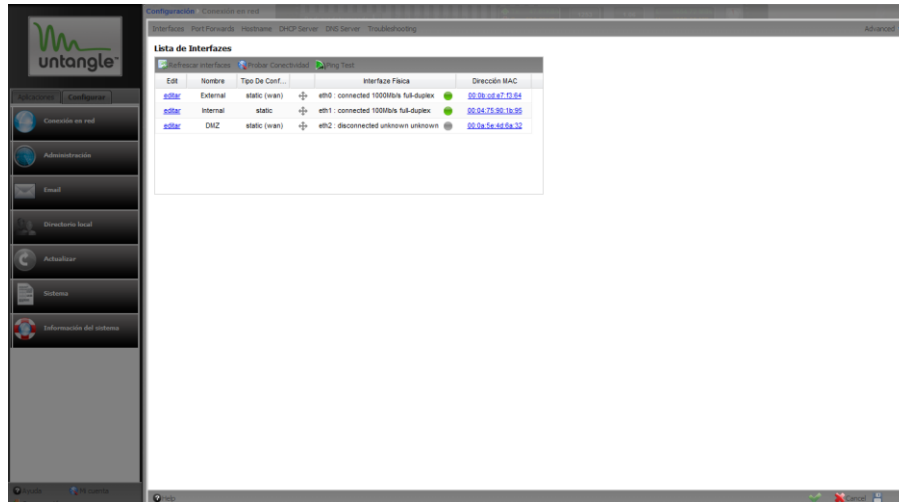


Figura 2.21: Firewall con sus reglas

En la tabla 2.6 se muestran los pasos para la configuración de la red dentro del servidor untangle:

Pasos	Descripción
1	La primera opción se configura las interfaces de las tarjetas de red, de las cuales físicamente se cuenta con 2 una de entrada (externa) y otra de salida (interna)
1.1	En la tarjeta externa se configura la IP pública que utilizamos para la conexión con el centro de telecomunicaciones principal y directamente al Paketeer, su configuración debe de ser una IP estática de la red X.X.X.X, con una máscara de red de 24 bits, en esta configuración es necesario determinar los DNS que son proporcionas por TELMEX para el campus ya que sin ellos no se lograría una conexión a internet

1.2	En la tarjeta interna se configura una IP estática determinando la red que vamos a administrar y proporcionar que será una red X.X.X.X, con una máscara de red de 24 bits
2	Hostname aquí se da el nombre de la máquina para que sea identificada a la red por su propio nombre sin tener que mostrar su IP. En este caso se llama Untangle.csa.unam.mx con un sufijo de nombre csam.unam.mx del servidor administrable
3	DHCP ésta, es una de las aplicaciones más importantes del servidor ya que tiene como misión la de proporcionar IP dinámicas a los usuarios conectados a la red X.X.X.X del CIEco. En esta opción de configuración se determina desde que IP se podrán conectar los usuarios y se puede tener IP reservadas, pues se cuentan con un “límite de alquiler” para las IP dinámicas y mientras estén reservadas no importara el límite de alquiler.
4	El servidor de DNS es proporcionado por el nombre del dominio de la red en este caso es: cieco.unam.mx

Tabla 2.6: Configuración de la red en untangle

Capítulo 3: Pruebas y Resultados de la Virtualización

3.1. Ahorro de Energía

Un estudio realizado acerca de la virtualización de servidores demuestra que ésta solución reducen los costos económicos y emisiones de CO₂, además de que propicia un ahorro de energía muy grande (eSemanal.mx, 2010).

Este ahorro se produce debido a que se pueden fusionar diez o más máquinas físicas en un único servidor, con lo que disminuye el consumo energético y los costos entre un 80 y un 90 por ciento. En este sentido, por cada servidor virtualizado, los usuarios pueden ahorrar en torno a 7.000 kilovatios hora (kWh), o cuatro toneladas de emisiones de CO₂ al año.

La virtualización también enfrenta retos que superar, pues si bien se consume menos energía, ésta será altamente variable. Existirán menos servidores, pero cada uno será más crítico que nunca. De tal forma, las aplicaciones pueden volver a asignarse en forma dinámica según se desee; sin embargo, la infraestructura de soporte no puede hacer lo mismo y pese a que la cobertura del centro de datos será más pequeña, la eficiencia total puede ser aún subóptima.

Chris Loeffler, administrador de aplicaciones globales, soluciones energéticas distribuidas en la compañía Eaton Corporation, señaló que la infraestructura energética y de enfriamiento, que pudo haber sido suficiente para las necesidades de pre-virtualización, podría volverse inadecuada cuando los patrones del rendimiento del centro de datos se alteren radicalmente (Solop, 2011).

Utilizando la virtualización se reduce el consumo de electricidad que si bien, puede ser modesto cuando se trata de un solo equipo, aumenta de manera proporcional cuando se habla de una gran cantidad de máquinas.

Son dos servidores que se virtualizaron durante el desarrollo de éste proyecto en el área de telecomunicaciones del CIEco, se observó que sí disminuye notablemente el consumo de energía dentro de ésta área. Ya que en un solo servidor se tienen tres máquinas virtuales que se encuentran en estado de prueba,

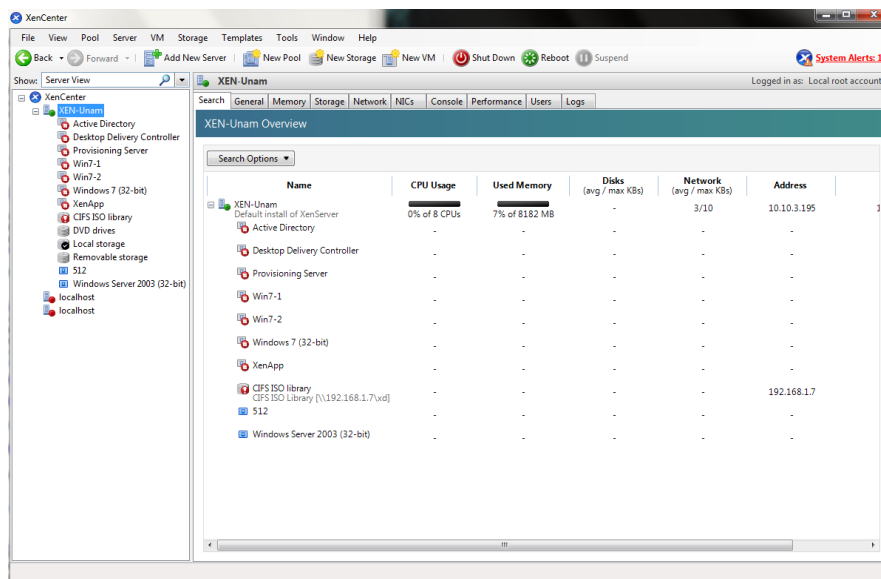
las tres se mantienen activas las 24 horas, debido a que sus sistemas así lo requieren.

Tal como se menciona anteriormente puede haber contras para éste proceso de virtualización, por el simple hecho de tener una cantidad de máquinas virtuales en un servidor físico, éste puede llegar a tener un rendimiento bajo a diferencia de si se tienen la misma cantidad de servidores físicos que funjan como cada una de las máquinas virtuales.

Sin embargo en éste proyecto se tomó en cuenta, el tamaño de cada máquina virtual para que no se sature y baje el rendimiento el servidor.

3.2. Uso de servicios virtualizados

La figura 3.1 se muestra todas las máquinas virtuales instaladas en el servidor:



Name	CPU Usage	Used Memory	Disks (avg / max KBs)	Network (avg / max KBs)	Address
XEN-Unam	0% of 8 CPUs	7% of 8192 MB	-	3/10	10.10.3.195
Active Directory	-	-	-	-	-
Desktop Delivery Controller	-	-	-	-	-
Provisioning Server	-	-	-	-	-
Win7-1	-	-	-	-	-
Win7-2	-	-	-	-	-
Windows 7 (32-bit)	-	-	-	-	-
XenApp	-	-	-	-	-
CIFS ISO library	-	-	-	-	-
CIFS ISO Library [\\192.168.1.7\vd]	-	-	-	-	192.168.1.7
512	-	-	-	-	-
Windows Server 2003 (32-bit)	-	-	-	-	-

Figura 3.1: Máquinas virtuales instaladas

En la figura 3.1 se puede observar que hay varias máquinas virtuales con diferentes nombres, en cada una de ellas se encuentra implementado lo que se hizo durante este proyecto.

1. En la primera y segunda máquina virtual se instaló la herramienta para alta disponibilidad *heartbeat*, figura 3.2. La idea principal de la alta disponibilidad se muestra en la siguiente figura, consistía en que si una máquina virtual fallaba, la otra se levantaría automáticamente para que las tareas y procesos no se detuvieran y se pudiera seguir trabajando con esta sin ningún problema, mientras se solucionaba el error de la máquina caída.

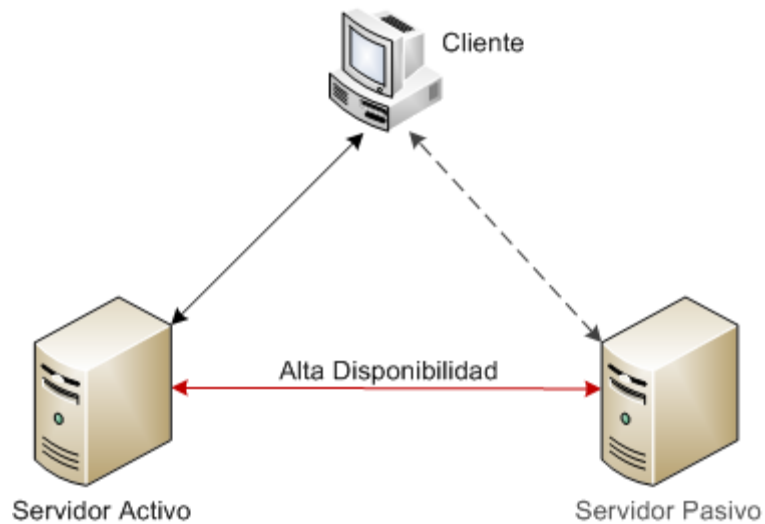


Figura 3.2: Alta disponibilidad

2. En la máquina virtual de la figura 3.3, se encuentran instaladas las herramientas para seguridad en Linux, como SpamAssassin, Mailwatch, MailScanner, Postfix y ClamAv, ya se describieron sus características y su instalación anteriormente.



Figura 3.3 Máquina virtual con herramientas de seguridad en linux

3. Posteriormente, en la máquina virtual de la figura 3.4 se encuentran los servidores de correo y servidores web además de Joomla, PHP5, MySQL, Apache, Xamp.



Figura 3.4: Máquina virtual con servidores

4. Finalmente en la figura 3.5 se tiene el servidor virtualizado para los clientes ligeros, en sus diferentes modalidades XenApp, XenDesktop y XenClient.

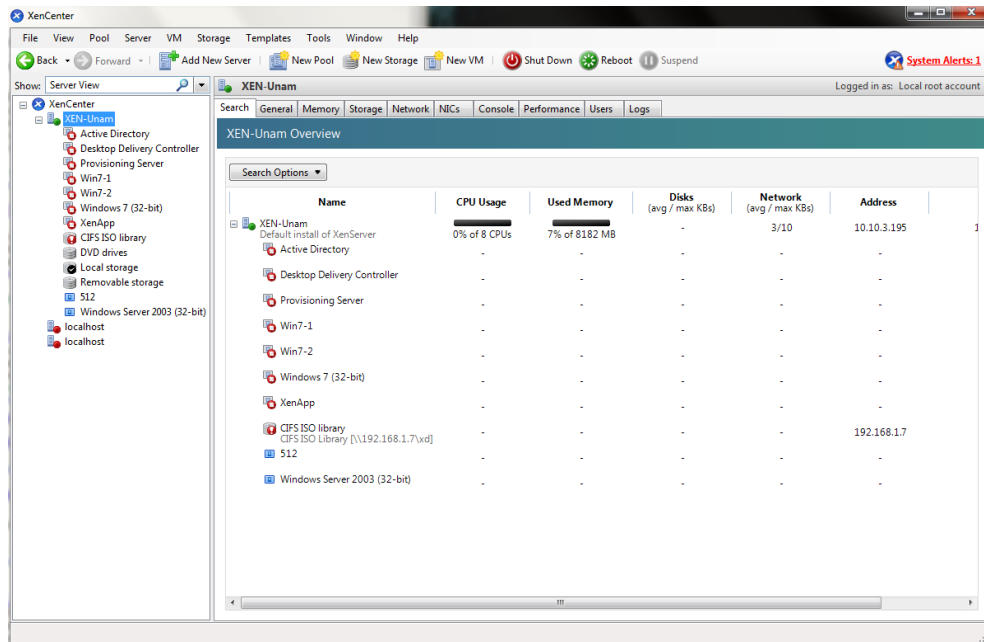


Figura 3.5: Servidor Virtualizado para los clientes ligeros

5. Para mejorar la red del CIEco y darle más seguridad, se instaló un servidor Untangle, el cual ayuda a la red a que sea más segura mediante la configuración de *Firewalls*, los cuales son reglas que deniegan el paso de información al menos que se permitan la abertura de ciertos puertos que permitan el paso de la misma.

3.3. Pruebas de rendimiento de los servicios virtualizados

Para el área de telecomunicaciones es muy importante saber el rendimiento de las máquinas virtuales que se encuentran dentro del servidor donde se estuvo

trabajando durante este proyecto, con la finalidad de analizar si fue viable haber virtualizado el servidor.

Se realizaron pruebas muy sencillas, en seguida se describen algunas de ellas:

- ⊕ Pings entre máquinas virtuales: Este con el simple hecho de poder analizar que existe conexión entre las máquinas virtuales del servidor. Se pudo observar que efectivamente mediante enviando un ICMP a las direcciones IP de las diferentes máquinas virtuales no se detectaron problemas de conectividad, además de que se obtuvo respuesta de ellas. Por otra parte el tiempo de respuesta fue aceptable para un servidor virtualizado.
- ⊕ Otra de las pruebas que se realizaron fue la de hacer una partición común para las máquinas virtuales, para poder hacer un intercambio de archivos entre estas. Como las máquinas virtuales tienen instalado el sistema operativo Linux, de esta forma es cómo se maneja el intercambio de archivos. Se hizo una transferencia de un archivo que pesaba 3gb, sin embargo el resultado fue bastante bueno, el tiempo de transferencia rebaso las expectativas que se tenían respecto a las máquinas virtuales. Sin embargo aún se siguen haciendo pruebas de este tipo para determinar que si es cosa de XenServer o de la distribución de Linux.
- ⊕ Descargas de Internet: el servidor físico se encuentra configurado con DHCP dinámico en el CIEco, así que las máquinas virtuales automáticamente obtienen una dirección ip válida para salida a internet. De esta manera se pueden descargar archivos de Internet desde cada máquina virtual, se pudo observar que algunas veces si hay un pequeño retraso en la descarga en comparación de una descarga normal de una PC que se encuentra conectada inalámbricamente a la red del CIEco, la tasa de transferencia es mayor que en la del servidor en este caso, sin embargo no varía mucho.

- ⊕ Acceso al servidor desde una red externa a la del CIEco: se realizó esta prueba ya que algunas veces por motivos de administración del servidor se debía acceder a él a horas que no fueran de trabajo en la UNAM, así que el servidor se configuró con una ip fija externa, de este modo se podría acceder a él aunque no estuviera el administrador en el CIEco, sin embargo manipular y administrar el servidor fue demasiado lento. Las máquinas virtuales no respondían de manera rápida y para hacer algo en ellas se llevaba el doble de tiempo que si estuviera trabajando en el CIEco.

Por el momento se están llevando estas pruebas constantemente para verificar el estado de cada máquina virtual. Posteriormente se implementaran más pruebas de rendimiento para seguir mejorando la evolución del proyecto.

Capítulo 4: Conclusiones y Recomendaciones

La decisión para determinar que herramienta de virtualización utilizar, se hizo después de una previa investigación acerca de éstas herramientas y se llegó a la conclusión de utilizar XenServer porque permite implementar y administrar de manera rápida y fácil equipos virtuales de alto rendimiento con Windows y Linux. Además puede gestionar su almacenamiento y los recursos de red desde una única consola de administración fácil de usar.

La instalación del XenServer se realizó en un periodo previo al inicio de este proyecto, sin embargo se volvió a realizar para comprobar que estaba funcionando correctamente el servidor.

Al inicio se tenían tres máquinas virtuales ya instaladas en el servidor, las cuales tenían la distribución de Fedora 13, sin embargo por problemas con esta distribución se optó por cambiar a una diferente como CentOS 5.5

Para implementar alta disponibilidad en las máquinas virtuales, se investigó sobre herramientas de éste tipo para poder realizar este proceso y finalmente se tomó la decisión de utilizar Heartbeat, ya que éste maneja un sistema “de latidos” para que los nodos verifiquen si el resto de nodos están en funcionamiento, además de ser una herramienta gratuita.

Trabajando con la herramienta Heartbeat se pudo observar que la configuración es algo difícil y requiere bastante tiempo, además de que se encontró cierta información que indica que la alta disponibilidad es a nivel hardware y no en software como se pretendía hacer.

Se realizó una prueba de alta disponibilidad con heartbeat en dos de las máquinas virtuales, la cual funcionó correctamente y se demostró que se puede realizar este proceso en las demás máquinas.

Se continuó con la instalación de aplicaciones de seguridad como el monitoreo de correos *antispam*, algunas de estas herramientas son Clamav, SpamAssassin, MailWatch, MailScanner, Postfix, con la finalidad de que el servicio de correo del

CIEco esté más controlado. Esto se realizó en una máquina virtual con sistema operativo Linux en la distribución CentOS 5.5.

Por otro lado se creó otra máquina virtual con la intención de mudar cierta información del centro de investigación a este servidor, por lo tanto se instalaron componentes como Xampp, Php, Mysql, Apache, para que esta máquina funcione como servidor web además de instalar un gestor de información llamado Joomla!. En esta máquina se encuentra el “Sistema de currícula” del CIEco.

Se aplicó la virtualización de un servidor con XenServer dentro de un laboratorio del centro de investigación, se crearon máquinas virtuales con herramientas tales como XenApp, XenDesktop y XenCliente, para mostrar las aplicaciones contenidas en las máquinas virtuales y hacer que las computadoras del laboratorio fungieran como clientes ligeros. Este laboratorio se encuentra funcionando correctamente con aplicaciones de Microsoft Office y ArcGis (ref).

Se llegó a la conclusión de posponer la adquisición de licencias de Citrix, ya que el CIEco por el momento no cuenta con el recurso económico necesario para estas.

Se implementó un servidor de seguridad con Untangle, el cual ayuda en la aplicación de *firewalls*, en donde se crearon ciertas reglas para filtrar el paso de información.

Un estudio realizado acerca de la virtualización de servidores demuestra que ésta solución reducen los costos económicos y emisiones de CO₂, además de que propicia un ahorro de energía muy grande (ref).

Utilizando la virtualización se reduce el consumo de electricidad que si bien, puede ser modesto cuando se trata de un solo equipo, aumenta de manera proporcional cuando se habla de una gran cantidad de máquinas.

Se hicieron algunas pruebas de rendimiento del servidor virtualizado para analizar la viabilidad de efectuar virtualización.

Referencias y Bibliografía

- Alegsa. (2009). *Definición de ICR*. Recuperado el 15 de Octubre de 2011, de Diccionario de Informática: <http://www.alegsa.com.ar/Dic/irc.php>
- Alvarez, M. A. (22 de Agosto de 2009). *Que es un firewall*. Recuperado el 25 de Mayo de 2011, de Que es cada tecnología: <http://www.desarrolloweb.com/articulos/513.php>
- Buenas Tareas. (2011). *Guía de Instalación de Untangle*. Recuperado el 10 de Mayo de 2011, de Tecnología: <http://www.buenastareas.com/ensayos/Guia-De-Instalacion-De-Untangle/894207.html>
- Cestero, J. M. (18 de Mayo de 2009). *Untangle, software para la protección perimetral de la red*. Recuperado el 23 de Mayo de 2011, de Software; Tecnología Pyme: <http://www.tecnologiapyme.com/software/untangle-software-para-la-proteccion-perimetral-de-la-red>
- Ciberaula. (2010). *Introducción, definición y evolución de php*. Recuperado el 10 de Mayo de 2011, de Artículos de interes: http://www.ciberaula.com/articulo/introduccion_php/
- Cibernetina. (2010). *Conceptos básicos del servidor web*. Recuperado el 25 de Abril de 2011, de Manuales: http://www.cibernetia.com/manuales/instalacion_servidor_web/1_conceptos_basicos.php
- Citrix. (2011). *Citrix; Products and Solutions*. Recuperado el 25 de Mayo de 2011, de Citrix: www.citrix.org
- Citrix. (2011). *Virtuallización claramente mejor con Citrix XenServer*. Recuperado el 15 de Mayo de 2011, de Citrix.
- Cruz-Chávez, M. A. (12 de Marzo de 2011). *MySQL*. Recuperado el 25 de Mayo de 2011, de Cursos en línea: <http://www.uaem.mx/posgrado/mcruz/cursos/miic/MySQL.pdf>
- Dueñas, J. B. (25 de Enero de 2011). *Cómo configurar un agrupamiento (cluster) de alta disponibilidad con Heartbeat en CentOS 5*. Recuperado el 20 de Mayo de 2011, de Alcance libre: <http://www.alcancelibre.org/staticpages/index.php/como-cluster-heartbeat-centos>
- eSemanal.mx. (22 de Diciembre de 2010). *Ahorro de energía con virtualización: Eaton*. Recuperado el 24 de Noviembre de 2011, de Noticias: <http://esemanal.mx/2010/12/ahorro-de-energia-con-virtualizacion-eaton/>
- Eugenio Villas, J. G. (2010). *Virtualización*. Recuperado el 3 de Marzo de 2011, de Virtualización de plataforma.

- Fundación Wikipedia, Inc. (27 de Marzo de 2011). *Alta Disponibilidad*. Recuperado el 1 de Abril de 2011, de Wikipedia: http://es.wikipedia.org/wiki/Alta_disponibilidad
- Hermida, H. H. (19 de Abril de 2011). *Instalación y configuración de Citrix Provisioning Services 5.6*. Recuperado el 12 de Octubre de 2011, de Provisioning Server: <http://www.bujarra.com/?cat=96>
- Herramientas Empresariales. (2011). *Beneficios empresariales de la virtualización SO*. Recuperado el 22 de Noviembre de 2011, de Herramientas empresariales: <http://herramientasempresariales.com.mx/2011/12/beneficios-empresariales-de-la-virtualizacion-so/>
- jmarrrior. (1 de Abril de 2008). *Desventajas de la virtualización*. Recuperado el 15 de Mayo de 2011, de Virtualizados: <http://www.virtualizados.com/10-desventajas-de-la-virtualizacion>
- Joomla. (2011). *Joomla!* Recuperado el 27 de Mayo de 2011, de Joomla!: <http://www.joomla.org>
- Linux para todos. (2009). *Servidor Web Apache en Centos*. Recuperado el 13 de Mayo de 2011, de Servidor web: <http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base%20de%20Conocimiento/Servidor+Web+Apache+en+CentOS>
- Linux para todos. (2010). *Instalación y Configuración de ClamAV en RedHat-CentOS*. Recuperado el 16 de Mayo de 2011, de Servidores de correo electrónico: <http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base+de+Conocimiento/Instalación+y+Configuración+de+ClamAV+en+RedHat-CentOS>
- Linux para todos. (2011). *Instalación y Configuración de MailScanner en RedHat-CentOS*. Recuperado el 16 de Mayo de 2011, de Servidor de correo electrónico: <http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base%20de%20Conocimiento/Instalación+y+Configuración+de+MailScanner+en+RedHat-CentOS>
- López, J. G. (24 de Octubre de 2011). *Alta Disponibilidad eb GNU/Linux*. Recuperado el 1 de Febrero de 2011, de Administración de Sistemas Operativos: http://www.adminso.es/wiki/images/3/31/Pfc_Fransico_cap4.pdf
- Montenegro, K. O. (29 de Junio de 2009). *ESTUDIO PARA EVALUAR LA CONFIABILIDAD Y CALIDAD DE SERVICIO EN APLICACIONES DE MISIÓN CRÍTICA, UTILIZANDO VIRTUALIZACIÓN*. Recuperado el 26 de Febrero de 2011
- Paredes, J. P. (24 de Mayo de 2010). *Alta Disponibilidad para Linux*. Recuperado el 1 de Febrero de 2011, de <http://mmc.geofisica.unam.mx/LuCAS/Presentaciones/200103hispalinux/paredes/pdf/LinuxHA.pdf>

Prosecure. (2010). *UTM*. Recuperado el 3 de Noviembre de 2011, de Seguridad en el Gateway para web :
<http://www.prosecure.netgear.es/pdf/datasheets/Analisis%20competitivo%20Prosecure%20UTM.pdf>

Red Hat, Inc. (2005). *Manual de Referencia, Red Hat* . Recuperado el 15 de Junio de 2011, de Red Hat Enterprise Linux 4: <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-httpd.html>

Scribd. (30 de Enero de 2011). *Hight Ability*. Recuperado el 23 de Febrero de 2011, de Scribd:
<http://es.scribd.com/deleted/36757812/58/Piranha>

Search Security. (Octubre de 2008). *What is firewall*. Recuperado el 21 de Mayo de 2011, de Firewall: <http://searchsecurity.techtarget.com/definition/firewall>

Solop, N. (2011). *La virtualizacion propicia un ahorro energetico que favorece al medio ambiente*. Recuperado el 20 de Noviembre de 2011, de Wetcom group:
<http://www.wetcom.com.ar/content/la-virtualizacion-propicia-un-ahorro-energetico-que-favorece-al-medio-ambiente/>

TechnoBlog; Blog de tecnología. (2010). *Como instalar Apache+Mysql+PHP en Centos 5.4*. Recuperado el 15 de Mayo de 2011, de Como instalar Apache+Mysql+PHP en Centos 5.4:
<http://www.technoblog.com.ar/index.php/2010/02/como-instalar-apachemysqlphp-en-ubuntu-5-4/>

Unam. (2011). *CSAM, Unam campus Morelia*. Recuperado el 29 de Enero de 2011, de Unam:
www.csam.unam.mx

Venema, W. (14 de Julio de 2008). *Postfix*. Recuperado el 14 de Octubre de 2011, de Postfix:
<http://doc.ubuntu-es.org/Postfix>

VozToVoice. (13 de Marzo de 2009). *Instalar y configurar un servidor SMTP/POP3/IMAP en CentOS con acceso TSL/SSL y SASL*. Recuperado el 20 de Mayo de 2011, de Talking around the world: <http://voztovoice.org/?q=node/219>

Wikipedia, Inc. (2011). *Active Directory*. Recuperado el 18 de Septiembre de 2011, de Wikipedia, Inc: http://es.wikipedia.org/wiki/Active_Directory

Wikipedia, Inc. (3 de Noviembre de 2011). *Caracteristicas Adicionales MySql*. Recuperado el 15 de Noviembre de 2011, de MySql:
http://es.wikipedia.org/wiki/MySQL#Caracter.C3.ADsticas_adicionales

Wikipedia, Inc. (12 de Septiembre de 2011). *Windows Server 2003*. Recuperado el 14 de Octubre de 2011, de Windows Server 2003: http://es.wikipedia.org/wiki/Windows_Server_2003

Anexos

Anexo A : *Instalación y configuración de XenServer*

Una vez que arranca el instalador del XenServer seleccionar el idioma del teclado, en este caso es, español y presionar el botón ok para continuar la instalación de XenServer.

La siguiente pantalla pide la confirmación para instalar el XenServer y advierte que instalarlo borrará todos los datos de los discos seleccionados salvo que se trate de una actualización.

Después aceptar el *EULA (End User License Agreement)*, que nos indica que el producto es software de un único usuario.

Lo siguiente será seleccionar el origen de la instalación: Local media (CD-ROM), HTTP, FTP o MFS, elegir la opción de cd-rom que es la más común, ya que se quemó la imagen en disco. También preguntará si se quiere instalar el paquete de XenServer de un segundo CD.

Ya que se instaló, teclear la contraseña de *root* el usuario principal o súper usuario.

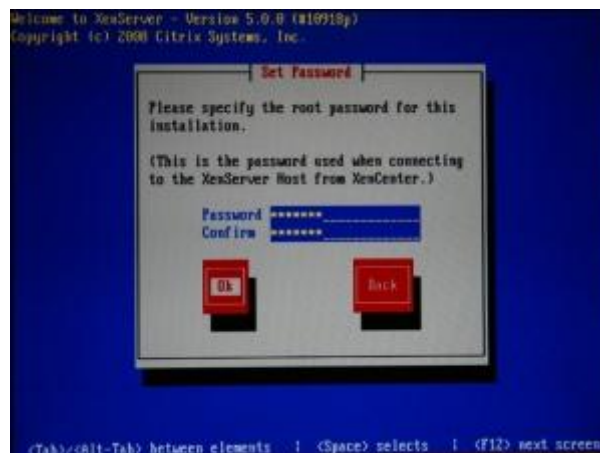


Figura A1: Contraseña root.

A continuación se deberá configurar la red y elegir entre usar DHCP o una IP estática. Para un servidor, lo normal es asignarle una IP estática, sin embargo en este caso se va a elegir DHCP.

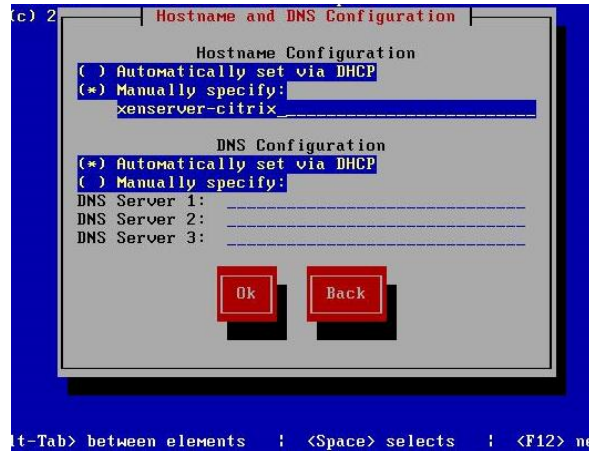


Figura A2: Selección de DHCP

Después asignar un nombre al equipo y a los servidores DNS (sistema de nombres de dominio).



Figura A3: Nombre del servidor

Seleccionar el área geográfica donde está el XenServer, en éste caso América y Ciudad de México.

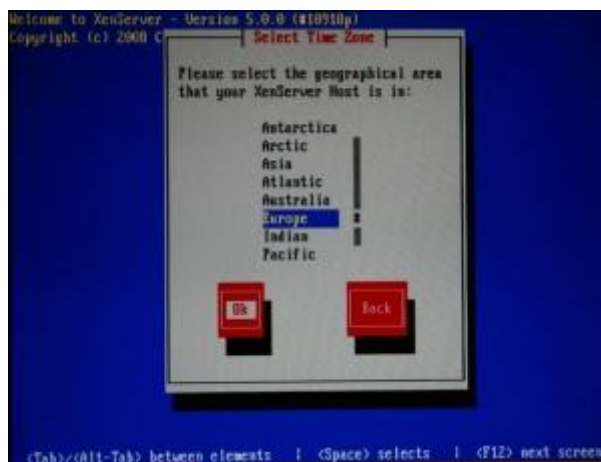


Figura A4: Localización de XenServer

También se debe indicar cómo se determinará la hora: automáticamente (usando NTP) o de forma manual.

Una vez que el Citrix XenServer ha terminado de recoger toda esta información, ya se puede instalar XenServer. Aunque el asistente da un último aviso de que perderemos todos los datos del disco duro donde se instalará, por eso es conveniente que donde se vaya a instalar este vacío.



Figura A5: Se instala XenServer

Una vez que se termina la instalación base del XenServer, éste pide que se inserte un disco extra, este disco es un paquete complementario para XenServer que contiene herramientas para la virtualización y transporte de maquinas virtuales.

El instalador detecta que el CD que se ha introducido es el pack de Linux..

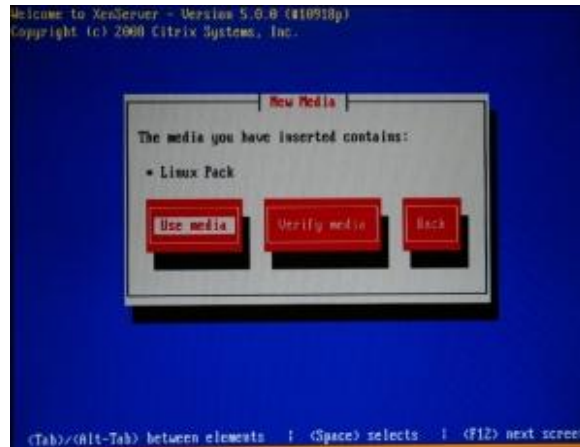


Figura A6: Instalación del segundo CD

Establacer la fecha y la hora, esto aparece durante la instalación del segundo CD.

Después aparecerá una pantalla que dice que se a completado la instalación, solo se debe retirar el CD y reiniciar para completar la instalación.

Ya reiniciado aparece la pantalla de configuración donde ésta da toda la información del servidor.



Figura A7: Figura 27. XenServer

Anexo B : Instalación y configuración de Heartbeat

Se asume que se dispone de dos equipos o máquinas virtuales, las cuales serán los dos nodos del agrupamiento, y tienen las siguientes características:

Nodo1:

Sistema operativo: CentOS 5.4.

Dirección IP eth0: 192.168.1.101/255.255.255.0, conectado a la LAN o hacia Internet, y con el nombre de anfitrión asociado a nombre.publico.nodo2.com.

Dirección IP eth1: 192.168.2.1/255.255.255.248, conectado con cable cruzado o a un switch o concentrador dedicado exclusivamente para los nodos del agrupamiento, o bien interfaz de Intranet en VirtualBox, y con el nombre de anfitrión asociado a nombre.privado.nodo1.com.

El nombre del anfitrión (hostname), definido en el fichero /etc/sysconfig/network, debe ser nombre.privado.nodo1.com.

Nodo 2:

Sistema operativo: CentOS 5.4

Dirección IP eth0: 192.168.1.102/255.255.255.0, conectado a la LAN o hacia Internet, y con el nombre de anfitrión asociado a nombre.publico.nodo2.com.

Dirección IP eth1: 192.168.2.2/255.255.255.248, conectado con cable cruzado o bien hacia un switch o concentrador dedicado exclusivamente para la comunicación entre los nodos del agrupamiento, o bien interfaz de Intranet en VirtualBox, y con el nombre de anfitrión asociado a nombre.privado.nodo2.com.

El nombre del anfitrión (hostname), definido en el fichero /etc/sysconfig/network, debe ser nombre.privado.nodo2.com.

Ambos nodos pueden ser diferentes en cuanto a arquitectura, capacidad y componentes.

Ambos nodos formarán un agrupamiento (*cluster*) de alta disponibilidad que responderá por la dirección IP 192.168.1.100/255.255.255.0, asociada al nombre nombre.publico.cluster.com.

Servicios que deben desactivarse

En ambos nodos, si estuvieran presentes, deben estar desactivados los servicios **avahi-daemon** y **avahi-dnsmconfd**, así como cualquier otro servicio que intente utilizar la interfaz eth1, misma que debe estar completamente dedicada a las comunicaciones de Heartbeat.

```
service avahi-daemon stop
service avahi-dnsmconfd stop
chkconfig avahi-daemon off
chkconfig avahi-dnsmconfd off
```

Es importante también desactivar el cortafuegos (*firewall*) predeterminado del sistema en ambos nodos, debido a que éste interfiere con la comunicación entre los nodos de heartbeat:

```
service iptables stop
service ip6tables stop
chkconfig iptables off
chkconfig ip6tables off
```

El muro cortafuegos de ambos nodos puede ser fácilmente gestionado a través de *Shorewall*, como se explica más adelante.

SELinux y Heartbeat

Lamentablemente, de modo predeterminado la implementación de SELinux incluida en CentOS 5.x carece de políticas que permitan funcionar al servicio heartbeat, a menos que se generen manualmente las necesarias o bien se ponga SELinux en modo permisivo o se desactive por completo éste.

Configuración del sistema con SELinux activo.

Particularmente se recomienda crear las políticas necesarias para SELinux. Es relativamente simple. El siguiente procedimiento deberá realizarse en ambos nodos.

Lo primero es cambiarse al directorio `/usr/share/selinux/packages`.

```
cd /usr/share/selinux/packages
```

Se crea un subdirectorio que será denominado heartbeat:

```
mkdir heartbeat
```

Se cambia a este nuevo subdirectorio:

```
cd heartbeat
```

Suponiendo que se van a configurar los servicios *shorewall* (o bien *iptables*), **httpd**, **named** y **vsftpd**, descargue el fichero `heartbeat1.te` desde Alcançe Libre:

```
wget -N
http://www.alcancelibre.org/linux/secrets/heartbeat1.te
```

El edite el fichero `heartbeat1.te` que se acaba de descargar:

```
vim heartbeat1.te
```

Y verifique que tenga el siguiente contenido:

```
module heartbeat1 1.0;

require {
    type proc_t;
    type urandom_device_t;
    type ftpd_t;
    type httpd_t;
    type iptables_t;
    type ndc_t;
    type initrc_t;
    type named_t;
    class unix_stream_socket { read write };
    class file read;
    class chr_file read;
}

#===== ftpd_t =====
allow ftpd_t initrc_t:unix_stream_socket { read write };

#===== httpd_t =====
allow httpd_t initrc_t:unix_stream_socket { read write };

#===== iptables_t =====
allow iptables_t initrc_t:unix_stream_socket { read write };

#===== named_t =====
allow named_t initrc_t:unix_stream_socket { read write };

#===== ndc_t =====
allow ndc_t initrc_t:unix_stream_socket { read write };
allow ndc_t proc_t:file read;
allow ndc_t urandom_device_t:chr_file read;
```

Lo anterior, que fue obtenido de la salida del comando **dmesg|grep audit|audit2allow -m heartbeat1>heartbeat1.te** en un sistema donde SELinux impedía a Heartbeat iniciar los servicios anteriormente mencionados. En realidad, define que se permite el modo de lectura y escritura cuando los servicios del directorio `/etc/init.d` sean iniciados por un zócalo generado por Heartbeat.

A continuación, se genera un fichero de módulo para SELinux (`heartbeat1.mod`) utilizando el mandato **checkmodule** de la siguiente forma:

```
checkmodule -M -m -o heartbeat1.mod heartbeat1.te
```

Luego, se procede a empaquetar el fichero `heartbeat1.mod` como el fichero `heartbeat1.pp`:

```
semodule_package -o heartbeat1.pp -m heartbeat1.mod
```

Finalmente se vincula el fichero `heartbeat1.pp` obtenido con las políticas actuales de SELinux y se cargan éstas en el núcleo en ejecución:

```
semodule -i  
/usr/share/selinux/packages/heartbeat/heartbeat1.pp
```

Una vez cargadas las nuevas políticas, se pueden eliminar los ficheros `heartbeat1.te` y `heartbeat1.mod`, pues solo será necesario que exista el fichero binario `heartbeat1.pp`.

Todo lo anterior se puede repetir utilizando otro nombre de fichero distinto para poder añadir más servicios. Es decir, si se van a añadir más servicios para ser gestionados por Heartbeat, configurar éstos en el fichero `/etc/ha.d/haresources`, como se describe más adelante en este mismo documento, reiniciar el servicio y realizar el siguiente procedimiento:

```
cd /usr/share/selinux/packages/heartbeat/  
dmesg|grep audit|audit2allow -m heartbeat2>heartbeat2.te  
checkmodule -M -m -o heartbeat2.mod heartbeat2.te  
semodule_package -o heartbeat2.pp -m heartbeat2.mod  
semodule -i  
/usr/share/selinux/packages/heartbeat/heartbeat2.pp  
rm -f heartbeat2.te heartbeat2.mod
```

```
service heartbeat restart
```

Configuración del sistema con SELinux en modo permisivo.

Si se desea, puede ponerse SELinux en modo permisivo en ambos nodos con el fin de evitarse tener que realizar los procedimientos anteriores. Edite el fichero `/etc/sysconfig/selinux`:

```
vim /etc/sysconfig/selinux
```

Cambie `SELINUX=enforcing` por `SELINUX=permissive`, a fin de mantener funcionando SELinux, y preservar todos los contextos de éste en el sistema de ficheros, pero sin interferir con el funcionamiento de Heartbeat:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of
enforcing.
#     disabled - SELinux is fully disabled.
SELINUX=permissive
# SELINUXTYPE= type of policy in use. Possible values are:
#     targeted - Only targeted network daemons are
protected.
#     strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

Reinicie el sistema en ambos nodos.

```
reboot
```

Realmente es poco recomendable desactivar por completo SELinux, siendo que las políticas necesarias pudieran aparecer en alguna actualización del paquete **selinux-policy-targeted**, o bien pudiera ser necesario recurrir a la protección que brinda esta implementación en un futuro a fin de evitar potenciales incidentes de seguridad que normalmente se evitarían utilizando SELinux.

En versiones recientes de Fedora, es posible evitar los problemas con SELinux, de manera fácil, ejecutando lo siguiente para permitir a heartbeat trabajar en modo sin confinar:

```
semanage fcontext -a -t unconfined_exec_semanaget
/usr/lib/heartbeat/heartbeat
```

El contexto **unconfined_exec_semanaget** es inexistente en CentOS 5 y Red Hat Enterprise Linux 5.

Configuración del Nodo 1

Ingresar como *root* o bien cambiar al usuario *root*.

```
su -l
```

Editar el fichero `/etc/hosts`:

```
vim /etc/hosts
```

Y definir los nombres asociados a la dirección IP pública del agrupamiento (cluster) y las direcciones IP de las interfaces eth0, las cuales corresponden a las interfaces públicas de los nodos:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1    localhost.localdomain localhost
::1        localhost6.localdomain6 localhost6
192.168.1.100 nombre.publico.cluster.com
192.168.1.101 nombre.publico.nodo1.com
192.168.1.102 nombre.publico.nodo2.com
```

Para complementar lo anterior, debe haber un DNS que se encargue de resolver estos nombres para la red local y/o hacia Internet.

Editar el fichero `/etc/hosts` y definir los nombres asociados a las direcciones IP de las interfaces eth1, las cuales corresponden a las interfaces privadas del cluster, a través de la cual se comunican los nodos:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1    localhost.localdomain localhost
::1        localhost6.localdomain6 localhost6
192.168.1.100 nombre.publico.cluster.com
192.168.1.101 nombre.publico.nodo1.com
192.168.1.102 nombre.publico.nodo2.com
192.168.2.1    nombre.privado.nodo1.com
192.168.2.2    nombre.privado.nodo2.com
```

Instalar los servicios que se van a gestionar a través del agrupamiento (cluster):

```
yum -y install httpd php vsftpd wget
```

Utilizando un editor de texto simple, crear el fichero /var/www/html/index.php:

```
vim /var/www/html/index.php
```

Y añadir el siguiente contenido:

```
<html>
<head>
<title>Este es el nodo 1</title>
</head>
<body>
<h1>Este es el nodo 1</h1>
<p>Este es el servidor principal que se presenta
normalmente.</p>
</body>
</html>
```

Crear el fichero /etc/httpd/conf.d/cluster.conf con el siguiente contenido:

```
# Definir valores con el nombre público y la dirección
# IP pública del cluster

NameVirtualHost 192.168.1.100:80

<VirtualHost 192.168.1.100:80>
    ServerName nombre.publico.cluster.com
    DocumentRoot /var/www/html
    ErrorLog logs/cluster-error_log
    CustomLog logs/cluster-access_log combined
    ServerAdmin alguien@algo.com

</VirtualHost>
```

Utilice cualquier editor de texto sobre el fichero `/etc/vsftpd/vsftpd.conf`:

```
vim /etc/vsftpd/vsftpd.conf
```

Y añadir al final de éste lo siguiente:

```
ftpd_banner=Bienvenido al servicio FTP del Nodo 1.  
chroot_local_user=YES  
chroot_list_enable=YES  
chroot_list_file=/etc/vsftpd/chroot_list
```

Generar con el mandato **touch** el fichero `/etc/vsftpd/chroot_list`:

```
touch /etc/vsftpd/chroot_list
```

Instalar el depósito YUM de Alcance Libre que incluye Shorewall:

```
cd /etc/yum.repos.d/  
  
wget http://www.alcancelibre.org/al/server/AL-Server.repo
```

Instalar Shorewall:

```
yum -y install shorewall
```

Cambie al directorio `/etc/shorewall`:

```
cd /etc/shorewall
```

Editar con vim el fichero `/etc/shorewall/shorewall.conf` y cambie `STARTUP_ENABLED=No` por `STARTUP_ENABLED=yes`:

```
STARTUP_ENABLED=Yes
```

A fin de que exista una comunicación sin restricciones entre ambos nodos cuando el cortafuegos esté detenido, es importante definir el siguiente contenido en el fichero `/etc/shorewall/routesstoped`:

```
eth0          192.168.1.102      critical
eth1          192.168.2.2       critical
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT
REMOVE
```

Definir las zonas del mudo cortafuegos en el fichero `/etc/shorewall/zones`:

```
fw          firewall
net         ipv4
loc         ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

Definir que interfaces de red corresponden a las zonas establecidas en el fichero `/etc/shorewall/interfaces`:

```
net  eth0          detect          dhcp,blacklist
loc  eth1          detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT
REMOVE
```

De igual forma definir las siguientes políticas en el fichero `/etc/shorewall/policy`:

```
fw          all          ACCEPT
loc         fw          ACCEPT
loc         net          REJECT          info
net         all          DROP            info
#LAST LINE -- DO NOT REMOVE
```

Considerando que se están configurando los servicios *shorewall*, *vsftpd* y *httpd*, se administrarán ambos servidores a través de SSH, limitando los pings desde cualquier zona a 5 conexiones por segundo con ráfagas de 2, definir las siguientes reglas para el fichero `/etc/shorewall/rules`:

```
ACCEPT all          fw          tcp          20,21
ACCEPT all          fw          tcp          80,443
ACCEPT all          fw          tcp          3306
ACCEPT all          fw          tcp          22
ACCEPT all          fw          icmp         8          -          -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT
```



```
REMOVE
```

Debido a un error en el guión %pre (pre-instalación) de los paquetes de heartbeat que son distribuidos a través de los depósitos **YUM** de CentOS, es importante crear previamente el usuario y grupo que utilizará heartbeat, o de otro modo fallará la instalación:

```
groupadd -g 496 haclient
useradd -M -g haclient -u 498 -d
/var/lib/heartbeat/cores/hacluster hacluster
```

Instalar el paquete heartbeat. Se instalarán automáticamente como dependencias los paquetes heartbeat-stonith y heartbeat-pils:

```
yum -y install heartbeat
```

Cambiarse al directorio /etc/ha.d

```
cd /etc/ha.d
```

Copiar los ficheros de ejemplo para configuración de heartbeat.

```
cp /usr/share/doc/heartbeat-*/ha.cf ./ha.cf
cp /usr/share/doc/heartbeat-*/haresources ./haresources
cp /usr/share/doc/heartbeat-*/authkeys ./authkeys
```

Añadir al final del fichero authkeys algo similar a lo siguiente:

```
# Define el esquema de autenticación por SHA1 y una
clave de acceso.
auth 2
2 sha1 p0n3r-aqu1-un4-clav3-d3-acceso-s3gur4
```

Se puede generar el contenido del fichero /etc/ha.d/authkeys, con un criptograma adecuado, utilizando el siguiente guión:

```
( echo -ne "auth 2n2 sha1 "; \
dd if=/dev/urandom bs=512 count=1 | openssl md5 ) >
/etc/ha.d/authkeys
```

Por motivos de seguridad, este fichero solo debe tener permisos de lectura y escritura para el usuario *root*. Cambiar el permiso de éste ejecutando lo siguiente:

```
chmod 600 authkeys
```

Editar el fichero *ha.cf*:

```
vim ha.cf
```

Añadir al final del fichero *ha.cf* lo siguiente:

```
logfile /var/log/ha-log
logfacility local0
keepalive 2
# Tiempo de espera para iniciar servicios si nodo principal
# deja de
# responder. Puede ajustarse a cualquier tiempo razonable.
# Ejemplo: 10 segundos.
deadtime 20
initdead 90
# interfaz de comunicación ente nodos
bcast eth1
udpport 694
auto_failback on
# Nombres de los nodos que participarán en el cluster.
# Deben ser diferentes a los nombres de anfitrión utilizados
# para las IP
# públicas de la las interfaces eth0. Solo son para uso
# interno.
# Los nombres deben estar resueltos en el fichero /etc/hosts
# con direcciones IP privadas en las interfaces eth1, la
# cuales corresponden a
# las interfaces privadas del cluster, a través de la cual se
# comunican los
# nodos del cluster.
node nombre.privado.nodo1.com
node nombre.privado.nodo2.com
```

Editar el fichero *haresources*:

```
vim haresources
```

Añadir al final del fichero *haresources* lo siguiente, donde se define el nombre del nodo 1, dirección IP que utilizará Heartbeat para servir los recursos, máscara de subred en formato de bits, nombre de interfaz de red donde se creará la interfaz virtual, dirección de difusión de la red (broadcast) y los servicios a controlar:

```
# En el ejemplo a continuación:
# nombre.privado.nodo1.com = nombre de anfitrión del nodo
principal
# 192.168.1.100 = dirección IP pública del cluster
# 24 = máscara en formato de bits
# eth0 = interfaz pública del cluster
# 192.168.1.101 = dirección IP del nodo principal a supervisar
# vsftpd httpd = servicios a brindar a través del cluster
nombre.privado.nodo1.com 192.168.1.100/24/eth0/192.168.1.255
shorewall vsftpd httpd
```

Desactivar los servicios que se van a gestionar a través del agrupamiento (cluster):

```
chkconfig httpd off
chkconfig vsftpd off
chkconfig shorewall off
```

Iniciar el servicio heartbeat:

```
service heartbeat start
```

Añadir el servicio heartbeat al arranque del sistema:

```
chkconfig heartbeat on
```

Los servicios shorewall, httpd y vsftpd iniciarán automáticamente poco después de iniciar el servicio heartbeat.

Configuración del Nodo 2

Ingresar como *root* o bien cambiar al usuario *root*.

```
su -l
```

Instalar los servicios que se van a gestionar a través del agrupamiento (cluster):

```
yum -y install httpd php vsftpd
```

Utilizando un editor de texto simple, crear el fichero `/var/www/html/index.php`:

```
vim /var/www/html/index.php
```

Y añadir el siguiente contenido:

```
<html> <head> <title>Este es el nodo 2</title> </head>
<body> <h1>Este es el nodo 2</h1> <p>Este es el servidor
secundario que se presenta cuando falla o se apaga el
<b>nodo 1</b>.</p> </body> </html>
```

A través de SCP, copiar desde el nodo 1 el fichero `/etc/httpd/conf.d/cluster.conf` dentro del directorio `/etc/httpd/conf.d/local`:

```
scp -p 192.168.1.101:/etc/httpd/conf.d/cluster.conf
/etc/httpd/conf.d/
```

Utilizar cualquier editor de texto sobre el fichero `/etc/vsftpd/vsftpd.conf`:

```
vim /etc/vsftpd/vsftpd.conf
```

Y añadir al final de éste lo siguiente:

```
ftpd_banner=Bienvenido al servicio FTP del Nodo 2.
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

Generar con el mandato **touch** el fichero `/etc/vsftpd/chroot_list`:

```
touch /etc/vsftpd/chroot_list
```

Instalar Shorewall:

```
yum -y install shorewall
```

Cambie al directorio `/etc/shorewall`:

```
cd /etc/shorewall
```

Editar con vim el fichero `/etc/shorewall/shorewall.conf` y cambie `STARTUP_ENABLED=No` por `STARTUP_ENABLED=yes`:

```
STARTUP_ENABLED=Yes
```

A fin de que exista una comunicación sin restricciones entre ambos nodos cuando el cortafuegos esté detenido, defina el siguiente contenido en el fichero `/etc/shorewall/routesstoped`:

```
eth0      192.168.1.101    critical
eth1      192.168.2.1     critical
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Definir las zonas del mudo cortafuegos en el fichero `/etc/shorewall/zones`:

```
fw      firewall
net     ipv4
loc     ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

Definir que interfaces de red corresponden a las zonas establecidas en el fichero `/etc/shorewall/interfaces`:

```
net     eth0          detect      dhcp,blacklist
loc     eth1          detect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Definir las siguientes políticas en el fichero `/etc/shorewall/policy`:

```
fw      all          ACCEPT
loc     fw          ACCEPT
loc     net          REJECT      info
net     all          DROP        info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Definir las siguientes reglas para el fichero `/etc/shorewall/rules`:

```
ACCEPT all          fw      tcp    20,21
ACCEPT all          fw      tcp    80,443
ACCEPT all          fw      tcp    3306
```

```
ACCEPT all          fw          tcp    22
ACCEPT all          fw          icmp   8      -      -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT
REMOVE
```

Crear el usuario y grupo que utilizará heartbeat:

```
groupadd -g 496 haclient
useradd -M -g haclient -u 498 -d
/var/lib/heartbeat/cores/hacluster hacluster
```

Instalar el paquete heartbeat:

```
yum -y install heartbeat
```

A través de SCP, copiar desde el nodo 1 el fichero /etc/hosts para reemplazar el fichero /etc/hosts local:

```
scp -p 192.168.1.101:/etc/hosts /etc/hosts
```

A través de SCP, copiar desde el nodo 1 el contenido completo del directorio /etc/ha.d dentro de /etc

```
scp -p 192.168.1.101:/etc/ha.d/* /etc/ha.d/
```

Desactivar los servicios que se van a gestionar a través del agrupamiento (cluster):

```
chkconfig httpd off
chkconfig vsftpd off
chkconfig shorewall off
```

Iniciar el servicio heartbeat:

```
service heartbeat start
```

Añadir el servicio heartbeat al arranque del sistema:

```
chkconfig heartbeat on
```

Los servicios shorewall, httpd y vsftpd iniciarán automáticamente solo cuando heartbeat detecte que ha fallado el nodo 1 o se ha perdido conectividad con éste.

Verificando el agrupamiento (cluster).

La mejor forma de verificar que todo funciona correctamente es acceder con el navegador hacia `http://nombre.publico.cluster.com/` o `http://192.168.1.100/`, o bien acceder a través de un cliente FTP hacia `nombre.publico.cluster.com` o `192.168.1.100`. Deberá de responder el nodo 1.

Apague el nodo 1 o detenga el servicio heartbeat en el nodo 1, espere 20 a 30 segundos e intente acceder hacia las direcciones anteriores. Deberá de responder el nodo 2. Volviendo a encender el nodo 1 o iniciando de nuevo el **servicio heartbeat**, espere 20 a 30 segundos e intente acceder nuevamente hacia las direcciones. Deberá de responder el nodo 1.

Mantener sincronizados los directorios.

Es importante resaltar que las interfaces eth1 de ambos nodos deben ser excluidas para realizar cualquier actividad. Deben ser utilizadas exclusivamente por el servicio de heartbeat. Utilice las interfaces eth0 para realizar sincronización de datos.

En el caso del nodo 2, se puede generar una tarea programada para que se ejecute cada cierto tiempo, utilizando **rsync** y configurando la cuenta de *root* de ambos nodos para utilizar SSH sin clave de acceso. En el siguiente ejemplo para entrada el fichero `/etc/crontab`, se sincroniza cada hora el `/var/ftp/pub` del nodo 2, a partir del directorio `/var/ftp/pub` del nodo 1:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
00 * * * * root rsync -avz \
```

```
    --exclude '*log' --exclude '*tmp/*' -e ssh --
delete-after \
    root@192.168.1.101:/var/ftp/pub /var/ftp/pub
```

En el caso del nodo 1, se asume que si este falla y es apagado, al iniciar sincroniza con el nodo 2, el cual estuvo trabajando y funcionando en ausencia del nodo 1. Puede agregarse el siguiente ejemplo al fichero /etc/rc.local, lo que corresponde a la sincronización de datos de los directorios /var/ftp/pub a partir del nodo 2 hacia el nodo 1 que se asume acaba de iniciar:

```
#!/bin/sh
#
# This script will be executed *after* all the other
# init scripts.
# You can put your own initialization stuff in here if
# you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
rsync -avz \
    --exclude '*log' --exclude '*tmp/*' -e ssh --
delete-after \
    root@192.168.1.102:/var/ftp/pub /var/ftp/pub
```


Anexo C : Instalación de Postfix

En la línea de comando de CentOS llamada terminal se teclearan los siguientes comandos para llevar a cabo la instalación:

```
yum install postfix
```

Ahora se configura el archivo /etc/postfix/main.cf:

```
nano -w /etc/postfix/main.cf
```

Busque los siguientes parámetros y cámbielos según dice aquí:

```
inet_interfaces = all

mydestination = $myhostname, localhost.$mydomain, localhost,
$mydomain

home_mailbox = mail/
```

Con esto se dice que Postfix responda a los pedidos en la red y además que use el formato **Maldir** que es mejor que el que viene por defecto, llamado **mbox**. Las líneas que empiezan con # son comentarios. Una vez hechos los cambios se tienen que guardar para que quede la instalación.

Reiniciar el servicio Postfix:

```
service postfix restart
```

Y agregarlo a los servicios que se iniciarán al cargar el sistema:

```
chkconfig --levels 345 postfix on
```

Anexo D : Instalación de ClamAv

Para poder realizar la instalación de ClamAV se deben agregar los repositorios de rpmforge, ya que ClamAV no está contenido en los repositorios originales de Centos.

Los repositorios *RMPforge* se agregaran de la siguiente manera. Acceda al portal web de RMPforge: <https://rpmrepo.org/RPMforge/Using>

Descargar el paquete enmarcado en el recuadro negro, en particular la versión para 32 bits (i386).

La razón del porque se descarga este paquete y no los demás es porque se tiene instalada la versión de Centos 5.5, la cual es con la que se ha estado trabajando durante el desarrollo de éste proyecto.

Al finalizar la descarga abrir una terminal, ir a donde descargo el paquete y posteriormente instalar de la siguiente manera:

```
rpm -ivh rpmforge-release-0.3.6-1.$dist.rf.$arch.rpm
```

Una vez concluida esta acción se podrá empezar a instalar ClamAV. Los paquetes que se instalaran serán los siguientes:

clamav El paquete antivirus

libclamav La API para integrar más modulos

clamtk interfaz gráfica basada en GTK

clamd Métodos para ejecutar el motor en segundo plano (demonio del sistema)

Instalar estos paquetes tecleando en consola lo siguiente:

```
sudo yum install clamav libclamav clamtk clamd
```

Para iniciar el Antivirus ClamAV por primera vez solo deberá teclear en terminal el siguiente comando:

```
/etc/init.d/clamd start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el Antivirus ClamAV. Estas opciones pueden ser consultadas enseguida:

start Inicia el servicio

stop Detiene el servicio

restart Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta

reload Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente

condrestart Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose

status Da a conocer el estado en el que se encuentra el servicio

Como alternativa también se puede ocupar el siguiente comando para iniciar el Antivirus ClamAV

```
[root@ localhost ~]# service clamd start
```

Y de igual manera se puede usar las opciones antes descritas en la tabla anterior. Recordar que estos comandos se ejecutan como *root*.

Anexo E : Instalación de SpamAssassin

Para empezar con la instalación de SpamAssassin solamente es seguir los siguientes pasos, teclearlos en la terminal de CentOS:

```
cd /etc/mail/spamassassin  
  
mv local.cf local.cf.orig  
  
nano local.cf
```

Añadir las siguientes líneas:

```
required_score      5.0
rewrite_header subject [SPAM]
report_safe         1
use_bayes           1
use_bayes_rules     1
bayes_auto_learn   1
skip_rbl_checks     0
```

Guardar los cambios y configurar Spamassassin con la siguiente línea para que arranque en automático:

```
chkconfig spamassassin on
```

Se procede a la instalación y configuración de *spamass-milter*, éste es un componente adicional para la biblioteca de filtros de correo (libmilter) de Sendmail, que se encarga de hacer pasar todo el correo entrante a través de SpamAssassin.

```
cd /usr/src
wget http://www.voztovoice.org/tmp/spamass-milter-0.3.1.tar.gz
tar -xf spamass-milter-0.3.1.tar.gz
cd spamass-milter-0.3.1
```

Si no se tienen instalados los programas y la librería para compilar las fuentes se tendrá que instalar los siguientes paquetes:

```
yum install gcc ncurses ncurses-devel make gcc-c++ libtermcap
libtermcap-devel zlib zlib-devel libtool
./configure
make
make install
```

Instalar el script para arrancarlo en automático como demonio:

```
cd contrib
```

```
nano spamass-milter-redhat.rc
```

Modificar las siguientes líneas:

```
SM_SOCKET=/var/run/spamassassin/spamass-milter.sock  
[ -x /usr/local/sbin/spamass-milter ] || exit 0  
PATH=$PATH:/usr/local/sbin
```

Guardar los cambios y copiar el archivo en la carpeta de los demonios:

```
cp spamass-milter-redhat.rc /etc/init.d/spamass-milter  
cd /etc/init.d  
chmod +x spamass-milter  
chkconfig --level 2345 spamass-milter on  
Ahora crear el archivo de configuración para spamass-milter:  
nano /etc/sysconfig/spamass-milter
```

Añadir:

```
SOCKET=/var/run/spamassassin/spamass-milter.sock  
EXTRA_FLAGS="-r 15"
```

Guardar los cambios y reiniciar el sistema para que SpamAssassin empiece a funcionar correctamente.

Anexo F : Instalación de Mailscanner

Uno de los requisitos para poder instalar MailScanner, es actualizar el *kernel* del sistema operativo, para hacerlo simplemente teclear lo siguiente en una terminal.

```
yum update kernel
```

Al terminar reiniciar el equipo. Una vez actualizado el kernel del sistema operativo se procede a instalar los siguientes paquetes:

```
yum install unrar spamassassin kernel-devel kernel-headers gcc  
gcc-c++ rpm-build gmp
```

Por último solo restaría instalar MailScanner, desafortunadamente este paquete no existe en los repositorios oficiales de centos por lo que se tendrá que descargar directamente de la página web de MailScanner. Para descargarlo solo haga lo siguiente:

<http://www.mailscanner.info/>

Y dar clic en la sección de “**downloads**”, esto conducirá a otra página. Descargar el paquete diseñado para entornos Red Hat, Centos o Fedora. Descomprimir el fichero recién descargado, y cambiarte a la carpeta recién creada:

```
tar -xzvf MailScanner-4.75.11-1.rpm.tar.gz  
cd MailScanner-4.75.11-1/
```

Por último se debe ejecutar el script que se encargara del proceso de instalación

```
install.sh
```

Este proceso dura aproximadamente entre 20 y 40 minutos.

Antes de iniciar el servicio de MailScanner se deberá detener el servicio de Sendmail, para ello hacer lo siguiente:

```
/etc/init.d/sendmail stop  
chkconfig --level35 sendmail off
```

Para iniciar el MailScanner por primera vez solo se deberá teclear en terminal el siguiente comando:

```
/etc/init.d/MailScanner start
```

Anexo G : Instalación de Mailwatch

MailWatch es un *front-end* basado en Web para MailScanner que permite analizar la actividad de MailScanner. Está escrito en PHP, MYSQL y JpGraph bajo licencia GNU. Para hacer la descarga ir a la siguiente dirección:
<http://mailwatch.sourceforge.net/doku.php>

Se verifica que estén instalados los paquetes necesarios

```
rpm -q php-gd
rpm -q mysql
```

Si no están instalados estos paquetes hay que instalarlos

Configurando php

Se edita el archivo /etc/php.ini para que las sentencias queden de la siguiente forma:

```
short_open_tag = On
safe_mode = Off
register_globals = Off
magic_quotes_gpc = On
magic_quotes_runtime = Off
session.auto_start = 0
allow_url_fopen = On
```

Configurando y arrancando Mysql

Se ejecutan los siguientes comandos:

```
mysql_install_db
mysqladmin -u root password yyyyy donde yyyyy es la clave del
usuario root
chkconfig mysqld on
service mysqld start
```

Instalación de MailWatch

```
tar -xfz mailwatch-1.0.3.tar.gz
cd mailwatch
mysql -p < create.sql pedirá una clave la clave es la de la base
de datos
```

Se crea el usuario para administrar MailWatch mediante los siguientes pasos:

```
mysql mailscanner -u xxxxx -p
Enter password: yyyyy
use mailscanner
```

```
INSERT INTO users VALUES ('xxxxx',md5('yyyyy'),'Administra','A','0','0','0','0');
EXIT
```

Donde xxxxx es el usuario para administrar mailwatch y yyyyy la clave del usuario

```
cp mailscanner/conf.php.example mailscanner/conf.php
vi mailscanner/conf.php
```

Se va a la línea 30 y se realiza los siguientes cambios:

```
define(DB_USER, 'root');
define(DB_PASS, "");
```

Se cambia por:

```
define(DB_USER, 'xxxxx');
define(DB_PASS, 'yyyyy');
```

Donde xxxxx es el usuario de la base de datos por lo general root de mysql y yyyyy es la clave de ese usuario.

En la línea 73 se realiza el siguiente cambio:

```
define(QUARANTINE_USE_FLAG, false);
```

Se cambia por

```
define(QUARANTINE_USE_FLAG, true);
```

```
vi MailWatch.pm
```

Se va a la línea 43 y se modifica para que quede de la siguiente forma:

```
my($db_user) = "root";  
my($db_pass) = "";
```

Se cambia por:

```
my($db_user) = "xxxxx";  
my($db_pass) = "yyyyy";
```

Donde xxxxx es el usuario de la base de datos y yyyyy su clave.

Ir a la línea 173 y se modifica para que quede de la siguiente forma:

```
MailScanner::Log::InfoLog("$$message{id}: Logged to MailWatch SQL");
```

Se cambia por:

```
MailScanner::Log::DebugLog("$$message{id}: Logged to MailWatch SQL");
```

Buscar la línea 326 y se modifica para que quede de la siguiente forma:

```
MailScanner::Log::InfoLog("Logging message $msg{id} to SQL");
```

Se cambia por:

```
MailScanner::Log::DebugLog("Logging message $msg{id} to SQL");
```

```
vi mailscanner/mailq.php
```

Ir a la línea 15 y se modifica para que quede de la siguiente forma:

```
case default:
```

Se cambia por:

default:

Se mueve al archivo de MailWatch.pm

```
mv MailWatch.pm /usr/lib/MailScanner/MailScanner/CustomFunctions
```

Se mueve la carpeta mailscanner a la carpeta para el Web

```
mv mailscanner /var/www/html
```

Dar permisos a las siguientes carpetas:

```
chown root:apache /var/www/html/mailscanner/images
```

```
chmod ug+rwx /var/www/html/mailscanner/images
```

```
chown root:apache /var/www/html/mailscanner/images/cache
```

```
chmod ug+rwx /var/www/html/mailscanner/images/cache
```

```
chown apache /var/www/html/mailscanner/temp
```

```
chmod gu+wr /var/www/html/mailscanner/temp
```

Configuración de MailScanner

```
vi /etc/MailScanner/MailScanner.conf
```

```
Quarantine User = root
```

```
Quarantine Group = apache (this should be the same group as your  
web server)
```

```
Quarantine Permissions = 0660
```

```
Quarantine Whole Message = yes
```

```
Quarantine Whole Message As Queue Files = no
```

```
Detailed Spam Report = yes
```

```
Include Scores In SpamAssassin Report = yes
```

```
Always Looked Up Last = &MailWatchLogging
```

```
Detailed Spam Report = yes
```

```
Include Scores In SpamAssassin Report = yes
```

Permisos a las bases bayesianas

```
chown root:apache /etc/MailScanner/bayes
```

```
chmod g+rws /etc/MailScanner/bayes
```

Para ingresar a ver el monitoreo:

<http://www.xxxx.com/mailscanner>

Donde xxxx es el nombre del servidor donde se instaló el Mailwatch.

En este url pedirá un usuario y una clave, los cuales son lo que se ingresaron en la base de datos con el comando **Insert**.

De esta manera se da por concluida la instalación de estos componentes de seguridad en Linux, algunos son algo difícil de configurar pero esto se hará una vez que se asignen las características de red como segmentos de red, nombres de dominio entre otras para tener un mejor control de los servicios.

Anexo H: Instalación de MySQL

El primer paso es instalar Mysql mediante el siguiente comando

```
yum install mysql mysql-server
```

Una vez instalado se configura para que inicie automáticamente con el comando:

```
chkconfig --levels 235 mysqld on
```

Y se arranca con:

```
/etc/init.d/mysqld start
```

Se tiene que instalar Apache con:

```
yum install httpd
```

Una vez instalado se configura para que inicie automáticamente con

```
chkconfig --levels 235 httpd on
```

Y se arranca con:

```
/etc/init.d/httpd start
```

En este punto si se navega con la dirección de servidor se tendría que ver algo así:



Figura H1: LocalHost Apache en navegador

Anexo I: Instalación de PHP

Se instala PHP y se vincula a Apache usando:

```
yum install php
```

Reiniciar Apache usando:

```
/etc/init.d/httpd start
```

Enseguida se genera un archivo para probar que PHP funciona correctamente usando:

```
touch /var/www/html/info.php
```

```
echo '<?php phpinfo(); ?>' > /var/www/html/info.php
```

Si se navega la URL <http://direccion server/info.php> se tendrá que ver lo siguiente:

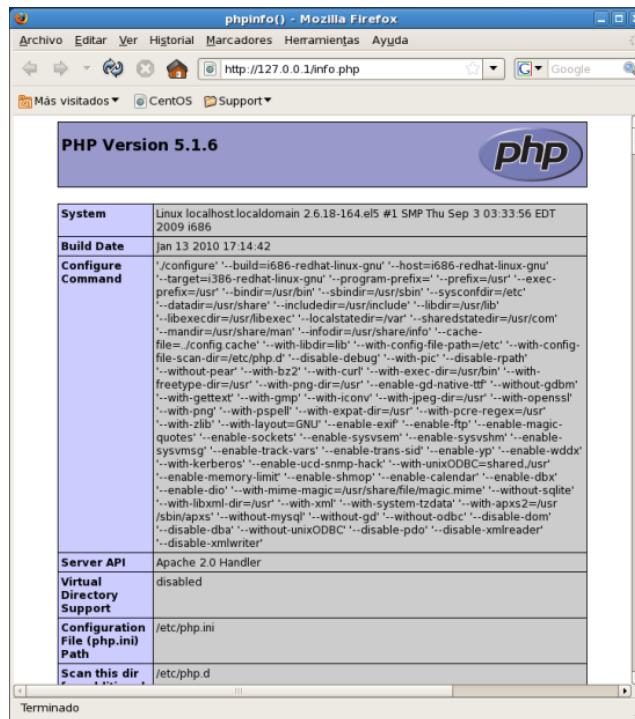


Figura I1: LocalHost del servidor PHP

Para finalizar solo resta agregar soporte de mysql a php usando el siguiente comando:

Implementación de servidores virtualizados que mejoren la eficiencia del uso de energía y servicios de red en centros de investigaciones.

```
yum install php-mysql
```

Reiniciar Apache usando

```
/etc/init.d/httpd start
```

Si se navega la URL `http://direccion server/info.php` tendrá que verse en la parte media de la página lo siguiente:

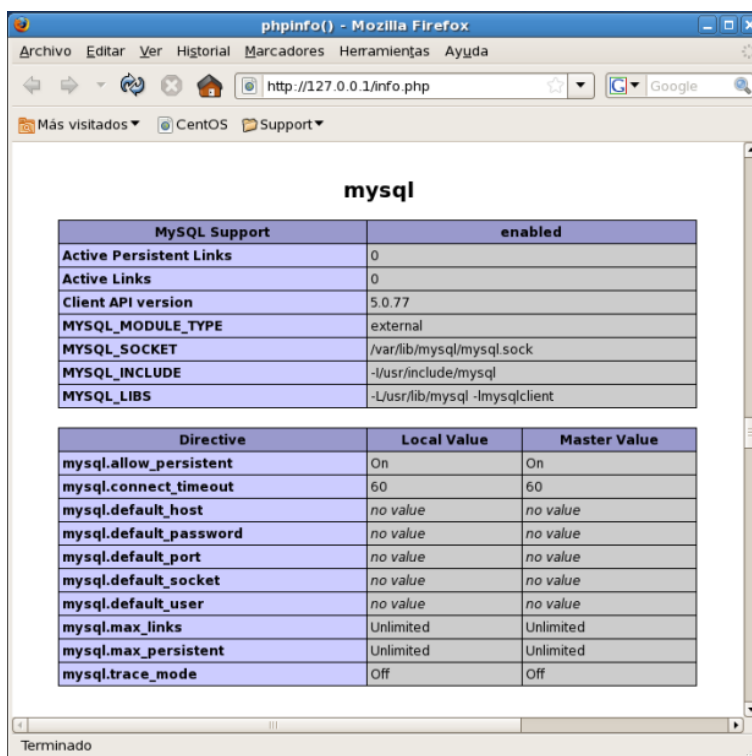


Figura I2: Servidor PHP com MySql

Anexo J: Instalación de Joomla!

En seguida se muestra el proceso de instalación de la herramienta Joomla en Linux:

Algunos requisitos previos a la instalación son:

- ⊕ Xampp para linux
- ⊕ Joomla
- ⊕ Un navegador web (puede ser Firefox, Konqueror, Opera)

- ⊕ Un navegador de archivos (konqueror o Nautilus) no es obligatorio pero para una mejor manipulación de archivos.
- ⊕ Iniciar el servicio de xampp como root, con el comando

```
/opt/lampp/lampp start
```

En la pantalla de consola se deberá ver algo como esto:

```
Starting XAMPP 1.6.8a...
```

```
LAMPP: Starting Apache...
```

```
LAMPP: Starting MySQL...
```

```
LAMPP started.
```

Para comprobar que el Xampp está funcionando hay que hacer una prueba. Abrir cualquier navegador disponible en la máquina y teclear en la barra de direcciones <http://localhost> y en seguida debe mostrar lo siguiente.



Figura J1: LocalHost de Xampp

Esta pantalla significa que el servicio se ha levantado de manera correcta.

Posteriormente se crea una base de datos de Joomla de la siguiente forma, en la ventana de comprobación de Xampp, se verá un panel en el lado izquierdo, dar clic en la opción phpmyadmin. Aparecerá una ventana como la siguiente:

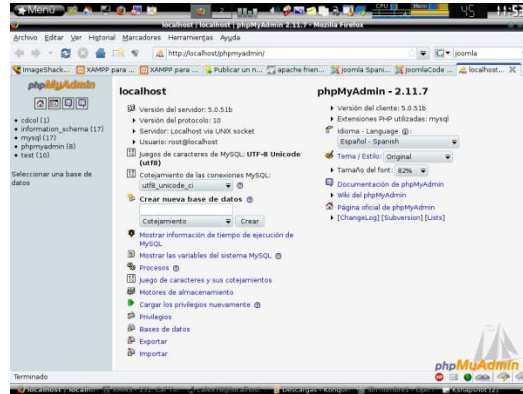


Figura J2: phpMyAdmin

En la opción crear una base de datos, se escribe cualquier nombre o como se quiera llamar a la base de datos para Joomla, por comodidad y para posterior utilización se llamará joomla.

Copiar joomla a carpeta de Xampp, desempaquetar la descarga de joomla y copia el contenido de la carpeta en:

```
/opt/lampp/htdocs
```

El copiado de archivos debe hacerse como *root*, por tanto, es recomendable abrir una consola, loguearse como *root*, y escribir en ella el comando **konqueror** o **nautilus**, para tener un navegador disponible con permisos de *root* y así poder copiar fácilmente los archivos.

Una vez copiados los archivos dirigirse al navegador web y escribir <http://localhost/joomla/>, debe aparecer una página como la siguiente:

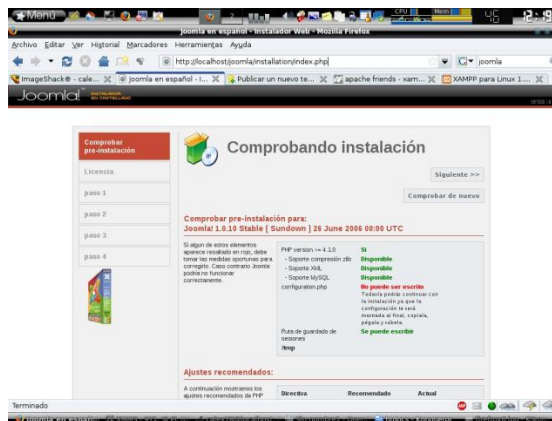


Figura J3: LocalHost de Joomla!

Si algún componente se encuentra en rojo, quiere decir que previamente se tiene que instalar o que no se encuentra instalado aún. De lo contrario dar en siguiente:



Figura J4: Paso 1 del asistente de configuración de Joomla!

En esta sección se encuentra la configuración de la base de datos MySQL, se debe llenar con los siguientes datos:

- ⊕ Nombre del servidor = localhost
- ⊕ Nombre del usuario MySQL= root
- ⊕ *Contraseña MySQL =
- ⊕ *Nombre de la base de datos MySQL = joomla
- ⊕ Prefijo de la tabla MySQL= jos_

- ⊕ Dar en siguiente: Nombre del sitio web. Simplemente es el nombre con el que se llamara al servidor.

Dar en siguiente y configurar email y contraseña, en contraseña, “contraseña” pero ahí se puede escribir la contraseña que se desee, con ésta se administrará posteriormente (los dos campos de arriba aparecen llenos por default)

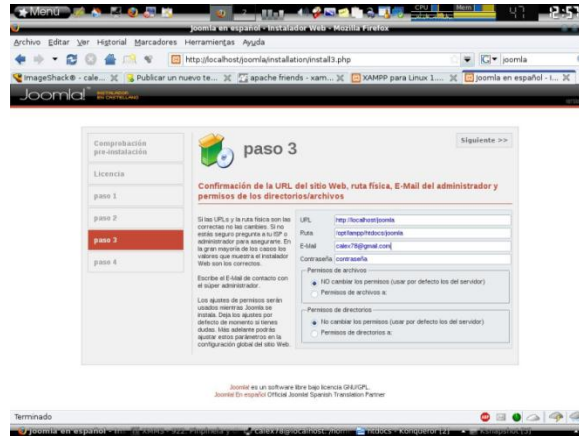


Figura J5: Paso 3 del asistente de configuración de Joomla!

Dar en siguiente y aparecerá la ventana de que Joomla ha sido instalado correctamente.

Es importante darle permisos de ejecución, basta con escribir los siguientes comandos en la terminal:

```
#chmod 777 configuration.php
```

Y borrar el archivo de instalación de Joomla de la carpeta joomla que se encuentra en htdocs.

Ahora bien escribir en el navegador <http://localhost/joomla/>, la siguiente página aparecerá:



Figura J6: Localhost de Joomla! configurado

Ahora si se tendrá que acceder como administrador para poder manipular el servidor. Para más detalles ver (Joomla, 2011).