ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

INFORME DE MATERIA DE GRADUACIÓN

" IMPLEMENTACION DE LA VIRTUALIZACION DE SERVICIOS EN LAS PYMES "

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentada por

RENE ALBERTO FRANCO ZAMBRANO

LUIS ALFREDO COLCHA GONZÁLEZ

Guayaquil - Ecuador

2012

TRIBUNAL DE SUSTENTACIÓN

_____

Rayner Stalyn Durango Espinoza

PROFESOR DE LA MATERIA DE GRADUACIÓN

_____

Giuseppe Blacio

PROFESOR DELEGADO POR EL DECANO DE LA FACULTAD

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

_____

René Alberto Franco Zambrano

_____

Luis Alfredo Colcha González

RESUMEN

El presente documento, consiste en la implementación de virtualizar los servicios importantes en una PYME como son Active Directory, Proxy y Correo, bajo una sola plataforma de virtualización como VMware. Así podemos optimizar los recursos y la administración de los sistemas principales.

Para este proyecto se estableció que la implementación de la infraestructura de virtualización, nos permitiría:

- Poder integrar varios servicios críticos bajo un solo hardware virtualizado.
- Brindar el máximo rendimiento que puede otorgar el hardware.
- Administración global centralizada y simplificada.
- Ejecutar distintos sistemas operativos de forma independiente sobre el mismo hardware.
- Reducción de costes de infraestructura física, operativos y por interrupciones de servicio.

Las herramientas a utilizar para poder llevar a cabo esta implementación son: VMware Workstation, ESXi, VMware VSphere Client, Windows Server 2003, Windows XP, Centos 5.4, Squid Proxy y SendMail.

ÍNDICE GENERAL

1 ANTECEDENTES Y JUSTIFICACIÓN 2

1.1 ANTECEDENTES 2

1.2 JUSTIFICACIÓN 3

1.3 DESCRIPCIÓN DEL PROYECTO 4

1.4 METODOLOGÍA 5

2 VMWARE WORKSTATION, ESXi Y VSPHERE CLIENT 8

2.1 VMWARE WORKSTATION 8

2.2 VMWARE ESXi 10

2.3 VSPHERE CLIENT 18

3 IMPLEMENTACIÓN 21

3.1 INTRODUCCION 21

3.2 HARDWARE 22

3.3 INSTALACIÓN 24

4 FUNCIONAMIENTO Y PRUEBAS 82

4.1 CONFIGURACIÓN EN EL ACTIVE DIRECTORY 82

4.2 PRUEBAS DE NAVEGACION EN LOS CLIENTES CON EL SQUID CONFIGURADO 85

4.3 CREACION DE CUENTAS DE CORREO Y PRUEBAS CON SENDMAIL 88

4.4 GRAFICAS DE RENDIMIENTO 93

CONCLUSIONES 111

RECOMENDACIONES 117

GLOSARIO DE TÉRMINOS 121

BIBLIOGRAFÍA 130

ÍNDICE DE FIGURAS

Fig. 1.1 Virtualización de Servicios sobre ESXi de una PYME. 6

Fig. 2.1 Ejemplo lógico de Virtualización de varios Sistemas 9

Fig. 2.2 Ejecución de varias aplicaciones sobre ESXi…….....11

Fig. 2.3 Infraestructura y Administración con VMware ESXi..... 18

Fig. 2.4 Gestión de VMware ESXi mediante vSphere Client…….....19

Fig. 3.1 Pantalla de instalación inicial……..……25

Fig. 3.2 Pantalla de selección del tipo de instalación……26

Fig. 3.3 Selección de cambio de directorio……..27

Fig. 3.4 Pantalla de selección de actualizaciones……..…28

Fig. 3.5 Pantalla de selección para experiencia de usuario……29

Fig. 3.6 Pantalla de creación de accesos directos……30

Fig. 3.7 Pantalla para iniciar la instalación……...31

Fig. 3.8 Pantalla para introducir una licencia válida……..…32

Fig. 3.9 Pantalla de finalización de la instalación……..33

Fig. 3.10 Pantalla de términos de licencia……...34

Fig. 3.11 Menú de arranque de VMware VMvisor……35

Fig. 3.12 Arrancando VMware ESXi……..…36

Fig. 3.13 Pantalla para seleccionar operación……37

Fig. 3.14 Pantalla de EULA……..……..38

Fig. 3.15 Pantalla para selección de disco duro……..…39

Fig. 3.16 Pantalla para confirmación de instalación……..…40

Fig. 3.17 Pantalla de instalación terminada……..…..41

Fig. 3.18 Pantalla de inicio de VMware ESXi……..……42

Fig. 3.19 Pantalla de configuración……..……43

Fig. 3.20 Establecer la configuración de Root……44

Fig. 3.21 Pantalla para cambiar la configuración de red……..……45

Fig. 3.22 Configuración de IP Estática……46

Fig. 3.23 Pantalla de bienvenida a WMware ESXi……47

Fig. 3.24 Descarga del archivo Vsphere client……..48

Fig. 3.25 Elección de idioma de instalación……..48

Fig. 3.26 Pantalla para la conexión del Client……49

Fig. 3.27 Números de días de prueba restantes…….....50

Fig. 3.28 Pantalla de inventory para introducir la licencia……51

Fig. 3.29 Pantalla para seleccionar configuration……52

Fig. 3.30 Pantalla de Licensed Features……..53

Fig. 3.31 Pantalla para el ingreso de licencia al host……54

Fig. 3.32 Ventana para añadir el número de licencia válido……55

Fig. 3.33 Información sobre la licencia introducida……56

Fig. 4.1 Usuarios y equipos de Active Directory..... 83

Fig. 4.2 Inicio de sesión del cliente Administración..... 84

Fig. 4.3 Prueba de conectividad hacia el dominio pyme.com. 85

Fig. 4.4 Servicio de Squid ejecutándose..... 86

Fig. 4.5 Direccionamiento de red de un usuario interno……...87

Fig. 4.6 Opciones avanzadas de Internet Explorer, Servidor Proxy……..…87

Fig. 4.7 Bloqueo de navegación a una página web prohibida……88

Fig. 4.8 Servicio SendMail ejecutándose……89

Fig. 4.9 Propiedades de cuentas de correo……....90

Fig. 4.10 Servidores de correo entrante y saliente……..91

Fig. 4.11 Cuerpo de correo para enviar hacia la cuenta consultor……92

Fig. 4.11 Recepción de correo desde la cuenta Administración……92

Fig. 4.12 Rendimiento Host-ESXi CPU……93

Fig. 4.13 Rendimiento Host-ESXi DataStore……94

Fig. 4.14 Rendimiento Host-ESXi Disk……95

Fig. 4.15 Rendimiento Host-ESXi Memoria……97

Fig. 4.16 Rendimiento Host-ESXi Network……98

Fig. 4.17 Rendimiento Squid Centos CPU……100

Fig. 4.18 Rendimiento Squid Centos CPU……101

Fig. 4.19 Rendimiento Squid Centos Memoria……102

Fig. 4.20 Rendimiento del CPU en bloqueo de páginas……104

Fig. 4.21 Rendimiento del Datastore en el bloqueo de páginas……105

Fig. 4.22 Rendimiento de memoria en el bloqueo de páginas……106

Fig. 4.23 Rendimiento del CPU en el Active Directory……108

Fig. 4.24 Rendimiento del Datastore en el Active Directory……109

Fig. 4.25 Rendimiento de memoria en el Active Directory……110

ÍNDICE DE TABLAS

Tabla I Características de hardware para Virtualizar 22

Tabla II Sistemas Operativos implementados.....2 ***¡Error! Marcador no definido.***

INTRODUCCIÓN

La virtualización, aprovechando la capacidad y potencia de los equipos actuales, se presenta como la respuesta a la necesidad de alcanzar la máxima eficiencia tecnológica. A través de software, la virtualización divide los recursos de un equipo informático para crear distintas máquinas virtuales que funcionan de manera independiente aunque no existan físicamente. Se trata de crear distintos entornos informáticos virtuales en un mismo hardware.

A medida que una empresa crece, adquiere diferentes equipos informáticos y establece distintos entornos para utilizar herramientas tecnológicas concretas, según las más puntuales necesidades de negocio.

Esta característica destaca por resultar extremadamente práctica y funcional para la empresa, ya que permite la consolidación de servidores; es decir, reduce el número de máquinas y optimiza el grado de uso de los recursos informáticos.

En concreto la media de utilización de un servidor físico en las PYMES es del 10%, y después de la virtualización la utilización media pasa a ser del 80%.

Se reducen los costes de infraestructura física (espacio, electricidad, refrigeración, hardware) gracias a la menor cantidad de servidores y de hardware necesarios para el buen funcionamiento de los servicios.

Mayor disponibilidad de aplicaciones y continuidad del negocio mejorada, disminuyendo el número de interrupciones de los servicios por mantenimiento planificados.

Menor tiempo de recuperación ante un desastre o incidentes imprevistos gracias a la alta disponibilidad y la facilidad para realizar copias de seguridad de los servidores virtuales.

Mejora en los procesos de clonación y copia de sistemas: Mayor facilidad para la creación de entornos de test que permiten poner en marcha nuevas aplicaciones sin impactar a la producción, agilizando el proceso de las pruebas. Reducción de los riegos de parada de la organización sin aumentar los costes ni la complejidad de los sistemas.

Administración global centralizada y simplificada. Gestión dinámica de los recursos de computación disponibles para dar respuesta a los cambios del mercado. Posibilidad de ejecutar antiguas aplicaciones imprescindibles en la organización sobre modernos servidores.

CAPÍTULO 1

1 ANTECEDENTES Y JUSTIFICACIÓN

1.1 ANTECEDENTES

Uno de los objetivos fundamentales que se consigue con la virtualización es la reducción de costes de hardware, de gestión, de aprovisionamiento y de consumo eléctrico. Además, aporta una funcionalidad de vital importancia para su empresa: garantiza la continuidad del negocio. La dependencia actual de los sistemas nos exige el funcionamiento de los servidores con alta disponibilidad.

Con la virtualización de servidores reducimos notablemente el tiempo de inactividad por paradas planificadas o no planificadas de servidores con una inmejorable relación calidad / precio.

En lugar de pagar para tener múltiples máquinas físicas de servidor que no vas a tener a pleno rendimiento, cada una está dedicada a una carga de trabajo específica. La virtualización del servidor hace posible que esas cargas de trabajo se vean consolidadas en un número menor de máquinas pero a pleno rendimiento.

1.2 JUSTIFICACIÓN

VMware ha desarrollado un aplicativo llamado ESXi-SEVER que es un sistema operativo basado en Unix (GNU/Linux) que nos permite virtualizar cualquier tipo de sistema operativo servidor, permitiéndonos una flexibilidad bastante buena, pues los recursos que usa esta mini distribución son mínimos, solo usa un máximo de 300 MHz de los procesadores y un poco menos de 500 megas de memoria para las aplicaciones, tanto las normales de un sistema operativo como las aplicaciones que permiten realizar las virtualizaciones.

En cuanto a espacio en disco duro solo usa una partición de 5 GB donde guarda el Sistema Operativo y otro par de particiones donde almacena el Boot y los logs, los archivos de las máquinas virtuales se almacenan en volúmenes. ESXi-Server soporta más de 128 servidores activos en un solo servidor físico.

ESXi Server es un software que constituye una capa de virtualización de recursos montada directamente sobre el hardware, sin necesidad de un sistema operativo base, ya que ESXi Server es un sistema operativo en sí. Con ESXi server, la gestión de recursos compartidos permite asignar niveles mínimos a las máquinas virtuales con motivo de garantizar un nivel de servicio mínimo, independiente de la carga del resto de máquinas virtuales.

1.3 DESCRIPCIÓN DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Virtualizar los servicios importantes de una Pyme, a través de la plataforma ESXi sobre VMware workstation, complementar con características necesarias para brindar un buen rendimiento y obtener las características de las cargas requeridas.

1.3.2 OBJETIVOS ESPECÍFICOS

- Evaluar los servicios principales que en la actualidad utilizan los pymes.
- Virtualizar estos servicios en un solo hardware, utilizando como sistema base VMware ESXi.
- Implementar el sistema de Gestión del ESXi mediante VSphere Client.
- Monitorear el rendimiento con todos los servicios levantados mediante indicadores.

El proyecto consiste en virtualizar la infraestructura IT de una Pyme, consolidar bajo un solo hardware varios servicios y así tener una administración centralizada. Todos los usuarios para poder navegar hacia internet deberán pasar por el proxy que estará virtualizado sobre Centos, así mismo los correos bajo Send Mail sobre el mismo Sistema Operativo. Mediante el Active Directory se llevara el control de usuarios. Para el proxy es necesario que el hardware tenga configurado dos interfaces de red.

El administrador de IT mediante VSphere Client podrá gestionar y observar el rendimiento de los sistemas virtualizados, puede ser desde un host remoto o desde el mismo Server.

1.4 METODOLOGÍA

Sobre un solo hardware se instalará el VMware Workstation con ESXi, para gestionar los sistemas virtualizados se utilizara el VSphere Client. En el Client se instalaran los sistemas operativos Windows Server 2003 con Active Directory y Centos 5.4 con Squid Proxy y SendMail. El Proxy con control de navegación proporciona a los usuarios poder navegar en internet y al administrador proteger el performance de la red mediante el bloqueo de páginas prohibidas.

Los clientes tendrán configurado la dirección proxy en su navegador Web. El programa utilizado como cliente de correo es el Thunderbird, el mismo es de distribución libre y posee la mayoría de las características principales del Outlook.

Todas las cuentas de usuarios estarán creadas en el Active Directory y registradas en el dominio para así llevar políticas de grupos para proteger la integridad de la Pyme. La infraestructura se muestra en la Figura 1.1.

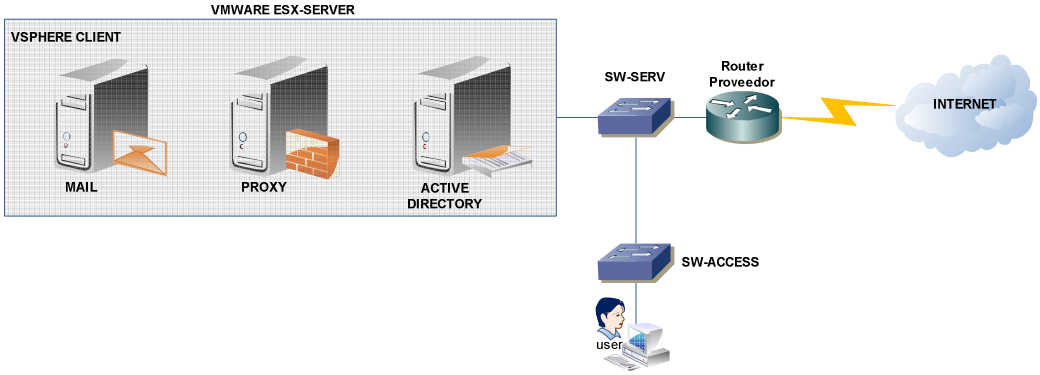


Fig. 1.1 Virtualización de Servicios sobre ESXi de una PYME.

CAPÍTULO 2

2 VMWARE WORKSTATION, ESXi Y VSPHERE CLIENT

2.1 VMWARE WORKSTATION

Las máquinas virtuales son entornos en los que se puede emular hardware físico similar a un PC de modo que se pueda correr un sistema operativo dentro de él. Se pueden instalar varias máquinas virtuales en una solo PC, e incluso, dependiendo del equipo, se puede ejecutarlos al mismo tiempo, e incluso ponerlos en red como si fueran máquinas reales.

Aunque existen varios software de virtualización, entre ellos, VMware, VirtualBox, VirtualPC, Citrix, etc., y algunos de ellos gratuitos, como VirtualBox y VirtualPC, muchas prácticas se han realizado físicamente, y posteriormente, se han simulado virtualmente con el programa VMware Workstation. VMWare es un software comercial y de pago, cuya empresa está especializada en software de virtualización**.**

VMWare Workstation, la ventaja de este software es la posibilidad de poner la máquina virtual en red de diversos modos: local, bridge, NAT y Sin conexión. También permite configurar los recursos: memoria, espacio de disco, procesador, lector de CD, disquetera, sonido, video y red que quieres asignar a la máquina virtual creada. Se puede instalar diversos sistemas operativos: toda la familia de Sistemas Operativos de Microsoft, desde MS-DOS hasta Windows

7, familia de distribuciones de Linux, e incluso algunos de la familia UNIX, como Solaris y BSD**.** Tiene la enorme ventaja de hacer capturas de las pantallas que van saliendo y guardarlas en disco.

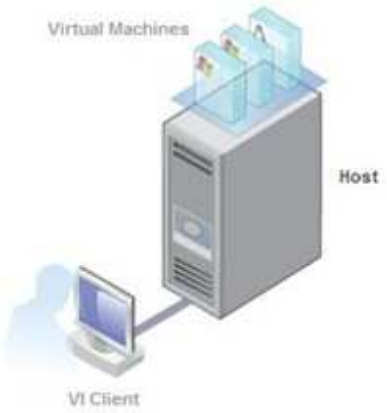


Fig. 2.1 Ejemplo lógico de Virtualización de varios Sistemas

También encontramos la posibilidad de ejecutar juegos que utilicen DirectX 9.0c Shader Model 3 y OpenGL 2.13D de forma muy mejorada, algo muy demandado en juegos de última generación. Ahora se soporta la creación de ordenadores virtuales mucho más potentes, con hasta 4 procesadores virtuales o 4 núcleos y 32Gb de RAM. Como medida de seguridad, se ha añadido encriptación AES de 256 bits y se ha mejorado notablemente la impresión de documentos. Además,

se ha añadido la opción de retroceder a copias de seguridad anteriores y, por supuesto, VMware Workstation 7 se ha testeado y asegurado su completa compatibilidad con Windows 7.

2.2 VMWARE ESXi

ESXi está diseñado para desplegar máquinas virtuales, minimizar los requisitos de configuración y simplificar el despliegue. Los clientes pueden instalar y desplegar máquinas virtuales en pocos minutos, especialmente cuando descargan e instalan dispositivos virtuales pre-configurados. Existen más de 800 dispositivos virtuales creados para el hipervisor de VMware en el VMware Virtual Appliance Marketplace, y ESXi incorpora una integración directa con el mismo, para permitir a los usuarios descargar y lanzar dispositivos virtuales de manera inmediata. Esto permite un nuevo y dinámico acercamiento a la entrega e instalación de software plug-and-play.

Construida sobre la tecnología probada y madura del hipervisor ESX, ESXi amplía esta tradición con una arquitectura independiente del sistema operativo que minimiza las posibilidades de ataque. ESXi incorpora funcionalidades, como 4 CPUs virtuales, 256GB hosts y de-duplicación de memoria, que permiten ejecutar las aplicaciones más intensivas en recursos. Esto permite a ESXi

ofrecer los ratios de consolidación más altos y, por tanto, el TCO y los costes por máquina virtual más bajos. Estas funcionalidades se adaptan perfectamente a un amplio conjunto de sistemas operativos, como Windows, Linux, NetWare y Solaris.

ESXi es la plataforma de virtualización de base sobre la que los clientes pueden construir para lograr disponibilidad de aplicaciones continua y seguridad de la infraestructura.

Fig. 2.2 Ejecución de varias aplicaciones sobre ESXi

2.2.1 FUNCIONES DE VMWARE ESXi

La Arquitectura:

- Arquitectura pequeña de disco de 32 MB.
- Virtualización del CPU.
- Virtualización de almacenamiento.
- Archivos de disco virtual, las máquinas virtuales ven sus propios archivos de disco virtual de forma privada.
- Sistemas de archivos en clúster VMFS, almacena archivos de discos virtuales en sistemas de almacenamiento compartido de alto rendimiento como canal de fibra o SAN.
- Administrador de volúmenes lógicos.
- Asignación de dispositivos sin procesar
- Virtualización de redes, máquinas virtuales en red como equipos físicos.

El Rendimiento y Escalabilidad:

- Rendimiento mejorado de las máquinas virtuales.
- Sobreasignación de memoria RAM.
- Mejora gestión de la energía.
- Permite a una sola máquina virtual utilizar hasta 4 procesadores físicos de forma simultánea.

- Admite potentes sistemas de servidores físicos, con un máximo de 32 CPU lógicos y 128 GB de RAM.
- Admite hasta 128 máquinas virtuales encendidas en un único servidor.

La Interoperabilidad:

- Hardware.
- Almacenamiento.
- Compatibilidad con NAS y SAN.
- Sistemas operativos como Windows, Linux, Solaris y Novell NetWare.
- Aplicaciones de software
- Compatibilidad con otros formatos de máquina virtual, puede ejecutar máquinas virtuales creadas que no son de VMWare.

La Facilidad de Gestión:

- Acceso Web a la infraestructura virtual.
- Acceso directo a máquinas virtuales a través de un navegador Web.
- Dispositivos remotos.
- Interfaz de línea de comando remota.

La Optimización de Recursos Distribuidos:

- Gestión de recursos para máquinas virtuales, se establecen cuotas de recursos mínimas, máximas y proporcionales para CPU, memoria, disco y ancho de banda de red.
- Asignación de prioridades para la capacidad de CPU.
- Asignación de prioridades para el tráfico de E/S de almacenamiento.
- Modelador del tráfico de red, se puede dar prioridad al tráfico de red de las máquinas virtuales según una cuota equitativa.

La Alta Disponibilidad:

- Almacenamiento compartido.
- Trayectorias múltiples en el acceso al sistema de almacenamiento integrado.
- Asociación de NIC mejorada donde se otorga a cada máquina virtual conectada a la red funciones integradas de protección contra errores de NIC y equilibrado de carga que permiten mayor disponibilidad del hardware y tolerancia a fallos.

La Seguridad:

- Compatibilidad con prácticas de seguridad de SAN.
- Identificación de VLAN aumentando la seguridad de la red por medio de la identificación.
- Políticas de seguridad de red de Nivel 2 reforzando la seguridad de las máquinas virtuales en la capa Ethernet.

2.2.2 FORMAS DE ADMINISTAR VMWARE ESXi

VMware ESXi server es un producto complejo que combina una consola basada en Linux (Red Hat). Existen varias formas de realizar la administración de VMware ESXi Server dependiendo de necesidades y presupuesto.

- Acceso por consola por medio del Service Console Como cualquier otro sistema operativo basado en Linux podemos acceder y realizar la administración por medio de una línea de comandos. Para poder trabajar sobre esta consola se requieren conocimientos de Linux y tiempo para aprender los comandos de administración de VMware ESXi Server.
- Acceso a la consola por SSH Se puede establecer una conexión al service console de un servidor VMware ESXi por medio del protocolo SSH y trabajar de la misma forma como si estuviera en la consola del

servidor. Para utilizar. Este método el servidor VMware ESXi deberá estar conectado a la red y tener un cliente ssh instalado en la pc desde la cual se desea acceder al servidor.

- Acceso al servidor VMware ESXi por medio del VMware Virtual Infrastructure (VI) Web Access La forma más simple de acceder a una interface de administración gráfica de un servidor VMware ESXi es utilizando la VMware Virtual Infrastructure (VI) Web Access interface. Esta interface se instala por defecto y para accederla lo único que se necesita es una pc conectada a la red y un navegador de internet. Acceder a la interface es tan simple como abrir un navegador y tipear la dirección IP del servidor. Lo que se obtendrá es una pantalla de bienvenida mostrando opciones de administración. El beneficio de utilizar esta interface es la posibilidad de acceder a una interface de operación básica (no todas las funciones de administración están disponibles) de un servidor VMware ESXi sin la necesidad de instalar un cliente local en el equipo que se utilizará para realizar la administración.
- Acceso a un servidor VMware ESXi por medio de VMware Virtual Infrastructure Client (VI Client) Esta es sin lugar a dudas la mejor forma de administrar remotamente un servidor VMware ESXi. El VMware VI Client es un software que se instala en la pc de administración remota y

para obtenerlo se puede descargar directamente desde la web gui. Los beneficios de utilizar este cliente son básicamente la posibilidad de acceder de forma completa a todas las funciones de VMware ESXi desde un único punto de administración. El único punto en contra es el requerimiento de instalación del VI Client para realizar la administración.

- Acceso por medio de VMware Virtual Infrastructure Client (VI Client) y VMware Virtual Center El mismo cliente (VI Client) puede ser utilizado para administrar un único servidor como también para administra la infraestructura de VMware completa. En lugar de apuntar el cliente al servidor VMware ESXi que queremos administrar todo lo que tenemos que hacer es tipear la dirección IP o el nombre de nuestro servidor VMware Virtual Center. Desde el VMware Virtual Center podrá administrar todos los servidores VMware ESXi server, Storage y redes virtuales que se encuentran configuradas en su infraestructura virtual. VMware Virtual Center es un producto adicional a VMware ESXi Server y requiere licencias adicionales.

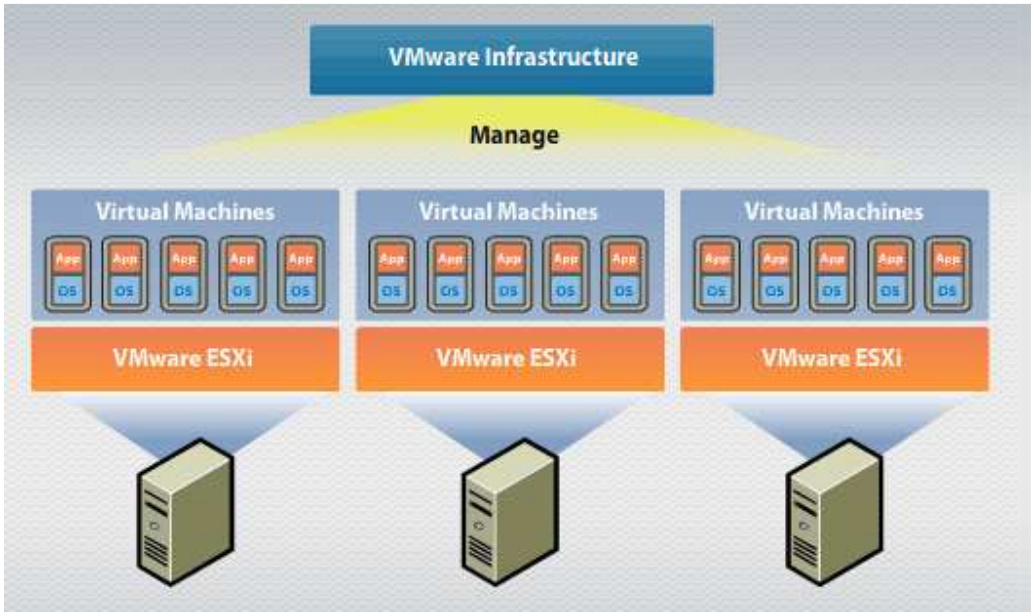


Fig. 2.2 Infraestructura y Administración con VMware ESXi

2.3 VSPHERE CLIENT

VMware vSphere Client es el cliente de administración usado por defecto por los administradores de VMware para gestionar y utilizar las máquinas virtuales que se crean en VMWare ESXi con la posibilidad de utilizarlo sin la necesidad de instalarlo en sus puestos de trabajo.

Es una aplicación basada en sistemas operativos de la familia de Windows que permite al administrador del centro de cómputo o a los operarios dentro del

mismo administrar los servidores ESXi tanto directamente a cada uno o como a través del vCenter server, esta aplicación se puede instalar por medio de un browser direccionando la dirección de los servidores ESXi y el servidor vCenter.

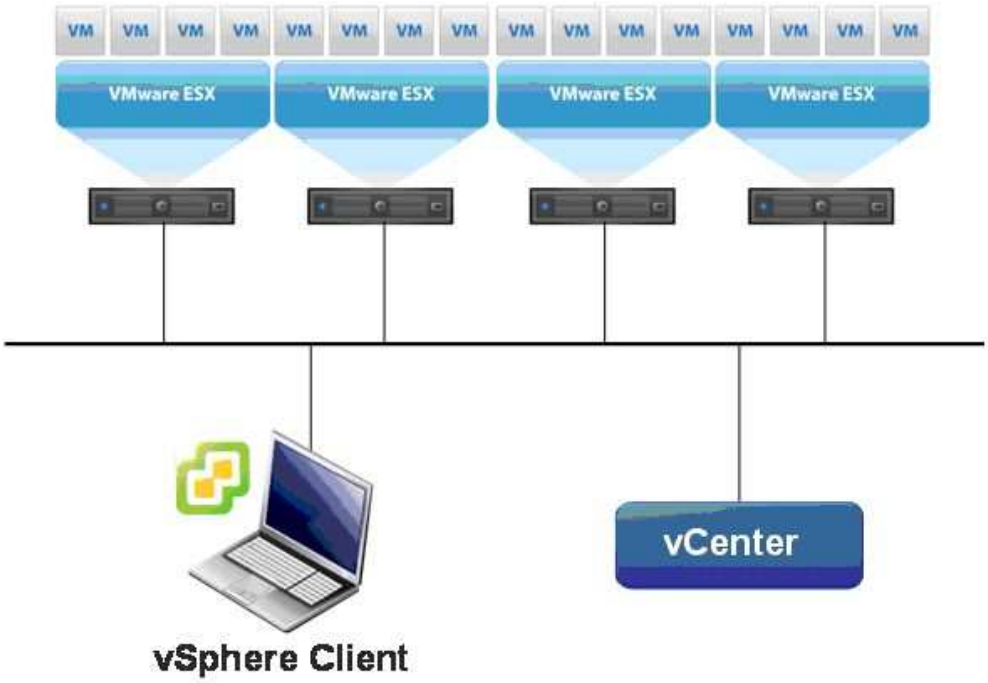


Fig. 2.4 Gestión de VMware ESXi mediante vSphere Client.

CAPÍTULO 3

3 IMPLEMENTACIÓN

3.1 INTRODUCCION

En una PYME con VMware ESXi proporciona una forma rápida de disminuir los gastos generales y simplificar las operaciones de negocios al permitir que funcionen múltiples sistemas operativos y aplicaciones en un solo servidor, gastando menos dinero en hardware, energía y enfriamiento, así como en la administración del servidor.

Las Pymes pueden manejar una gran afluencia en la cantidad de servidores o realizar la consolidación virtual a la vez que ahorran tiempo, dinero y recursos durante el proceso.

La administración será centralizada donde se podrán gestionar los sistemas operativos con los servicios instalados y así poder monitorear el rendimiento cuando todos los usuarios estén haciendo peticiones hacia los servicios. El propósito de esta implementación es disminuir recursos que se utilizan con varios servidores (uno para cada servicio), integrando todo virtualizado bajo un solo hardware sobre una plataforma robusta como ESXi.

3.2 HARDWARE

Para virtualizar es muy importante los recursos de hardware, principalmente memoria RAM, procesador y disco duro. Al ser el recurso principal donde se hospedan todos los sistemas operativos de servidor con las aplicaciones importantes de una empresa, debe estar disponible siempre para los clientes y no sufrir de retrasos cuando se hagan peticiones o consultas.

3.2.1 SERVIDOR PARA VIRTUALIZAR

Para esta implementación consideramos un hardware con las siguientes características:

Tabla I Características de hardware para Virtualizar

PROCESADOR	MEMORIA RAM	DISCO DURO	INTERFAZ DE RED
INTEL CORE I5, 2.67 GHZ	8 GB	640 GB	10/100/1000

3.2.2 SISTEMAS OPERATIVOS

La elección de la mejor plataforma para virtualizar es crucial al momento de implementar una infraestructura virtualizada. Por lo general en una Pyme se tienen sistemas operativos licenciados y open source. VMWare ha facilitado con el tema de licenciamiento para Pymes, ya que su distribución de Workstation y ESXi para virtualizar no tienen costo y son robustas ya que se pueden virtualizar diversos sistemas operativos con sus respectivas aplicaciones comunes. Para la implementación hemos considerado los siguientes sistemas operativos:

Tabla III Sistemas Operativos implementados

SISTEMA OPERATIVO	VERSION
VMWARE WORKSTATION	7
VMWARE ESXi	4.1
VMWARE VSPHERE CLIENT	4.0
WINDOWS SERVER	2003
WINDOWS XP	2002 SP3
CENTOS SERVER	5.3

3.3 INSTALACIÓN

Antes de comenzar la instalación debemos tener listo el hardware donde se van a montar todos los sistemas virtualizados. Este equipo debe tener un Sistema Operativo tipo servidor que sea robusto y tenga compatibilidad con diferentes aplicaciones. Para nuestro todo se va a instalar sobre Windows 7 Ultimate. Sobre una sola partición principal podemos trabajar, ya que con el ESXi a cada máquina virtual creada le vamos a dar un tamaño en disco mínimo dependiendo de la aplicación que este sobre cada sistema virtualizado. Este valor depende del tamaño de cada PYME, de la cantidad de usuarios que tenga y del tipo de negocio que se dedique.

3.3.1 INSTALACIÓN DE VMWARE WORKSTATION

Esta distribución la podemos descargar si costo (debemos registrarnos para que nos otorguen una licencia) desde la página oficial de WMware. A continuación se detalla el paso a paso de la instalación [1]:

Paso 1

Para empezar con la instalación de VMware Workstation 7 ejecutamos el programa de instalación ***VMware-workstation-full-7.1.4-385536.exe***,

transcurridos unos segundos nos aparecerá una ventana del asistente de instalación del VMware Workstation 7 como muestra la (Fig. 3.1):

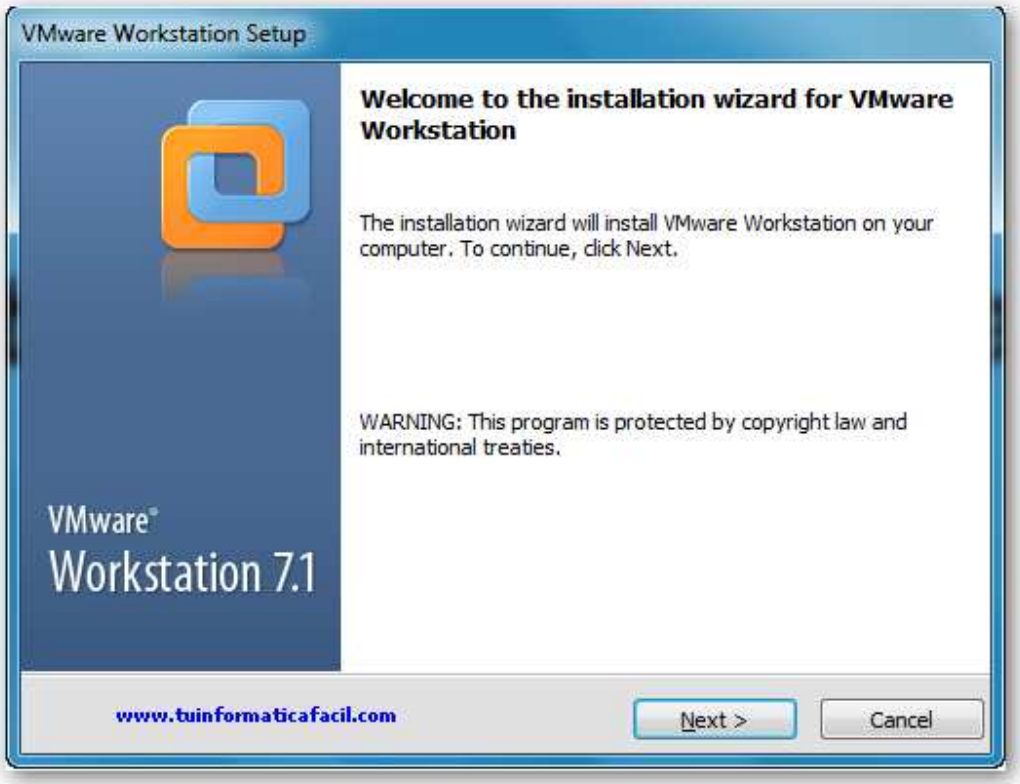


Fig. 3.1 Pantalla de instalación inicial

Paso 2

La primera ventana del proceso de instalación nos brinda dos posibilidades para determinar cómo queremos realizar la instalación (Fig. 3.2), Typical, esta opción realizará la instalación de los componentes mínimos y necesarios para poder

trabajar con VMware Workstation 7, Custom, con esta opción podemos decidir la instalación de complementos o funciones adicionales para poder usar funcionalidades específicas.

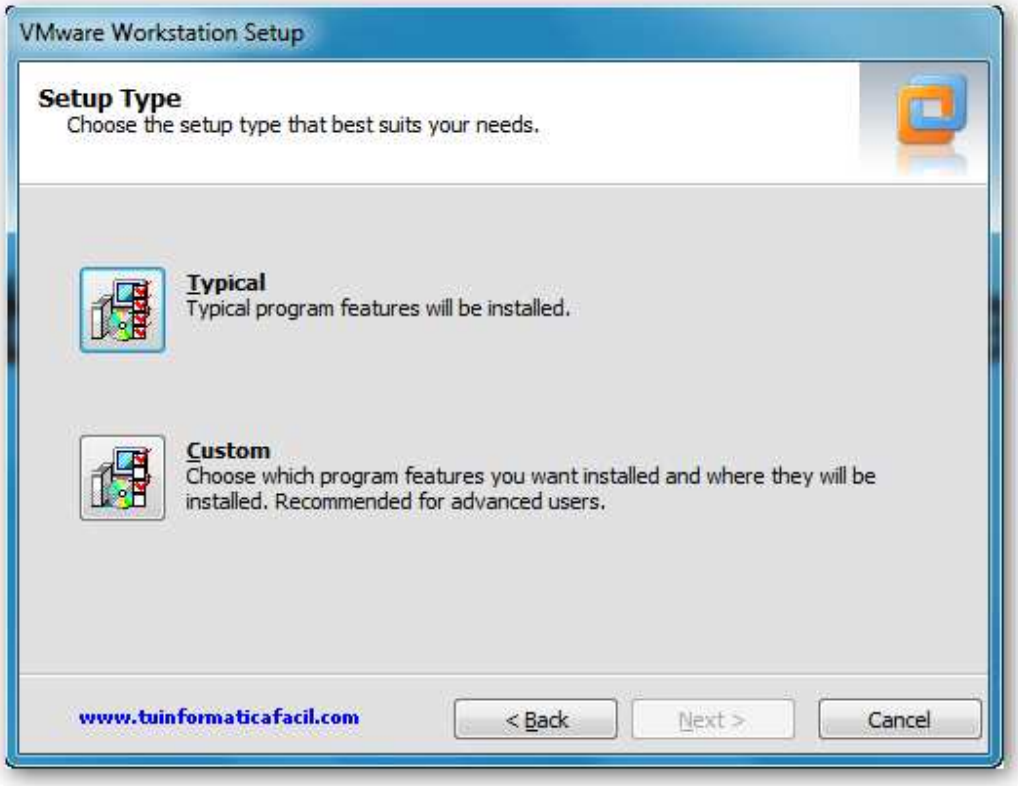


Fig. 3.2 Pantalla de selección del tipo de instalación

Paso 3

Seleccionamos la opción Typical, ahora nos aparece la información sobre el directorio donde se va a instalar el software VMware Workstation 7, si lo deseamos podemos cambiar el directorio destino pulsando en el botón Change (Fig. 3.3) y luego Next para modificar.

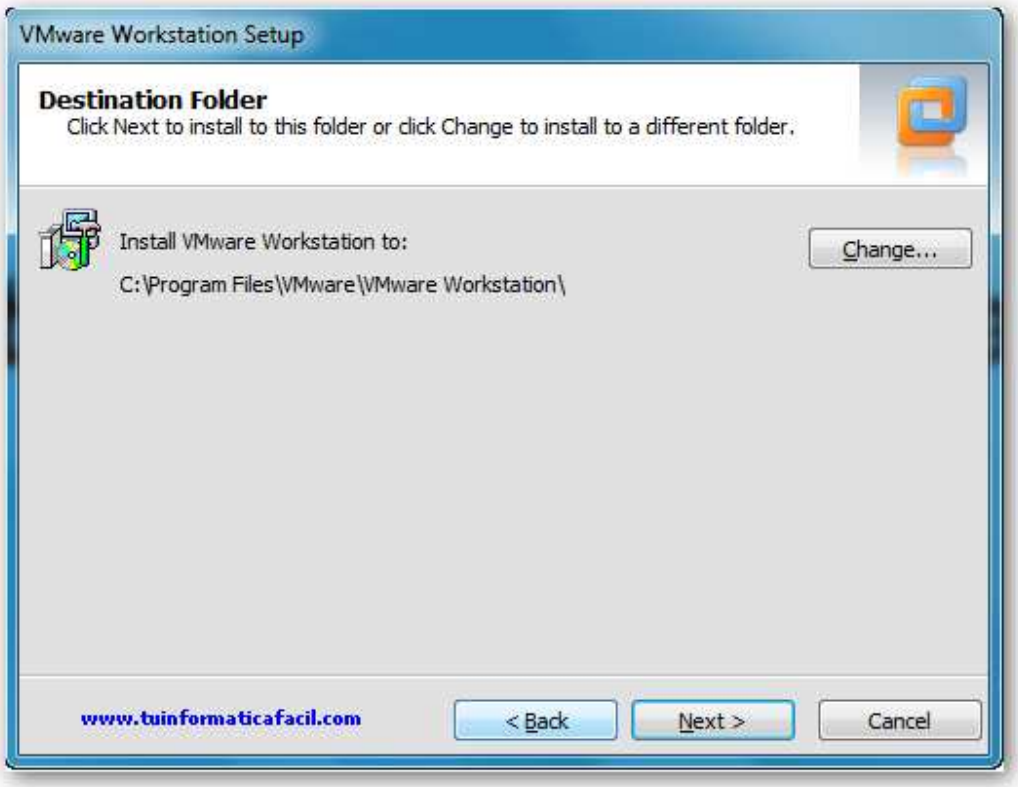


Fig. 3.3 Selección de cambio de directorio

Paso 4

Software update**,** por defecto aparece seleccionada la opción 'Check for product updates on startup' (Fig. 3.4), esta opción hará que cada vez que arranque el VMware Workstation 7 realizará una comprobación sobre si hay actualizaciones del software, si no deseamos que realice esta operación desmarcamos esta opción y seleccionamos Next.

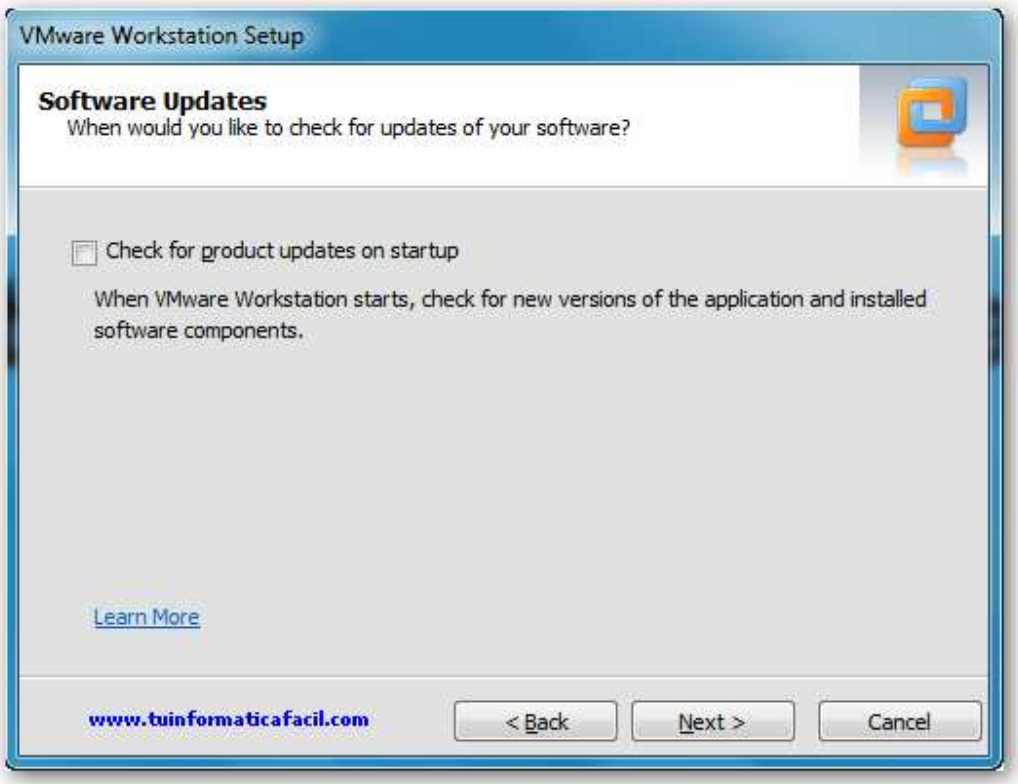


Fig. 3.4 Pantalla de selección de actualizaciones

Paso 5

User Experiences (Fig. 3.5), esta opción habilita a VMware Workstation 7 enviar información de tu sistema para labores de análisis de rendimiento, si no se necesita esta opción la desmarcamos. Seleccionamos Next para continuar.

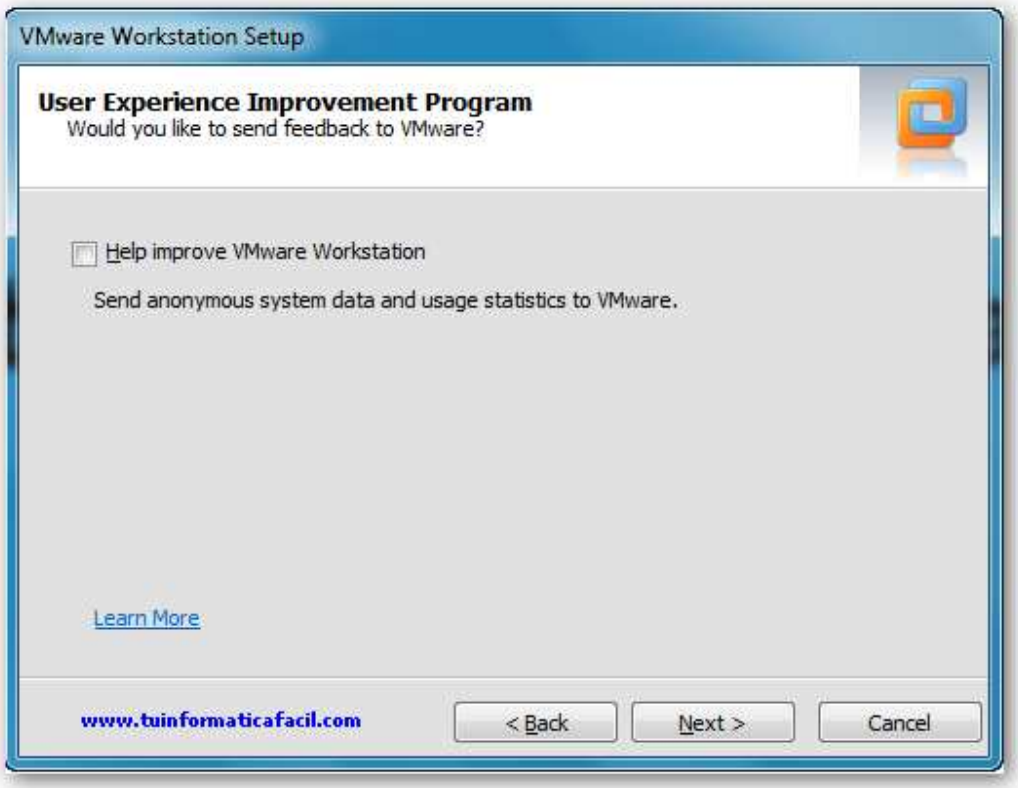


Fig. 3.5 Pantalla de selección para experiencia de usuario

Paso 6

Shortcuts (Fig. 3.6), aquí el asistente de instalación creará los iconos en el escritorio, la carpeta de inicio y la barra de inicio rápido.

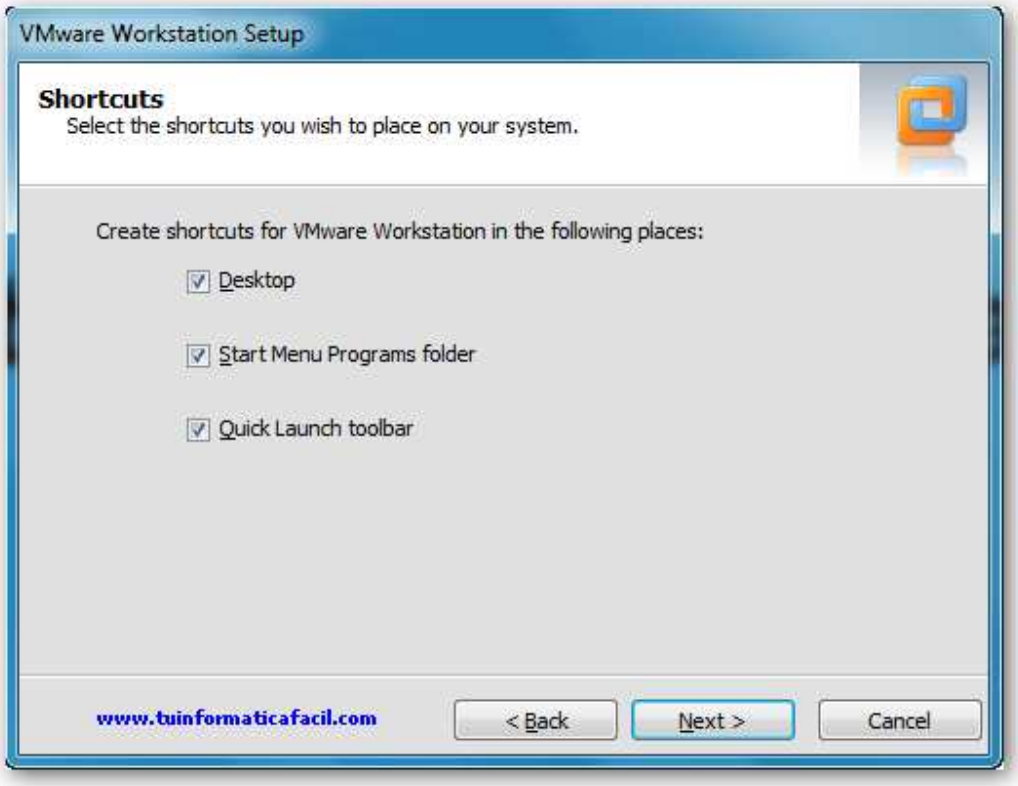


Fig. 3.6 Pantalla de creación de accesos directos

Paso 7

El asistente nos informa que está preparado para realizar la instalación (Fig. 3.7), pulsamos continue y comenzará la instalación.

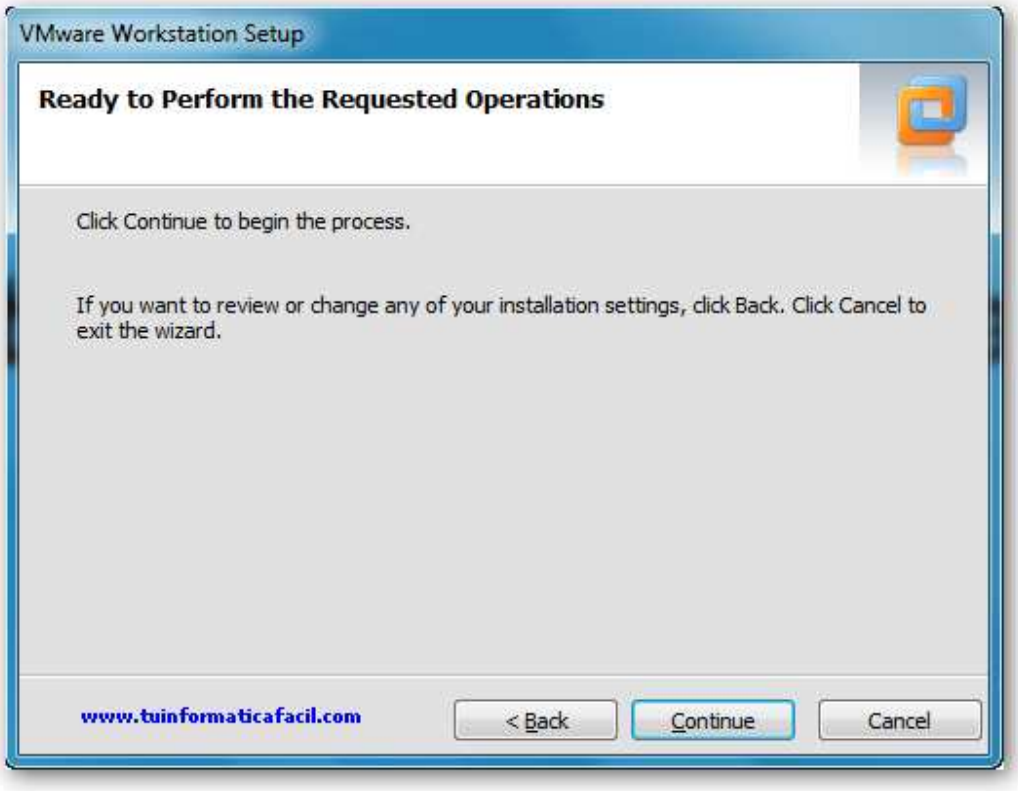


Fig. 3.7 Pantalla para iniciar la instalación.

Paso 8

Cuando ha finalizado la fase de instalación del software nos aparece una ventana donde se debe introducir una licencia (Fig. 3.8) y pulsamos el botón Enter, en caso de no tener una licencia pulsamos el botón Skip y continuamos.

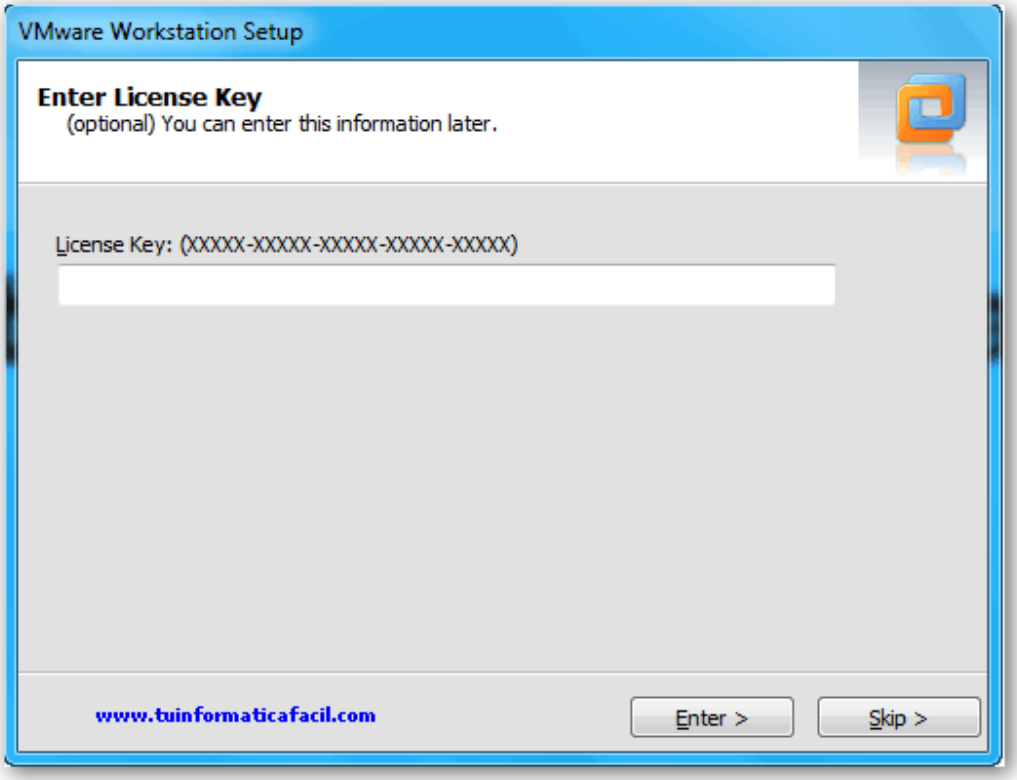


Fig. 3.8 Pantalla para introducir una licencia valida

Paso 9

Al finalizar la instalación debemos reiniciar el equipo para que tengan efecto todos los cambios y podamos empezar a trabajar (Fig. 3.9).

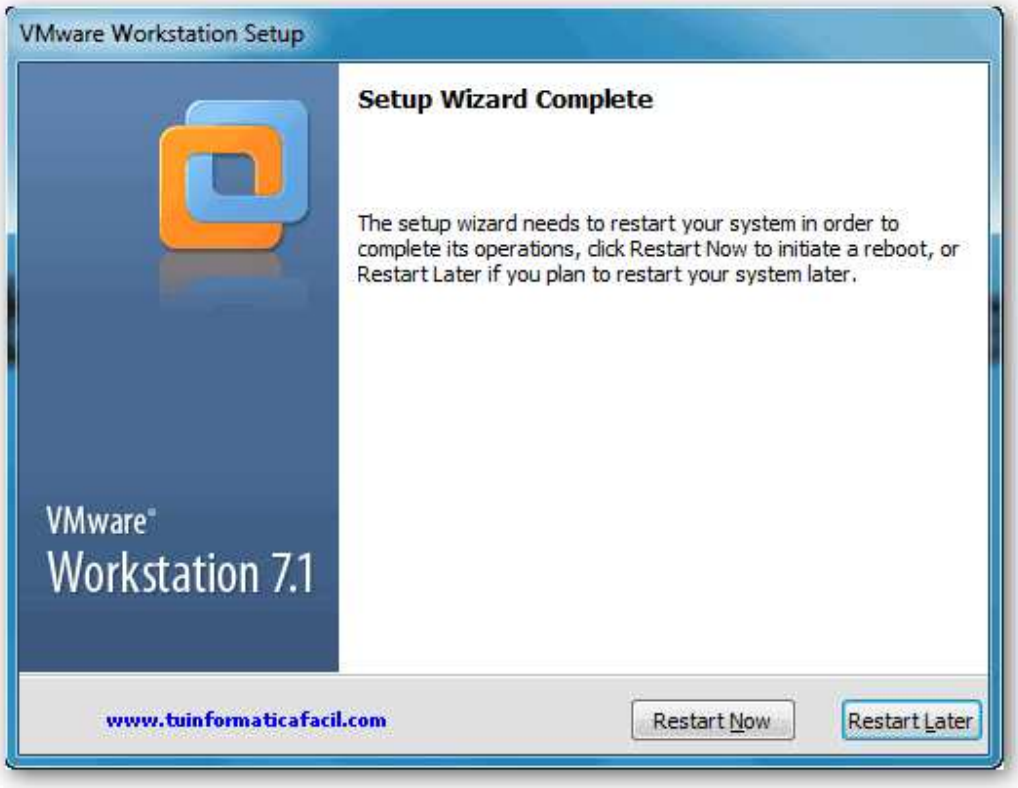


Fig. 3.9 Pantalla de finalización de la instalación.

Paso 10

Cuando ejecutamos por primera vez VMware Workstation 7 nos aparece una ventana con los términos de la licencia, marcamos “Yes” y pulsamos OK para continuar empezar a trabajar (Fig. 3.10).

Fig. 3.10 Pantalla de términos de licencia

3.3.2 INSTALACIÓN DE VMWARE ESXi

Antes de comenzar la instalación debemos tener en consideración algunos puntos como: revisar la guía de compatibilidad, descargar la imagen ISO desde la página oficial de VMware (hay que registrarse para que nos otorguen una licencia sin costo) y grabar en un cd la imagen. Al arrancar el servidor debemos introducir el CD con el ESXi y debemos seguir los siguientes pasos de instalación [2]:

Paso 1

Cuando bootea el CD nos aparece el menú de arranque con una opción (Fig. 3.11).

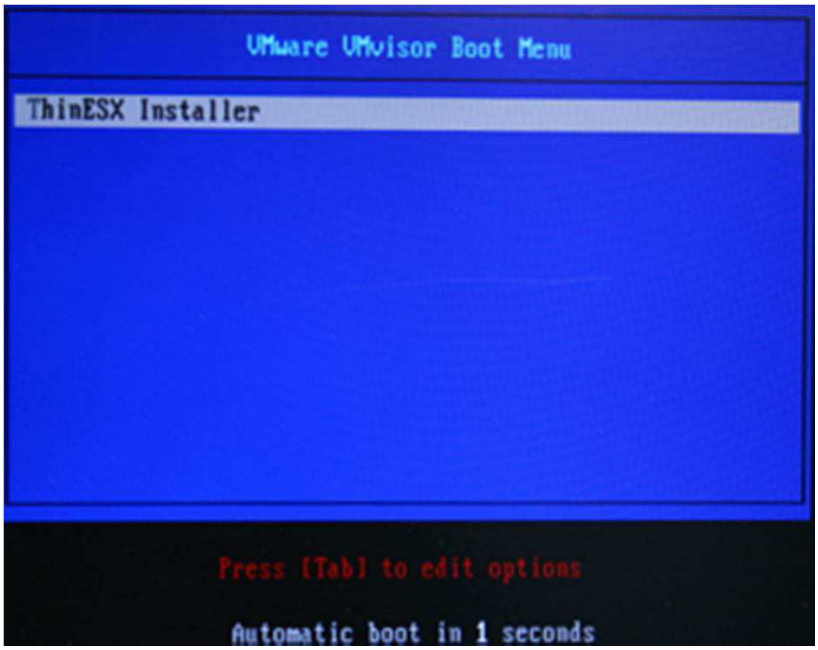


Fig. 3.11 Menú de arranque de VMware VMvisor

Paso 2

De forma automática comienza el arranque del instalador (Fig. 3.12).

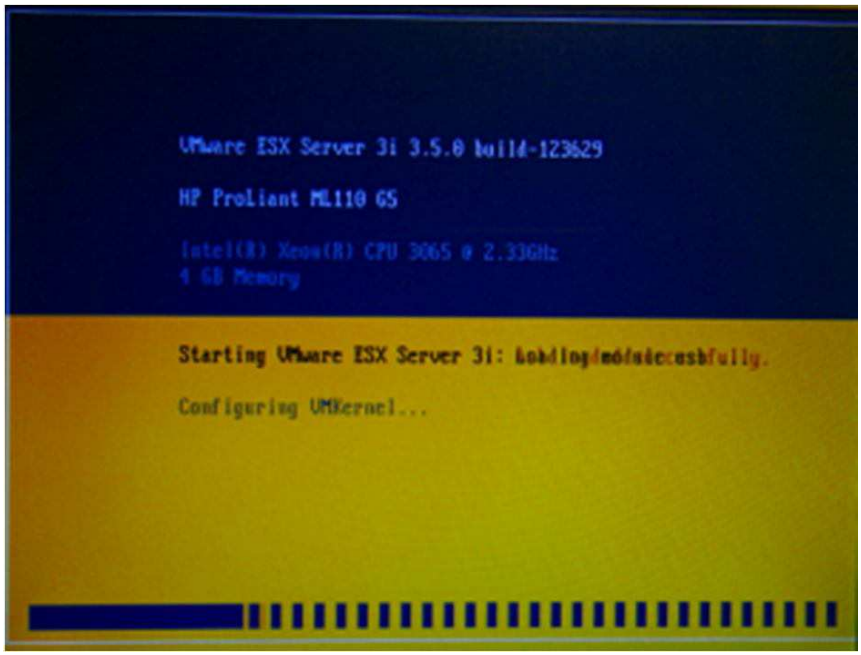


Fig. 3.12 Arrancando VMware ESXi

Paso 3

A continuación se nos pregunta por la operación que queremos realizar:

cancelar, reparar o instalar. Pulsando la tecla Intro seleccionamos instalar (Fig. 3.13).

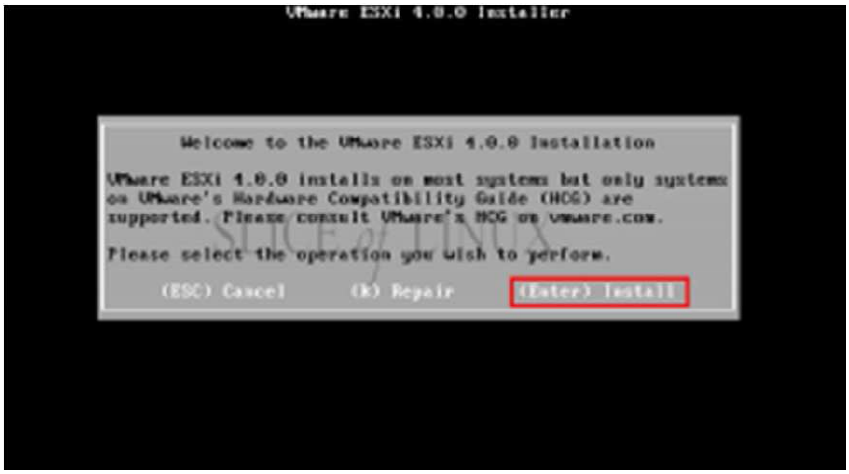


Fig. 3.13 Pantalla para seleccionar operación

Paso 4

El siguiente paso consiste en aceptar el EULA (End User License Agreement) después de leerlo para aceptarlo pulsamos la tecla F11 (Fig. 3.14).

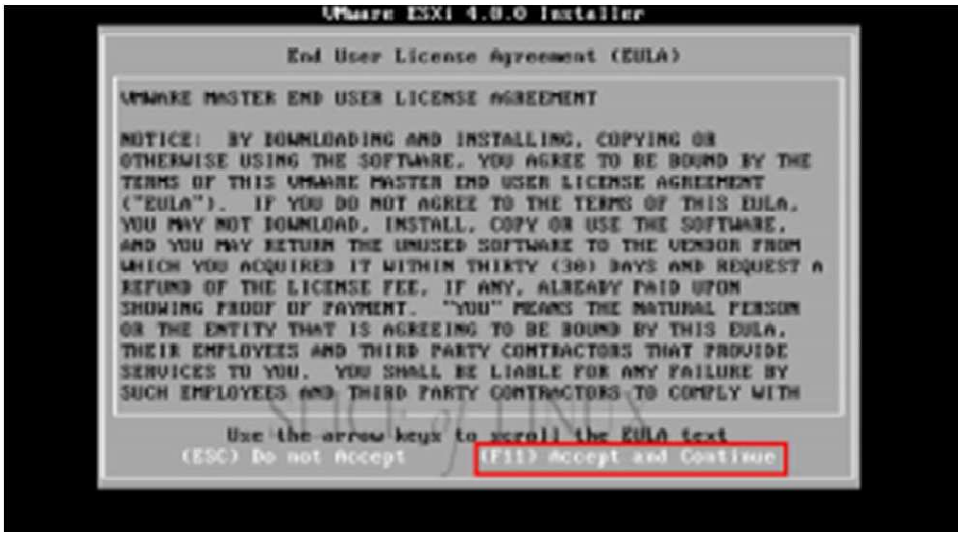


Fig. 3.14 Pantalla de EULA

Paso 5

Seleccionamos el disco duro donde se instalará el sistema (Fig. 3.15).

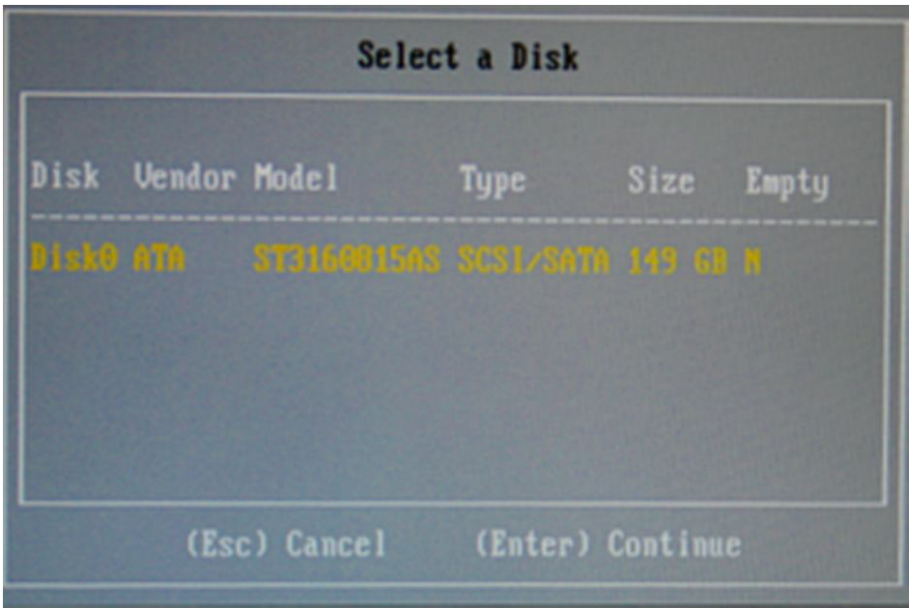


Fig. 3.15 Pantalla para selección de disco duro

Paso 6

Ahora confirmamos que vamos a instalar VMware ESXi en el disco que habíamos seleccionado. Lo hacemos pulsando F11 (Fig. 3.16)

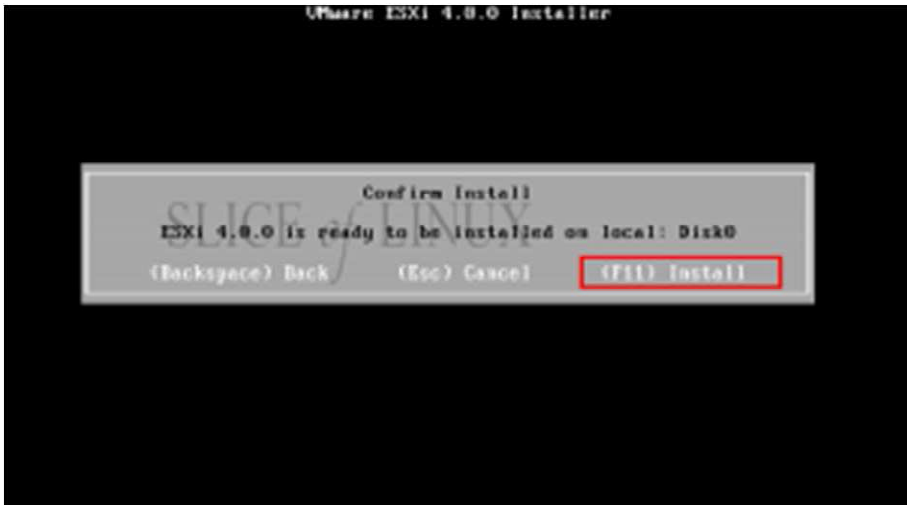


Fig. 3.16 Pantalla para confirmación de instalación.

Paso 7

La instalación se hace en muy poco tiempo, luego recibimos un mensaje de que se ha instalado correctamente y tenemos que reiniciar. Extraemos el CD y pulsamos Intro para reiniciar (Fig. 3.17).

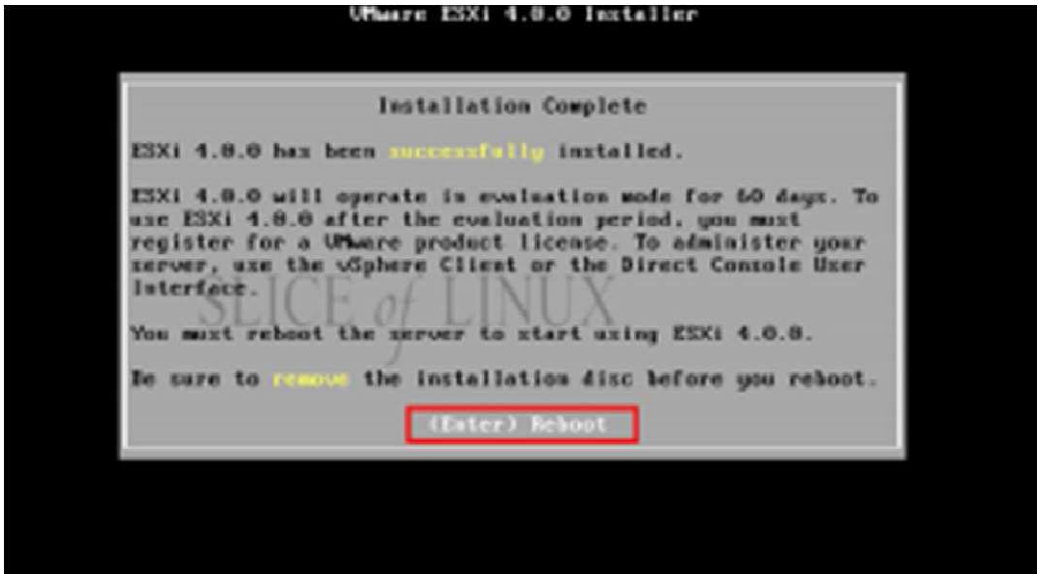


Fig. 3.17 Pantalla de instalación terminada.

Paso 8

Al reiniciar el sistema nos encontramos con la pantalla de inicio del VMware ESXi y antes de empezar a trabajar con él, deberemos configurarlo pulsando la tecla F2 (Fig. 3.18).

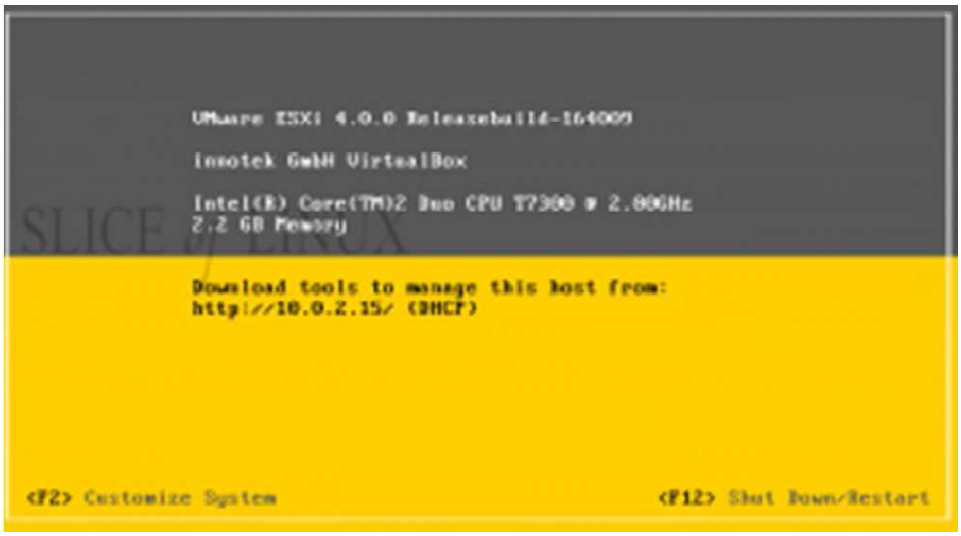


Fig. 3.18 Pantalla de inicio de VMware ESXi.

Paso 9

Lo primero que debemos hacer es establecer una contraseña para el usuario root que, por defecto, no la tiene. Para esto nos situamos sobre Configure Root Password y pulsamos Intro (Fig. 3.19).

Fig. 3.19 Pantalla de configuración.

Paso 10

Escribimos la nueva contraseña para el usuario root y pulsamos Intro (Fig. 3.20).

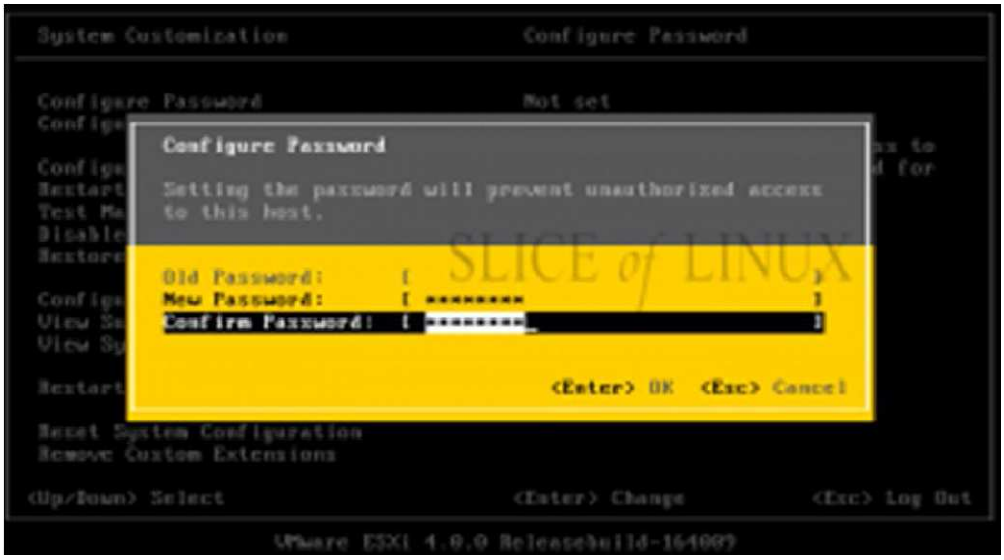


Fig. 3.20 Establecer la configuración de Root.

Paso 11

Ahora podemos cambiar la configuración de red. Es conveniente que la IP del VMware ESXi sea fija. Por lo tanto, nos situamos sobre Configure Management Network y pulsamos Intro (Fig. 3.21)

Fig. 3.21 Pantalla para cambiar la configuración de red.

Paso 12

A continuación seleccionamos Set static IP address and network configuration con la barra espaciadora y escribimos la nueva configuración. Para terminar pulsamos Intro (Fig. 3.22).

Fig. 3.22 Configuración de IP Estática.

Paso 13

Abrimos un navegador en el equipo con Windows y escribimos la dirección IP que hemos configurado en el servidor VMware ESXi. Así llegamos a la página de bienvenida del servidor ESXi (Fig. 3.23).

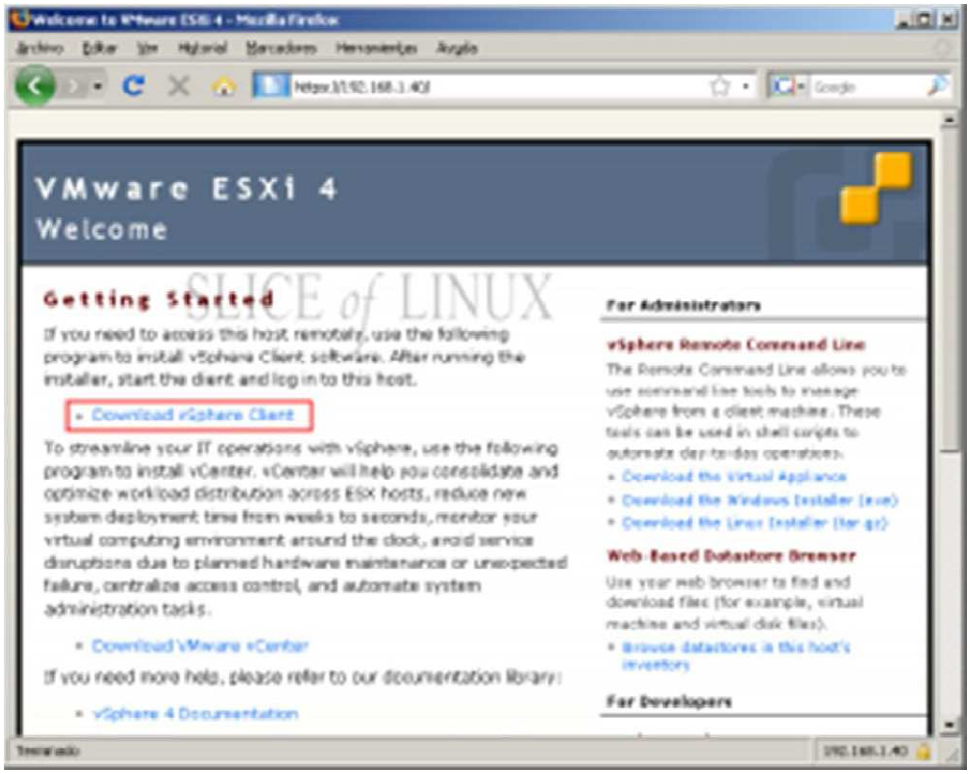


Fig. 3.23 Pantalla de bienvenida a WMware ESXi.

3.3.3 INSTALACIÓN DE VMWARE VSPHERE CLIENT

Desde la página de bienvenida del servidor VMware ESXi 4 podemos obtener el programa que nos va a permitir la administración completa del servidor de forma remota. Debemos seguir los siguientes pasos [3]:

Paso 1

Seleccionamos la opción de Download vSphere Client y procedemos a la descarga del archivo (Fig. 3.24).

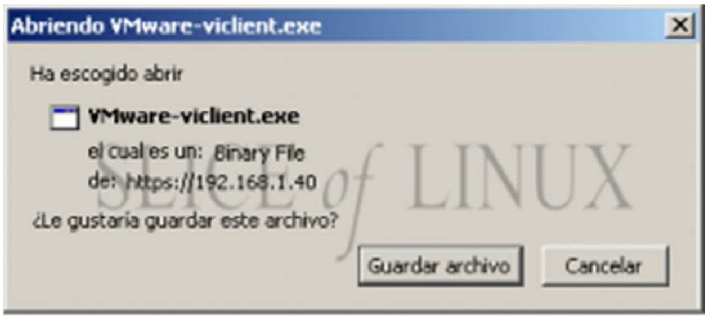


Fig. 3.24 Descarga del archivo Vsphere client

Paso 2

Una vez descargado el archivo, para instalar VMware vSphere Client sólo tenemos que seleccionar el idioma (Fig. 3.25).

Fig. 3.25 Elección de idioma de instalación.

Paso 3

Una vez instalado ejecutamos VMware vSphere Client y nos aparece la ventana para establecer la conexión y en la que deberemos introducir la IP del servidor ESXi, el nombre de usuario y la contraseña. En principio, sólo existe el usuario root con la contraseña que establecimos anteriormente (Fig. 3.26).

Fig. 3.26 Pantalla para la conexión del Client.

Paso 4

Al ingresar al vSphere Client se mostrara un mensaje de recordatorio sobre el número de días del periodo de prueba que nos quedan. Sí, VMware ESXi 4 es gratis pero necesita de un número de licencia. (Fig. 3.27).

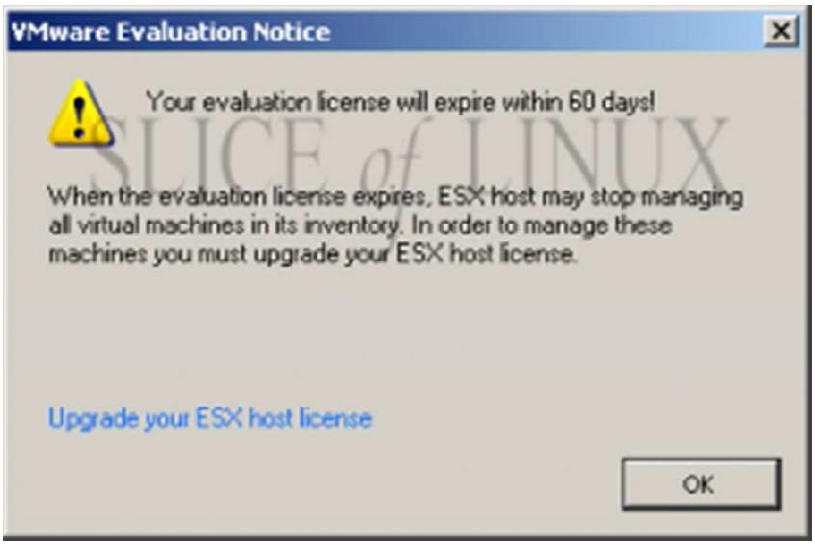


Fig. 3.27 Números de días de prueba restantes.

Paso 5

Debemos introducir el código de licencia seleccionado en inventory (Fig. 3.28).

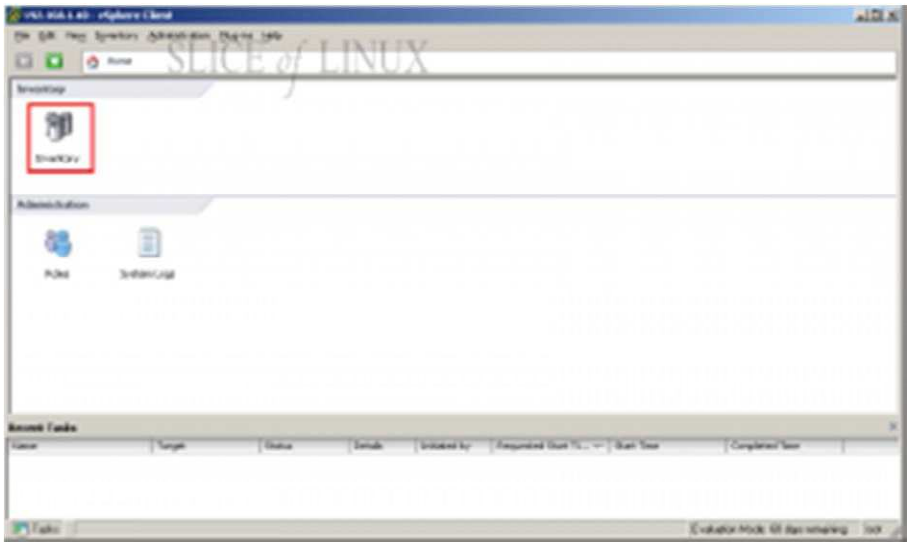


Fig. 3.28 Pantalla de inventory para introducir la licencia.

Paso 6

En el panel de la izquierda de Inventory nos muestra la IP de nuestro servidor y a la derecha un conjunto bastante amplio de pestañas. Seleccionamos sobre la pestaña Configuration (Fig. 3.29).

Fig. 3.29 Pantalla para seleccionar configuration.

Paso 7

Desde configuration seleccionamos Licensed Features en la sección de Software y, a continuación, seleccionamos en Edit (Fig. 3.30).

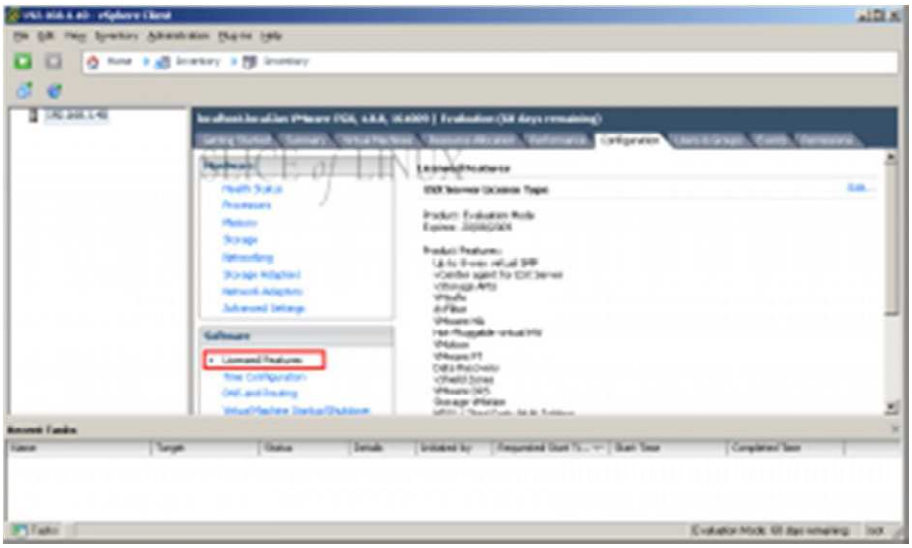


Fig. 3.30 Pantalla de Licensed Features.

Paso 8

Luego nos aparecerá una ventana en la que seleccionamos Assign a new license key to this host y seleccionamos sobre Enter Key (Fig. 3.31).

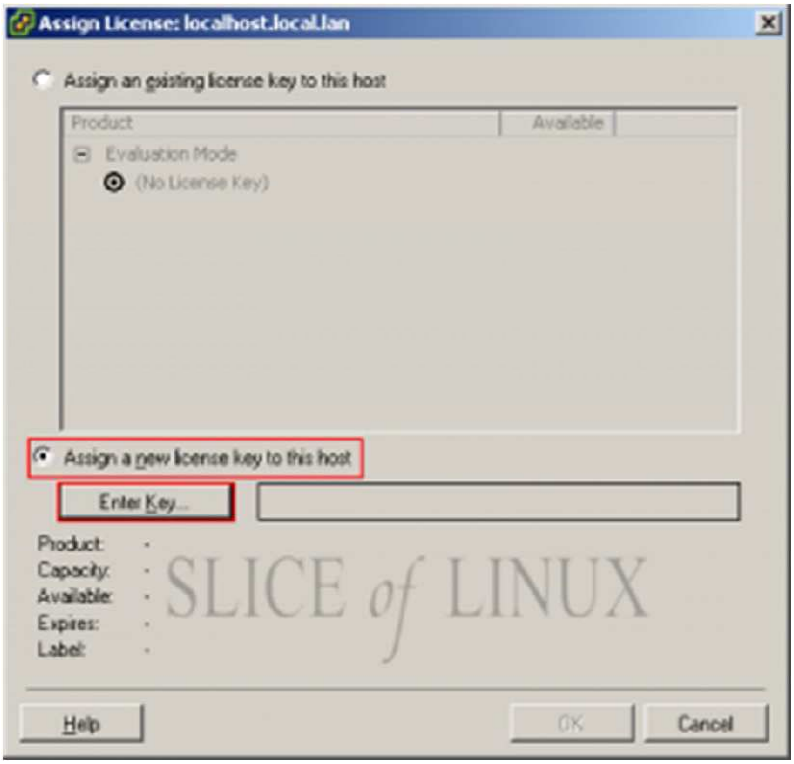


Fig. 3.31 Pantalla para el ingreso de licencia al host.

Paso 9

Escribimos el código de licencia que nos proporciona VMware y seleccionamos en OK (Fig. 3.32).

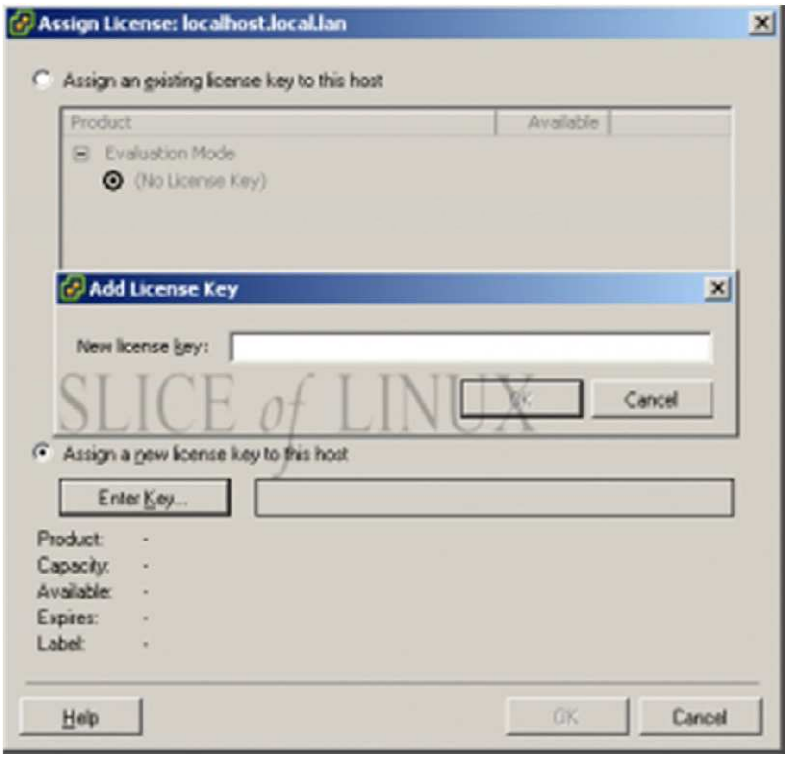


Fig. 3.32 Ventana para añadir el número de licencia válido.

Paso 10

Observamos las características de la licencia introducida y seleccionamos OK (Fig. 3.33). Luego de este punto ya podemos empezar a crear máquinas virtuales a través de VMware VSphere Client y administrar el server de forma remota.

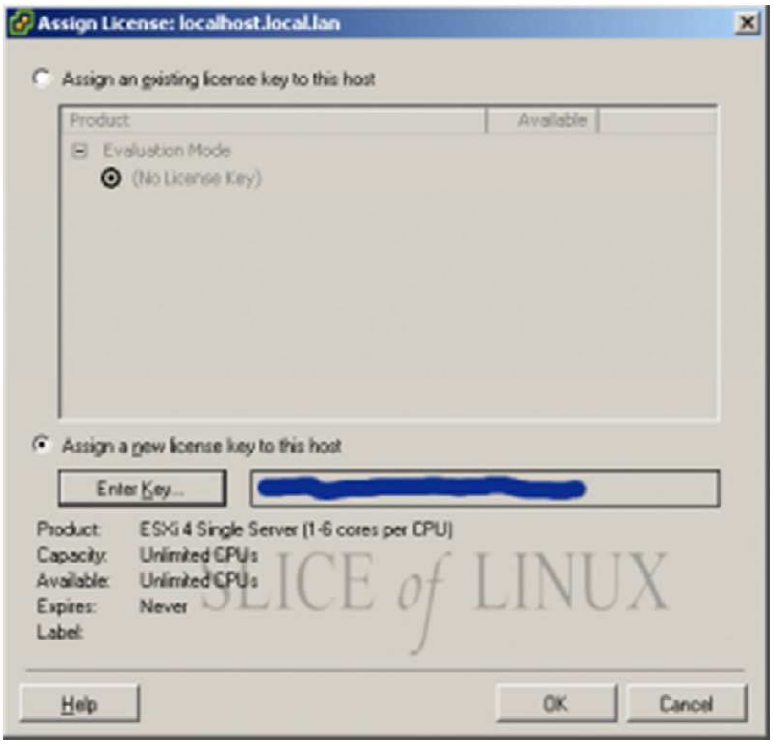


Fig. 3.33 Información sobre la licencia introducida.

3.3.4 SQUID PROXY

El Squid Proxy lo vamos a instalar y configurar bajo Centos 5.4 que es una distribución de Linux para servidores muy estable. En la ventana de terminal del Centos ejecutamos los siguientes comandos [4]:

Procederemos a instalar el Squid:

[root@proxycliente ~]# yum install squid

Configuramos el servicio:

[root@proxycliente ~]# vi /etc/squid/squid.conf

Nos dirigimos a la siguiente línea para habilitar el puerto a utilizar:

 # Default: http_port 3128

http_port 3128

Configuraremos el cache de memoria con la siguiente línea:

cache_mem 16 MB

Modificamos el espacio que tendrá nuestro cache. El valor 100, quiere decir que dispondremos de 100MB de cache en nuestro disco, podemos aumentarlo si deseamos almacenar más cache y usar menos ancho de banda, no es recomendable modificar los otros valores:

cache_dir ufs /var/spool/squid 100 16 256

Procederemos ahora a crear la ACL, con la cual permitiremos la navegación a la red LAN. Por lo cual nos dirigiremos a la siguiente ubicación en el archivo:

#Recommended minimum configuration:

acl all src 0.0.0.0/0.0.0.0

acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255

acl to_localhost dst 127.0.0.0/8

Debajo de la línea “acl manager proto cache_object” ingresamos lo siguiente:

acl [nombre de la lista] src [IP de la red/mask, “red lan interna”]

acl localnet src 172.16.12.0/255.255.255.0

Una vez creada la regla procederemos a darle permiso, por lo cual nos dirigiremos a la siguiente ubicación:

 # And finally deny all other access to this proxy

http_access allow localhost

http_access deny all

Debemos tener en cuenta que el orden de las reglas es importante, por lo cual ingresaremos la siguiente línea:

http_access allow “nombre_de_acl_creada”

 # And finally deny all other access to this proxy

http_access allow localhost

http_access allow localnet

http_access deny all

Una vez hecha la configuración procederemos a guardar.

Ahora crearemos el espacio swap con el siguiente comando:

[root@proxycliente ~]# squid -z

2011/01/14 12:35:26| Creating Swap Directories

[root@proxycliente ~]#

Una vez creado el swap, iniciaremos el servicio, no debe aparecer ningún error:

root@proxycliente ~]# service squid start

Iniciando squid: . [OK]

Para confirma que se está ejecutando o saber si está arriba el servicio digitamos el siguiente comando:

[root@proxycliente ~]# service squid status

Se está ¡ejecutando squid (pid 3041)...

Si no tenemos ningún problema ahora ejecutaremos el siguiente comando para que al encender el servidor se ejecute automáticamente:

[root@proxycliente ~]# chkconfig squid on

En el web browser de las máquinas de los usuarios, en las opciones avanzadas debemos configurar para que navegue con dirección proxy, la misma que es la del Squid.

Para confirmar que estén navegando revisamos el log en la siguiente ubicación:

[root@proxycliente ~]# tail -f /var/log/squid/access.log

1295027189.407 782 172.16.1.2 TCP_MISS/200 658 GET http://www.eluniverso.com/versiones/v1/img/Global/fd_DgSolActGris.gif - DIRECT/200.7.198.3 image/gif

1295027189.515 633 172.16.1.2 TCP_MISS/200 812 GET http://www.eluniverso.com/versiones/v1/img/Global/fd_CvSolGris.gif - DIRECT/200.7.198.3 image/gif

1295027189.614 726 172.16.1.2 TCP_MISS/200 571 GET http://www.eluniverso.com/versiones/v1/img/Global/fd_CvBt.gif - DIRECT/200.7.198.3 image/gif

3.3.5 RESTRICCION DE ACCESO A SITIOS DE INTERNET

Al denegar el acceso a ciertos sitios de red permite hacer mejor uso del ancho de banda con el que se dispone. Esta configuración se la hace cuando ya se tiene un Squid proxy levantado, consiste en denegar el acceso a nombres de dominio o direcciones de Internet que contengan patrones en común.Debemos ejecutar los siguientes comandos [5]:

Se debe crear un archivo donde se definirá la lista de expresiones:

vim /etc/squid/listas/expreg-denegadas

Esta lista puede contener cualquier expresión regular que se considere sea usualmente utilizadas en las direcciones de ciertos sitios:

adult

celebri

mp3

otrositioindeseable.com

playstation

porn

sex

sitioindeseable.com

taringa

torrent

warez

wii

Esta lista, la cual deberá ser completada con todas las palabras consideradas prohibidas y direcciones de Internet que se consideren pertinentes, la guardaremos como /etc/squid/listas/expreg-denegadas.

Debemos editar el archivo /etc/squid/squid.conf.

Añadimos una lista de control, denominada expreg-denegadas, de acceso tipo url_regex (expresiones regulares del URL), que defina la lista en el archivo /etc/squid/listas/expreg-denegadas:

acl expreg-denegadas url_regex "/etc/squid/listas/expreg-denegadas"

Debemos tener en la sección de Listas de Control de Acceso algo similar a lo siguiente:

#

 # Recommended minimum configuration:

acl all src 0.0.0.0/0

acl manager proto cache_object

acl localhost src 127.0.0.1/8

acl localnet src 192.168.1.0/24

acl password proxy_auth REQUIRED

acl expreg-denegadas url_regex "/etc/squid/listas/expreg-denegadas"

Modificamos una Regla de Control de Acceso existente agregando con un símbolo de ! que se denegará el acceso a la Lista de Control de Acceso denominada expreg-denegadas:

http_access allow localnet !expreg-denegadas

La regla anterior permite el acceso a la Lista de Control de Acceso denominada localnet, niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Acceso denominada expreg-denegadas.

Reglas de control de acceso: denegación de sitios.

#

 # INSERT YOUR OWN RULE(S) HERE TO allow ACCESS FROM YOUR CLIENTS

#

http_access allow localhost

http_access allow localnet password !expreg-denegadas

http_access deny all

Para restringir el acceso por dominios, se crea un archivo con lista con dominios:

vim /etc/squid/listas/dominios-denegados

Los nombres pueden ser nombres de dominio específicos:

www.facebook.com

www.twitter.com

plus.google.com

www.eluniverso.com

www.hotmail.com

Editamos el archivo /etc/squid/squid.conf:

vim /etc/squid/squid.conf

Añadimos una lista de control, denominada dominios-denegados, de acceso tipo dstdomain (dominios de destino), que defina la lista en el archivo /etc/squid/listas/dominios-denegados:

acl dominios-denegados dstdomain "/etc/squid/listas/dominios-denegados"

Incluimos una regla de control de acceso que deniegue el acceso a sitios que estén incluidos en la lista de dominios:

http_access allow localnet !expreg-denegadas !dominios-denegados

Debemos permitir el acceso a sitios particulares de internet, utilizamos el editor de texto para crear el archivo /etc/squid/dominios-permitidos:

vim /etc/squid/dominios-permitidos

El contenido puede ser una lista de dominios, o bien dominios de nivel superior, que se considere deban ser accedidos por la red local en cualquier momento, y sin restricciones:

.alcancelibre.org

.edu

.edu.ec

.extra.ec

.gob

.gov

.milenio.com

.org

.unam.mx

www.google.com

Este archivo será definido en una Lista de Control de Acceso del mismo modo en que se hizo con el archivo que contiene dominios y palabras denegadas:

acl dominios-permitidos dstdomain "/etc/squid/dominios-permitidos"

Para hacer uso del archivo, se debe utilizar la expresión ! en la misma línea utilizada para la Regla de Control de Acceso establecida para denegar el mismo:

http_access allow all dominios-inocentes

Finalmente, hay que reiniciar la configuración de Squid para que tomen efecto los cambios, y se puedan realizar pruebas:

service squid reload

3.3.6 SENDMAIL Y DOVECOT

Para que los usuarios puedan enviar y recibir correos vamos a configurar un servidor local que se encargue de estas operaciones, al ser una Pyme podemos trabajar sobre el mismo servidor que hace Proxy ya que la cantidad de usuarios no justifica colocar un equipo independiente, solo debemos dejar una partición de disco donde se almacenaran los correos por un período de tiempo determinado. Todas las cuentas de correo estarán almacenadas en el servidor y se deberán configurar user y password para cada cliente que utilice el servicio. Ejecutando los siguientes comandos podemos levantar nuestro servidor de correos [6]:

Para la instalación ejecutamos el comando:

yum -y install sendmail sendmail-cf dovecot m4 make cyrus-sasl cyrus-sasl-md5 cyrus-sasl-plain

Creamos usuarios a través del método de autenticación para SMTP, Sendmail utilizará SASL. Por tal motivo, las cuentas de usuario de correo deberán de seguir el siguiente procedimiento:

useradd -s /sbin/nologin ricardo

Asignamos claves de acceso en el sistema para permitir autenticar a través de los métodos PLAIN y LOGIN para autenticar SMTP y a través de los protocolos POP3 e IMAP:

passwd ricardo123

La autenticación para SMTP a través de cualquier mecanismo requiere se active e inicie el servicio de saslauthd del siguiente modo:

chkconfig saslauthd on

service saslauthd start

Establecemos los dominios que vamos administrar en el fichero /etc/mail/local-host-names del siguiente modo:

dominio.com

mail.dominio.com

dominio2.com

mail.dominio2.com

Configuramos los dominios permitidos para poder enviar correo con la línea:

vi /etc/mail/relay-domains

Por defecto, no existe dicho fichero, hay que generarlo. Para fines generales tiene el mismo contenido de /etc/mail/local-host-names a menos que se desee excluir algún dominio en particular:

dominio.com

mail.dominio.com

dominio2.com

mail.dominio2.com

Definimos la lista de control de acceso en:

vi /etc/mail/access

Incluimos solo las direcciones IP locales del servidor, y la lista negra de direcciones de correo, dominios e IPs denegadas. Considerando que cualquier IP que vaya acompañada de RELAY se le permitirá enviar correo sin necesidad de autenticar, lo cual puede ser útil si se utiliza un cliente de correo con interfaz HTTP (Web mail) en otro servidor:

 # Check the /usr/share/doc/sendmail/README.cf file for a description

of the format of this file. (search for access_db in that file)

 # The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc

 # package.

#

 # by default we allow relaying from localhost...

localhost.localdomain RELAY

localhost RELAY

127.0.0.1 RELAY

#

 # Dirección IP del propio servidor.

192.168.1.254 RELAY

#

 # Otros servidores de correo en la LAN a los que se les permitirá enviar

 # correo libremente a través del propio servidor de correo.

192.168.1.253 RELAY

192.168.1.252 RELAY

#

 # Direcciones IP que solo podrán entregar correo de forma local, es decir,

 # no pueden enviar correo fuera del propio servidor.

192.168.2.24 OK

192.168.2.23 OK

192.168.2.25 OK

#

 # Lista negra

usuario@spam.com REJECT

spam.com.ec REJECT

10.4.5.6 REJECT

#

 # Bloques de Asia Pacific Networks, ISP desde el cual se emite la mayor

 # parte del Spam del mundo.

 # Las redes involucradas abarcan Australia, Japón, China, Korea, Taiwan,

 # Hong Kong e India por lo que bloquear el correo de dichas redes significa

 # cortar comunicación con estos países, pero acaba con entre el 60% y 80%

 # del Spam.

222 REJECT

221 REJECT

220 REJECT

219 REJECT

218 REJECT

212 REJECT

211 REJECT

210 REJECT

203 REJECT

202 REJECT

140.109 REJECT

133 REJECT

61 REJECT

60 REJECT

59 REJECT

58 REJECT

No es conveniente estar autenticando la cuenta de root a través de la red para revisar los mensajes originados por el sistema. Se debe definir alias para la cuenta de root a donde re-direccionar el correo en el fichero /etc/aliases del siguiente modo:

root: albertoadm

Es muy común usar archivos planos para hacer una lista de los usuarios a los que quisiéramos enviar un mail, para eso hay que modificar el fichero /etc/aliases y colocar lo siguiente al final:

administracion::include:/etc/depadministracion.txt

Luego para refrescar los alias de sendmail es necesario ejecutar el siguiente comando:

Newaliases

Modificamos el fichero /etc/mail/sendmail.mc para habilitar o desactivar funciones de sendmail:

vi /etc/mail/sendmail.mc

El parámetro **confSMTP_LOGIN_MSG** permite establecer el mensaje de bienvenida al establecer la conexión al servidor. Es posible ocultar el nombre y al versión de sendmail, esto con el objeto de agregar seguridad por secreto. Funciona simplemente haciendo que quien se conecte hacia el servidor no pueda saber que software y versión del mismo se está utilizando. Se recomienda utilizar lo siguiente:

define(`confSMTP_LOGIN_MSG',`$j ; $b')dnl

Se realiza una conexión hacia el puerto 25 del servidor:

$ telnet 127.0.0.1 25

Trying 127.0.0.1...

Connected to nombre.dominio.

Escape character is '^]'.

220 nombre.dominio ESMTP ; Mon, 17 May 2004 02:22:29 -0500

quit

221 2.0.0 nombre.dominio closing connection

Connection closed by foreign host.

$

Utilizando la siguiente línea confAUTH_OPTIONS, permitirá realizar autenticación a través del puerto 25 por cualquier método, incluyendo PLAIN, el cual se realiza en texto simple. Esto implica cierto riesgo de seguridad:

define(`confAUTH_OPTIONS',`A')dnl

De modo predefinido Sendmail escucha peticiones a través de la interfaz de loopback 127.0.0.1 y no a través de otros dispositivos de red. Solo se necesita eliminar las restricciones de la interfaz de loopback para poder recibir correo desde Internet o la LAN. Localizamos la siguiente línea:

DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl

Eliminamos el valor Addr=127.0.0.1 y la coma (,) que le antecede, del siguiente modo:

DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl

Se recomienda desactivar la siguiente función a fin de impedir aceptar correo de dominios inexistentes (generalmente utilizado para el envío de correo masivo no solicitado o Spam), solo basta comentar esta configuración precediendo un dnl, del siguiente modo:

dnl FEATURE(`accept_unresolvable_domains')dnl

Habilitamos las siguientes líneas para definir la máscara que utilizará el servidor para el tema de enmascaramiento:

MASQUERADE_AS(`dominio.com')dnl

FEATURE(masquerade_envelope)dnl

FEATURE(masquerade_entire_domain)dnl

Si se van a administrar múltiples dominios, declare los dominios que no se quiera enmascarar con el parámetro MASQUERADE_EXCEPTION del siguiente modo:

MASQUERADE_AS(`dominio.com')dnl

MASQUERADE_EXCEPTION(`dominio2.net')dnl

MASQUERADE_EXCEPTION(`dominio3.org')dnl

MASQUERADE_EXCEPTION(`dominio4.com.mx')dnl

FEATURE(masquerade_envelope)dnl

FEATURE(masquerade_entire_domain)dnl

Añadir al final del fichero /etc/mail/sendmail.mc un parámetro que defina que dominio.com se trata de un dominio local:

Cwdominio.com

Si se desea cargar listas negras para mitigar el Spam, pueden añadirse las siguientes líneas justo arriba de MAILER (smtp)dnl.

Se debe modificar el fichero /etc/dovecot.conf y habilitar los servicios de imap y/o pop3 del siguiente modo (de modo predefinido están habilitados imap e imaps):

 # Protocols we want to be serving:

 # imap imaps pop3 pop3s

protocols = imap pop3

El servicio se agrega al arranque del sistema y se inicia del siguiente modo:

chkconfig dovecot on

service dovecot start

Para reiniciar el servicio de Sendmail debemos ejecutar el comando:

service sendmail restart

Para depurar posibles errores, se puede examinar el contenido de la bitácora de correo del sistema en /var/log/maillog del siguiente modo:

tail -f /var/log/maillog

Debemos verificar el servicio desde una terminal, ejecutando el programa telnet dirigido hacia el puerto 25 de la dirección IP principal del sistema:

$ telnet 192.168.0.254 25

Saludamos al sistema con el comando HELO seguido del nombre del dominio local:

HELO nombre.dominio

El servidor de correo deberá contestar:

250 nombre.dominio Hello nombre.dominio [192.168.1.254], pleased to meet you

El servidor deberá contestar lo siguiente al terminar la conexión:

221 2.0.0 nombre.dominio closing connection

Connection closed by foreign host

Ejecutamos el comando MAIL FROM especificando la cuenta de correo de un usuario local del sistema del siguiente modo:

MAIL FROM:

El servidor de correo deberá contestar lo siguiente, a menos que especifique una cuenta de correo con un dominio distinto a los especificados en el fichero /etc/mail/relay-domains:

250 2.1.0 ... Sender ok

Ejecutamos el comando RCPT TO especificando una cuenta de correo existente en el servidor del siguiente modo:

RCPT TO:

El servidor de correo deberá contestar lo siguiente:

250 2.1.5 ... Recipient ok

Ejecutamos el comando DATA:

DATA

El servidor de correo deberá mostrar lo siguiente:

354 Enter mail, end with "." on a line by itself

Escribimos el texto que se desea incluir en el mensaje de correo electrónico. Al terminar finalice con un punto en una nueva línea:

Hola, este es un mensaje de prueba.

El sistema deberá mostrar lo siguiente:

250 2.0.0 k263wEKK006209 Message accepted for delivery

Ejecutamos el mandato QUIT:

QUIT

El servidor deberá terminar la conexión:

221 2.0.0 nombre.dominio closing connection

Connection closed by foreign host.

CAPÍTULO 4

4 FUNCIONAMIENTO Y PRUEBAS

4.1 CONFIGURACIÓN EN EL ACTIVE DIRECTORY

4.1.1 CREACIÓN DE CUENTAS DE USUARIOS

Para autenticar a todos los usuarios internos debemos crearles cuentas validas con el propósito de tener control en cada equipo registrado al dominio, podemos crear grupos por departamento y dentro de cada grupo los usuarios pertenecientes. Para nuestra simulación creamos 2 usuarios llamados: Administración y Consultoría. Nuestro dominio es pyme.com [8].

1. En el botón **Inicio**, seleccionamos **Todos los programas**, **Herramientas administrativas** y, hacemos clic en **Usuarios y equipos de Active Directory**.
2. Expandimos nuestro dominio **pyme.com** damos clic en el signo + (Fig. 4.1).
3. Damos clic con el botón secundario del *mouse* en una unidad organizativa creada o simplemente seleccionamos **Nuevo** y, damos clic en **Usuario** o **Usuario nuevo** en la barra de herramientas del complemento.

4. Escribimos la información del usuario. Nombre, Apellido y nombre de inicio de sesión.
5. Seleccionamos Siguiente para continuar.
6. Escribimos un password en los cuadros **Contraseña** y **Confirmar contraseña** y, después, **Siguiente**.
7. Seleccionamos en **Finalizar** para aceptar la confirmación en el siguiente cuadro de diálogo.

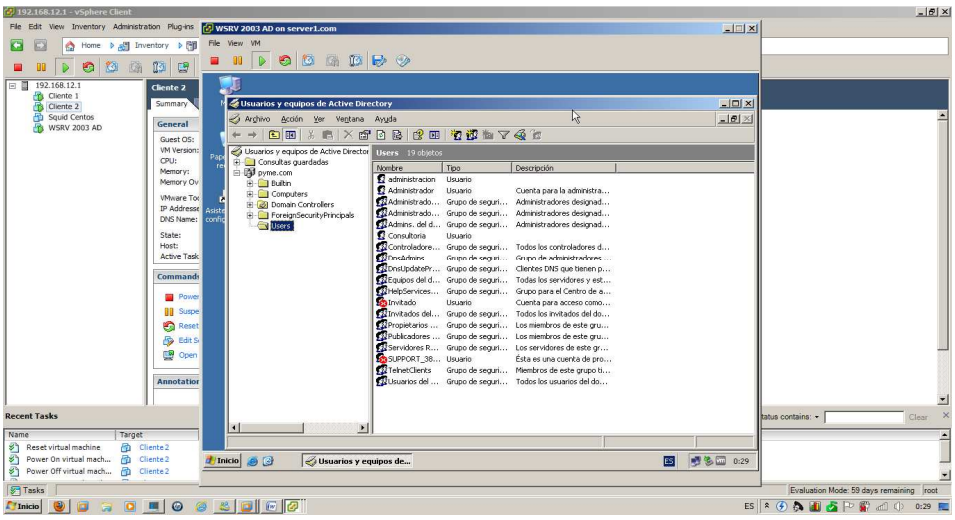


Fig. 4.1 Usuarios y equipos de Active Directory.

4.1.2 PRUEBAS DE LAS CUENTAS CREADAS CON EL DOMINIO

Para poder iniciar sesión en las cuentas Administración y Contraloría, debemos ingresar el usuario con su respectivo password configurado. Adicional cada máquina de usuario debe estar registrada en el dominio [9].

1. Iniciamos sesión ingresando usuario y password (Fig. 4.2), para esta demostración solo vamos a mostrar el usuario Administración.
2. Desde el menú ejecutar ingresamos al **cmd** para realizar una prueba de ping hacia nuestro dominio pyme.com. Si la conectividad es exitosa la maquina ya es parte de nuestro dominio (Fig. 4.3).

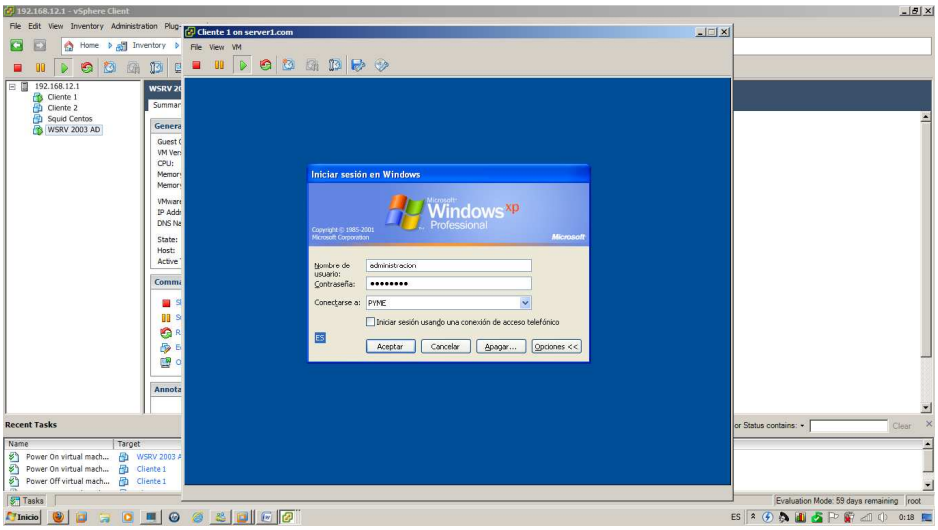


Fig. 4.2 Inicio de sesión del cliente Administración.

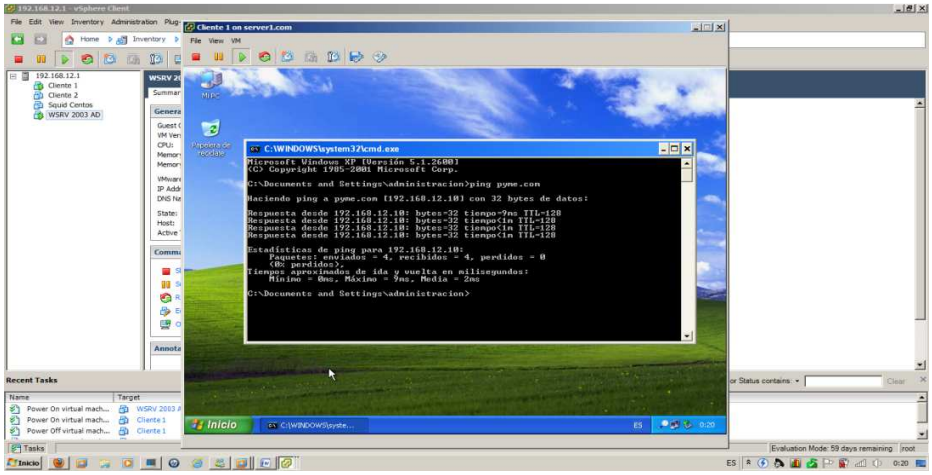


Fig. 4.3 Prueba de conectividad hacia el dominio pyme.com.

4.2 PRUEBAS DE NAVEGACION EN LOS CLIENTES CON EL SQUID CONFIGURADO

Todos los usuarios deberán tener configurada la dirección del servidor proxy en sus navegadores web para poder salir hacia internet. De igual manera tendrán limitantes hacia las páginas web a navegar, ya que se tiene un bloqueo de páginas prohibidas.

1. Cuando el servidor Centos este arriba, desde una ventana de terminal verificamos el status del Squid proxy (Fig. 4.4).

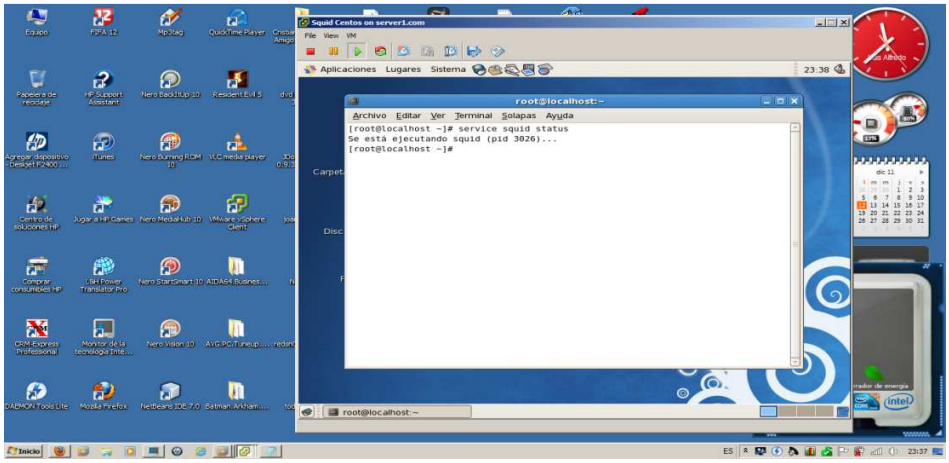


Fig. 4.4 Servicio de Squid ejecutándose.

2. Verificamos que nuestro cliente tenga configurado como Gateway la dirección IP de nuestro Squid proxy (Fig. 4.5), esto con el fin de que pueda salir hacia internet, ya que el Squid tiene configurada 2 interfaces de red (un adaptador para la LAN y un adaptador para la WAN).

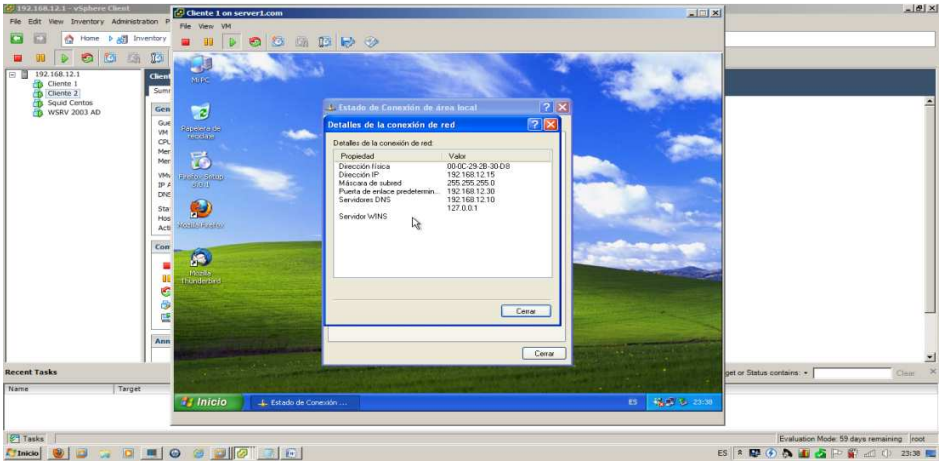


Fig. 4.5 Direccionamiento de red de un usuario interno.

3. En el explorador web que se utilice debemos tener la dirección IP del Squid para nuestro caso 192.168.12.30 con puerto 3128, la configuramos en la ruta como muestra la figura (Fig. 4.6):

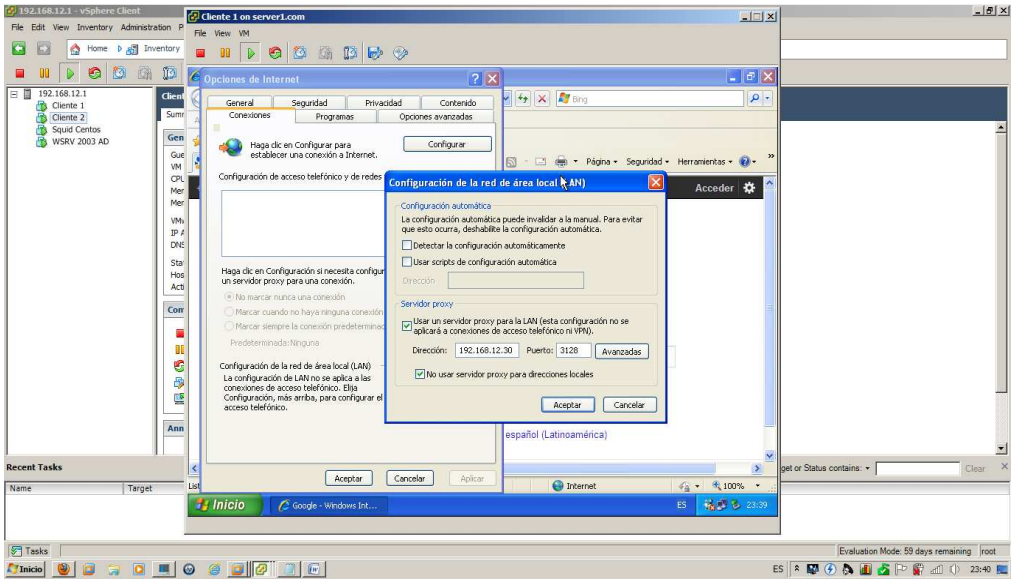


Fig. 4.6 Opciones avanzadas de Internet Explorer, Servidor Proxy

4. Realizamos una prueba de navegación hacia una página web bloqueada en nuestro Squid (Fig. 4.7), para esta demostración es www.eluniverso.com:

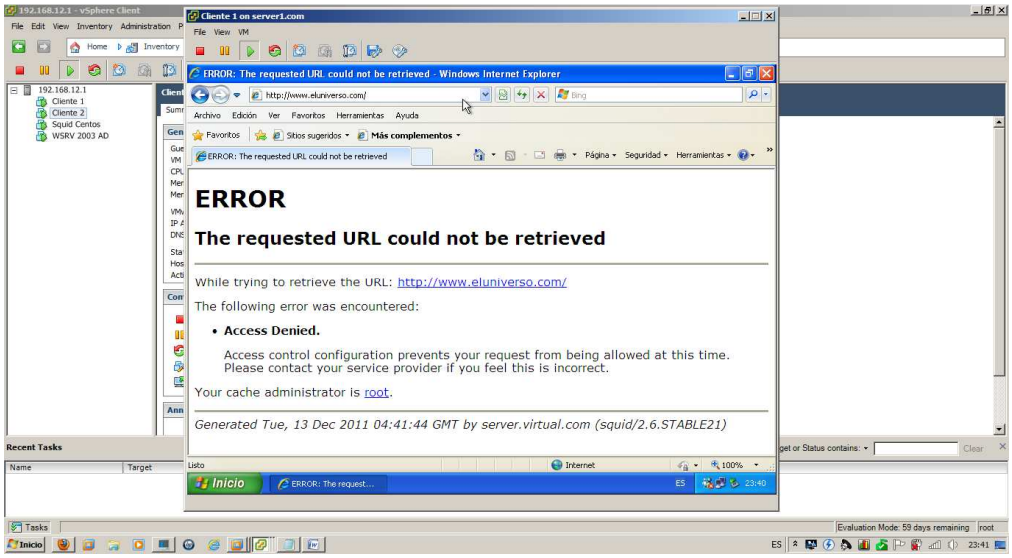


Fig. 4.7 Bloqueo de navegación a una página web prohibida.

4.3 CREACION DE CUENTAS DE CORREO Y PRUEBAS CON SENDMAIL

Cada usuario que este en el dominio pyme.com tendrá una cuenta de correo registrada en el servidor SendMail. Las pruebas de envío y recepción se hicieron entre cuentas de usuarios internos usando el dominio @server.virtual.com.

1. Verificamos en el servidor Centos el status del servicio SendMail si esta levantado (Fig. 4.8):

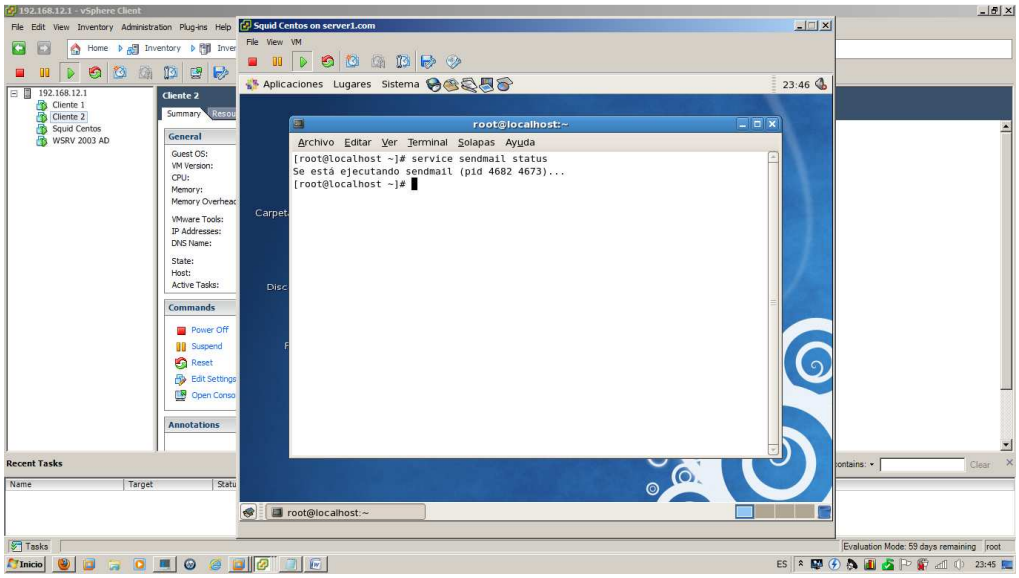


Fig. 4.8 Servicio SendMail ejecutándose.

2. Para cada cliente de correo en nuestro caso Outlook Express se debe configurar las cuentas creadas en el servidor SendMail. Primero se configura la cuenta de correo (Fig. 4.9), para este ejemplo usamos el usuario Administración:

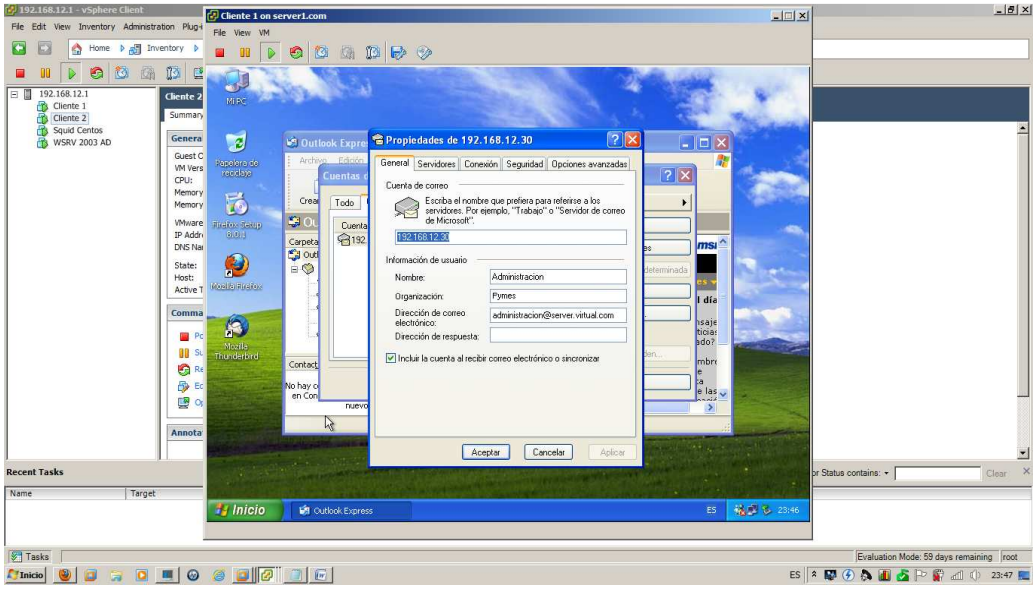


Fig. 4.9 Propiedades de cuentas de correo.

3. Configuramos los servidores de entrada POP3 y saliente SMTP necesarios para el envío y recepción de correo (Fig. 4.10):

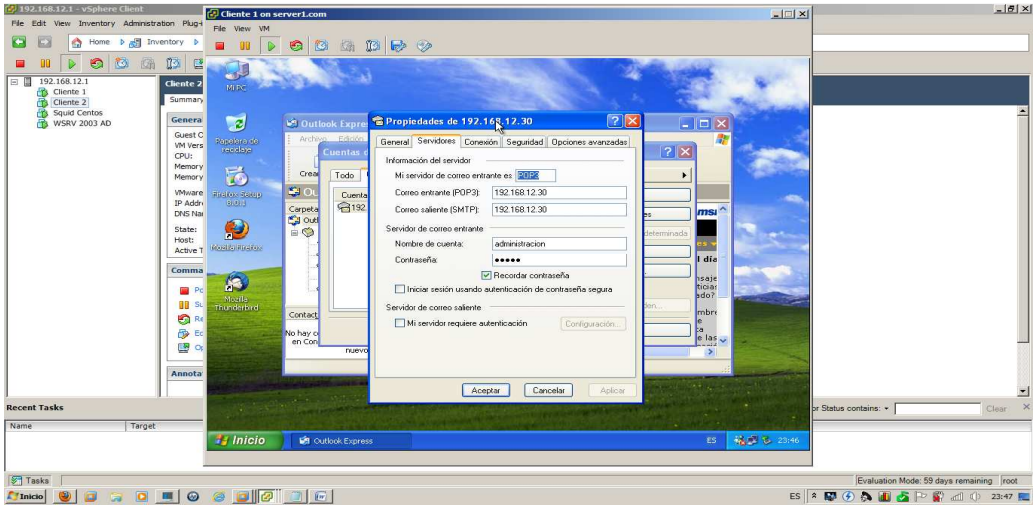


Fig. 4.10 Servidores de correo entrante y saliente.

4. Las pruebas de envío y recepción de correo se la realiza desde la cuenta creada para Administración y Contraloría, administración@server.virtual.com hacia consultor@server.virtual.com (Fig. 4.11):

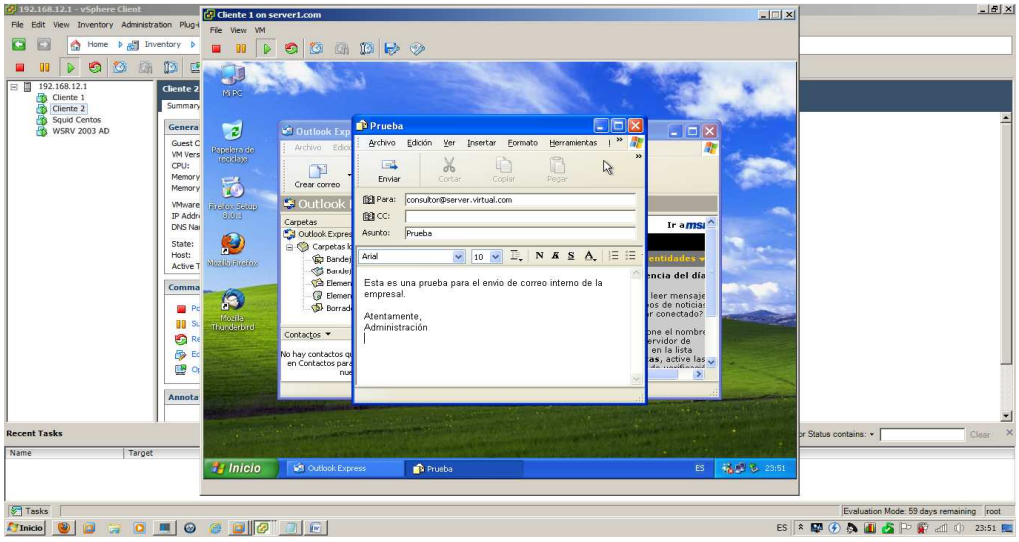


Fig. 4.11 Cuerpo de correo para enviar hacia la cuenta consultor.

5. Revisamos que el correo haya llegado al usuario consultor (Fig. 4.12):

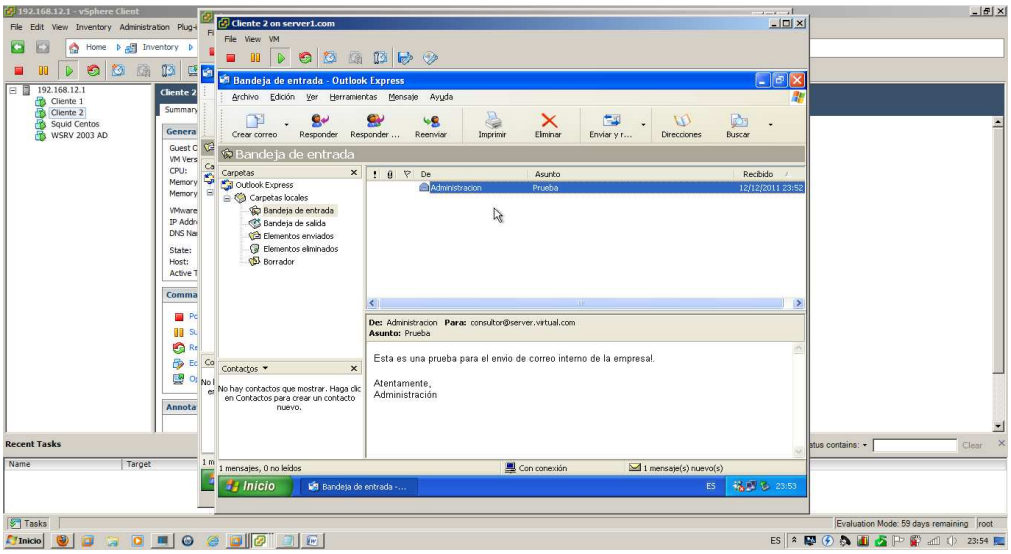


Fig. 4.11 Recepción de correo desde la cuenta Administración.

4.4 GRAFICAS DE RENDIMIENTO

4.4.1 INDICADORES DE ENVIO Y RECEPCION DE CORREOS

En estas graficas vamos a demostrar el comportamiento del CPU, Datastore, Memoria y Network en el momento que los clientes estén enviando correos a través del SendMail.

- Se utilizó en porcentaje casi el 80% del CPU del ESXi cuando se enviaron correos. Hubo también un pico más alto de rendimiento 8000 MHZ del procesador. El porcentaje más bajo es del 23% con un uso de procesador de casi 2000 MHZ (Fig. 4.12).

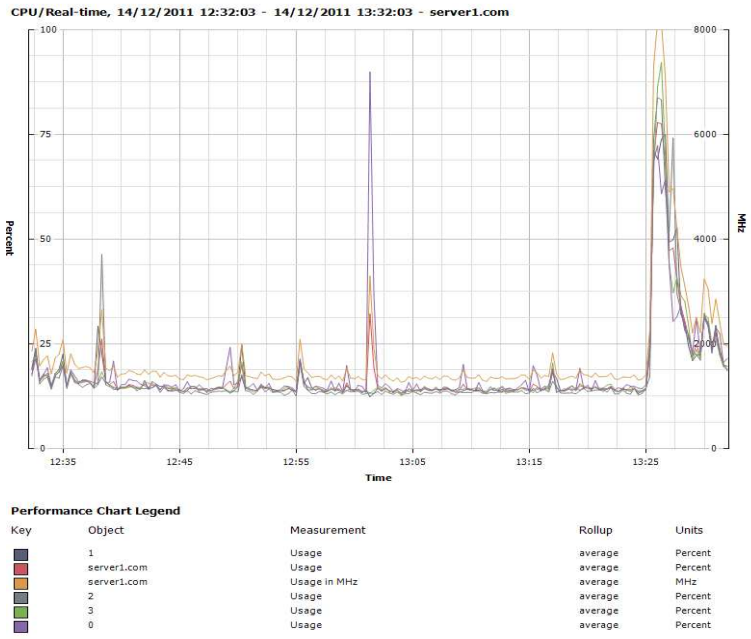


Fig. 4.12 Rendimiento Host-ESXi CPU.

- Observamos el rendimiento más alto de carga del Datastore que es de 120 milisegundos a las 12:42.
- El rendimiento más bajo de carga es de 20 milisegundos a las 13:25 (Fig. 4.13).

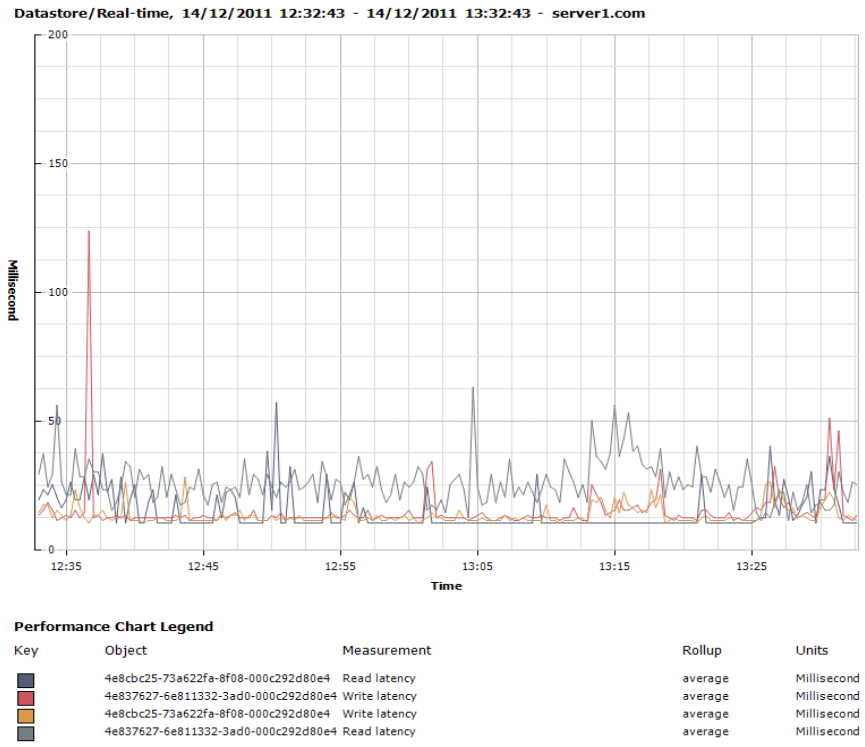
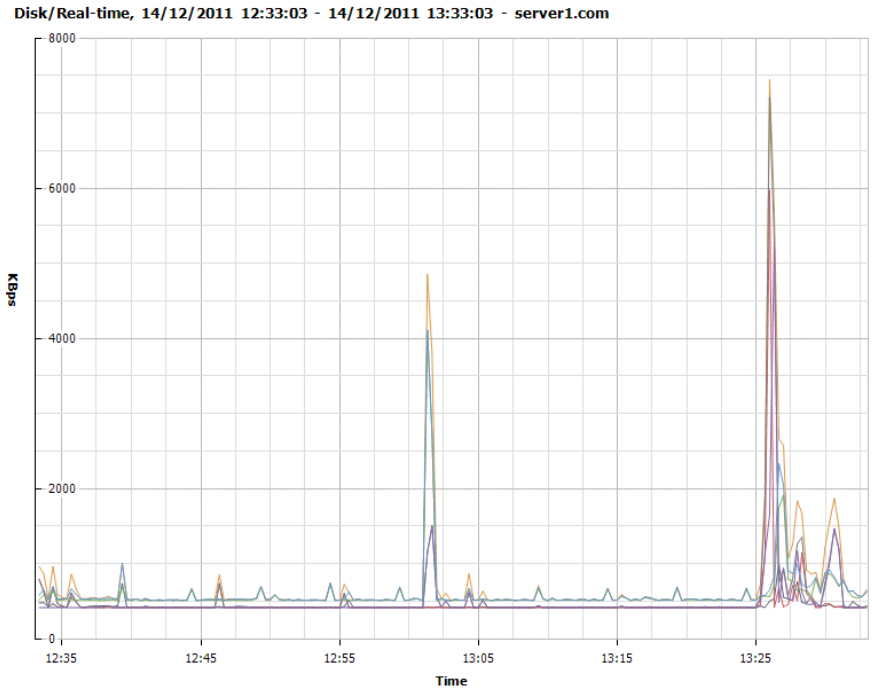


Fig. 4.13 Rendimiento Host-ESXi DataStore.

- El rendimiento más bajo de uso de disco es aproximadamente 1000 Kbps.
- El rendimiento más bajo de escritura de disco es aproximadamente 500 Kbps.
- El rendimiento más alto de escritura de disco es aproximadamente 7500 Kbps (Fig. 4.13).



Performance Chart Legend

Key	Object	Measurement	Rollup	Units
	mpx.vmhba0:C0:T1:L0	Write rate	average	KBps
	mpx.vmhba0:C0:T1:L0	Read rate	average	KBps
	server1.com	Usage	average	KBps
	server1.com	Read rate	average	KBps
	mpx.vmhba0:C0:T0:L0	Write rate	average	KBps
	mpx.vmhba0:C0:T0:L0	Read rate	average	KBps
	server1.com	Write rate	average	KBps

Fig. 4.14 Rendimiento Host-ESXi Disk.

- El rendimiento de memoria shared common es de 15000000 Kilobytes.
- El rendimiento de memoria consumida es de 32000000 Kilobytes.
- El rendimiento de memoria concedida (granted) es de aproximadamente 3000000 Kilobytes
- El rendimiento de memoria activa en de 18567680 Kilobytes.
- Como se observa en la gráfica la memoria swap usada es de valor 000000 Kilobytes (Fig. 4.15).

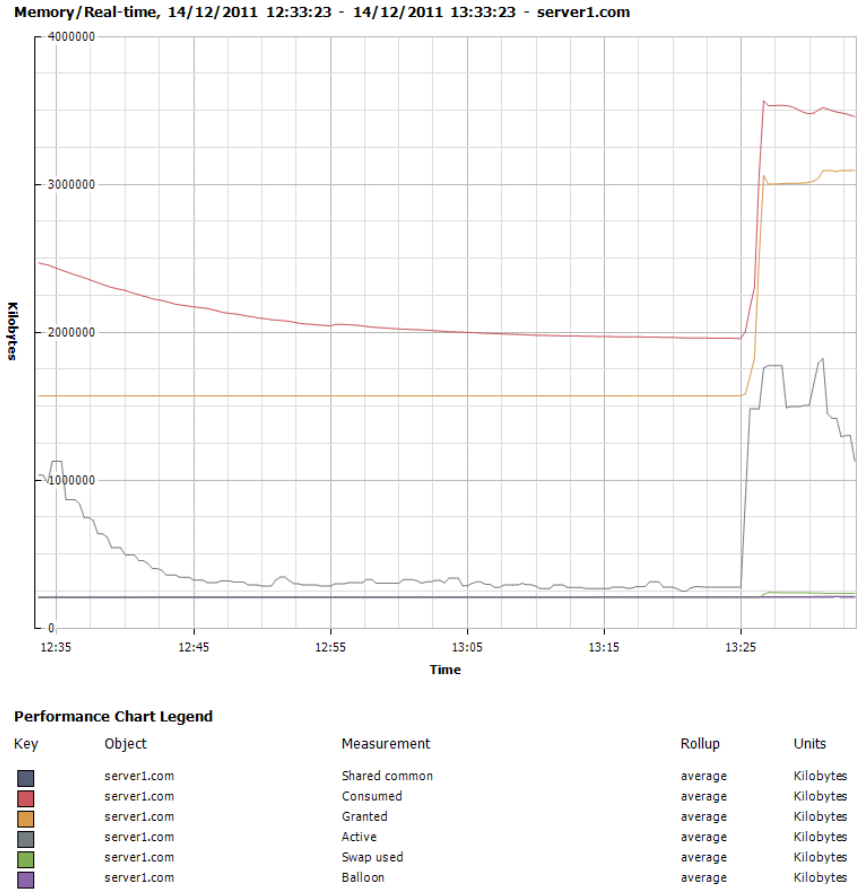


Fig. 4.15 Rendimiento Host-ESXi Memoria.

- El ancho de banda en la transmisión de datos vmnic0 (adaptador de red para LAN) es de 850 kbps.
- El ancho de banda en la transmisión de datos vmnic1 (adaptador de red para WAN) es de 820 kbps.
- El ancho de banda para la recepción de datos del ESX es de 800 kbps.

- El ancho de banda para la transmisión de datos del ESXi es de 812 kbps.
- El ancho de banda para la recepción de datos en el vmnic0 (adaptador de red para LAN) es de 842 kbps.
- El ancho de banda para la recepción de datos en el vmnic1 (adaptador de red para WAN) es de 812 kbps (fig. 4.16).

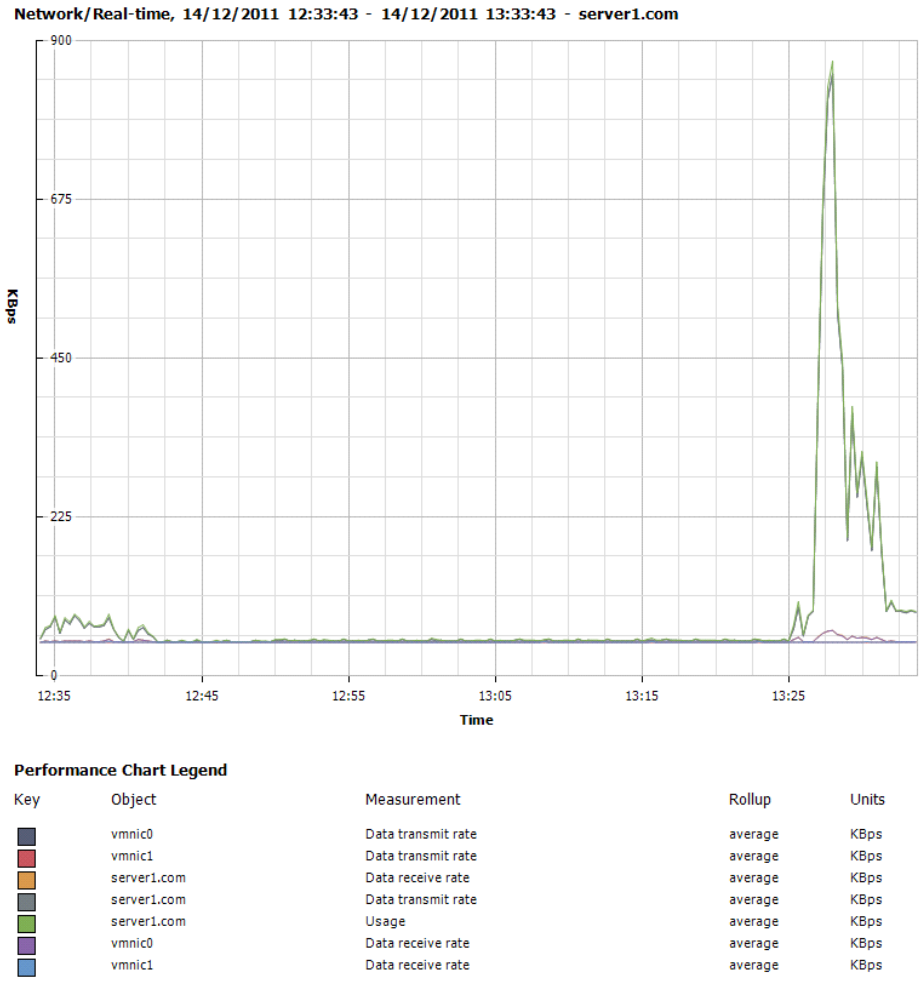


Fig. 4.16 Rendimiento Host-ESXi Network.

4.4.2 INDICADORES DEL SERVIDOR SQUID PROXY

Para este punto hemos considerado observar los rendimientos en CPU, Datastore y Memoria, ya que para red es recomendable utilizar un graficador de enlaces WAN dedicado para observar los picos de navegación.

- El porcentaje de rendimiento que utilizo el Squid se observa en un 73%, esto quiere decir un uso en MHZ de 1600.
- El rendimiento en el Core 0 es de 317 MHZ, mientras el del Core 1 es de 1224 MHZ (Fig. 4.17).

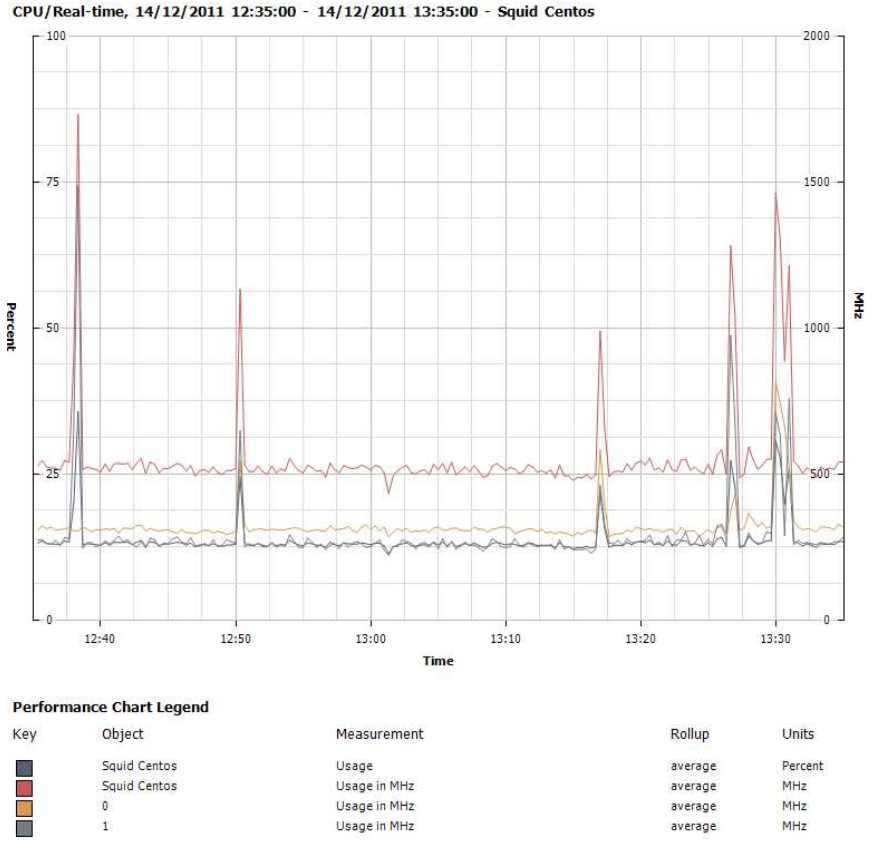


Fig. 4.17 Rendimiento Squid Centos CPU.

- En el Datastore observamos que el write latency llega a los 80 milisegundos. Mientras que el read latency es de 55 milisegundos (Fig. 4.18).

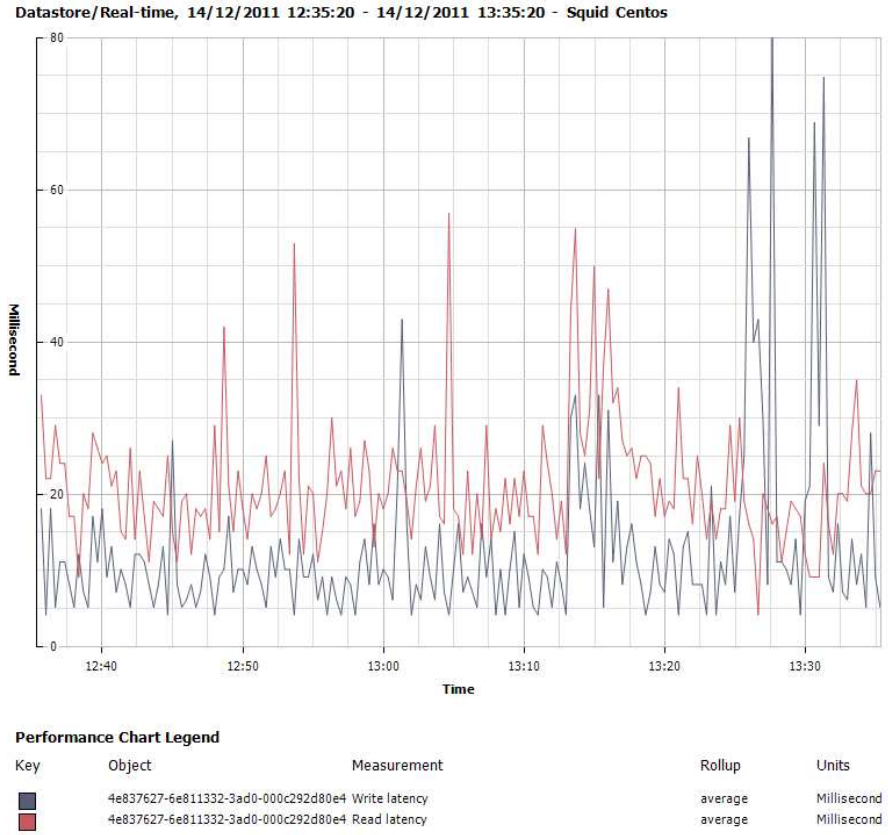


Fig. 4.18 Rendimiento Squid Centos CPU.

- El rendimiento de memoria granted es de aproximadamente 500000 kilobytes, esto quiere decir que es mucho menor al consumo de envío de correos.
- El rendimiento de memoria activa es de aproximadamente 161314 kilobytes, menor al consumo de envío de correo

- El rendimiento de memoria consumida es de aproximadamente 475000 kilobytes, mucho menor al consumo de envío de correos (Fig. 4.19).

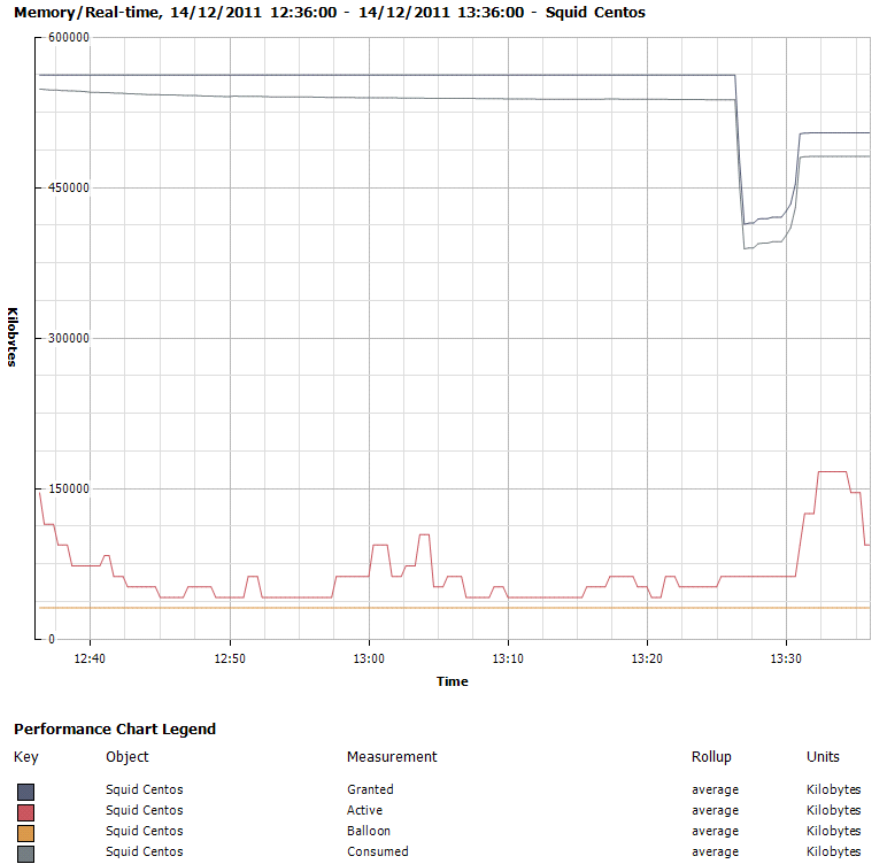
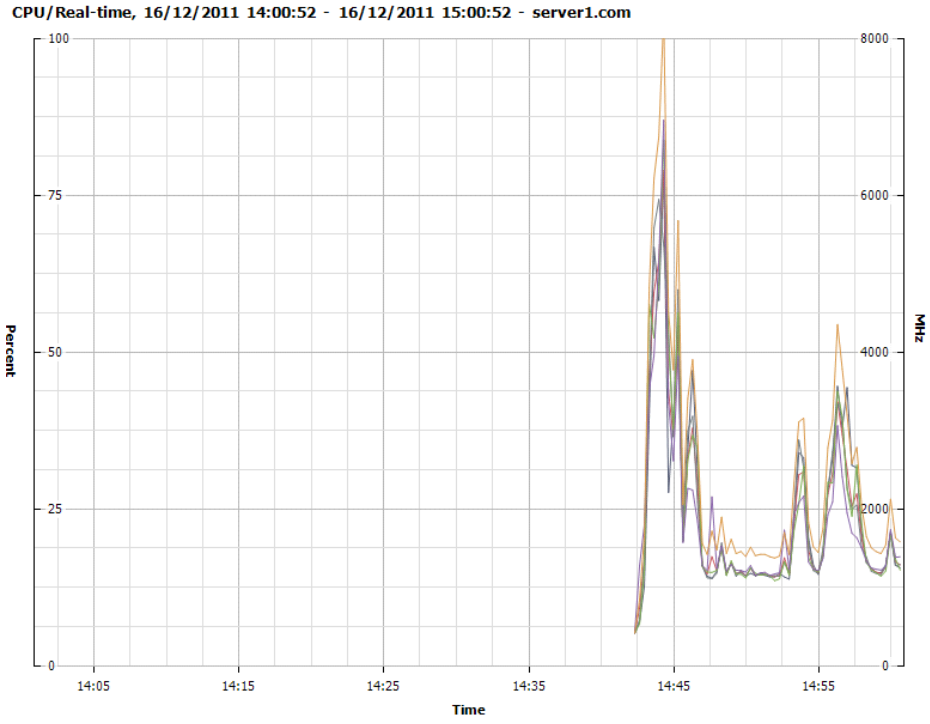


Fig. 4.19 Rendimiento Squid Centos Memoria.

4.4.3 INDICADORES DEL SERVIDOR SQUID CONTROL DE NAVEGACION

Para estas pruebas vamos a considerar medir rendimiento en CPU, Datastore, y Memoria. El control de navegación se considera en cierto punto no tan crítico para el tema de rendimiento, ya que no siempre el usuario va intentar ingresar a las páginas bloqueadas. El cliente al observar el mensaje de página bloqueada no volverá a intentar sobre la misma.

- Se utilizó un porcentaje de casi el 90% del CPU del ESXi cuando se trató de navegar pero el bloqueo de páginas web restringidas lo prohibió.
- El pico más alto de rendimiento se mostró en 7000 MHZ del uso de procesador.
- El porcentaje más bajo es del 23% con un uso de procesador de casi 1500 MHZ (Fig. 4.20).



Performance Chart Legend

Key	Object	Measurement	Rollup	Units
	1	Usage	average	Percent
	server1.com	Usage	average	Percent
	server1.com	Usage in MHz	average	MHz
	2	Usage	average	Percent
	3	Usage	average	Percent
	0	Usage	average	Percent

Fig. 4.20 Rendimiento del CPU en bloqueo de páginas.

- El rendimiento de la latencia en lectura es promedio de 160 milisegundos y en escritura de 177 milisegundos (Fig. 4.21).

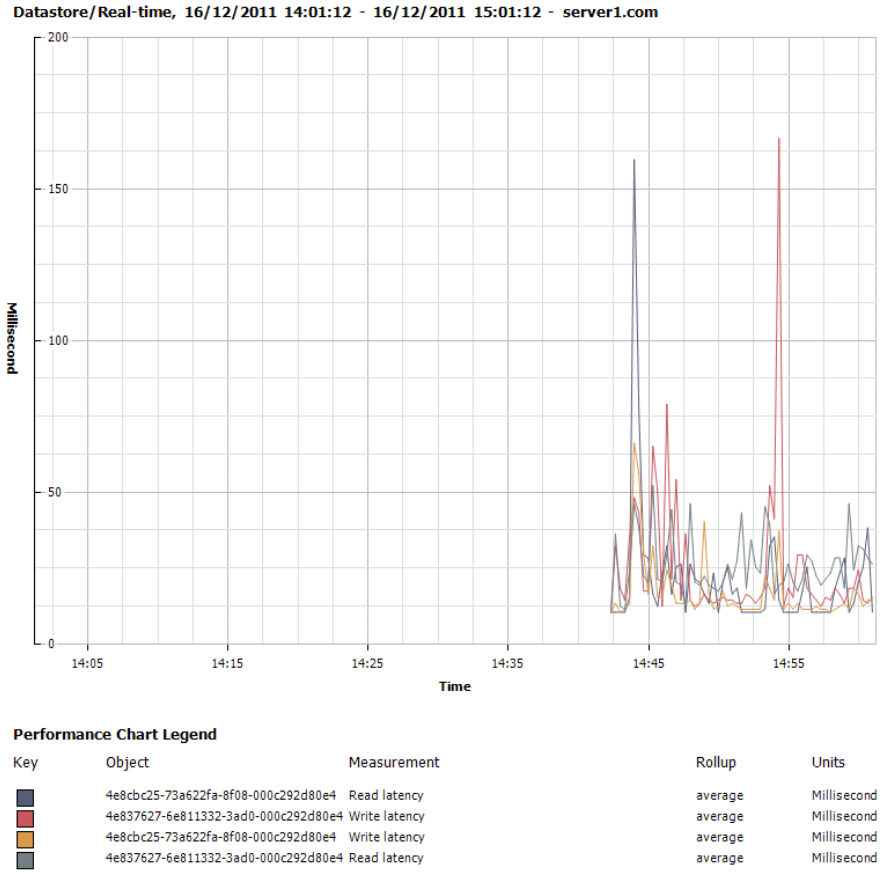


Fig. 4.21 Rendimiento del Datastore en el bloqueo de páginas.

- Los rendimientos de memoria shared common 16007081 Kilobytes, similar al consumo de envío de correo. Quiere decir que en el momento de petición del usuario el querer ingresar a una página y está bloqueada obtendremos consumos similares al correo.

- Los recursos de memoria consumida son de 22650533 Kilobytes
- Los recursos de memoria concedida son de aproximadamente 3000000 Kilobytes.
- Los recursos de memoria activa son de 17557680 Kilobytes.
- La memoria swap usada por lo general tendrá un valor de 000000 Kilobytes, ya que tenemos suficientes recursos para solventar estas peticiones (Fig. 4.22).

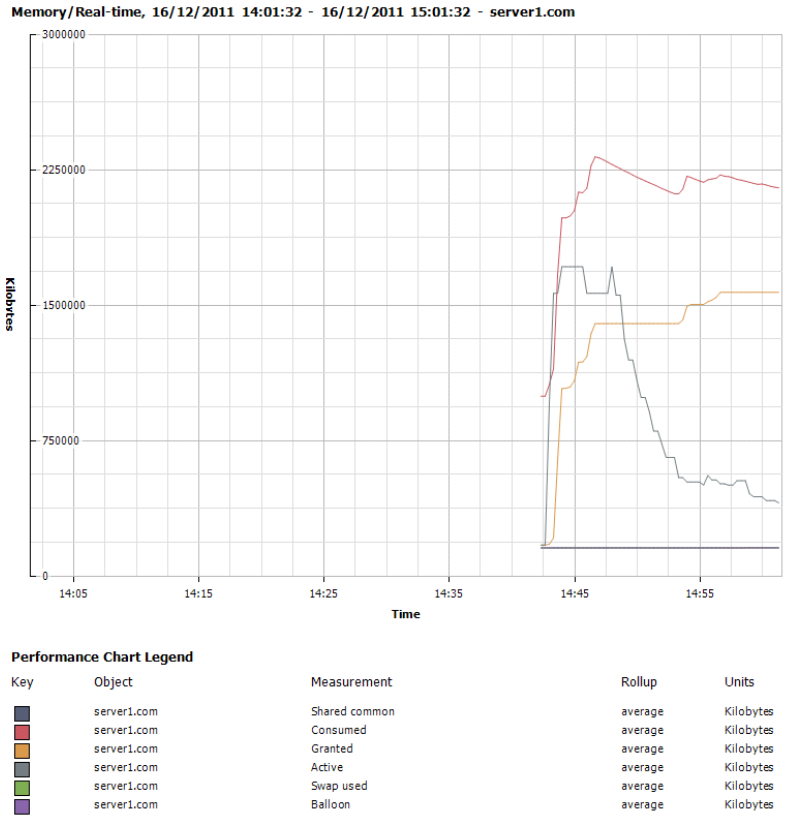


Fig. 4.22 Rendimiento de memoria en el bloqueo de páginas.

4.4.4 INDICADORES DEL SERVIDOR ACTIVE DIRECTORY

Este servidor es el que obtiene la base de datos de todos los usuarios, tendrán que autenticarse cada vez que inicien sesión hacia el Active Directory. Vamos a observar el rendimiento en CPU, Datastore y Memoria.

- El rendimiento porcentual de uso en procesamiento llego al 91%, esto cuando se están autenticando los usuarios. En MHZ llegamos al 4200.
- El uso en el Core 0 es de 3862 MHZ.
- El uso en el Core 1 es de 4121 MHZ (Fig. 4.23).

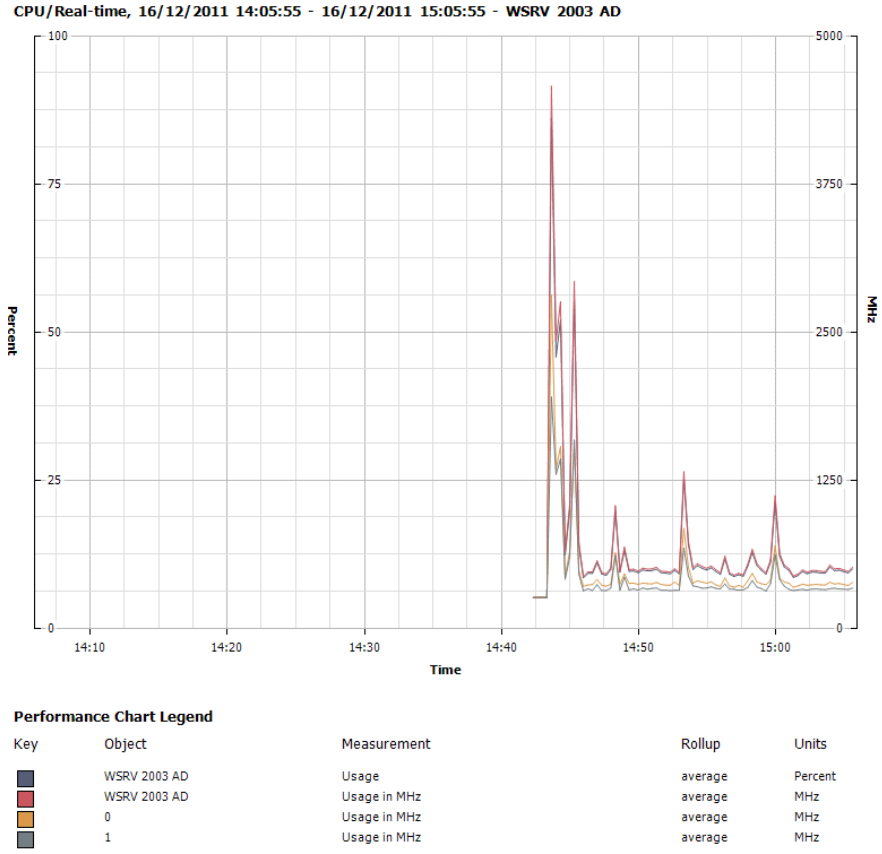


Fig. 4.23 Rendimiento del CPU en el Active Directory.

- El Datastore no muestra un valor de escritura que llega a los 75 milisegundos. En lectura es de 162 milisegundos (Fig. 4.24).

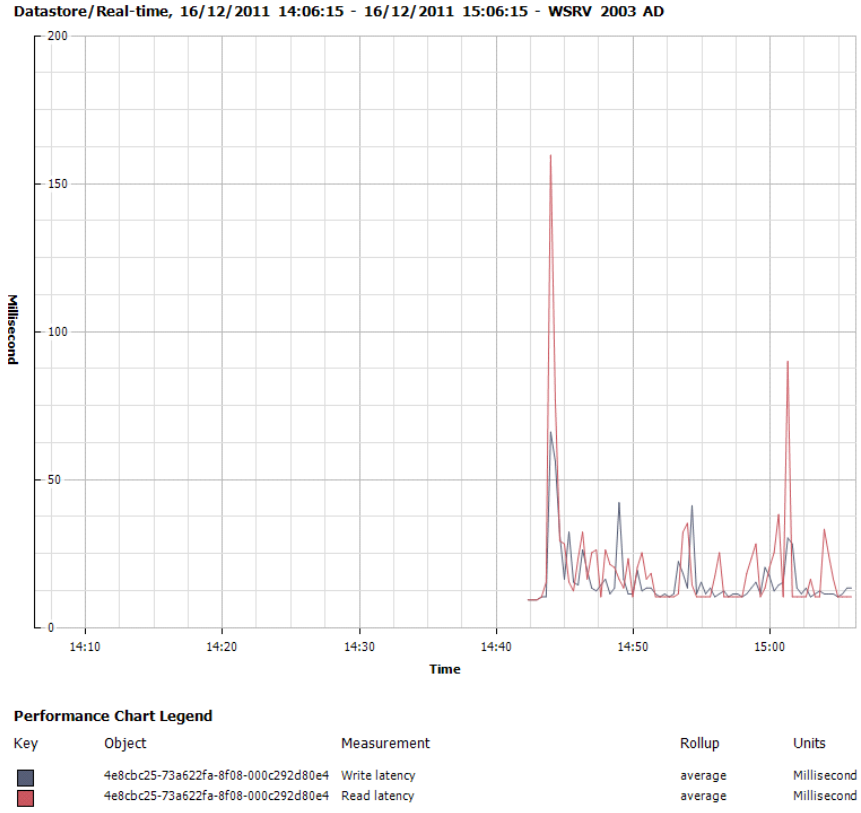


Fig. 4.24 Rendimiento del Datastore en el Active Directory.

- La memoria concedida (granted) tiene un valor aproximado de 900000 kilobytes, esto quiere decir que su consumo es alto. El correcto rendimiento depende el configurar un valor correcto promedio de memoria para el servidor.
- El rendimiento de memoria activa alcanza un valor de 782421 kilobytes.

- El rendimiento de memoria consumida es aproximadamente 421357 kilobytes (Fig. 4.24).

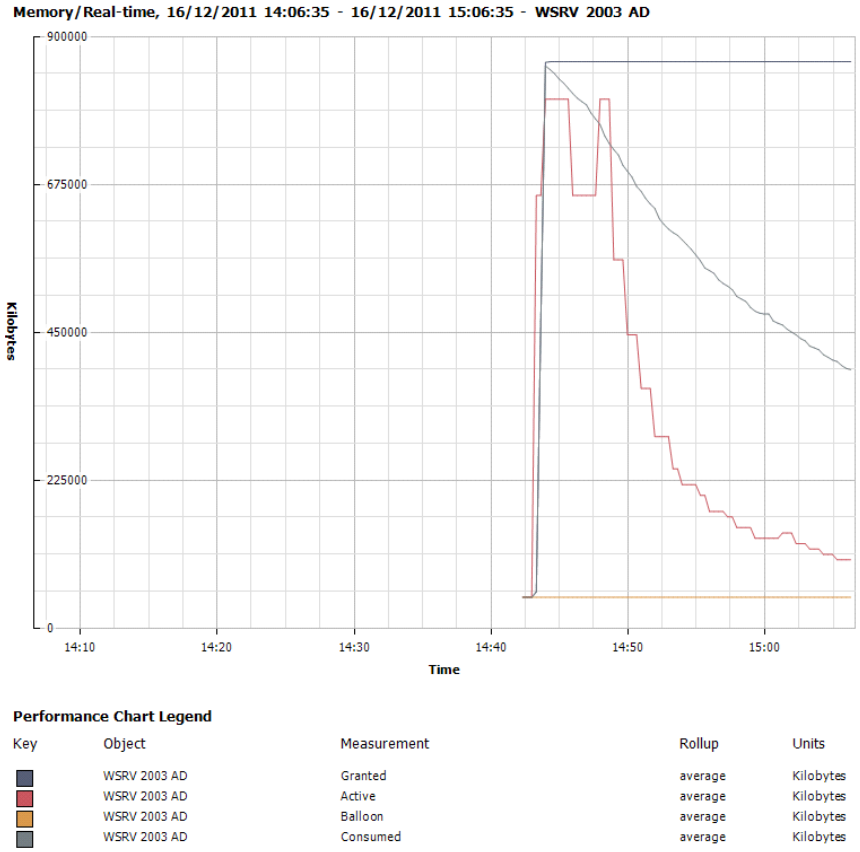


Fig. 4.25 Rendimiento de memoria en el Active Directory.

CONCLUSIONES

1. La disponibilidad de los servicios importantes que se necesitan en las Pymes es crucial, para obtener menores tiempos de latencias en el envío de información y así ofrecer un rendimiento óptimo al usuario final para no parar los procesos internos de donde se obtienen las ganancias.

2. La importancia de que en la infraestructura se involucre con software libre, ya que esta es una herramienta de trabajo poderosa en ambientes donde el presupuesto para pagar por software licenciado es limitado.

3. Mejorar la privacidad y él envió de los datos, esto nos permite tener un manejo más centralizado y privado de los datos de la pequeña empresa, es decir asignar ciertos recursos y privilegios para distintos tipos de empleados hacia quien va dirigida una aplicación.

4. El Mantenimiento de un solo servidor Físico, es más económico, que a varios equipos, se ahorra espacio y material físico, menor número de servidores en la empresa, mejor aprovechamiento de los mismos y ahorro de energía para la pequeña empresa.

5. Las pruebas del rendimiento nos indican que el acceso a disco es rápido sin importar la memoria RAM asignada.

6. Es importante saber seleccionar los indicadores correctos al momento de medir el rendimiento, para esta infraestructura se consideró: utilización y distribución del CPU físico, carga promedio del CPU, utilización y distribución del CPU lógico, memoria en uso, disco reads/segundos, disco write/segundos, NIC MB transmitidos/segundos, porcentaje de uso del CPU, porcentaje del sistema, memoria VM asignada, memoria VM activa.

7. Debemos tomar en cuenta los warnings al momento de monitorear el rendimiento. Por ejemplo para CPU el uso prolongado >80%, longitud de cola por CPU >10, para la memoria el total de paginación mayor a 200-300 I/O por segundo, para disco físico >20ms el promedio de transferencia por segundo, >3 la longitud promedio de colas, para la NIC si en la red se están encolando los paquetes recibidos.

8. **Perfmon.-** podemos usar esta herramienta que viene incluida en nuestros sistemas Windows, esta nos permite el monitoreo de recursos en vivo y también la capacidad de crear contadores con los cuales nosotros podemos

definir tiempos a monitorear ciertos aspectos como puede ser red,cpu,memoria,etc

9. **Capacity Planner.-** nos ofrece la capacidad de poder analizar el comportamiento de nuestra infraestructura, planeación y nos provee con reportes y recomendaciones de posibles escenarios de consolidación para un mejor rendimiento del Datastore, memoria, red, memoria VM asignada, memoria VM activa.

10. **Esxtop.-** esta herramienta incluida tanto en ESX como ESXi nos permite poder monitorear distintos aspectos de nuestro host, podemos monitorear RAM, CPU, red, almacenamiento, etc. Es una herramienta que ejecutamos en la línea. de comando directamente en los hosts o también podemos ejecutarla de forma remota (resxtop).

11. Otra forma de monitorear los recursos que usan las Vm’s y el Host es a través del servicio “Data Collector Service”, que nos muestra equipos en la red local, guarda información del OS, hardware, aplicaciones en uso, métricas del consumo en una base de datos local.

12. Para identificar rendimientos por medio de la consola ejecutamos Esxtop, ingresamos la tecla “m” después ingresamos la tecla “f” y nos aseguramos de que los siguientes indicadores estén activados “j,k,p”.

13. Para la medición del rendimiento del CPU por consola activamos la vista de Vm’s ingresando la tecla “V”(mayúscula) y esta nos muestra la primera vista del rendimiento de CPU por host, por maquina virtual, por aplicación, por sistema operativo instalado, además de crear un pool de rendimiento del sistema completo.

14. Para la medición del rendimiento del Disco ingresamos en la consola la tecla ”u”, después se ingresa la tecla “f” y verificamos que los siguientes medidores estén activados “f,g,h,i,L”

15. Para el rendimiento optimo y seguro de la red del Host ESXi también podemos hacerlo por consola ingresando la tecla “n” donde nos mostrara el porcentaje de paquetes transmitidos que se han caído (%DRPTX) por algún problema en nuestra red física, alto consumo de la misma, problemas de hardware, etc. Además de mostrar el porcentaje de paquetes recibidos que

se han caído (%DRPRX), por cuestiones de recursos del lado de las Vm’s o porque se está teniendo un buffer overflow a nivel de la nic del Host.

RECOMENDACIONES

1. Considerar siempre el hardware y software para futuros crecimiento en una empresa ya que esta puede tener crecimiento en 1 o 2 años y la infraestructura debe estar preparada para soportarla.

2. Poner almacenamiento suficiente para los discos locales y buenas controladoras con cache (1GB de cache). Los discos SAS mínimo 10K.

3. Utilizar otro servidor con vCenter, que puede hacer réplicas de local a local de todo el entorno virtualizado.

4. Adicionalmente crear otra partición de Datastore que sirva como una partición swap para un mejor manejo de la escritura y lectura del servidor ESXi.

5. Para un favorable rendimiento entre la maquina nativa y la virtual, debemos configurar el mismo número de CPU físico que tiene el sistema nativo en el entorno virtual. Para la memoria es recomendable realizar lo mismo.

6. Recordar que si se implementa el entorno en un solo host, cuando este en algún momento falle la empresa se para, debe haber como mínimo un backup para las aplicaciones críticas.

GLOSARIO DE TÉRMINOS

PROXY: Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor al que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

DOMINIO: El propósito principal de los nombres de dominio en Internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada nodo activo en la red, a términos memorizables y fáciles de encontrar.

BRIDGE: Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete.

Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red.

NAT: Es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

AES: Es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

TCO: El coste total de propiedad (proveniente del término anglosajón Total Cost of Ownership o TCO), es un método de cálculo diseñado para ayudar a los usuarios y a los gestores empresariales a determinar los costes directos e indirectos, así como los beneficios, relacionados con la compra de equipos o programas informáticos.

SAN: Una red de área de almacenamiento, es una red concebida para conectar servidores, matrices de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

NAS: Servidor de Acceso a la Red (Network Access Server) es un punto de entrada que permite a los usuarios o clientes acceder a una red.

SSH: Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

ACL: Permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante"

VIRTUALIZACION: Es la creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

VMFS: Tecnología exclusiva de VMware, es el sistema de almacenamiento de información predeterminado para archivos de máquinas virtuales en particiones y discos SCSI físicos. El almacenamiento de información central de las máquinas virtuales con VMware VMFS ofrece más control, flexibilidad y performance para administrar su entorno de TI virtualizado

RAM: Memoria de acceso aleatorio, es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados.

CPU: La unidad central de procesamiento, es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

NIC: Tarjeta de red o adaptador de red que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras (discos duros, CD-ROM, impresoras, etc.).

VLAN: Es un método de crear redes lógicamente independientes dentro de una misma red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local.

ETHERNET: Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.

ISO: Es un archivo donde se almacena una copia o imagen exacta de un sistema de ficheros, normalmente un disco óptico. Se rige por el estándar ISO 9660 que le da nombre.

HTTP: Protocolo de transferencia de hipertexto usado en cada transacción de la World Wide Web (WWW).

SWAP: Espacio de intercambio es una zona del disco (un fichero o partición) que se usa para guardar las imágenes de los procesos que no han de mantenerse en memoria física.

URL: Es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones, presentaciones digitales, etc.

SASL: Simple Authentication and Security Layer (capa de seguridad y autenticación simple). Es un framework para autenticación y autorización en protocolos de Internet. Separa los mecanismos de autenticación de los protocolos de la aplicación permitiendo, en teoría, a cualquier protocolo de aplicación que use SASL usar cualquier mecanismo de autenticación soportado por SASL.

POP3: Post Office Protocol (Protocolo de la oficina de correo) clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

IMAP: Es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor.

SMTP: Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

WAN: Una red de área amplia, acrónimo de la expresión en idioma inglés wide area network, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente.

LAN: Una red de área local, es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro.

BIBLIOGRAFÍA

[1] Vmware Workstation 7: Como instalar Vmware 7 Workstation para windows, http://www.tuinformaticafacil.com/vmware/como-instalar-vmware-workstation-7-para-windows/pagina-1/, 3 de septiembre del 2011.

[2] Vmware ESXi: Instalar Vmware ESXi Hypervisor, http://sliceoflinux.com/2009/03/04/instalar-vmware-esxi-hypervisor/, 4 de marzo del 2009

[3] Vmware Vsphere Client: Como instalar Vmware Vsphere Cliente 4.0, http://www.aprendeinformaticaconmigo.com/instalar-vmware-vsphere-client-40, 10 de octubre del 2010

[4] Squid Proxy: Como instalar y configurar el Squid Proxy en Centos 5, http://www.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base+de+Conocimiento/Servidor+Proxy, 4 de Agosto del 2011

[5] Control de Navegación: Como configurar el control de navegación web en Centos 5, http://www.alcancelibre.org/staticpages/index.php/19-2-como-squid-

restriccion-web, 18 de abril del 2009

[6] SendMail y Dovecot: Como configurar el servicio de correo para envío y recepción en Centos 5, http://superahacker.blogspot.com/2009/04/sendmail-y-dovecot-en-linux-centos-5.html, 4 de marzo del 2009

[7] Creación de Cuentas de Usuario: Guía detallada de administración de Active Directory, Usuarios y equipos Active directory en Windows server 2003, http://www.microsoft.com/spain/technet/recursos/articulos/admng.mspx, 17 de septiembre del 2004

[8] Prueba de Cuentas de Usuario: Guía detallada de administración de Active Directory, crear una cuenta de usuario en Windows server 2003, http://www.microsoft.com/spain/technet/recursos/articulos/admng.mspx, 17 de septiembre del 2004