



**UNIVERSIDAD NACIONAL AUTONOMA DE
MEXICO
FACULTAD DE ESTUDIOS SUPERIORES
ACATLÁN**

**FUNDAMENTOS DE LA VIRTUALIZACIÓN DE
SERVIDORES USANDO LA TECNOLOGÍA
VMWARE ESX.**

TESINA

**QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN MATEMATICAS APLICADAS Y COMPUTACION.**

**PRESENTA:
IVAN DARIO LOPEZ MARTINEZ**

**ASESOR:
LIC. OSCAR GABRIEL CABALLERO MARTINEZ.**

Septiembre 2013



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

Sin contemplación alguna agradezco a Dios, que me da todo y me ha permitido la vida para la realización de tantos proyectos exitosos.

A mis padres, hermanas, que han sido mi mayor apoyo, motivación, que su único propósito es verme en la vida como una persona triunfadora.

A mis padres, Tommy y Ricardo, por sus consejos y sabiduría, demostrándome que todo en la vida es posible con mucho esfuerzo, ahínco y perseverancia. Gracias por que a pesar de las circunstancias tan difíciles, creyeron en mí y siempre estuvieron ahí, con todo tipo de apoyo, el cual ha generado este triunfo que quiero lo sientan suyo.

A mi Madre Tommy (Q.P.D), a su memoria le dedico este gran logro, porque de ella tuve un apoyo constante e incondicional, y sé que desde arriba ella comparte el gozo de mi éxito; Gracias MAMA con el corazón te lo digo, muchas gracias.

Gracias a mi asesor, Oscar Caballero, por compartir su conocimiento, su sabiduría y experiencia, y apoyarme sin condición alguna en su asesoría para realizar este trabajo, a todos mis maestros, por compartir sus conocimientos, sabiduría y experiencia.

A la Máxima casas de Estudios, por darme la oportunidad de ser parte de ella, por brindarme una plataforma tan robusta, completa y exitosa, me siento orgulloso y soy privilegiado con tal honor, GRACIAS UNAM.

ÍNDICE:	Pág.
INTRODUCCIÓN.....	4

CAPITULO 1. HISTORIA DE LA VIRTUALIZACIÓN.

1.1 ORIGENES Y EVOLUCION DE LA VIRTUALIZACION.....	7
1.2 ¿QUÉ ES LA INFRAESTRUCTURA DE VMWARE ESX 3?.....	9
1.3 ¿QUÉ ES VMWARE VSPHERE 4.0?.....	11
1.4 DIFERENCIAS ENTRE ESX 3.5 Y ESX 4.....	13
1.5 VMWARE VCENTER (DATACENTER).....	15

CAPÍTULO 2. VIRTUALIZACIÓN DE SERVIDORES.

2.1 EL SERVIDOR ESX 3.5 LA INSTALACION.....	17
2.2 EL VMWARE ESXI 3.5.....	26
2.3 EL DATACENTER 2.X VMWARE CONOCIDO TAMBIÉN COMO EL SERVIDOR VCENTER.....	31
2.4 EL CLIENTE DEL VMWARE VCENTER.....	38
2.5 EL SERVIDOR DE LICENCIAS (VCENTER 2.X).....	39
2.6 EL VCONVERTER Y SUS GENERALIDADES.....	40
2.7 INSTALACION DEL ESX 4.0 ACTUALMENTE CONOCIDO COMO VSPHERE 4.0.....	44

CAPÍTULO 3. DISPOSITIVOS DE ALMACENAJE Y NETWORKING.

3.1 ALMACENAJE.....	53
3.2 ADMINISTRACIÓN DE RECURSOS.....	67
3.3 EL MODELO DE RED VIRTUAL (VIRTUAL NETWORKING).....	71

CAPITULO 4. HERRAMIENTAS ÚTILES DESDE LA LÍNEA DE COMANDO.

4.1 EXHIBIENDO INFORMACIÓN DEL SERVIDOR.....	80
4.2 INTRODUCIÉNDONOS A EL MODO DE MANTENIMIENTO DESDE LA LÍNEA DE COMANDO.....	81
4.3 MONITOREANDO EL USO DEL CPU.....	81
4.4 MONITOREANDO EL USO DE LA MEMORIA RAM.....	82

4.5 MONITOREANDO EL DESEMPEÑO DEL ALMACENAMIENTO.....	85
4.6 MONITOREANDO EL USO DE LA RED (NETWORKING).....	86

CAPITULO 5. SEGURIDAD DE LA INFRAESTRUCTURA VIRTUAL EN GENERAL.

5.1 CONFIGURANDO EL CONTROL DE ACCESO AL SERVIDOR VCENTER.....	88
5.2 ADMINISTRACIÓN DE PERMISOS.....	90
5.3 FORTALECIENDO LA SEGURIDAD DEL VCENTER EN LA COMPUTADORA SERVIDOR.....	91
5.4 SEGURIDAD EN LA RED DE CONTROL DE ACCESO A LA CONSOLA DE SERVICIO.....	92
5.5 AUTENTICACIÓN MEDIANTE EL SERVICIO DEL DIRECTORIO ACTIVO.....	93
5.6 IMPLEMENTACIÓN DE UNA POLÍTICA DE CONTRASEÑA PARA CUENTAS LOCALES.....	94
5.7 RESPALDOS EN EL AMBIENTE VIRTUAL ----EL RESPALDO CONSOLIDADO VIRTUAL.....	95
5.8 RESTAURACIÓN DE RESPALDOS.....	97

CONCLUSIONES.....	98
Referencias Web y Bibliografía.	99

INTRODUCCIÓN.

La elección de este tema obedece a la razón, de que en los últimos años, la tecnología ha avanzado exponencialmente, y por ende, las soluciones a la problemática en informática en el campo de IT (Information Technology), por lo cual se han desarrollado tecnologías más complejas para el procesamiento automatizado de datos.

En la actualidad las aplicaciones son un recurso informático vital, así como el soporte para las mismas, las hay de alta, mediana y baja prioridad. Es por eso que la industria de IT ha generado nuevas tecnologías que además, son herramientas poderosas en el desarrollo del procesamiento de datos y su mantenimiento; esta investigación, esta enfocada a la virtualización, como un recurso informático, con una amplia gama de alternativas a la solución de cualquier problemática que involucre una tarea virtualizable.

Pero, ¿Qué en realidad es la Virtualización en términos informáticos? En Informática, **virtualización** se refiere, a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor, Monitor de máquina virtual), que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución.

Esta capa de software (VMM) maneja, gestiona y arbitra, los cuatro recursos principales de una computadora (CPU, Memoria, Red, Almacenamiento), y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. De modo que nos permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico.

La virtualización como tal, no es un concepto nuevo, hablaremos de sus orígenes y evolución hasta el día de hoy; en nuestra investigación nos enfocaremos a aplicaciones de una compañía líder en productos de solución virtualizable, que ha ido desarrollando aplicaciones cada vez más complejas y completas, sobresaliendo de entre muchas compañías y productos de Virtualización.

VMware es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un ordenador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (**simulador**), proporciona un ambiente de ejecución similar a todos los efectos de un ordenador físico (excepto en el puro acceso físico al hardware simulado), con el CPU (puede ser más de una), el BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

Un virtualizador por software permite ejecutar (simular), varios ordenadores (sistemas operativos), dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. No obstante, y al ser una capa intermedia entre el sistema

físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos, suficiente para usarse en entornos de producción.

VMware es similar a su homólogo **Virtual PC**, aunque existen diferencias entre ambos que afectan a la forma en la que el software, interactúa con el sistema físico. El rendimiento del sistema virtual, varía dependiendo de las características del sistema físico en el que se ejecute, y de los recursos virtuales (CPU, RAM, etc.), asignados al sistema virtual.

Mientras que Virtual PC emula una plataforma x86, VMware la virtualiza, de forma que la mayor parte de las instrucciones en VMware, se ejecuta directamente sobre el hardware físico, mientras que en el caso de Virtual PC, se traducen en llamadas al sistema operativo, que se ejecuta en el sistema físico.

Así pues, **VMware Inc.**, (VM de *Virtual Machine*), es una empresa filial de EMC Corporation, que proporciona la mayor parte del software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen **VMware Workstation**, y los gratuitos; **VMware Server** y **VMware Player**. El software de VMware puede funcionar en Windows, Linux, y en la plataforma Mac OS X, que corre en procesadores INTEL, bajo el nombre de **VMware Fusion**. El nombre corporativo de la compañía es un juego de palabras, usando la interpretación tradicional de las siglas «VM», en los ambientes de computación, como máquinas virtuales (**Virtual Machines**).

En nuestra Investigación, hablaremos más a detalle de un producto en específico de esta compañía, la infraestructura de servidores VMware ESX, que es una plataforma de virtualización a nivel de centro de datos. Es el componente de su producto VMware Infrastructure, que se encuentra al nivel inferior de la capa de virtualización, el hipervisor, aunque posee herramientas y servicios de gestión autónomos e independientes.

Está compuesto de un sistema operativo autónomo, que proporciona el entorno de gestión, administración y ejecución al software hipervisor, y los servicios y servidores que permiten la interacción con el software de gestión y administración con las máquinas virtuales.

La virtualización ofrece muchas ventajas significativas, incluyendo la consolidación de servidores, el servidor de rápido aprovisionamiento, nuevas opciones en la recuperación de datos en caso de desastres, una seguridad más robusta y mejores oportunidades para mantener un servicio de alto nivel, por nombrar algunos.

Tal vez la razón más común es la consolidación de servidores. Así pues, otros beneficios son: el poder mejorar el uso de nuestros procesadores, mientras que se produce la reducción de las necesidades de espacio del RACK, y consumo de energía en el centro de datos. Dicha tecnología nos proporciona una visión excelente de por qué, la virtualización se ha convertido en una solución tan popular. El simple proceso de mover un servidor de un centro de datos de un cierto lugar a otro, que si se hiciera de manera física sería más complejo.

El presente trabajo es una guía muy completa de principio a fin, que va llevando paso a paso en cada proceso, de cómo instalar, configurar, administrar y monitorear, un entorno virtual usando la infraestructura VMware ESX y todos los productos involucrados, derivados de la suite de VMware.

El objetivo principal es dar a conocer todos los elementos de la tecnología, sus beneficios y su desempeño en el ámbito de la Virtualización para el campo de IT. El desarrollo de la investigación se realizara mediante las siguientes etapas:

1. Exposición de los fundamentos de la tecnología.
2. Explicación detallada de los procesos de instalación, configuración, dispositivos de almacenaje y Networking.
3. Explicación de la seguridad en todos los niveles, monitoreo a través de la línea de comando, y prevención en caso de desastre, Backup (respaldo) de recursos virtualizables, así como una conclusión del uso de la tecnología de VMware ESX.

CAPITULO 1

HISTORIA DE LA VIRTUALIZACIÓN.

1.1 ORIGENES Y EVOLUCION DE LA VIRTUALIZACION.

La virtualización empezó a desarrollarse en la década de los sesenta para particionar los mainframes de gran tamaño, a fin de mejorar su utilización. En la actualidad, los ordenadores basados en la arquitectura x86, tienen que resolver los mismos problemas de rigidez e infrautilización, que se planteaban para los mainframes en aquella década. VMware inventó la virtualización para la plataforma x86, en la década de los noventa para abordar los problemas de infrautilización y de otra índole, a lo largo de un proceso que obligó a superar gran cantidad de desafíos. En la actualidad, VMware es líder mundial en virtualización para x86, con más de 190,000 clientes, incluido el 100% de las empresas de la lista Fortune 100. [1,8]

1.1.1 Los comienzos: Virtualización de Mainframes.

Fue IBM, quien empezó a implementar la virtualización hace más de 30 años, como una manera lógica de particionar ordenadores mainframe en máquinas virtuales independientes. Estas particiones, permitían a los mainframes realizar múltiples tareas: ejecutar varias aplicaciones y procesos al mismo tiempo. Dado que en aquella época los mainframes eran recursos caros, se diseñaron para particionar como un método de aprovechar al máximo la inversión. [1,8]

La virtualización se abandonó de hecho en las décadas de los ochenta y principios de los noventa, cuando las aplicaciones cliente-servidor y los servidores x86, y escritorios económicos, establecieron el modelo de informática distribuida. La amplia adopción de Windows y la emergencia de Linux como sistemas operativos de servidor en los años noventa, convirtieron a los servidores x86, en el estándar del sector informático. El incremento de implementaciones de servidores x86 y escritorios, generó nuevos problemas operacionales y de infraestructura de TI. Entre estos problemas se incluyen los siguientes:

- **Baja utilización de la infraestructura.** Las implementaciones típicas de servidores x86 logran un promedio de utilización de entre un 10% y un 15% de la capacidad total, según señala la International Data Corporation (IDC), una empresa de estudios de mercado. Normalmente, las organizaciones ejecutan una aplicación por servidor para evitar el riesgo de que las vulnerabilidades de una aplicación, afecten a la disponibilidad de otra aplicación en el mismo servidor.
- **Incremento de los costos de infraestructura física.** Los costos operativos para dar soporte al crecimiento de infraestructuras físicas han aumentado a un ritmo constante. La mayor parte de las infraestructuras de TI, deben permanecer operativas en todo momento, lo que genera gastos en consumo energético, refrigeración e instalaciones que no varían con los niveles de utilización.
- **Incremento de los costos de gestión de TI.** A medida que los entornos se hacen más complejos, aumenta el nivel de especialización de la formación y la experiencia

que necesita el personal de gestión de infraestructuras y consecuentemente, aumentan los costos asociados a dicho personal. Las organizaciones gastan cantidades desproporcionadas de dinero y recursos en tareas manuales ligadas al mantenimiento de los servidores, y aumenta la necesidad de la plantilla de personal para realizarlas.

- **Insuficiente protección ante desastres y Failover.** Las organizaciones se ven cada vez más afectadas por las interrupciones del servicio de las aplicaciones críticas del Servidor y la falta de acceso a escritorios de usuario final fundamentales. La amenaza de ataques a la seguridad, desastres naturales, pandemias y terrorismo han acentuado la importancia de la planificación de la continuidad del negocio, tanto en lo relativo a escritorios como a servidores.
- **Escritorios de usuario final de mantenimiento elevado.** La gestión y la seguridad de los escritorios empresariales plantean numerosos desafíos. Controlar un entorno de escritorios distribuidos y aplicar políticas de gestión, acceso y seguridad sin perjudicar la capacidad del usuario de trabajar con eficacia es complejo y costoso. Se tienen que aplicar continuamente muchos parches y actualizaciones en el entorno del escritorio para eliminar los riesgos de seguridad.

1.2 VMWARE INC.

VMware, Inc., es una empresa con sede en Palo Alto, California, con más de 7.500 empleados y clientes alrededor de 120.000, incluyendo el 100% de las Fortune 100. En el año 2007, tuvo ingresos de más de 1,33 mil millones dólares. VMware es una compañía de rápido crecimiento que se inició en 1998 y tiene ahora más de 20.000 asociaciones con empresas que van desde muy pequeñas a muy grandes.

VMWARE fue fundada en 1998 por Diane Greene, Vicepresidenta Ejecutiva de la Corporación EMC, y Presidenta de VMware. [1,10]

Green lleva más de veinte años desempeñándose en el terreno tecnológico, incluyendo posiciones de liderazgo técnico en Tandem, una firma especializada en sistemas de computación altamente resistente a fallas, Silicon Graphics, empresa pionera en gráficos 3D, Sybase, una importante firma que se dedica a la gestión de información; siendo también CEO de VXtreme, la cual se creó en 1995 con el objetivo de producir una solución de video por Internet de alta calidad, enfocado a los negocios.

Fundo la compañía con el objetivo original, de incorporar tecnología de máquinas virtuales de clase mainframe a los computadores estándar de la industria. VMware (Virtual Machine ware) fabricó su primer producto, VMware Workstation, en 1999 e ingresó al mercado de servidores en el 2001 con VMware GSX Server y VMware ESX Server. Con el lanzamiento de VMware Virtual Center en 2003 y la innovadora tecnología VMotion, la empresa se situó como uno de los sólidos líderes en el mercado, recientemente emergente de la Infraestructura virtual. En 1999, VMware introdujo la virtualización en los sistemas x86, como un medio para solucionar muchos de estos problemas y transformar dichos sistemas, en infraestructuras de hardware compartido de uso general que ofrecen un aislamiento completo, movilidad y opciones de elección del sistema operativo en los entornos de aplicaciones. A diferencia de los mainframes, las máquinas x86, no fueron

diseñadas para admitir una virtualización completa, por lo que VMware tuvo que superar muchos desafíos para crear máquinas virtuales a partir de la arquitectura x86.

La función básica de la mayoría de los CPU, tanto en mainframes como en PC, es ejecutar una secuencia de instrucciones almacenadas (es decir, un programa de software). En los procesadores x86, había 17 instrucciones específicas, que generaban problemas al virtualizar, y provocaban que el sistema operativo mostrara una advertencia, de que se cerraría la aplicación o simplemente que fallaría completamente. Como consecuencia, estas 17 instrucciones, constituyeron un obstáculo importante para la implementación inicial de la virtualización de ordenadores x86.

Para hacer frente a las instrucciones problemáticas de una arquitectura x86, VMware desarrolló una técnica de virtualización adaptable que las “atrapa” cuando se generan y las convierte en instrucciones seguras, que se pueden virtualizar y, al mismo tiempo, que permite al resto de instrucciones ejecutarse sin intervención. El resultado es una máquina virtual de alto rendimiento, que se adapta al hardware del Host, y mantiene una total compatibilidad de software. VMware fue pionero en esta técnica y actualmente es el líder indiscutido de la tecnología de la virtualización.

Los administradores empezaron a buscar productos de gestión de la virtualización, que les permitieran aumentar la escala de sus entornos virtuales, sin dejar de aprovechar los beneficios de los costos y mantener una alta disponibilidad. Con una mayor presión para seguir reduciendo los costos, ofrecer mejores soluciones de infraestructura, y "hacer más con menos", los administradores comenzaron a hacer una prioridad de la virtualización.

1.3 ¿QUÉ ES LA INFRAESTRUCTURA DE VMWARE ESX 3?

VMware Infraestructura ESX 3 (VI3), es fácilmente la plataforma de virtualización más utilizado hoy en día. Es bien probada y se ha utilizado en aplicaciones que van desde muy pequeño; instalaciones localizadas con sólo un puñado de servidores; a instalaciones excepcionalmente grandes de granjas de servidores en las grandes corporaciones. Su infraestructura es robusta, escalable, fácil de administrar, y flexible. También es pequeña y rápida, lo que significa que, las instalaciones virtuales que se ejecutan sobre esta, tienen más energía del procesador y otros recursos disponibles trabajando para estos, lo que en otras compañías se usaría un software mucho más pesado y complicado.

VMware Infraestructura ESX 3, es una plataforma autónoma, basada en su propio sistema operativo. Su sistema es como la mayoría de las plataformas al realizarse la virtualización, como se haría en una máquina virtual en plataformas Linux / Unix, Mac OS X, o de la plataforma Windows. [1,7]

Su plataforma se compone de varios productos importantes, incluyendo ESX, ESXi, vCenter Server, y el Conversor vCenter. VMware ha cambiado recientemente los nombres de sus componentes del VirtualCenter Server (ahora vCenter Server), y el cliente de VMware Infraestructura (en la actualidad vCenter cliente), sin embargo, los productos en

sí mismos no se han modificado, solo tienen nuevos nombres. Vamos a utilizar la nueva terminología en este trabajo. El nombre actual de VMware es el de ESX Server 3.5 y ESXi, los cuales son el corazón de la suite del producto del VI3. Funcionan como un hipervisor, o como la capa de virtualización, y es el pilar para el paquete entero del VI3 y VI4.

Durante el proceso de instalación para el Servidor ESX, se instalan dos componentes que interactúan el uno con el otro para proveer un ambiente dinámico y robusto de virtualización: La Consola de Servicio y el VMkernel.

1.3.1 La Consola de Servicio

Para todos los efectos, es el sistema operativo usado para manejar ESX Server y las máquinas virtuales que estén corriendo sobre el servidor. La consola incluye servicios similares, como en otros sistemas operativos, tales como un firewall, (el protocolo de manejo de redes simples), conocido como los agentes, y un web server. Pero no obstante, la Consola de Servicio carece de muchas de las características y beneficios que cualquier otro sistema tiene. Esta deficiencia, sirve como una ventaja real, en hacer de la Consola de Servicio una máquina de apoyo, de término medio de virtualización. [1]

El otro componente instalado es el **VMkernel**. Mientras la Consola de Servicio brinda acceso para el VMkernel, es este, el verdadero fundamento del proceso de la virtualización.

El VMkernel maneja y administra el acceso virtual de máquinas para el hardware físico subyacente, por medio de la programación de tiempos en el CPU, la administración de la memoria, y el interruptor virtual del proceso de datos.

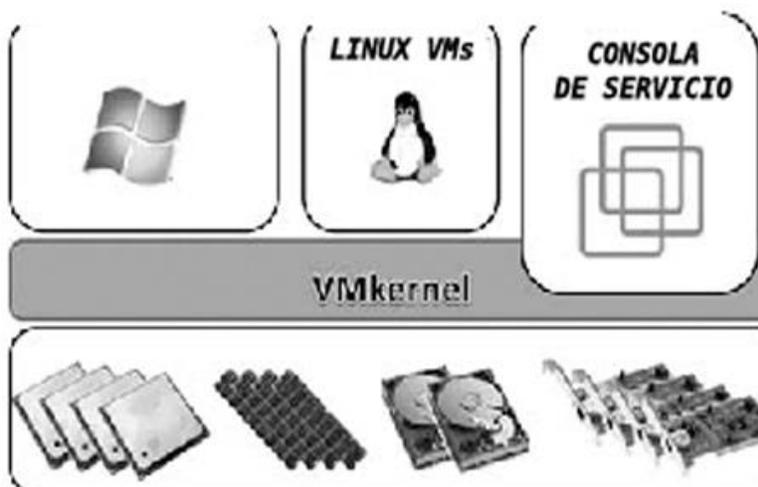


Fig. 1.1
Al instalar el servidor ESX se instalan los dos componentes interoperables:
1) La consola de servicio derivada de un ambiente Linux, 2) El VMkernel la máquina virtual administradora.

El ESXi es la siguiente generación del pilar de virtualización VMware, en la cual se soporta la carga para una arquitectura de 32 MB como la instalación de un hipervisor sólo. El ESXi es *sólo* un hipervisor y no brinda seguridad en una Consola acompañante de Servicio.

1.3.2 El VMware Virtual SMP

El producto de Multiprocesamiento del VMware Virtual Symmetric (SMP), está contenido en la infraestructura virtual. Les sirve a los administradores para construir máquinas virtuales con procesadores virtuales múltiples. El VMware Virtual SMP le permite a ESX Server, ser instalado en servidores con múltiples procesadores; Es la configuración de procesadores múltiples *dentro de* una máquina virtual. [1]

Las diferencias se aprecian en la siguiente figura.

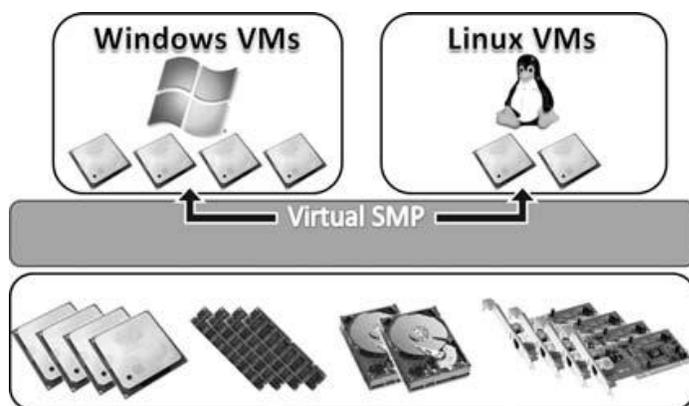


Fig. 1.2
El VMware Virtual SMP
Soporta la creación de máquinas virtuales con dos o cuatro procesadores y núcleos. Que actúan como procesadores físicos. Así como memoria RAM, y tarjetas de Ethernet.

1.4 ¿QUÉ ES VMWARE VSPHERE 4.0?

En junio de 2009 VMware ESX 4.0 fue lanzada al mercado, y ahora entra en los productos de la VSphere 4.0 suite. La suite VSphere 4.0 engloba tanto vCenter y ESX 4.0, junto con otros productos que no se discutirán en este trabajo. Esta nueva versión no sólo trae mejoras acrecentadas, sino que incorpora la plataforma de virtualización a un nuevo nivel, que le permite al usuario pensar en términos de instalaciones completas o implementaciones en lugar de gestionar solo un sitio servidor por servidor. [4,10]

Cabe mencionar que ESX 4.0 es un producto totalmente nuevo:

- ESX 4 es de 64-bits, en comparación con las versiones de 32-bit de ESX 3.x
- ESX 4 soporta más hardware y más máquinas virtuales.

La nueva versión pone la línea para los productos de virtualización comercial aún mayor, con nuevas características como tolerancia a fallos, VShield, interruptores distribuidos, y mucho más.

ESX 4.0 trae un enorme conjunto de mejoras en el ámbito de almacenamiento en ESX. El aprovisionamiento a medida para los discos virtuales permite a las máquinas virtuales utilizar el almacenamiento según sea necesario, eliminando una fuente importante de espacio desperdiciado en un área de almacenamiento.

Aquí hay 10 características que vsphere4 presenta como mejoras a sus antecesores.

1.4.1 El servidor del vCenter en modo vinculado.

Este modo le permite conectar servidores múltiples del vCenter en una forma moderna "vinculada". Hacer esto les permite compartir licencias y roles, y provee con una visión general, del ambiente virtual completo.

1.4.2 Perfiles del Host

Los perfiles del Host, son provistos en la modalidad de la suite Enterprise, sirven para facilitar la sustitución de una plantilla de un servidor ya existente ESX por un servidor nuevo. Esta característica es un beneficio enorme, ya que no se necesita otra vez, manualmente, configurar redes, almacenamiento, etcétera, dentro de su nuevo servidor ESX.

1.4.3 El desempeño, las gráficas, y los acontecimientos.

El CPU, la memoria, el almacenamiento, y las gráficas de redes serán ahora exhibidos en una página central. Con una visión más clara de gráficas mejoradas, los clientes se beneficiarán con los mensajes de acontecimiento más exactos, los ajustes de alarma, y los errores reportados.

1.4.4 La VMoción de almacenamiento dentro de vCenter.

Se puede iniciar una VMoción de almacenamiento dentro del cliente del vCenter. Esto elimina la necesidad de hacerlo por la línea de comando o tener que instalar pluggins adicionales de otras compañías como se hacía en las versiones Esx 3.x

1.4.5 La VMoción ha sido mejorada.

La compatibilidad de VMoción mejorada (EVC por sus siglas en ingles) le permite a los clientes iniciar la compatibilidad VMoción entre Intel FlexMigration y AMD-V tecnologías extendidas de Migración. Esto quiere decir que ahora se puede mover un servidor en uso entre Host, usando diferentes tecnologías de un CPU.

1.4.6 La máquina virtual en uso con un soporte implementado.

Se le puede añadir los recursos al CPU y a la memoria de una máquina virtual existente sin tener que reiniciar la maquina virtual.

1.4.7 Las mejoras virtuales del hardware de la máquina.

Las máquinas virtuales ahora pueden escalarse emulando ocho procesadores virtuales SMP y hasta 255GB De RAM.

El VSphere soporta a los dispositivos IDE, la interfaz de sistemas informáticos SCSI por Serial (SAS), y VMXNET que es la tercera generación del soporte de la red.

1.4.8 Las mejoras físicas de Nodo.

Los hosts físicos ahora pueden tener hasta 1TB de memoria, 64 CPUs lógicos, y 320 máquinas virtuales corriendo dentro de ellos. La arquitectura de 64 bit del ESX4 le permite mayor capacidad de memoria, mejor desempeño, y un soporte del hardware invaluable en comparación con las versiones previas.

1.4.9 Las mejoras de almacenamiento.

ESX 4.0 trae un set enorme de mejoras para el área de almacenamiento dentro de ESX. El abastecimiento para discos virtuales, permite a las máquinas virtuales utilizar almacenamiento en base según las necesidades, eliminando una fuente principal de espacio desperdiciado en un área de almacenamiento de la red (SAN). La característica VMFS Volume Grow, le permite dinámicamente, aumentar un sistema de Archivo de Máquina Virtual, sin cortar el uso a las máquinas virtuales encendidas. Hay también soporte mejorado, para el servicio de red de archivos y los iniciadores del software iSCSI, el cual, da un soporte del suministro para FramesStations de tamaño gigante desde 1GB hasta redes locales de 10GB.

1.4.10 El interruptor distribuido.

Un interruptor distribuido es provisto en la modalidad Enterprise plus, que nos permite a los usuarios, crear un switch virtual para todos los hosts ESX para conectar y utilizarse. Esto ayuda a reducir el mantenimiento de la red y les permite a las máquinas virtuales ser migradas a cualquier otro Host, usando la VMoción, sin tener que preocuparse por las conexiones de la red.

1.5 DIFERENCIAS ENTRE ESX 3.5 Y ESX 4

En seguida se presenta una tabla comparativa entre la versión más reciente y la pasada: VMware vSphere 4.0. (ESX 4.x) y productos Virtuales de Infraestructura (ESX 3.x) tienen configuraciones de máximos, dentro de un margen en el cuál pueden funcionar correctamente. Se incluye esta información realmente relevante para la planificación antes de instalar una de las dos tecnologías y ver cual se adapta más a nuestras necesidades, si el ESX/ESXi 3.x/4.x o vCenter. Estos valores pueden ser cruciales al planificar el ambiente virtual. A través de ellos, nos podemos familiarizar con los máximos diferentes. [1,10]

Tabla 1.1 Máximos de configuración de las dos Infraestructuras. [1,10]

Detalle/ Valor	Máximo ESX 3.5	Máximo ESX 4.0
Numero de CPUs virtuales por m/virtual	4	8
SCSI adaptadores por m/virtual	4	4
Dispositivos por adaptador SCSI	15	15
SCSI targets por m/virtual	60	60
Tamaño del disco SCSI	2TB	2TB
Tamaño de RAM por m/virtual	64GB	255GB
Tamaño de archivo swap por m/virtual	64GB	255GB
Numero de NICs por m/virtual	4	10
Numero de dispositivos IDE por m/virtual	4	4
Numero de controladores IDE por m/virtual	1	1
Número de unidades floppy por m/virtual	2	2
Numero de puertos paralelos por m/virtual	3	3
Numero de puertos seriales por m/virtual	4	4
Numero de CPUs virtuales por host	128	256
Numero de procesadores por host	32	64
Numero de CPUs lógicos (con hyperthreading)	32	64
Numero de CPUs virtuales por núcleo	8 (se incrementan a 20 en update)	20
Cantidad de RAM por host	128GB (se incrementa a 256GB en update)	- 512GB
Numero de consolas remotas en m/virtual	10	40
VMDirectPath PCI/PCIe dispositivos por m/virtual	-	2
VMDirectPath SCSI targets por m/virtual	-	60

1.6 VMWARE VCENTER (DATACENTER)

VMware VirtualCenter es la consola de comando central y de control, usado en el entorno del VMware, para configurar, aprovisionar, y manejar los ambientes virtualizables de la suite Enterprise. VirtualCenter fue primero lanzado como la versión 1.0, cuando VMware ESX Server estaba en la versión del 2.0.1, desde entonces se han sumado aun más características y mayor funcionalidad. [1,2]

VMware ha puesto conjuntamente y ha lanzado una herramienta para el VMware Datacenter, que es la hoja contable de la calculadora de tamaño de la base de datos es imprescindible conocerla al planear la instalación del datacenter. La calculadora estimará el tamaño de la base de datos del VirtualCenter, después de cierto tiempo que ya este corriendo dicha base. Esta estimación se calcula basada en información provista acerca de la VMware Infrastructure 3, la implementación, como el número de hosts y máquinas virtuales. Hay dos versiones de la calculadora para el VirtualCenter 2: La versión de 2.0.1 Patch 2 y otra para VirtualCenter 2.0.1 Patch 2 o posterior.

Actualmente hay cinco componentes que conforman al VirtualCenter.

1. **VirtualCenter Management Server** es el puesto de control central para toda configuración, es el abastecimiento y la administración del ambiente del VMware.
2. **VirtualCenter Database** es la parte clave de almacenamiento, usado para almacenar toda la información del servidor físico, las piscinas del recurso así como también las máquinas virtuales que son manejadas por el VirtualCenter.
3. **El cliente virtual de Infraestructura** es el cliente administrativo usado para conectar y maneja al VirtualCenter Servidor de administración o el VMware ESX servidor directamente.
4. **VirtualCenter Agent** es el agente del servidor ESX usado para conectarse a VirtualCenter en el servidor VMware ESX. Es bueno saber si tenemos un problema es recomendable algunas veces reiniciar el servicio de el mware-ypxa al igual que mgmt-vmware de los hosts del VMware ESX.
5. **La infraestructura virtual para el acceso a red.** Le permite la administración virtual de las máquinas, así como regula el acceso para consolas sin necesidad del uso del cliente. Sin embargo este método es sumamente limitado en su funcionalidad.

La Gerencia de gran escala

El VirtualCenter puede soportar y manipular hasta 200 hosts (sistemas anfitriones) y 2000 máquinas virtuales con una sola instancia del Datacenter (VirtualCenter).

El VMkernel es el núcleo, semilla o pilar, en la cual está todo el software construido: Es el sistema operativo. Es muy parecido al kernel de Linux, (y está construido en base al core de Linux), sin necesidad de cualquier otro software. La Consola de Servicio (o COS) es una forma de alternativa para comunicarse con este y configura al VMkernel usando el estándar de Linux y comandos específicos de VMware para modificar y ajustar los parámetros. Típicamente, la administración se hará por el cliente del Vcenter; Sin embargo,

pueden haber casos donde se puede lograr tareas más fácilmente desde línea de comando pero a veces se tendrá que usar porque no se tendrá acceso al Vcenter.

La tecnología de VMware ha diseñado El Servidor ESX para funcionar sólo con partes específicas de hardware y tiene el soporte con la opción a quitar cualquier clase de dispositivos que no se estarán usando, por consiguiente se aligera el código del kernel, lo cual permite una ligera instalación del kernel y paquetes de herramientas con poco siendo completamente autónomo y personalizable sin necesidad de otro sistema operativo. Esto es una de las cosas que le da al VMware una ventaja por encima de otras tecnologías de virtualización que requieren instalación sobre una plataforma estándar como sistema base, por lo que solo tendría instalado controladores y características que se usaran. Es realmente importante verificar el hardware sobre el cual se correrá el entorno de virtualización, porque VMware no soportara directamente hardware de cualquier PC de escritorio.

Sin embargo, todo lo que un servidor necesita, estará bien soportado. Esto es que instalara el sistema operativo más ligero que soporte con lo menos posible y aun sea funcional, las máquinas virtuales y el hardware.

Capítulo 2. VIRTUALIZACION DE SERVIDORES.

A continuación explicaremos la instalación detallada de ESX 3.5 la cual es muy parecida al entorno de Linux y su instalación, en concreto con la distribución de Red Hat, es así que el instalador ha tomado como base al wizard (instalador) de Red Hat haciendo algunas modificaciones. [1,9]

ESX 4.0 y ESXi 4.0, ahora pueden ser instalados y virtualizados dentro de la VMware Workstation y VMware Fusion. Esto es realmente fabuloso ya que permite instalar, probar, y obtener una percepción del producto en un ambiente virtualizado antes de implementarlo en el hardware físico. Antes de comenzar a instalar el ESX, se deberá comprobar que el hardware es completamente compatible visitando al siguiente URL, se notará que el ESX 3.5 tiene un rango más amplio de soporte de hardware que su sucesor más nuevo, el ESXi:

2.1 EL SERVIDOR ESX 3.5 LA INSTALACION.

ESX Server 3.5, tiene los siguientes requisitos del hardware, (véase los máximos de configuración en la tabla del capítulo anterior, [Tabla 1.1]):

- Al menos dos procesadores de entre 1500MHz como el Intel Xeon y posteriores, AMD Opteron (de 32 bits), 1500MHz Intel ViiV, o procesadores - AMD A64 X2 - de doble core.)
- 1GB de memoria RAM mínimo
- Uno o más controladores de Ethernet (se recomienda un mínimo de cuatro puertos para la consola de servicio, VMkernel, Virtual Machine Network, etc.)
- Almacenamiento directo acoplado (DAS) o una red de almacenamiento acoplado (NAS).

Para evitar la posible de pérdida de datos hay que asegurarse de remover cualquier tipo de dispositivo de almacenamiento, como: Canal de Fibra, DAS, o discos ISCSI, antes de iniciar la instalación del ESX. [1, 8,9]

El instalador tiene un par de modos:

2.1.1 El modo gráfico

Es el método recomendado para la instalación. Usa un ratón y una interfaz gráfica para guiarnos a través de la instalación. Éste es el método que usaremos.

2.1.2 El modo del texto

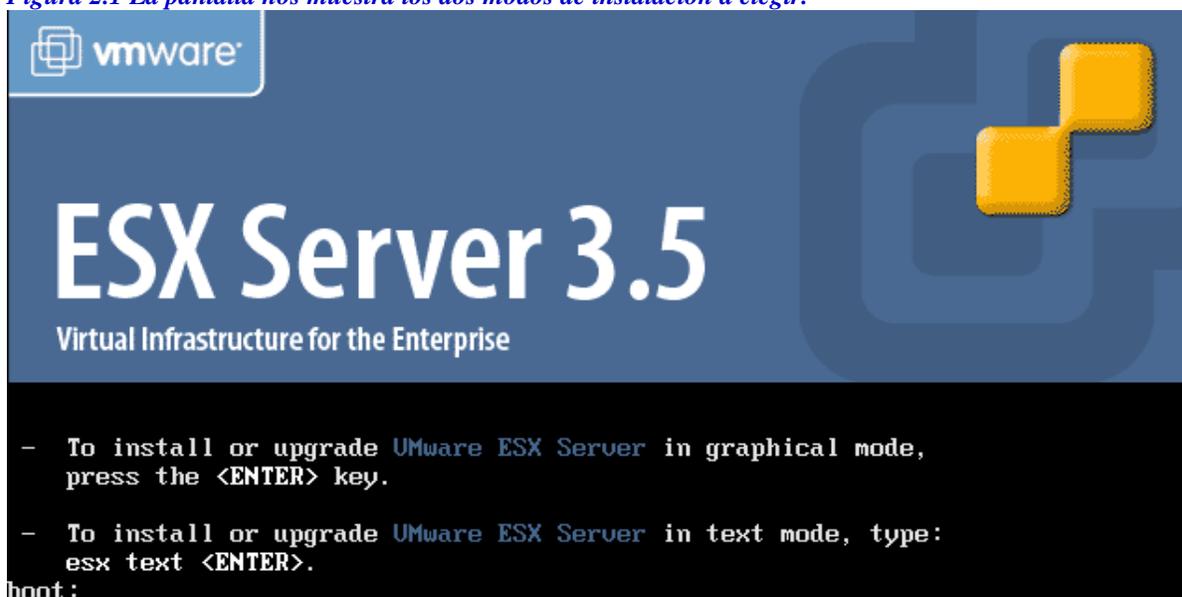
Un modo único en texto para instalar el ESX; esta opción es normalmente usada cuando se tiene problemas con el mouse o problemas de vídeo en el instalador gráfico. Para empezar la instalación, hay que asegurarse de que el servidor ESX, ha sido configurado para arrancar desde el CD, esto se configura desde el BIOS. Después, se presentan los pasos siguientes.

Al arrancar desde el CD-ROM, se presentara la primera pantalla que permite elegir el método de instalación. Presionamos la tecla enter, para aceptar el método por defecto que

es el instalador gráfico. Si se teclaea el modo texto sería **esx text**, para invocar el modo de texto. (Figura 2.1).

El instalador comenzará a cargar, se desplegará otra pantalla que permitirá realizar una prueba de CD-ROM para detectar errores. Si se desea seguir con el test, se usa la tecla tabulador, para iluminar y elegir el modo de prueba (Test button); De otra manera, se presiona la tecla Salto (skip) para continuar la instalación (Figura 2.2).

Figura 2.1 La pantalla nos muestra los dos modos de instalación a elegir.



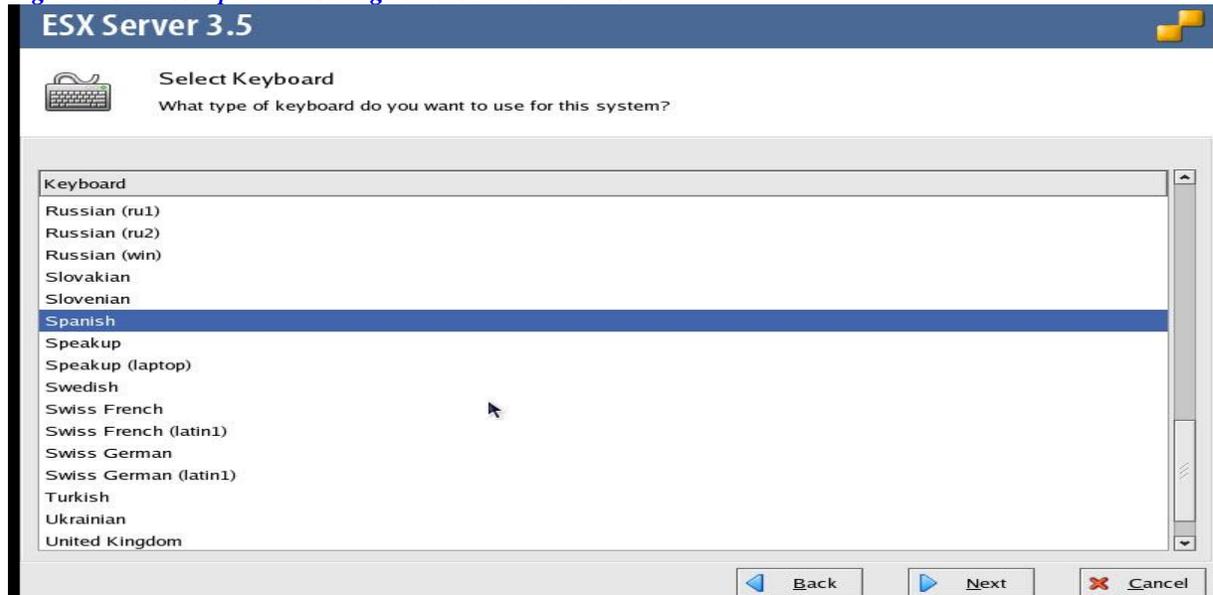
Aparecerá otra pantalla que nos indica que se llevara a cabo el test de CD, porque lo detecto, si se está ejecutando la instalación desde una imagen de ISO o desde la unidad de CD, y se sugiere presionar saltar el paso si así fuere necesario.

Figura 2.2 La pantalla nos muestra si se desea realizar la prueba del CD.



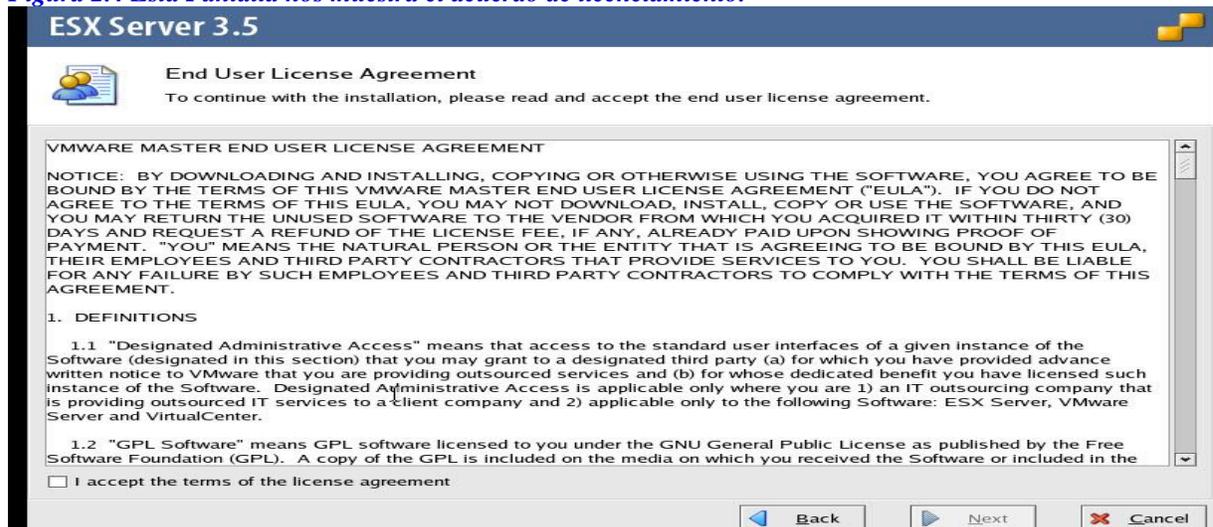
1. Una pantalla de bienvenida será presentada. Daremos un clic sobre el botón siguiente para proceder hacia la configuración de nuestro teclado, donde se seleccionará la configuración de teclado predeterminado en español. Damos un clic en siguiente para continuar.

Figura 2.3 En esta pantalla se elige el idioma del teclado.



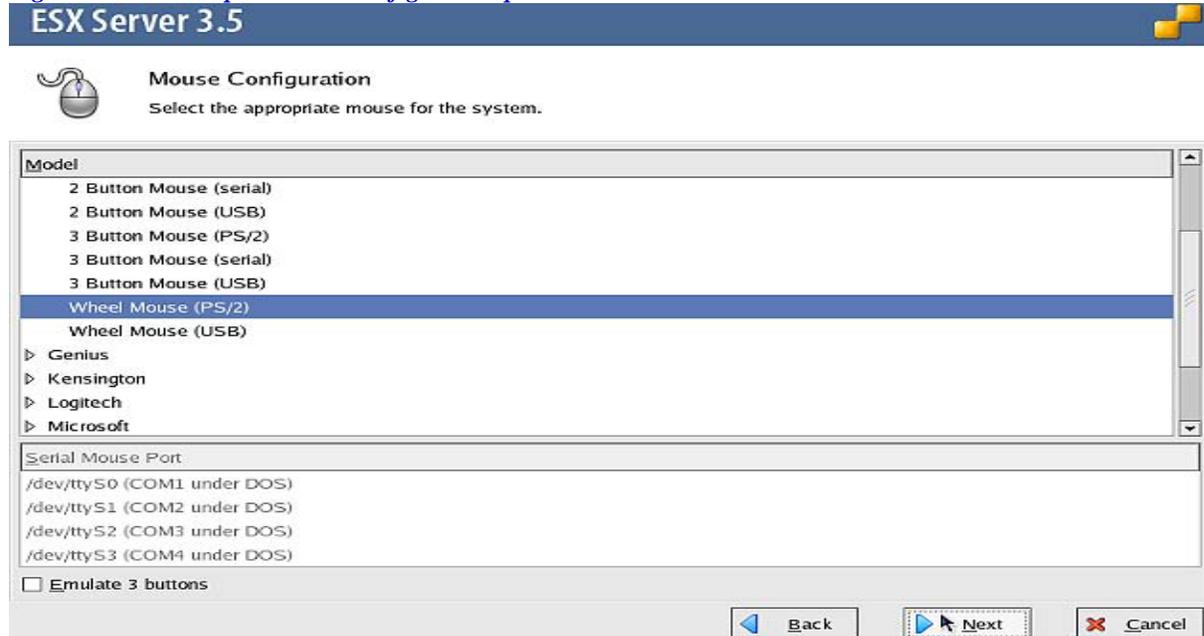
2. El menú de configuración del ratón aparece, permitiendo seleccionar al tipo de ratón para su ESX Server. Daremos aceptar por defecto así como esta. A continuación damos un clic sobre el Siguiente botón.
3. La pantalla del acuerdo de licencia ESX aparecerá. Seleccionamos "Acepto Los términos de este acuerdo de licencia" y damos un clic en siguiente:

Figura 2.4 Esta Pantalla nos muestra el acuerdo de licenciamiento.



Damos un clic y procedemos a la siguiente pantalla.

Figura 2.5 En esta pantalla se configura el tipo de mouse.



4. El instalador comenzará en busca de versiones de ESX previas. Si una es encontrada, se recibirán las siguientes opciones:

2.1.3 UPGRADE

Esta opción puede servir para actualizar un servidor existente ESX; Sin embargo, esto no es recomendable. Es mejor usar el Update Manager dentro de la suite de VCenter, ya que es un método mucho más seguro.

2.1.4 INSTALAR

Esto instalará una versión limpia de ESX y borrará cualquier otra instalación previa existente, incluyendo todos los ajustes de configuración y datos.

Si ésta es la primera vez que el disco ha sido usado, el instalador también dará un aviso para inicializar en un disco vacío.

Figura 2.6 En esta pantalla se elige la opción de instalar por primera vez.



4. La pantalla de configuración de particiones aparecerá, para configurar las particiones del ESX Server.

Existen dos opciones aquí:

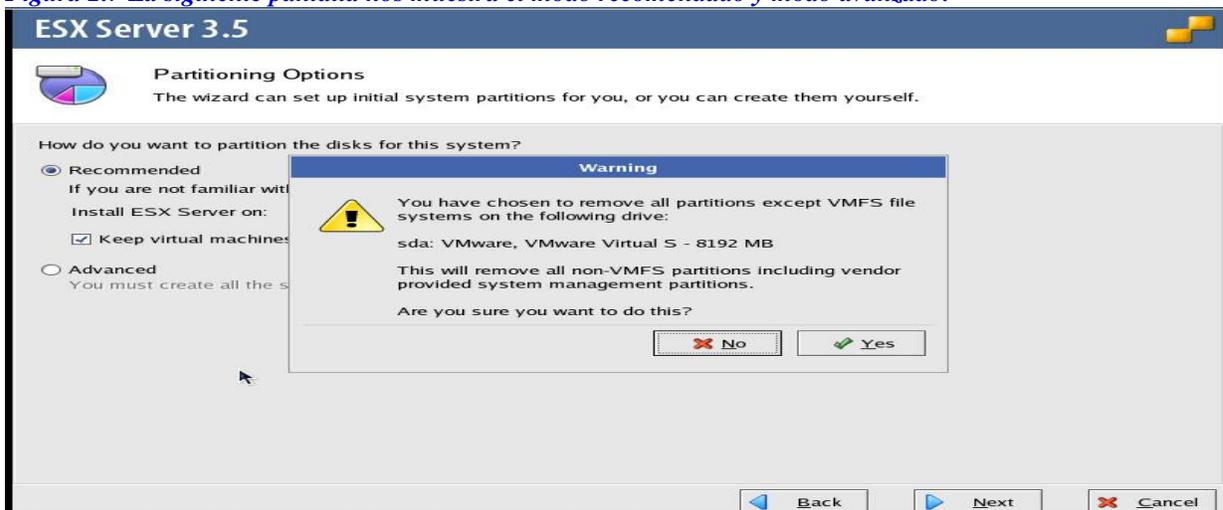
2.1.5 Modo Recomendado

Configura las particiones ESX predeterminadas basadas en el tamaño del disco duro. Este es el método recomendado, a menos que se requiera configurar particiones para una configuración personalizada a la medida.

2.1.6 Modo Avanzado

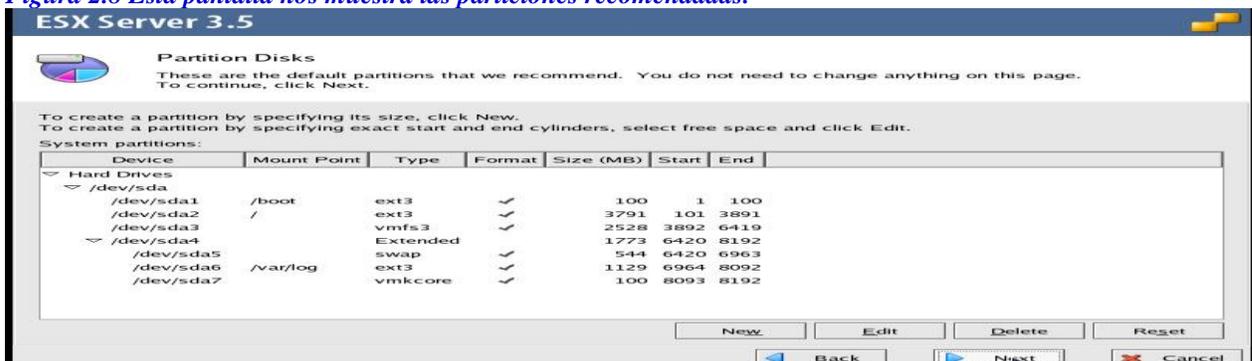
Este modo permite especificar cada ajuste de las particiones y los tamaños que tendrán, basándose en el tamaño del disco duro.

Figura 2.7 La siguiente pantalla nos muestra el modo recomendado y modo avanzado.



Escogeremos la partición del disco en el cual ESX será instalado, y damos un clic en la opción "mantener máquinas virtuales y el VMFS (el sistema virtual de archivo de máquina) que los contiene "; esto se realiza principalmente al instalar sobre otra instalación previa del ESX, para conservar cualquier máquina virtual existente y sus datos. Damos un clic sobre el botón siguiente para ver la configuración final, luego otro clic sobre el botón Siguiente para continuar.

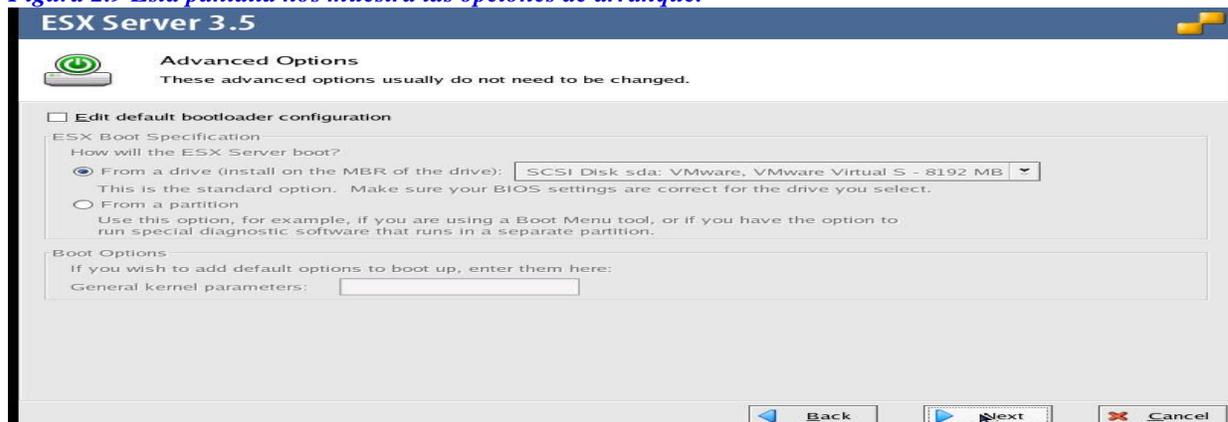
Figura 2.8 Esta pantalla nos muestra las particiones recomendadas.



Este es el modo personalizado si así se requiriera.

Para evitar la posible pérdida de datos nos aseguramos de remover cualquier unidad de almacenamiento conectada, como Canal de Fibra, DAS, o discos iSCSI, antes de la instalación inicial de ESX.

Figura 2.9 Esta pantalla nos muestra las opciones de arranque.



7. La configuración de la ventana de arranque (booteo), se cargará, dándonos opciones de cómo el servidor de Esx, iniciara. Hay dos opciones aquí:

2.1.7 Opciones

- **Desde el disco duro (instalación sobre el MBR del disco duro)**

El primer disco será seleccionado. Si se cambia esto, es importante que se seleccione el primer disco listado en el BIOS. Ya está activado por defecto, ésta es la opción que se utiliza en la mayoría de las instalaciones del ESX.

- **Desde una partición**

Esta opción servirá para instalaciones del legado donde el BIOS se guarda sobre un registro maestro del boot, (inicio).

2.1.8 Opciones de inicio (booteo)

Nos permite configurar parámetros específicos del kernel que será cargado al momento de reiniciar el ESX Server.

Como mencionados previamente, recomendamos dejar las selecciones predeterminadas para la configuración del bootloader.

Como una nota al margen, si se decide ir de los botones de Atrás o siguiente durante la instalación, nos aseguraremos que los ajustes predeterminados de selección no se cambien. Dé un clic sobre el botón siguiente para continuar.

8. La sección de configuración de la instalación de la red (**Figura 2.10**), nos permite especificar el tipo de red y el tipo de la dirección que se usará en el ESX Server. Esta pantalla está compuesta de cuatro secciones diferentes:

2.1.9 La Tarjeta De Interfaz De Red

La interfaz de la red que nuestro sistema de administración de red ESX Server usará.

Nos gusta usar la primera interfaz en el servidor o la tarjeta accesoria, principalmente porque Cuando se administra a un gran número de hosts físicos es más fácil acordarse de cuál interfaz está siendo usada en cada uno.

2.1.10 La dirección de la red y el nombre del host.

Se tiene la opción para usar a DHCP para nuestro servidor ESX, pero esto no es recomendado. Por defecto, nos será pedida una dirección IP estática. Llenaremos el resto de los campos vacíos de la configuración de la dirección IP de la red si así fuera necesario.

2.1.11 Ajustes para VLAN

Esto nos permitirá especificar si su ESX Server estará en un VLAN específico. Si no estamos seguros, consultaremos la configuración de la red local en la que estemos, para obtener esta información.

2.1.12 "Creando una red predeterminada para" máquinas virtuales.

Esta opción está habilitada por defecto. Debemos deshabilitarla porque nuestras máquinas virtuales serán colocadas en la misma red al igual que la consola de servicio/Administrador de la red. Después de entrar la información apropiada de la red, damos un clic sobre el botón siguiente para continuar. En la siguiente pantalla ([Figura 2.11](#)), seleccionaremos el huso/horario, en el cual nuestro Servidor ESX estará ubicado, en nuestro caso, será América/Mexico_city; Continuamos presionando el botón siguiente.

Figura 2.10 La pantalla nos muestra la configuración de la red.

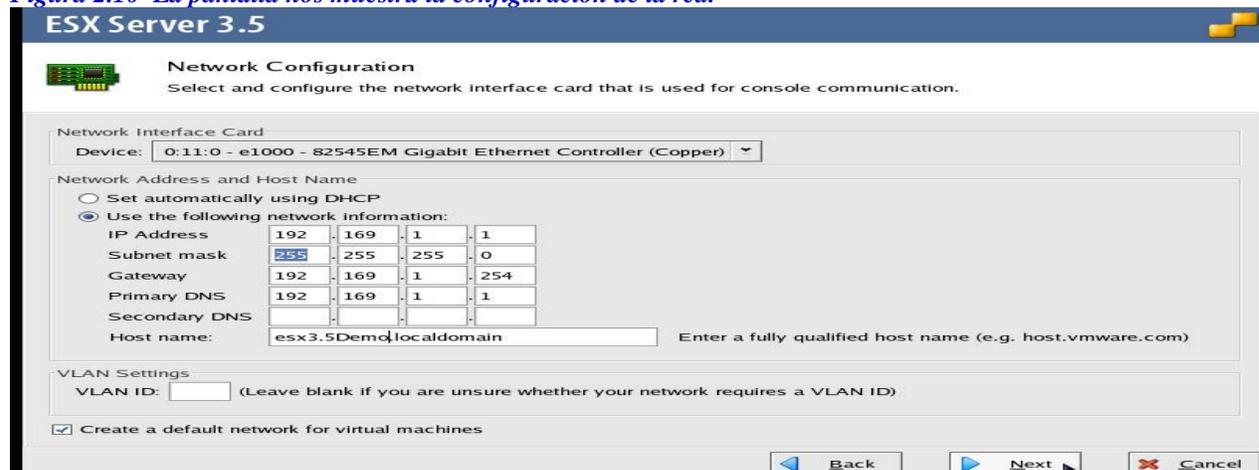
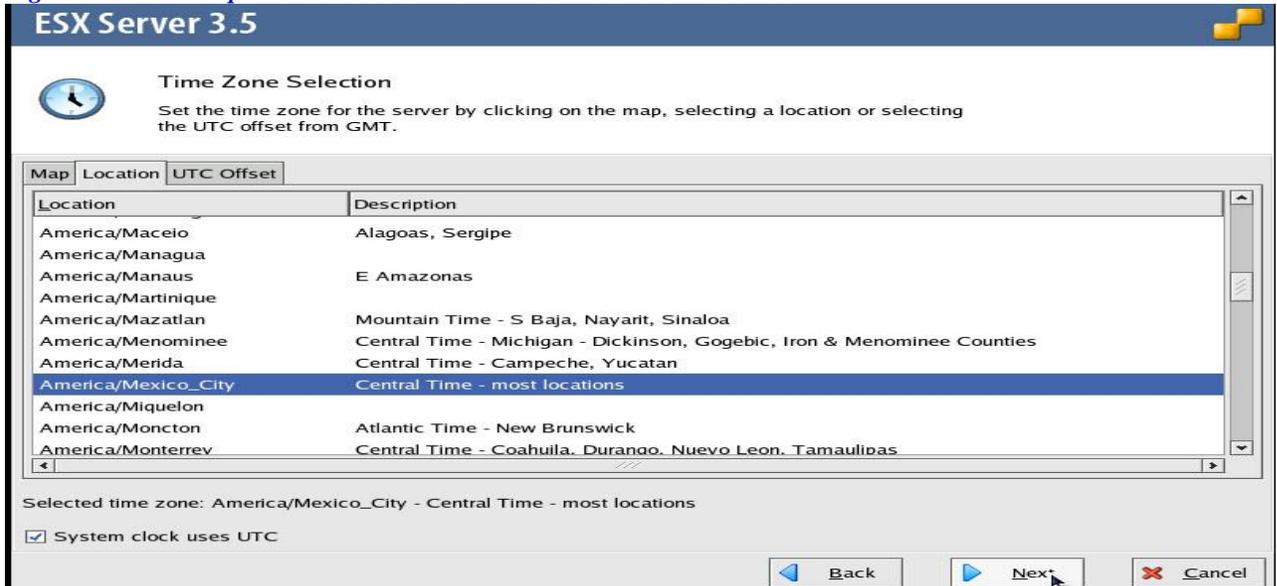


Figura 2.11 En esta pantalla se selecciona el Huso/Horario del sistema.



Una ventana nueva (Figura 2.12), aparecerá, pidiéndonos la contraseña de raíz. Introducimos la contraseña de raíz y damos de alta algunas cuentas adicionales que podríamos necesitar en nuestro Servidor de ESX, presionando el botón siguiente para continuar.

Figura 2.12 La pantalla nos muestra como se establece la contraseña de raíz.

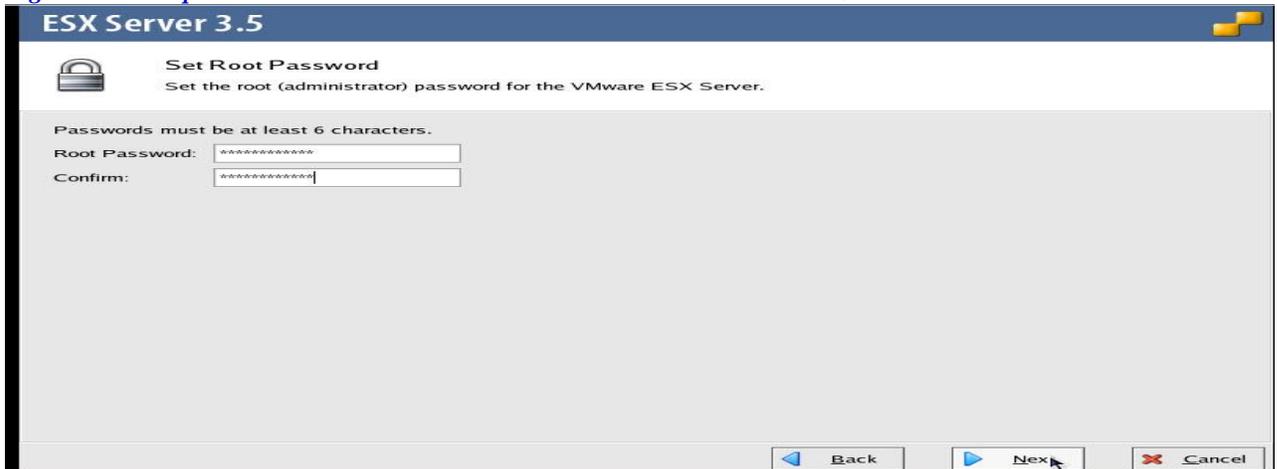
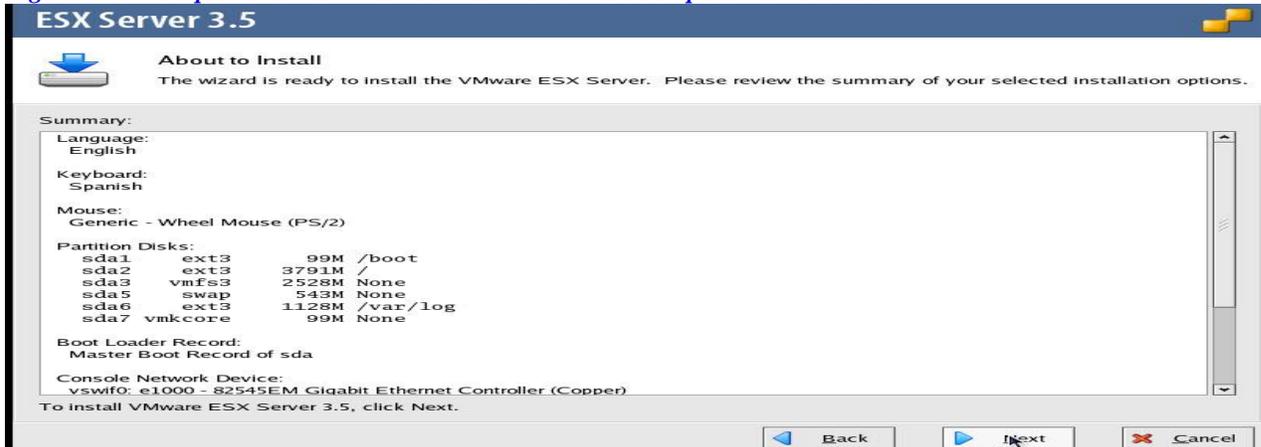
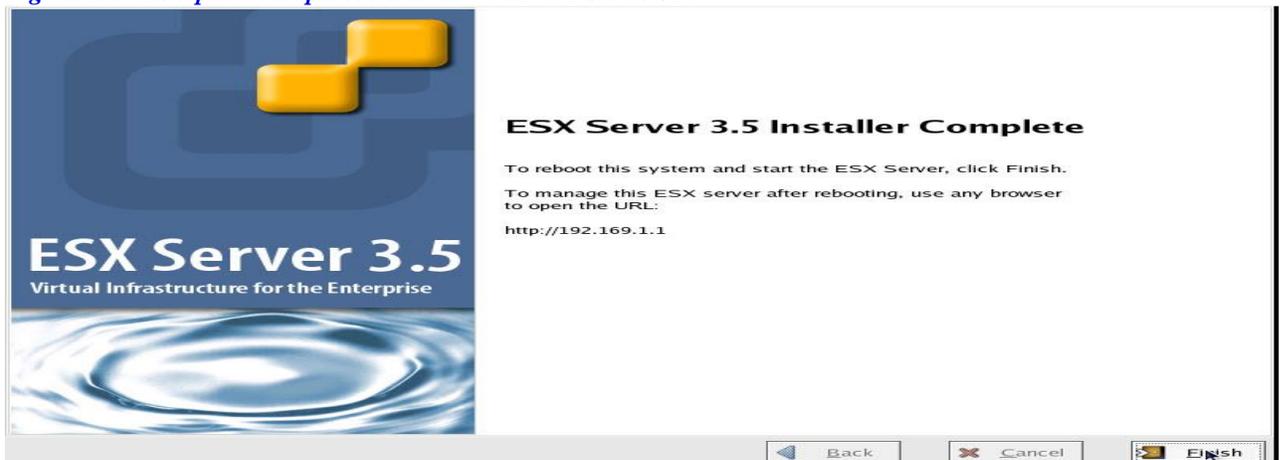


Figura 2.13 Esta pantalla nos muestra el resumen antes de empezar la instalación.



10. La ventana final que nos resta ver de la instalación es el resumen (Figura 2.13). Esta sería la última oportunidad que tenemos para hacer cualquier cambio en los ajustes de instalación que previamente hemos configurado, repasamos cuidadosamente, que todo esté bien. Presionamos el botón siguiente para empezar la instalación. Cuando toda la instalación termino, daremos un clic sobre el botón de terminar (Finish) y el instalador terminara y reiniciara el equipo y expulsara el CD de la unidad del CD rom.

Figura 2.14 Esta pantalla aparecerá al terminar la instalación.



En la pantalla inferior se ve como todo ha sido cargado con éxito.

Figura 2.15 Esta pantalla nos muestra que nuestro sistema ha empezado a trabajar.

```
VMware ESX Server version 3.5.0
Starting vmkernel initialization...
initializing memory ...
initializing chipset ...
initializing timing ...
initializing scheduler ...
initializing device support ...
initializing processors ...
initializing interrupts ...
Enabling interrupts ...
vmkernel loaded successfully.
```

2.2 EL VMWARE ESXI 3.5

El ESXi es una forma más nueva de la tecnología que procesa con lo mínimo posible. No incluye o depende de una consola de servicio y puede desempeñarse bien con el hiper-visor con una instalación que abarca un espacio de 32MB del disco. En el Servidor de ESX, la consola de servicio funciona con la parte superior del hipervisor a través de las máquinas virtuales instaladas. En el ESXi, el hipervisor es todo lo que se instala. [3,5] Esto permite las adiciones más rápidas de hardware en las piscinas (pools) existentes.

Si queremos añadir un nuevo servidor a nuestro rack, no tendremos problema, solo lo enlazamos, lo echamos a andar, instalamos el ESXi, colocamos la contraseña de raíz y detalles de sistema de redes, y nos tomara de un minuto a dos para configurar la red virtual y habremos acabado. Ésta es una forma asombrosamente rápida para crear o expandir un clúster ya existente de hardware de ESX. La versión instalable más asombrosa del ESXi es la versión incrustada (embebida). Es ahora posible comprar hardware que este pre-configurado con ESXi previamente instalado en él. Esto elimina por completo el paso de instalación y acelera el proceso de configuración.

Los beneficios de la utilización del ESXi sobre el producto estándar ESX, son; que este es sumamente liviano y se instala rápidamente, puede ser comprado en algunos servidores de compañías como DELL y de otros vendedores como una opción incrustada, no tiene consola de servicio, y requiere menos parches y mantenimiento. El ESXi está también disponible gratis e incluye las funciones básicas necesitadas para iniciar un ambiente virtual.

Antes de comenzar a instalar a ESXi, debemos comprobar que nuestro hardware es completamente compatible. ESX 4.0 y ESXi 4.0 ahora pueden ser instalados y virtualizados, dentro de una VMware Workstation y una VMware Fusión. Esto nos permite instalar, probar, y obtener una percepción real de los productos antes de implementarlos en nuestro hardware físico.

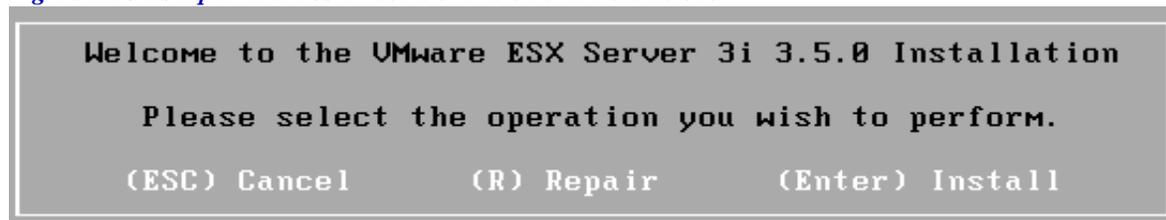
A partir de la Actualización 3, ESXi tiene los siguientes requisitos del hardware:

- 1500MHz en el procesador Intel Xeon y modelos posteriores o AMD Opteron (en modo de 32 bits) para ESXi.
- 1500MHz en el procesador Intel Xeon y modelos posteriores o AMD Opteron (en modo de 32 bits) para el Virtual SMP
- 1500MHz en el procesador Intel Viiv o AMD A64 X2 en procesadores de doble núcleo.
- 1GB de mínimo de RAM
- Controladores para la tarjeta de red Broadcom NetXtreme 570x Gigabit o los adaptadores del 100/1000 de Intel PRO.
- Adaptadores básicos SCSI-Adaptec Ultra160, Ultra320, Fusion-MPT de Lógica de integración a gran escala LSI, o la mayoría de los controladores para el NCR/Symbios SCSI.
- Adaptadores RAID-Dell PercRAID (Adaptec RAID y LSI MegaRAID) o controladores IBM ServeRAID.

Esta lista representa los requisitos mínimos para instalar a ESXi, pero muchos dispositivos más están disponibles. Para asegurarnos de una compatibilidad completa, buscaremos por nuestro hardware correcto en el siguiente url de la compañía VMWARE, en específico en: <http://www.vmware.com/resources/compatibility/search.php?action=base&deviceCategory=server> [w1]

Una vez que el booteo (arranque inicial) se ha completado, el instalador presentará un par de opciones: Podemos elegir cancelar la instalación, actualizar una instalación existente, o instalar una instalación nueva (Figura 2.16) del ESXi. Una vez que hemos seleccionado la instalación apropiada, será mostrado el EULA. Presionamos F11 para aceptar y continuar la instalación.

Figura 2.16 Esta pantalla nos muestra el inicio de la instalación.



Seleccionamos el disco en el cual deseamos instalar el ESXi. Típicamente, éste será nuestro disco local. También, nos aseguraremos haber desconectado cualquier dispositivo de SAN y dispositivos de almacenamiento de agregado directo, para prevenir cualquier pérdida de datos accidental. Una vez que hemos seleccionado el disco, la instalación comenzará y tomará sólo algunos minutos. Cuando este completa, quitamos el CD-ROM y el reiniciamos el sistema. A diferencia de una instalación normal ESX, ESXi requiere un poco más de configuración después de la instalación inicial, porque la única cosa que está siendo configurada durante la instalación es el disco sobre el cual el hipervisor va a ser instalado. Una vez que el servidor nuevo del ESXi ha sido reiniciado, notaremos que aparece una pantalla que es similar a la pantalla de la consola ESX pero con dos opciones nuevas: F11 para volver a arrancar el sistema y F2 para manipular el sistema. Para empezar la configuración, nos aseguramos de tener un teclado y un monitor conectado en el servidor del ESXi. Presionamos F2 para acceder a la utilidad basada en el menú de configuración,

que nos despliega la pantalla principal en la cual toda la configuración del ESXi se llevara a cabo (Figura 2.17).

Figura 2.17 Esta pantalla nos muestra la configuración del password de raíz (root).



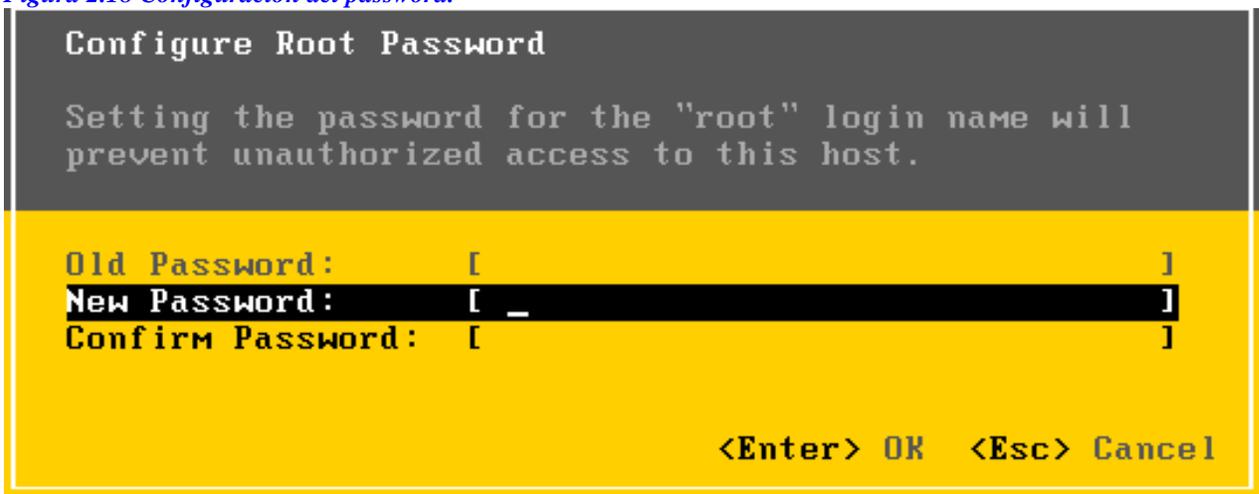
2.2.1 Configuración del Modo de Bloqueo

Este modo está deshabilitado por defecto. Si se habilita, impide que los usuarios accedan remotamente al servidor del ESXi, como el usuario de la cuenta raíz.

2.2.2 Configuración de la Contraseña de la cuenta de Raíz.

Ésta es la primera opción que necesitaremos configurar, no está lista por defecto. La contraseña que colocamos aquí quedara por defecto para la cuenta de raíz del usuario.

Figura 2.18 Configuración del password.



2.2.3 Configuración de la red a nivel central

Por defecto, ESXi será configurado para usar el Protocolo Dinámico de Configuración del Host (DHCP) y automáticamente tratará de configurar la dirección IP. Sin embargo,

podemos modificar nuestra red para usar una dirección IP estática usando las herramientas provistas dentro de la interfaz Central de la Red. El uso de una dirección IP estática es muy recomendado. Como se muestra (Figura 2.19), la interfaz Central de red, ofrece algunas opciones para configurar nuestro servidor del ESXi. La opción de Adaptadores de la Red nos permite hacer una selección de cuál el adaptador de la red se usara para la consola de servicio de la dirección IP, si se tuviera más que una interfaz disponible; Las interfaces se etiquetarían así *vmnic0*, *vmnic1*, etc.

También tenemos la opción para configurar nuestra consola de servicio de dirección IP para un uso específico de la VLAN. Esto es un ajuste optativo. La siguiente opción en la lista es la IP Configuración de protocolo entre redes. Aquí, se tiene la opción para configurar el DHCP o una dirección IP estática. Escogiendo lo último configurado que nos permitirá entrar en la información básica necesaria, como la dirección IP, la máscara de subred de comunicación, y el portal de acceso (Gateway) (Figura 2.20). La pantalla de configuración Central de la red, también provee opciones para configurar los servidores de DNS y sus respectivos sufijos de DNS:

Reiniciando la Central de la Red.

Al hacer cambios a una dirección IP estática o renovando un protocolo de comunicación de DHCP en la red se puede requerir el reinicio de la Central de la red.

Figura 2.19 Configuración Central de la red.



El Test o prueba del Centro de la red.

El chequeo del centro de la red, nos permitirá mediante el comando **ping**, rastrear diferentes hosts y resolver las entradas de DNS.

Configuración del Teclado

El ESXi soporta la configuración del idioma para diferentes teclado: Inglés esta por defecto, pero podemos hacer una selección de ruso francés, alemán y japonés. No incluye soporte para el teclado en español esta versión.

La Vista de Información del Soporte

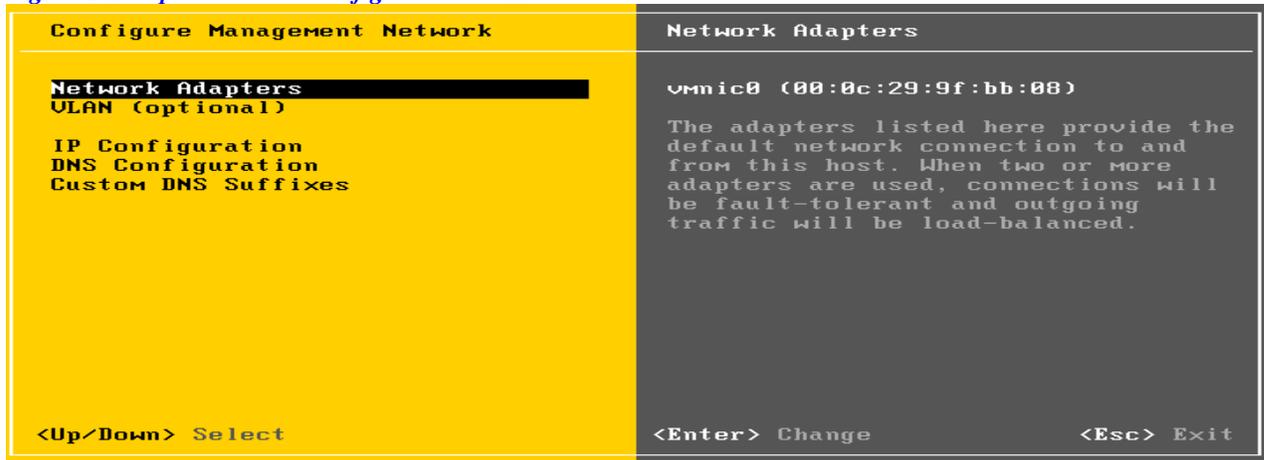
Ninguna de las opciones de configuración están disponibles en este menú; Sin embargo, provee una descripción general de información acerca de donde tenemos la llave de

licencia del servidor del ESXi, número de serie, y la huella de SSL, y el URL para sitio Web del soporte de nuestro producto VMware.

La vista de reportes del Sistema.

Existen tres opciones disponibles aquí, para visualizar los archivos de reporte generados de entrada. Como se muestra (Figura 2.21), se puede visualizar los archivos de reporte (logs) de mensajes de sistema, configuración, y del agente de la administración central general (hostd).

Figura 2.20 Opciones de la Configuración de Red.



2.2.4 Reinicio de los Agentes de la administración general central.

De vez en cuando es necesario reiniciar el sistema de los agentes de la administración general en el Host del ESXi sin tener que reiniciar el servidor mismo. Si los agentes de la administración general son reiniciados, todos los clientes (como clientes del vCenter y el servidor del vCenter) remotamente conectados se desconectaran. Es importante notar que en nuestro servidor del vCenter; el Host, aparecerá como desconectado, mientras la red de la gerencia se reanuda; Sin embargo, sus máquinas virtuales continuarán prendidas y trabajando.

Reseteando ajustes personalizados.

Reseteando los ajustes personalizados pondrá todas las variables del Servidor ESX como venían de fabrica.

Figura 2.21 Pantalla de vista del archivo de reportes de incidencias.



2.3 EL DATACENTER 2.X VMWARE CONOCIDO TAMBIÉN COMO EL SERVIDOR VCENTER.

El VMware vCenter, provee una posición central para administrar y manipular todas las máquinas virtuales conectadas en nuestra red de VMware. Este producto viene por separado y requiere de un sistema dedicado o exclusivo como Windows server o un Windows virtualizado y una base de datos como (Oracle o Microsoft SQL Server) Una vez instalado y configurado, hará que el trabajo de administración de base de datos se torne más fácil; El Vcenter provee una forma para distribuir recursos, manejar usuarios, mover máquinas virtuales de un lugar del hardware físico a otro (inclusive maquinas en pleno funcionamiento), programación de tareas, y muchas cosas más. [1, 2,3]

2.3.1 Requerimientos para la instalación del VMware vCenter 2.x Server.

Uno de los requerimientos es el siguiente: Windows 2000 Server con SP4 Update Rollup 1, Windows XP Profesional con SP3, Windows 2003 Server con SP1 y SP2 (todas las versiones exceptuando las de 64 bits), o Windows 2003 Server R2

- Un procesador a 2.0GHz o más rápido Intel o AMD X86
- 2GB o más de RAM
- El 560MB mínimo de espacio en el disco duro (de 2- 4GBes recomendado)
- 10/100/1000 Ethernet Adaptador (de la marca Gigabit es recomendado)
- VMware vCenter también puede ser instalado dentro de una máquina virtual incrustado en el ambiente ESX. Presentamos la siguiente tabla con los valores máximos del vCenter para los servidores ESX 3.5 y vSphere 4.0.

Tabla 2.1 Máximos del vCenter. [1,9]

Objeto/ Valor	Máximo ESX 3.5	Máximo ESX 4.0
Numero de máquinas virtuales encendidas a (32-bit)	2,000	2,000
Hosts por servidor de vCenter a (32-bit)	200	200
Máquinas virtuales registradas a (32-bit)	-	3,000
Hosts por servidores de vCenter server (64-bit)	-	300
Numero de máquinas virtuales encendidas a (64-bit)	-	3,000
Máquinas virtuales registradas a (64-bit)	-	4,500
Servidores vinculados al vCenter	-	10
Hosts en un ambiente modo-vinculo	-	1000

Tabla 2.2 Máximo de máquinas virtuales del vCenter. [1,9]

Objeto/ Valor	Máximo ESX 3.5	Máximo ESX 4.0
Máquinas virtuales encendidas en modo-vinculo	-	10,000
Máquinas virtuales registradas en modo-vinculo	-	15,000
Conexiones concurrentes del cliente de vSphere a (32-bit)	20	15
Conexiones concurrentes del cliente de vSphere a (64-bit)	-	30
Hosts por Datacenter	50	100

2.3.2 Requerimientos de la base de datos para el Servidor VMware vCenter 2.x

El Servidor vCenter requiere una de las siguientes bases de datos:

- Microsoft SQL SERVER 2000 Estándar con SP4
- Microsoft SQL SERVER 2000 la Empresa con SP4
- Microsoft SQL SERVER 2005 Estándar con SP1 o SP2
- Microsoft SQL SERVER 2005 la Empresa con SP1 o SP2
- Microsoft SQL SERVER 2005 Express con SP2 (no recomendado para producción, solo para ambientes de prueba)
- Oracle 9i Release 2 Estándar: Aplicando el 9.2.0.8.0 del parche al servidor y el cliente
- Oracle 9i Release 2 l Empresarial: Aplicando el parche 9.2.0.8.0 al servidor y el cliente
- Oracle 10g Release 1 Estándar (10.1.0.3.0)
- Oracle 10g Release 1 Empresarial (10.1.0.3.0)
- Oracle 10g Release 2 el Estándar (10.2.0.1.0): Aplicando el parche 10.2.0.3.0 al servidor y Cliente, luego aplicando el parche 5699495
- Oracle 10g Release 2 Empresarial (10.2.0.1.0): Aplicando el parche 10.2.0.3.0 al servidor y Cliente, luego aplicando el parche 5699495. [1,4]

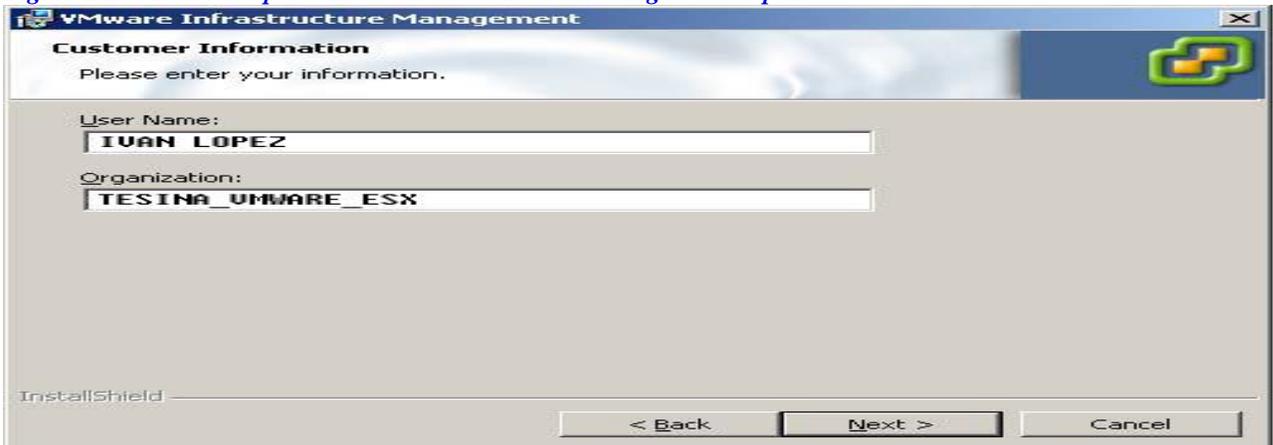
1. Ya sea insertando el CD-ROM y ejecutando el *autorun.exe* empecemos la instalación, o manualmente damos un clic en el *autorun.exe* localizado en el archivo de ZIP previamente descargado; nos aparecerá una pantalla similar. Damos un clic en siguiente para continuar.

Figura 2.22 La pantalla muestra el inicio del instalador del VMware vCenter 2.x.



2. La página de introducción nos expone los beneficios de la tecnología del vCenter Server. Una vez que hemos leído esto, damos un click en siguiente para continuar.
3. Leamos el acuerdo de licencia y aceptémoslo haciendo click sobre “acepto los términos” en el acuerdo de licencia. Hay un círculo al lado de esta declaración que ahora mostrará un punto. Damos un Click en el botón siguiente para continuar la instalación.
4. Se nos indicara ahora teclear información acerca de nosotros como es el nombre y la compañía; Al terminar, damos un click en siguiente para continuar.

Figura 2.23 Muestra la pantalla de los datos del usuario según corresponda.



5. Ahora decidiremos qué partes de la aplicación se instalaran. Tenemos tres opciones diferentes, Como se muestra abajo (Figura 2.24) (los nombres son diferentes en el instalador, porque aunque el VMware ha cambiado los nombres del producto, en los instaladores no se han actualizado, por ello, no se reflejan estos cambios), estas son:

Instalación del VMware Cliente Infrastructure (el cliente vCenter)

Esta opción instalará sólo el cliente del vCenter (anteriormente conocido como el cliente VI) sin instalar las partes del servidor del vCenter. Esta opción es apropiada para una desktop o una estación de trabajo que se usará para operar el servidor del vCenter.

El cliente es automáticamente instalado con la siguiente opción.

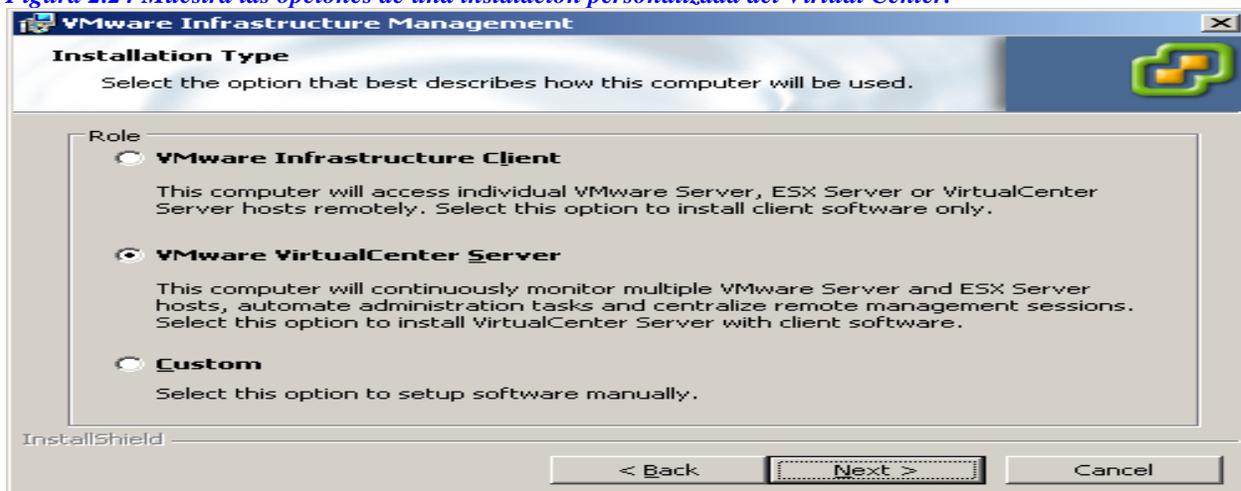
Instalación del VirtualCenter Server (vCenter Server)

Ésta es la instalación recomendada: Incluye al cliente VI (el cliente vCenter) VirtualCenter Server (vCenter Server), Actualización de la administración central, y VMware Converter versión empresarial para el VirtualCenter Server (vCenter Converter).

La instalación personalizada

Esta opción nos permite instalar cualquier combinación de las cuatro partes mencionadas: El cliente VI (el cliente vCenter), Virtual Center Server (vCenter Server) la actualización de la administración central, y el VMware Converter Enterprise para VirtualCenter Server conocido como el (VCenter Converter). Una vez que hemos escogido el método de instalación deseado para usar, damos un clic sobre el botón siguiente para continuar.

Figura 2.24 Muestra las opciones de una instalación personalizada del Virtual Center.

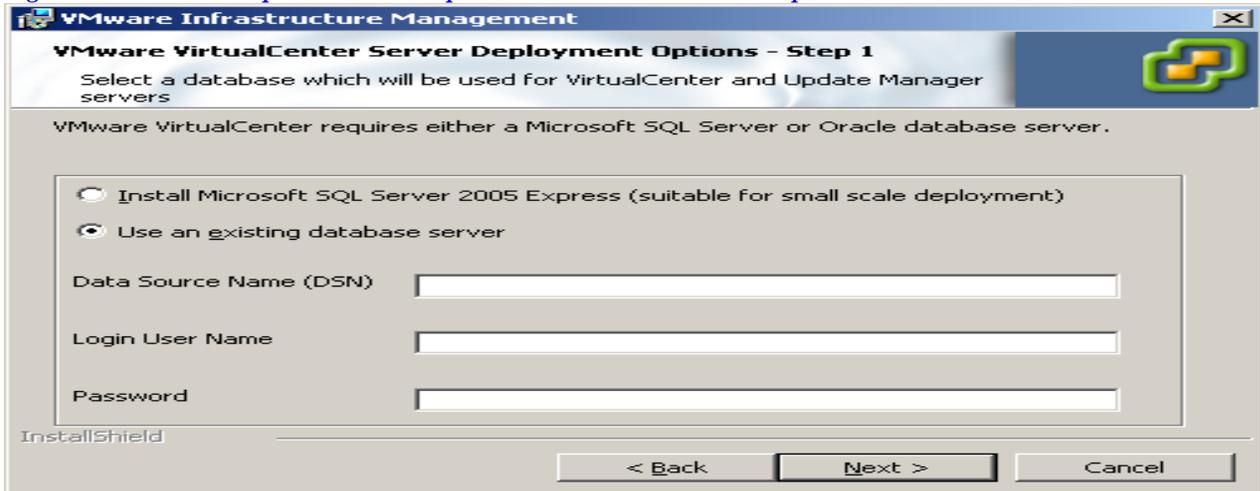


Ahora escogeremos el método de la base de datos (**Figura 2.25**). El vCenter Server Soporta el SQL SERVER Microsoft 2005 Exprés (MSDE), el Microsoft SQL SERVER 2000, El SQL SERVER Microsoft 2005, y ORACLE 10g. Para instalaciones en ambientes de producción, VMware nos recomienda no usar Microsoft SQL Server Desktop Engine (MSDE), que viene incluido en la instalación porque solo soporta 5 Hosts y 50 máquinas virtuales; así que si asumimos que la instalación estará en un ambiente de producción, seleccionamos la opción de "Usar un servidor de bases de datos existentes", y rellenamos los campos necesarios con la información de la base de datos pertinente, teniendo en cuenta lo siguiente:

- Debemos establecer las conexiones ODBC antes de usar el Microsoft SQL Server u Oracle como administrador de bases de datos. Esto puede ser realizado en el panel de control de Windows.
- El nombre de la fuente de datos (DSN) debe ser un sistema DSN.
- Si se está usando un servidor local de SQL con autenticación de Windows NT, nos aseguramos dejar el nombre de usuario y campos de contraseña en blanco. De otra manera, introducimos el nombre de usuario y la contraseña.

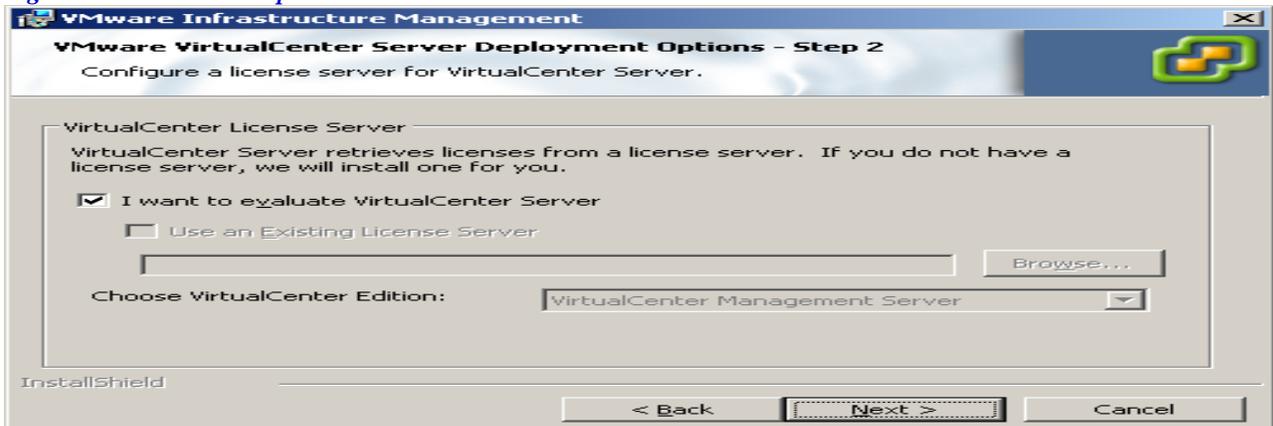
Una vez que hemos introducido la información con éxito, presionamos el botón Siguiente para continuar la instalación.

Figura 2.25 Muestra la pantalla con la opción de la base de datos correspondiente.



7. Después, necesitamos seleccionar una licencia para el servidor. Hay un par de opciones aquí: (Figura 2.26). Si pensamos en usar el vCenter Server en el modo de evaluación para 60 días, hacemos la selección "quiero evaluar el Virtual Center Server" opción. Esto instalará el producto completamente, el cual puede variar del modo de evaluación a un modo de licencia permanente después si se requiere. Para usar un archivo de licencia, primero damos un clic ala casillita marcada del modo de evaluación. La ruta predeterminada es *C:\Archivos de programa\VMware\VMware License Server Licenses\vmware.lic* aparecerá, permitiéndonos hacer una lectura para seleccionar nuestro archivo de licencia. Presionamos el botón siguiente para continuar. De lo contrario si planeamos usar un servidor con licencia desde un principio, damos un clic en la opción de casilla en "uso de una Licencia de servidor existente", seleccionamos la edición de la versión del vCenter Server que hayamos adquirido si la hemos comprado, y presionamos siguiente para continuar.

Figura 2.26 Muestra la opción de licenciamiento.



8. Si seleccionamos la opción personalizada de la instalación, tendremos permiso de modificar los puertos sobre los cuales las aplicaciones del Servidor del vCenter se ejecutarán (Figura 2.27). Modificamos estos o dejamos los que están por defecto, y damos un clic en siguiente para continuar la instalación.

Figura 2.27 Se muestran las opciones de la configuración de los puertos.



9. Luego entonces, recibiremos las instrucciones para introducir la información acerca del sistema en el cual los componentes del vCenter Server van a ser instalados (Figura 2.28):

VC protocolo entre redes Server

La dirección IP o el dominio le da nombre al sistema en el cual el vCenter Server será instalado. Normalmente, ambas opciones aparecerán en el menú.

VC Servidor del Puerto

Este valor puede modificarse sólo durante una instalación personalizada.

El acceso al sistema /contraseña del administrador/contraseña, controlamos el acceso al sistema con la cual podemos acceder a Windows en el sistema en el cual se instalará el vCenter Server. Una vez introducimos los valores apropiados, damos un clic sobre el botón Siguiente para continuar la instalación. Si se eligió hacer una instalación personalizada, procedamos al paso 10; de otra manera, nos saltamos al paso 12 para continuar la instalación.

Figura 2.28 Muestra las credenciales a introducir del Virtual Center.



10. Durante una instalación personalizada, recibiremos instrucciones de introducir información para el VMware Update Manager. Podemos usar la misma base de datos como la que hemos usado previamente para el servidor del vCenter, o una base de datos diferente (Figura 2.29). Si estamos de acuerdo con estos ajustes, damos un clic sobre el botón siguiente para continuar la instalación.

Figura 2.29 Muestra la configuración del VMware Update Manager



11. Después de configurar los ajustes del Gerente de Actualización (Update Manager), si se está realizando una instalación personalizada, recibiremos instrucciones de introducir información para el segmento del Convertidor de vCenter. (Figura 2.30).

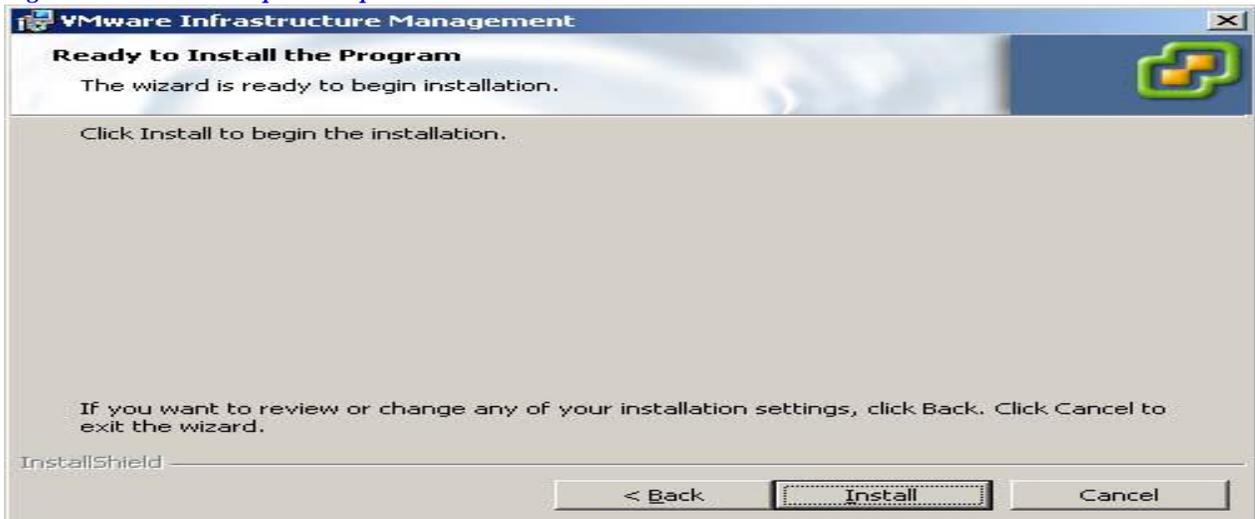
Introducimos información acerca del IP y del puerto o aceptamos los que están por defecto, y damos un click en siguiente para continuar nuestra instalación.

Figura 2.30 Configuración de asignación del segmento específico de red.



12. Damos un clic sobre el botón Instalar (Figura 2.31) para iniciar la instalación. Durante el proceso de instalación todas las partes serán instaladas, junto con el .NET si es que este faltara en el sistema de nuestro servidor.

Figura 2.31 Muestra la pantalla para iniciar la instalación.



Después de que la instalación se ha completado, damos un clic sobre el botón de Final para empezar a configurar nuestros servidores ESX.

2.4 EL CLIENTE DEL VMWARE VCENTER

El cliente del vCenter (anteriormente el cliente del VMware Infrastructure) es usado para el manejo individual los Hosts del ESX así como también para proveer una interfaz de administración al Servidor del vCenter. Este producto viene incluido con la descarga del vCenter Server.

La instalación del cliente 2.x vCenter.

Los requisitos del cliente del vCenter son:

- Uno de los siguientes sistemas operativos de 32 bits:
 - Windows 2000 el Servidor con SP4 Update Rollup 1
 - Windows XP Profesional con SP3.
 - Windows 2003 el Servidor con SP1 y SP2
 - Windows 2003 el R2 del Servidor
 - Windows Vista Business.
 - Windows Vista Enterprise.
- El Framework .NET 2.0 (este viene incluido con el instalador del cliente del VCenter)
- Un procesador a 266MHz Intel o AMD X86
- Mínimo 256MB en RAM (2GB es recomendado)
- El espacio de 150MB en disco duro para la instalación básica (el espacio adicional es requerido si se requiere almacenar las maquinas virtuales locales)
- El adaptador de Ethernet 10/100/1000 (de la marca Gigabit es recomendado)

El cliente del vCenter se instala por lo regular junto con la instalación del vCenter Server. Una vez descargado, corremos la aplicación. La instalación es muy intuitiva y fácil de realizar.

2.5 EL SERVIDOR DE LICENCIAS (VCENTER 2.X)

Es posible administrar nuestras licencias del VMware en cada máquina individualmente usando las licencias provenientes de nuestro host. Sin embargo, es mucho más conveniente, especialmente si nuestras redes crecen, establecer un servidor de licencia del VMware como un depósito y usarlo para administrar nuestras licencias, permitiéndoles interactuar entre los hosts. Al hacerlo así, nos abre nuevas opciones que no tenemos disponibles al usar licencias individuales provenientes de nuestros hosts, como el VMotion utilizado para mover las máquinas virtuales de un Host físico a otro. En particular, un servidor de licencias habilita el planificador distribuido de recursos y las características de alta disponibilidad en el ESX y el vCenter.

Instalación del Servidor de licencias (vCenter 2.x)

El servidor de licencias nos presenta los siguientes requisitos para instalarlo:

- Uno de los siguientes sistemas operativos: Windows 2000 SERVER con SP4 Update Rollup 1, Windows XP PRO con SP2, Ventanas 2003 SERVER con SP1 y SP2 (todas las versiones excepto la de 64 bits), o Windows 2003 Server R2
- Un procesador a 266MHz Intel o AMD X86 o mas rápido.
- 256MB en RAM mínimo (512MB es mas recomendado)
- Espacio en disco duro 25MB para una instalación básica
- Un adaptador de Ethernet 10/100/1000 (de la marca Gigabit se recomienda).

Si se usa el instalador del VMware Infrastructure, automáticamente instalará el servidor de licencias. Sin embargo, es posible instalar el servidor de licencias en otro servidor. Para instalar esta parte, navegamos hacia la carpeta `\vpx` en el CD de la instalación y ejecutamos el archivo `de VMware-licenseserver.exe` para empezar la instalación.

2.6 EL VCONVERTER Y SUS GENERALIDADES.

El vConverter es una aplicación gratis disponible en sitio de VMware, que nos permite transformar servidores físicos en servidores virtuales fácilmente, moviéndolos desde nuestra máquina (s) a nuestro sistema de ESX VMware. Hay dos formas en las que esto puede hacerse. En una *migración en frío*: Si apagamos un servidor y lo convertimos mientras este está fuera de servicio. Con vConverter, también tenemos, una *migración caliente*: Nos permite convertir y mover un servidor prendido corriendo en uso. El VMware Converter nos permite también tomar máquinas virtuales viejas y moverlas hacia una red nueva, mientras las actualizamos a su versión más actual.

La instalación del vConverter.

La instalación de vConverter es muy metódica.

Los componentes del vCenter Converter Standalone 4.x (el cliente, el servidor, y el agente) pueden ser instalados en las siguientes plataformas:

- Windows 2000 con SP4
- Windows XP Professional (de 32 bits y de 64 bits)
- Windows 2003 (de 32 bits y de 64 bits)
- Windows Vista (de 32 bits y de 64 bits)
- Windows Server 2008 (de 32 bits y de 64 bits)
- Linux Red Hat Enterprise 4.0 (de 32 bits y de 64 bits)
- Linux Red Hat Enterprise 5.0 (de 32 bits y de 64 bits)
- Linux SUSE Server Enterprise 10 (de 32 bits y de 64 bits)
- Ubuntu 6.x
- Ubuntu 7.x (de 32 bits y de 64 bits)

El vCenter Converter Standalone 4.x servidor y los componentes del agente (sin soporte a cliente) también puede ser instalado en las siguientes plataformas:

- Linux Red Hat Enterprise 3.0
- Linux SUSE Enterprise Server 8
- Linux SUSE Enterprise Server 9 (de 32 bits únicamente)
- Ubuntu 5.x

El vConverter puede ser descargado del siguiente URL (el registro es requerido para bajarlo, y tendremos dos opciones: una para plataformas que soportan Windows y otro para plataformas que soportan Linux). [w3] La compañía de VMware, ha hecho un gran trabajo al ponernos la misma Interfaz Gráfica del Usuario lateral de Windows para la versión de las herramientas en Linux, dándonos así la misma "percepción" con cualquier versión de plataforma que se prefiera.

La Instalación bajo la plataforma de Windows

Para instalar vConverter en Windows:

1. Bajamos el archivo ejecutable para Windows.
2. Ejecutamos el instalador, haciendo clic sobre siguiente en la pantalla de introducción.
3. Aceptamos el acuerdo de licencia dando un clic en la casilla en blanco que dice: "que acepto los términos en el acuerdo de licencia"

Y haciendo clic en el botón siguiente para continuar.

4. Escogemos el directorio en el cual se instalaran los archivos. El instalador tomara el que está por defecto *C:\Program Files\VMware\VMware vCenter Converter Standalone*. Ya que estamos conformes con esto, damos un clic al botón siguiente para continuar la instalación.

5. Seleccionamos el tipo de instalación que queremos realizar. Hay dos opciones aquí, como se muestra (Figura 2.32):

La instalación local

Esta nos instala el vCenter Converter en el servidor. Y nos permite crear y manipular las tareas de conversión desde este servidor local solamente.

La instalación del Servidor/cliente (avanzada)

Esta opción establece un modelo de cliente /servidor para el vCenter Converter. Aquí, podemos instalar individualmente al cliente, al servidor, y / o a las partes del agente en el servidor local. Si escogemos "instalación local", procedamos al paso 7; de otra manera, continuamos hacia el paso 6.

Figura 2.32 La pantalla a continuación muestra las opciones de tipo de instalación a realizar.

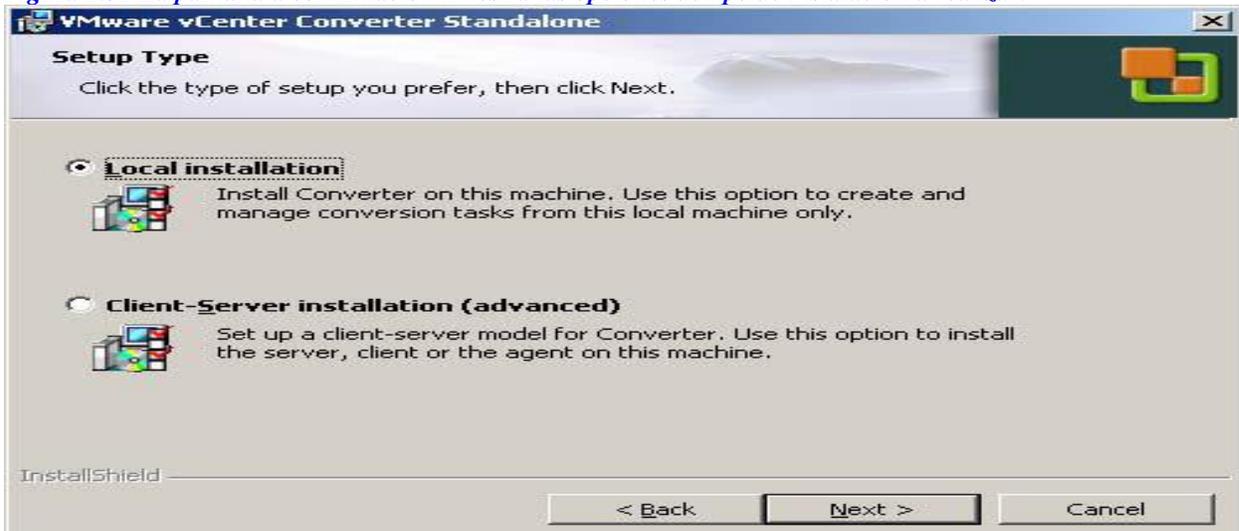


Figura 2.33 Se muestra el modo avanzado o personalizado.



6. La opción de instalación Avanzada, nos brinda la oportunidad de especificar cuáles puertos del vCenter Converter serán usados. (Figura 2.34). Por configuración de fábrica son:

- El HTTP Puerto de servicio -_ 443
- El HTTPS Puerto de servicio -_ 80
- El Puerto de Servicio del Agente -_ 9089

Si estamos conformes con estos puertos, damos un clic en siguiente para continuar la instalación.

Figura 2.34 Configuración avanzada para la personalización de los puertos.



7. Ahora podemos seguir con la instalación. Dando un clic en Instalar para continuar.

8. Cuando la instalación se ha completado, tendremos la opción para que automáticamente se ejecute el cliente del vCenter Converter. Damos un clic sobre el botón de Terminar para completar la instalación.

La Instalación bajo la plataforma de Linux

En cada uno de las diversas distribuciones de Linux se ha probado, que las opciones de configuración de instalación de fábrica predeterminadas trabajan bien. Aquí están los pasos a seguir:

1. Descargamos el instalador basado en Linux.
2. Extraemos el archivo tar *al ejecutar* `tar xvzf Vmware-converter*.tar.gz`, al hacerlo así, nos creara un directorio llamado *vmware-converter-distrib*.
3. Nos movemos hacia el directorio *de vmware-converter-distrib*.
4. Ejecutamos el archivo *de vmware-install.pl* como *root (usuario raíz)* (se puede cambiar al usuario *raíz* o podemos usar el comando `sudo` para tener acceso a todo sin restricciones).
5. Se nos presentara el acuerdo de licencia. Presionamos la barra espaciadora para deslizarnos hacia abajo del acuerdo. Cuando se nos pida, tecleamos **sí** para aceptar el acuerdo y presionamos la tecla `Enter` para continuar la instalación.
6. Después de aceptar el acuerdo de licencia, el instalador nos preguntara si deseamos instalar el cliente del vCenter Converter Standalone. Por defecto tenemos que **Sí**, así es podemos presionar la tecla `Enter` para continuar.
7. El instalador nos vuelve a preguntar si deseamos instalar el servidor del vCenter Converter Standalone. Otra vez, por defecto es **Sí**, así es que presionamos la tecla `Enter` para continuar. **[2, 3,4]**
8. El instalador nos pedirá el directorio en el cual deseamos instalar los archivos ejecutables. La ruta por defecto es ***/usr/bin***; sin embargo, podemos modificar la ruta si lo deseamos. Presionamos la tecla `Enter` para continuar.
9. El instalador nos preguntara en que ruta se instalaran los archivos de la biblioteca VMware vCenter Converter Standalone. La ruta predeterminada es ***/usr/lib/vmware-vcserver-converterstandalone***; Sin embargo, podemos ponerlos en un directorio diferente. Después, solo presionamos **←** tecla `ENTER`; Y nos movemos a la siguiente página.
10. Después, el instalador preguntará si queremos crear la ruta para los archivos de la biblioteca. Por predeterminación es **Sí**, así es que podemos presionar la tecla `Enter` para continuar la instalación.
11. Se nos indicara especificar la ruta que contiene los directorios *del init* para *rc0.d* y *rc6.d*. La ruta predeterminada es ***/etc***. Presionamos la tecla `Enter` para aceptar la ruta predeterminada, o después podemos especificar la ruta personalizada si se requiere.
12. Especificamos la ruta para los scripts *init* del sistema. La predeterminada es ***/etc/init.d***. Presionamos la tecla `Enter` para aceptar la que está por defecto o la personalizada si así se requirió.
13. Tenemos la opción para permitir el acceso remoto en el vCenter Converter Standalone. La opción predeterminada es **NO**, pero se puede cambiar esto a **Sí**, por si queremos permitir que otros clientes del vCenter Converter se conecten a esta instancia. Presionamos la tecla `“Enter”`, para aceptar lo predeterminado, o lo hacemos así, después de cambiar el valor.
14. Especificamos el directorio en el cual queremos que los iconos sean instalados (la ruta predeterminada es ***/usr/share/icons***). Presionamos la tecla `Enter` para aceptar lo predeterminado, o lo hacemos así, después de indicar nuestra ruta personalizada.

15. Especificamos el directorio que contiene nuestros archivos de entrada del menú (la predeterminada es `/usr/share/applications`). Presionamos la tecla Enter para aceptar lo predeterminado, o después lo hacemos así, al especificar una ruta personalizada.

La instalación ahora comenzará. Una vez que la instalación se ha completado, podemos checar que todo se instaló bien mediante el menú de Herramientas de Sistema en nuestro ambiente de Windows X11 o ejecutar el cliente desde una consola en la línea de comando corriendo la aplicación así: `vmware-converter-client`

2.7 INSTALACION DEL ESX 4.0 O ACTUALMENTE CONOCIDO COMO VSPHERE 4.0

De una forma muy similar como ya vimos, a la instalación del ESX 3.5, esta nueva versión tiene un interfaz gráfica muy amigable que nos facilita mucho la instalación.

ESX 4.0 también usa una versión mejorada y actualizada de la plataforma de Linux RedHat en específico la versión: RedHat Enterprise 5.x. **[1, 4,10]**

Antes de comenzar la instalación del ESX 4.0, debemos comprobar que nuestro hardware es completamente compatible visitando al siguiente URL:

<http://www.vmware.com/resources/compatibility/search.php?base&deviceCategory=server> **[W1]**

La imagen ESX en ISO está disponible para la descargarla en <http://www.vmware.com/download/vi/>. **[W2]**

ESX 4.0 se basa en una arquitectura de hardware de 64 bits, es muy diferente a la versión previa, la cual corría sólo a 32 bits, sólo lo podemos instalar en una arquitectura de 64 bits. VMware nos sugiere lo siguiente como los requisitos mínimos para la instalación del 4.x ESX Server:

- Un procesador que soporta instalaciones de 64 bits (por ejemplo, cualquier AMD Opterons, e Intel Xeon 3000/3200, 3100/3300, 5200/5400, 7100/7300 y 7200/7400).
 - 2GB en RAM mínimo.
 - Uno o más controladores de Ethernet (recomendamos un mínimo de cuatro).
- VMware nos sugiere controladores basados en Broadcom o Intel, pero usted puede comprobar el hardware en la lista de compatibilidad para otras opciones.
- El almacenamiento local, disco duro de Hardware iSCSI, o almacenamiento SAN.

El instalador tiene los mismos modos u opciones de instalación, como el ESX 3.5 que son el modo gráfico y el modo texto e incluye otras tres opciones para inicializar la instalación:

Instalación del ESX 4.0 en el modo gráfico.

Es el método recomendado para la instalación. Requerimos para este método un ratón y una interfaz gráfica que nos guiara a través de la instalación.

Instalación del ESX 4.0 en el modo texto.

Este modo es único en texto para instalar a ESX. Esta opción es normalmente usada cuando se tiene cualquier problema con el ratón o el vídeo en el instalador gráfico.

El instalador tiene los mismos modos u opciones como el ESX 3.5 que son el modo gráfico y el modo texto e incluye otras tres opciones para inicializar la instalación:

Método por scripts del ESX 4.0 usando un dispositivo USB y el comando ks.cfg

Esto nos permite construir un script de arranque e iniciar la instalación desde un almacenamiento de USB.

Método por scripts del ESX 4.0 para el primer disco

Este método engloba a nuestra instalación predeterminada incluida por defecto en el ESX 4.0 como imagen, y no puede ser personalizado. Así que, la contraseña predeterminada para la instalación es *mypassword*.

Método por scripts del ESX 4.0 para el primer disco (Sobrescribiendo el VMFS)

Al igual que el anterior método engloba una instalación predeterminada incluida en el ESX 4.0 como imagen, y no puede ser personalizada. Esta opción borrara cualquier almacenamiento VMFS que podamos tener, al igual que nos borrara cualquier máquina virtual al mismo tiempo. La contraseña predeterminada para la instalación es *mypassword*. Para empezar la instalación, nos aseguraremos que nuestro servidor este configurado desde el BIOS para arrancar desde el CD-ROM. Luego entonces, cuando arrancamos desde el CD-ROM del ESX 4.0, veremos la nueva pantalla de instalación (**Figura 2.35**) con las opciones que acabamos de mencionar.

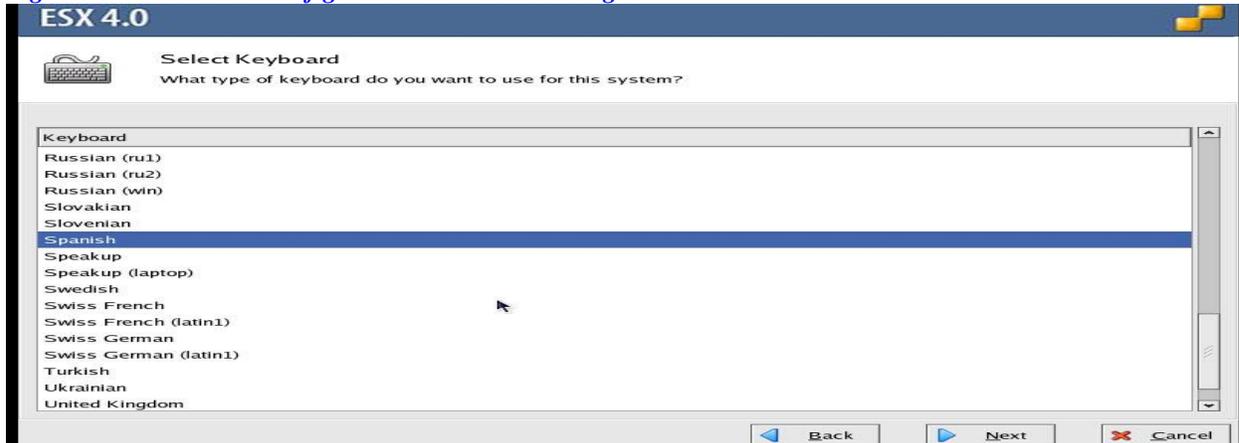
Figura 2.35 Muestra el menú inicial de la pantalla para la instalación del ESX 4.0



Aquí están los pasos de instalación:

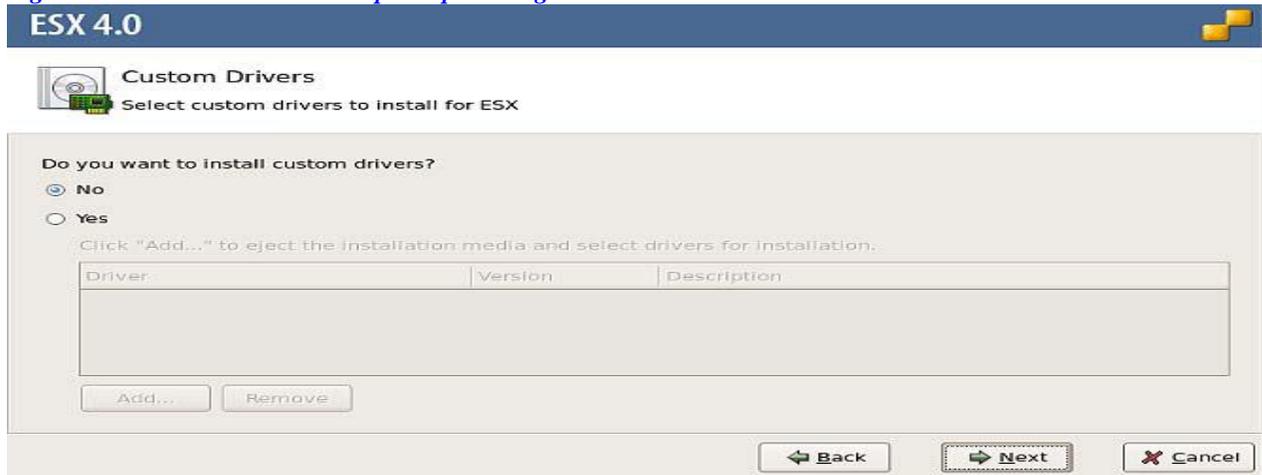
1. Vamos a iniciar nuestra instalación usando el modo gráfico, ya que es el método más común en condiciones normales siendo el más usado. Cuando empieza la instalación, notamos mejoras respecto a las versiones anteriores del ESX.
2. Una vez que la instalación ha comenzado, tenemos una pantalla de bienvenida dándonos instrucciones para comprobar el hardware, y asegurarse de la compatibilidad con el ESX 4.0. Para continuar con la instalación, damos clic sobre el botón siguiente y aceptamos el acuerdo de licencia dando un clic en la casilla. Damos un clic en siguiente para continuar otra vez.
3. Se nos presenta la opción de la configuración del teclado, seleccionamos en español por supuesto. Típicamente, aquí podemos usar cualquier configuración de teclado que deseemos (**Figura 2.36**). Damos un clic en siguiente para continuar.

Figura 2.36 Muestra la configuración del teclado a elegir.



4. La siguiente pantalla es nueva en esta versión de ESX 4.0; nos permite cargar controladores para un hardware más específico, esto es fantástico, por si tenemos algún hardware incompatible con el ESX 4.0. (Figura 2.37). De hecho es en esta pantalla que tenemos la oportunidad de instalar cualquier controlador de hardware, porque después no podremos añadirlo es muy importante saber esto. El instalador nos mostrará una advertencia manifestando que el instalador va a cargar nuestros controladores. Una vez que este paso es realizado, no se puede agregar ningún controlador personalizado. Si ya estamos seguros de haber añadido lo que deseamos podemos continuar, presionamos el botón de SI y los controladores se comenzaran a cargar. Cuando la carga termine, el instalador dirá que se ha completado en un 100 %. Damos un clic sobre el botón siguiente para continuar la instalación.

Figura 2.37 Muestra una nueva opción para cargar controladores a la carta.



5. Después, tenemos la opción para introducir un número de serie de licencia y puede ser ahora o después (Figura 2.38). Ésta es una nueva pantalla dentro del instalador de ESX 4.0. Si elegimos introducir el número de serie más tarde, el instalador nos dará una licencia de prueba predeterminada por 60 días.

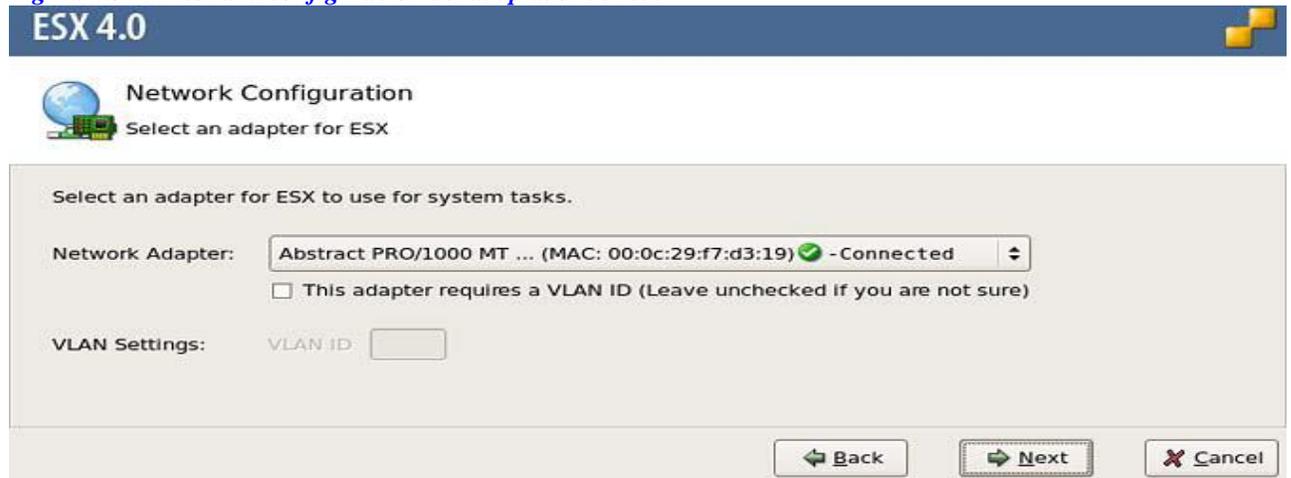
Si no tenemos una licencia, podemos usar esta opción para instalar el ESX 4.0 e introducir el número de serie posteriormente. Damos un clic en siguiente para continuar la instalación una vez que hemos seleccionado cualquier opción.

Figura 2.38 Esta pantalla nos muestra la opción para introducir el número serie de la licencia.



6. Después, seleccionamos el adaptador de la red, que realizara las tareas del sistema; a esto generalmente se le conoce como la consola de servicio (Figura 2.39). Si nuestra red requiere identificación VLAN, también tenemos la opción para introducir el ID aquí. Si no estamos seguros, dejamos el espacio vacío; se puede configurar esta opción más tarde, después de haber instalado el ESX 4.0, lo podemos hacer mediante el cliente del vCenter. Una vez que se ha seleccionado el adaptador de la red, damos un clic sobre el botón siguiente para continuar la instalación.

Figura 2.39 Muestra la configuración del adaptador de red.

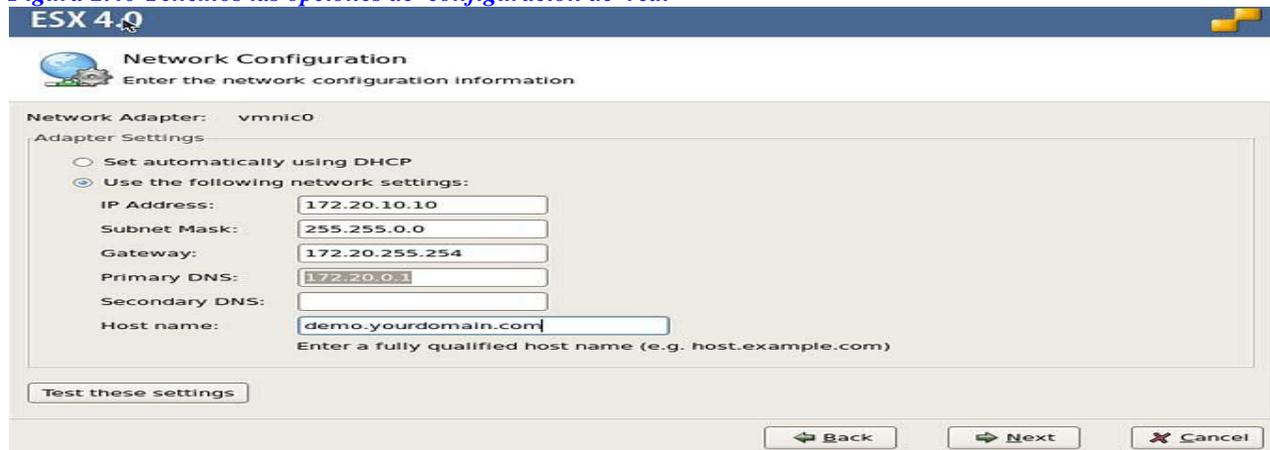


7. Ahora tenemos las opciones para configurar las redes del sistema (Figura 2.40).

Tenemos dos opciones aquí: “Dejar que automáticamente se use el DHCP” o “Usar los siguientes ajustes de red”. Generalmente, si vamos a realizar algún “Deploying” (ejecución o implementación de algún script o aplicación), con el ESX Server, en un ambiente de producción, debemos usar la última opción. Sin embargo, pudieran existir casos donde no tendremos información básica del IP address, así que el DHCP trabajará bien, solo

debemos asegurarnos de cambiarlo más tarde. La pantalla de configuración de la red en ESX 4.0 también tiene un botón de "prueba de estos ajustes", así que podemos validar los ajustes de la red antes de continuar la instalación. Una vez que hemos introducido la configuración de la red, damos un clic sobre el botón Siguiente para continuar la instalación.

Figura 2.40 Tenemos las opciones de configuración de red.



8. Después, se nos presenta las opciones de configuración de almacenamiento Estándar o Avanzado (Figura 2.41). En nuestro caso vamos a usar la opción Estándar de instalación y dejar que el instalador configure las particiones predeterminadas por nosotros. Sin embargo, si nuestra configuración fuese diferente, podríamos requerir el uso de la opción Avanzada, donde manualmente podemos configurar los diferentes aspecto de las particiones del almacenamiento. Las dimensiones recomendadas para las particiones del disco en el modo avanzado se encuentran enlistadas en la tabla 2.3.

Seleccionamos el método que deseamos usar para configurar el almacenamiento y damos un clic sobre el botón siguiente para continuar. Si tenemos cualquier dispositivo de hardware conectado (tal como un canal de fibra óptica, un disco iSCSI, un dispositivo DAS) es preciso removerlo ahora antes de empezar la instalación del ESX 4.0, para evitar pérdida de datos.

Tabla 2.3 Tamaño de las particiones del disco. [10]

Punto de Montaje	Tipo	Tamaño	Notas
Swap	Swap	600MB	Le permite a la consola de servicio usar memoria basada en discos cuando la memoria física no está accesible.
/boot	ext3	1.25GB	Soporta y aloja las imágenes del bootloader kernel del Servidor ESX y la partición llamada vmkcore.
/	ext3	10GB ^a	Soporta y aloja al sistema operativo, archivos de Configuración y aplicaciones de terceros.
/var	ext3	2GB ^b	Almacenaje de los log files (archivos de registro)

/vmfs

vmfs

Aloja la porción restante del disco en esta partición.

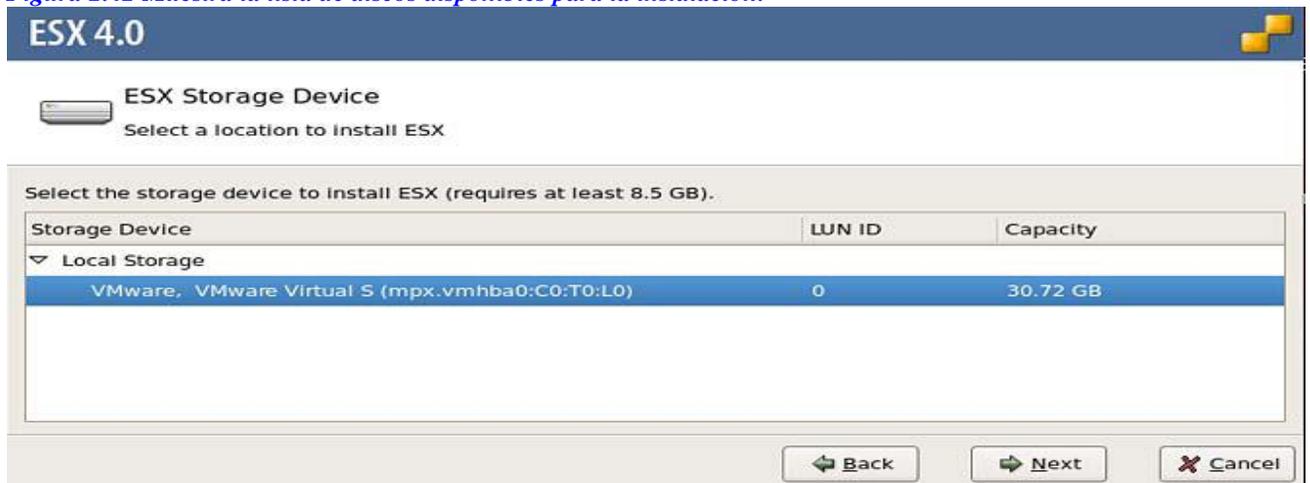
- a) La / partition debe ser de al menos 5GB de tamaño. Para mayor seguridad, recomendamos ajustar este valor a 10GB.
- b) La /var partition debe ser de al menos 2GB de tamaño.
- c) La /vmfs partition no necesita estar configurada en un disco local, a menos que no se tenga ningún almacenaje SAN conectado. Sin embargo, a menudo es conveniente tener un archivo de almacenaje local /vmfs para prueba, generalmente una partición local de tipo /vmfs y usará el resto de espacio del disco duro local.

Figura 2.41 Muestra opciones de configuración de almacenamiento estándar o avanzado.



9. El instalador nos muestra un listado de discos disponibles para la instalación del ESX 4.0 (Figura 2.42). Seleccionamos el disco en el cual queremos instalar el ESX 4.0 y damos un clic sobre el botón siguiente.

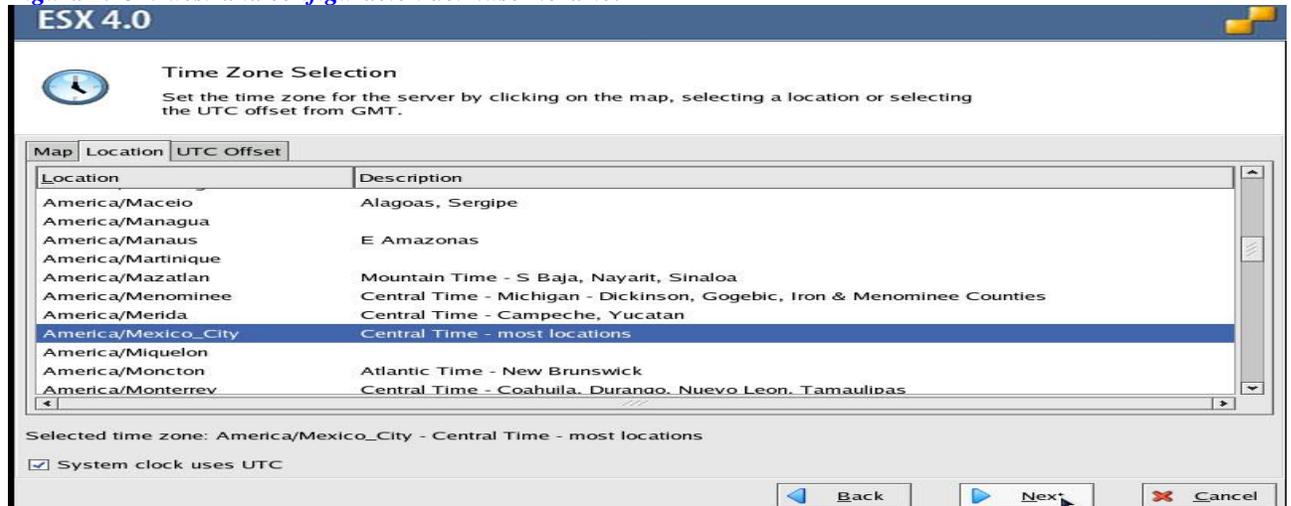
Figura 2.42 Muestra la lista de discos disponibles para la instalación.



10. Una vez que los discos están particionados, necesitaremos seleccionar el huso horario en el cual nuestros servidores están ubicados (Figura 2.43). Es muy importante asegurarnos de que nuestros Servidores ESX 4.0, han sido ajustados a la zona horaria correcta y que

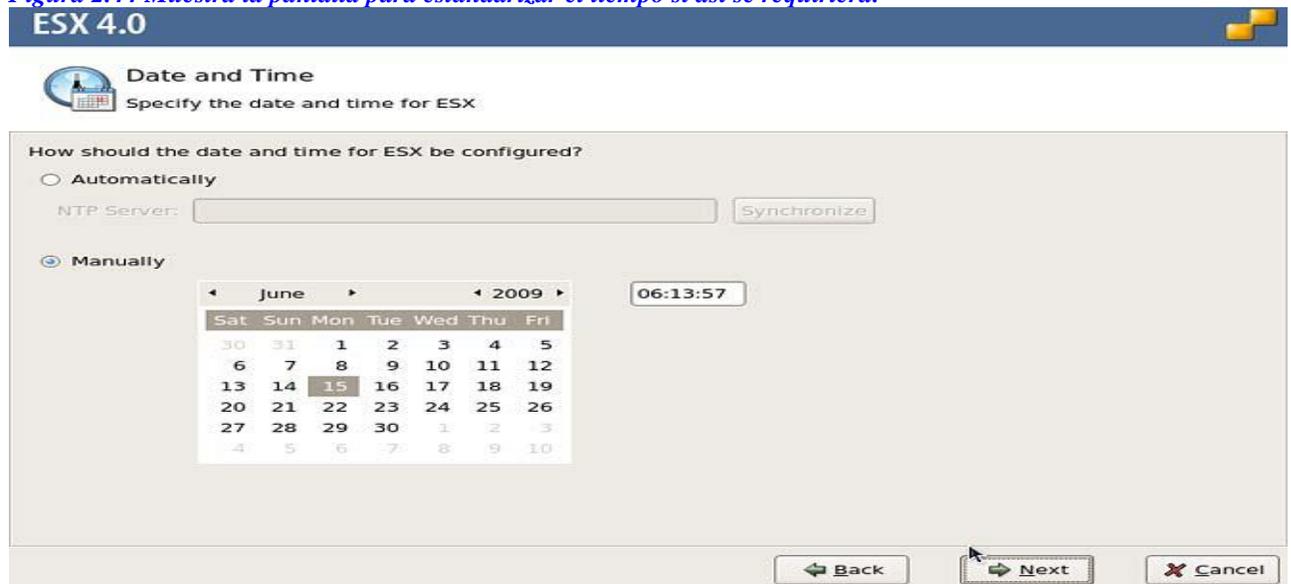
todo el grupo de nuestros ESX tenga la misma zona de horaria para asegurar la compatibilidad entre los nodos. Si tuviéramos un clúster de servidores. Una vez que hemos seleccionado el huso horario, en nuestro caso América/México_City, presionamos el botón siguiente para continuar nuestra instalación.

Figura 2.43 Muestra la configuración del huso-horario.



11. Como mencionamos es de suma importancia, asegurarnos que todos nuestros Servidores ESX, hayan sido configurados con el mismo tiempo y tengan la misma zona horaria (Figura 2.44). En este paso, tenemos la opción de configurar un servidor NTP (servidor de Protocolo de Tiempo de la Red) o ajustar el tiempo manualmente. Sugerimos que si tenemos un NTP, todos nuestros hosts en el ESX se basen en el. Una vez configurada la fecha y el tiempo, presionamos el botón siguiente.

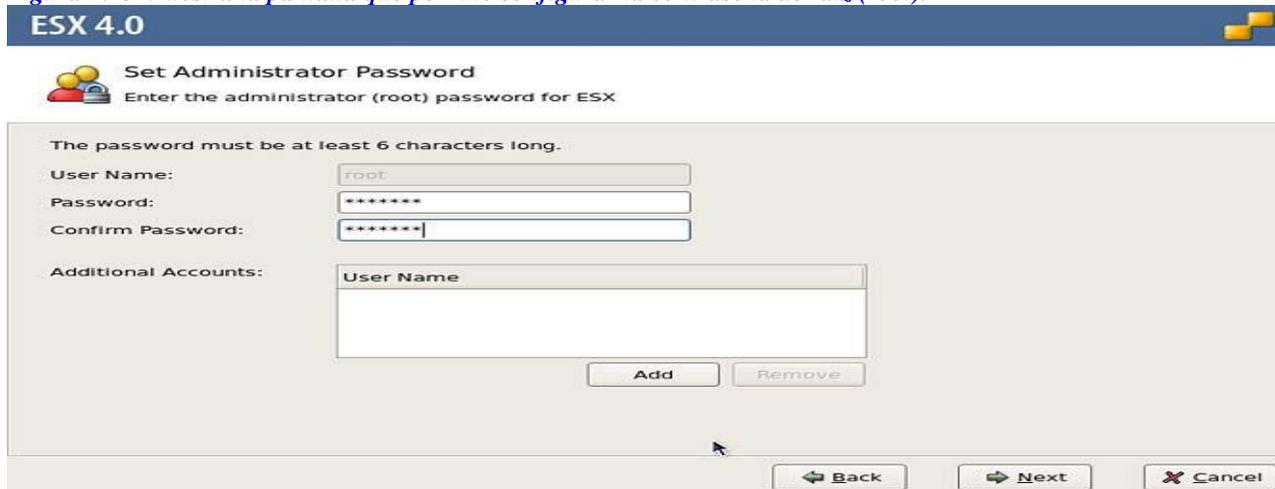
Figura 2.44 Muestra la pantalla para estandarizar el tiempo si así se requiriera.



12. Después en la siguiente pantalla, necesitamos colocar la contraseña del usuario raíz del Servidor ESX 4.0 (Figura 2.45). La contraseña de la cuenta raíz es lo que se usará al

principio para conectarse al ESX. También tendremos la opción de añadir otras cuentas del usuario en esta pantalla si así se desea. Una vez que hemos terminado, damos un clic sobre el botón Siguiente para continuar la instalación.

Figura 2.45 Muestra la pantalla que permite configurar la contraseña de raíz (root).



13. Finalmente, tenemos la pantalla del resumen de la instalación, la cual debemos revisar, por si necesitamos realizar un cambio de última hora, dando un clic en el botón de atrás para hacerlo así. (Figura 2.46). Una vez que estamos satisfechos, damos un clic sobre el botón siguiente y la instalación comenzará. Este proceso puede tomar entre 15 y 20 minutos, dependiendo de la velocidad de nuestro Servidor. Cuando la instalación se ha completado, presionamos el botón de terminar (Finish).

Figura 2.46 Tenemos la pantalla de resumen antes de iniciar la instalación.



Nuestro nuevo servidor de ESX 4.0 se reiniciara, y una pantalla parecida a la inferior (Figura 2.47) nos aparecerá. A este punto, solo podemos agregar y configurar nuestro nuevo servidor desde el cliente del vCenter. Enhorabuena hemos terminado de instalar y configurar nuestro servidor ESX 4.0.

Figura 2.47 Pantalla final de instalación del ESX, listo para iniciar.

```
UMware ESX 4.0.0 build-140815

UMware, Inc. UMware Virtual Platform

2 x Intel(R) Core(TM)2 Duo CPU T8300 @ 2.40GHz
2.2 GB Memory

Download tools to manage this host from:

http://192.168.3.9/

To open the ESX console, press Alt-F1.
To return to this screen, press Alt-F11.
```

Capítulo 3.

DISPOSITIVOS DE ALMACENAJE Y NETWORKING (REDES)

3.1 ALMACENAJE

En este capítulo se describe las diversas opciones disponibles de los dispositivos de almacenaje, recursos de piscina y networking. El tipo de almacenamiento que elijamos para correr en nuestra infraestructura virtual hará la diferencia sobre el buen desempeño de nuestro sistema virtual. En la primera parte de dispositivos de almacenaje, analizaremos los pros y contras de los diferentes dispositivos y protocolos de estos. **[1, 3, 5,6]** Antes de discutir cualquier opción, necesitamos entender la anatomía y tecnología de SCSI.

Modelo SCSI

Al igual que en la interconexión de sistemas abiertos del protocolo (OSI) modelo de networking, que está constituida por varias capas que ofrecen diferentes funciones. Así también, esta arquitectura de almacenamiento se compone de capas. El nombre oficial para este modelo es el *Modelo de Arquitectura de SCSI (SAM)*. Este modelo de tres capas consta de comandos, protocolos de transporte e interconexiones.

SCSI comandos: Los comandos son en realidad directivas reales para enviar o recuperar datos de un dispositivo SCSI. Las órdenes pueden ser compartidas y tener un común acceso, entre todos los dispositivos SCSI, o ellas puede ser específicamente, un tipo particular de dispositivo como un disco duro.

SCSI protocolos de transporte: Estos protocolos son responsables del agrupamiento de la información en bloques para la transmisión, monitoreando esta transmisión para que llegue con éxito, y hacen una selección sobre qué bloques de datos van hacia "x" dispositivo.

SCSI interconexiones: Estas (que en realidad son tarjetas SCSI en el sistema) _ son las responsables del señalamiento que realmente transmite los datos. Todos los dispositivos SCSI son identificados por un nombre de tres partes, comprendiendo un bus SCSI de datos, un target (Objetivo), y un LUN:

- *El bus SCSI de datos:* Un bus de datos es una tarjeta SCSI en el sistema. Puede ser una tarjeta conectada en paralelo a un disco local, una tarjeta de Canal de Fibra, o a un Centro de Información de Red (NIC)

Conectado a un almacenamiento de iSCSI.

- *Los Targets:* Éstos son recursos de almacenamiento independientes.

- *Los LUN:* Los números de la Unidad lógica, son los SCSI clientes que residen adentro del Target. Un LUN puede ser un disco solo o un grupo de discos en una cierta clase de configuración RAID.

Las comunicaciones SCSI son consideradas cliente /servidor. Los clientes son conocidos como *los Iniciadores*, y los servidores son conocidos como los Targets (objetivos). Si una aplicación quiere escribir en un disco SCSI, el iniciador externa una orden de escritura. El comando es enrutado hacia la correcta interconexión, usando un protocolo de

interconexión. El target (destino), ejecuta el comando y envía de regreso una respuesta para dejar saber al iniciador que su petición ha sido recibida con éxito.

SCSI es conocido como un protocolo de nivel de bloques, considerando la NAS (La red de Almacenamiento conectado), generalmente usa un archivo de nivel de protocolos. Tenemos que decidir si iniciamos o arrancamos nuestro ESX (booting), desde un dispositivo SAN o un SCSI, lo podemos hacer con ambos desde la SAN con Canal de fibra e iSCSI vía TCP/IP, la diferencia si usamos iSCSI, es que necesitamos usar un iniciador del hardware en lugar de un iniciador del software. Probablemente la mejor opción a usar es el modelo de comandos SCSI. La única diferencia respectó de las opciones SAN es cómo los comandos realizan contacto con los discos. Al usar el SCSI local, los comandos viajan a través del controlador de SCSI hacia el disco. Si estuviéramos usando Canal de Fibra o iSCSI, los comandos son encapsulados en un protocolo de comunicación y enviados hacia unidades remotas de discos.

Aquí tenemos los pros y contra de arranque (booting) desde un dispositivo SAN:

El Pro: La ventaja de arrancar desde un dispositivo SAN, es que no se tiene la necesidad de discos duros en nuestro servidor Las unidades de disco duro en su servidor. Los discos duros locales probablemente no tendrán el desempeño del Canal de Fibra y por consiguiente tendrán una alta probabilidad de fracaso.

La Contra: La desventaja de arrancar desde un dispositivo SAN, es nuestro que ESX no tenga discos duros locales porque ahora está compartiendo el ancho de banda con el resto del tráfico SAN. Inclusive no podemos arrancar nuestro servidor si tenemos problemas con el dispositivo SAN que le impiden alcanzar el arranque del LUN.

A continuación, tenemos como comparar protocolos de bloques-nivel y archivos-nivel:

De Bloque-nivel: SCSI es un protocolo de bloque-nivel. Es decir, sus datos son manejados con respecto a cómo almacena la información en el disco duro- en bloques de tamaño definido. Los dispositivos de SAN e iSCSI transmiten los datos en bloques.

De archivo-nivel: Los protocolos de Archivo-nivel, por otra parte, leen y escriben datos en archivos de diferente longitud. Estos archivos son posteriormente almacenados, en bloques en el disco, pero eso pasa únicamente después de ser transferidos como archivos de diferente longitud. Los dispositivos de red conectada de Almacenamiento (NAS), usan protocolos de archivo- nivel (ya sean NFS o CIF). El iSCSI es una tecnología más nueva. Sin embargo, al igual que el Canal de Fibra, iSCSI pone los SCSI comandos y los bloques de datos en marcos de red. La diferencia es que iSCSI usa el TCP/IP protocolo de redes para la transmisión de los datos, en lugar del Protocolo del Canal de Fibra (FCP). Para enmarcar a los datos, iSCSI necesita un protocolo de iniciador.

Este puede ser:

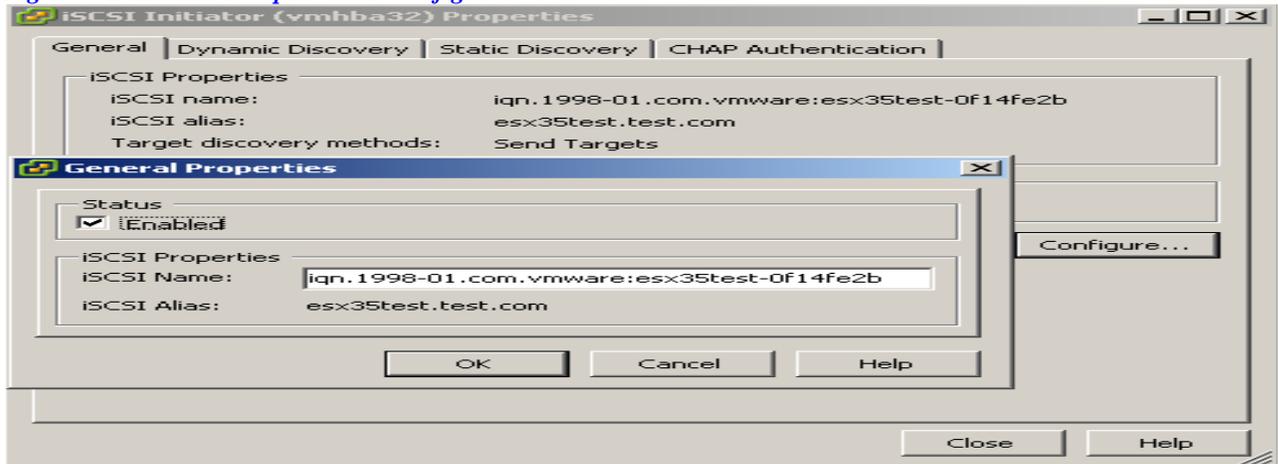
Iniciador basado en software: como el iniciador de software de la compañía Microsoft para SCSI.

Iniciador basado en hardware: Como un tarjeta de red TOE.

Si usamos una tarjeta de red TOE como hardware iniciador, la tarjeta hace una referencia en similitud a un iSCSI HBA.

Podemos usar ambos, iniciadores de software y hardware al mismo tiempo.

Figura 3.1 Muestra las opciones de configuración iSCSI.



Las comunicaciones en un iSCSI SAN. Los nodos del iSCSI son iSCSI dispositivos. Estos pueden ser iniciadores, Targets, o ambos. Independientemente, de que necesitan nombres y direcciones de IP. El uso de la tecnología iSCSI tiene las siguientes ventajas sobre usar Canal de Fibra:

El costo: El iSCSI puede costar aproximadamente desde 20 a 70 por ciento menos que el canal de Fibra, dependiendo del equipo y configuración.

La tolerancia a errores: El iSCSI puede ser configurado a un alto nivel de tolerancia contra errores, usando iniciadores de Ethernet switches y de discos al mismo tiempo.

El enrutamiento: Debido a que está basado en el protocolo entre redes TCP/IP, iSCSI es capaz de enrutarse sobre el IP network (red) sin requerir de un Gateway.

La familiaridad: El iSCSI usa el protocolo estándar de transmisión TCP/IP que ya conocemos, en el equipo con el que ya estamos familiarizados.

Aquí hay algunas desventajas al usar el iSCSI:

La velocidad: La velocidad del iSCSI está bajo la dependencia de la velocidad subyacente de la red. Depende del tráfico, puede ser mucho más lento que el Canal de Fibra.

La eficiencia: El iSCSI tiene un porcentaje más alto de rezago en la transmisión de datos, que el Canal de Fibra. Esto se debe a que, el porcentaje de información de tamaño del marco es mucho más pequeño con TCP/IP en comparación con el FCP, así que tenemos que transmitir más bits para mover la misma cantidad de datos.

Usa más Ciclos del CPU: Si estamos usando un iniciador de software, nos acaparara una cierta cantidad del desempeño de la CPU, dependiendo de la cantidad de paquetes que se estén transmitiendo. La única forma para evitar esta variable incalculable es usar un iniciador del hardware.

La seguridad: Es mucho más fácil para hackear la seguridad en un iSCSI, que en el Canal de Fibra, especialmente cuando nuestra carga de transmisión de datos es del doble de nuestro cliente habitual que los datos que se enlazan en red, como su transporte SAN (no recomendable). El esquema más seguro, es crear un protocolo separado entre redes físicas y lógicas “Ip”, para el tráfico de nuestro iSCSI.

Canal de fibra

Los dispositivos SAN de canal fibra son tolerantes a fallos, y con tecnología experimentada. La tecnología de canal de fibra empezó 1985 y obtuvo aprobación del ANSI en 1994. Un dispositivo SAN con canal de fibra puede ser desplegado en tres topologías físicas:

Punto a punto: En este esquema dos dispositivos son conectados directamente uno en seguida del otro.

En un ciclo arbitrado: Un dispositivo 1 se conecta a un dispositivo 2, el cual su vez se conecta con un dispositivo 3, etcétera, hasta que el *enésimo* dispositivo, se conecta de regreso al dispositivo 1. Muy similar a la topología de una red anillo Token.

Por medio de un dispositivo de switch (interruptor): Todos los dispositivos están conectados a un switch y al Canal de fibra. Estos interruptores proveen rutas de datos optimizadas, tal como una red de Ethernet por switches en topología de estrella. Esta topología fue la primer, bien soportada por la tecnología Vmware.

Obtenemos muchas ventajas si usamos un canal de fibra SAN:

Tecnología madura: Es una tecnología experimentada, esto significa la mayor parte los problemas tienen solución.

Tolerancia a errores: Podemos configurarla a un nivel alto contra errores.

Velocidad: Es típicamente más rápido que iSCSI.

Eficiencia: Cuadro por cuadro, el Canal de Fibra es más eficiente que iSCSI.

Si tuviéramos un rezago de transmisión de datos de un 50 % en una iSCSI, sobre el canal de fibra solo tendríamos el 13% de rezago.

Seguridad: Usando *enmascaramiento de zonificación* y *LUN* (son los métodos encargados de regular que dispositivos pueden verse entre sí), podemos esconder partes del SAN de muchos servidores diferentes para la seguridad, e impedir la sobrescritura accidental de los datos. Aquí tenemos las desventajas:

El costo: El uso de canal de fibra es más costoso que el uso del iSCSI. Sin embargo, usted tiene muchas más opciones en Canal de fibra ya que puede comprar las opciones por separado, mientras que el iSCSI, típicamente las vende todas juntas.

Gateway- portales de acceso: Necesitamos un Gateway de acceso para enrutar el tráfico del Canal de Fibra sobre el protocolo entre redes, lo cual requiere comprar más hardware, software y soporte.

Capacitación: Además se requiere capacitación en la nueva tecnología en lugar de usar lo más conocido que todos conocemos la conexión Ethernet.

Figura 3.2 Muestra la lista de los adaptadores de almacenaje disponibles.

Device	Type	SAN Identifier
vmhba6 QLogic QLE406x	Fibre Channel	21:01:00:1b:32:27:05:6f
vmhba3	iSCSI	iqn.2000-04.com.qlogic:ql...
vmhba4	iSCSI	iqn.2000-04.com.qlogic:ql...

NAS

El NAS es típicamente un dispositivo de almacenamiento de plug-and-play que soporta uno o ambos de los dos protocolos:

NFS (el sistema de archivos de red): Que es de código abierto.

El bloque de Mensaje del servidor (SMB): SMB es un Sistema de Redes de Windows.

El VMware usa el protocolo de servicio de red de archivos NFS, porque es un estándar más abierto que el SMB. La mayor parte de los componentes del VMware datacenter, como la VMoción y el DRS, trabajan con NAS.

Para que VMware use el NAS, necesitamos lo siguiente:

Un **puerto del VMKernel** en el interruptor virtual que se conecta al NAS.

Un **NAS de parte compartida**, con lo siguiente:

- *Acceso de escritura/lectura*
- *La habilidad para VMware de ejecutarse como usuario de la raíz*
- *La restricción de escribir sobre todos archivos antes de notificar al cliente que archivo de escriturase ha realizado.*

El Uso de un parámetro sync (sincronización) al crear la parte compartida.

Aquí tenemos algunas ventajas de la tecnología NAS:

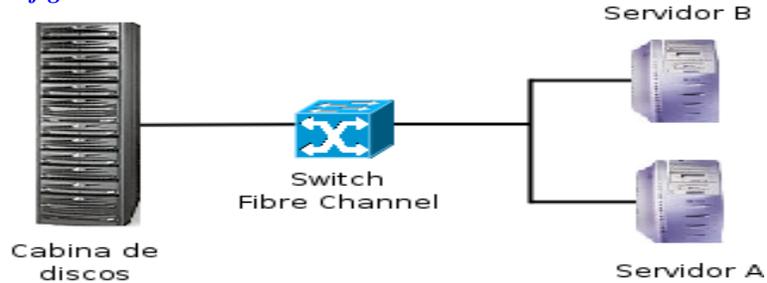
El almacenamiento es relativamente barato: NAS es grande para cualquier cosa que no requiera un rendimiento alto. Podemos almacenar archivos ISO en NAS y esto nos genera un gran archivo o un almacenamiento de tres en la fila.

La facilidad de uso: NAS es sumamente fácil para desplegar (Deploy) y conectarse.

Diferencias entre SAN y NAS

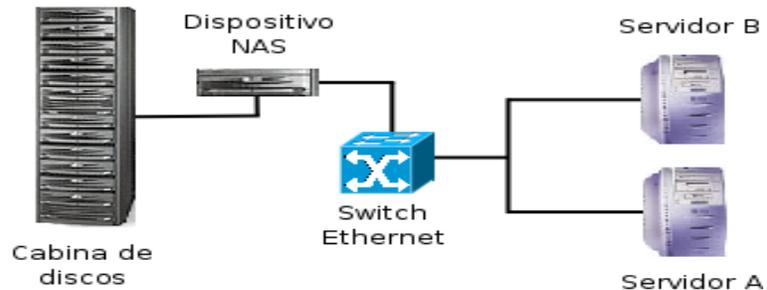
La mayor diferencia entre el **SAN** y el **NAS** es que el primero está conectado a los servidores mediante redes de altísima velocidad (normalmente canales de fibra) y el segundo está conectado a la red local, donde su desempeño depende de la velocidad de la misma. [8] En una **SAN** la información se almacena en la red **SAN**, y en el modelo **NAS** los clientes tienen que solicitar los archivos a los servidores para que éstos se los suministren. **SAN** es un sistema de discos que se conecta a los servidores mediante redes de altísima velocidad (generalmente canal de fibra). Se suele usar en servidores de BBDD donde los archivos de sistema, no se pueden montar por NFS o SAMBA y se necesita una comunicación rápida. [W3]

Figura 3.3 Configuración de la SAN.



El **NAS** es un sistema de discos que se conecta a la red como cualquier otro dispositivo y se le asigna una dirección IP como un miembro más de la red. La comunicación puede darse por protocolos como SAMBA o NFS.

Figura 3.4 Configuración de la NAS.



Lo siguiente es una lista de SAN y NAS de las prácticas óptimas:

El uso la tarjeta HBA tolerante de fallos en cada servidor.
El uso de interruptores de Fibra tolerante de fallos o de Ethernet en los SANs.
El uso de RAID tolerante de fallos para todos los LUNs.
El uso de los iniciadores de hardware iSCSI para el mejor desempeño de la UPC.
La configuración de un dispositivo iSCSI en una red física separada.
El uso del canal de Fibra (Channel SAN), cuándo el rendimiento específico alto es una prioridad. [5,8]El uso de un iSCSI si el costo es importante sin perder un rendimiento alto. El uso específico de un NAS para los propósitos que requieren un rendimiento específicamente inferior .El uso específico de hardware SAN que este certificado por VMware. La óptima colocación y configuración de máquinas de entrada/salida sobre diferentes LUNs y en nodos de CLUSTER diferentes para un desempeño óptima. La provisión de las diferentes rutas activas para almacenamiento de la optimización de máquinas de entrada/salida en la maximización del desempeño si es que nuestro SAN la soporta. La configuración de fábrica en el acceso múltiple ISL para interruptores SAN para aumentar el ancho de banda. La asignación de una zona única, entre el iniciador ESX y los puertos de proceso de almacenamiento para aislar iniciadores, desde el canal de fibra SAN, para el establecimiento registrado de notificaciones de cualquier avería.

Conectándose a los dispositivos de almacenaje.

Los host de ESX se conectan a una amplia variedad de subsistemas de almacenamiento. La mayoría de ellos usa el protocolo (la interfaz de sistemas informáticos pequeños) SCSI de bloque -nivel, pero algunos usan los protocolos de archivo-nivel también.

El Modelo Vmware de Almacenamiento de 3 capas.

VMware Infraestructuras ESX 3.x y 4.x, usan un modelo de almacenamiento a capas, que comprende lo siguiente: archivos de maquina virtual, un sistema robusto único de archivo de sistema llamado VMFS, designado para manipular el acceso a los archivos de la máquina virtual, y el almacenamiento en crudo de los subsistemas. [5,8]

El modelo de tres capas de almacenamiento está constituido como sigue:

- **La capa de la virtual de la máquina:** Esta es la capa en la cúspide consta de los archivos en el disco de la maquina virtual. Hay un archivo de disco para cada unidad de disco duro en una máquina virtual.
- **La capa del Host:** Es la capa intermedia que consta de la unidad lógica de números (LUN) en formato VMFS-FORMAT. Esta capa permite a los múltiples Hosts ESX el acceso a los archivos de la maquina virtual. Sólo un host ESX puede tener cualquier archivo virtual de la máquina corriendo a la vez.
- **La capa de almacenamiento en crudo:** La capa inferior consta del conjunto de sus arreglos de almacenamiento, los discos locales, y la red conectada de almacenamiento (NAS). Aquí, nuestros discos son agrupados para proveer alguna forma de tolerancia a fallos. Los grupos del disco son presentados en la capa intermedia como LUNs o en caso de ser NAS, como un NFS compartido.

Los anfitriones (Host ESX) ven particiones en este orden: primero por referencias a la tarjeta del Host; después por el identificador del adaptador; después el ID del target SCSI; el numero de LUN; y finalmente, el número de la partición.

El multiruteo (multipathing)

El Multipathing o El multiruteo, provee el acceso no-tolerante a fallas a los LUNs. Si perdiéramos el acceso hacia el procesador de almacenamiento en nuestro SAN, nuestro sistema puede acceder a los LUNs a través de una ruta de otro procesador de almacenamiento. Si perdiéramos una tarjeta HBA, una tarjeta alterna puede ser usada afín de que mantengamos la conectividad crítica de nuestro anfitrión Host ESX al almacenamiento. [5,8] A continuación tenemos cuatro rutas posibles que el servidor puede usar para llevarnos a un LUN 0 (sólo una ruta se puede estar en ejecución a la vez).

HBA 1 para el Procesador De Almacenamiento A hacia el LUN 0.

HBA 1 para el Procesador De Almacenamiento B hacia el LUN 0.

HBA 2 para el Procesador De Almacenamiento A hacia el LUN 0.

HBA 2 para el Procesador De Almacenamiento B hacia el LUN 0.

Multiruteo con el Canal de Fibra

Necesitamos al menos dos tarjetas HBA en cada Host ESX para realizar la multiruta.

ESX automáticamente configura la multiruta, dependiendo del tipo de arreglo que sea detectado en nuestra SAN. Ésta es otra razón muy buena para escoger sólo el hardware

SAN en las opciones de compatibilidad del hardware (HCL). Necesitamos saber lo siguiente:

Multipathing automáticamente se releva para evadir la falla desde una HBA hacia otra en cualquier caso de falla de hardware, de esta manera no tenemos nunca una interrupción. Sólo una sola ruta está disponible para cualquier LUN en cualquier momento. [5,8]

Hay dos políticas de multiruteo que son: los más recientemente usados (MRU) y la ruta fija (también conocida como una sola ruta predeterminada).

- MRU* en esta política, se continúa usando cualquier ruta que este actualmente en marcha. Si la ruta 1 falla y la ruta 2 está disponible, el sistema continúa usando la ruta 2 hasta que la ruta 1 vuelve a estar disponible otra vez. En otras palabras, MRU hace el salto a un ruta disponible mientras la dañada se recupera. Ésta es la política predeterminada para los arreglos de almacenamiento activos / pasivos en ejecución.

- El camino fijo* es justo lo contrario de MRU. Usa la ruta predeterminada en cualquier momento que la ruta está disponible. Si la ruta predeterminada deja de funcionar, otra ruta será usada. Hasta que la ruta predeterminada sea funcional otra vez, hasta este momento se convierte en una ruta “en Activo”, es decir en ejecución. Éste es el ajuste de fábrica para el estado activo/pasivo de nuestros discos en ejecución. No deberíamos cambiar manualmente los ajustes de fábrica predeterminado por VMware, los establece automáticamente de esta manera, basado en el tipo configuración de almacenamiento que se tenga.

Multiruteo con iSCSI

El protocolo TCP/IP provee la multiruta a través del protocolo entre redes IP de enrutamiento. El iSCSI, hace el uso de peticiones mejor conocidas como- SendTargets- estas se comunican y negocian con las direcciones y puertos del procesador de almacenaje que permiten el acceso a las diferentes rutas hacia los LUNS. [5,8] Si deseamos manualmente configurar las rutas SCSI necesitamos saber lo siguiente el iniciador del iSCSI puede estar situado en la parte superior de los múltiples NICS.

Los NICs y el enrutamiento de IP proveen el multiruteo.

Los algoritmos fijos y MRU son lo mismo para iSCSI.

Las rutas son descubiertas con las peticiones de los iSCSI SendTargets.

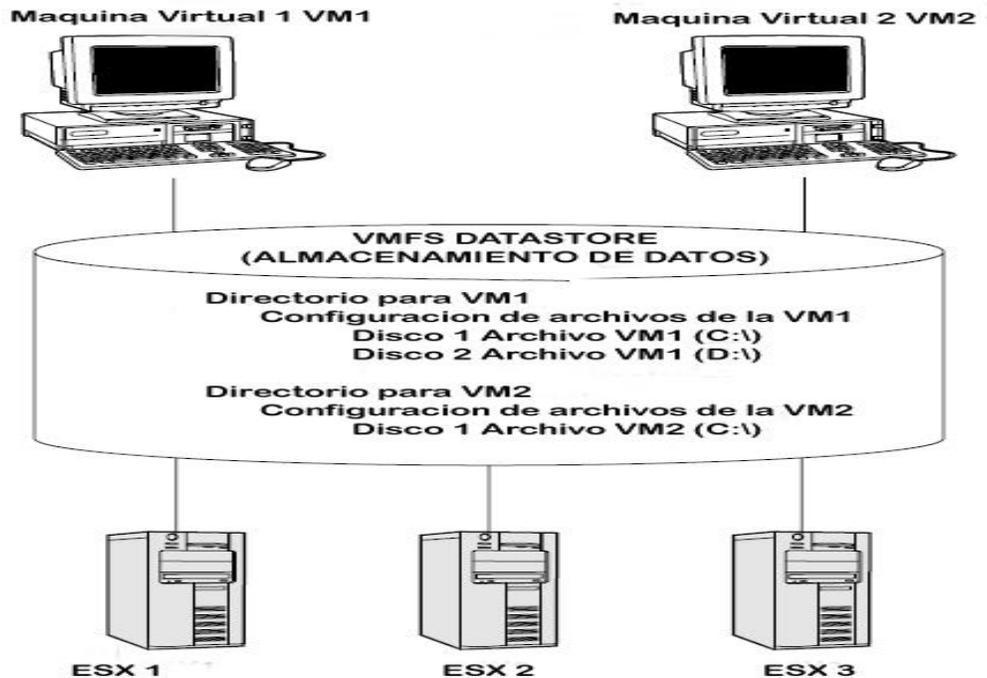
Sólo las configuraciones activas/pasivas serán soportadas. El direccionamiento hacia ambos iSCSI y el canal de fibra HBA hacia el mismo LUN todavía no es soportado.

El sistema de archivo del VMware (VMFS)

Es un archivo avanzado, multimaestro, distribuido en el archivo de seguridad y bloqueo del sistema. El VMFS está diseñado para ser de un rendimiento específicamente alto, es un archivo clustered (agrupado) de sistema. [5,8] Una forma fácil de explicarlo es comparándolo con un típico sistema de archivo. Un sistema de archivo típico le permite sólo a un servidor tener acceso de escritura/lectura. Pero en el caso del VMFS permite el acceso múltiple a varios servidores de lectura/escritura simultáneamente. Sin preocuparnos de la seguridad de la información en lo absoluto. VMFS hace uso distribuido de acarreo, para proveer recuperación rápida, así como también impedir que en el disco los servidores sobrescriban los mismos archivos.

Cuando se formatea un área de almacenaje de datos con formato de VMFS, se crea un archivo basado en un iSCSI archivo de sistema. Esto quiere decir que cualquier protocolo que soporte los comandos de un iSCSI lo puede acceder. Esto incluye iSCSI del Canal de Fibra, iSCSI, y un dispositivo SCSI localmente conectado.

Figura 3.5 Muestra el flujo del archivo VMFS. [5,8]



Creando áreas de almacenamiento de datos VMFS

Para crear un área de almacenamiento, lo hacemos a través del Add Storage Wizard.

Para añadir almacenamiento, hacemos lo siguiente:

1. Accedemos dentro del nuestro servidor usando el VIC.
2. Resaltamos con el mouse nuestro servidor.
3. Damos un clic sobre la pestaña de Configuración.
4. Damos un clic sobre el enlace de Adaptadores De Almacenamiento en la sección de Hardware a la izquierda de la pantalla.
5. Damos un clic sobre el enlace Rescan (re escaneo) en la esquina superior derecha de la pantalla.
6. Damos un clic sobre el enlace de Almacenamiento (SCSI, SAN, y NFS) en la sección del Hardware del lado izquierdo de la pantalla.
7. Damos un clic sobre el enlace de añadir Almacenamiento en la esquina superior derecha de la pantalla.

Figura 3.6 Muestra la pestaña de configuración de almacenamiento.

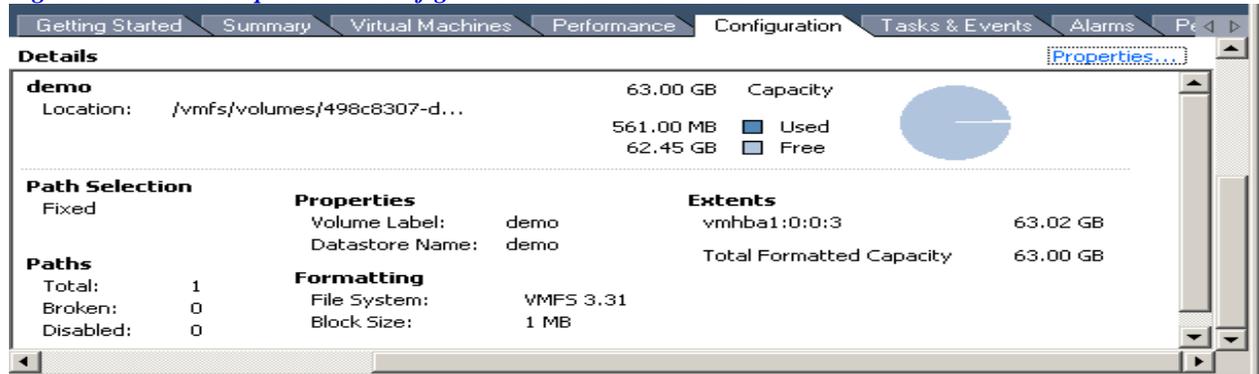
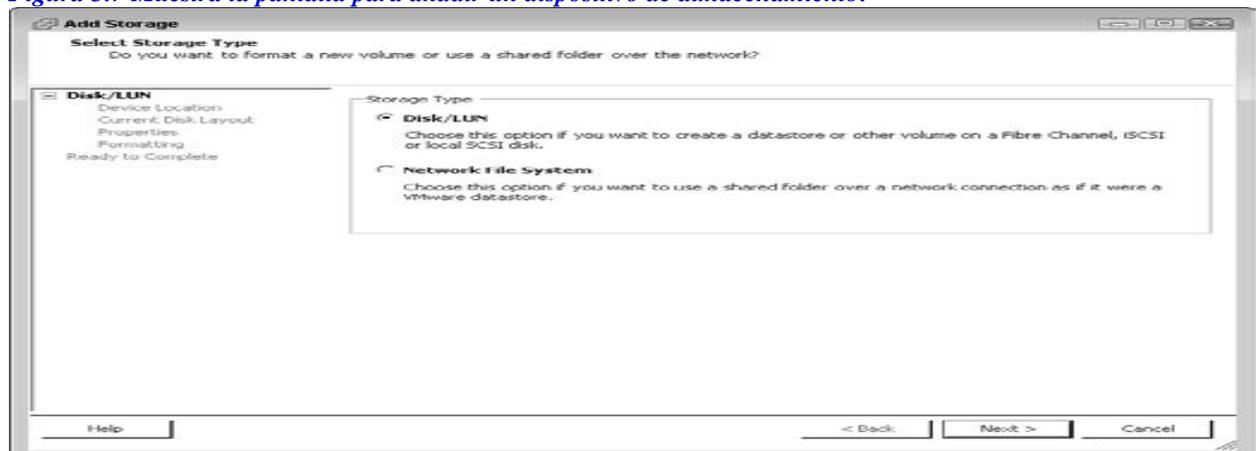


Figura 3.7 Muestra la pantalla para añadir un dispositivo de almacenamiento.



8. Escogemos el DISK/LUN como el tipo de almacenamiento.
 9. Damos un clic sobre el LUN que queremos agregar de la lista y luego damos un clic en siguiente.
 10. Revisamos el Layout del Disco y luego damos un clic en siguiente.
 11. Introducimos el nombre del área de almacenamiento de Datos y luego damos clic en siguiente.
 12. Escoja el tamaño máximo de Archivo que queramos y que pueda ser soportado y luego damos clic en siguiente.
 13. Revisamos la información. Si esta correcta, damos un clic en Finish.
- Nuestro nuevo VMFS de área de almacenamiento de datos ahora aparecerá con el resto de nuestro almacenamiento.

A continuación tenemos unas tablas de máximos generales para el ESX 3.5 y el Vsphere 4.0 de los distintos dispositivos de almacenamiento hasta ahora expuestos.

Tabla 3.1. Máximos generales de almacenamiento [1]

Detalle/ Valor	Máximo ESX 3.5	Máximo ESX 4.0
Tamaño del bloque de VMFS.	8MB	8MB
Tamaño máximo de dispositivos I/O (Antes de dividirlos).	32MB	32MB
El tamaño en bruto de mapeo del dispositivo.	2TB	2TB
Numero recomendado de hosts que se puede compartir en un volumen VMFS mientras existen máquinas Virtuales corriendo y expandiéndose sobre el volumen.	32	64
Numero de hosts por clúster.	32	32
Numero de volúmenes VMFS Configurados por servidor.	256	256
Numero de extensiones por volumen de VMFS.	32	32
Numero de HBAs (host bus adaptadores de cualquier tipo).	16	8
Numero de targets por HBA (iSCSI HBA).	15(64)	256

Tabla 3.2 Máximos de almacenamiento del VMFS2 [1]

Detalle/ Valor	Máximo ESX 3.5	Máximo ESX 4.0
Tamaño extendido	2TB (100MB min)	2TB
Tamaño del volumen	64TB	64TB
Tamaño Archivo (Tamaño de bloque = 1MB)	456GB	456GB
Tamaño Archivo (Tamaño de bloque = 8MB)	3.5TB	2TB
Tamaño Archivo (Tamaño de bloque = 64MB)	28.5TB	27TB
Tamaño Archivo (Tamaño de bloque = 256MB)	64TB	64TB
Archivos por volumen.	256+ (64 × número de Extensiones adicionales)	256+ (64 × número de Extensiones adicionales)
Tamaño extendido.	2TB	-
Tamaño del volumen.	64TB (2TB × 32 extendidos)	64TB
Tamaño de volumen (tamaño del bloque = 1MB)	~50TB	-
Tamaño de volumen (tamaño del bloque = 2MB)	64TB	-
Tamaño de volumen (tamaño del bloque = 4MB)	64TB	-
Tamaño de volumen (tamaño del bloque = 8MB)	64TB	-
Tamaño de archivo (tamaño del bloque = 1MB)	256GB	256GB
Tamaño de archivo (tamaño del bloque = 2MB)	512GB	512GB
Tamaño de archivo (tamaño del bloque = 4MB)	1TB	1TB
Tamaño de archivo (tamaño del bloque = 8MB)	2TB	2TB
Archivos por directorio	~30,000	~30,000
Directorios por volumen	~30,000	~30,000
Archivos por volumen	~30,000	~30,000

Tabla 3.3 Máximos del Canal de fibra de almacenamiento [1]

Detalle/valor	Máximo ESX 3.5	Máximo ESX 4.0
LUNs (número de unidades lógicas) por servidor	256	256
Tamaño del LUN	2TB	2TB
Número de rutas a un LUN específico	32	32
Número total de rutas sobre un servidor	1,024	1,024
LUNs abiertos concurrenciamente por toda m/virtual	256	256
ID de los LUN	256	256
HBA's por host	8	8
Targets por HBA	256	256
Puerto de HBA	16	16

Tabla 3.4 Máximos de almacenamiento NAS [1]

Detalle/Valor	Máximo ESX 3.5	Máximo ESX 4.0
Numero predeterminado de NAS (Almacenamiento conectado de Network) Almacenaje de datos.	8	8
Numero de almacenaje de NAS	32 (requiere cambios Avanzados de ajuste)	64(requiere cambios avanzados de ajuste)

Tabla 3.5 Máximos de almacenamiento de ISCSI (INTERNET SCSI) [1]

Objeto/valor	Máximo ESX 3.5	Máximo ESX 4.0
LUNs por servidor	256	256
LUNs concurrendamente usados	-	256
Targets dinámicos por puerto	-	64
Targets estáticos por puerto	-	61
Total de targets (estáticos + dinámicos no deben exceder este número)	-	256
Rutas hacia el LUN	-	8
Total de rutas	-	1024

Tabla 3.6 Máximos de software de almacenamiento de ISCSI [1]

Objeto/valor	Máximo ESX 3.5	Máximo ESX 4.0
LUNs por servidor	256	256
LUNs concurrendamente usados	-	256
Targets	64	-
Puertos límite de Ethernet con Software de pila de discos iSCSI stack	-	8
Total de targets (estático + dinámico no deben exceder este número)	-	256
Rutas hacia el LUN	-	8
Total de rutas	-	1,024

Figura 3.8 Muestra la configuración del almacenamiento por dispositivos disponibles.

Configuration					
Tasks & Events					
Alarms					
Permissions					
Maps					
Storage					
Identification	Device	Capacity	Free	Type	
ELISCSI01	vmhba19:0:0:1	999.75 GB	173.94 GB	vmfs3	
ELISCSI02	vmhba19:1:0:1	999.75 GB	358.02 GB	vmfs3	
ELISCSI03	vmhba19:2:0:1	999.75 GB	229.05 GB	vmfs3	
ELISCSI04	vmhba19:3:0:1	999.75 GB	195.24 GB	vmfs3	
esx1cluster2:stor...	vmhba7:0:0:3	60.00 GB	59.45 GB	vmfs3	
ESXCluster2DS	vmhba21:0:2:1	1.09 TB	1,015.41 GB	vmfs3	

3.2 ADMINISTRACIÓN DE RECURSOS.

La administración de recursos es la llave en cualquier ambiente virtualizado. En el contexto de VMware ESX y vSphere, la administración de recursos incluye agrupamiento de servidores (clustering), alta disponibilidad (HA), y el planificador distribuido de recursos (DRS). [1,6,7]

Los grupos (clusters) del VMware

Los grupos dentro del ambiente ESX le permiten mancomunar a los ESX Hosts físicos múltiples para crear una piscina virtual de recursos y combinarlos. Los tres elementos principales de agrupamiento de Clúster de VMware son: el DRS, no-tolerancia a fallas (FT, disponible en ESX 4.x), y las partes de HA.

VMware HA (alta disponibilidad)

Nos provee de un motor inteligente en base a costos-eficiencia que provee una gran disponibilidad dentro de nuestro Clúster ESX. Por ejemplo, si tenemos un grupo de cuatro nodos, Y un nodo en el grupo falla, podemos configurar el HA para que trabaje automáticamente y que ponga en marcha las máquinas virtuales del nodo fallido en cualquier nodo restante que exista como repuesto en los recursos disponibles.

El DRS de VMware

El planificador distribuido del recurso, activamente nos monitorea todas las máquinas virtuales en un clúster y administra sus recursos. El DRS puede ser configurado para proveer al administrador, con líneas de directivas en las cuales las máquinas virtuales pueden ser movidas hacia otro Host. También podemos configurar el DRS para automáticamente encargarse de la migración a través de la VMoción.

Piscinas de Recurso (Pools)

Las piscinas del recurso pueden usarse para crear particiones disponibles de memoria y CPU usando el recurso de pools (piscinas), podemos administrar mejor a través de los diferentes departamentos o dentro de un grupo de servidores. [7] Por ejemplo, quizá queremos dar a nuestro equipo del área de producción 20GHz de CPU y 20GB de memoria RAM y al equipo de desarrollo 10GHz de CPU y 10GB de memoria RAM. Podemos realizar esto mediante la creación de piscinas de recurso y la asignación de las máquinas virtuales para los departamentos correspondientes con sus respectivas piscinas según lo decidamos. Tenemos una piscina maestra de recurso llamada *General* y dos *Piscinas de*

subrecursos llamadas *Producción y Desarrollo*. En esta configuración, a las piscinas de subrecursos les son asignados recursos desde la piscina maestra de recurso (General). En este ejemplo, las piscinas de subrecurso, llamadas Desarrollo y Producción se les ha asignado la cantidad mostrada en la figura de abajo. (Figura 3.9)

Figura 3.9 Muestra la asignación para las piscinas de recurso.

CPU Reservation:	0 MHz	Memory Reservation:	0 MB
CPU Reservation Used:	17667 MHz	Memory Reservation Used:	20964 MB
CPU Unreserved:	4094 MHz	Memory Unreserved:	8041 MB
CPU Reservation Type:	Expandable	Memory Reservation Type:	Expandable

View:

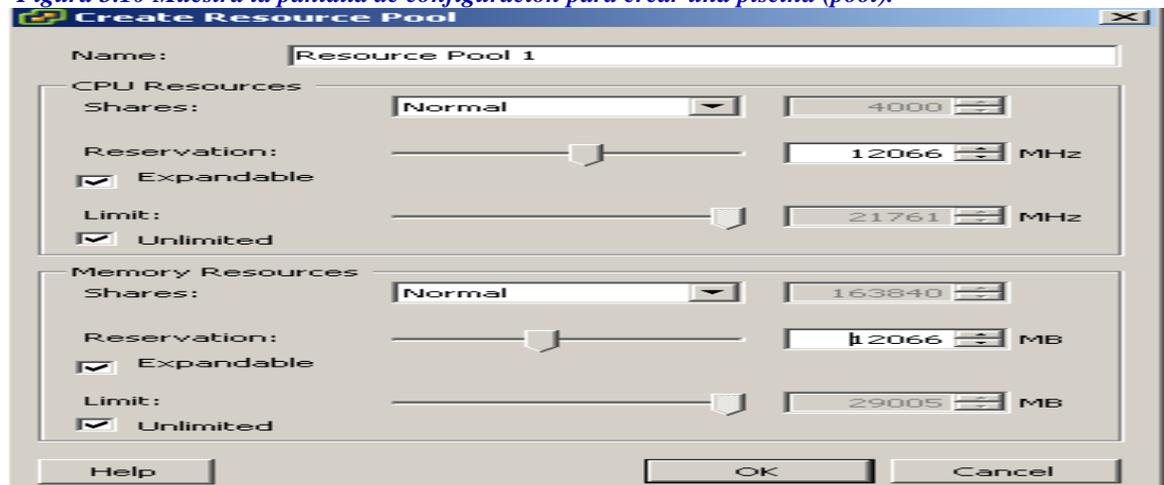
Name	Reservation - MHz	Limit - MHz	Shares	Shares Value	% Shares	Type	App Owner
Development	12496	Unlimited	Normal	4000	50	Expandable	
Production	5171	Unlimited	Normal	4000	50	Expandable	

Como crear una piscina

Las piscinas de recurso son una gran forma para administrar y compartir recursos entre grupos o departamentos dentro de nuestra organización. (Figura 3.10) Antes de que las piscinas del recurso puedan estar habilitadas en un clúster, necesitaremos asegurarnos que el DRS está habilitado. [7,9] Para habilitar una piscina del recurso en un grupo, nos logueamos dentro de nuestro servidor del vCenter y seguimos estos pasos:

- 1.- Damos un clic derecho en el clúster en el cual queremos crear la piscina del recurso y escogemos la opción de "Nueva Piscina de recurso".
- 2.- Se nos presentara una nueva ventana desde la cual podemos configurar la piscina de recurso. Las asignaciones de recursos de memoria y CPU para la piscina del recurso trabajan de modo semejante a la forma que trabajan para máquinas virtuales. Por ejemplo, demos este recurso con los siguientes valores de fondo común una reservación de 12,066MB de memoria RAM y 12,066MHz de CPU. Porque nosotros dejaremos la opción Expandible habilitada, la piscina puede explotar por encima de una reservación de 12,066 MHZ, así que limitamos de esta forma que no exceda la cantidad predeterminada y lo podemos reajustar los valores para repartirlos entre los departamentos de producción y desarrollo antes mencionados.

Figura 3.10 Muestra la pantalla de configuración para crear una piscina (pool).



3. Cuando hemos terminado, damos un clic sobre el botón OK y la piscina de recurso se agregará. Añadir nuevas máquinas virtuales nuevas dentro de la piscina de recurso puede hacerse de dos formas:

- Arrastrando la máquina virtual dentro de la piscina de recurso en el cliente del vCenter.
- Colocando una máquina virtual nueva dentro de una piscina existente del recurso cuando se crea una máquina virtual.

Creando Un Grupo (Clúster) (Figura 3.11)

Crear un clúster dentro de vCenter, le permite combinar a los múltiples ESX Hosts en un grupo centralizado, colocando todos sus recursos de CPU y memoria RAM, dentro de una piscina general para ser usado por las máquinas virtuales. Cuando se agrega a un Host ESX a un clúster, automáticamente los llegarán a estar disponibles para el uso de las máquinas virtuales. [7,9] El VMware nos permite un máximo de 16 ESX hosts en un clúster de vCenter 2.5x. Y en el vCenter 4.x podemos tener hasta 32 ESX hosts en un clúster.

El VMware ha hecho un trabajo realmente impresionante al hacer que el añadir un nuevo clúster sea tan fácil en el vCenter:

1. Cargamos el cliente del vCenter y nos logueamos dentro de nuestro servidor del vCenter.

2. Damos clic derecho en el nombre del datacenter y el seleccionamos Cluster Nuevo. El asistente de creación (wizard), del nuevo cluster, aparecerá para guiarnos a través del proceso de creación del nuevo Clúster. La primera pantalla en el asistente de instalación, nos pedirá introducir el nombre del nuevo clúster y que indiquemos si habilitamos o no estas dos características:

VMware HA

Esta característica está disponible sólo para los usuarios que tienen una licencia válida de la extensión del producto HA. Cuando habilitamos esta opción de VMware HA, detectará y proveerá un modo rápido de recuperación de máquinas virtuales por si algún Host ESX nos fallara. Ésta es una característica optativa y no necesitamos habilitarla al crear un clúster básico.

VMware DRS

Esta característica también requiere de una licencia válida. El DRS le permite al servidor del vCenter administrar a los Hosts como si fueran una piscina de recursos agregada. Los clústeres pueden estar divididos en pequeños grupos para el uso de las piscinas de recurso. El VMWARE DRS también le permite al vCenter administrar recursos en las máquinas virtuales, inclusive colocándolos en diferentes Hosts y ser usado en conjunto con el VMoción. Ésta es una característica optativa que no se requiere para crear un nuevo clúster. Cuando hayamos hecho nuestras selecciones, presionamos el botón siguiente para continuar.

Figura 3.11 Muestra el menú de creación de un nuevo Clúster.



2. Después, se nos preguntara donde queremos almacenar los swap files para las máquinas virtuales.

El VMware nos da dos opciones aquí:

- Almacene el swapfile en el mismo directorio como la máquina virtual. (Recomendable.)
- Almacene el swapfile en el datastore especificado por el HOST. (Esta opción no es recomendada, porque podríamos experimentar un desempeño menor.) Hacemos nuestra selección, luego presionamos el botón de siguiente para continuar.

4. Finalmente, revisamos el resumen y damos un clic Final para iniciar la construcción del nuevo Clúster. Ahora podemos agregar los Hosts ESX al nuevo Clúster. A continuación tenemos unas tablas generales de máximos de los recursos para el ESX 3.5 y el Vsphere 4.0. [1,10]

Tabla 3.7 Máximos de recursos de pool HA Clúster

Objeto/valor	Máximo ESX 3.5	Máximo ESX 4.0
Hosts por (HA) clúster de alta disponibilidad	32	32
Máquinas virtuales por HA clúster	-	1,280
Máquinas virtuales por host en un HA clúster	-	100
Host de rescate de conexión por clúster	4	4
Rescate de conexión como porcentaje del clúster	50.00%	50.00%

Tabla 3.8 Máximos de recursos del pool DRS Clúster

Objeto/Valor	Máximo ESX 3.5	Máximo ESX 4.0
Hosts por recursos distribuidos del planificador (DRS) clúster	-	32
Máquinas Virtuales por DRS clúster	-	1,280
Máquinas virtuales por host en DRS clúster	-	256

Tabla 3.9 Máximos de los recursos de pool (piscina) [1,10]

Objeto/valor	Máximo ESX 3.5	Máximo ESX 4.0
Piscinas de recurso por ESX host	512	4,096
Ramificaciones por piscina de recursos	256	1,024
Profundidad de árbol por piscina de recursos	12	12
Profundidad de árbol por piscina de recursos en un Clúster DRS	10	10
Recurso de piscina por clúster	128	512

3.3 EL MODELO DE RED VIRTUAL (VIRTUAL NETWORKING).

Las Opciones Virtuales del Interruptor

Existen muchas opciones de configuración para interruptores virtuales. Podemos asignar redes virtuales de área local (VLANs) y seguridad, así como también el límite de la cantidad de tráfico que las máquinas virtuales puedan generar. Adicionalmente, se puede asignar muchos NICs para un interruptor virtual para una carga balanceada y para la no-tolerancia a fallas. Los NICs son conocidos como *adaptadores de enlace hacia arriba*. Los adaptadores múltiples de enlace hacia arriba son una elección sabia para los ambientes de producción. [7, 8,10] Si queremos una red virtual aislada, podemos establecer un interruptor virtual sin un adaptador de enlace hacia arriba. Cualquier máquina virtual conectada dentro de un interruptor desconectado sólo pueden comunicarse una con la otra: Nunca podrá comunicarse con las maquinas virtuales externas conectadas a otro interruptor virtual. Esto nos permite crear un gran ambiente experimental aislado. Sin embargo, si queremos que nuestro ambiente experimental accediera al mundo exterior, lo podemos conseguir. Las máquinas virtuales pueden ser configuradas con dos tarjetas de la red, una para actuar como un firewall y otra como un router. Este router, que se conecta a ambos, los

interruptores virtuales desconectados y los físicamente conectados, puede usarse para determinar qué flujos de tráfico en la red entra y sale de nuestro ambiente de prueba.

Los interruptores virtuales tienen muchas similitudes con los interruptores físicos:

- Están dotados de numerosos puertos para conectarse a las máquinas virtuales.
- Cada marco es reenviado a uno o más puertos para la transmisión.
- Ofrecen soporte para VLANs.
- Tienen puertos de velocidad variable.
- Ofrecen políticas seguridad.

Y a pesar de sus similitudes, los interruptores virtuales y los interruptores físicos también tienen diferencias:

- Podemos cambiar el número de puertos en un interruptor virtual.
- Varios NICs físicos pueden ser asignados a un interruptor virtual solo para combinar el rendimiento específico o para la No-tolerancia a fallas.
- Los interruptores virtuales son únicamente software y existen en los confines del VMkernel.
- Los interruptores virtuales no tienen que aprender sus tablas de direcciones de la MAC, ellos ya las conocen porque los interruptores y los adaptadores virtuales de la red son ambos dispositivos únicos de software.
- Los interruptores virtuales saben la configuración de los adaptadores virtuales de la red conectado a ellos.
- No podemos configurar en cascada a los interruptores virtuales como lo hacemos con los interruptores físicos.

Las funciones de los interruptores virtuales

Los interruptores virtuales realizan tres funciones diferentes para un Host ESX. Cada función es considerada un tipo de conexión diferente o puerto:

La máquina virtual: Como el nombre lo indica, *los puertos virtuales de la máquina* están donde conectamos las máquinas virtuales. [7,8] Los puertos virtuales de la máquina conectan sus máquinas virtuales una con otra y se conectan con las que están fuera. Cada máquina virtual se conecta dentro de un puerto en uno o más interruptores virtuales. Cualquier adaptador de enlace hacia arriba que le asignemos al interruptor virtual provee un puente hacia nuestra red física.

El VMkernel: Las conexiones del VMkernel acceden a los servicios basados en la IP, tal como el almacenamiento IP sistema de redes, IP entre redes, y la VMoción. *La VMoción nos* permite mover las máquinas virtuales de un anfitrión ESX para otro aun corriendo.

Los interruptores virtuales le proveen la conectividad de IP (protocolo entre redes) al VMkernel. Esto nos permite conectarnos a la línea de comando en nuestro servidor de forma remota. También permite al VMkernel acceder al almacenamiento basado en protocolos entre redes, como red (NAS) y la Interfaz Pequeña (iSCSI).

La Consola de Servicio: Este tipo de conexión le provee el acceso a los servicios de administración del ESX. Son también *conocidos como servicios base de la administración*. Los interruptores virtuales acceden a los servicios bases de la gerencia. La Consola de Servicio se conecta a un puerto virtual del interruptor. Los clientes virtuales (VIC) de

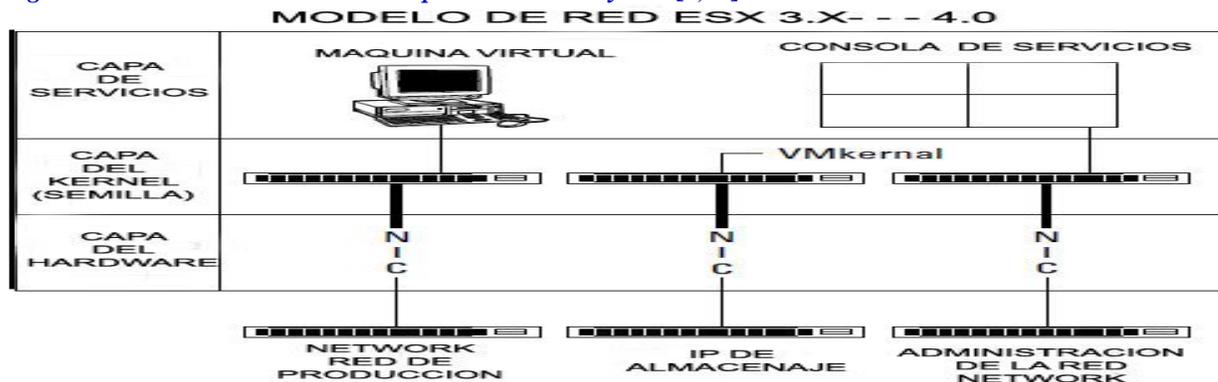
Infraestructura se conectan a la Consola de Servicio y de esta forma podemos configurar y operar nuestro servidor. Es altamente recomendable tener un puerto de consola de Servicio de repuesto en caso de que perdamos uno debido a una falla de hardware. Sin la Consola de Servicio, solo podemos acceder a nuestro ESX mediante la línea de comando.

Modelo de red

Este modelo de red de tres capas está constituido, en resumen, como sigue:

La capa que se encuentra en la cúspide es la capa de servicios; nuestra consola de servicio y las máquinas virtuales residen aquí. Los servicios en la capa de servicios conectan a las máquinas virtuales. Los interruptores virtuales existen en la capa del VMkernel, que es la capa intermedia. De hecho, la semilla (kernel) misma se conecta a uno o más interruptores. El Kernel (semilla), también controla el acceso al hardware, provee los medios para los adaptadores de enlace hacia arriba de asignación que se conectan con los interruptores virtuales. Los adaptadores de enlace hacia arriba NIC's, se conectan a su red física que es la capa inferior de hardware.

Figura 3.11 Muestra el modelo de red para el ESX 3.x y 4.0 [1,10]



Creando un interruptor virtual.

Durante la instalación del ESX Server, se crea el interruptor predeterminado junto con la Consola de Servicio. Notemos que todos los puertos de la consola de servicios son designados con la siguiente nomenclatura por convención: vSwif #:IP_Address. [1,8]

Para crear un interruptor virtual, tenemos que conectarnos o acceder en el sistema a través del cliente del vCenter. Una vez dentro seguimos estos pasos:

1. Damos un clic sobre nuestro ESX host para seleccionarlo.
2. Damos un clic sobre la pestaña de Configuración.

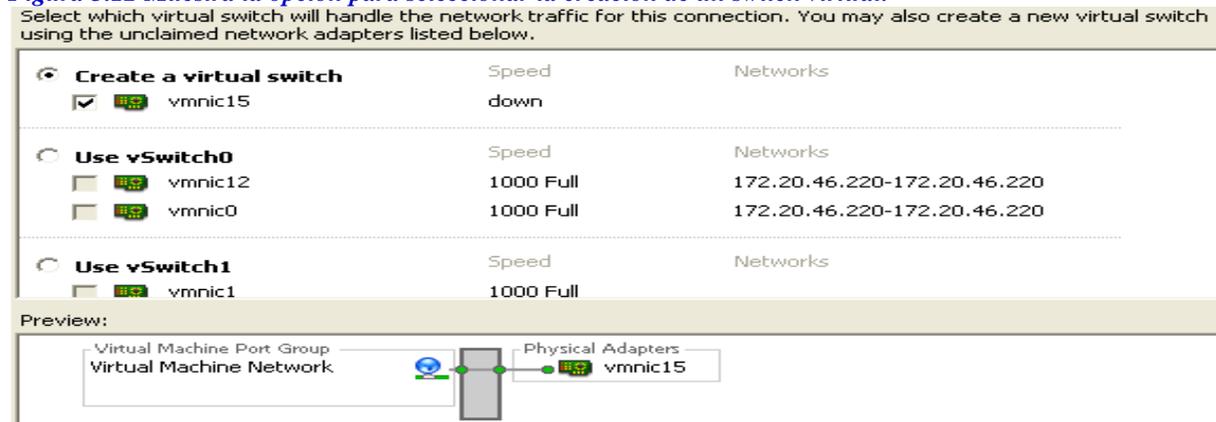
La sección de Sistema de Redes de la pestaña de Configuración muestra los interruptores, los grupos de puertos, y las máquinas virtuales conectadas entre sí.

3. En la sección de Hardware, damos un clic sobre Networking link (vinculo).
4. Damos un clic en añadir Networking, (sobre la esquina superior derecha).

El asistente de networking se abrirá. El primer paso es escoger la clase de conexión que el interruptor proveerá. Podemos añadir otro tipo de conexiones y NICs adicionales más tarde, modificando las propiedades de los switches.

5. Escogemos el tipo de conexión apropiado y luego damos un clic en siguiente. En este caso, seleccionamos Máquina Virtual.
6. Seleccionamos el adaptador físico que queremos que este interruptor use seleccionando la casilla de verificación apropiada.
7. Seleccionamos crear un Interruptor Virtual y luego damos un clic sobre el botón siguiente. *(Figura 3.12)*
8. Aceptamos la pestaña predeterminada de la red y luego damos un clic sobre el botón siguiente.
9. Damos un clic en finish, para terminar.

Figura 3.12 Muestra la opción para seleccionar la creación de un switch virtual.



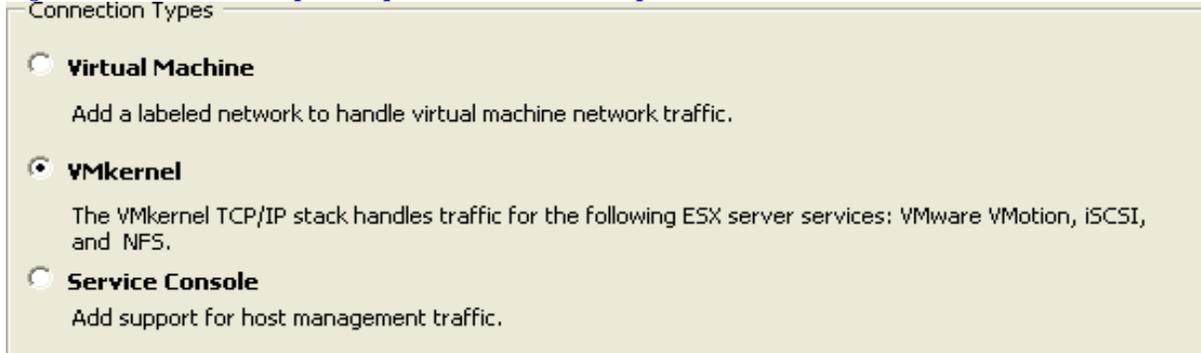
Creación de un puerto de Vmkernel.

El ESX3 usa un puerto de VMkernel para manejar todo tráfico basado en redes para software iSCSI, VMoción, y NFS, porque estas tecnologías son basadas en redes y pueden usar el mismo VMkernel.

Los puertos del VMkernel pueden ser configurados en el vCenter o mediante la línea de comando.

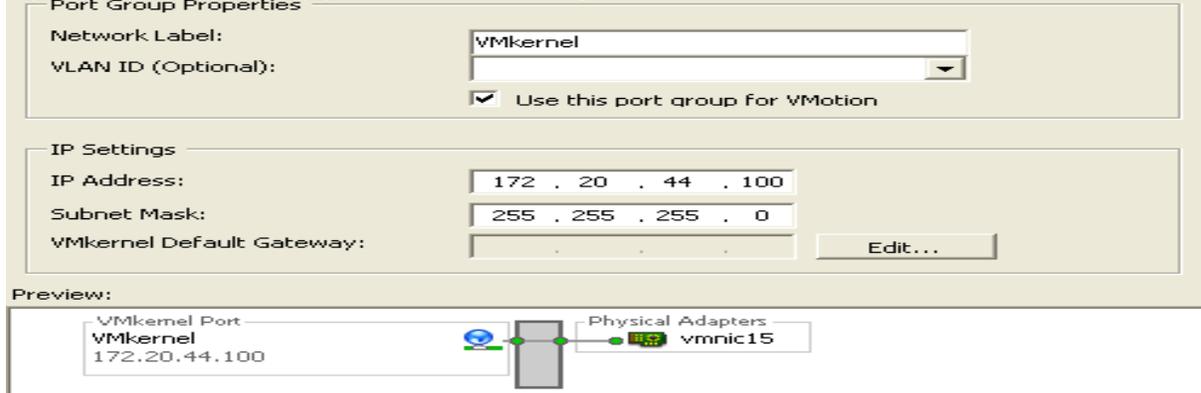
1. Nos logueamos dentro del vCenter Server y seleccionamos el servidor de la lista de inventario.
 2. Seleccionamos la pestaña de Configuración del panel de la ventana correcto y navegamos hacia Networking. Cualquier configuración actual de la red se mostrara. Damos Un Clic en añadir un networking link para crear un interruptor virtual nuevo.
 3. Tres opciones se presentaran. Escogemos la opción del VMkernel, la cual nos permite añadir un puerto del VMkernel para administrar y manipular el tráfico de TCP/IP para la VMoción, NFS, o iSCSI. *(Figura 3.13)*
- Damos un clic en siguiente para continuar.

Figura 3.13 Muestra las opciones para la creación de un puerto de Vmkernel.



4. Hacemos una selección de "crea un interruptor virtual" y seleccionamos el *vmnic* que se usará para manipular el tráfico de la VMoción, por ejemplo. Damos un clic en siguiente para continuar.

Figura 3.14 Muestra la configuración del Vmkernel para la Vmoción.



5. El paso que configura el VMkernel para la VMoción se hace también aquí: "Usemos este puerto de grupo para el VMoción", debe ser habilitado y seleccionado. Esto nos permite al puerto del grupo, regular el tráfico del VMoción. (Figura 3.14)
6. Introducimos la dirección de protocolo IP, y llenamos los campos de la máscara de subred. Si tuviéramos que detallar mas los ajustes de la red para ser configurados, tales como portales de acceso, Gateways, Routing, y los servidores de DNS, damos un clic sobre el botón de Edición para configurarlos. Guardamos los cambios dando un clic en OK, y después damos un clic en siguiente para continuar.
7. Checamos la pantalla de resumen y damos un clic en Finish, para finalizar la configuración.

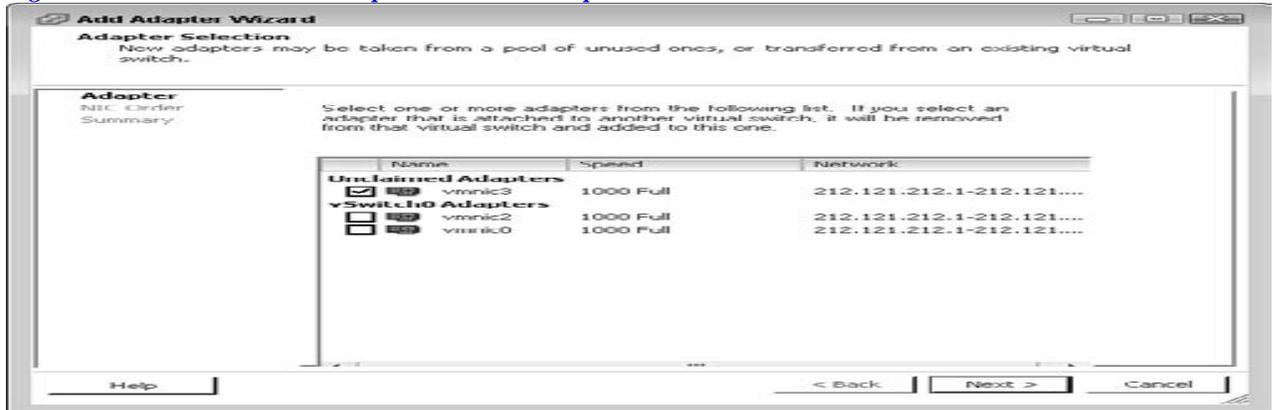
Añadir adaptadores de red (networking).

Si queremos añadir adaptadores de network, adicionales seguimos estos pasos:

1. Damos un clic sobre nuestro ESX HOST para seleccionarlo. [1,8]
2. Damos un clic sobre la pestaña de Configuración.
3. En la sección de Hardware, damos un clic sobre el enlace de Sistema de Redes Networking link.
4. Damos un clic sobre el enlace de Propiedades más cercano a nuestro interruptor.
5. Damos un clic sobre la pestaña de los Adaptadores de la Red.

6. Damos un clic sobre el botón Add, para iniciar el asistente de añadir Adaptador.
(Figura 3.15).
7. Seleccionamos la casilla de verificación que está al lado del adaptador que queremos agregar y damos un clic en el botón siguiente.

Figura 3.15 Muestra la ventana para añadir un adaptador de red.



8. Aceptamos la Orden predeterminada del NIC y luego damos un clic en siguiente.
9. Revisamos la página de resumen y luego damos un clic en Finish (terminar).

La configuración de los NICs.

La pestaña del NIC Teaming está dividida en tres secciones:

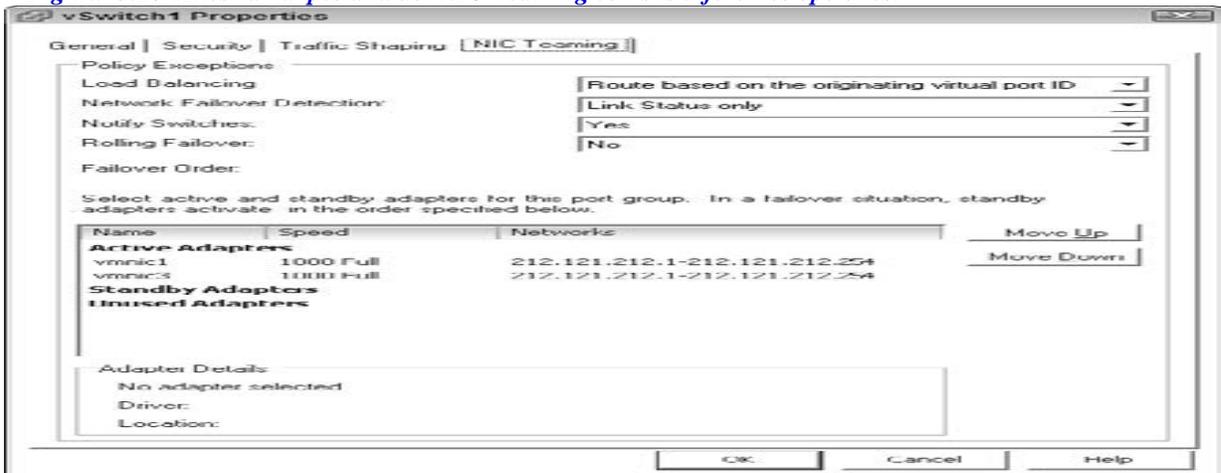
Las Excepciones de Política: Aquí es donde configuramos nuestras políticas.

Los adaptadores: Aquí, especificamos el estado de cada NIC asignado al interruptor.

Los Detalles del Adaptador: En esta opción, hacemos que el driver y la ranura de PCI de cada adaptador resalten. [6,8]

Las Excepciones de Política: La Carga Balanceada. (LOAD balancing). El balanceo de la carga nos ofrece tres formas diferentes a escoger por las cuáles el adaptador de enlace hacia arriba, regula el tráfico saliente. Podemos escoger el de puerto virtual basado en un algoritmo, el basado en la dirección MAC algoritmo, o el basado en una dirección IP algoritmo, y escoger una orden explícita de rescate de la conexión FAILOVER. Cada uno tiene sus pros y contras. Depende de la configuración pero el más usado es el de la dirección MAC.

Figura 3.16 Muestra la pestaña del NIC Teaming con sus diferentes opciones.



Prácticas óptimas de networking para VMware ESX 3.x y 4.0

- Debemos almacenar nuestra consola de servicio en una red separada por seguridad.
- Debemos evitar que nadie tenga control de la Consola de Servicio, para que no tenga acceso al mando del servidor.
- Debemos almacenar nuestros puertos del VMkernel en una red separada para obtener un rendimiento específico.
- Recordemos que la memoria de la máquina virtual es copiada sobre esta red cuando usamos el VMoción.
- Siempre debemos usar múltiples adaptadores de enlace hacia arriba por sus capacidades de rescate de la conexión Failover.
- Siempre debemos usar múltiples adaptadores de enlace hacia arriba por sus capacidades para nivelar la carga.
- Debemos separar las máquinas virtuales la una de la otra para su mejor desempeño y mejor seguridad. Podemos realizar esto con grupos de puertos o podemos separar los interruptores virtuales.
- Debemos usar el número adecuado de interruptores según las necesidades.
- Los sistemas tienen menos problemas al arrancar y son más fáciles de localizar las averías.
- Debemos usar los ajustes predeterminados a menos que necesitemos modificarlos.
- Debemos usar un firewall virtual si es necesario proteger nuestras máquinas más importantes. Lo podemos hacer usando un interruptor virtual sin enlace hacia arriba.
- El uso de adaptadores y un interruptor virtual con adaptadores de enlace hacia arriba que se conecten a una máquina virtual realizando el papel de firewall.
- Debemos hacer uso de las VLANs y políticas de seguridad si necesitamos seguridad adicional. [6, 8,10]

Tenemos las tablas de máximos generales de Networking para nuestro Servidor ESX 3.5 y ESX 4.0 [6,10]

Tabla 3.10 Máximos de redes (Networking)

Objeto/valor	Máximos ESX 3.5	Máximos ESX 4.0
Adaptadores físicos e100 NICs	26	-
Adaptadores físicos e1000 NICs (PCI-x)	32	32
Adaptadores físicos e1000 NICs (PCI-e)	32	32
Adaptadores físicos Broadcom NICs	20	-
igb 1GB Puerto de Ethernet (Intel)	-	16
tg3 1GB Puertos de Ethernet (Broadcom)	-	32
bnx2 1GB Puertos de Ethernet (Broadcom)	-	16
Forcedeth 1GB Puertos de Ethernet (NVIDIA)	-	2
Scio 10GB Puertos de Ethernet (Netherion)	-	4
nx_nic 10GB Puertos de Ethernet (Net-XEN)	-	4
ixgbe Oplin 10GB Puertos de Ethernet (Intel)	-	4
bnx2x 10GB Puertos de Ethernet (Broadcom)	-	4
Numero de dispositivos de PCI VMDirectPath por host	-	8
Numero de grupo de puertos por switch estándar	512	512
Numero de NICs en un equipo	32	-
Numero de puertos de Ethernet	32	-
Numero de virtual NICs por switch virtual	1,016	-
Numero de switches virtuales por host	127	248
Número de grupos de puertos (VLANs)	4,096	4,096

Tabla 3.11. Networking Redes de vNetwork de switch distribuidas valores máximos (solo para 4.0)

Objeto/valor	Máximos ESX 3.5	Máximos ESX 4.0
Total de puertos para switches virtuales por host (vDS and vSS ports)	-	4,096
Puertos distribuidos para switches virtuales del network por vCenter	-	6,000
Grupos distribuidos por vCenter	-	512
Switches distribuidos por vCenter	-	16
Hosts por switch distribuido	-	64

Capítulo 4.

HERRAMIENTAS ÚTILES DESDE LA LÍNEA DE COMANDO.

En este capítulo nos enfocaremos en usar la línea de comando (CLI), provista por VMware ESX y el vSphere Asistente Management (vMA), que es una importante herramienta, que usamos cuando no tenemos acceso a la consola de servicios mediante una interfaz gráfica de VMware vSphere. Mencionaremos los comandos más importantes directamente con el uso indicado es decir; exhibir información del servidor y el monitoreo del uso virtual del CPU, la memoria RAM, del desempeño del almacenamiento y el desempeño del networking. Algunos comandos mostrados son usados en plataformas de UNIX, otros si son exclusivos de nuestro VMware ESX SERVER infraestructura.

[1, 5, 8,10]

4.1 EXHIBIENDO INFORMACIÓN DEL SERVIDOR

Si queremos exhibir información actual acerca de nuestro ESX Server la solución es ejecutar el comando de `esxcfg-info` en el ESX Server. Esta herramienta de la línea de comando es una forma poderosa pero simple para enterarnos de la información de nuestro ESX Server y su ambiente. Usando el comando de **esxcfg-info**, podemos obtener a detalle información acerca de la configuración y hardware del servidor con la sintaxis siguiente:

\$ esxcfg-info -h

El uso: El modo de `esxcfg-info` y sus prefijos

- | | |
|------------------|---|
| - a, -- all | Imprime toda la información. |
| - w, -- hardware | Imprime la información del hardware. |
| - r, -- resource | Imprime la información del recurso. |
| - s, -- storage | Imprime información de almacenamiento. |
| - n, -- network | Imprime la información de la red. |
| - y, -- system | Imprime la información del sistema. |
| - o, -- advopt | Imprime las opciones avanzadas. |
| - u, -- hwuuid | Imprime información del hardware uuid. |
| - b, -- bootuuid | Imprime información del hardware uuid. |
| - e, -- boottype | Imprime el tipo arranque. |
| - c, -- cmdline | Imprime información del vmkernel de la línea de comando. |
| - f, -- format | Imprime la información en un formato determinado y los valores válidos están en formato "xml" y "perl". |
| - h, -- help | Imprime este mensaje. |

Las opciones pueden ser introducidas en cualquier combinación para exhibir información específica. Si ejecutamos un comando de `esxcfg-info` por si solo o con un prefijo -a, nos desplegara todos los valores. El siguiente ejemplo exhibe la primera parte y las primeras líneas de salida de la información de uno de nuestros sistemas:

\$ esxcfg-info | more

+Host:

\ == +Hardware info:

```

|---- BIOS UUID.....0x44 0x45 0x4c 0x4c 0x34 0x0 0x10
0x38 0x80 0x56 0xb6 0xc0 0x4f 0x4b 0x46 0x31
|---- Product Name.....PowerEdge R900
|---- Vendor Name.....DELL INC.
|---- Serial Number.....XXXXXXXX
|---- Hardware Uptime.....1762529093951

```

La información que podemos obtener acerca de nuestro sistema con el uso de este comando es tan integral, que podemos tener el deseo de exportarla hacia un archivo de texto, y esto se hace de la siguiente manera:

```
esxcfg-info > esxcfginfo12102008.txt
```

4.2 INTRODUCIÉNDONOS A EL MODO DE MANTENIMIENTO DESDE LA LÍNEA DE COMANDO.

Si no podemos acceder a nuestra Interfaz Gráfica de Usuario del vCenter, y queremos poner a nuestro servidor ESX, en el modo de mantenimiento. Nos logueamos dentro de nuestro ESX host, mediante el SSH o directamente desde la consola. [1,10] Para iniciar el modo de mantenimiento, usamos esta herramienta de comandos:

```
vimsh -n -e /hostsvc/maintenance_mode_enter
```

Para salir el modo de mantenimiento, tecleamos esto:

```
vimsh -n -e /hostsvc/maintenance_mode_exit
```

Estos comandos no están documentados y no tienen soporte directo de la empresa de VMware. Sin embargo, trabajan correctamente en el ESX 3.x. Alternativamente, podemos usar el VI Perl ToolKit, para iniciar el modo de mantenimiento con la API prevista por la empresa VMware.

4.3 MONITOREANDO EL USO DEL CPU

Si queremos monitorear el uso del CPU de nuestro ESX Server, usamos la herramienta *del esxtop*. Desde la línea de comando de nuestro ESX Server, ejecutamos lo siguiente:

```
esxtop
```

Esta utilidad es muy similar al *esxtop*, en ambientes de Unix, *esxtop*. Una vez que *el esxtop* se está ejecutando, presionamos *c* para cambiar al el modo del CPU. Esto exhibirá las estadísticas actuales de uso, de nuestra CPU del servidor. [1, 8,10]

Figura 4.1 Pantalla que muestra el despliegue de las estadísticas del sistema.

```

8:56:45am up 28 days 23:29, 155 worlds; CPU load average: 0.17, 0.16, 0.18
PCPU(%): 9.46, 7.53, 7.07, 8.24, 26.36, 19.56, 9.59, 15.81 ; used total: 12.95
CCPU(%): 1 us, 2 sy, 97 id, 0 wa ; cs/sec: 676

```

ID	GID	NAME	NWLD	%USED	%RUN	%SYS	%WAIT	%RDY	%IDLE	%OVRLP	%CSTP	%MLMTD
1	1	idle	8	704.24	707.88	0.00	0.00	99.86	0.00	0.01	0.00	0.00
2	2	system	6	0.02	0.02	0.00	600.00	0.00	0.00	0.00	0.00	0.00
6	6	helper	23	0.02	0.02	0.00	2300.00	0.03	0.00	0.00	0.00	0.00
7	7	drivers	15	0.01	0.01	0.00	1500.00	0.00	0.00	0.00	0.00	0.00
8	8	vmotion	1	0.00	0.00	0.00	100.00	0.00	0.00	0.00	0.00	0.00
9	9	console	1	4.19	4.16	0.04	96.41	0.38	96.37	0.07	0.00	0.00
18	18	vmware-vmkauthd	1	0.00	0.00	0.00	100.00	0.00	0.00	0.00	0.00	0.00

La primera línea exhibida nos muestra: (*Figura 4.1*)

- El tiempo actual (8:56:45 a.m., En nuestro ejemplo)
- El tiempo transcurrido desde el último reinicio
- El número de cuantas maquinas virtuales están actualmente corriendo
- El desempeño del CPU promedio sobre 1, 5, y 15 minutos

La línea PCPU (%) despliega el porcentaje de utilización del CPU por la utilización del CPU físico y el promedio total de todos los CPUs físicos.

La línea CCPU (%) muestra el tiempo de procesador como lo reporta el ESX Server o la consola. Este es un tiempo variable del usuario, que es contrario al PCPU, el cuál registra el tiempo desde la perspectiva del CPU.

Debajo de las líneas del PCPU y CCPU, tenemos los siguientes atributos disponibles:

ID

Indica el número del procesador

GID

Indica el número de las piscinas del recurso actualmente corriendo.

NAME

Indica el nombre del proceso actualmente corriendo

NWLD

Indica el número de maquinas virtuales o entornos en el grupo

%USED

Indica el porcentaje de uso de la CPU física consumido por la piscina del recurso, máquina virtual, o entorno.

%RUN

Indica el porcentaje del tiempo total programado (sin tener en cuenta el tiempo del hyper-threading ni del sistema)

%SYS

Indica el tiempo de sistema: El tiempo que transcurre mientras el código del kernel se ejecuta.

%WAIT

Indica el porcentaje total de tiempo de la piscina del recurso o entorno que se ha gastado en un estado de espera.

%RDY

Indica el porcentaje de tiempo de la piscina del recurso, la máquina virtual, o mundo que se ha gastado al momento y está listo para correr, pero en espera de obtener una orden del CPU.

%IDLE Indica el porcentaje de tiempo del mundo VCPU que se ha gastado en un ciclo de tiempo desocupado (éste tiene aplicación sólo para el mundo VCPU; para otros casos, este campo será cero)

%OVRLP

Indica el porcentaje de tiempo transcurrido por los servicios del sistema trabajando para otros entornos.

4.4 MONITOREANDO EL USO DE LA MEMORIA RAM.

Si queremos monitorear la memoria del ESX Server usando la línea de comando, tenemos que hacer uso de la utilidad *del esxtop*. Desde la línea de comando en nuestro ESX Server, ejecutamos el siguiente comando:

esxtop

Una vez que *el esxtop* se ejecuta, presione la tecla **m** para cambiar al modo de memoria. Esto exhibirá las estadísticas de uso actual de memoria del servidor. La salida será similar a la figura de abajo. *El esxtop* tiene una percepción en la salida muy similar al estándar de Unix, pero además provee información extra, específica para nuestro ESX. [1,8,10]

Figura 4.2 Pantalla que nos muestra el usos de la memoria y su disponibilidad.

```
6:27:47am up 1:03, 53 worlds; MEM overcommit avg: 0.27, 0.25, 0.14
PMEM /MB: 1047 total: 272 cos, 135 vmk, 55 other, 585 free
VMKMEM/MB: 731 managed: 43 minfree, 222 rsvd, 417 ursvd, high state
COSMEM/MB: 30 free: 543 swap_t, 543 swap_f: 0.00 r/s, 0.00 w/s
PSHARE/MB: 12 shared, 4 common: 8 saving
SWAP /MB: 0 curr, 0 target: 0.00 r/s, 0.00 w/s
MEMCTL/MB: 0 curr, 0 target, 0 max
```

GID	NAME	NWLD	MEMSZ	SZTGT	TCHD	%ACTV	%ACTVS	%ACTVF	%ACTVN	OVHDIUW	OVHD	OVHDMAX
15	vmware-vmkauthd	1	5.48	5.48	1.59	0	0	0	0	0.00	0.00	0.00
16	TEST01	5	512.00	320.54	30.72	0	2	0	0	15.38	26.81	78.32
17	TEST02	5	256.00	253.68	30.72	0	3	0	0	13.12	24.79	94.65

La primera línea exhibida nos muestra: (Figura 4.2)

- El tiempo actual (6:27:47 a.m., En nuestro ejemplo)
- El tiempo desde la última que se reinicio el servidor.
- El número de entornos actualmente corriendo.
- El promedio de exceso de memoria sobre los minutos 1, 5, y 15.

La siguiente línea, PMEM, nos despliega la memoria total física. En nuestro ejemplo, el Servidor ESX tiene un 1GB (1047MB) de memoria. Veamos el significado de las siguientes prefijos-variables.

total

Hace referencia a la cantidad total de memoria en el ESX Server.

cos

Hace referencia a la cantidad de memoria asignada a la consola ESX Server.

vmk

Hace referencia a la cantidad de memoria actualmente usada por el VMkernel del ESX Server.

other

Hace referencia a la cantidad de memoria actualmente usada por todo excepto el VMkernel y la consola.

free

Hace referencia a la cantidad de memoria que está disponible en el servidor.

La herramienta de la línea de comando VMKMEM nos despliega las estadísticas de memoria que el VMkernel utiliza, incluyendo las siguientes variables:

manage

Hace referencia al total de memoria de la máquina que está siendo administrada por el VMkernel del Servidor ESX.

minfree

Hace referencia a la cantidad mínima de memoria virtual que el ESX intenta mantener libre.

rsvd

Hace referencia a la cantidad de memoria reservada por piscinas del recurso.

ursvd

Hace referencia al total de memoria de la máquina sin reserva.

state

Nos indica el estado actual de memoria de la máquina este estado tendrá uno de los 4 valores siguientes:

El estado “alto”, ocurre si, la memoria disponible es mayor o igual para 6 % del total “cos” memoria de la consola. El estado es “suave” en el 4 %, “duro” en 2 %, y “bajo” en 1 %. Entonces, el estado alto nos indica que la memoria de la máquina no está bajo ninguna presión y el punto bajo nos indica que la memoria de la máquina esta bajo presión.

El comando **COSMEM** nos muestra estadísticas de memoria que están siendo reportadas por la consola ESX Server. Todos los valores están especificados en millones de megabytes. Los valores-prefijos que se presentan aquí son:

free

Hace referencia a la cantidad de memoria sin uso que el ESX Server tiene.

swap_t

Hace referencia al espacio de intercambio total configurado en nuestro ESX Server.

swap_f

Hace referencia a la cantidad de espacio libre de intercambio que nuestro ESX Server tiene.

r/s

Hace referencia a la tasa en la cual la memoria está siendo intercambiada desde el disco.

w/s

Hace referencia a la tasa en la cual la memoria está siendo intercambiada hacia el disco.

El comando **PSHARE** nos indica el estatus de la página-intercambio actual, en las siguientes categorías. Todos los valores están especificados en millones de megabytes:

shared

Hace referencia a la cantidad de memoria física que este siendo compartida.

common

Hace referencia a la cantidad de memoria física que se comparte entres dos entornos.

saving

Hace referencia a la memoria guardada de la pagina-compartida.

El comando **SWAP** nos da información sobre el uso de intercambio en el ESX Server. Otra vez, todos los valores están en millones de megabytes:

curr

Hace referencia a la cantidad actual de memoria de intercambio que está siendo usada por el ESX Server.

target

Hace referencia a la posición del disco donde el ESX Server espera que el archivo de memoria de intercambio sea albergado.

r/s

Hace referencia a la tasa en la cual el ESX Server intercambia memoria adentro del disco.

w/s

Hace referencia a la tasa en la cual el ESX Server intercambia memoria desde fuera hacia el disco.

4.5 MONITOREANDO EL DESEMPEÑO DEL ALMACENAMIENTO.

Al usar el *esxtop*, nosotros también podemos monitorear las estadísticas del disco y localizar averías en nuestra infraestructura de almacenamiento.

Con el comando **esxtop**

Si estamos familiarizados ya, con el *esxtop* comando sobresaliente en Unix. Una vez que el *esxtop* esta ejecutándose, presionamos la tecla **d** para cambiar al modo de almacenamiento. Esto nos desplegara las estadísticas para los adaptadores SCSI del servidor, incluyendo los adaptadores del BUS (HBAs) y los hosts conectados a través de iSCSI y la fibra NAS. [1, 8,10]

Figura 4.3 Pantalla que nos muestra el almacenamiento.

```
8:53:53am up 102 days 22:19, 128 worlds; CPU load average: 0.18, 0.18, 0.18
ADAPTR CID TID LID WID NCHNS NTGTS NLUNS NVMS AQLEN LQLEN WQLEN ACTV QUED %USD
vmhba19 - - - - 1 5 5 111 64 0 0 - - -
vmhba20 - - - - 1 5 5 111 64 0 0 - - -
vmhba21 - - - - 1 1 1 10 4096 0 0 - - -
vmhba22 - - - - 1 1 1 10 4096 0 0 - - -
vmhba23 - - - - 1 2 2 8 975 0 0 - - -
```

La primera línea nos despliega la siguiente información: (*Figura 4.3*)

- El tiempo actual (8:53:53 a.m., En nuestro ejemplo)
- El tiempo desde el último reinicio de sistema.
- El número actual de entornos ejecutándose.
- La carga de la CPU promedio para el sistema

Para desplegar variables adicionales mientras se ejecuta el *esxtop*, podemos presionar la tecla **f** para ver los diferentes variable-prefijos:

ADAPTR

Nos muestra el adaptador del cual se desplegaran sus estadísticas.

AQLEN

Hace referencia a la profundidad de cola del adaptador de almacenamiento. Éste es el máximo número de comandos activos del vmkernel del ESX Server en ejecución para el cual el controlador del adaptador es configurado para soportarlos.

LQLEN

Hace referencia del número activo de comandos en ejecución para el cual el LUN tiene permitido tener.

QUED

Hace referencia a los comandos que el sistema actualmente tiene en cola. Esto se aplica solo a los entornos/LUNs.

READS /s

Hace referencia al número de comandos que son leídos por segundo. Los caminos múltiples serán mostrados de forma separada.

WRITES /s

Hace referencia al número de escrituras expedidas por segundo. Los caminos múltiples serán mostrados de forma separada.

MBREAD /s

Hace referencia al número de millones de megabytes leídos por segundo. Los caminos múltiples serán mostrados de forma separada.

MBWRN / s

Hace referencia al número de millones de megabytes escritos por segundo. Los caminos múltiples serán mostrados de forma separada.

DAVG/cmd

Hace referencia a la latencia del dispositivo por comando entre el almacenamiento y el adaptador.

KAVG/cmd

Hace referencia a la latencia del VMkernel por comando.

GAVG/cmd

Hace referencia a la latencia del guest (del huesped) en promedio del sistema operativo, por cada comando. Otras herramientas útiles para monitorear el uso del disco, como *perfmon* e *iostat*, también pueden ser ejecutadas desde la línea de comando del ESX Server. Éstas son herramientas útiles que son nativas en un entorno de Linux y estas nos pueden ayudar en la localización de averías a lo largo de la ejecución del *esxtop*.

4.6 MONITOREANDO EL USO DE LA RED (NETWORKING)

Si queremos monitorear nuestros adaptadores de red mediante la línea de comando.

Usamos la utilidad *del esxtop* para monitorear el uso de la red. [1,8]

Desde la línea de comando de nuestro ESX Server, corremos lo siguiente:

esxtop

Una vez que *el esxtop se está ejecutando*, presionamos la tecla **n** para cambiar al modo de red. Esto exhibirá las estadísticas actuales de la red del servidor. (Figura 4.4)

Figura 4.4 Pantalla que muestra la configuración de la red vía línea de comando.

```
9:25:20am up 20 days 23:58, 162 worlds; CPU load average: 0.31, 0.30, 0.26
```

PORT ID	UPLINK	USED BY	DTYP	DNAME	PKTTX/s	MbTX/s	PKTRX/s	MbRX/s	%DRPTX	%DRPRX
16777217	Y	vmnic0	H	vSwitch0	10.84	0.02	12.05	0.01	0.00	0.00
16777218	N	0:NCP	H	vSwitch0	0.00	0.00	0.00	0.00	0.00	0.00
16777219	Y	vmnic44	H	vSwitch0	0.20	0.00	1.61	0.00	0.00	0.00
16777220	N	0:CDP	H	vSwitch0	0.00	0.00	0.00	0.00	0.00	0.00
16777221	N	0:vswif0	H	vSwitch0	10.84	0.02	10.64	0.01	0.00	0.00
16777222	N	1116:VDI01	H	vSwitch0	0.20	0.00	0.00	0.00	0.00	0.00
33554433	Y	vmnic1	H	vSwitch1	0.00	0.00	0.60	0.00	0.00	0.00
33554434	N	0:NCP	H	vSwitch1	0.00	0.00	0.00	0.00	0.00	0.00
33554435	N	0:CDP	H	vSwitch1	0.00	0.00	0.00	0.00	0.00	0.00
33554436	N	0:vmk-tcpip-172.20.4	H	vSwitch1	0.00	0.00	0.00	0.00	0.00	0.00
50331649	Y	vmnic49	H	vSwitch2	0.00	0.00	0.00	0.00	0.00	0.00
50331650	N	0:NCP	H	vSwitch2	0.00	0.00	0.00	0.00	0.00	0.00
50331651	Y	vmnic45	H	vSwitch2	472.42	0.33	1171.51	11.72	0.00	0.00
50331652	N	0:CDP	H	vSwitch2	0.00	0.00	0.00	0.00	0.00	0.00

Si estamos familiarizados con este comando de Linux echemos un vistazo a los siguientes valores desplegados en la figura de arriba.

PORT ID

Hace referencia a él Id del puerto virtual del dispositivo de la red.

UPLINK

Nos indica si, si o no el puerto de la red es un enlace hacia arriba (Y = sí, N = no).

USED BY

Nos indica el usuario virtual del dispositivo de la red.

DTYP

Nos indica el tipo de dispositivo virtual de la red (H=hub, S=switch).

DNAME

Nos indica el nombre virtual del dispositivo de la red.

PKTTX /s

Nos indica el número de paquetes transmitidos por segundo.

MbTX/s

Nos indica el número de megabits transmitidos por segundo.

PKTRX /s

Nos indica el número de paquetes recibidos por segundo.

CAPITULO 5.

SEGURIDAD DE LA INFRAESTRUCTURA VIRTUAL EN GENERAL.

En este capítulo hablaremos de la seguridad de la infraestructura virtual en general, considerando que esta, no es una meta sino una búsqueda; así pues, el mejoramiento de la seguridad en nuestro entorno virtual es vital. Considerando esto, presentaremos diversas formas que nos ayudaran a mejorar la seguridad de nuestros diversos componentes en nuestro ambiente VMware ESX. [1, 3, 8,10]

5.1 CONFIGURANDO EL CONTROL DE ACCESO AL SERVIDOR VCENTER

Gran parte de la seguridad de cualquier ambiente, radica en asegurarnos que el acceso para los recursos de nuestra infraestructura virtual, este regulado correctamente. Los usuarios deben tener acceso sólo a las áreas necesarias para realizar sus trabajos y sólo deben realizar las tareas que son aplicables para eso. [1,2] Como una parte crucial de la funcionalidad a nivel de la administración general del vCenter Server, el Servidor provee un control basado en roles de acceso, (RBAC) para el entorno VMware vCenter. La Implementación del Servidor ESX RBAC, provee un fino control granular, sobre tareas específicas de los usuarios para poder echar mano de ellas después. Para poder configurar el control de acceso apropiadamente, debemos primero entender los roles que están disponibles en el vCenter Server, los que se pueden configurar, así también como los predefinidos. El vCenter Server viene con un número predefinido de roles. Estos roles proveen un punto de partida para que los clientes hagan otros roles personalizados según las necesidades del modelo administrativo de la organización. Estos son los roles predefinidos que ya vienen disponibles con el vCenter Server en el momento de la instalación:

Rol de Ningún Acceso: Este rol es obvio -- niega el acceso de cualquier objeto hacia un usuario o grupo, principalmente para que ningún usuario o grupo tengan permisos en una arquitectura de hipo-hierachi a un nivel superior a ellos, solo los permisos a su nivel. Esta configuración la podemos usar para crear excepciones en donde un usuario o grupo tienen acceso a todas las maquinas o piscinas virtuales, exceptuando solo algunas.

Rol de sólo lectura: Este rol solo permite a un usuario o grupo visualizar el inventario del vCenter Server. Por consiguiente no permite a ningún usuario o grupo interactuar con ninguna maquina virtual de ninguna forma ya sea a través del vSphere-cliente o el web-cliente y solo nos permite ver el estado de encendido del entorno.

Rol del Administrador: Cualquier usuario o grupo asignado a un objeto con el rol del administrador, tendrá todos los permisos administrativos de forma completa sobre ese objeto en el vCenter Server. Un usuario o grupo con el rol de administrador puede cambiar el hardware asignado a la máquina virtual, conectar y desconectar soporte lógico informático, iniciar y detener cualquier máquina virtual, y modificar sus parámetros de desempeño. Es importante entender que un usuario o grupo con el rol de Administrador no tiene ningún privilegio dentro del sistema operativo huésped (Guest), instalado en el interior de las maquinas virtuales.

Esos privilegios deben ser asignados desde adentro de ese invitado, mediante la instancia del sistema correspondiente.

Rol de Usuario Virtual de poder de la Máquina (Sample o plantilla) el rol de usuario de Poder de la Máquina Virtual asigna permisos que permiten configurar dispositivos de CD/DVD y floppy multimedia, cambiar el estado de encendido, tomar y borrar fotos instantáneas del desempeño (snapshots), y modificar a configuración. Estos permisos aplican solo a las maquinas virtuales. Un usuario o grupo con este rol no debe ser capaz de modificar ajustes de los objetos tales como las piscinas de recurso.

Rol de usuario virtual de la Máquina (Sample o plantilla)

Este rol concede a un usuario o grupo la capacidad de interactuar con una máquina virtual, pero no la capacidad para cambiar su configuración. Los usuarios pueden operar los controles de encendido de la maquina virtual y cambiar los medios virtuales como CD/DVD o floppy, si es que tienen acceso a estos. Los permisos del vCenter Server son granulares.

Rol de administrador de la Piscina del recurso (Sample o plantilla) sobre este rol, el administrador de la Piscina del Recurso ha sido habilitado para manejar y configurar recursos con una piscina de recursos, incluyendo máquinas virtuales, piscinas pequeñas, tareas programadas, y alarmas.

Rol del Usuario de respaldo consolidado VMware (Sample o plantilla) Como el nombre del rol lo indica, tiene los privilegios requerido para realizar un respaldo de una máquina virtual usando la herramienta (VCB).

Rol del consumidor del Datacenter (Sample o plantilla) Este rol está dirigido hacia los usuarios que necesitan sólo un permiso: El permiso para establecer el espacio de un datastore. Claramente, este un rol muy limitado.

Rol del consumidor de la red (Sample o plantilla) Parecido al rol anterior tiene sólo un permiso, y este es para asignar redes. Si los roles no se adaptan a nuestras necesidades los podemos modificar con una funcionalidad del cliente Vsphere a la cual accedamos navegando hacia la área de roles ya sea usando la barra de navegación o seleccionando Vista de administración de roles. El área de Roles exhibe todos los roles actualmente predefinidos. Haciendo un clic derecho sobre rol nos despliega comandos para clonar, editar, o quitar un rol. Existe también un botón de añadir un rol justo debajo de la barra de navegación para crear uno nuevo.

El Rol de Ningún Acceso, el rol de Sólo Lectura, y el rol Administrador predefinidos, no pueden alterarse o borrarse, para modificarlos debemos clonarlos primero y editar la copia de alguno de ellos.

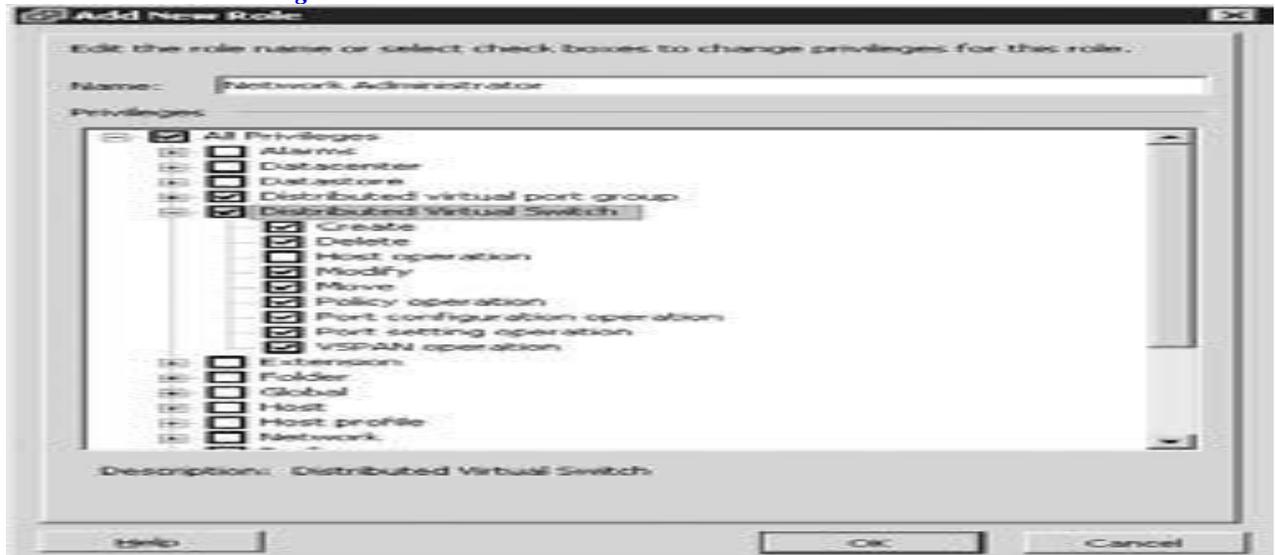
Creación de un nuevo rol.

Para crear un nuevo rol, realizamos estos pasos: (*Figura 5.1*) [6,8]

1. Nos Conectamos a una instancia del vCenter Server con el cliente de vSphere.
2. Seleccionamos la vista de administración de roles.
3. Damos un clic sobre el botón de añadir rol.
4. En la ventana de diálogo de añadir nuevo rol, especificamos un nombre para el nuevo rol.
5. De la lista de privilegios, seleccionamos los privilegios que queremos concederle a este rol.
6. Damos un clic sobre el botón Ok para guardar los ajustes y crear el nuevo rol.

Si olvidamos dar privilegios lo podemos editar.

Figura 5.1: La ventana de diálogo del rol, Add New, nos permite especificar los privilegios asignados para un nuevo rol en una base granular.



Edición de un rol

Editar un rol existente es necesario cuando nuestro rol incluye o excluye privilegios que deberían ser incluidos o no. [6,8] Para editar un rol, realizamos estos pasos:

1. Nos Conectamos a una instancia del vCenter Server con vSphere Client.
2. Seleccionamos LA vista de la administración de roles.
3. Damos un clic derecho sobre el rol que queremos editar y seleccionamos Edición del rol.
4. En la ventana de diálogo de edición del rol, especificamos un nombre nuevo para el rol (si así lo deseáramos) y añadimos o removemos privilegios de la lista de privilegios.
5. Damos un clic sobre el botón Ok para guardar los cambios y regresamos al cliente de vSphere.

Clonar un rol.

Para hacer una copia clónica de un rol existente, realizamos estos pasos:

1. Nos conectamos a una instancia del vCenter Server con el cliente del vSphere.
2. Seleccionamos vista de la administración de roles.
3. Damos un clic derecho sobre el rol que queremos clonar y seleccionamos Clonar.
4. Un nuevo rol aparece en la lista de roles. Escribimos un nombre para el nuevo rol, y luego presionamos a tecla Enter. [6,8]

5.2 ADMINISTRACIÓN DE PERMISOS

Después de que hemos creado los roles necesarios, debemos combinar esos roles con un usuario o grupo para crear un *permiso*. Luego asignamos el permiso a un objeto para ponerlo en marcha. [6, 8,10] Podemos asignar permisos desde cualquier vista de inventario: es decir, desde los anfitriones. Y los Grupos (clústeres), VMs Y Plantillas, Datastores, y el Sistema de Redes. En todas las diferentes vistas, el proceso es el mismo.

Para asignarle un permiso a un objeto, realizamos estos pasos:

1. Estando conectados a una instancia del vCenter Server, navegamos en el cliente vSphere sobre la vista de inventario para el tipo de objeto en el cual Queremos asignar el permiso. Por ejemplo, si queremos asignar un permiso sobre un anfitrión específico del ESX/ESXi, navegamos hacia las vistas de hosts y clústeres.
2. Seleccionamos el objeto sobre el cual el permiso deberá ser asignado.
3. Seleccionamos la pestaña de permisos del panel de contenido que está a la derecha.
4. Damos un clic derecho en un área en blanco de la pestaña de Permisos y seleccionamos agregar permiso. Esto abre la ventana de diálogo de asignación de Permisos.
5. Debajo de Usuarios Y Grupos, seleccionamos el botón Añadir.
6. Seleccionamos los grupos o usuarios específicos para incluirlos en el rol. Cuando veamos que se agregaron todos los usuarios y los grupos, damos un clic sobre el botón Ok.
7. En la sección asignación del rol, seleccionamos el rol que queremos asignar para los grupos y usuarios seleccionados.
8. Si queremos que el permiso se aplique a los objetos hijos, seleccionamos la casilla dejar heredarse a los objetos hijos.
9. Si necesitamos agregar a más usuarios o grupos con otros roles, repetimos los pasos desde el 5 hasta el 8.
10. Cuando hemos acabado de asignar roles a los usuarios y grupos, damos un clic sobre el botón Ok para regresar al cliente vSphere. Los permisos aparecerán en la pestaña de Permisos sobre el objeto seleccionado. Si necesitamos quitar un permiso, simplemente damos un clic derecho sobre el permiso y le damos borrar. Para cambiar el rol asignado sobre el permiso, damos un clic derecho sobre el permiso y seleccionamos propiedades.

5.3 FORTALECIENDO LA SEGURIDAD DEL VCENTER EN LA COMPUTADORA SERVIDOR.

Mencionaremos algunas directivas generales para fortalecer y endurecer la seguridad de nuestro entorno virtual.

- Tenemos que asegurarnos conservar la computadora del vCenter Server con los parches correctamente instalados y las actualizaciones más recientes.
- La publicación de la documentación de las mejores prácticas para las bases de datos es de vital importancia nos ayudara a resolver problemas de una manera eficaz.
- Tenemos que asegurarnos de endurecer la seguridad no sólo de la computadora del vCenter Server, sino también el sistema de la computadora que tiene corriendo la base de datos del vCenter Server. **[1,6,8,10]**
- Debemos proceder a endurecer la seguridad de acuerdo con las políticas y normas de la compañía, esto es instalar y configurar correctamente nuestros agentes de antivirus, sistemas de detección de intrusión, y cualquier otro software de seguridad requerido.
- Si estamos usando autenticación de Windows con un Servidor SQL, usemos una cuenta de servicio dedicada para el Servidor vCenter. No debemos compartirla con otros servicios o aplicaciones.
- Tenemos que reemplazar los certificados predeterminados que se firman solos SSL, con certificados válidos SSL, desde una autoridad fiable de raíz.
- Restrinjamos el acceso físico a la computadora del vCenter Server a personal autorizado solamente.

Remoción del acceso administrativo por defecto del Servidor vCenter.

Por defecto, cuando el vCenter Server es instalado, el grupo de Administradores locales en la computadora del servidor del vCenter, le es concedido el rol con todos los privilegios sobre el objeto del datacenter dentro del Servidor vCenter. Este acceso administrativo predeterminado expone al servidor del vCenter Server a personal que no tiene que tener acceso dentro del entorno VMware vSphere. Para remover el acceso administrativo predeterminado en el Servidor vCenter, sigamos los siguientes pasos.

1. En la computadora del vCenter Server, use la consola de administración de la computadora para crear un grupo local nuevo. Al cual podemos llamar administradores del vCenter o algo semejante.
2. Creamos un usuario nuevo y lo colocamos en el grupo recién creado, hay que asegurarnos de no colocar este usuario en el grupo local de Administradores.
3. Nos logueamos en el sistema de la computadora del vCenter Server usando una cuenta con permisos administrativos.
4. Ejecutamos el cliente del vSphere y nos conectamos a una instancia del Servidor del vCenter.
5. Asignamos el rol de Administrador al nuevo grupo creado en el paso 1 al objeto del Servidor del vCenter en la cúspide de la jerarquía. Tenemos que asegurarnos de dejar seleccionada la casilla de propagación de herencia al objeto hijo.
6. Nos salimos del sistema y nos logueamos de nuevo sobre el usuario que creamos en el paso 2.
7. Nos logueamos en el servidor del vCenter Server usando el cliente vSphere y nos aseguramos de que somos capaces de desempeñar todas las tareas disponibles asignadas para el administrador del Servidor vCenter.
8. Removemos el permiso sobre el objeto del Servidor del vCenter para el grupo local de los administradores.
9. Si estamos usando el Directorio Activo, creamos un grupo en el Directorio activo y lo agregamos al grupo local que se creó en el paso 1. Agregamos el dominio de usuarios al dominio de grupo si es necesario. Después de hacer este proceso, sólo los usuarios que son miembros del grupo local (o el grupo Activo de dominio del Directorio, donde aplique) tendrán permisos administrativos dentro del servidor vCenter.

5.4 SEGURIDAD EN LA RED DE CONTROL DE ACCESO A LA CONSOLA DE SERVICIO.

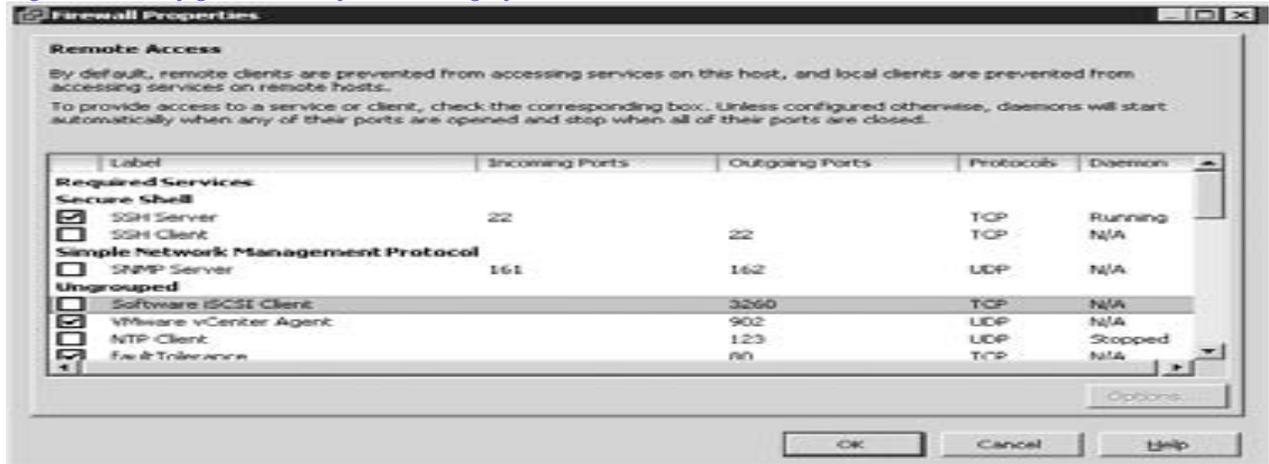
Para ayudar a controlar el acceso a la red por medio de la consola de servicio del ESX, la compañía de VMware suministra un firewall para dicha Consola, y un comando para configurar el firewall. Lo podemos configurar a través del cliente del Vsphere o usando la línea de comando. Si decidimos hacerlo mediante la línea de comando, usamos el siguiente **esxcfg-firewall**

El cual nos habilita o deshabilita servicios del network a través del firewall de la consola de servicio. Este comando aplica solo para las plataformas VMware ESX. Para configurar el firewall de la consola de Servicio mediante el cliente del vSphere, realizamos los siguientes pasos:

1. Nos conectamos a una instancia del servidor vCenter usando el cliente vSphere. Si existen muchas instancias del servidor vCenter Server en nuestro ambiente virtual, nos aseguramos de conectarnos en la instancia que manipula el Host que deseamos configurar.

2. Navegamos a través de la vista de inventario de los Hosts y clústeres usando la vista del menú, la barra de navegación, o el atajo de combinación de teclas Ctrl +Shift +H.
3. Seleccionamos un host ESX del inventario a la izquierda.
4. Seleccionamos la pestaña de Configuración del panel de contenido que está en la derecha.
5. Seleccionamos el enlace del Perfil de Seguridad que está situado debajo de Software.
6. Las conexiones entrantes y salientes permitidas actuales a través de la regulación del firewall se encuentran en una lista en el panel de contenido. Si necesitamos hacer modificaciones, damos un clic en el enlace de Propiedades.
7. En la ventana de diálogo de propiedades del Firewall, seleccionamos o deseccionamos los servicios de quién se nos ha indicado modificar. [1, 2,4, 8,10]

Figura 5.2 Configuración del firewall vía gráfica.



8. Damos un clic sobre Ok para regresar al cliente de vSphere.

5.5 AUTENTICACIÓN MEDIANTE EL SERVICIO DEL DIRECTORIO ACTIVO

Para configurar el ESX y usar el servicio del directorio para la autenticación, usaremos el comando **esxcfg-auth**. Tenemos que usar el comando **esxcfg-auth** para configurar el VMware ESX y autenticar contra un dominio de Directorio Activo, realizando estos pasos:

1. Echamos mano de una tecnología remota de consola como HP iLO o del uso de la consola física, para loguearnos dentro del Host del ESX y introducimos el comando **su-** para establecer privilegios de la raíz. Porque en realidad estamos modificando los comportamientos de la autenticación, no es recomendable a usar una conexión remota como SSH para esta tarea.
2. Introducimos el siguiente comando para habilitar la autenticación del Directorio activo **esxcfg-auth --enabled --addomain <nombre del dominio> --addc <nombre del dominio>**
3. Creamos cuentas locales para el ESX con nombres de usuario que coincidan con las cuentas del directorio activo que les será permitido el acceso dentro del Host ESX. [1,10] No hay necesidad de colocar una contraseña en la cuenta local.
4. Mientras estemos logueados en el sistema como raíz, comprobamos la facultad de loguearnos dentro del host ESX, con una cuenta del Directorio Activo usando la

autenticación SSH. Cuando se nos indique introducir la contraseña, especificamos aquella que esta almacenada en el Directorio Activo.

5. Si el acceso al sistema falla, revisamos el archivo log, situado en esta ruta `/var/log/secure` para la identificación de cualquier posible error. Sí no falla, y nos logueamos con éxito, habremos completado la configuración.

5.6 IMPLEMENTACIÓN DE UNA POLÍTICA DE CONTRASEÑA PARA CUENTAS LOCALES.

Para configurar la política de contraseña en un Host del VMware ESX, sigamos los siguientes pasos:

1. Usando la herramienta PuTTY.exe (sobre Windows), una consola terminal (sobre Linux o Mac OS X), una tecnología remota de consola como HP iLO, o una consola física, nos logueamos dentro del host ESX e introducimos el comando `su-` para establecer los privilegios totales de la cuenta raíz (root).

2. Usamos el comando `esxcfg-auth` para establecer la edad máxima de la contraseña en nuestro ejemplo será por 90 días:

`esxcfg-auth - passmaxdays = 90`

3. Colocamos el número de días, y una advertencia nos estará indicando con antelación de 14 días que la contraseña caducara:

`esxcfg-auth - passwarnage = 14`

Podemos ver los ajustes actuales de la política de la contraseña, al ejecutar el siguiente comando **`esxcfg-auth -probe`** desde la Consola de Servicio. Esto exhibirá los ajustes actuales en una pantalla. Necesitaremos repetir estos comandos en cada anfitrión HOST ESX dónde estos ajustes deben ser aplicados. [1,10]

Desactivando las acciones de Copiar y Pegar.

Por defecto, la consola remota del cliente de vSphere, provee la funcionalidad del uso de las acciones **copiar y pegar**, que mueven los datos y de una máquina virtual hacia una estación de trabajo local. Para impedir esta función, desactivamos estas acciones al añadir las siguientes líneas a los archivo de configuración las máquinas virtuales que deseemos afectar:

`isolation.tools.copy.disable "true"`

`isolation.tools.paste.disable "true"`

Deshabilitar dispositivos innecesarios

Si queremos prevenir que cualquier usuario o proceso dentro de una máquina virtual tenga el poder de conectar o desconectar dispositivos tales como el disco flexible floppy, una unidad de CD/DVD, o un adaptador de red. Tenemos que añadir este parámetro de configuración al archivo de configuración de la máquina virtual:

< El nombre del dispositivo > `.allowGuestConnectionControl "false"`

Debemos reemplazar aquí *< el nombre del dispositivo >* con el nombre del dispositivo real, como `ethernet0` o `floppy0`. Haciendo esta modificación nos aseguramos de que sólo los usuarios que han sido facultados con privilegios accedan dentro del Servidor vCenter y por ende puedan conectar o desconectar dispositivos como la unidad de disquete, unidad de CD/DVD, o un adaptador de red.

5.7 RESPALDOS EN EL AMBIENTE VIRTUAL.

-----EL RESPALDO CONSOLIDADO VIRTUAL.

En nuestro entorno virtual contamos con muchas técnicas para respaldo, tales como. La cinta como respaldo, el disco-a-disco-a-casete, la replicación, por mencionar las más comunes. [1, 8,10]

En esta investigación, nos enfocaremos al nuevo producto de la compañía VMware para realizar respaldos, la herramienta conocida como **Respaldo Consolidado Virtual**.

El VMware Respaldo Consolidado (**VCB** por sus siglas en Inglés **Vmware Consolidated Backup**), es una aplicación basada en una interfaz de ventanas, que provee una alternativa de respaldo centralizada para hacer copia de reserva de máquinas virtuales a través de un servidor proxy, sin afectar las características esenciales de la máquina virtual. Fue diseñada específicamente para que los ambientes virtuales minimicen el impacto sobre el servidor del host durante operaciones de respaldo. VCB es una tecnología de disponibilidad y no puede hacer copias de reserva de máquinas virtuales, por sí misma, pero en lugar de eso, se auxilia con una herramienta de otra compañía de respaldos que le ayuda hacer los respaldos desde los hosts de los servidores. Trabaja tomando una foto (Snapshot) de la máquina virtual, lo cual suspende la escritura en el disco original, y luego copia el disco original en un servidor proxy, donde el disco de la máquina virtual es montado en el servidor proxy de respaldo. Luego respalda el contenido de la máquina virtual como una imagen virtual del disco o como un conjunto de archivos y directorios, y luego desmonta el disco virtual y elimina la foto. Este respaldo es realizado sobre la tecnología SAN y no sobre la red, lo que da como resultado mayor velocidad en los procesos de respaldo.

Las ventajas de usar a VCB

- Elimina la necesidad de instalar un agente del respaldo del software en cada máquina virtual que se quiera respaldar.
- La nueva versión ahora soporta los respaldos de las máquinas virtuales sobre SAN, iSCSI, NFS, y el disco local.
- Esta tecnología es soportada y compatible con el software más común de respaldo, incluyendo a Symantec NetBackup y Backup Exec, CA Arcserve, CommVault Simpana, HP Data Protector, e IBM Tivoli Storage Manager.
- Soporta ambos niveles de almacenamiento, el completo y el parcial, sobre Máquinas virtuales corriendo sobre Windows y los respaldos de imágenes para máquinas virtuales corriendo sobre cualquier sistema operativo (Windows y/o Linux).
- Se integra con VSS para proveer consistencia a nivel aplicación sobre aplicaciones VSS.

Las desventajas de usar a VCB

- Es una tecnología costosa, requiere de un servidor físico aparte y una tarjeta del Canal de Fibra, para respaldar las Máquinas virtuales sobre SAN.
- El soporte está limitado a sistemas operativos como Windows y Linux.
- Puede requerir de espacio adicional excesivo sobre SAN, para hacer respaldo de Máquinas virtuales.

- El archivo individual de restauración requiere más pasos y es más complicado de usar.
- Puede ser muy complicada para instalarse, configurarse, y para su mantenimiento.

El respaldo consolidado es una gran solución para remover la carga de respaldo de nuestros anfitriones (Hosts), y es más conveniente para ambientes muy grandes. Su funcionamiento a grandes rasgos es el siguiente:

1. El respectivo software de respaldo inicia el trabajo de respaldo sobre una máquina virtual.
2. El script de pre-respaldo empieza a ejecutarse.
3. El respaldo Consolidado virtual corre un comando de VMsnap y VCB Mounter.
4. El sistema de archivo de la maquina virtual se desactiva y entonces es congelado por unos instantes
5. Una foto se toma.
6. La máquina se descongela para que pueda aplicársele los cambios, los cuáles son rastreados y guardados en un archivo diferencial.
7. Una lista del bloque se crea. La lista es simplemente un apuntador hacia los bloques de información que crean el archivo VMDK, que es el archivo que contiene la información base de la maquina.
8. El nivel de bloque de información de la máquina virtual es copiado en el respaldo del proxy sobre el SAN. La información aparece como archivos sobre el respaldo del proxy.
9. El archivo delta se aplica a la máquina virtual cuando la foto es removida.
10. El script de pre-respaldo termina y el control de la ejecución es devuelto al software de respaldo.
11. La información virtual de la máquina es copiada desde el punto de montaje para grabarse en la cinta.
12. El respaldo se verifica (esto es optativo, pero es ampliamente recomendado).
13. El script de post-respaldo empieza a ejecutarse.
14. Los archivos de la foto son eliminados del punto de montaje para dejarlo limpio.
15. El trabajo de respaldo ha sido completado.

Figura 5.3 Relación de la configuración de red en el respaldo.

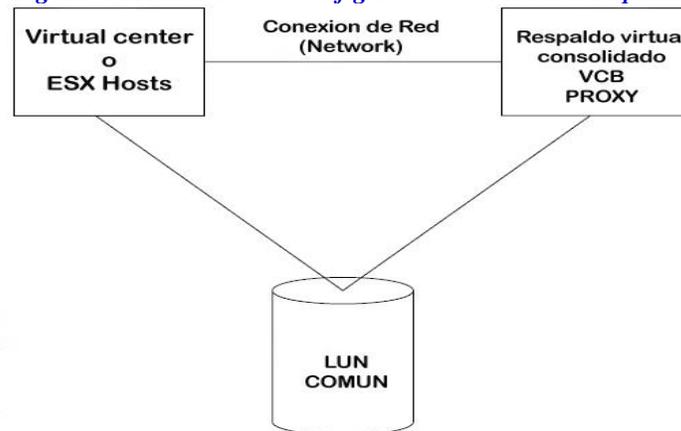


Tabla 5.1 Comparación entre las herramientas de respaldo.

Tipo de Respaldo	Min OTR*	Min OPR**	Costo	Complejidad
MV Respaldo caliente	< una hora	24 horas	Bajo	Baja
Respaldo agente de Cinta	1-24 horas	24 horas	Mediano	Media
Replicación por Almacenamiento	<cinco minutos	Tiempo Real	Alto	Alta

*El objetivo mínimo de tiempo de recuperación es un estimado basado sobre la experiencia del tiempo típico requerido de una recuperación de información usando una herramienta específica. Dependiendo de la cantidad de información que será respaldada y recuperada.

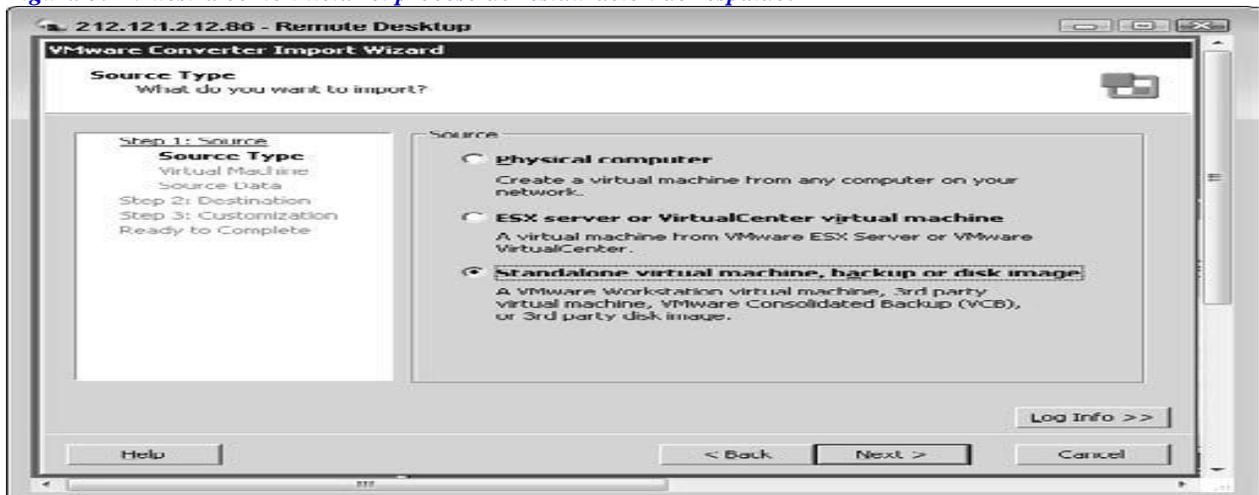
**El mínimo OPR se basa en la frecuencia en la que se realizan los respaldos. Es decir, respaldos diarios proveen un <OPR de 24 horas, mientras que respaldos semanales proveen un < siete días OPR.

5.8 RESTAURACIÓN DE RESPALDOS.

La Restauración de respaldos es sumamente fácil, ya sea que tengamos que restaurar una imagen o simplemente un solo archivo. Para restaurar una máquina virtual entera desde una imagen, seguimos estos pasos:

1. Restauramos los archivos más recientes de respaldo basado en imágenes hacia nuestro punto de montaje. [1, 9,10]
2. Ejecutamos la aplicación del VMware Converter.
3. Hacemos uso del VMware Converter seleccionando la opción de Máquina Virtual Standalone, después seleccionamos respaldo, o imagen de Disco como nuestra opción de origen para empezarla a restaurar. (Figura 5.4). Si solo necesitáramos de un sólo archivo o dos, solo restauramos aquellos archivos en El servidor de respaldo Proxy y los copiamos a nuestra Máquina Virtual a través de la red. De manera opcional, si tenemos agentes de respaldo instalados en la máquina virtual, podemos restaurar el archivo directamente en esta. La Infraestructura VCB Framework, nos ofrece algunas nuevas herramientas para ser añadidas a nuestro set de herramientas de respaldo. Dependiendo de nuestra situación en particular, podríamos solo utilizar el VCB, usándolo solo para respaldar por medio de la red a través de los agentes de respaldo o el uso combinado de los dos métodos. Algunas veces los agentes los podemos elegir como una opción de software de respaldo a la carta, básicamente depende de nuestro número de servidores el uso de las alternativas de respaldo, para evitar comprar agentes de otras compañías que no necesitemos.

Figura 5.4 Muestra como iniciar el proceso de restauración de respaldo.



CONCLUSIONES:

La investigación nos permitió presentar una guía concisa y detallada, de la tecnología de Virtualización de Servidores ESX, describiendo sus requerimientos físicos de hardware, importancia, su origen, evolución, implementación, mantenimiento, monitoreo y auditoración en el ámbito de seguridad y alcance de desempeño del software VMware ESX.

Esta amplia referencia nos permitió conocer de una manera clara, como se trabaja con las diferentes versiones de dicha tecnología, cuáles son sus ventajas, desventajas, a la vez de sus mejoras en las versiones más recientes, y nos permite vislumbrar lo que sus sucesores (versiones posteriores) serán en un futuro no muy lejano.

En mi opinión esta es la tecnología líder en el ramo de virtualización, ya que se ha preocupado por la estabilidad, la adaptabilidad, seguridad, consistencia, robustez y facilidad de uso en muchos de sus componentes de la suite ESX. Como se ha mostrado en cuanto a los requisitos mínimos de memoria y CPU, el sistema de ESX tiene la característica de auto administrar y usar de una manera muy eficiente nuestros recursos físicos, le saca el mayor provecho, lo cual se traduce en un performance impecable y puntual.

En sus versiones más recientes sus interfaces gráficas cada vez más amigables y fáciles de operar, nos van llevando por procesos que son más complicados de lo que parecen pero por su exquisitez gráfica, tenemos la cobertura de una guía precisa al instalar y configurar muchos de los componentes de la Suite.

En mundo totalmente inclinado hacia el campo de la informática, soluciones poderosas como esta, permiten llevar a productos de tanta calidad como este, al siguiente nivel en la escala evolutiva del desarrollo tecnológico mundial en el campo de IT.

Referencias web

w1. <http://www.vmware.com/>

<http://www.vmware.com/resources/compatibility/search.php?action=base&deviceCategory=server>

W2 <http://www.vmware.com/download/vi/>.

W3. <http://infodocs.net/articulo/san/diferencias-entre-san-y-nas>

W4 <Http://vmware.com/download/converter>

BIBLIOGRAFÍA:

1. Troy, Ryan, Helmke, Mathew. **VMWARE Cookbook**, Edit. O'REALLY Media Inc., U.S.A., 2010, 281 págs.
2. Marshall, David. **VMWARE ESX, Essentials in the Virtual Data Center**, Edit. CRC Press Publishing Inc., U.S.A., 2009, 237 págs.
3. Siebert, Eric, **VMWARE VI3 Implementation and administration**, Edit. Prentice Hall (Pearson Education Inc), U.S.A., 2009, 495 págs.
4. Jin, Steve, **VMWARE VI and vSphere SDK, Managing the VMware Infraestructure and vSphere**, Edit. Prentice Hall, U.S.A., 2008, 620 págs.
5. Rule Jr., David, **How to cheat at configuring VMWARE ESX**, Edit. Syngress Publishing, U.S.A., 2007, 372 págs.
6. McCain, Chris, Rivera, Rawlison, **Mastering VMWARE Infraestructure 3**, Edit. Wiley Publishing Inc. (Sybex), U.S.A., 2008, 554 págs.
7. Haletky, Edward L., **VMWARE ESX SERVER In The Enterprise (Designing and Securing Virtualization Servers)**, Edit. Prentice Hall (Pearson Education Inc.), U.S.A., 2008, 551 págs.
8. Lowe, William J., **VMWARE Infraestructure 3 for Dummies**, Edit. Wiley Publishing Inc., U.S.A., 2008. 335 págs.
9. Dittner, Rogier, Rule Jr., David, **The Best Damn Server Virtualization book period**, Edit. Syngress Publishing Inc., U.S.A., 2007, 931 págs.
10. Lowe, Scott, **Mastering VMware Vsphere 4**, Edit. Wiley Publishing Inc. (Sybex), U.S.A., 2010. 673 págs.