

USERS

Técnico en

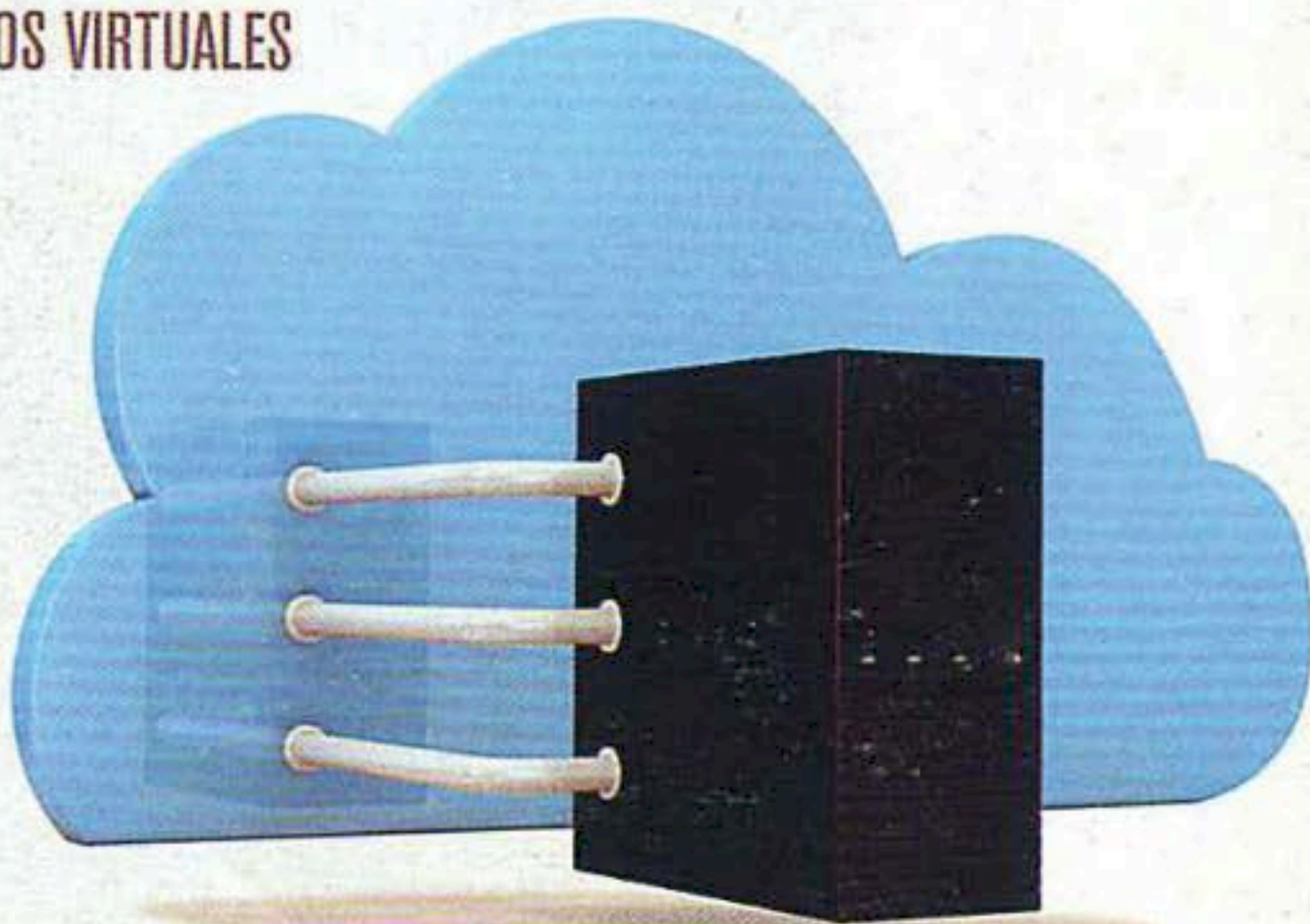
REDES & SEGURIDAD

4

VIRTUALIZACIÓN

EXPLORE LOS ASPECTOS INDISPENSABLES PARA
APROVECHAR AL MÁXIMO ESTA NUEVA TENDENCIA

- ▶ ANÁLISIS DE ALTERNATIVAS DISPONIBLES
- ▶ DISTINTAS TECNOLOGÍAS
- ▶ SERVIDORES Y ESCRITORIOS VIRTUALES
- ▶ HERRAMIENTAS VMWARE



USERS

Técnico en
REDES
& SEGURIDAD

4

VIRTUALIZACIÓN



SOLO VÁLIDO PARA LA REPÚBLICA ARGENTINA

SUSCRÍBASE ANTES
Y GANE HASTA \$105*

+54 (011) 4110 - 8700
usershop.redusers.com

(EXCLUSIVO SUSCRIPTORES / NO SUSCRIPTORES HASTA \$80*) * AL SUSCRIBIRSE AL CURSO COMPLETO,
GANA AUTOMÁTICAMENTE UNA ORDEN DE COMPRA PARA ADQUIRIR NUESTROS PRODUCTOS.



TÍTULO: Virtualización

COLECCIÓN: Pocket Users

FORMATO: 13.5 x 19 cm

PÁGINAS: 96

Copyright © Fox Andina en coedición con Dálaga S.A. MMXIII.

Hecho el depósito que marca la ley. Reservados todos los derechos de autor.

Prohibida la reproducción total o parcial de esta publicación por cualquier medio o procedimiento y con cualquier destino.

Primera impresión realizada en enero de MMXIII.

Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. De Buenos Aires.

Todas las marcas mencionadas en este libro son propiedad exclusiva de sus respectivos dueños.

ISBN 978-987-1857-79-1

Virtualización / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013.

96 p.; 19 x14 cm. - (Pocket users; 29)

ISBN 978-987-1857-79-1

1. Informática. I. Budris, Paula, coord.

CDD 004

Prólogo **al contenido**

Muchas empresas crecen poco a poco y, generalmente, comienzan a medir sus ganancias según la cantidad de productos que pueden fabricar en comparación con los empleados que tienen. Al contratar a alguien nuevo, se supone que pueden producir más, pero llega un momento en que esta comparación deja de tener sentido. Al crecer, dejamos de fabricar tanto y nos cuesta más capital de trabajo. Es entonces cuando comenzamos a necesitar abogados, contadores y sistemas, pues estamos creciendo en infraestructura empresarial. La buena implementación de los sistemas que mantienen esta infraestructura puede llegar a ahorrarnos grandes cantidades de dinero. Hoy en día, los sistemas son indispensables para continuar creciendo. Existen sistemas en los supermercados, los bancos, las automotrices, las petroleras, en todos los negocios. No podemos escapar de ellos.

Este libro está dedicado a enseñar una tecnología que revolucionó la forma de trabajar en varias compañías: la virtualización con VMware. La buena implementación de estas herramientas se va a volver indispensable en algunos años más, y esta obra nos ayudará en ese sentido, porque nos enseña cómo maximizar los recursos y evitar los riesgos de continuidad del negocio.

Enzo Augusto Marchionni
Octavio Formoso

Contenido del libro

CAPÍTULO 1

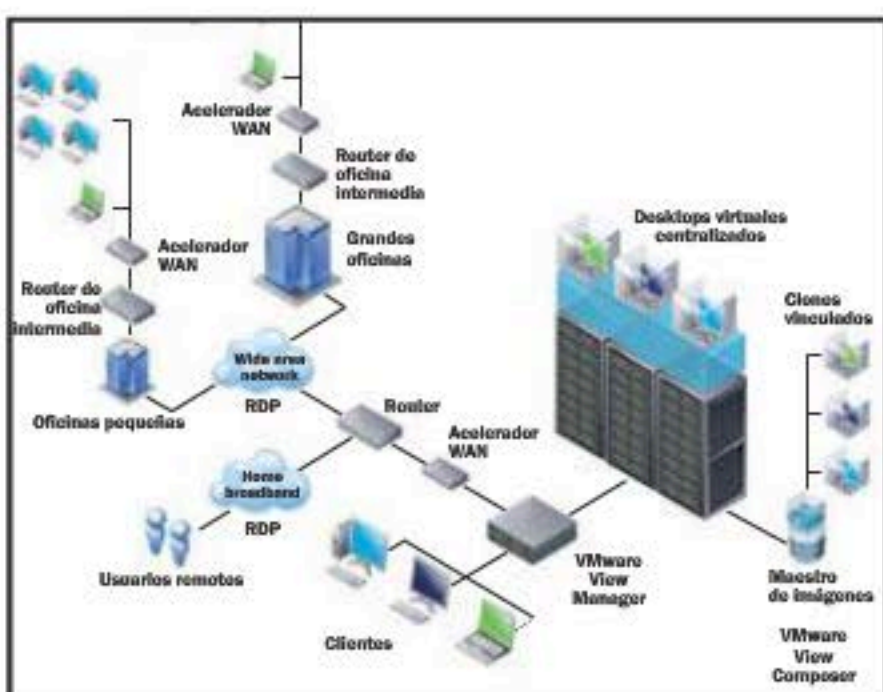
INTRODUCCIÓN A LA VIRTUALIZACIÓN DE SERVIDORES

Conceptos básicos	8
Qué es la virtualización	8
Historia de la virtualización	12
Los inicios: System/360	13
1998: v irtualización de sistemas de cómputo	13
Arquitecturas x86	14
2006: infraestructura virtual	15
El presente	17

CAPÍTULO 2

SOLUCIONES DE VIRTUALIZACIÓN EN EL MERCADO

Diferentes tecnologías	20
Cómo virtualizar un servidor	23



Descripción del procedimiento	25
-------------------------------	----

Migración de un servidor físico a uno virtual	27
---	----

Virtualización de servidores y escritorios	29
---	----

Infraestructura virtual	31
View Connection Server	33
Dispositivos	34

CAPÍTULO 3

VMWARE COMO
HERRAMIENTA
DE VIRTUALIZACIÓN 35

Por qué utilizar VMware	36
El futuro cercano	36
Infraestructura de VMware	37
VMware Workstation y VMware Player	37
ESXi	38
Más herramientas	38



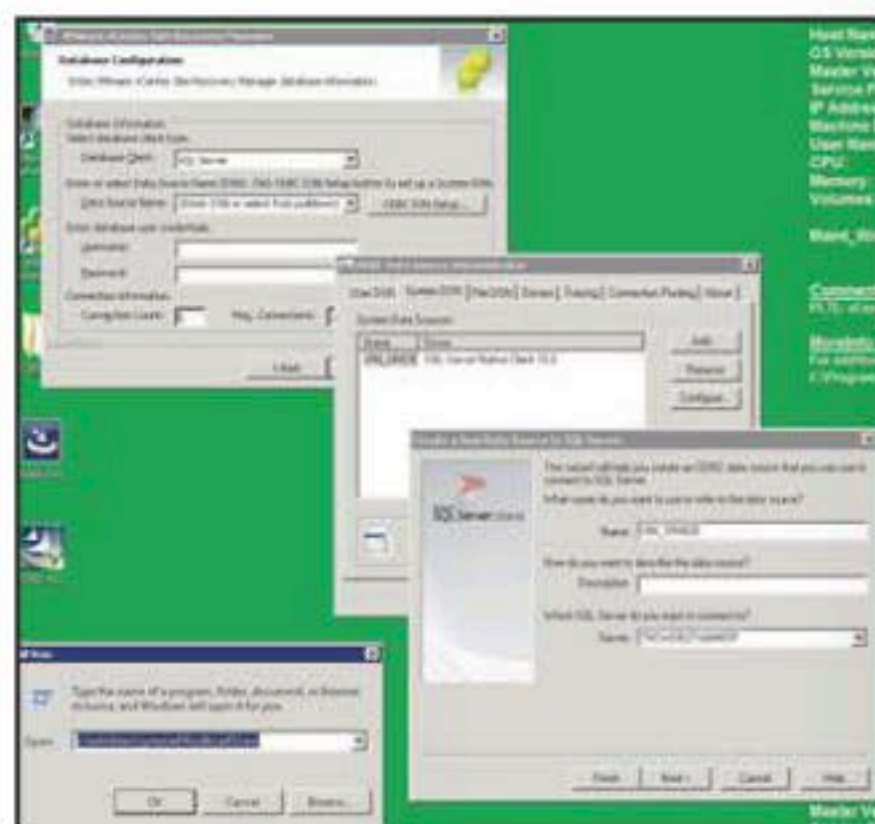
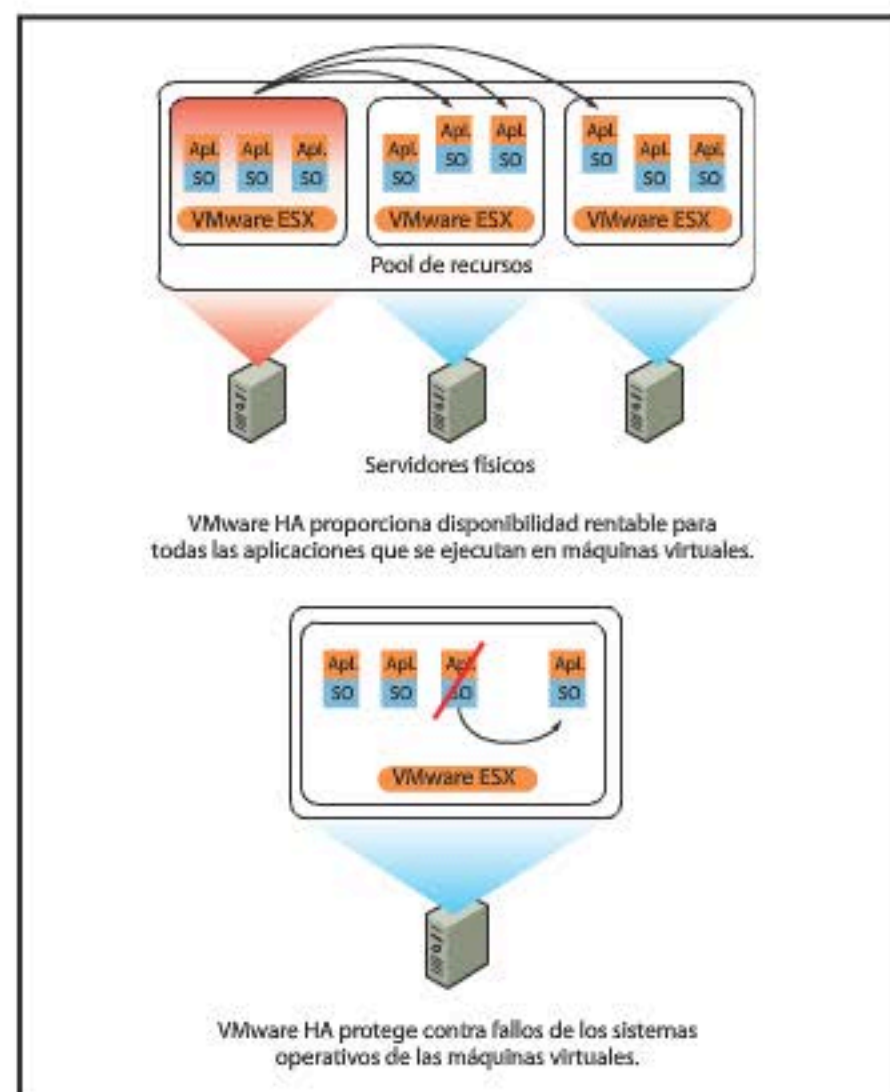
Cómo instalar un ESXi	40
Crear una máquina virtual	43
Consola gráfica de administración ESXi	47
VMware vCenter	48
Descripción y características	48
Detalles de la implementación	49
Particularidades del storage compartido	50
Cómo hacer un cluster	50
Cómo agregar nodos ESXi	54
HA, DRS, VMotion y Storage VMotion	56
VMotion	57
Storage VMotion	59
HA	61
DRS	63
Fault Tolerance	64
Snapshot	68

CAPÍTULO 4

HERRAMIENTAS PARA LA

PLATAFORMA VMWARE 69

VMware vCenter Operations	70
Interfaz	70
Distintas licencias y posibilidades	73
Instalación	74
Pasos por seguir en la instalación	74
vCenter Infrastructure Navigator	79
VMware Chargeback Manager	79
VMware Configuration Manager	79
Site Recovery Manager	80
Requisitos mínimos para la instalación	81
Instalación de storage y ODBC	82
Instalación de SRM	86
Configuración del sistema	88



Capítulo 1

Introducción a la virtualización de servidores

Veremos el concepto de virtualización,
analizaremos su historia y su evolución.

Conceptos básicos

Antes de comenzar con la administración de la virtualización de servidores, debemos saber qué es lo que estamos administrando, y conocer sus conceptos arquitectónicos y tecnológicos. Más adelante, esto nos permitirá entender la historia y la evolución de la virtualización. Con este objetivo, definiremos qué es una máquina virtual, y sus distintos componentes. También, detallaremos las posibilidades que tenemos al manejar estas tecnologías en lugar de utilizar servidores físicos.

QUÉ ES LA VIRTUALIZACIÓN

Con seguridad, conocemos más de una definición de **virtualización**, pero, para simplificar y acotar este concepto, diremos que es una técnica avanzada que permite compartir el hardware de la mejor manera posible, ahorrando dinero y maximizando los recursos económicos y administrativos que giran alrededor de la administración de servidores. Además, podríamos decir que es la forma de reaprovechar los recursos físicos de una computadora; donde ayer funcionaba solamente una, hoy funcionan dos, tres o más. Estas computadoras, en la actualidad, son llamadas **máquinas virtuales**.

Una máquina virtual es un concepto lógico de todos los componentes de un servidor físico. Cada componente físico de un servidor contiene un programa que realiza determinada tarea; así, por ejemplo, la placa de video tiene su programación a bajo nivel para manejar gráficos, y lo

mismo sucede con cada uno de los componentes que agreguemos como puertos. Todos estos programas a bajo nivel fueron llevados a la capa de aplicaciones. Se emularon los componentes tomando solo sus programas, a tal extremo que hoy Cisco tiene en el mercado switches virtuales que contienen la misma programación que sus switches físicos, pero es tan solo un programa. Entonces, si unimos cada uno de estos programas, obtenemos una máquina virtual, es decir, una emulación de un servidor físico, que es un programa de computación a otro nivel. Si bien este concepto de **emulación** puede parecer poco significativo y dar a entender que una máquina virtual tiene menos potencia que sus iguales físicos, esto no es así. En la actualidad, los servidores virtuales son tan potentes como los físicos, o más. Obviamente, existe una limitación relacionada con las capacidades del servidor físico que contiene estos sistemas, pero, si contamos con hardware nuevo (que posee capacidades mucho mayores que las encontradas en años anteriores) y colocamos un sistema para virtualizar servidores de años y años de existencia, resulta sencillo entender que son mucho más potentes que sus similares físicos.

La virtualización permite migrar sistemas de antaño a hardware nuevo. Es decir, los servidores virtuales pasan a ser objetos que se van moviendo de un lugar a otro, independizados de su hardware. Hoy podrían estar en un servidor físico, y mañana en otro. La virtualización nació con el objetivo de economizar recursos. Por ejemplo, el uso de un determinado servidor físico a lo largo del mes puede ser muy bajo, nunca llega al

100%. En el caso de la CPU, su uso durante algunos días del mes, en promedio, es del 10% y, por el contrario, a fin de mes, cuando debemos hacer un cierre de la facturación, puede llegar al 100%, o en ciertos meses, al 130%. Si bien el hardware es necesario, nunca se aprovecha su poder de cálculo como se debiera. La virtualización de servidores viene a dar una solución en estas situaciones, brinda ahorro, agilidad en la administración y aprovechamiento del hardware al máximo.

Hypervisores

La virtualización se da gracias a una nueva gama de sistemas operativos llamados **hypervisores**,

que se instalan en los servidores físicos como una capa de abstracción, es decir, una interfaz entre el hardware y los sistemas operativos virtualizados. Estos sistemas operativos físicos están preparados para administrar los recursos entre varias máquinas virtuales utilizando distintas reglas que dependerán de cada tecnología. Comparten el uso de los recursos para ofrecer un poco a cada máquina virtual, pero siguen teniendo un mismo espacio total de disco, las mismas placas de red, el mismo tamaño de memoria RAM y la misma cantidad de CPU. Es decir, cada máquina virtual cuenta con una porción de estos componentes del servidor físico.

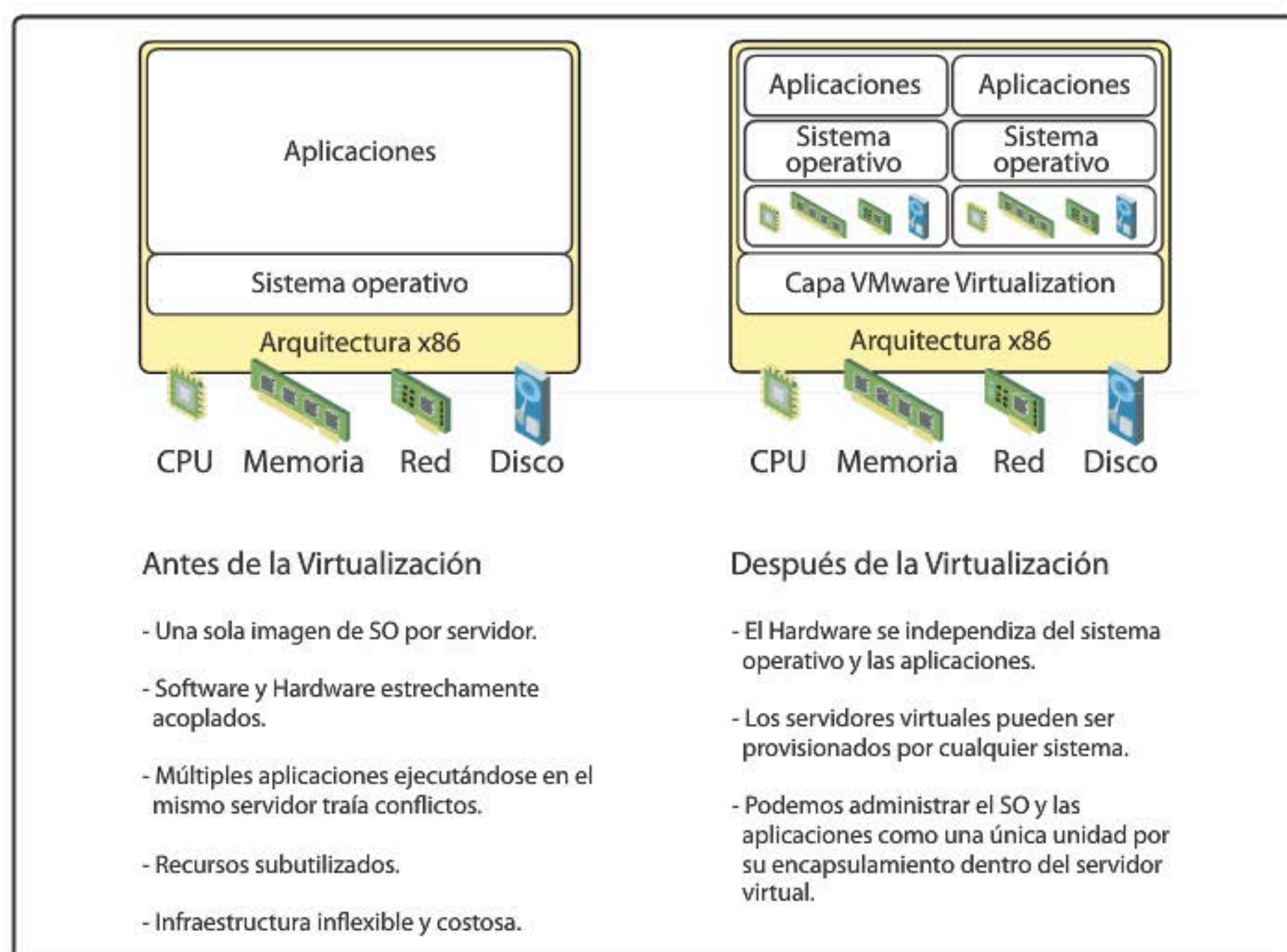


Figura 1. Comparación de una máquina física y una máquina virtual.

Lo que hacen muchos hypervisores es compartir uno o varios recursos entre distintas máquinas virtuales, por ejemplo, determinado espacio de memoria RAM de varias máquinas virtuales que son iguales. De esta manera, si tenemos dos sistemas operativos virtuales que son Windows 2008 y cargan las mismas **DLL** a memoria, ellos podrían utilizar el mismo espacio de memoria sin saberlo. Como el hypervisor sabe que esos espacios son iguales, tratará de maximizar el uso de la memoria RAM física y, para ello, realiza este uso compartido para las máquinas virtuales.

Hoy en día, la virtualización no se relaciona tan solo con hypervisores y máquinas virtuales, sino que aparece también en aplicaciones y hasta en dispositivos celulares. Así, las aplicaciones de una empresa podrían colocarse en un único servidor y ser utilizadas de manera remota por todos los empleados. Este es el concepto de aplicación virtual de Citrix. También es posible combinar esto con el uso de máquinas virtuales, con lo cual obtenemos máquinas virtuales que contienen estas aplicaciones virtualizadas.

En el caso de los celulares, la virtualización plantea el hecho de tener más de un perfil asociado a un mismo teléfono. De esta forma, rápidamente podríamos pasar desde un perfil de trabajo a un perfil de uso personal; cada uno tendría sus aplicaciones relacionadas, sus números telefónicos, agendas, calendario, etcétera. Al igual que la virtualización de servidores, se busca maximizar el uso de los recursos, en este caso, de un celular.

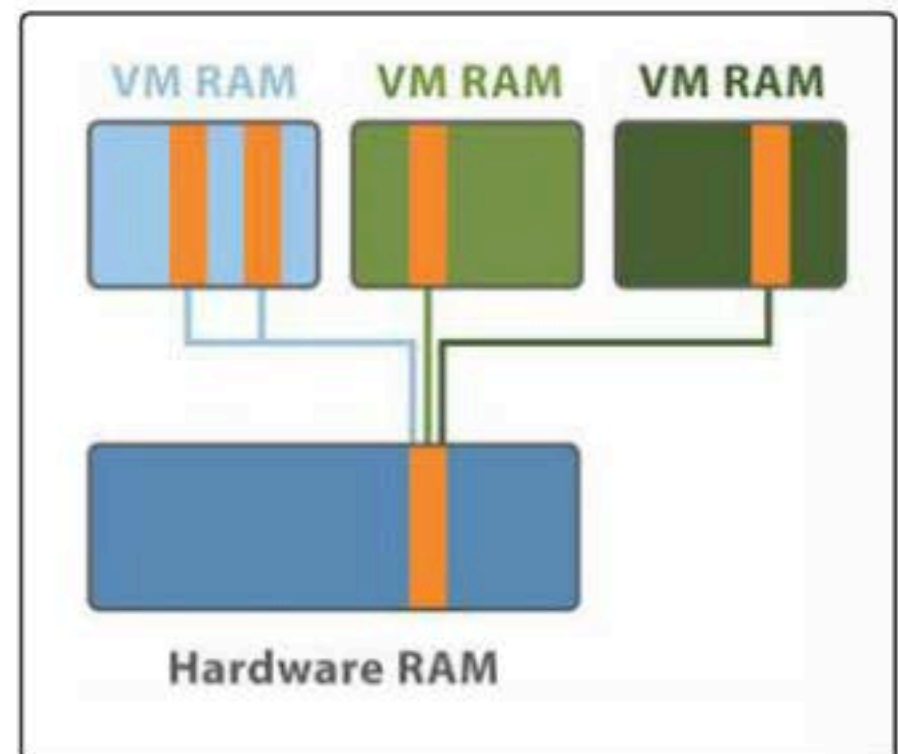


Figura 2. Sistemas virtualizados que comparten la memoria RAM.

La virtualización de máquinas físicas, de aplicaciones, de celulares y otros sistemas busca economizar recursos. El ahorro que da la virtualización tiene lugar en distintos niveles: en la instalación de cables y discos, servidores físicos, espacio, refrigeración, horas de trabajo y administración, gastos en seguridad, energía, etcétera. Cuando una empresa estudia la adopción de una nueva solución de software y hardware, analiza en especial dos grandes aspectos: **funcionalidad** y **costo**. Dicho de otra manera, la relación **costo/rendimiento** de los productos involucrados. Una de las causas de la adopción de la virtualización es justamente la excelente relación costo/rendimiento que posee.

Storage

El **storage** es el más nombrado de los variados sistemas críticos de los cuales depende la virtualización. Para asegurarnos de que una solución de virtualización de servidores sea escalable y de que las máquinas virtuales sigan funcionando en

caso de que alguna falle, necesitamos algún tipo de almacenamiento especial: un storage. Este es un sistema de almacenamiento externo, confiable y escalable, utilizado por las empresas en muchas arquitecturas. Además, posee tecnología que sigue avanzando día a día, y se vuelve cada vez más crítico.

El almacenamiento es otorgado a los sistemas operativos hypervisores, para que luego estos puedan dárselo a los sistemas virtuales que soportan. Estos espacios de almacenamiento se denominan, por lo general, **datastores**. Los hypervisores se encargan de dividir físicamente cada datastore para ofrecer la cantidad necesaria de disco a cada máquina virtual. El procedimiento sería el siguiente:

- Las redes virtuales se conectan a un dispositivo físico que el hypervisor maneja, por lo tanto, las tarjetas virtuales de las distintas máquinas se conectarán, quizás, al mismo dispositivo físico en un hypervisor.
- Los ciclos de CPU del hypervisor son distribuidos por cada CPU virtual a las máquinas virtuales. El hypervisor se encargará de dar más ciclos o menos, según necesite la máquina virtual.

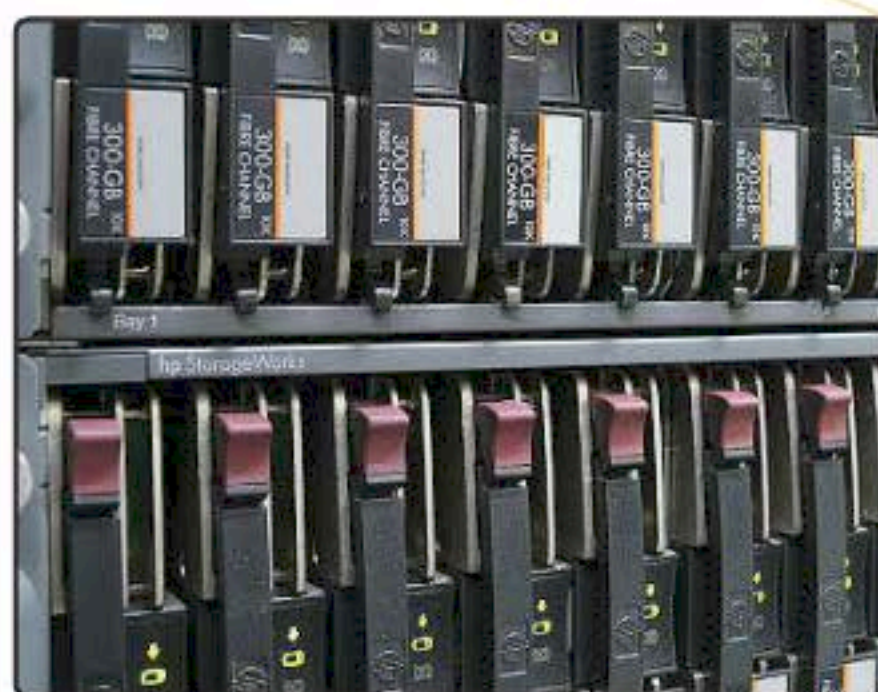


Figura 3. Las unidades de storages pueden estar constituidas por apenas un par de discos o por grandes cantidades.

Con la virtualización ya no será necesario refrigerar decenas de racks con servidores físicos, sino que con uno alcanza. Cada hypervisor, dependiendo de sus capacidades y los tamaños de máquina virtual, puede almacenar entre cinco y veinte servidores virtuales. También existen servidores físicos más potentes que extienden estos límites día a día.

Los gastos de administración de storage se ahorran de manera considerable. Ya no hay que instalar sistemas operativos físicos con todo lo que esto conlleva. No hay que establecer configuraciones específicas para cada servidor, porque todos pasan a ser iguales. Las



HOST Y GUEST

Se denomina **host** al equipo físico, el hypervisor, en donde se ejecuta una determinada cantidad de máquinas virtuales. En cambio, **guest** es el término que se utiliza para identificar a la máquina virtual.

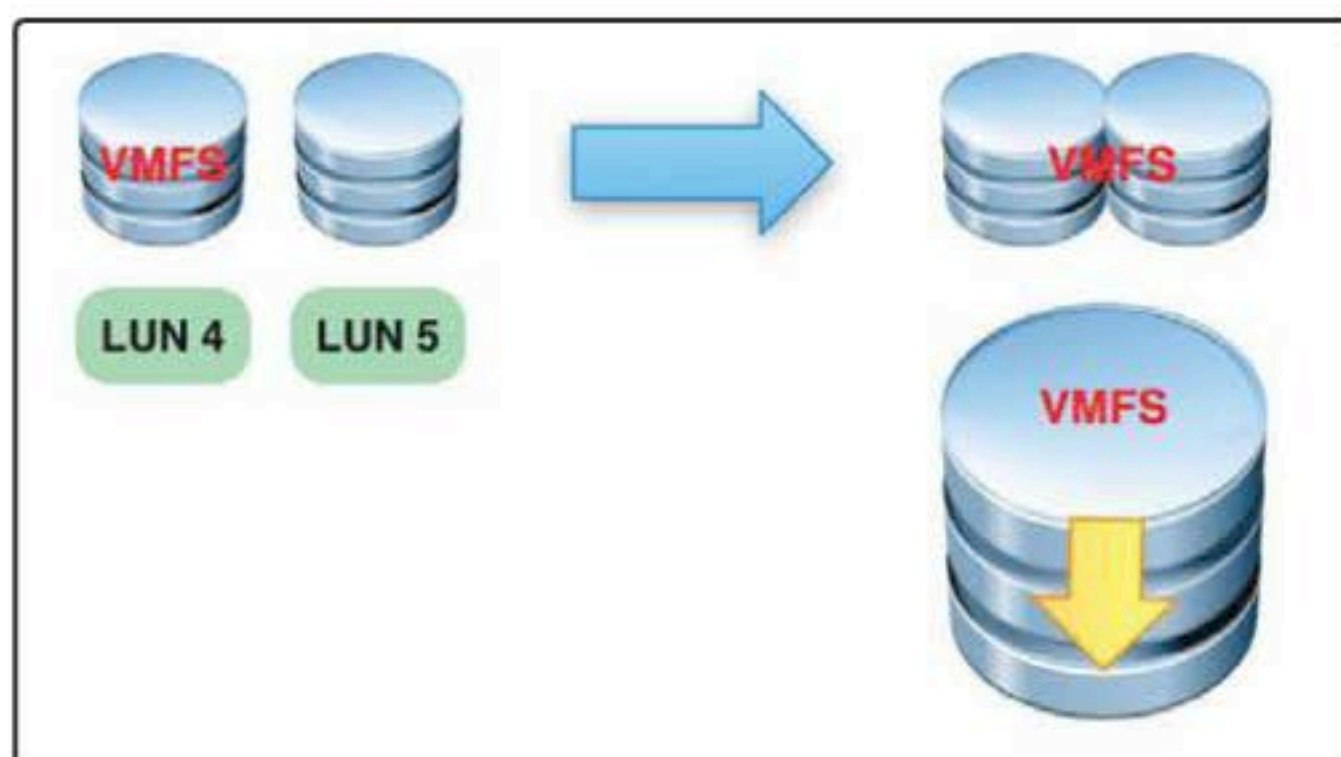


Figura 4. Distintos LUNs de discos pueden conformar un solo datastore.

migraciones, actualizaciones, backups y recuperación de equipos son muchísimo más fáciles que hace unos años.

La independización del hardware es algo clave en todo esto, porque permite que una máquina virtual que corre en una computadora de escritorio pueda funcionar en un servidor x86 en la Argentina, y, luego, ser migrado a Colombia u otros sistemas, sin ningún tipo de problemas.

Los tiempos de parada de los servidores se han reducido enormemente, y surgieron muchas opciones de alta disponibilidad, de recuperación de desastres y sistemas de backup. Durante los

últimos diez años, esos sistemas evolucionaron al igual que la virtualización.

A continuación, haremos un recorrido por el desarrollo de la virtualización.

Historia de la virtualización

Conocer la historia de la virtualización nos permitirá obtener confianza en nuestro accionar diario, porque saber que esta tecnología existe desde hace mucho tiempo nos dará certezas a la hora



DATASTORE

Es un espacio de almacenamiento para las máquinas virtuales. Un datastore puede ser creado a partir de los discos locales de cada host, o desde un subsistema de almacenamiento externo, utilizando protocolos FC, FCoE, iSCSI o NFS.

de tomar decisiones. Muchas empresas han sorteado varios obstáculos en toda esta evolución, y las que comenzaron antes que otras pueden tener el privilegio de seguir desarrollando el concepto de virtualización en el tiempo.

LOS INICIOS: SYSTEM/360

El primer concepto relacionado con la virtualización surgió en los años 60 con la creación por parte de IBM del mainframe S/360, que ostentaba una enorme capacidad de procesamiento de hasta 2 procesadores y un máximo de 2 MB de memoria RAM. Los mainframes eran computadoras de grandes dimensiones que ocupaban pisos enteros en las empresas y donde se corrían la mayoría de las aplicaciones que la sustentaban. En la actualidad, estas capacidades pueden parecer una broma, pero, para la época, eran muy significativas. Los IBM S/360 se produjeron en el Centro Científico de Cambridge en cooperación con los investigadores del MIT (Massachusetts Institute of Technology), uno de los centros de tecnología más prestigiosos del mundo.

Se comenzaron a fabricar el 7 de abril de 1964, y su presentación oficial fue en agosto de 1965. Los ingenieros de IBM pudieron ver qué gran capacidad de cómputo se perdía al mantener ocioso el sistema en la utilización de los mainframes antiguos (anteriores al S/360). Lo que ellos inventaron fue un procedimiento para repartir el uso de la capacidad total del S/360 en estructuras virtuales más pequeñas. Gracias al sistema operativo de tiempo compartido desarrollado por la misma empresa, el CP/CMS, que traía consigo

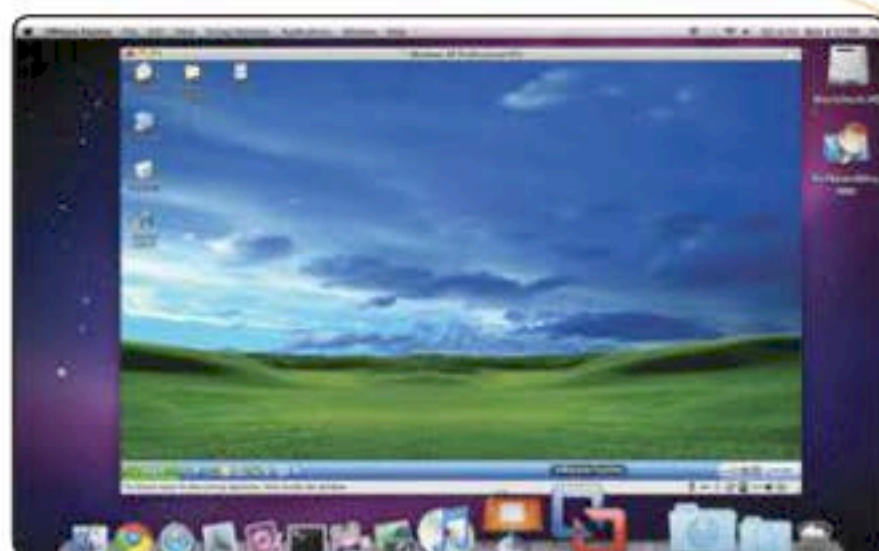


Figura 5. Una máquina virtual puede correr en cualquier servidor que disponga de determinados recursos asignados a ella.

el S/360, pudieron asignar a cada usuario una porción de procesamiento independiente, de forma virtual, de modo que el usuario obtenía un subsistema S/360 separado, para su uso personal. El uso del mainframe, de esta forma, ya no era centralizado como los antiguos sistemas, sino que distribuía su capacidad con todos los usuarios. En los antiguos datacenters, cada programa que corría en los mainframes ocupaba todo su tiempo de trabajo; hasta que no se terminaba con las salidas de un programa, no se pasaba al siguiente. Esta circunstancia daba la posibilidad de que los programas utilizaran gran capacidad de cómputo, pero, en la mayoría de los casos, dejaban ocioso el sistema. Con el S/360, al distribuir los subsistemas virtuales, se logró que varios programas de usuarios corrieran al mismo tiempo utilizando el mismo mainframe.

1998: VIRTUALIZACIÓN DE SISTEMAS DE CÓMPUTO

En 1998, la empresa VMware presentó una patente en EE.UU. con el concepto que

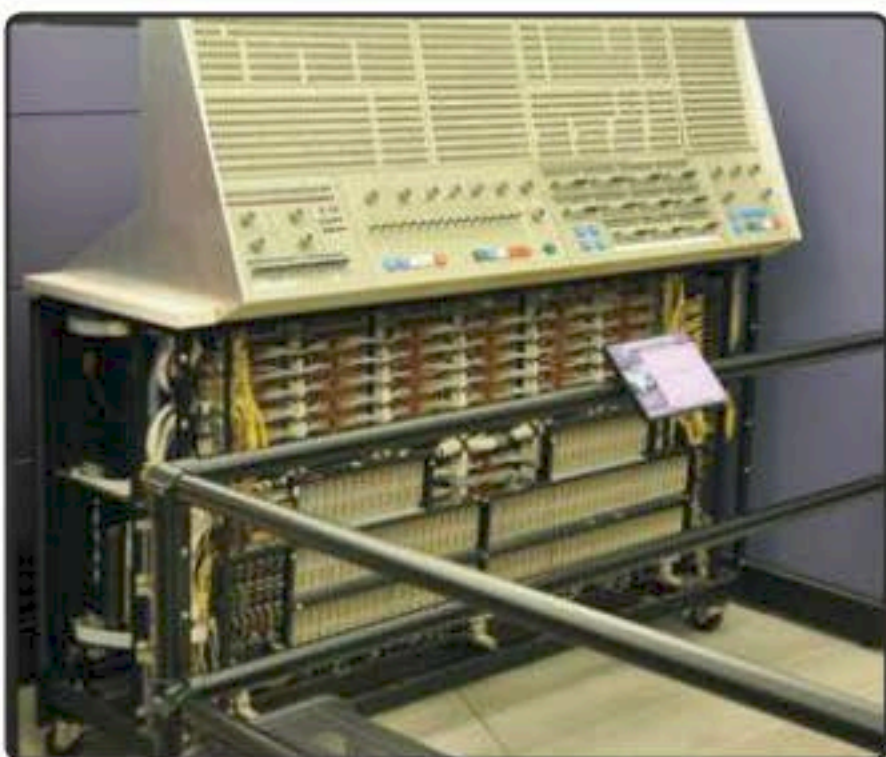


Figura 6. El mainframe System/360 creado por IBM, el origen de la virtualización.

revolucionaría el mercado: **System and Method for Virtualizing Computer Systems** (sistema y método para la virtualización de sistemas de cómputo), que describía todos los componentes para crear la virtualización.

El sistema patentado ya había sido utilizado desde hacía bastante tiempo en muchas investigaciones para evaluar sistemas de multiprocesadores, investigaciones de cálculos avanzados y



Figura 7. Uno de los primeros servidores físicos x86 que reemplazaron a los mainframes.

rendimiento en procesadores. Un ejemplo que se nombra en la patente es que corrieron el sistema en una Power PC de Macintosh (una máquina de escritorio de la época) para probar aplicaciones para 68000 arquitecturas diferentes.

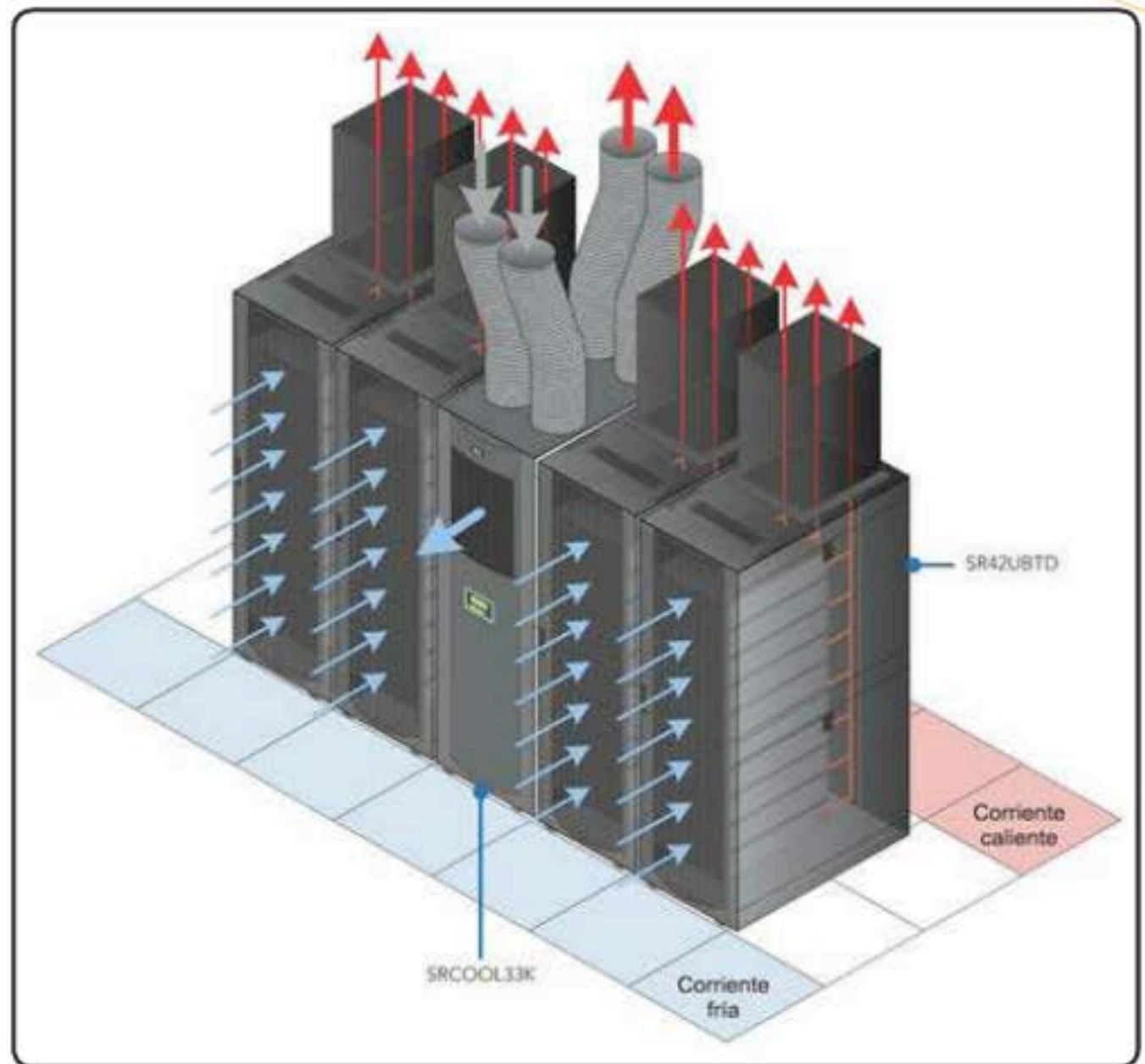
El sistema corría en sistemas operativos de **host** (así es como se llama a los sistemas operativos instalados en el hardware base en la patente de VMware), que podían ser, aparte de Power PC de Apple, Windows NT de Microsoft, y Linux. Varios sistemas operativos podían ser virtualizados en las máquinas de aquel entonces, algunos de ellos eran: Microsoft DOS, Windows 3.1, Windows 95, Windows 98, Windows NT, Linux y Unix. Podemos deducir entonces que los sistemas de host nombrados en las patentes eran servidores físicos y máquinas de escritorio muchísimo más chicas que los grandes mainframes.

ARQUITECTURAS X86

Durante los años de convivencia entre los grandes mainframes y los nuevos servidores **x86**, las empresas fueron migrando a arquitecturas x86. Podían realizar los mismos objetivos con muchos menos recursos económicos, ya que los mainframes representaban un costo muy alto para los sectores de IT. Con el uso de servidores más chicos, el centro de cómputos redujo sus dimensiones, pero comenzó a tenerse gran cantidad de interconexiones, racks, consumos de mano de obra que antes no se tenían, ingeniería de aire acondicionado, etcétera.

De todas formas, estos costos eran muy bajos comparados con los de la compra de un

Figura 8. El gráfico indica cómo debería circular el aire en un datacenter.



mainframe, por lo tanto, fueron bien aceptados, y los mainframes se dejaron de lado. Sin embargo, se observó que seguía habiendo recursos de hardware ociosos. Había que maximizar otra vez la inversión de la compra de servidores.

En ese momento, entonces, se desarrolló el sistema de virtualización de VMware. Este concepto de virtualización de IBM, aplicado con éxito en los años 60, generó un cambio de gran magnitud más de 30 años después. Con el patentamiento de VMware y su aplicación en los servidores basados en arquitecturas x86, servidores mucho más chicos, más baratos y de menores prestaciones lograron dar vuelta el mercado. Aunque se basó en un concepto existente,

logró algo en definitiva impensado en aquellos años: imponerse en el mercado empresarial y aplicar ese concepto de IBM sobre una plataforma muy diferente. Su estabilidad fue tal que logró la adopción del mercado de servidores en forma masiva y sorprendentemente rápida.

2006: INFRAESTRUCTURA VIRTUAL

Recién en el año 2006 se logró, otra vez, centralizar el cómputo hasta llegar a consumir el 100% de los recursos de hardware durante más del 80% de la operatoria diaria, lo que le da al valor de la inversión un gran resultado. En el año 2006, VMware lanzó el producto **Virtual Infrastructure** en el cual reunía un concepto de clusters armados con sistemas operativos propios, llamados ESX/ESXi (los hypervisores) con



Figura 9. VMware provee de una calculadora online para saber cuánta energía ahorramos.

un manejador de la arquitectura central, llamado **Virtual Center**.

VMware ya no era un producto que se instalaba sobre un sistema Windows, Power PC o Linux solamente, sino que pasaba a ser algo mucho más grande. Comenzó así la era de la infraestructura virtual luego de varias horas gastadas de ingeniería en sistemas.

Este producto, basado en un hypervisor muy robusto, ofrecía conceptos avanzados de administración, alta disponibilidad y balanceo de carga, que permitía correr aplicaciones críticas con una robustez de la que no era

fácil dar crédito si no lo veíamos con nuestros propios ojos. En un principio, fue bautizado como **VMware Infrastructure ESX**, y había una opción gratuita llamada **ESXi**. Esta ganó mucho terreno en los últimos años; por rendimiento, seguridad y otros aspectos, logró quedarse como único hypervisor en las versiones actuales de VMware.

La empresa modificó el accionar de muchas compañías y cambió la forma de ver los datacenters, convirtió a los servidores en objetos que podían ir para un lado o para el otro de manera independiente de dónde estuvieran físicamente.



Figura 10. Un servicio de cloud computing muy conocido es el de SalesForce.

SPLIT BRAIN

Es una condición que ocurre en una solución de cluster por la falla de la conexión privada entre los nodos. Cada nodo cree que el resto no funciona y trata de ejecutar todos los recursos del cluster, provocando mal funcionamiento e, incluso, pérdida y corrupción de datos.

La virtualización en general y la consolidación de servidores físicos en particular lograron eliminar la proliferación de servidores de manera casi incontrolable y sus consecuencias. De esta forma, el procesamiento de datos y la ejecución de servicios de infraestructura fue mutando, con la adopción de las arquitecturas x86, de una modalidad centralizada a su antítesis, es decir, a un procesamiento claramente distribuido. Luego, más tarde, con la adopción de la virtualización de VMware, las empresas de nuevo dieron vuelta el tablero, centralizando lo que antes habían descentralizado.

La infraestructura virtual de VMware marcó el comienzo de una era en la que se prioriza el aprovechamiento de los recursos. Se logra así un cambio drástico en la forma de ver la infraestructura, como **infraestructura de servidores** a nivel económico dentro de la empresa. Se piensa en su costo asociado contraponiendo los requerimientos del negocio. Allí es donde VMware y la virtualización ganan todas las batallas.

EL PRESENTE

En la actualidad, todos los proyectos de IT de las empresas nacen con servidores virtuales. Ya casi



Figura 11. Un enclosure contiene todos los servidores blade, compartiendo energía, refrigeración y otras conexiones.

no se habla de instalación de servidores físicos, el concepto de virtualización llegó a cada rincón de la compañía. Empresas en este punto de maduración están listas para adoptar el segundo nivel, la automatización de la virtualización, mediante el uso de técnicas de **cloud computing**.

Si bien este concepto es muy amplio y este libro no pretende explicarlo, podemos decir que tendría que ser el objetivo a largo plazo de cualquier empresa que ya tenga virtualización. La virtualización está mutando también con la combinación y migración de servidores comunes a servidores tipo blade.



SISTEMA OPERATIVO CP/CMS

Este sistema operativo fue diseñado en la década de 1960 por IBM y fue reconocido por su gran funcionalidad. El CP-40/CMS fue el primer sistema operativo capaz de crear máquinas virtuales. Estos sistemas operativos solo corrían en plataformas mainframe.



Figura 12. Cada dispositivo del enclosure es hot swap, esto quiere decir que se puede cambiar mientras está encendido el cajón.

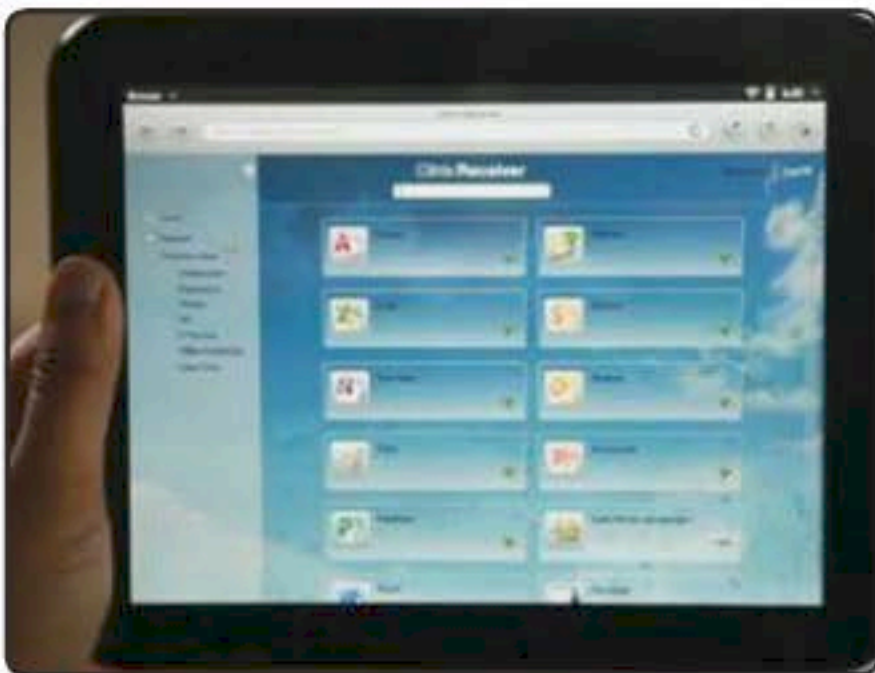


Figura 13. Podemos administrar nuestra infraestructura desde cualquier dispositivo.

Los blades son servidores más reducidos en tamaño, que conforman un cajón llamado **enclosure**. Los enclosures fueron pensados como pequeños datacenters que centralizan la refrigeración de varios servidores y, también, las interconexiones de energía y redes. Permiten a su vez ofrecer alta disponibilidad a varios servidores a un bajo costo. Hay diversas tecnologías en el mercado, y cada una tiene características especiales. Por ejemplo, los enclosure HP tienen una capa de red conformada por unos switches dentro del cajón llamado **virtual connect**, que permite virtualizar redes desde el hardware en forma directa.

Tanto Cisco como IBM tienen sistemas similares. Esto le da un plus a toda nuestra infraestructura, y se siguen inventando elementos a diario. Hoy las consolas de administración de la infraestructura virtual corren bajo servicios web, pueden ser accedidas desde una portátil, una computadora de escritorio, una tablet o un teléfono celular.

Sin dudas, los límites de la virtualización no tienen fin, y esta seguirá evolucionando con el tiempo.



RESUMEN

En este capítulo vimos los distintos conceptos fundamentales de la virtualización. También analizamos su historia y, sobre todo, sus orígenes, para entender un poco más qué es lo que utilizamos todos los días y poder tomar decisiones certeras basándonos en la confianza en ciertas soluciones.

Capítulo 2

Soluciones de virtualización en el mercado

Detallaremos algunas soluciones del mercado, y las tecnologías de servidores y PCs de escritorio.

Diferentes tecnologías

Existen en el mercado diferentes tecnologías implementadas por varias empresas de virtualización. Como vimos en el capítulo anterior, IBM es parte de esa lista, pero la más conocida es VMware, debido a su amplia trayectoria y a haber iniciado la era de la virtualización en x86. Hay otras que la siguieron y hoy ofrecen algunas alternativas de Hypervisores. Entre las empresas que podemos nombrar, además de VMware e IBM, están Microsoft, Citrix, Oracle, Parallels, RedHat y otras como Novell, que este último año no apareció en el cuadrante Gartner. Otras menos conocidas, que no tuvieron mucha repercusión, son Basilisk, BOCHS, Virtuozzo, vMac y SheepShaver. Este orden está dado por el cuadrante en el año 2012.

Si bien Microsoft comenzó a dedicarse a la virtualización diez años después que VMware, avanzó rápidamente este último tiempo; por lo menos, mucho más que el resto de sus competidores.

IBM ya está fuera de este listado porque el núcleo de su negocio ha tomado otros rumbos. Microsoft quedó en el segundo puesto con su sistema de virtualización Hyper-V, integrado en Windows Server 2008 y en los nuevos Windows Server 2012.

El sistema operativo de Microsoft evolucionó mucho, y en estos últimos tiempos, la firma ha escuchado a sus usuarios, y ahora brinda

distintas posibilidades de instalación, desde una versión sin interfaz gráfica, al mejor estilo Linux/UNIX; hasta las versiones gráficas a las cuales se les puede asignar todo tipo de roles de File Server, Print Server, Web Server y Virtual Server. Es preciso hacer una diferenciación entre dos tipos de sistemas que ofrecen estas empresas: los de tipo I y los de tipo II. Tanto ESXi (VMware), como Xen Server, KVM, Oracle VM o Hyper-V son sistemas del tipo 1, que se instalan directamente en el hardware; es decir, son sistemas operativos puros.

En el tipo 2 podemos encontrar tanto a Virtual Server, de Microsoft, como otras soluciones que se instalan arriba de otro sistema operativo, ya sea Windows o Linux. Algunos competidores en este rango son VMware Server, VMware Workstation, VMware Player, Virtual Box, QEMU y Virtual PC.

Fuera de lo que son los Hypervisores, otra firma que ofrece soporte para todas las empresas de virtualización es Intel. También AMD, su competidora, tiene soluciones de virtualización, pero Intel fue pionera y es la más utilizada en la actualidad por casi todos los servidores del mercado.

La tecnología que ofrece Intel amplía al máximo la capacidad de los procesadores, y hoy hasta es posible aislar la ejecución de los sistemas operativos virtuales cargados en el sistema. Esto favorece extraordinariamente la estabilidad de los sistemas virtuales y su seguridad.

Como en Intel, la virtualización se expande en

TECNOLOGÍAS DE VIRTUALIZACIÓN	
EMPRESA	SOLUCIÓN
VMware	vSphere www.vmware.com/products/vsphere
Microsoft	Hyper-V www.microsoft.com/hyper-v-server
Citrix	XenServer www.citrix.com/xenserver
Oracle	Oracle VM www.oracle.com/us/technologies/virtualization
Oracle Solaris	Oracle Solaris Containers www.oracle.com/us/products/servers-storage/solaris/virtualization
RedHat	Enterprise Virtualization www.latam.redhat.com/rhel/virtualization
Parallels	Parallels Server www.parallels.com/virtualization/server
Novell	Suse Linux Enterprise Server www.novell.com/es-es/products/server/virtualization.html

Tabla 1. Soluciones de virtualización de diferentes empresas.

todas las empresas de informática, y las soluciones en el mercado crecen de modo exponencial. Compañías como Intel dan soluciones a componentes específicos de la infraestructura. HP también lo hace, por ejemplo, con una gran solución llamada Virtual Connect para su línea de Enclosures. Esta herramienta permite virtualizar conexiones de red dentro del cajón. Es una capa de virtualización entre las conexiones físicas a un switch en el cajón, y las conexiones a los blades (servidores) en el mismo cajón. Estas conexiones son de red LAN y fibra para los discos.

Por su parte, Cisco comercializa switches virtuales que tienen toda la lógica de los físicos, pero la empresa tuvo que evolucionar para tomar el control de las redes virtuales. Symantec, al igual que otras compañías desarrolladoras de antivirus, tiene en el mercado servidores que funcionan como centralizadores de antivirus para cada Hypervisor, al omitir los clientes en las máquinas virtuales, sacar carga a estas últimas y obtener el control central de todos los equipos. Muchas empresas han evolucionado hacia la virtualización, y continuarán haciéndolo durante varios años más.

Como vimos antes, la virtualización es una tecnología presente en celulares, escritorios, redes, backups, microprocesadores, etc. En

unos años, el problema será cómo harán todas estas empresas para convivir.

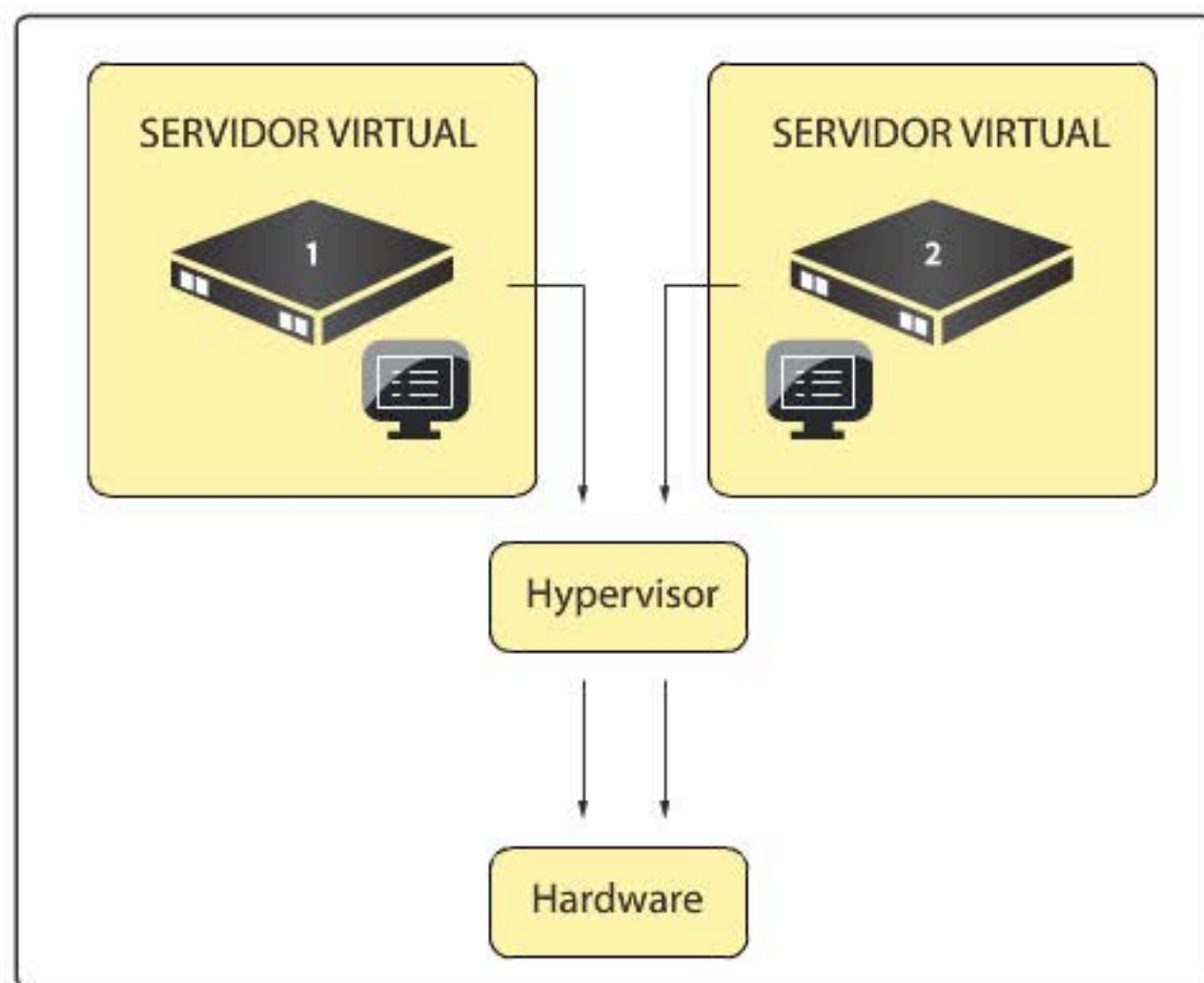


Figura 2. Tipo I: una capa de Hypervisor que maneja directamente el hardware para las máquinas virtuales.

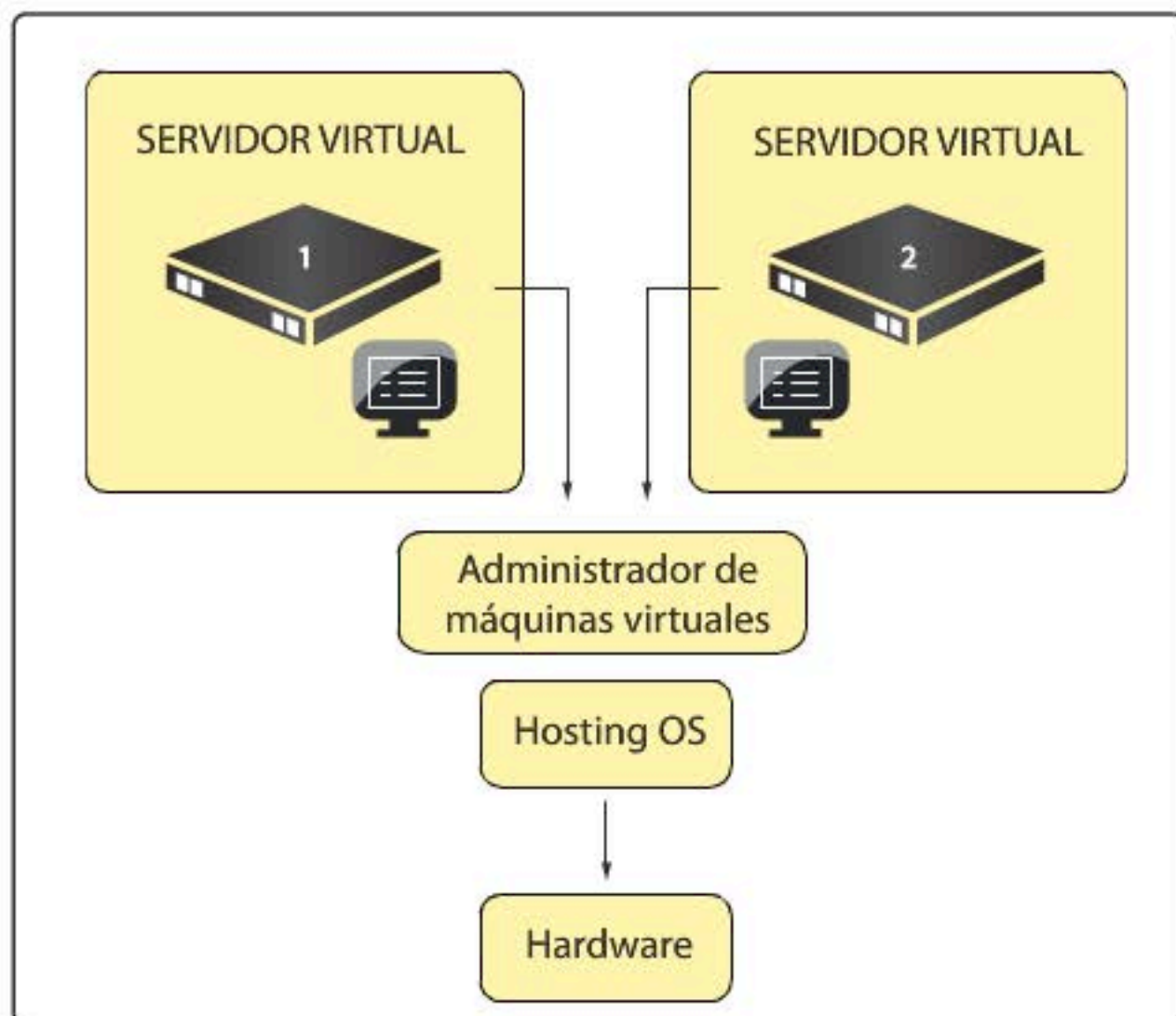


Figura 3. Tipo II: otra capa más que corresponde al SO que alberga el sistema de virtualización.

Para esto, ya hay organismos creados por varias de ellas encargados de estandarizar los distintos componentes virtuales que se van desarrollando. De esta forma, podremos virtualizar un servidor físico y moverlo a donde queramos usando la tecnología de cualquier empresa.

El estándar más conocido hoy es OVF (Open Virtualization Format), un sistema de distribución de archivos comprimidos avalado por las principales competidoras del rubro. Si bien tenemos este formato estándar para todas las tecnologías que están floreciendo, aún falta dar un paso esencial: pasar de un servidor físico a uno virtual. Veremos los detalles de este tema a continuación.

Cómo virtualizar un servidor

Hay muchos servidores físicos que brindan servicios en las empresas. A continuación, veremos cómo transformarlos en virtuales sin perder datos, permisos ni configuraciones, y manteniendo la continuidad del negocio, al hacer los cambios en el menor tiempo posible. Así, podremos optimizar nuestra infraestructura en cuanto a consumo de hardware, ahorro de recursos, agilidad en la administración, y gran posibilidad de expansión y actualización. Hace tiempo, era impensable pasar un servidor físico a uno virtual; directamente, nadie hablaba de eso. Hoy en día, es un trabajo que está



Figura 4. Los cajones blade de HP son increíbles; permiten sacar y cambiar casi cualquier componente en caliente.

en pleno auge. Ya en el informe del año 2011 de la empresa Gartner acerca de las visiones de los principales CEOs de la industria, se ubicaba la virtualización en el primer puesto. Si buscamos, además, los aspectos relevantes dentro de este tema, la conversión de servidores físicos en virtuales era el ganador, y no hay personal capacitado para llevar a cabo esta tarea dentro de las organizaciones. Este libro tratará de arrojar luz sobre estas cuestiones.

Antes era muy complicado realizar esta tarea, y ocurrían muchas fallas al hacerlo, pero con la nueva versión de VMware Converter, numerosos

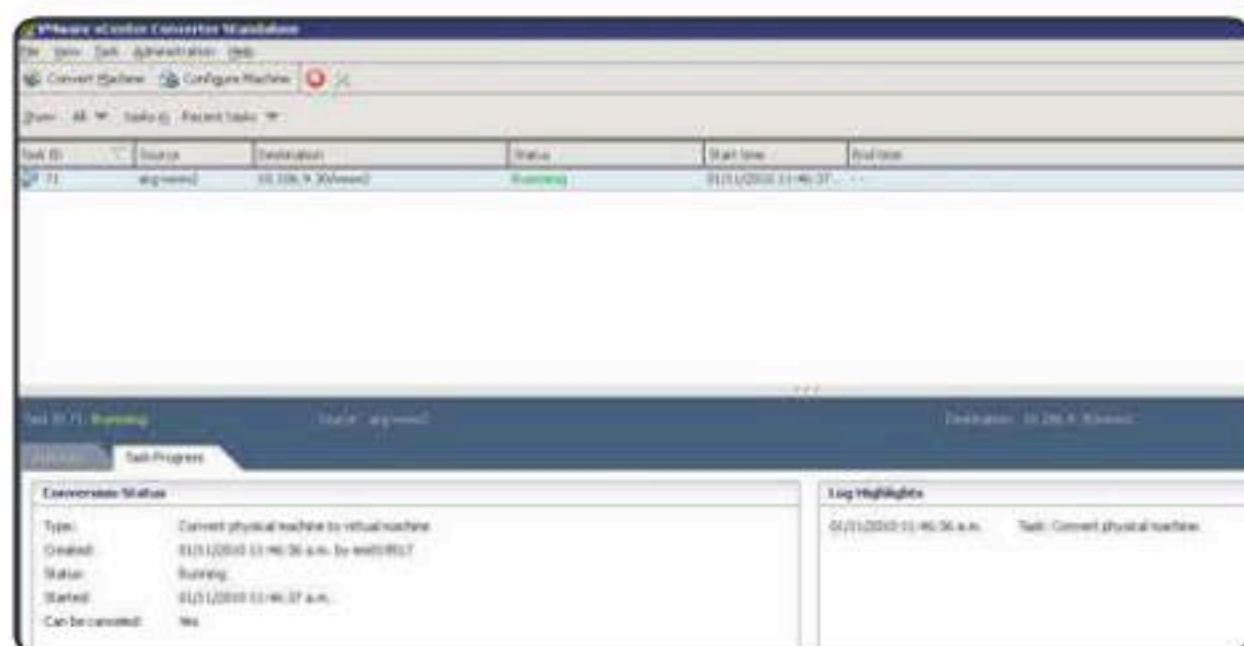


Figura 5. La consola de Converter es sencilla, informa las tareas que se realizaron, las que están en curso y las que fallaron.

inconvenientes se han solucionado. VMware ofrece, de modo gratuito en el mercado, esta formidable herramienta que no tiene competidores. En el proceso de migración de una máquina física a otra virtual, se requiere más que saber utilizar la herramienta VMware Converter, seguir un par de pasos y oprimir **Next**. Aquí veremos algunos detalles de su uso y aprenderemos todo lo que ocurre alrededor cuando virtualizamos un servidor.

Hay varios aspectos para tener en cuenta. Por ejemplo, supongamos que tenemos que migrar un servidor web que contiene 20 sitios productivos, a los cuales se conectan usuarios de la empresa más otro grupo de usuarios externos. De allí se sacan informes porque hay un Report Services instalado, a la vez que se lo usa como servidor FTP. Por eso decimos que no solo es cuestión de saber utilizar la herramienta, sino que también necesitamos administrar muchos responsables, coordinar con numerosos usuarios y efectuar las tareas fuera de horario. Todo esto, sin mencionar las configuraciones de red que se pierden al virtualizar. El proceso deja una copia

exacta del servidor, pero, lamentablemente, los controladores de red se destruyen y se reemplazan por los virtuales, con lo cual se pierden las configuraciones de IP, MAC Address y rutas estáticas. Tengamos en cuenta que también puede tener acceso a redes a las cuales nuestro Hypervisor no llega, o puede tener configuradas varias direcciones IP.

Al migrar un servidor físico a uno virtual, debemos ser cuidadosos con las configuraciones de red; principalmente, con la cantidad de IPs, la tabla de ruteo, las reglas en el firewall, además de la dirección MAC del controlador, que debemos copiar por precaución.

Otro aspecto importante es si tenemos un servidor de aplicaciones, en cuyo caso la sincronización de datos es muy crítica. Tal vez estemos realizando la copia del servidor en línea y, mientras hacemos el cambio de físico a virtual, alguien actualiza una carpeta de la aplicación. El error que se provoca es la pérdida de información. Lo recomendable, entonces, es fijar reuniones con todos los especialistas, usuarios y administradores que

tienen incidencia en el servidor por virtualizar, e incluirlos en el proceso para que nada falle. Si el usuario está avisado, no debería actualizar una carpeta en el rango horario de migración.

El problema es exponencial al migrar un servidor de base de datos. Hoy se habla de almacenamientos de TB de información. ¿Qué sucede una vez que realizamos la copia virtual? Al segundo siguiente, la información entre los dos servidores es diferente. Lo recomendable en este caso es planificar un horario de migración, bajar las bases de datos y virtualizar el servidor. Luego de efectuar la copia, hay que verificar su funcionamiento y poner en línea las bases de datos otra vez.

DESCRIPCIÓN DEL PROCEDIMIENTO

El procedimiento de migración es muy sencillo; lleva tiempo, pero es simple. Como primera medida, debemos generar un plan. Una práctica recomendable es virtualizar el equipo previamente, ponerlo en un ambiente de prueba y verificar que funcione como corresponde. Hacer la copia no interfiere en las actividades cotidianas. Quizá si el sistema está basado en Windows 2000 o anterior, necesitará

un reinicio, pero nada más; solo se instala un agente de VMware Converter y se comienza a copiar la información. El destino de la copia puede ser cualquier ambiente de VMware o un archivo OVF. De la familia de VMware puede migrarse a un formato de VMware Player, VMware Workstation, Server o ESX/ESXi. Lo recomendable para la prueba es utilizar la versión Server, más ágil y sencilla, y con la cual no comprometemos servidores ESXi productivos. Luego sí, hay que hacer la migración real.

Para armar el plan, comenzamos por contactar a los usuarios, ver los tiempos posibles y definir una agenda; luego, anotamos todas las posibilidades de pérdida de datos, sincronización o configuraciones, para estar al tanto de ellas e ir directamente al problema si debemos realizar tareas de troubleshooting. En la fase de la virtualización, solo debemos utilizar VMware Converter desde el server destino o desde un server que esté en el medio de los dos.

Una vez finalizada la copia, vamos a contar con ambos servidores, uno físico y otro virtual; el físico estará productivo hasta que hagamos el cambio al virtual. La manera más simple de hacerlo es bajar la placa de red física y levantar



NO ESTAR SOLO CON LA VIRTUALIZACIÓN

Es preciso hacer un plan que involucre a los usuarios y a los demás departamentos. Un trabajo bien hecho genera confianza en las personas y, por ende, colaboración ante cualquier cambio futuro.

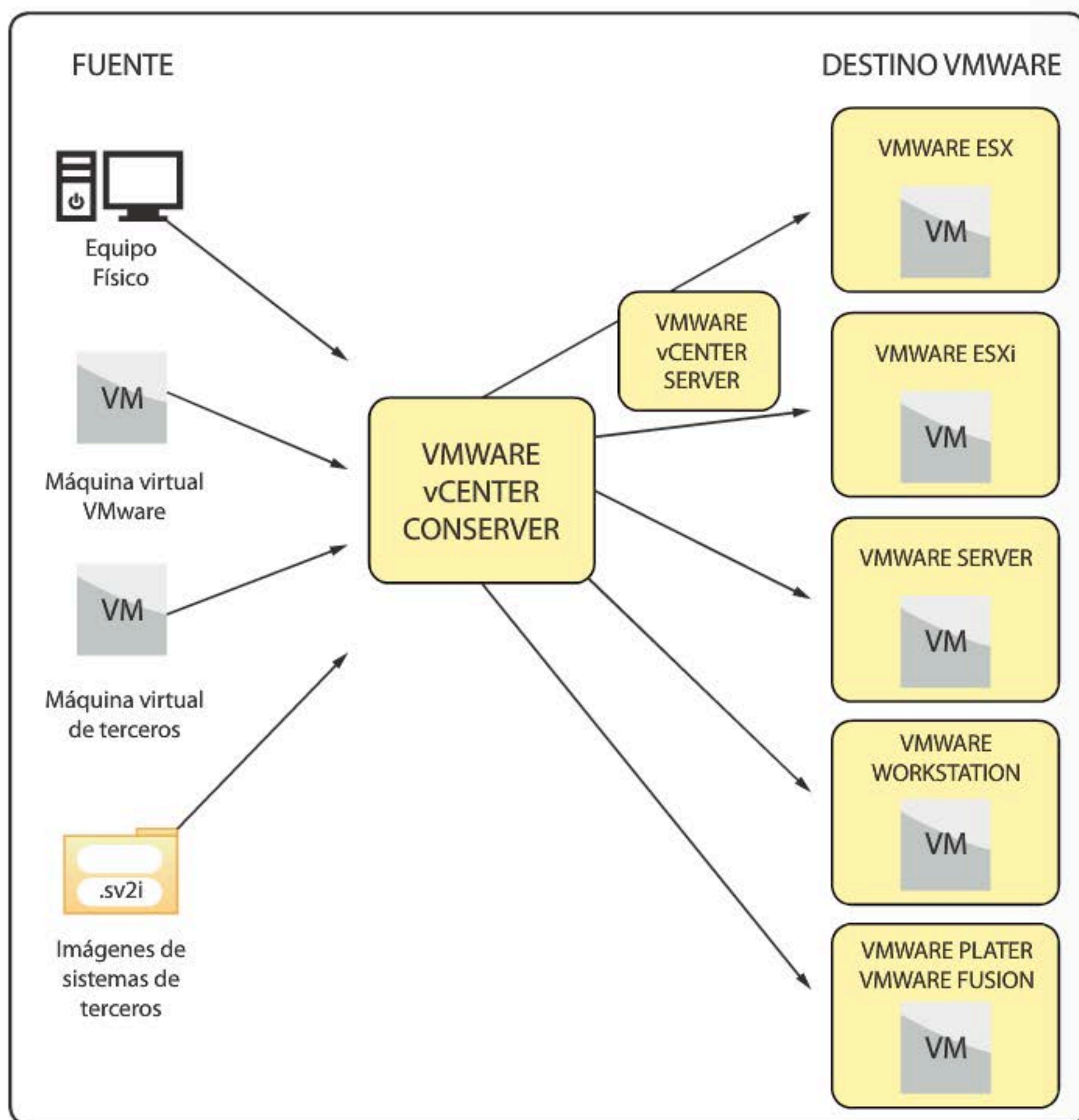


Figura 6. VMware Converter permite pasar distintos tipos de máquinas virtuales, físicas e imágenes a varios productos de la empresa.

la placa de red del virtual. Al tener la misma IP, el servidor experimentará un microcorte, pero durante solo unos segundos. Esta tarea, obviamente, no puede realizarse con bases de datos y sistemas críticos, sino únicamente con ciertos

servidores de la red. Debemos saber cuál es el mejor momento para hacer el cambio del servidor físico por el virtual, e implementarlo. Lo recomendable es tener una consola IP conectada al servidor físico para no perder conexión

cuando demos de baja la placa de red. Si todo funciona correctamente, estaremos en posición de decir que el servidor físico ya no lo es más, y ahora es virtual. Procedemos a apagar el hardware físico que no utilizamos y a reciclarlo o donarlo a alguna institución benéfica.

MIGRACIÓN DE UN SERVIDOR FÍSICO A UNO VIRTUAL

Como detallamos anteriormente, el procedimiento consiste en utilizar VMware Converter, que copiará el agente por nosotros, mandará a reiniciar el servidor si es necesario y comenzará a copiar. Luego, para finalizar, hacemos el cambio.

A continuación, veremos un paso a paso para que, una vez que tengamos todo planeado y coordinado, entremos en la fase de virtualización.

La instalación de VMware Converter es muy

sencilla, solo debemos seguir unos pocos pasos. No tendremos complicaciones, e incluso, podremos correr el software en una máquina no muy grande.

En el paso 2 del procedimiento anterior, donde elegimos **Power-on machine** también tendremos la opción de migrar el servidor cuando está apagado. Otra posibilidad es hacerlo desde algún otro formato de máquinas virtuales, desde Microsoft Virtual Server 2005, desde Hyper-v, desde VMware Workstation o Player (para pasarlo a un ambiente ESX), y otros. En el paso 3 también podríamos utilizar la opción automática, pero, si la virtualización falla por algún motivo, tendremos que instalar el cliente otra vez, y esto lleva unos minutos que ahorraremos si elegimos la forma manual.

PASO A PASO /1 Convertir un servidor físico en virtual

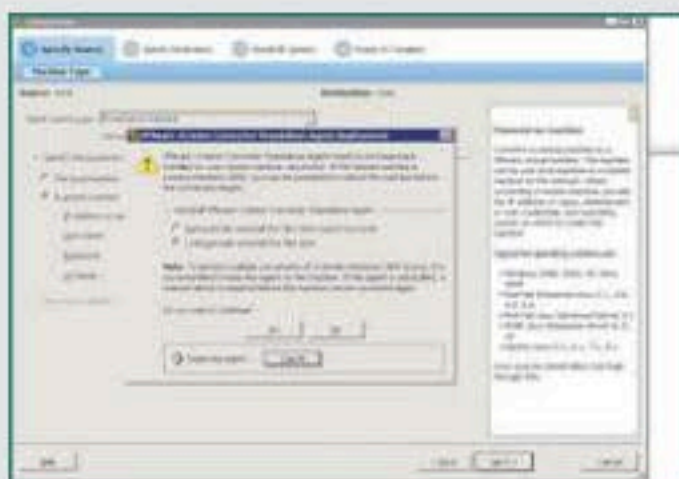
1



Descargue VMware Converter e instálelo en cualquier servidor o PC. Puede obtenerlo desde: www.vmware.com/products/converter. Ejecute la aplicación en un equipo de la red. Elija la opción **Powered-on machine** en **Select source type**. Luego, vaya a **A remote machine** y complete la información.

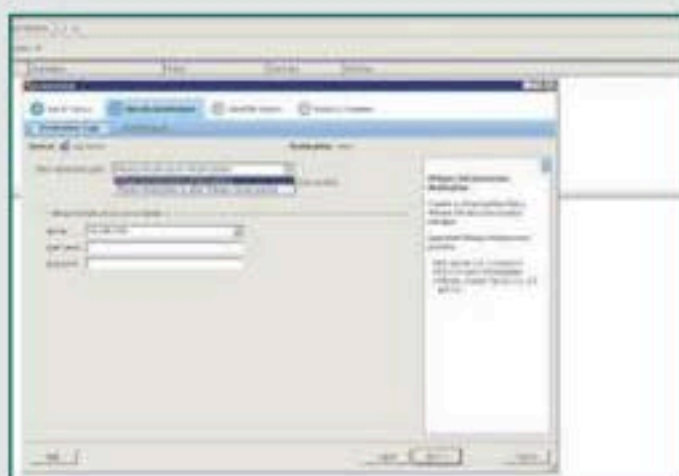
PASO A PASO /1 (cont.)

2



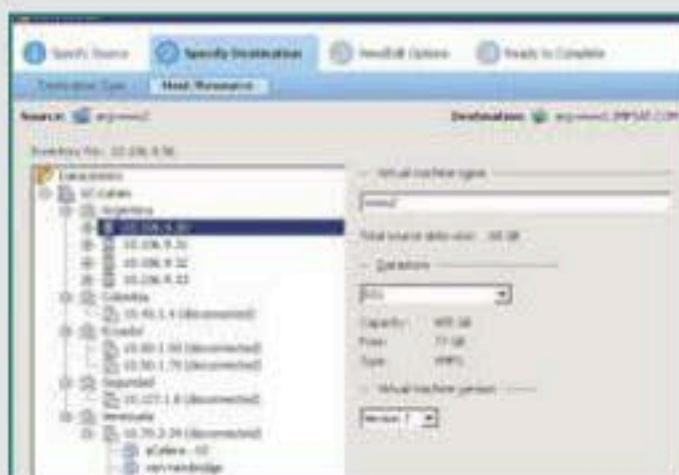
Seleccione la opción **I will manually uninstall the files later** y oprima **YES** para iniciar la instalación del cliente.

3



Elija el destino, si es un **VMware Infrastructure (ESX)** u otro tipo de aplicación, como **VMware Workstation**. Complete los datos debajo y oprima **Next>**.

4



Seleccione el storage de destino, y complete los datos de versión y nombre. Presione el botón **Next>**.

PASO A PASO /1 (cont.)

5



Vea el resumen, pulse **Next>** y, luego, oprima el botón **Finish** para comenzar a virtualizar. Más tarde verifique el avance y si la tarea se completó sin errores.

Los gastos de administración se reducen de manera incalculable. Ya no hay que instalar sistemas operativos físicos con todo lo que esto conlleva; ni es necesario establecer configuraciones específicas para cada servidor, porque todos pasan a ser iguales. Las migraciones, actualizaciones, backups y recuperación de equipos son muchísimo más fáciles de hacer que hace unos años.

Virtualización de servidores y escritorios

La modalidad de trabajo tradicional, que ha sido usada desde hace años con el comienzo del procesamiento de datos distribuido, no ha mejorado con el correr del tiempo más que en

el equipamiento empleado. Algunos de los aspectos que podemos nombrar, que representan problemáticas asociadas a este tipo de arquitectura, son la complejidad a la hora de migrar de sistema operativo y de hardware, el modo de controlar la fuga de información, el consumo de energía, el costo de componentes y recursos humanos para dar soporte, y más.

Otra característica de esta forma de trabajo es que todo gira en torno al desktop. Esto significa que el centro de administración depende del desktop que se esté usando, ya que este determina qué aplicaciones se pueden utilizar, qué usuarios pueden acceder y a dónde. La capacidad de procesamiento de cada desktop es una de las causas principales del nivel de productividad que el usuario puede lograr.

La evolución de estos dispositivos se caracterizó por proveer al mercado de equipos

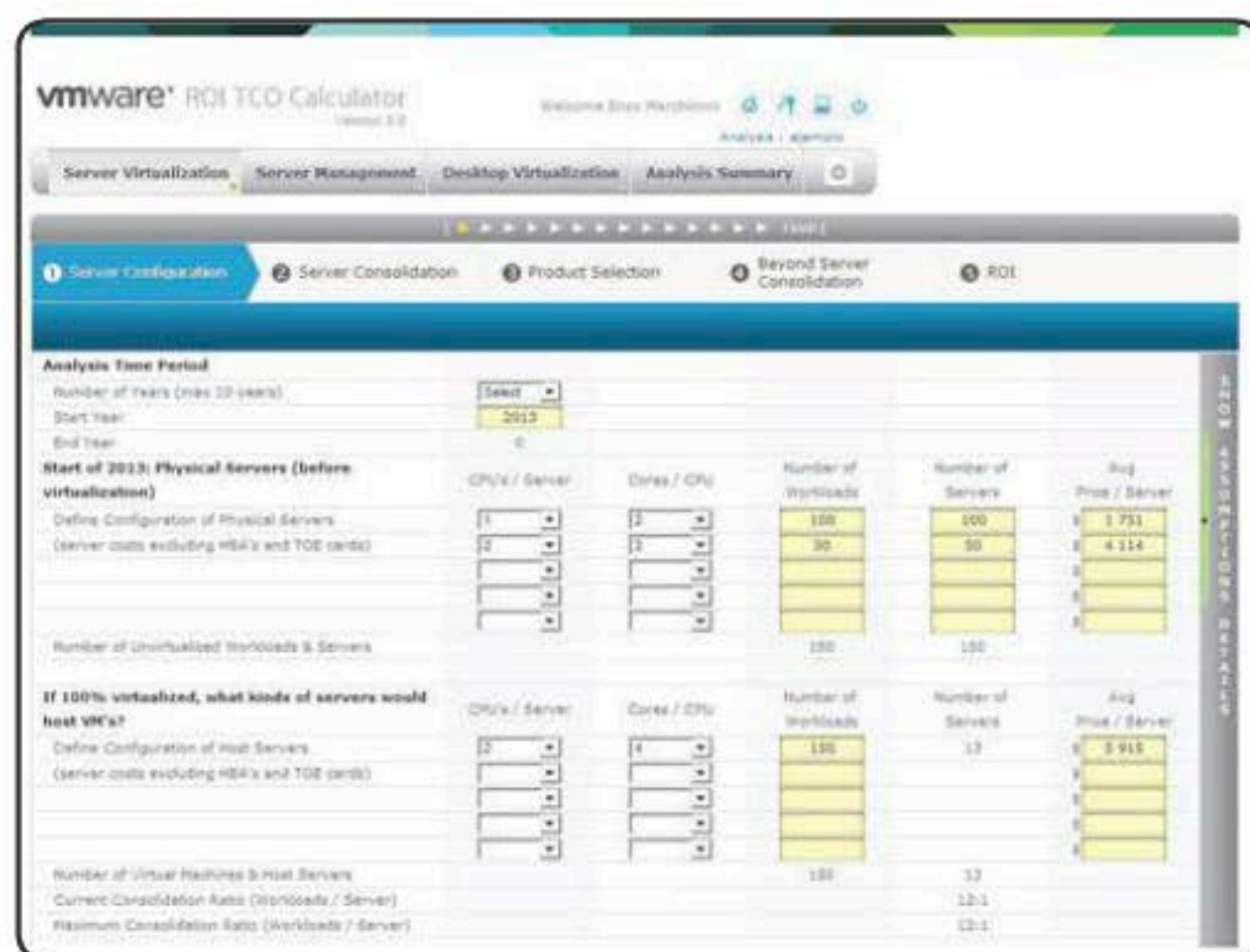


Figura 7. En el sitio oficial de VMware, encontramos una calculadora para poder obtener el retorno de la inversión.

más poderosos, pequeños y de menor costo, a la vez que generó dependencia al usuario y a su productividad.

En la actualidad, las empresas medianas y grandes cuentan con un departamento de IT propio o tercerizado, cuya área de soporte está dividida, principalmente, en soporte a infraestructura y soporte a usuarios. Esta última atiende problemas referidos a la falla de los equipos, el uso de las aplicaciones y la migración de datos por recambio tecnológico, que generan que el

usuario no pueda trabajar normalmente hasta que sean resueltos.

El concepto aplicado al desktop va mucho más allá porque, si bien el hecho de virtualizar es en esencia el mismo, involucra componentes que, históricamente, estuvieron fuera del datacenter y que tratan con problemáticas completamente diferentes. Estamos hablando de un cambio aún mayor que la virtualización en sí misma, y que abarca áreas tan disímiles como son el usuario final y el

THIN CLIENT

Un thin client es un dispositivo con un sistema operativo especialmente diseñado para permitir que el usuario se conecte a un sistema de terminal, como, por ejemplo, Terminal Services de Windows, Citrix y VMware View.

datacenter, entre otras.

VMware View permite que el concepto de desktop sea independiente del hardware a partir de varios componentes: la **virtualización del desktop**, la **paquetización de aplicaciones** y la posibilidad de conectarse al entorno de trabajo cada vez desde más **dispositivos**.

La arquitectura de VMware View cambia radicalmente el concepto de la infraestructura utilizada hasta hoy, al mejorar cada aspecto y simplificar no solo la experiencia del usuario, sino también la seguridad, la performance, la disponibilidad y la resolución de problemas asociados al uso diario del desktop y sus aplicaciones.

La arquitectura puede separarse en tres niveles:

- La **infraestructura virtual**, que aloja los desktops virtuales.
- El **View Connection Server**, que establece el vínculo entre el usuario y su desktop.
- Los **dispositivos**, que pueden utilizarse dentro de la empresa y fuera de ella a través de un vínculo para acceder a la solución.

Vamos a profundizar el concepto asociado a cada nivel para entender con claridad el funcionamiento de la solución y las enormes ventajas que proporciona con respecto a la solución tradicional de desktops físicos.

INFRAESTRUCTURA VIRTUAL

Este nivel se ocupa de almacenar y ofrecer los desktops virtuales para los usuarios. El encargado de hacer esto no es otro que **vSphere**, el mismo que nació para crear la infraestructura virtual para servidores.

Dependiendo del tipo de licenciamiento utilizado, podremos contar con diferentes niveles: de alta disponibilidad, balanceo de carga, fault tolerance, switches distribuidos, etc.

El licenciamiento llamado **add-on** sirve cuando se quiere utilizar una infraestructura virtual existente e incluye solo las conexiones al View Connection Server, por lo que las funcionalidades a este nivel dependerán de lo que ya se dispone para los servidores virtuales.

El licenciamiento llamado **bundle** incluye tanto las licencias para establecer las conexiones



APAGAR LAS CONEXIONES DE RED

Cuando terminamos de hacer la copia, es aconsejable encender el equipo sin conexión a la red, configurar las placas de red tal como estaban en el servidor físico, verificar las aplicaciones y revisar cualquier otra cuestión relacionada.

como un vCenter sin límites (que permite solo crear máquinas virtuales de tipo desktop) y todas las licencias de tipo Enterprise Plus que se consideren necesarias para servir a los desktops virtuales de la solución.

El licenciamiento de la solución se define por **conexión concurrente**, y no, por usuario. Esto

quiere decir que, si en una solución existen 300 usuarios pero se conectan 150 en forma concurrente, solo se precisarán 150 licencias de VMware View.

La comunicación entre este nivel y el View Connection Server se realiza utilizando vCenter, en donde también se activan funcionalidades

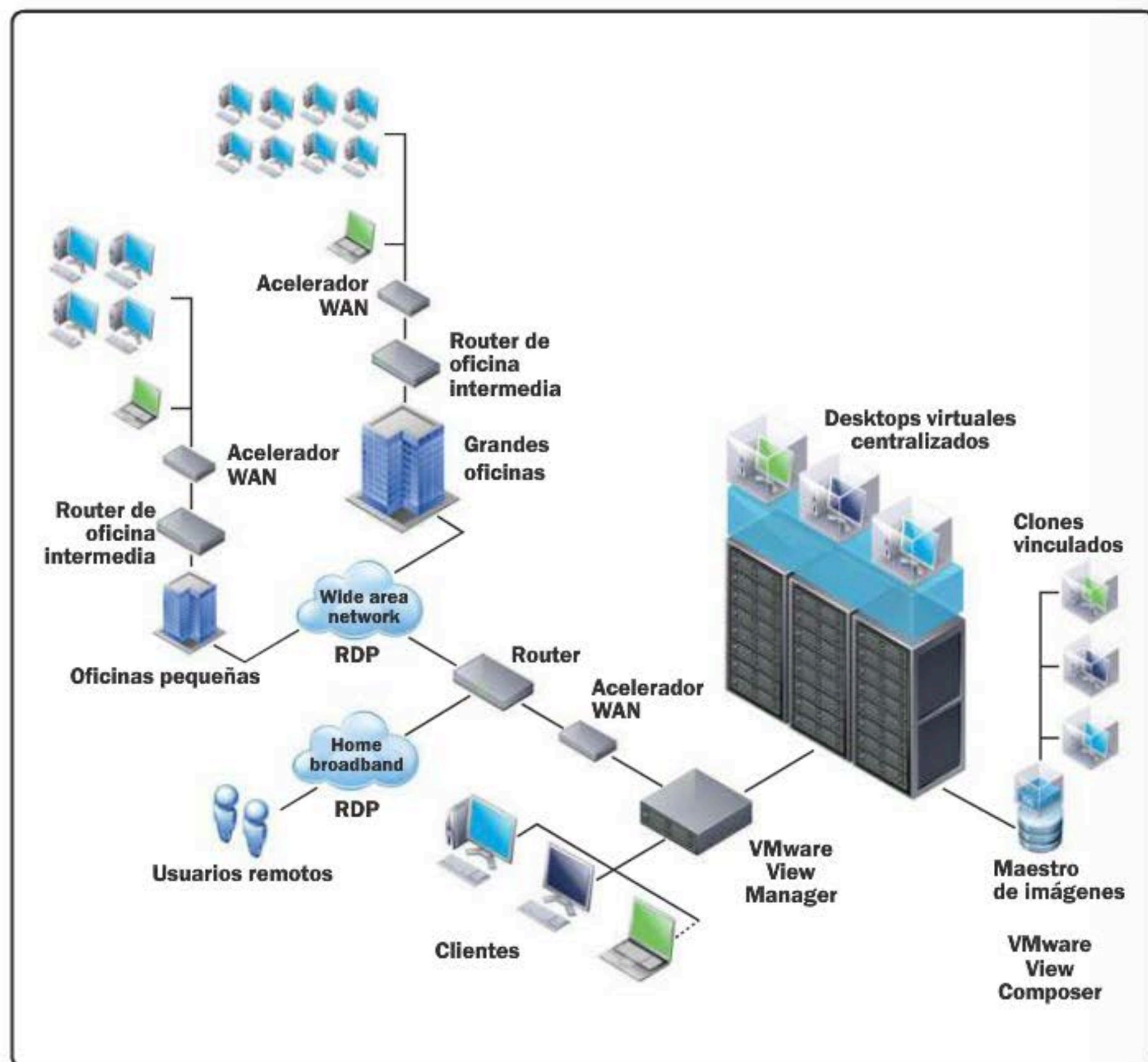


Figura 8. Infraestructura de VMware View que muestra las opciones de comunicación y los niveles de la arquitectura.

avanzadas, como **Composer**, de la que hablaremos más adelante en este capítulo.

Funcionalidades como generación de snapshots, clonación, pool de recursos y organización por carpetas son utilizadas para que la solución de virtualización de desktops funcione como se espera, más allá de que, para el usuario, sea completamente transparente.

El diseño de la infraestructura es una tarea clave en esta solución; incluso, tal vez, más necesaria que la virtualización de servidores. La capacidad de consolidación de desktops virtuales es mayor por servidor, y una caída del servicio o un problema de performance afectará notablemente a una gran cantidad de usuarios.

Por lo contrario, una infraestructura bien diseñada generará un entorno de enorme rendimiento y alta disponibilidad, para ofrecer a los usuarios una gran experiencia al utilizar la plataforma y, así, mejorar la productividad y minimizar los incidentes de soporte.

VIEW CONNECTION SERVER

Posee cuatro roles diferentes que pueden ser utilizados o no, dependiendo de la arquitectura

de la solución que se quiera implementar: **View Connection Server**, **View Replica Server**, **View Security Server** y **View Transfer Server**.

View Connection Server es a VMware View lo que vCenter es a vSphere. Este componente activa todas las funcionalidades de la solución, valida a cada usuario que quiere acceder a su desktop virtual, y se encarga de que este acceda a la **vm** (**virtual machine** o máquina virtual) correcta utilizando el protocolo de comunicación apropiado y aplicando las políticas previamente definidas. Se debe instalar en un servidor separado de otras funciones y es la pieza clave de la solución.

DISPOSITIVOS

Cualquier dispositivo que ejecute el agente View puede acceder a conectarse al View Connection Server para trabajar con el desktop virtual que le es asignado al usuario. Cuando se inicia el cliente de View, este se conecta al **Connection Server**, que espera un usuario y una contraseña para ser validado, tal como si nos estuviéramos logueando desde una PC.

Dependiendo de quién sea el usuario, se le presenta uno o varios pools de desktops



VIEW CONNECTION SERVER

Es un componente también llamado broker de conexión. Se encarga de validar cada intento de conexión de los usuarios de VMware View para asegurar que están autorizados a utilizar la solución.

para acceder. Cuando el usuario selecciona el pool, automáticamente es logueado al desktop virtual que le corresponde.

VMware View está siendo adoptado con la misma velocidad que la virtualización de servidores, por lo que, hoy en día, existen muchas formas de acceder a nuestro desktop virtual: utilizando una PC o una notebook, con Windows, Linux o Mac; teléfonos con Android o Mac OS; una tablet con Android o un iPad, y thin clients. Incluso, hay sistemas operativos diseñados para ser instalados en PCs o notebooks, que los convierten en thin clients.

Una vez más, notamos la relevancia con el

origen de la virtualización, ya que los thin clients nacen con el concepto de terminales usadas para que los usuarios trabajen conectados a los mainframes, de donde surgió la virtualización.



RESUMEN

En este capítulo conocimos los distintos jugadores del mercado de la virtualización, las empresas y los diferentes sistemas que existen. También vimos la virtualización de servidores y escritorios, y trabajamos sobre la solución de VMware View para escritorio.

Capítulo 3

VMware como herramienta de virtualización

Veremos por qué utilizar VMware como herramienta de virtualización y los detalles de su infraestructura.

Por qué utilizar VMware

Elegimos VMware entre todas las posibilidades del mercado porque es una empresa que a lo largo de su vida ha sido sólida en su comportamiento, respetando la compatibilidad de los productos, crecimientos y roadmaps, y hasta ha modificado su interacción con los usuarios.

Como una muestra de esto, durante el año 2012 ocurrió algo inesperado, inédito para VMware y para toda la industria. Con la nueva versión de 5.0 de vSphere, VMware pretendía cambiar el modelo de licenciamiento de cada host. El cambio era muy brusco, y la comunidad de usuarios alrededor de todo el mundo se hizo escuchar. La empresa tuvo que dar marcha atrás con sus cambios y rediseñar el licenciamiento una vez más.

Desde el punto de vista de los usuarios, VMware posee una gran comunidad, integrada por personas apasionadas por sus productos, que buscan cómo resolver los problemas de distintas formas y comparten las soluciones en blogs, redes sociales y foros. Entre ellos, hay expertos licenciados, como venía acostumbrando Microsoft al mercado, y muchos otros que no lo son, pero que saben muchísimo y hacen crecer esta comunidad planteando problemas y soluciones de igual manera.

VMware ha ganado en el cuadrante Gartner por varios años consecutivos en el mercado de

virtualización y aún lo sigue haciendo. Como sabemos, fue la pionera en virtualización en x86. Microsoft comenzó a experimentar 10 años más tarde al igual que muchas otras empresas. La virtualización fue solo el primer paso, ya que ha creado un ejército de aplicaciones arriba de esta arquitectura para dar más soporte, inteligencia y dinamismo a toda la infraestructura.

EL FUTURO CERCANO

En la actualidad, VMware está encaminada hacia el **cloud computing**; si bien allí tiene varios competidores creemos que está haciendo las cosas muy bien al igual que lo hicieron con la virtualización.

En el campo de la infraestructura, donde se busca armar un servicio o **SaaS (Softwares as a Service)** o infraestructura como servicio), tienen un gran competidor: **Amazon**. Esta empresa fue la primera en incursionar en la computación en la nube y se encuentra muy avanzada.

Por eso, varios arquitectos y directivos de Amazon y VMware han formado una gran empresa, llamada **Nimbula**, que ofrece nubes privadas. VMware seguramente será una gran jugadora dentro de estos proyectos. Debemos estar preparados y comenzar por estudiar estas herramientas y su mundo primero.

Por todas estas razones y porque el 90% del mercado ha tomado a VMware como su motor de virtualización, es que la elegimos como herramienta para desarrollar en este libro.



Figura 1. Hay varias opciones de herramientas en el sitio de VMware para investigar y probar.

A continuación, explicaremos las posibilidades que nos ofrece con su arsenal de aplicaciones.

Infraestructura de VMware

Si bien VMware brinda una gran diversidad de soluciones de virtualización, en esta obra nos centraremos en la solución para servidores. Esta está formada por varios productos, que conoceremos a continuación.

VMWARE WORKSTATION Y VMWARE PLAYER

VMware Workstation y VMware Player se usan en ambientes pequeños y de prueba.

Hace tiempo, Player se utilizaba para correr una única máquina virtual. Permitía utilizar otro sistema operativo, pero no crear una máquina virtual desde cero ni modificarla. A partir de la versión 3.1, es posible crear máquinas virtuales, modificarlas, utilizarlas al mismo tiempo si abrimos varias instancias, etcétera, y siempre con licencias gratuitas. Actualmente se encuentra en la versión 5.

Workstation es un poco más avanzado. Alrededor de octubre de 2010, VMware liberó su licencia, así que podemos utilizarlo de forma gratuita también. Hace un mejor uso y administración del hardware y trae más funcionalidades que Player, por ejemplo, los snapshots para tomar una imagen congelada de un estado de nuestras máquinas virtuales (más adelante veremos los detalles). Además, podemos realizar aplicaciones para el ambiente virtual, ya que se integra con Visual Studio, Eclipse y otros entornos de desarrollo. Para la enseñanza es muy apropiado; podemos armar un ambiente de servidores virtuales para que los estudiantes los



VMWARE PLAYER EN VEZ DE XP MODE

Gran cantidad de personas recomiendan el uso de VMware Player en Windows 7 en reemplazo del Windows XP mode. VMware Player administra de mejor forma el acceso a la CPU y la memoria de la computadora.

utilicen en algún curso y, luego, volverlos a un estado anterior. Aunque posee características más avanzadas que Player, ambos tienen en común que, si se apagan, también lo hacen todas las máquinas virtuales que soportan.

ESXi

ESXi está orientado a los ambientes empresariales, tiene una mayor capacidad de resguardo para aplicaciones críticas y es el comienzo para escalar a la mejor opción de virtualización VMware vCenter.

Los servidores ESXi traen un sistema operativo creado por VMware para uso exclusivo en virtualización. Este sistema está basado en Linux, adaptado y personalizado por investigadores y grupos de desarrolladores de VMware. Las licencias que utiliza son gratuitas.

La consola de servicio en el ESXi fue extraída, y esto le brinda más seguridad porque concentra la administración por consola en otro servidor, como lo requieren ciertos estándares. No se puede acceder por la Web, y todos los errores que la consola de servicio podría llegar a tener fueron eliminados junto con sus 2 GB de información.

Su antecesor traía la consola, lo que lo hacía muy inseguro, razón por la cual dejaron de fabricarlo y soportarlo. De esta manera, la actualización del ESXi es más rápida. Estos sistemas solo funcionan en servidores con capacidad de virtualización a nivel microprocesador.

ESXi se habilita para ser contactado por un cliente de conexión llamado vClient, que se conecta con el servidor de forma remota. En cada servidor ESXi, podemos crear varias máquinas virtuales. La cantidad y el límite dependen de los recursos físicos del servidor, en especial, de la cantidad de memoria RAM, el espacio en disco y la capacidad del microprocesador. Seguramente, vamos a instalar más de un servidor ESXi, cada uno con distintos recursos para compartir y diferentes servidores virtuales. Todos ellos pueden administrarse en conjunto si instalamos VMware vCenter. Este sistema necesita una base de datos y debe ser instalado sobre un servidor de plataforma Windows. Más adelante conoceremos sus detalles.

MÁS HERRAMIENTAS

Hasta ahora vimos que contamos con VMware Player, VMware Workstation, los servidores ESXi



COMPATIBILIDAD CON VMWARE

En www.vmware.com/resources/compatibility/search.php, podemos comprobar la compatibilidad de los productos VMware con el hardware y los sistemas operativos que serán instalados en máquinas virtuales.

con sistema operativo propio VMkernel, VMware vClient para administración remota y también vCenter. Además, existen otras herramientas que conforman la infraestructura de la solución.

Una de las más importantes es VMware vCenter Converter, de la que hemos hablado en el **Capítulo 2**. Con ella, migramos máquinas virtuales entre plataformas y, también, virtualizamos servidores físicos.

Algunas otras herramientas interesantes que podemos destacar son VMware Tools, vCenter Update Manager, VMware vCenter Orchestrator y VMware Fusion.

VMware Tools integra una serie de características que se instalan en las máquinas virtuales: hardware virtual, drivers y conectores para el servidor que la contiene.

Índice de productos		
SECCIÓN DE GESTIÓN DE INFRAESTRUCTURA	SECCIÓN DE GESTIÓN DE APLICACIONES	SECCIÓN DE GESTIÓN DE SEGURIDAD
VMware vSphere	VMware vCenter Server	VMware vCenter Site Recovery Manager
VMware vCloud Director	VMware vCenter Orchestrator	VMware vCenter Lab Manager
Familia de productos VMware	VMware ACE	VMware vCenter Capacity IQ
vCenter	VMware Workstation	VMware vCenter Configuration Manager
VMware ESXi	VMware Player	VMware vCenter Converter
VMware vSphere Hypervisor (ESX)	VMware Fusion	
PRODUCTOS DE SEGURIDAD	PRODUCTOS DE MAC	SECCIÓN DE APLICACIONES
Familia de productos VMware	VMware Fusion	VMware vCenter Application Discovery Manager
vShield		VMware vCenter AppSpeed
VMware vShield App		VMware Studio
VMware vShield Edge		
VMware vShield Endpoint		
OTROS	PLATAFORMA DE APLICACIONES	
VMware Data Recovery	VMware vFabric 3.0 Server	
VMware vCloud	VMware vFabric Hyperic	
VMware vCloud Planner		
Cloud Foundry 100N		
VMware Compliance Checker		
SUSE Linux Enterprise Server for VMware		
	SECCIÓN DE ACTIVIDAD DE TI	
	VMware vCenter Chargeback	
	VMware Service Manager	

Figura 2. En el sitio de VMware, hay varias herramientas que podemos disfrutar sin restricciones.

Con vCenter Update Manager, podemos actualizar el servidor vCenter, los servidores ESXi y las VMware Tools en cada máquina virtual.

VMware Orchestrator lo utilizamos para automatizar tareas que realizamos en forma

PRODUCTOS DESTACADOS DE VMWARE

HERRAMIENTAS

DESCRIPCIÓN

VMware Player

Se utiliza para crear máquinas virtuales en testing, que corren en forma individual. Gratis.

VMware Workstation

Podemos crear varias máquinas virtuales en nuestro escritorio, obtener snapshots y clonar equipos. La licencia es paga.

ESXi

Su licencia es gratuita, es el hypervisor de VMware.

VMware vClient

Se utiliza como cliente de escritorio para contactarse con el servidor ESXi. Viene incluido en las versiones de ESXi, Virtual vCenter y vSphere.

Tabla 1. VMware cuenta con una gran variedad de soluciones para los servidores.

manual. Hay distintas opciones para elegir, que son de gran ayuda para acortar tiempos.

VMware Fusion, en su actual versión 5, es usado para hacer funcionar máquinas virtuales en plataformas Mac de Apple. La última novedad es que podemos tener Windows 8 corriendo dentro una Mac. A continuación, veremos un resumen de todas las herramientas nombradas.

Existen otras herramientas que vamos a ir nombrando más adelante, a medida que avancemos con los conocimientos de las herramientas básicas.

VMware brinda una gran diversidad de soluciones de virtualización

Cómo instalar un ESXi

Como primer paso, deberemos bajarnos el archivo **.ISO** y grabarlo en un DVD o CD, dependiendo de la versión. Si tenemos una consola ILO remota, también lo podemos montar desde allí. Es muy sencillo de instalar. Solo colocamos el sistema operativo en la unidad de CD o DVD y seguimos los pasos que se detallan a continuación.

Vamos a mostrar la instalación conectados al servidor desde una consola física remota al centro de cómputos; no es una ILO, pero se le parece bastante. También lo podemos instalar conectados directamente al equipo con un monitor, teclado y mouse.

PASO A PASO /1 Instalar un servidor ESXi

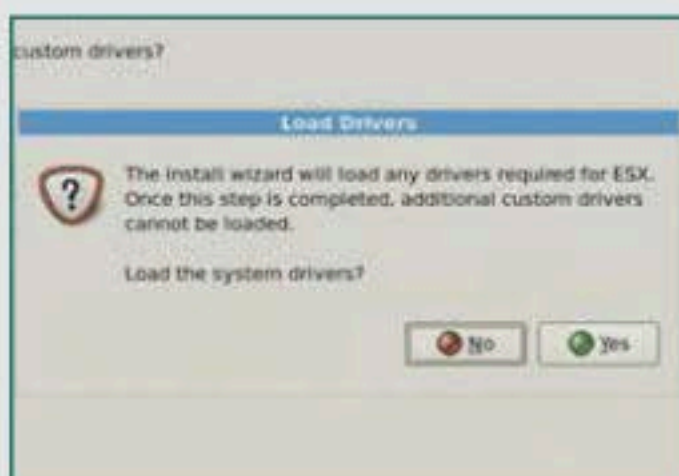
1



Ponga en funcionamiento el servidor con el CD o DVD en la unidad lectora. Todos los datos del disco duro se borrarán. Haga clic en **Next**.

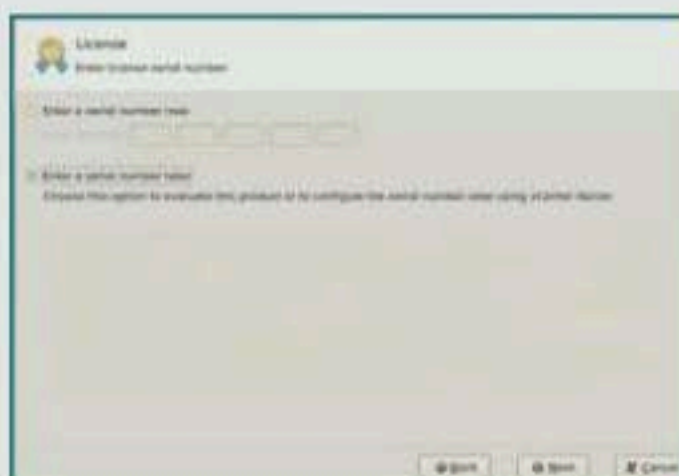
PASO A PASO /1 (cont.)

2



Luego de confirmar el contrato de licencia y elegir el lenguaje del teclado, pulse **YES** en la ventana que le pregunta si quiere cargar los controladores en el equipo.

3



Después de cargar los drivers, ingrese los datos de las licencias si los tiene, o elija la opción **Enter a serial number later**. Haga clic en **Next**.

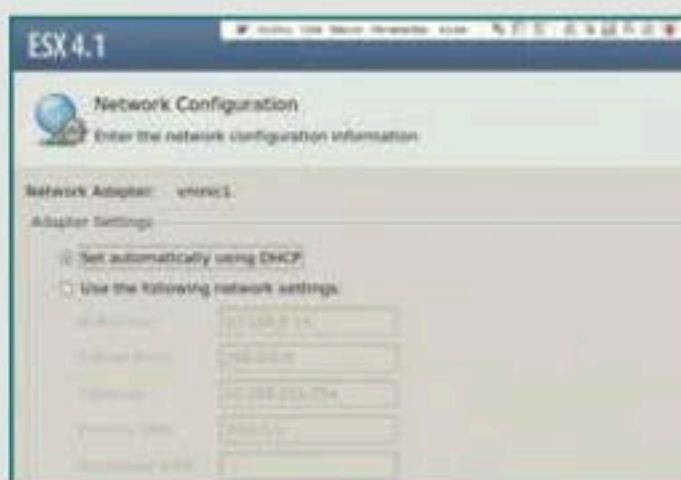
4



En este paso, elija la placa de red con la que trabajará. Figurarán en verde las que estén conectadas con un cable. Elija la correcta y haga clic en **Next**.

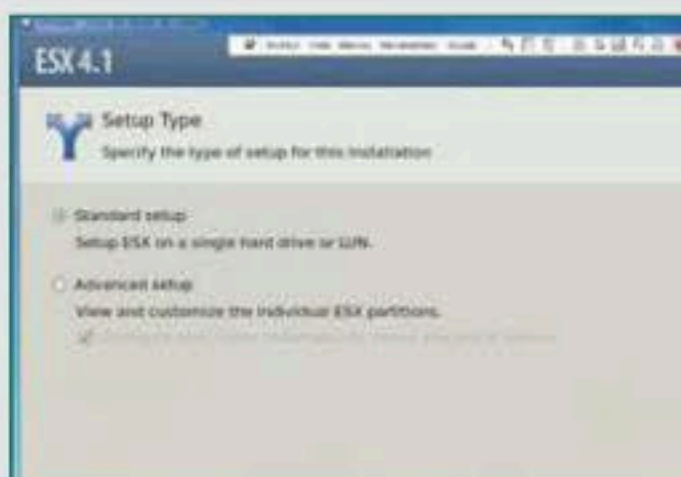
PASO A PASO /1 (cont.)

5



Ingresa la configuración de red para su equipo. Luego, haga clic en **Test these settings** para que la configuración de red tenga efecto. Pulse **OK** cuando se muestre en pantalla y, luego, el botón **Next**.

6



Elija la manera en que particionará los discos; estándar dividirá el disco en forma automática. Así quedará dividido el disco para el funcionamiento del ESXi. Pulse **Next**. Luego, acepte la distribución y oprima nuevamente **Next**.

7



Elija la zona horaria y pulse **Next**. A continuación, puede configurar la fecha manualmente o configurar un servidor NTP para sincronizar el tiempo para el servidor.

PASO A PASO /1 (cont.)

8



Debe elegir una contraseña para la administración e ingresarla en los campos **Password** y **Confirm Password**. Luego, pulse **Next**. Vea el resumen, oprima **Next** y comience la instalación.

9



Al finalizar, reinicie el equipo. Luego, entre a la consola de administración de línea de comandos oprimiendo **ALT + F1** e ingrese el usuario una vez que el equipo haya terminado de iniciar.

Así tendremos nuestro primer ESXi instalado. De la misma manera, podremos instalar la cantidad de servidores que necesitemos.

A medida que crece una infraestructura, la administración de todos los servidores sin perder un detalle de licencias, de rendimiento, de configuración se volverá muy engorroso, pero VMware nos da la posibilidad de administrarlos todos juntos con vCenter.

Crear una máquina virtual

En el capítulo anterior aprendimos a virtualizar un servidor, pero también es posible crear una máquina desde cero. Las máquinas virtuales pueden crearse desde una migración o desde la consola de administración. Solo debemos tener en cuenta las capacidades que necesitamos

y las disponibles en el servidor físico. VMware siempre nos va a alertar si esto no es posible o si elegimos alguna configuración que no se pueda manejar. Es importante tener en cuenta varias opciones antes de pasar a la tarea de crear la máquina virtual:

- Cómo configurar las placas de red virtuales y cuántas necesitamos.
- El tamaño del disco virtual y dónde lo vamos a alojar.

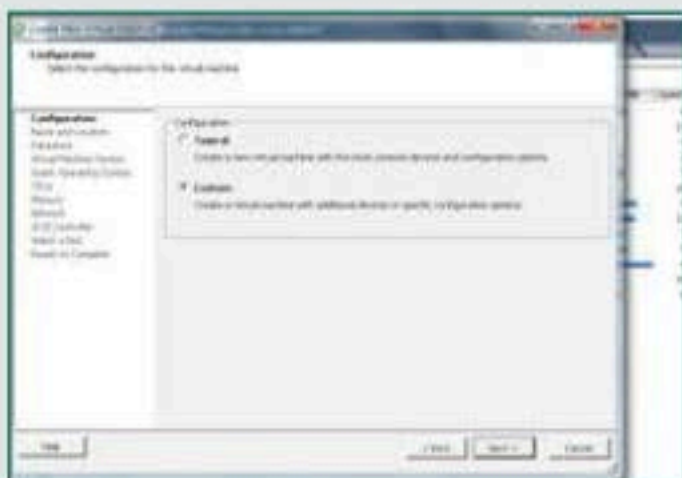
- Las necesidades de memoria RAM del equipo que vamos a crear para comparar con lo que nos puede ofrecer el servidor físico.

No hay mejor forma de aprender que probando. Luego, podremos eliminar la máquina que no utilicemos. La creación de una máquina virtual en ESXi es similar a como se hace en las otras opciones de virtualización. Debemos hacer un clic derecho sobre el servidor y seguir las opciones. A continuación, veremos cómo crear una máquina virtual en un servidor ESXi.

PASO A PASO /2

Crear una máquina virtual en un ESXi

1



Abra la consola del ESXi conectándose con el vClient. Después, ubíquese con el mouse sobre el servidor ESXi y haga un clic derecho. Elija **New Virtual Machine** y luego el modo **Custom**.

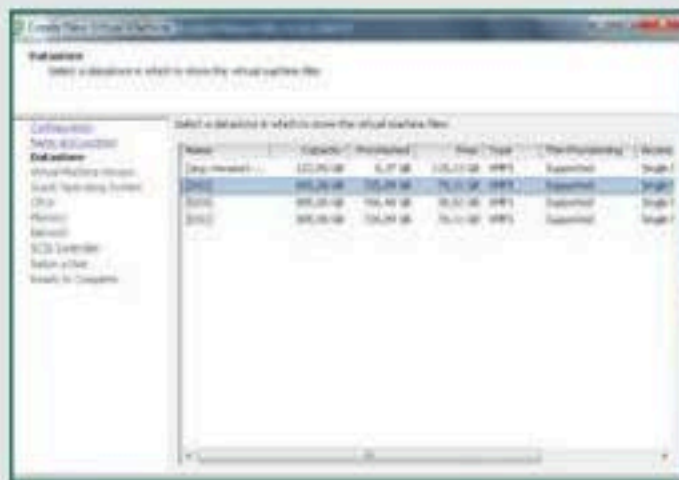


INSTALAR VMWARE TOOLS EN CADA MÁQUINA VIRTUAL

Si instalamos las herramientas, no distinguiremos si estamos en el servidor virtual o en nuestro propio escritorio. La velocidad de intercambio de información entre la máquina virtual y la física aumenta notablemente.

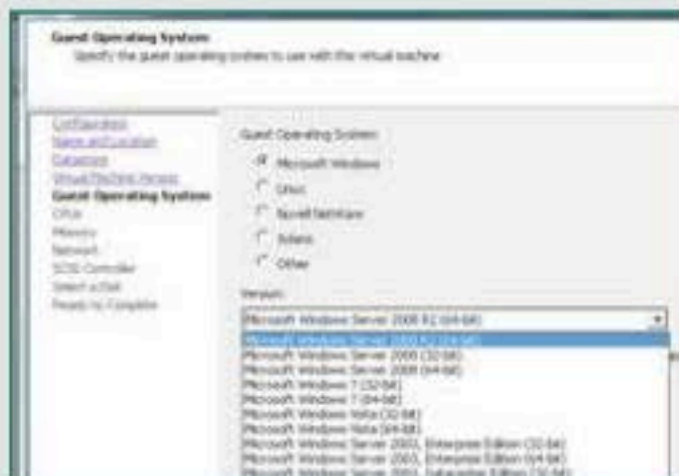
PASO A PASO /2 (cont.)

2



Ingrese un nombre, pulse **Next** y, en el paso siguiente, elija dónde va a ubicar los archivos de la máquina virtual. Seleccione la unidad de almacenamiento correspondiente.

3



Seleccione una versión de máquina virtual, puede ser 4 para ESX 3.5 o anteriores, o versión 7 a partir del ESX 4.0. Oprima **Next>** y, luego, elija el sistema operativo para instalar del listado que aparece en pantalla.

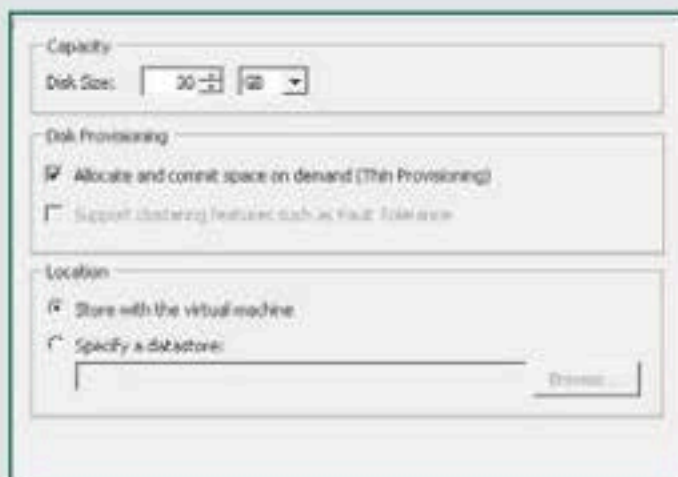
4



Indique la cantidad de microprocesadores virtuales que va a asignar, la cantidad de memoria, el tipo y cantidad de placas de red virtuales. Elija **VMXNET3** para aprovechar todos los recursos de la virtualización.

PASO A PASO /2 (cont.)

5



Debe adoptar un controlador SCSI y luego configurar un nuevo disco duro virtual o utilizar alguno guardado. Pulse **Next>**. Ingrese un tamaño de disco y elija una forma de entregar el espacio del disco físico. Seleccione **Thin Provisioning** para seguir.

6



Revise el resumen de la creación y cree la máquina virtual mediante el botón **Finish**. Luego, diríjase a la consola, haga clic derecho en la nueva máquina virtual, elija **Power** y, luego, **Power on** para encenderla.

Todas las tareas de poner en producción un servidor las hicimos tan solo en 5 minutos. Notaremos una gran aceleración con respecto a un servidor físico.

Una vez que creamos el servidor virtual, ya estamos en condiciones de instalar el sistema operativo para el servidor. El procedimiento es sencillo. En las opciones de cualquiera de las consolas de VMware, podremos mapear tanto una imagen ISO como una unidad de disco compacto para

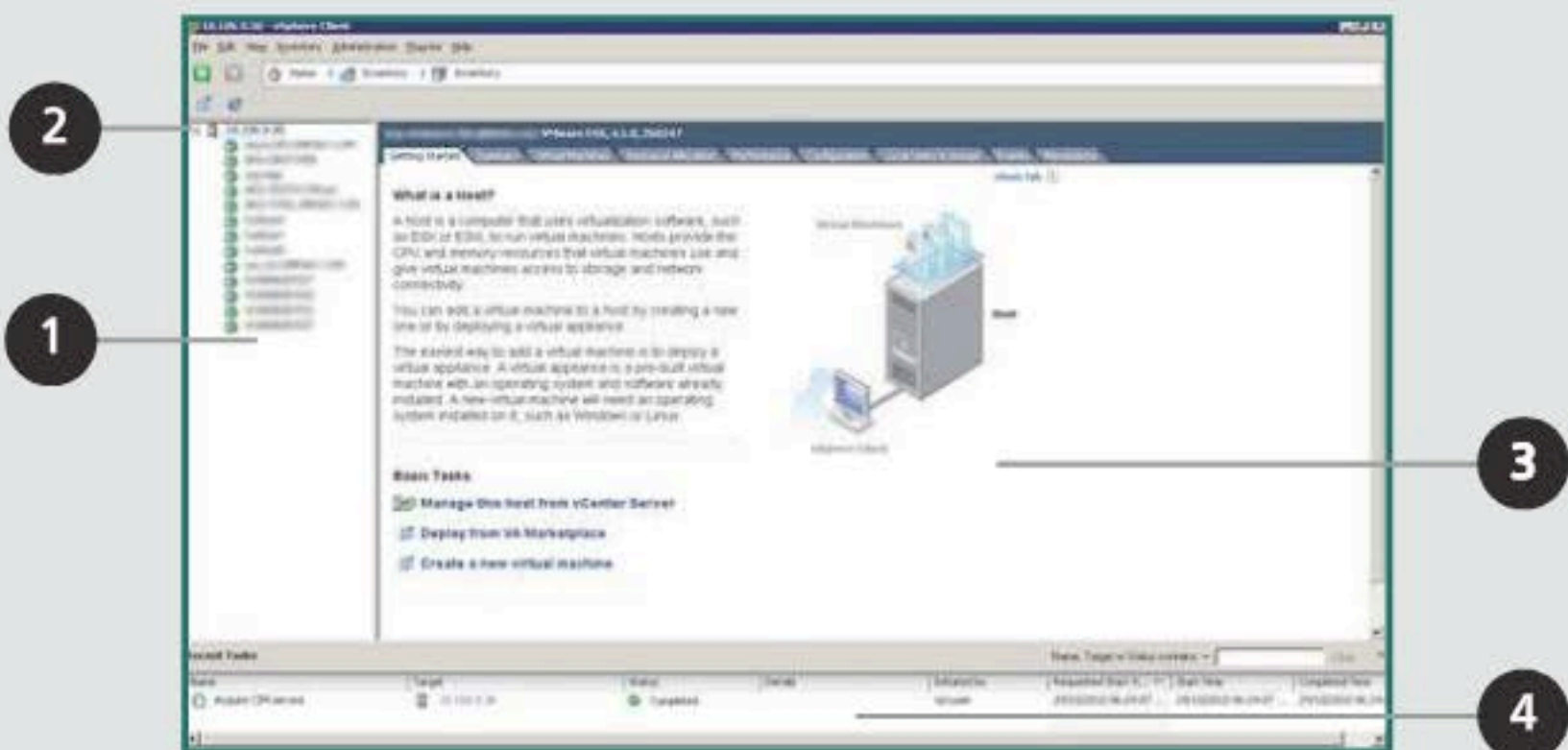
proceder a la instalación. Lo único que hay que tener en cuenta es que debemos mapearla una vez que el servidor virtual está encendido. Lo que conviene hacer en estos casos es seleccionar la entrada al BIOS no bien encendemos el servidor virtual y, recién entonces, mapear el disco de instalación. Un detalle de esta configuración es que, al reiniciar el equipo virtual, el disco se desconectará automáticamente, por lo que, si necesitamos seguir una instalación, deberemos volver a configurar la unidad de disco compacto.

Consola gráfica de administración ESXi

La consola gráfica es otra forma de administración del ESXi, con la que podremos hacer muchas de las operaciones que realizamos desde

una línea de comandos, pero de manera gráfica. Se compone de tres grandes grupos de información; por un lado, el servidor ESXi y las máquinas virtuales; por otro lado, los detalles del servidor ESXi y de cada máquina virtual; más abajo, vemos la lista de tareas que se van realizando a medida que van pasando. No importa el usuario, se informan todas las tareas realizadas en el servidor.

GUÍA VISUAL /1 Sectores de la consola gráfica



1. **Servidores virtuales:** en este apartado, se ve el detalle de los distintos servidores virtuales que tenemos.
2. **Servidor ESXi:** el servidor ESXi se identifica por IP. Este alojará los distintos servidores virtuales.
3. **Detalles:** en la parte central de la pantalla, veremos distintas solapas con información detallada de la configuración, recursos, rendimiento, usuarios, eventos y permisos del servidor ESXi. Posicionándonos en cada servidor virtual, conoceremos sus detalles.
4. **Tareas:** en el sector inferior, podemos observar las tareas a medida que se vayan sucediendo.

La consola mostrada en la **Guía visual** anterior pertenece al cliente de escritorio para VMware llamado **vClient**.

VMware vCenter

Ya sabemos cómo administrar un servidor ESXi, pero ¿qué pasa si tenemos dos, tres o diez servidores? ¿Cómo los administramos? La solución de VMware para este caso es **VMware vCenter**. Con esta herramienta, podremos centralizar toda la administración de varios servidores ESXi en una sola consola, compartir recursos, comparar estadísticas y también mover máquinas virtuales entre los distintos servidores con mínima pérdida de datos. Veremos una introducción, conoceremos cómo implementarlo y cómo clonar servidores.

DESCRIPCIÓN Y CARACTERÍSTICAS

vCenter es sin dudas una de las mejores soluciones para centralizar la administración del ambiente virtual. Además, permite la automatización de ciertas configuraciones, la optimización de recursos y una gran capacidad para

incrementar la alta disponibilidad de los servidores. Entre sus mejores beneficios encontramos:

- La posibilidad de establecer prioridades de negocios de manera predefinida para volcar los recursos de hardware hacia donde lo demande la empresa, en el momento que lo necesite. Para esto utiliza **VMware DRS**.
- Permite migrar máquinas entre distintos nodos ESXi, sin pérdida de datos, sin reinicios y sin necesidad de mantenimiento. Esto lo realiza mediante **VMware Vmotion**.
- Independización de las aplicaciones del hardware y de las operaciones de sistemas, utilizando **VMware HA**.

Para poder activar estas características de HA y DRS, y hacer Vmotion entre los distintos nodos que queremos administrar con vCenter, estos deben tener las mismas características de hardware y las mismas conexiones de red. A su vez, deben compartir una unidad de almacenamiento. Los archivos de los servidores virtuales se almacenarán en esa unidad compartida, y solo se tomarán de los nodos los recursos de microprocesador y memoria RAM.



THIN PROVISIONING

Configurando los discos con la opción **Thin Provisioning**, nos aseguramos el máximo aprovechamiento del almacenamiento. A medida que la máquina lo necesite, se le va otorgando más espacio en disco.

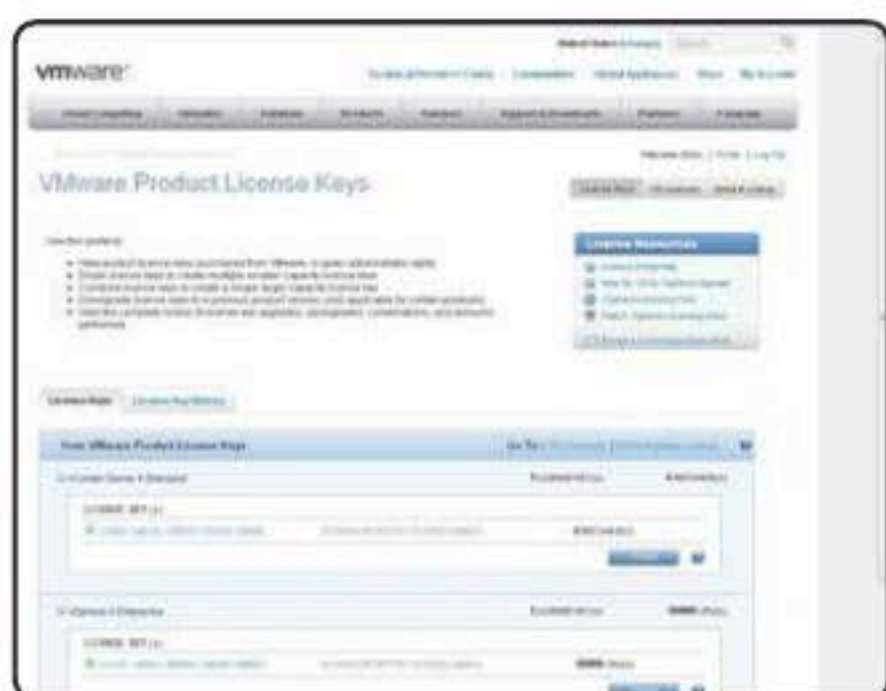


Figura 3. Una vez que entramos al portal de VMware con nuestras credenciales, vemos el sitio de licencias.

De esta manera, podemos administrar varios ESXi y contar con varios clusters administrados, y, en cada uno de ellos, tendremos equipos con las mismas características, como dijimos anteriormente.

Por otro lado, vCenter trae una característica de HA que permite que los equipos tengan el menor tiempo de bajada posible. Si se cae un nodo, si se rompe o deja de funcionar, las máquinas virtuales que aloja se reiniciarán y aparecerán distribuidas entre los otros nodos que conformen el cluster. Por esta razón, los nodos de un mismo cluster deben ser iguales.

Para acceder a la consola, nos conectamos con el vClient, al igual que lo hacíamos en un nodo ESXi, pero esta vez en el VMware vCenter. Para esto, debemos ser usuarios administradores del servidor o podemos administrar los permisos de forma más avanzada integrando el vCenter con **Active Directory**. Al poner productivo un servidor, obtendremos gran velocidad de trabajo, ya que podremos realizar templates (plantillas de servidores), clonar (copiar servidores) y crear un servidor virtual con unos pocos clics.

Mediante una API de programación llamada **VMware Infrastructure SDK**, vamos a integrar aplicaciones y crear las nuestras mediante el consumo de servicios web.

DETALLES DE LA IMPLEMENTACIÓN

Para la implementación, podemos usar un servidor virtual o uno físico. Es aconsejable tener como resguardo un servidor fuera de la **granja virtual**, un servidor que sea físico y, más tarde, virtualizarlo. Entonces, tendremos el servidor físico funcionando y el virtual apagado.

vCenter trabaja con dos bases de datos, una para la administración de los servidores virtuales y otra para la administración de los parches.



ALARMAS

En vCenter, existe la posibilidad de configurar alarmas centralizadas. Esto es más productivo que tener una definición de alarmas para cada nodo. Podremos monitorear el uso de discos, de CPU, de caída de servidores, de movimientos de nodo y de caídas de red.

La consola mostrada en la **Guía visual** anterior pertenece al cliente de escritorio para VMware llamado **vClient**.

VMware vCenter

Ya sabemos cómo administrar un servidor ESXi, pero ¿qué pasa si tenemos dos, tres o diez servidores? ¿Cómo los administramos? La solución de VMware para este caso es **VMware vCenter**. Con esta herramienta, podremos centralizar toda la administración de varios servidores ESXi en una sola consola, compartir recursos, comparar estadísticas y también mover máquinas virtuales entre los distintos servidores con mínima pérdida de datos. Veremos una introducción, conoceremos cómo implementarlo y cómo clonar servidores.

DESCRIPCIÓN Y CARACTERÍSTICAS

vCenter es sin dudas una de las mejores soluciones para centralizar la administración del ambiente virtual. Además, permite la automatización de ciertas configuraciones, la optimización de recursos y una gran capacidad para

incrementar la alta disponibilidad de los servidores. Entre sus mejores beneficios encontramos:

- La posibilidad de establecer prioridades de negocios de manera predefinida para volcar los recursos de hardware hacia donde lo demande la empresa, en el momento que lo necesite. Para esto utiliza **VMware DRS**.
- Permite migrar máquinas entre distintos nodos ESXi, sin pérdida de datos, sin reinicios y sin necesidad de mantenimiento. Esto lo realiza mediante **VMware Vmotion**.
- Independización de las aplicaciones del hardware y de las operaciones de sistemas, utilizando **VMware HA**.

Para poder activar estas características de HA y DRS, y hacer Vmotion entre los distintos nodos que queremos administrar con vCenter, estos deben tener las mismas características de hardware y las mismas conexiones de red. A su vez, deben compartir una unidad de almacenamiento. Los archivos de los servidores virtuales se almacenarán en esa unidad compartida, y solo se tomarán de los nodos los recursos de microprocesador y memoria RAM.



THIN PROVISIONING

Configurando los discos con la opción **Thin Provisioning**, nos aseguramos el máximo aprovechamiento del almacenamiento. A medida que la máquina lo necesite, se le va otorgando más espacio en disco.

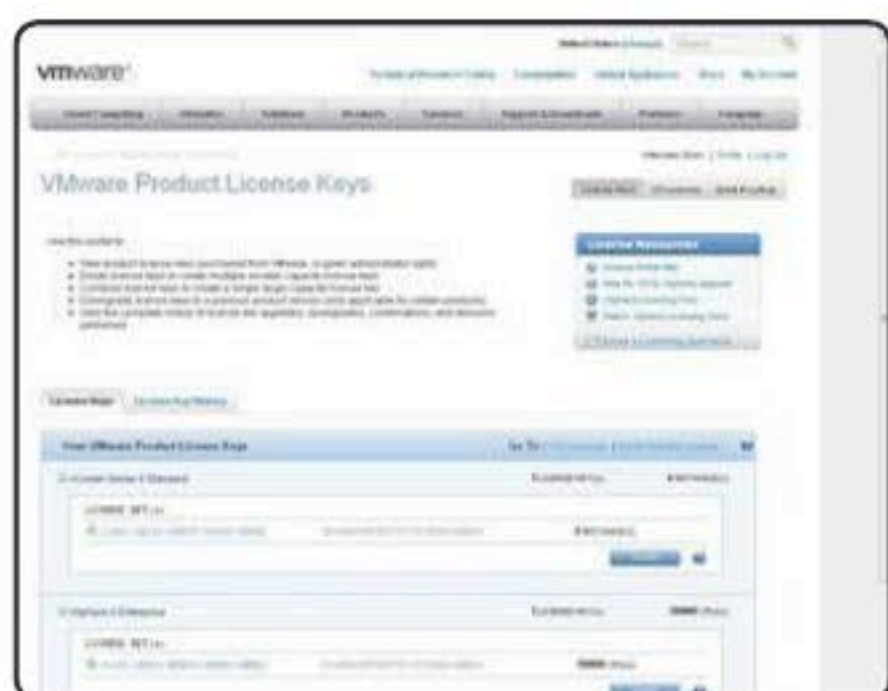


Figura 3. Una vez que entramos al portal de VMware con nuestras credenciales, vemos el sitio de licencias.

De esta manera, podemos administrar varios ESXi y contar con varios clusters administrados, y, en cada uno de ellos, tendremos equipos con las mismas características, como dijimos anteriormente.

Por otro lado, vCenter trae una característica de HA que permite que los equipos tengan el menor tiempo de bajada posible. Si se cae un nodo, si se rompe o deja de funcionar, las máquinas virtuales que aloja se reiniciarán y aparecerán distribuidas entre los otros nodos que conformen el cluster. Por esta razón, los nodos de un mismo cluster deben ser iguales.

Para acceder a la consola, nos conectamos con el vClient, al igual que lo hacíamos en un nodo ESXi, pero esta vez en el VMware vCenter. Para esto, debemos ser usuarios administradores del servidor o podemos administrar los permisos de forma más avanzada integrando el vCenter con **Active Directory**. Al poner productivo un servidor, obtendremos gran velocidad de trabajo, ya que podremos realizar templates (plantillas de servidores), clonar (copiar servidores) y crear un servidor virtual con unos pocos clics.

Mediante una API de programación llamada **VMware Infrastructure SDK**, vamos a integrar aplicaciones y crear las nuestras mediante el consumo de servicios web.

DETALLES DE LA IMPLEMENTACIÓN

Para la implementación, podemos usar un servidor virtual o uno físico. Es aconsejable tener como resguardo un servidor fuera de la **granja virtual**, un servidor que sea físico y, más tarde, virtualizarlo. Entonces, tendremos el servidor físico funcionando y el virtual apagado.

vCenter trabaja con dos bases de datos, una para la administración de los servidores virtuales y otra para la administración de los parches.



ALARMAS

En vCenter, existe la posibilidad de configurar alarmas centralizadas. Esto es más productivo que tener una definición de alarmas para cada nodo. Podremos monitorear el uso de discos, de CPU, de caída de servidores, de movimientos de nodo y de caídas de red.

Debemos tener espacio para estas bases en las unidades de almacenamiento. Estas pueden instalarse en el mismo servidor en donde tenemos el vCenter o en otro.

En caso que sea necesaria una actualización del vCenter, podemos crear backups y toda una serie de tareas de mantenimiento para el servidor, pero la experiencia dice que es más fácil instalar todo desde cero. Solo deberemos agregar los nodos nuevamente y configurar algunos elementos; la instalación será más limpia y funcionará mucho mejor. Además, nos ahorraremos gran cantidad de problemas de instalación de plugins, ya que solamente debemos volver a habilitarlos.

En el caso de realizar solo una actualización sobre el vCenter ya instalado, a veces los plugins no funcionan correctamente. Debemos tener un storage compartido para los nodos ESXi, que puede estar conectado a través de un canal de fibra o iSCSI.

PARTICULARIDADES DEL STORAGE COMPARTIDO

El storage compartido debe ser compatible con los productos de VMware, es decir, avalado en la planilla de compatibilidad. Si esto no es así, es posible que lo instalemos y configuremos correctamente y, luego, obtener fallas que aparecen y desaparecen. Un problema muy común en estas circunstancias es que los LUNS se pueden desconectar sin razón alguna. Los **LUNS**, básicamente, son las unidades de disco que nos dan los administradores de storage.

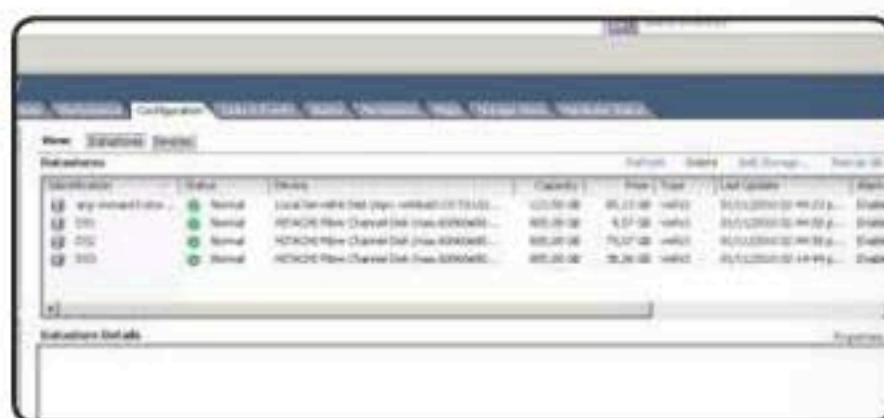


Figura 4. Una vez realizado el scan, figurará la nueva conexión en la consola.

Como primer paso entonces, al momento de definir un almacenamiento compartido debemos revisar el sitio de compatibilidad. Cuando ya lo hayamos definido, conectado y configurado en la consola del storage, hay que configurar los LUNS en los nodos ESXi. Vamos a tener que configurar los mismos LUNS para los mismos nodos en el mismo cluster. Podemos llegar a configurar más de un LUN para distintos clusters y luego, al crear un servidor virtual, elegir dónde almacenarlo.

En el caso de una conexión de fibra, solamente debemos conectar los cables al equipo e ir a la consola de administración. En la solapa de configuración vamos hasta **Storage** y allí oprimimos **Rescan All**, como vemos en la **Figura 5**. Una configuración un poco más avanzada sería configurar dos cables para un mismo LUN, con lo que tendríamos alta disponibilidad a nivel de disco. Esta es una de las mejores prácticas recomendadas.

CÓMO HACER UN CLUSTER

Los clusters agrupan nodos ESXi para balancear las cargas de las demandas de CPU y memoria. Todos los nodos que configuremos en un mismo cluster deben poder acceder a la misma unidad

PASO A PASO /3 (cont.)

3

Automation level

☐ Manual
vCenter will suggest migration recommendations for virtual machines.

☐ Partially automated
Virtual machines will be automatically placed onto hosts at power on and vCenter will suggest migration recommendations for virtual machines.

☒ Fully automated
Virtual machines will be automatically placed onto hosts when powered on, and will be automatically migrated to attain best use of resources.

Migration threshold: Conservative ——— Aggressive

Apply priority 1, priority 2, priority 3, and priority 4 recommendations.
vCenter will apply recommendations that promise even a moderate improvement to the cluster's load balance.

Seleccione las opciones de **DRS: Manual o Partially automated**, para que no se muevan automáticamente; **Fully automated**, para modo automático. Elija un modo de agresividad medio. Pulse **Next>**.

4

Power Management

DPM uses Wake-on-LAN, SPBE, or I/O to power on hosts. When using SPBE or I/O, configure SPBE or I/O separately for each participating host prior to enabling DPM. For all power on methods, test each standby for each participating host prior to enabling DPM.

Specify the default power management for the cluster:

☒ Off
vCenter will not provide power management recommendations. Individual host overrides may be set, but will not become active until the cluster default is either Manual or Automatic.

☐ Manual
vCenter will recommend evacuating a host's virtual machines and powering off the host when the cluster's resource usage is low, and powering the host back on when necessary.

☐ Automatic
vCenter will automatically execute power management related recommendations.

DPM Threshold: Conservative ——— Aggressive

Seleccione las opciones de **DPM**. En este caso, elija **Off** para desactivarlo. Pulse **Next>**.

5

Host Monitoring Status

ESX hosts in this cluster exchange network heartbeats. Disable this feature when performing network maintenance that may cause isolation responses.

☒ Enable Host Monitoring

Admission Control

Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

☒ Enable: Do not power on VMs that violate availability constraints

☐ Disable: Power on VMs that violate availability constraints

Admission Control Policy

Specify the type of policy that admission control should enforce:

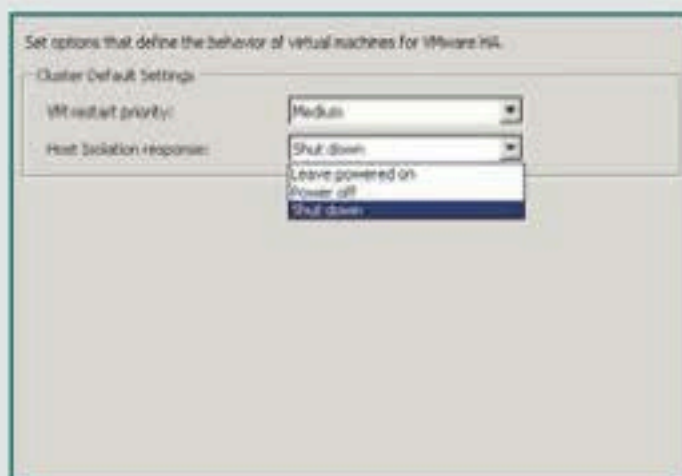
☒ Host failures cluster tolerates: 1

☐ Percentage of cluster resources reserved as failover spare capacity: 25 %

Habilite la opción de monitoreo de los hosts haciendo un clic en **Enable Host Monitoring**. Marque **Enable** en **Admission Control** para que solo se enciendan los servidores virtuales que no pongan en peligro el cluster. Elija una regla de failover en la zona **Admission Control Policy**. Pulse **Next>**.

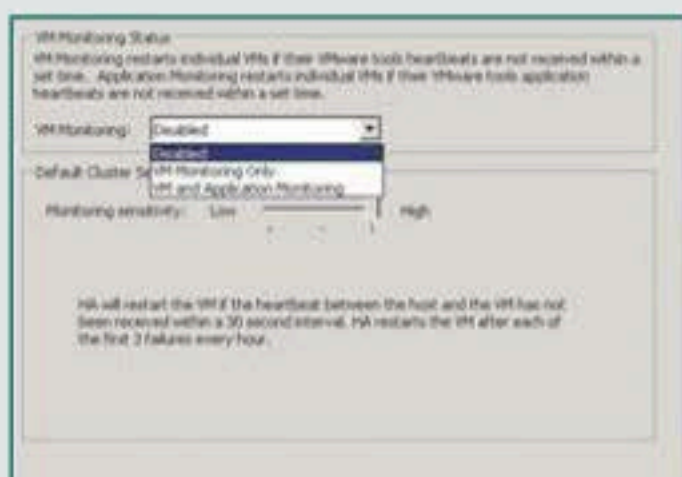
PASO A PASO /3 (cont.)

6



Seleccione una política para la alta disponibilidad; las máquinas de nivel bajo, medio o alto se apagarán si así sucediera. Las máquinas se pueden desconectar, apagar o dejar prendidas. Pulse **Next>**.

7



Establezca una política para monitorear los servidores virtuales y los appliances. Esta opción reiniciará el sistema si descubre una falla. Debajo, elija una sensibilidad del monitoreo. Pulse **Next>**.

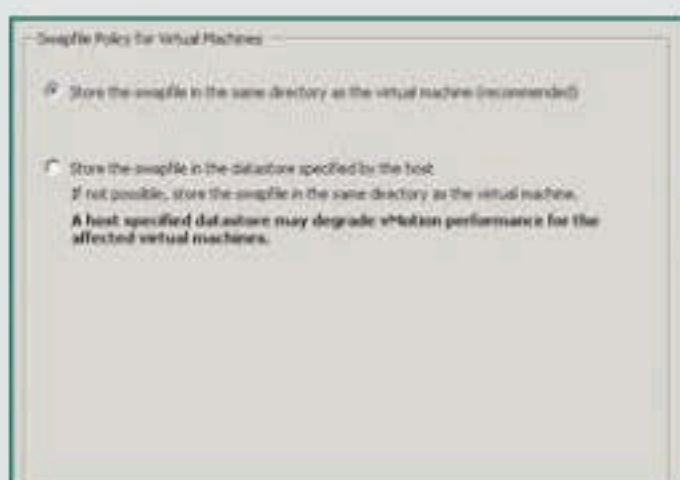
8



Puede habilitar la compatibilidad con algún modelo de microprocesador en particular. En este caso, déjelo deshabilitado, elija **Disable EVC**. Pulse **Next>**.

PASO A PASO /3 (cont.)

9



Elija dónde almacenar los archivos swap, seleccione la primera opción, que es la recomendada. Pulse **Next>**, luego lea el resumen y haga clic en **Finish**.

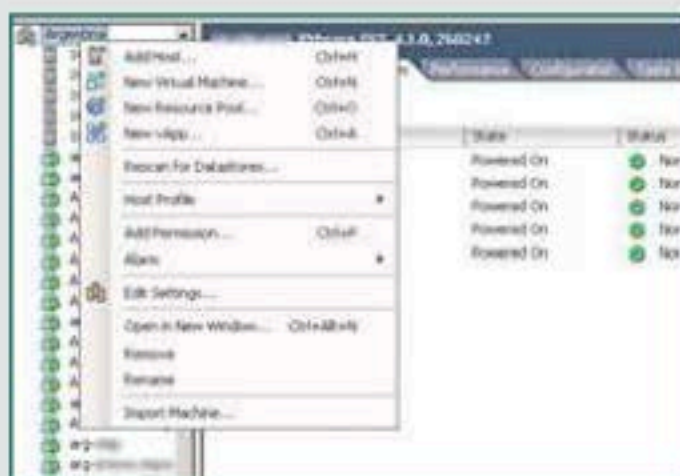
CÓMO AGREGAR NODOS ESXi

Ahora, luego de crear el cluster, veremos cómo agregarle nodos ESXi. Esta es una tarea muy fácil y es la forma en que el vCenter administra los nodos. Puede haber ciertos errores si tenemos el firewall del nodo habilitado, pero

generalmente no ocurren problemas mayores. Recordemos que los nodos que agreguemos a un cluster deben ser iguales. En caso contrario, vCenter nos alertará de que el nodo ESXi que queremos agregar no es compatible con los otros nodos del cluster.

PASO A PASO /4 Agregar nodos ESXi

1



Abra la consola de vCenter y haga un clic derecho sobre el cluster. Elija la opción **Add host**. Pulse **Next>**.

PASO A PASO /4 (cont.)

2

Ingrese la dirección IP del servidor ESXi y los datos del usuario **root** para conectarse. Pulse **Next>**.

3

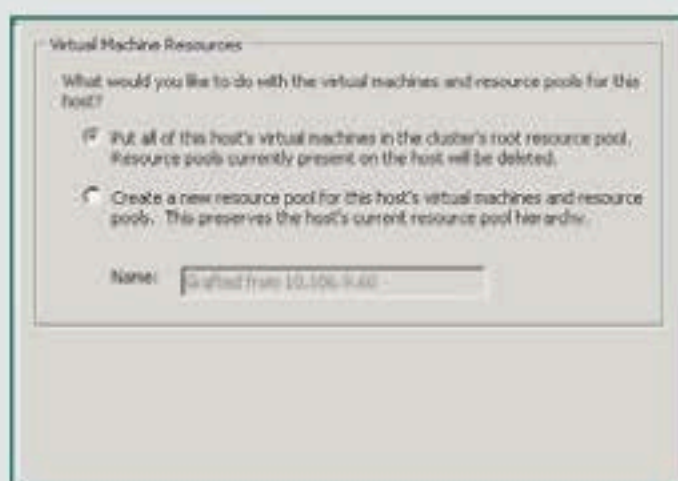
En la ventana de advertencia pulse **Yes**. Solo brinda información sobre un certificado SHA1 para el nodo ESXi.

4

Elija una clave de licencia para el nodo ESXi, puede ser una ya cargada en el vCenter, dejarla en modo evaluación o ingresar alguna otra. Pulse **Next>**.

PASO A PASO /4 (cont.)

5



Configure cómo administrar los recursos del nodo que va a conectar. Elija la primera opción para poner todo en un mismo pool de recursos. Pulse **Next>**, lea el resumen y, luego, haga clic en **Finish**.

En el caso de que queramos corroborar la funcionalidad de un nodo antes de ponerlo en la granja en modo automático, nos conviene desactivar DRS antes de anexar el nuevo nodo. Entonces, una vez deshabilitado, incorporamos el nuevo nodo y hacemos una prueba manual con vMotion para ver si el servidor virtual no tiene interrupciones, si no se corrompe al pasar o si ocurre algo inesperado. Una vez realizadas varias pruebas de ida y de vuelta, configuramos nuevamente DRS de manera automática para todo el cluster. Esta práctica también es recomendable cuando necesitamos sacar un nodo del cluster. La idea sería desactivar DRS automático y mover uno a uno los servidores virtuales hacia los otros nodos para verificar las cargas con vMotion. Una vez que el nodo que queremos retirar se queda sin máquinas virtuales procedemos a apagarlo, actualizarlo o lo que necesitemos hacer. Hay una opción automática que realiza estas acciones

de mover los servidores a otro lugar para desactivar el nodo. Solo debemos hacer un clic derecho y elegir la opción **Enter Maintenance Mode**. Esta acción moverá los servidores virtuales y distinguirá el nodo dentro del cluster como en modo mantenimiento. Si todavía tenemos activado DRS, solo se desactivará ese nodo en cuestión, y el DRS se seguirá usando en los otros nodos. No perderemos la carga balanceada aunque el procedimiento puede resultar peligroso. Lo importante es que podemos elegir cómo hacerlo.

HA, DRS, vMotion y Storage vMotion

En esta sección, analizaremos las herramientas más poderosas de la infraestructura de VMware.

VMOTION

VMotion es una herramienta esencial en la infraestructura virtual, que, básicamente, permite mover un servidor virtual de un nodo ESXi a otro. Esta opción es realmente interesante porque, al utilizarla, no tendremos ninguna pérdida de conexión ni bajada de servicio al mover el equipo. Esto se debe al sistema de archivos que utilizan los ESXi, llamado **VMFS**.

Una vez configurada la red para VMotion, debemos hacer una prueba de migración. Las migraciones pueden hacerse en caliente o en frío, es decir, con el servidor encendido o apagado.

VMotion es indispensable para crear centros de cómputos dinámicos y automatizados. Ahora se pueden realizar las tareas de mantenimiento del hardware físico sin afectar la continuidad del negocio en ningún aspecto. Es una tecnología del año 2004, o sea que, al momento de escribir este libro, tiene un desarrollo de más de 8 años.

Para conectar los nodos al storage y utilizar VMotion, aparte de poder conectar una **SAN** (Storage Area Network) por fibra, también soporta compatibilidad con **NAS** (Network

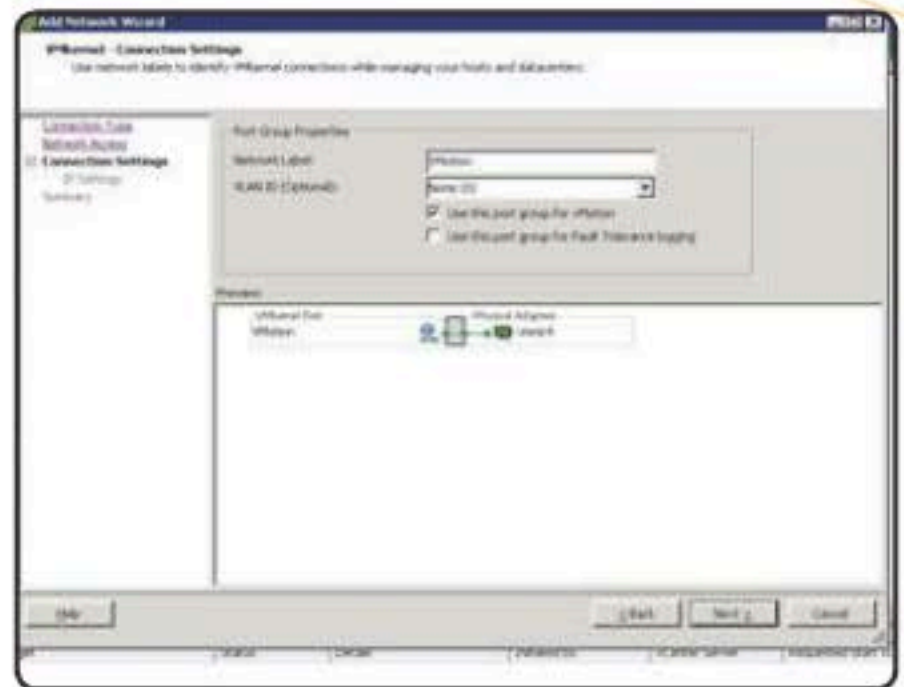


Figura 5. Al crear un switch virtual, debemos seleccionar el tipo de VMkernel y el check para que vSphere sepa que esa placa será usada por VMotion.

Attached Storage) y **SAN iSCSI**, que son sistemas de almacenamiento económicos.

Las tareas de migración poseen prioridades y se pueden programar para que sean realizadas a determinada hora del día. Porque podríamos tener un problema si un servidor virtual se moviera cuando no se tiene que mover, por alguna razón. Supongamos que estamos realizando una tarea de configuración de una placa de red en un nodo, y algún administrador pone en VMotion un servidor virtual con destino al nodo que estamos arreglando. Se podrían perder el



SISTEMA DE ARCHIVOS VMFS

El sistema de archivos **VMFS** es exclusivo de VMware, brinda privilegio a los nodos **ESXi** para que puedan leer y escribir coordinada y simultáneamente los mismos archivos al mismo tiempo.

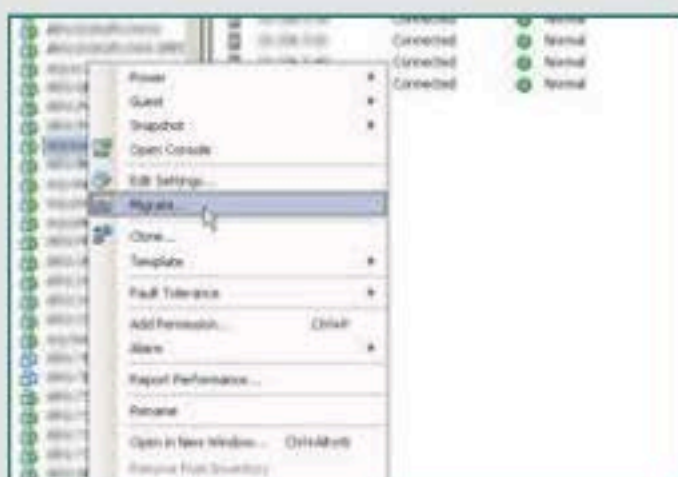
servicio y la continuidad del negocio. Para ello, la consola tiene una vista de todas las tareas que se realizan en vCenter en la solapa **Tasks**.

Ante cualquier circunstancia parecida, podríamos cancelar la operación. También la comunicación en este caso es esencial.

PASO A PASO /5

Realizar VMotion en un servidor

1



Abra la consola de vCenter y ubíquese sobre el servidor virtual que desea mover a otro host. La solapa **Summary** le indica en qué host se encuentra. Haga un clic derecho y en el menú elija **Migrate...**

2



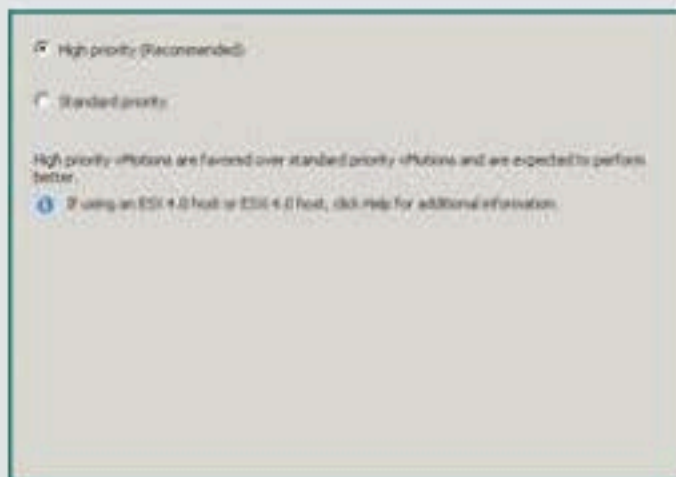
Elija la primera opción de **Change host**, pulse **Next** y seleccione el cluster donde va a ubicar el servidor virtual. Si elige el cluster **DRS**, indicará dónde ubicarlo, si no, puede elegir directamente un host expandiendo el árbol. Presione **Next>**.

HOSTS Y CLUSTERS

Se llama hosts a los nodos ESXi con los que contamos en nuestra infraestructura virtual. Estos hosts pueden agruparse en distintos conjuntos de carga balanceada y tolerante a fallas. A estos grupos, se los llama clusters.

PASO A PASO /5 (cont.)

3



Seleccione el pool de recursos que va a consumir el servidor virtual y, luego, pulse **Next>**. Elija la prioridad con la que realizará la tarea. Pulse **Next>**, lea el resumen y comience la migración. Verá el detalle en la solapa **Tasks** en la parte inferior de la consola.

STORAGE VMOTION

Storage VMotion realiza una función similar a VMotion, pero traslada la máquina de ubicación física y no de nodo. En este caso, tampoco hay pérdida de datos ni de comunicación, y también trabaja en frío o en caliente. Acelera en gran medida las migraciones con respecto a los sistemas tradicionales, sin interrupciones y sin necesidad de coordinar la bajada de servicios, porque esta no existe. Nos permite deshacernos de storage antiguos y difíciles de gestionar. Veamos cómo funciona.

Storage VMotion copia el directorio principal a la nueva ubicación antes de mover el archivo de disco del servidor virtual (archivo **VMDK**). Este directorio contiene los archivos de configuración, intercambio y registros del servidor virtual. Luego, copia el contenido de todo el archivo **VMDK** en el destino y utiliza el seguimiento de los bloques modificados para mantener la

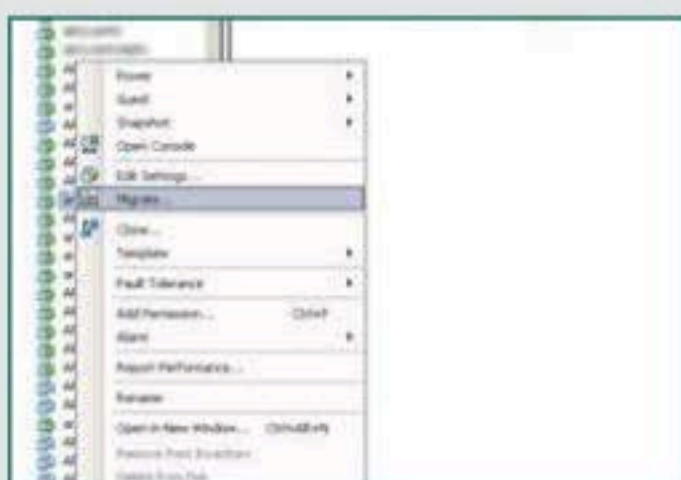
integridad de los datos en el proceso de migración. Verifica las zonas del disco que se han escrito en el primer contacto entre la **fuentes** y el **destino**, y realiza una segunda **iteración** de la copia de las zonas que cambiaron desde la primera iteración. Así sucesivamente hasta que no haya más cambios.

Luego, se suspende el servidor virtual y se lo vuelve a activar rápidamente; empieza a utilizarse entonces el directorio principal y los archivos de la ubicación destino. Antes de que el servidor esté operativo en su totalidad, Storage VMotion borra los archivos en la fuente para asegurar la integridad de la información.

Storage VMotion traslada la máquina de ubicación física y no de nodo

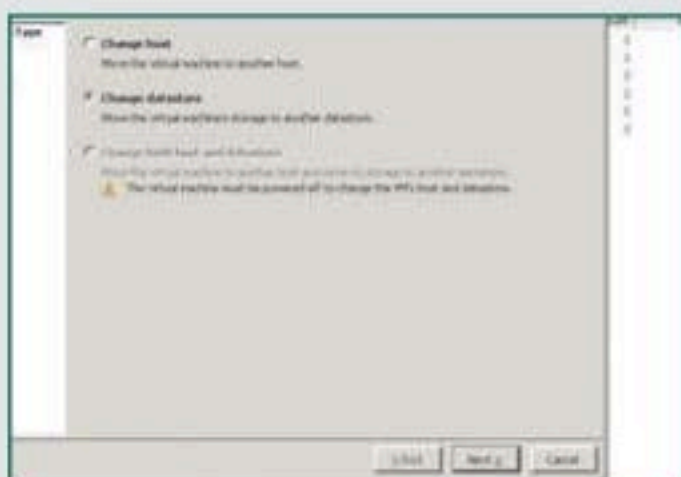
PASO A PASO /6 Realizar Storage VMotion

1



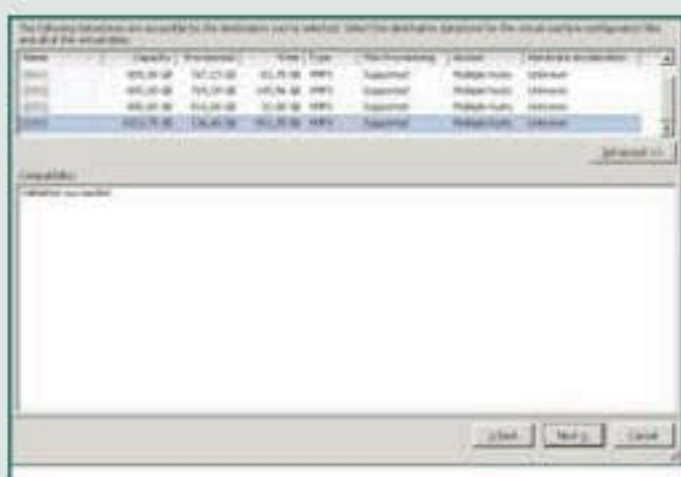
Abra la consola vCenter y haga un clic derecho sobre el servidor virtual que desea trasladar. En el menú, seleccione **Migrate** para empezar la tarea.

2



Elija la opción **Change datastore** para migrar el servidor virtual a otro storage. Pulse **Next>**.

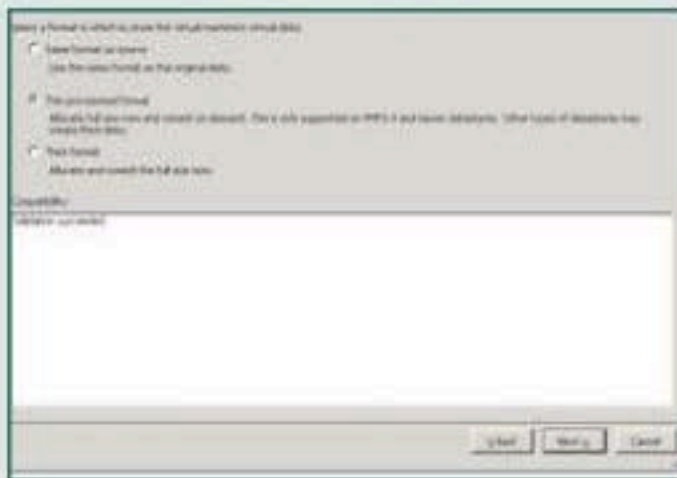
3



Seleccione el storage al cual moverá el servidor virtual, tenga en cuenta el espacio libre que necesita el servidor. Pulse **Next>**.

PASO A PASO /6 (cont.)

4



Elija el formato de disco. **Thick format** es para equipos que tendrán sus discos estáticos y **thin provisioning** para equipos con discos de crecimiento dinámico. Pulse **Next>**, lea el resumen y haga clic en **Finish** para terminar.

HA

HA permite tener alta disponibilidad en los equipos virtuales, algo que era inimaginable con los servidores físicos. Anteriormente, si un servidor físico fallaba, el servicio moría con el servidor hasta que lo arregláramos. Para esto, se utilizaban varios métodos de recuperación: backups, imágenes de recuperación o un equipo en **Spare**.

Estas soluciones significaban una gran inversión de dinero, al necesitar un spare por cada modelo de servidor. Si nuestra empresa abarcaba varias localidades, ciudades o países,

debíamos tener uno en cada lugar para hacer un cambio rápido y obtener el mínimo tiempo posible de bajada del servicio.

Con el advenimiento de la virtualización, el hardware pasa a ser un objeto virtual, mucho más maleable que el hardware físico. Con HA activado en una infraestructura virtual, cuando un nodo ESXi falla por alguna cuestión de hardware, un error de energía o por cualquier otra causa, todos los servidores virtuales son trasladados hacia otro nodo que tenga recursos disponibles y reiniciados de manera automática. Esto marca



SERVIDOR EN SPARE

Un servidor en Spare implica tener un segundo equipo igual al principal, que espera apagado hasta que el primero se rompa. Permitirá, ante una falla de hardware, hacer un cambio rápido de los elementos que conforman el equipo dañado y volver a tenerlo online.

una gran diferencia, dándonos de un 97% a un 100% de disponibilidad. Y no solo eso, si el sistema operativo provoca un error, el servicio de

HA lo monitorea, detecta el problema y reinicia la máquina de manera automática. Dos ventajas de alta disponibilidad juntas.

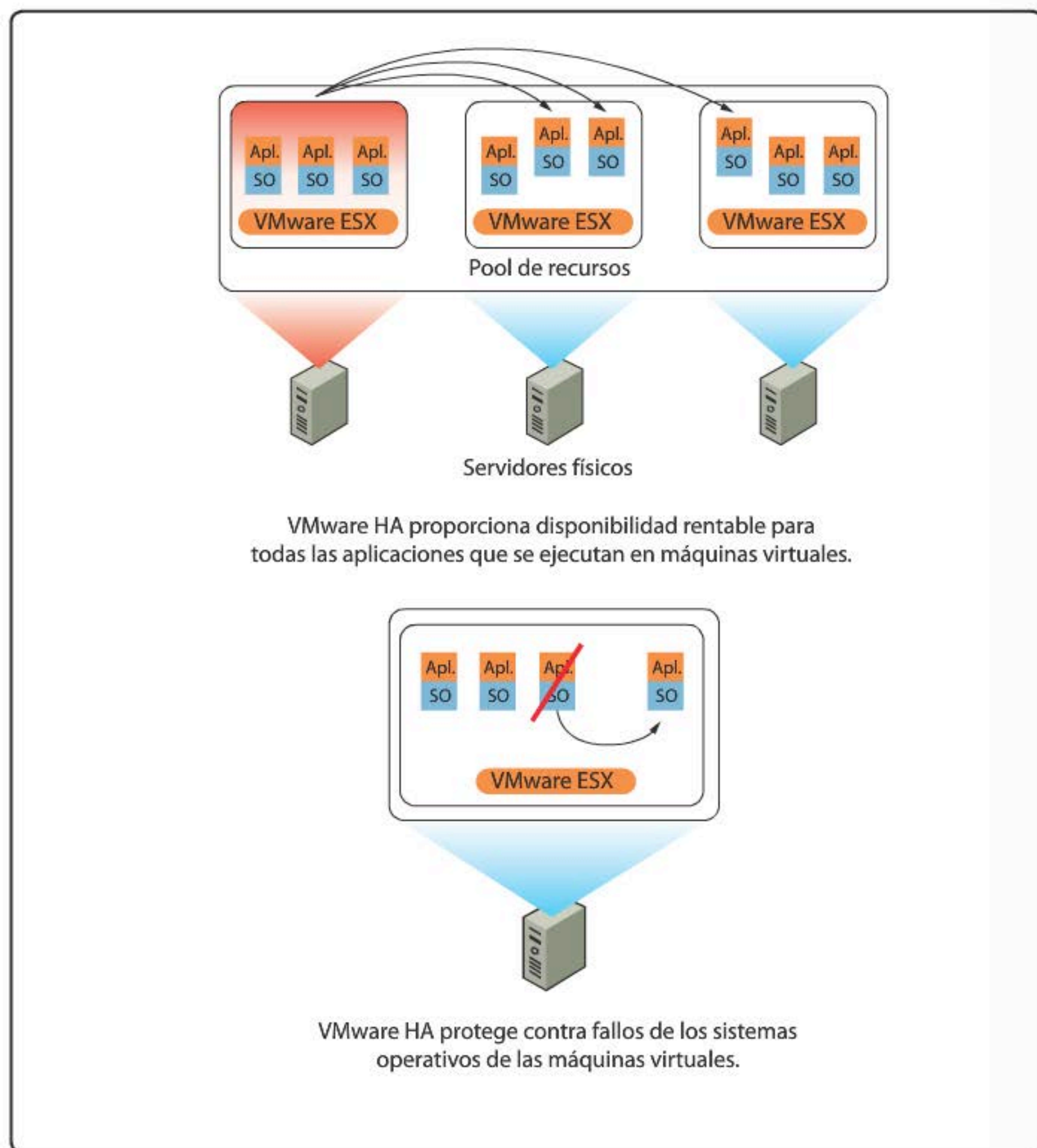


Figura 6. Si falla un nodo ESXi o una máquina virtual, HA los reinicia para mantener el mínimo de pérdida de servicio posible.

También genera un gran ahorro en lo que se refiere a la administración de un sistema de **failover** por los conocimientos y la complejidad que esto requiere en comparación con los sistemas tradicionales.

Podríamos extender esta ventaja de disponibilidad a servidores que no consideramos críticos, brindándole robustez a toda la infraestructura y no solo a determinados sistemas.

El servicio de HA del vCenter utiliza un agente para monitorear los nodos ESXi y los servidores virtuales. El agente se instala en los nodos cuando habilitamos HA en el cluster y, en los servidores virtuales, cuando instalamos las VMtools. Este agente mantiene un **heartbeat** con los servidores pertenecientes a un pool de recursos. La última versión de ESXi, la 5, no solo tiene un heartbeat por las placas de la consola, sino también a través de las conexiones de storage.

HA es un sistema inteligente que monitorea, a cada segundo, la utilización de la capacidad. Reserva siempre espacio adicional para poder reiniciar las máquinas virtuales en otros nodos. Si esta capacidad no se contempla o se degrada, no se podrá seguir agregando equipos al entorno virtual de ese pool de recursos, y VMware no permitirá encender más servidores. También es posible configurar, por cada servidor virtual, una prioridad de reinicio, porque algunos servidores son más críticos que otros y deben ser reiniciados en primer orden. No tiene sentido reiniciar un servidor que no es importante antes que uno crítico.

DRS

DRS (Distributed Resource Scheduler) se complementa extraordinariamente con el servicio de HA. Balancea los clusters de servidores entre los nodos para optimizar los recursos disponibles y no sobrecargar el hardware; asigna recursos según la demanda de los servidores virtuales y la saturación de los servidores físicos. Los recursos se agrupan en un pool de recursos, puede haber uno o varios. También es posible priorizar en el sistema de DRS las aplicaciones críticas ante las no críticas de acuerdo con las necesidades del negocio de la empresa.

Es posible configurar el servicio de DRS para que funcione de manera manual o automática, aunque de forma **manual**, solo informará qué servidor recomienda mover y a qué nodo. Tiene varios niveles de recomendaciones y, según ellas, la forma **automática** puede ser más o menos agresiva. Al ser más agresiva, mueve más servidores y les hace caso a más recomendaciones

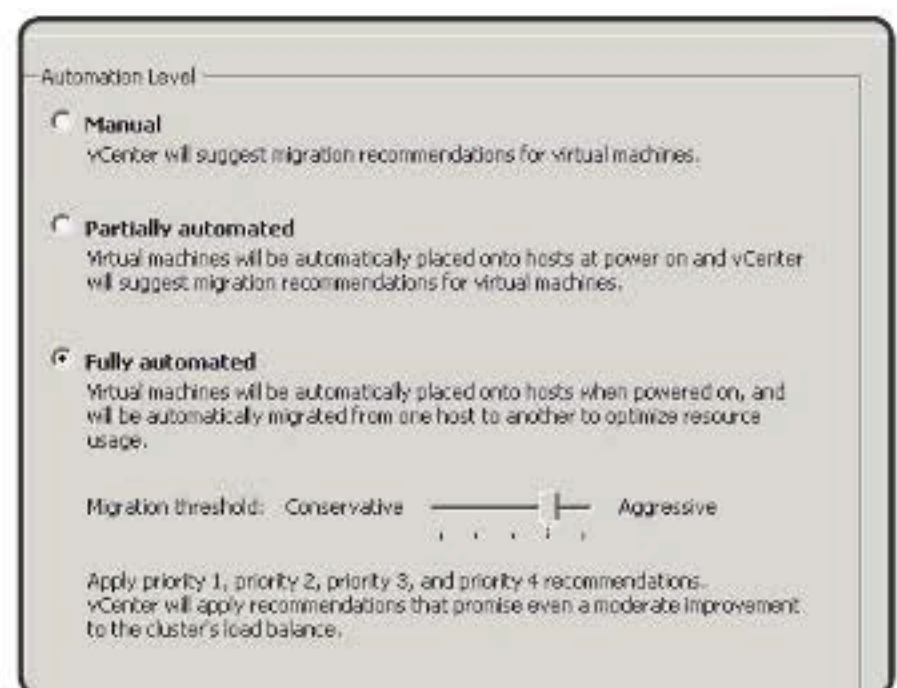


Figura 7. DRS brinda tres posibilidades para funcionar: manual, parcialmente automático y completamente automático.

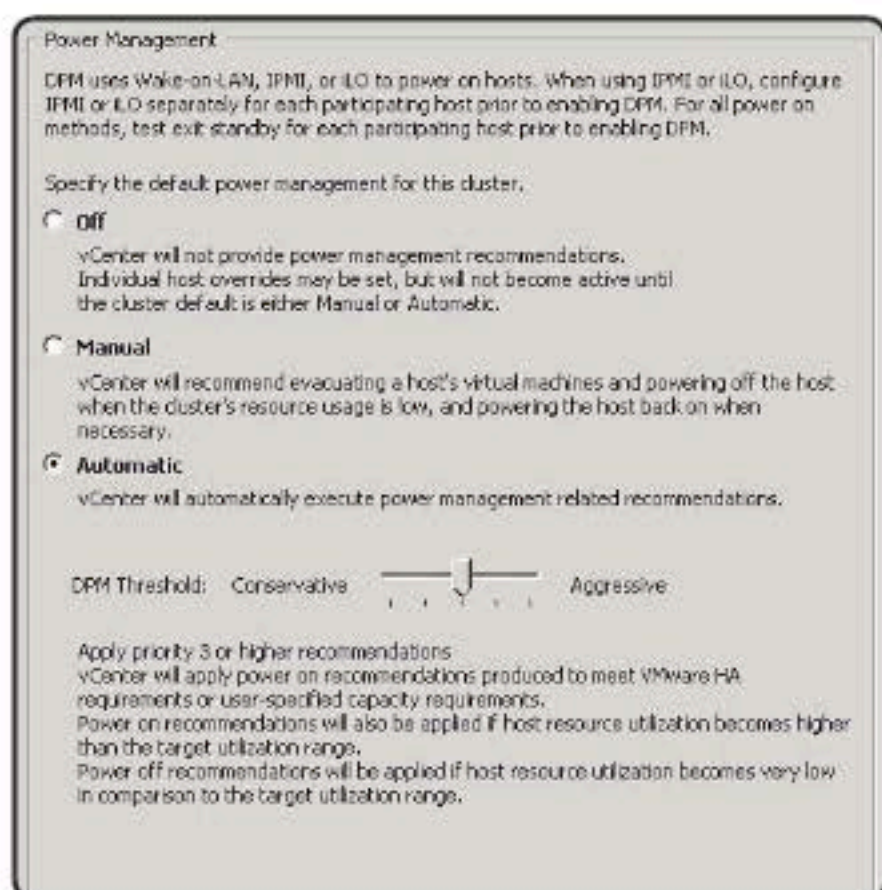


Figura 8. El DPM puede estar apagado, en modo manual o automático.

que si no fuese agresiva. Esto puede generar un gran desgaste para el hardware, si se está continuamente moviendo equipos virtuales, por eso se recomienda un nivel medio de agresividad para esta herramienta.

DRS funciona según reglas predefinidas en su configuración. Permite a un solo administrador manejar un gran pool de recursos y automatizar el mantenimiento de hardware. Otra característica muy interesante es que podemos configurar la afinidad de los servidores virtuales, establecer

que un servidor virtual pueda moverse a ciertos nodos o a todos. También trae una opción de DPM (Distributed Power Management) que aporta gran ahorro a una empresa.

Con la opción de DPM, VMware ofrece compatibilidad con las necesidades de la **Green Technology Wave** o tecnología de onda verde, movimiento que busca minimizar los consumos de energía para tener un planeta más limpio de polución y conservar los recursos.

Fault Tolerance

Fault Tolerance es la herramienta destacada de VMware ante todos los otros competidores. Debe configurarse de forma especial, al igual que VMotion: usa el mismo tipo de switch virtual (VMkernel) y necesita una VLAN propia con una IP fija. Al crear el switch virtual, en vez de elegir el check de VMotion, elegimos el de Fault Tolerance. Cada nodo ESXi debe tener una placa de red dedicada para este servicio conectada a Gbit. Al habilitarla para un servidor, se creará una copia exacta del servidor objetivo y se la dejará en modo pasivo. Tendremos dos copias



DPM (DISTRIBUTED POWER MANAGEMENT)

Cuando el DPM detecta que la carga de trabajo disminuye, reagrupa todos los servidores virtuales para apagar nodos ESXi innecesarios. Cuando la carga sube, los enciende en forma automática.

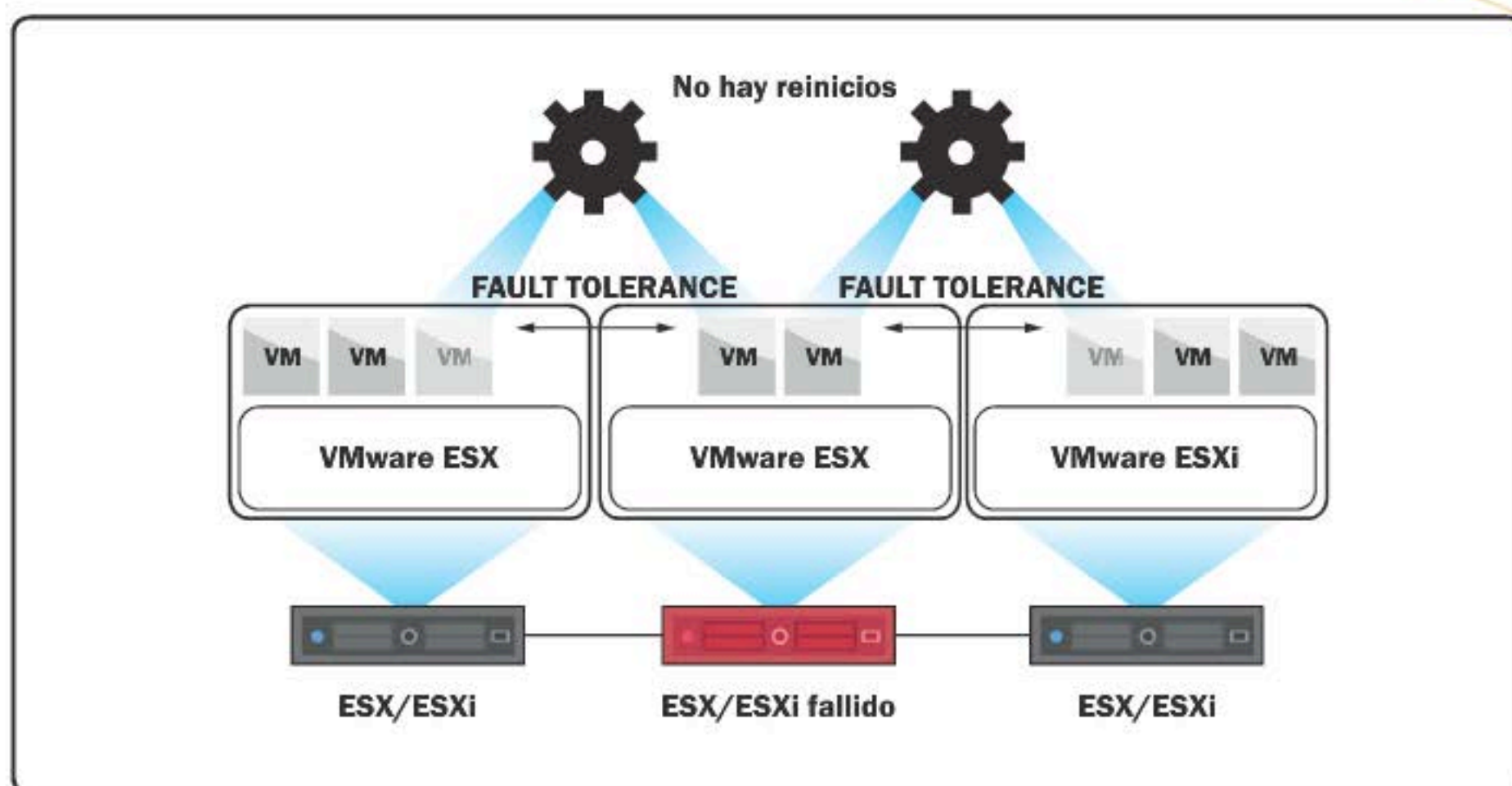


Figura 9. La infraestructura virtual queda intacta ante un error de la infraestructura física.

iguales de un mismo servidor en distintos nodos ESXi. Ante cualquier interrupción del servidor objetivo, el pasivo tomará el control al igual que en un cluster físico. Esto elimina el tiempo de bajada para cualquier servidor.

Sin dudas, es la mejor solución para los sistemas, ya que elimina el tiempo de parada de los servidores. Es alta disponibilidad real, 100% asegurada. Hay algunos requisitos para implementar Fault Tolerance, que debemos tener en cuenta antes de habilitar un servidor virtual:

- Los nodos deben tener una instalación ESXi versión 4.0 o superior.
- Debe haber un cluster HA.
- El servidor virtual no puede tener ningún CD, imagen o disco conectado.
- El servidor virtual debe estar en un almacenamiento compartido entre los nodos.
- El servidor virtual debe tener una configuración de discos thick. Un servidor con discos thin no podrá colocarse en Fault Tolerance.
- El servidor virtual debe tener una sola CPU virtual.
- El consumo de recursos aumentará un poco más.
- DRS se deshabilitará para el servidor virtual que obtenga la opción de Fault Tolerance, ya que se torna innecesario.
- No es posible realizar snapshots, por lo tanto, no se podrán hacer backups del servidor.
- No se podrá mover el servidor de LUN utilizando Storage VMotion.

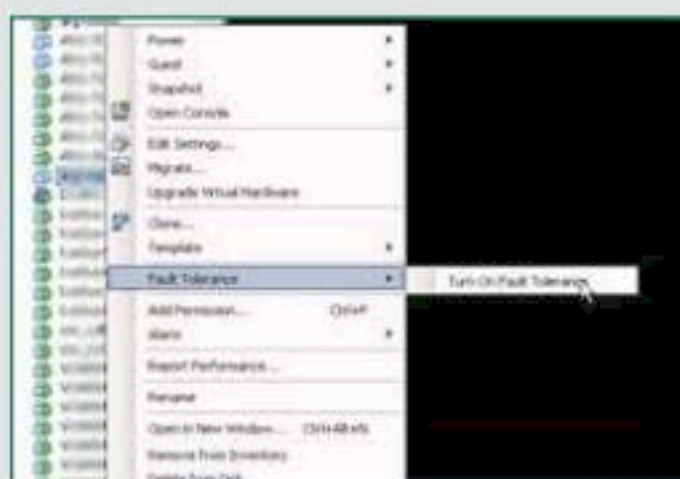
Luego de configurar la placa, si nos ubicamos sobre un nodo ESXi y vamos a la solapa **Summary**, en la sección de las características generales, veremos un campo que dice **Host Configured for FT: Yes**.

Esto significa que Fault Tolerance está configurado de manera correcta en el nodo. Solo falta indicarle a algún servidor virtual que se coloque en Fault Tolerance. A continuación, vemos cómo hacerlo.

PASO A PASO /7

Habilitar Fault Tolerance para un servidor virtual

1



Vaya a la consola de vSphere y, sobre el servidor que quiera proteger, haga un clic derecho. En el menú, elija **Fault Tolerance/Turn on Fault Tolerance**.

2



Pulse **Yes** en la ventana que le advierte que no tiene sentido tener el DRS activado para este servidor, por eso, se desactivará.

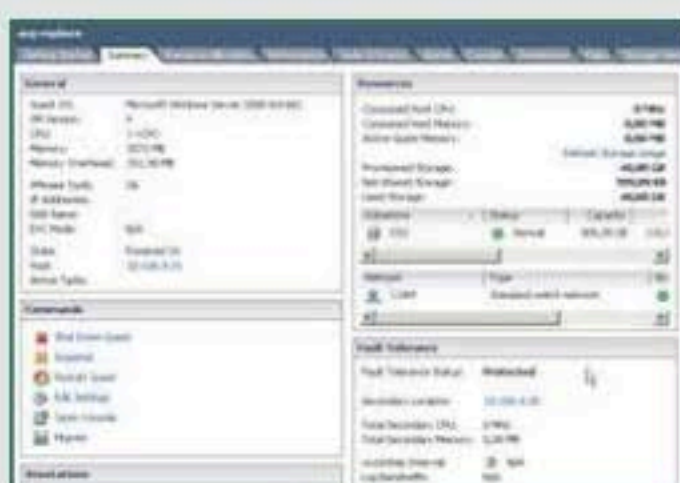


ACTUALIZACIÓN DE ESXI 4.1 A 5.1

Las versiones 4.X de ESXi no se pueden administrar con vSphere 5.1. Para ello, tenemos que instalar desde cero los nodos ESXi o actualizarlos con Update Manager desde un vCenter 5.

PASO A PASO /7 (cont.)

3



La tarea comenzará a desarrollarse; observe en **Tasks** su secuencia. Luego, verifique en la solapa **Summary** del servidor protegido, que en el recuadro de **Fault Tolerance** diga **Protected**.

Las actividades se replican y coordinan entre el servidor objetivo y el pasivo gracias a una tecnología llamada **VMware vLockstep**. Esta toma el servidor primario y el secundario, y los hace ejecutar idénticas secuencias de instrucciones de sus plataformas. Además, captura todo los cambios a nivel procesador, y dispositivos de entrada y salida, y los replica. Estas réplicas de eventos se hacen a grandes velocidades al estar conectadas en una red de Gbit.

Cuando se corrompe el servidor primario, el nodo ESXi mantiene las instrucciones que no se

pudieron llevar a cabo en él y habilita el secundario como primario para que continúe la operación. En ningún momento hay pérdida de datos o modificaciones. Luego, por HA, el primario que había fallado vuelve a incorporarse al cluster, pero en el papel de secundario. Todo el proceso es transparente para los usuarios finales y totalmente automático sin intervención de ningún administrador.

Para que funcione vLockstep, es necesario que la CPU física de cada nodo tenga esa capacidad. VMware ha trabajado con empresas como

▶ SNAPSHOT

Los snapshots son imágenes, fotografías del estado de un equipo en un determinado momento. Algo parecido a un punto de restauración, pero mucho más potente, ya que nos permite ir y venir en un árbol de descendencia.

Intel y AMD para que existan instrucciones especiales para usar esta tecnología. Es una extensión de instrucciones, y las CPU de los nodos deben ser compatibles para habilitar Fault Tolerance. Fault Tolerance puede fallar si queremos habilitarlo en equipos virtuales con grandes discos o si el almacenamiento de los nodos es muy lento. Para habilitar Fault Tolerance en estos casos, necesitamos apagar el equipo, habilitarlo y luego volver a encenderlo.

Snapshot

Hace algunos años, con servidores físicos, era imposible pensar en un snapshot. Lo más parecido que existía era un equipo de repuesto, pero nada más que eso. Un **snapshot** es algo similar a tomar una foto de un instante en el tiempo del servidor. Veamos un ejemplo para entender claramente de qué se trata esta herramienta. Creamos un equipo virtual para la entrega de un servidor de testing, instalamos el sistema operativo y tomamos un snapshot

(**snap_testing**). Luego, instalamos una base de datos, configuramos la administración, tomamos un snapshot y entregamos el sistema a quien lo haya pedido (**snap_DB**). En esta etapa, es posible volver al primer snapshot tomado (**snap_testing**), donde solo tenemos el sistema operativo instalado, y, si nos piden un servidor de correo, instalamos el servicio y creamos otra rama de snapshot (**snap_correo**). Supongamos que, más tarde, nos piden nuevamente un servidor de base de datos (**snap_DB**); entonces, volvemos al snapshot de base de datos y continuamos desde allí dejando sin efecto el de correo. Es importante no tener varios snapshots sin uso, ya que desaprovecharíamos el espacio en disco. Los snapshots conservan varios estados de las máquinas virtuales; entre los datos que se guardan, tenemos el estado de la memoria y de los discos, la configuración de la máquina virtual y, también, los datos del BIOS. Los snapshots son fundamentales para la creación de backups, ya que las herramientas de backup crean un snapshot para tomar la copia y, así, separar la demanda de la red del equipo productivo.



RESUMEN

En este capítulo analizamos la elección de VMware como software de virtualización. También, aprendimos cuáles son los sistemas de virtualización de VMware y cómo funcionan. Para terminar, conocimos otras tecnologías alrededor de esta solución.

Capítulo 4

Herramientas para la plataforma VMware

Veremos las principales herramientas
para aplicar sobre la infraestructura VMware.

VMware vCenter Operations

vCenter Operations es una herramienta de monitoreo y estadísticas que se integra en toda la arquitectura VMware. Con la versión actual, la 5, podemos monitorear uno o más vCenters. Esta es una gran diferencia con respecto a la versión anterior, que requería un servidor (**appliance**) por cada vCenter. No había forma de unificar todas las consolas de VMware Operations en una sola. Otra diferencia es que ahora son dos servidores los que componen la solución, conformando una **vApp**.

INTERFAZ

Para acceder a la interfaz, podemos hacerlo a través del cliente de vSphere (vClient) o desde una dirección web, funcionalidad que brinda uno de los servidores de VMware Operations. Para el acceso y las configuraciones, disponemos de los mismos permisos que en vCenter. Estos son trasladados a la consola de monitoreo, por lo tanto, tendremos el acceso por validación de usuarios locales del vCenter, así como también por validación con usuarios de Active Directory (sistema de directorio del dominio de una empresa).

Para entender lo que significa una herramienta de monitoreo de cuarta generación como esta, veremos algunos detalles. Al ingresar a la consola principal, encontraremos dos indicadores muy importantes en el ambiente IT y que nunca se pudieron medir con certeza: la salud (**Health**) y el riesgo (**Risk**) de toda la infraestructura. Estos se basan en datos de los servidores físicos (ESXi), de los servidores virtuales, de la red y del storage, que son muy dinámicos y difíciles de medir en una gran empresa por la cantidad de datos disponibles. Los indicadores dotan a los departamentos de IT de una inteligencia y una efectividad que no podían tener con herramientas anteriores.

Consola principal

La consola principal se distribuye en tres columnas dinámicas. La primera es un árbol en el que podemos observar los distintos vCenters, los datacenters que se encuentran en ellos, los clusters que guardan, los hosts ESXi, las virtuales y también los datastores. En la columna del medio, se ven los detalles de los elementos seleccionados en el árbol de la izquierda. Así se arma una matriz de información. Seleccionamos el tipo de información requerida y el lugar desde donde lo queremos ver. La tercera columna es de resumen



APPLIANCE

Los appliances son máquinas virtuales que podemos bajar directamente desde el sitio web de VMware. Estas máquinas virtuales vienen instaladas con un sistema operativo (casi siempre Linux) y otro sistema que brinda un servicio específico.



Figura 1. La consola muestra gran cantidad de información de manera gráfica.

de alertas e indicadores. Las columnas de los costados pueden ocultarse, para tener una visión más clara de los datos, por eso son dinámicas.

El árbol de la izquierda permite ir bajando de granularidad. Si aparece un error en una máquina virtual en particular, podemos saber en qué host ESXi, cluster, datacenter y vCenter se encuentra. De esta forma, es posible solucionar el problema con rapidez.

En la parte central de la consola, hay 5 o 6 solapas de información, que varían según la licencia del producto. Las solapas básicas son Tablero de control (**Dashboard**), Operaciones (**Operations**), Planeamiento (**Planning**), Alertas (**Alerts**) y Análisis (**Analytics**).

Este sistema de monitoreo queda instalado sin necesidad de clientes ni de ninguna otra configuración. El sistema va aprendiendo a medida que adquiere datos.

Solapa Dashboard

Dashboard contiene un resumen de todo lo que debemos conocer de la infraestructura para saber si funciona bien o no. Con VMware podemos monitorear la salud de todo el sistema, desde el hardware (nodos físicos), las conexiones de red, el storage, el estado de las máquinas y las máquinas virtuales. Estos indicadores se actualizan todos los días a la medianoche, por eso, no es posible acceder a la información online.

La salud del punto de la infraestructura donde estemos parados dependerá de la carga de trabajo (**Workload**), las anomalías (**Anomalies**) y las fallas (**Faults**). Entre estos factores, se hace un promedio, y ese es el valor final que se muestra como salud del sistema.

El riesgo se compone del tiempo que queda para consumir los recursos (**Time Remaining**) según la utilización de CPU, memoria, E/S de disco y red. En la versión Advanced, aparecen otros componentes para este indicador: la capacidad remanente (**Capacity Remaining**) y el estrés del sistema (**Stress**). A diferencia del tiempo remanente, la capacidad remanente se mide en cantidad de máquinas virtuales que quedan para dar vida. El estrés indica la cantidad de horas en que el sistema estuvo sobreexigido.

Solapa Operations

Operations se divide en cinco vistas: Ambiente (**Environment**), Marcadores (**Scoreboard**), Detalles (**Details**), Eventos (**Events**) y Métricas varias (**All Metrics**). Para entender las vistas, debemos saber qué significan los colores de los

gráficos: verde (todo está bien), amarillo (algo está fuera de lo normal), naranja (el recurso está degradado), rojo (algo está en mal estado), gris (los equipos están apagados, y no hay datos de ellos).

Environment despliega una vista con todos los recursos de la infraestructura, donde se resaltan los equipos que se conectan entre sí desde el vCenter hasta los datastores.

Scoreboard presenta un mapa con la ponderación de los distintos marcadores de los equipos afectados que se relacionan.

Details ofrece un resumen ponderado de los cuatro indicadores, infografías varias de uso de CPU, memoria, disco y red de cada equipo. En cada gráfico es posible cambiar ciertos parámetros, para hacer una medición que se ajuste a nuestras necesidades. Si presionamos los signos +, se detallan datos del storage con números de consumo de I/O, paquetes perdidos, latencia, etcétera.

En **Events**, tenemos un resumen de la cantidad de eventos generados en una línea de tiempo, con colores que detallan si son críticos o no.



Figura 2. En la vista de detalles, vemos las infografías de cada dispositivo.

En **All Metrics**, se encuentran todos los recursos de los cuales tenemos datos. Podemos analizar su estado en el tiempo y crear nuestro propio informe. Tan solo debemos abrir el árbol de recursos y hacer un doble clic para que se agregue al informe comparativo que queremos realizar.

Solapa Planning

Planning se divide también en cinco vistas que brindan datos de capacidad, utilizando gráficos. La subvista más interesante es Sumario porque resume datos de la infraestructura que nos permiten saber cuántas máquinas desplegamos y cuántas podríamos desplegar



PREGUNTAS SOBRE EL ENTORNO

Siempre debemos preguntarnos si nuestra infraestructura es saludable; tendremos que saber si los recursos son suficientes y, por último, sobre todo entender que su optimización es algo primordial.

una semana o un año después. Además, informa sobre los recursos remanentes de los distintos puntos de toda la arquitectura.

Solapa Alerts

Alerts nos ayuda a realizar todo el troubleshooting para encontrar las fallas del sistema. Posee filtros para aplicar en las alertas de toda la infraestructura, desde máquinas virtuales, servidores ESXi y datastores.

Al realizar doble clic sobre un alerta, se muestra su detalle y, desde allí, podemos acceder a la máquina o dispositivo afectado para relacionar los eventos que llevaron a que ocurra tal acontecimiento.

Solapa Analysis

En **Analysis**, veremos informes analíticos de consumos de I/O por máquina virtual, por ejemplo, o la capacidad remanente de los hosts ESXi al analizar la carga de trabajo agrupados por clusters.

Solapa Reports

Reports, disponible en la licencia Advanced y anteriormente en la herramienta Capacity IQ de VMware, ofrece varios tipos de informes que podemos obtener según el punto de

la infraestructura donde estemos posicionados, como la cantidad de máquinas virtuales apagadas y la utilización de los hosts.

DISTINTAS LICENCIAS Y POSIBILIDADES

Existen cuatro versiones de VMware Operations: **Standard**, **Advanced**, **Enterprise** y **Enterprise Plus**. Standard y Advanced son para pequeños y medianos negocios, mientras que Enterprise y Enterprise Plus son exclusivas para empresas. La versión Advanced cumple con gran cantidad de requerimientos y mejora los niveles de SLA.

Todas las licencias contienen las siguientes herramientas:

- **Paneles de control:** presentan una panorámica de toda la infraestructura.
- **Alertas inteligentes proactivas:** ofrecen notificaciones proactivas de nuevos problemas de salud, rendimiento y capacidad.
- **Análisis de rendimiento automático:** aprenden el estado de la infraestructura a partir de las buenas prácticas de VMware (cuanto más tiempo de recaudación de datos tenga, más exacta será la información).



CONSUMO DE I/O

Los I/O vienen de las palabras Input y Output; en castellano, entrada y salida de datos. Este parámetro puede medirse según los distintos tráfico que utilizan los dispositivos.

- **Umbrales dinámicos:** trabajan de acuerdo con la suposición de que los datos se distribuyen analizados de forma estadística.

Dos herramientas muy importantes que también están incluidas en todas las versiones son la medición de la capacidad del sistema total y el seguimiento de cambios realizados por la correlación de eventos dados.

Desde la versión Advanced, se incorporan las funcionalidades que antes estaban en Capacity IQ. Estas permiten tener paneles de tendencias de funcionamiento, emulación y modelos de escenarios, así como también todo tipo de reportes y alertas.

INSTALACIÓN

A continuación, vamos a aprender a aplicar VMware vCenter Operations en nuestra infraestructura. Antes de comenzar, veremos qué son las vApps, porque la última versión de la herramienta viene en ese formato.

vApps

Las **vApps** o **Virtual Appliances** (una no muy afortunada traducción sería **aparatos virtuales**) son soluciones de sistemas prefabricados. Están constituidas por una o más máquinas virtuales, tratadas como una unidad: son instaladas, actualizadas, mantenidas y administradas como un conjunto único. Actualizar las vApps es muy fácil, una vez que sabemos que los parches funcionan en uno, lo harán en los demás. La distribución de las appliances se realiza mediante un formato estándar industrial denominado **Open Virtual Format (OVF)**.

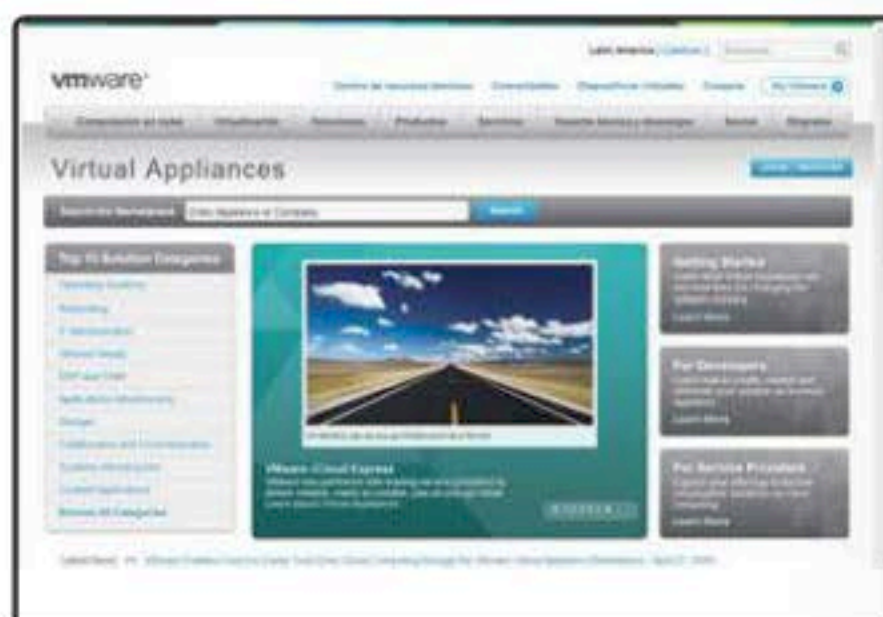


Figura 3. En www.vmware.com, hay miles de vApps, algunas pagas y otras gratuitas.

PASOS POR SEGUIR EN LA INSTALACIÓN

En la versión anterior a la 5, eran dos servidores por separado: VMware Operations y VMware Capacity IQ.

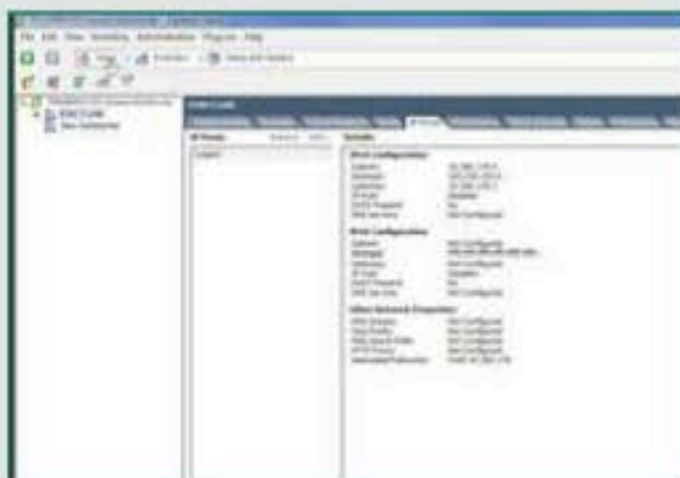
En esta nueva, se integran las dos herramientas en una sola. El despliegue del OVF configurará una vApp con dos servidores virtuales dentro. Se generará un pool de recursos para que consuman, y veremos datos particulares de la aplicación en conjunto desde los detalles de la vApp. Lo más importante en la instalación es la generación de un pool de direcciones IP (**IP Pool**), que debemos crear antes de realizar el despliegue.

Si bien se utilizará una IP fija para los equipos, hay que crearla igual porque, de otra forma, no podremos instalar la herramienta. Dividiremos en dos partes los pasos para la instalación. En la primera, crearemos un IP Pool en vSphere y, en la segunda, veremos el despliegue y la configuración del OVF de VMware Operations.

PASO A PASO /1

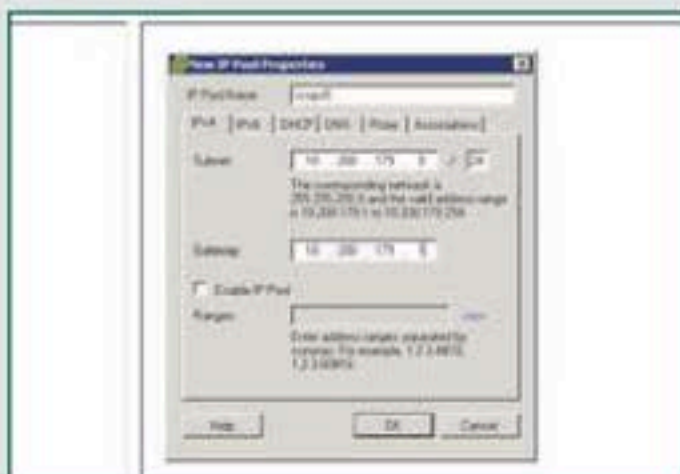
Generación de un IP Pool

1



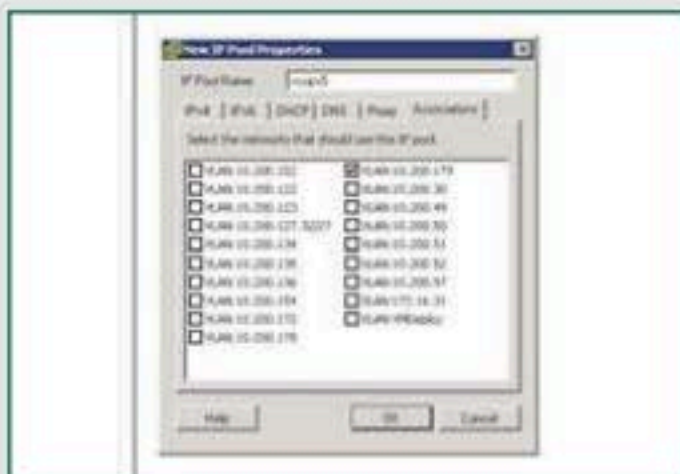
Vaya a la consola del producto, el cliente vSphere. Ubíquese sobre el datacenter donde va a instalar la aplicación y seleccione la solapa **IP Pools**. Haga clic en **Add...**.

2



En la ventana emergente, ingrese un nombre que identifique a la aplicación. Luego, complete los campos de subred (**Subnet**) y de la puerta de enlace (**Gateway**).

3



Vaya a la solapa **Associations** de la misma ventana, seleccione la subred correspondiente en donde va a estar instalada la aplicación y haga clic en **OK**.

PASO A PASO /2

Instalación del OVF de VMware Operations

1



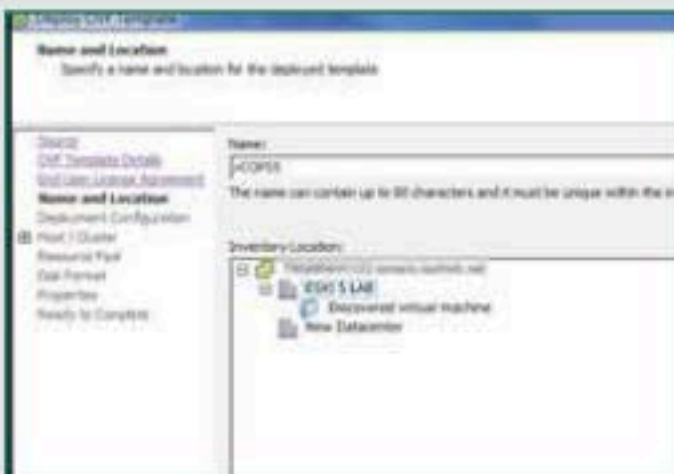
Baje desde el sitio de VMware la imagen OVF del instalador. Dentro de la consola de vSphere, vaya al menú **File/Deploy OVF Template...**

2



Ubique la imagen OVF en el disco, donde lo haya guardado. Luego, aparecerá la información del producto si la imagen no está dañada. Para continuar, haga clic en **Next>**.

3



Acepte el contrato de licencia, pulse **Accept** y luego **Next>**. Ingrese un nombre para ubicar la vApp en el datacenter. Luego, seleccione el datacenter donde instalará el producto y pulse **Next>**.

PASO A PASO /2 (cont.)

4



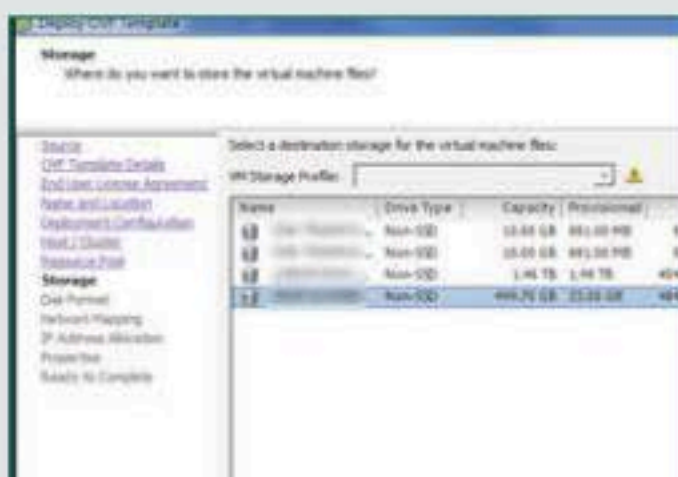
Elija un tamaño para la infraestructura desde el menú **Configuration**. Esto es para saber cuántas CPUs necesitará cada servidor, cuánta memoria y qué tamaño de disco requiere la base de datos. Pulse **Next>**.

5



Seleccione el cluster o el host ESXi donde quedará instalado el producto. Pulse **Next>**. Seleccione el pool de recursos (**Resource Pool**) que desee para la aplicación. Elija el cluster completo si no tiene ninguno creado. Pulse **Next>**.

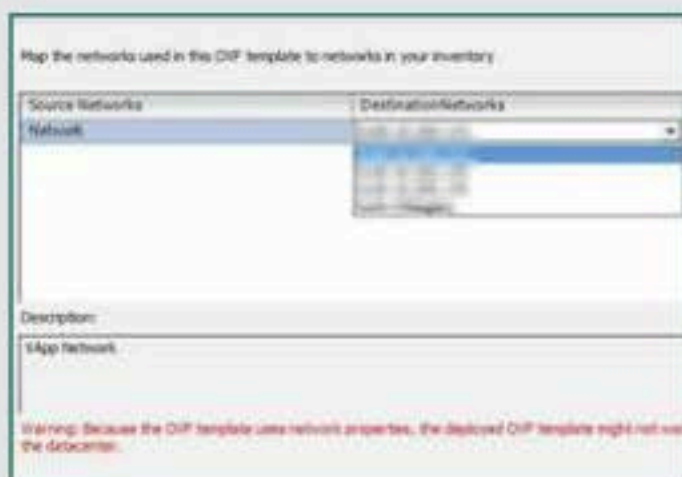
6



Indique el datastore donde ubicará la aplicación. En caso de soportarlo, especifique si habilita o no el Storage DRS para esta máquina. Haga clic en **Next>**.

PASO A PASO /2 (cont.)

7



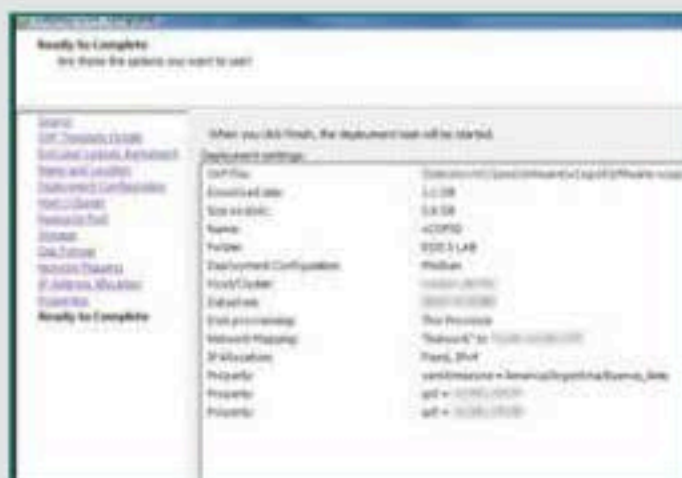
Elija el formato del disco virtual que se creará: **Thick Provision** o **Thin Provision**. Pulse **Next>**. Seleccione la red en la cual trabajará VMware Operations. Pulse **Next>**.

8



Elija la opción **Fixed** en la locación de IP para poder configurar una IP fija para los servidores. Pulse **Next>**. Indique el **Time Zone** de su país y complete las direcciones de IP de los dos servidores. Haga clic en **Next>**.

9



Vea el resumen y compruebe que los datos son correctos. Seleccione la casilla **Power on after deployment** para encender la vApp no bien termine de instalarse. Pulse **Finish**.

Una vez que se despliegue el OVF, verá en la consola la vApp con los dos servidores en funcionamiento. Si tarda mucho en encender, acceda a la consola de cada servidor y revise los errores.

VCENTER INFRASTRUCTURE NAVIGATOR

vCenter Infrastructure Navigator es muy útil cuando hablamos de una infraestructura a nivel empresa, porque las dimensiones que esta puede llegar a alcanzar son inmensas.

Nos brinda la posibilidad de acercarnos un poco más a las aplicaciones que corren sobre nuestro datacenter y observar, con detenimiento, las dependencias entre ellas. Podremos saber, por ejemplo, cuántos servidores de aplicaciones están corriendo en toda nuestra infraestructura; buscar distintos tipos de sistemas, como bases de datos, servidores de correo electrónico, servidores web, servidores de aplicaciones, servidores de archivos y muchos más.

Esta herramienta relaciona cada punto de la infraestructura con cada aplicación que corre en ella. De esta manera, si nos posicionamos en un datastore o un dispositivo de red, veremos todas las aplicaciones que estamos afectando si llegamos a hacer algún cambio. Además, como es parte de VMware Operations, tiene una navegación similar, por lo tanto, podemos ir viendo cada dispositivo y sus dependencias con una estructura de árbol. Sin dudas, es una gran herramienta para tener en cuenta a la hora de mejorar nuestro conocimiento y administración sobre la arquitectura de la empresa.

VMWARE CHARGEBACK MANAGER

VMware Chargeback Manager sirve en especial para obtener datos económicos de nuestro datacenter, porque visualiza los costos reales de los consumos de virtualización. Es totalmente moldeable a cualquier organización, ya que se pueden definir los modelos de costos y políticas para cada una. Los datos son recolectados directamente desde los vCenters, asegurando la más completa y precisa información de todo el entorno. Además, permite con rapidez distinguir los costos y consumos de distintos departamentos. Como se integra con **VMware vCloud**, es parte esencial si queremos disponer de las herramientas para crear un cloud privado dentro de nuestra empresa. Sin dudas, si queremos obtener reportes de datos económicos y métricas, es la herramienta ideal.

VMWARE CONFIGURATION MANAGER

VMware Configuration Manager se utiliza para obtener datos más cercanos a los sistemas operativos que corren en nuestra infraestructura. A través de ella, se obtiene información sobre los sistemas de archivos, las configuraciones de red, la administración de usuarios, los grupos, los servicios de los sistemas, los parches, los cambios de red, los logs y mucho más. Se pueden realizar, también, distintas reglas de estándares por cumplir y saber si se cumplen o no, dejándola actuar y observando sus informes.

Con esta herramienta, es posible automatizar millones de configuraciones de forma masiva, acción que de otra forma debiéramos hacer servidor por servidor. Además, las podemos poner

en un calendario y horario para que corran a una determinada hora. Tiene muchísimas opciones y parámetros para poder hacer lo que se nos ocurra en nuestra infraestructura de sistemas operativos virtuales. Sin dudas, es un gran paso, antes de pensar en un cloud privado.

Site Recovery Manager

Site Recovery Manager (SRM) es una herramienta que hace posible tener una solución de DRP para la infraestructura virtual completa. Provee una consola con los planes de recuperación de uno o varios servidores, que permite oprimir un botón y restaurar toda la infraestructura. De esta manera, en minutos, damos continuidad a esos servidores en otro sitio distinto de donde corrían.

Además, permite la prueba no disruptiva de todo el sistema de DRP, la automatización de los procesos de recuperación y la migración de equipos. Para que todo quede funcionando correctamente, es necesario realizar varios pasos y controles y coordinar distintos departamentos.

Por eso es necesario entender la arquitectura que necesitamos. En principio, requerimos dos vCenters. Uno es el sitio productivo que vamos a proteger, y el otro, el sitio de recuperación. En el sitio de protección se generarán los **grupos de protección**, que se componen de uno o más servidores virtuales. En el sitio de recuperación, construiremos los **planes de recuperación** de los grupos de protección preestablecidos. Cada grupo de protección puede tener uno o varios planes de recuperación. Esta flexibilidad permite optar por recuperar dos o tres servidores o todo el datacenter. Otra opción es recuperar los equipos en distintos sitios. Podemos tener un gran sitio productivo y dos sitios de recuperación, donde repartiremos la carga productiva por un tiempo acotado.

SRM se conecta con el vCenter mediante un plugin, que tiene un apartado para la administración y maneja de forma automática las órdenes a las cajas de storage. Para esto, es necesario instalar algunas herramientas que veremos más adelante.

Si utilizamos certificados propios en la infraestructura de VMware, debemos tener precauciones con la instalación de vCenter. El certificado de SRM debe tener un campo en donde figure el servidor



IP POOL

Son un conjunto de direcciones IP, asignadas a diferentes sistemas dentro de una empresa. Por ejemplo, si generamos máquinas en forma automática desde una consola de vSphere, necesitaremos que el vCenter le asigne una IP a cada nueva máquina.

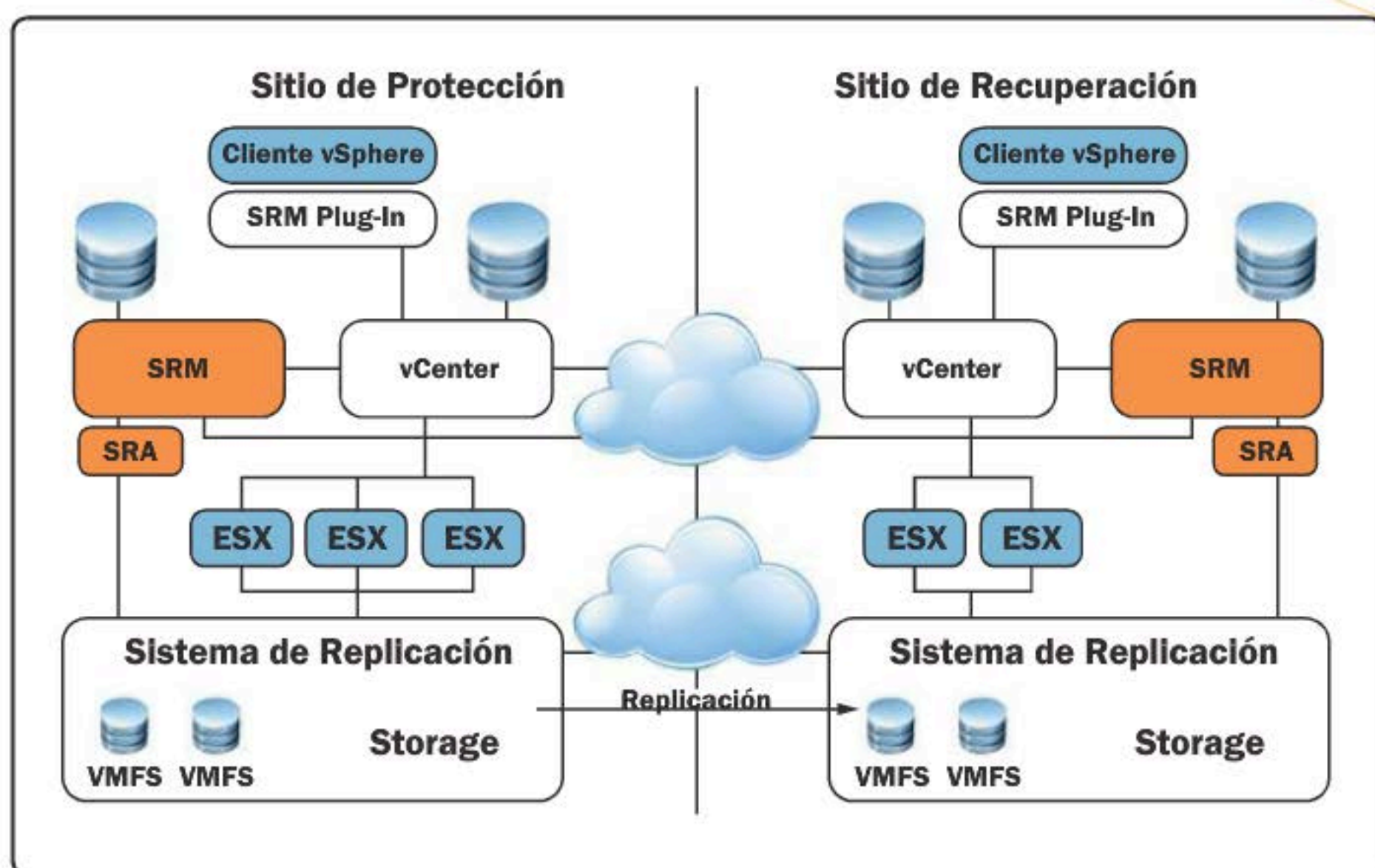


Figura 4. Diagrama de SEM, con los dos sitios y los roles intervinientes.

vCenter en el que va a ser instalado. Entonces, tendremos dos vCenters certificados y dos SRM certificados que deben hablar entre sí. Para esto, es necesario que el nombre del certificado sea igual en el sitio de protección y en el sitio de recuperación.

SRM se instala sobre un sistema operativo Windows, que puede ser el mismo vCenter u otro equipo, y necesita una base de datos para

correr, que puede ser MS SQL, Oracle o DB2. Antes de comenzar con la instalación, necesitamos una conexión de ODBC a la base de datos.

REQUISITOS MÍNIMOS PARA LA INSTALACIÓN

Hay varios requisitos mínimos que debemos tener en cuenta a la hora de instalar VMware SRM. Respecto al hardware, necesitamos:

STORAGE

Se denomina storage a las cajas de discos que utilizan los datacenters para contener sus datos. Vienen de distintos tamaños, según la cantidad de discos que posean, y se conectan a los servidores generalmente por placas de fibra o placas de red Ethernet.

- Un procesador de 2 Ghz, Intel o AMD x86.
- 2 GB de memoria RAM.
- 5 GB de espacio en disco.

Esto es para cada sitio en donde instalemos SRM, dos sitios por lo menos: uno de protección y otro de recuperación.

En caso de instalar el SRM sobre un servidor vCenter, debemos sumar los requisitos del vCenter con los de SRM para tener un estimado del equipo que se va a emplear.

Necesitamos también algún tipo de **replicación de discos**. Hasta la versión 4 de SRM, disponíamos de las replicaciones de terceros, con lo cual se utilizaba su software para la tarea. Cada proveedor ofrecía un par de conectores que se instalaban sobre Windows y con los cuales se podía comandar la caja de discos. SRM conocía todos los conectores y automáticamente manejaba los comandos simples a la hora de ejecutar el DRP. Con la versión 5 de SRM, disponemos de vSphere Replication, una solución propia de VMware.

En el caso de que utilicemos un storage de terceros, necesitaremos el conector propio del fabricante, que vincula el sistema operativo Windows y SRM contra la caja de storage.

Cada uno de los sitios por replicar debe tener un datacenter como mínimo creado en vCenter. Otro detalle es que ambos sitios deben tener la misma tecnología y ser pares. También, los requisitos de

recursos de un lado y del otro deben ser similares ya que, si no, las máquinas se apagarán en caso de pasar a un sitio con menores recursos.

Hay dos **versiones** de VMware SRM: Standard y Enterprise. La primera la utilizaremos para instalar una instancia que administre no más de 75 servidores virtuales. En caso de pasar este límite, usaremos SRM Enterprise.

El **licenciamiento** de la versión 4 se realizaba por procesador de cada nodo. En la versión 5 es por máquina virtual. Si disponíamos de licencias de la versión 4, estas se pueden convertir a razón de cinco máquinas virtuales por cada licencia de procesador anterior. De esta forma, un cliente que tenga una licencia de 25 procesadores recibirá una licencia de la versión 5 de 125 máquinas virtuales.

INSTALACIÓN DE STORAGE Y ODBC

Para la implementación de SRM, primero debemos definir el storage que vamos a utilizar. Podemos elegir cualquiera de los partners del mercado o utilizar vSphere Replication. En este caso, usaremos una caja de storage EMC VMAX conectada mediante FC.

El conector es una combinación de herramientas: **EMC Solution Enabler** es una consola para enviar comandos contra la caja de storage, y **SRDF SRA** es el conector entre la consola y el SRM. En este ejemplo, tomaremos el conector SRDF para versiones de SRM 5.0 y debemos instalar una herramienta de más. Si usáramos otro tipo de storage, con instalar la herramienta de SRA es suficiente.

PASO A PASO /3

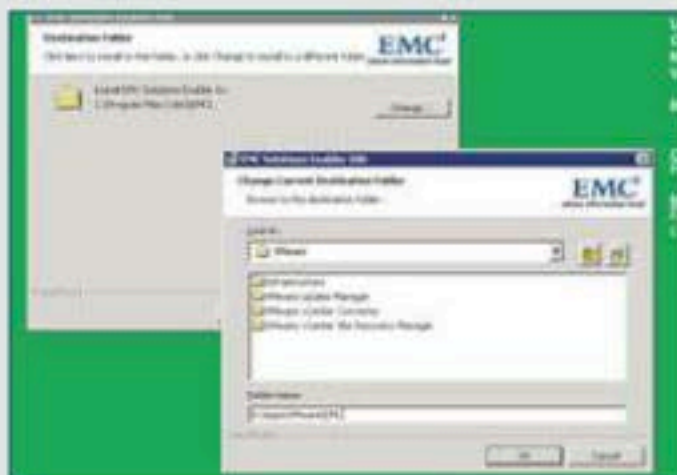
Instalación de EMC Solution Enabler

1



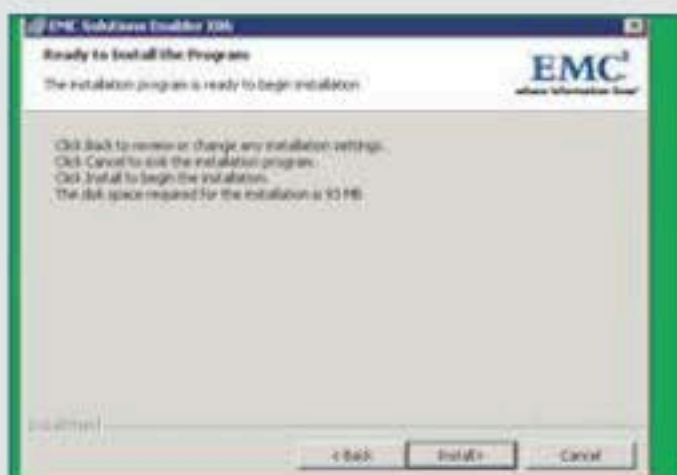
Baje la última versión de **Solution Enabler** desde el sitio web de EMC. Ejecute su instalación con permisos de Administrador y pulse **Next>**.

2



Seleccione la ubicación del software en el disco local mediante el botón **Change...**, haga clic en **OK** y, luego, en **Next>**.

3



Deje seleccionada la opción **Typical** y pulse **Next>**. Seleccione la opción **EMC SE SRM Daemon** y pulse **Next>**. Verifique el resumen y, si está de acuerdo, haga clic en **Install>** y, luego, en **Finish**.

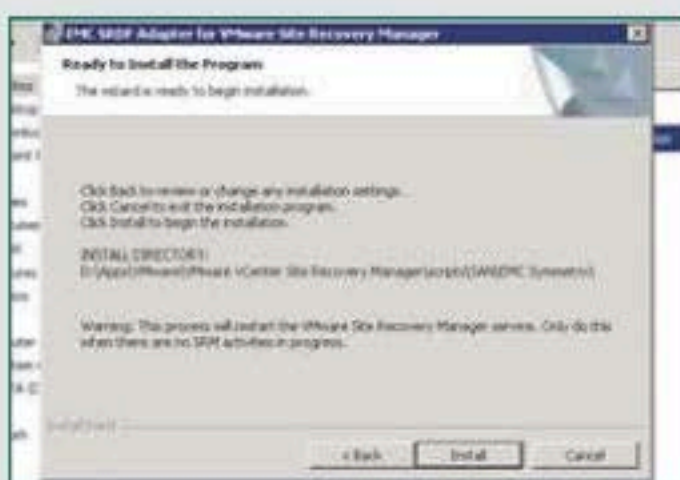
PASO A PASO /4 Instalación del SRDF

1



Baje la última versión de **EMC SRDF Adapter** desde el sitio web de EMC. Ejecute su instalación con permisos de Administrador y pulse **Next>**.

2



La pantalla siguiente es por si tiene instalado el SRM. Pulse **Next**. Verifique el resumen, haga clic en **Install>** si le parece correcto y, luego, en **Finish**.

Recordemos que otro requisito es tener una base de datos para SRM en cada sitio de la infraestructura, y configurar los ODBC para conectar los sistemas operativos con las bases. SRM utiliza una conexión de ODBC de 32 bits.

Con respecto a los usuarios, debemos establecer uno que utilizará el SRM para conectarse en cada sitio, en cada vCenter. También tenemos los usuarios de ambas bases de datos, que utilizaremos a la hora de la instalación del producto.

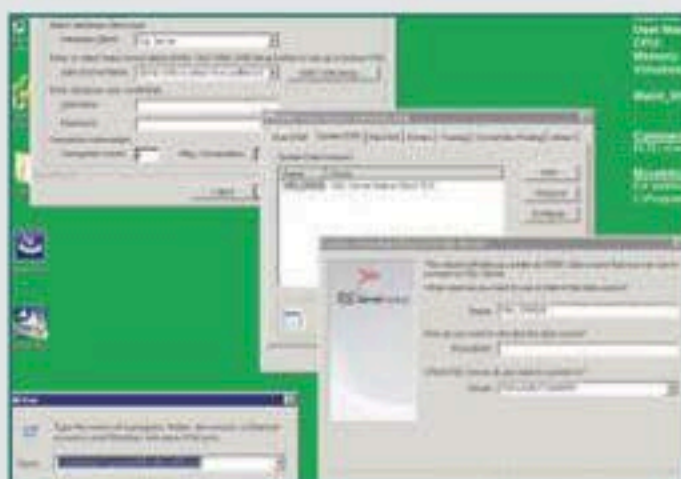
► THICK PROVISION Y THIN PROVISION

Son dos formatos de disco virtual que podemos ofrecer a un equipo virtual. El primero es más estático que el segundo; si necesitamos 200 GB de disco duro, le reservamos físicamente 200 GB. En el segundo caso, le reservamos un mínimo.

PASO A PASO /5

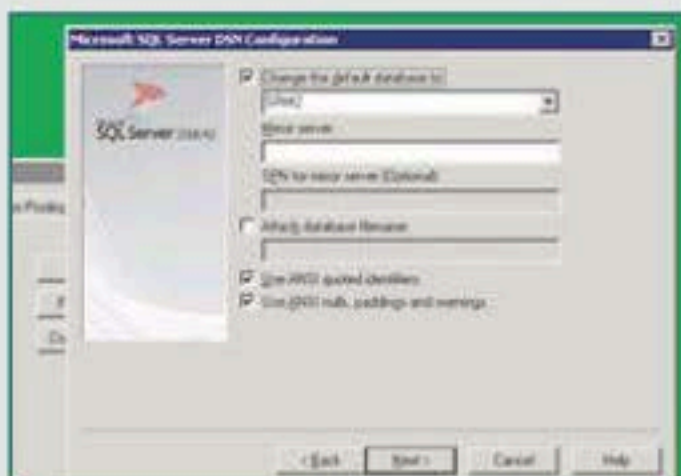
Configurar conexión ODBC de 32 bits

1



Vaya a **Inicio/Ejecutar** e ingrese **c:\windows\syswow64\odbcad32.exe**. En la ventana que se abre, seleccione **System DSN** y pulse **Add...**. Luego, complete el nombre de la conexión en **Name** y el del servidor de base de datos en **Server**.

2



Ingresa el nombre de usuario para la base de datos y la contraseña. Pulse **Next>**. Luego, seleccione la instancia de base de datos creada para SRM y pulse **Next>**.

3



Complete las opciones, en caso de que sea necesario, y haga clic en **Finish**. Realice un test de conexión pulsando **Test Data Source...**. Si es correcto cierre la ventana. En caso contrario, revise los pasos anteriores.

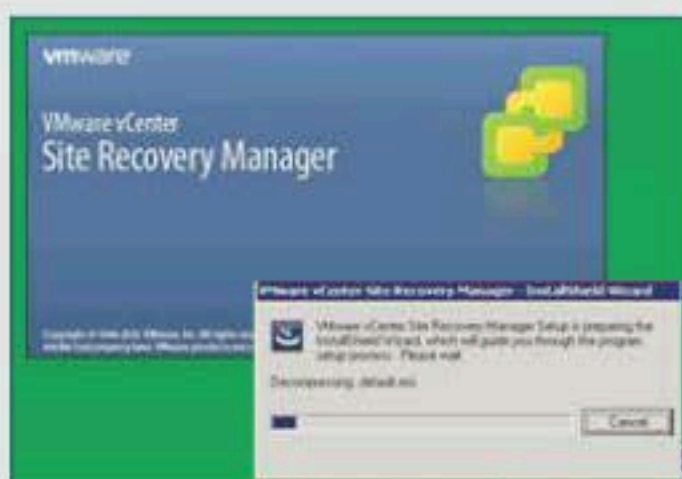
INSTALACIÓN DE SRM

Luego de instalar las herramientas de storage, continuaremos con SRM. Debemos instalarlo en cada sitio que utilicemos para la infraestructura. Es importante tener en cuenta que, si el vCenter

utiliza certificados, debemos generar nuevos certificados para SRM, porque de lo contrario no podrá conectarse con el vCenter. En nuestro ejemplo, instalaremos la solución en un ambiente sin certificados.

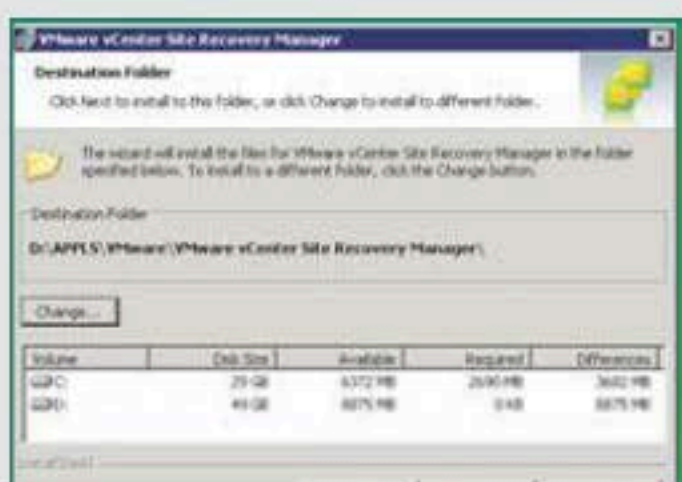
PASO A PASO /6 Instalación de SRM

1



Baje la versión de SRM que va a utilizar desde el sitio web de VMware, mediante su nombre de usuario. Ejecute el software con permisos de Administrador.

2



En la ventana de bienvenida, pulse **Next**. Visualice la patente del producto y pulse **Next>**. Acepte el contrato de licenciamiento y pulse **Next>**. Corrobore la ubicación en donde se alojará SRM y Presione **Next>**.

► CONEXIÓN A LA CONSOLA DE SRM

Vamos a ver en varias oportunidades que, en la consola de SRM, obtenemos errores de conexión. Esto se da porque, después de determinado tiempo, nuestro usuario se desloguea de la consola automáticamente.

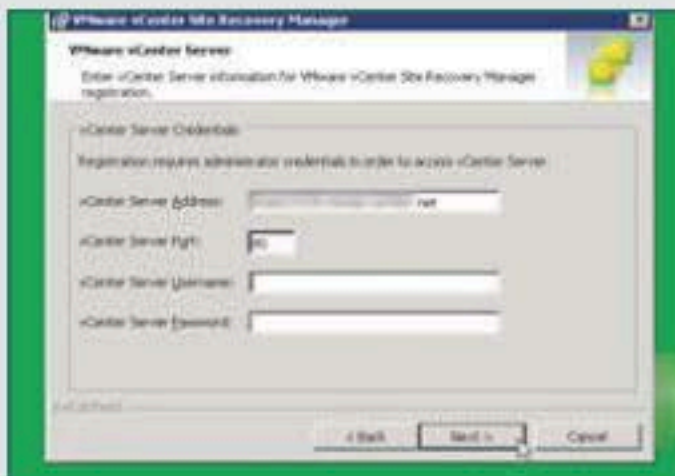
PASO A PASO /6 (cont.)

3



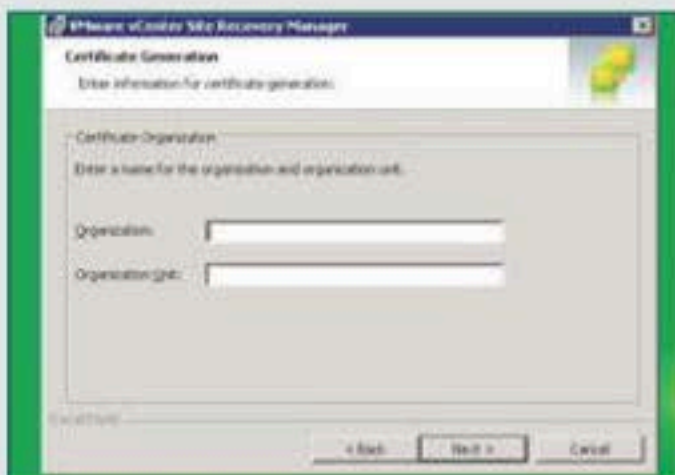
Seleccione una opción de storage. Si decide instalar **vSphere Replication**, deje dicha opción seleccionada, en caso contrario, seleccione **Do not install vSphere Replication**. Pulse **Next>**.

4



Ingrese los datos del vCenter donde está instalando el SRM para poder conectarse: **nombre de red, puerto**, usuario y **contraseña**. Pulse **Next>**.

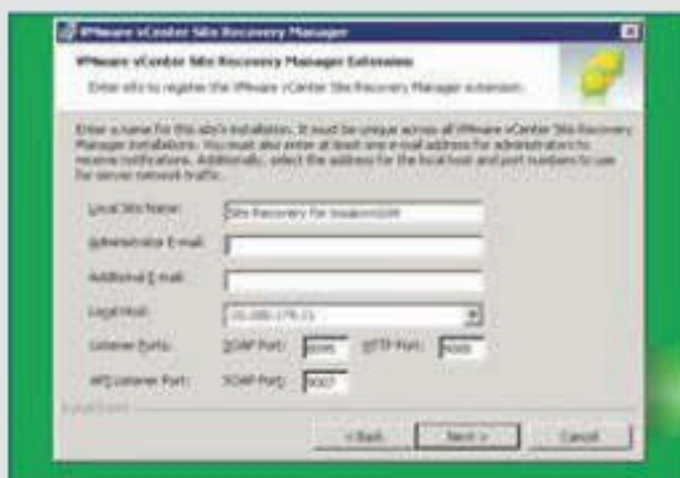
5



Debe optar por un certificado o generar uno automáticamente. Elija la primera opción y pulse **Next>**. Ingrese el nombre de la empresa en **Organization** y de su unidad de negocio, en **Organization Unit**. Pulse **Next>**.

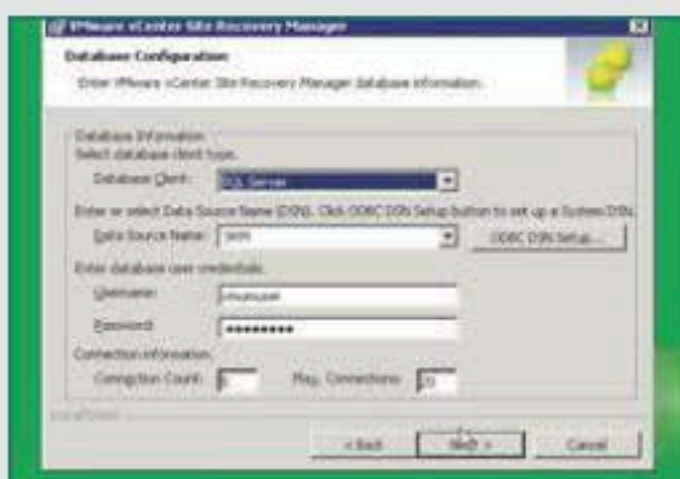
PASO A PASO /6 (cont.)

6



Ingrese un nombre para el sitio de SRM en **Local Site Name** y una dirección de e-mail en **Administrator E-mail** para notificar a los administradores. En **Local Host**, deje seleccionada la opción de reconocimiento por IP. Pulse **Next>**.

7



Complete los datos de la base de datos que utilizará el SRM. Seleccione el cliente y el nombre de la conexión ODBC. Luego, ingrese un nombre de usuario para el sistema SRM en **Username** y la contraseña en **Password**. Pulse **Next>**.

Para comenzar la instalación, pulse **Install** y, cuando haya finalizado, presione **Finish**. Ahora debemos realizar el mismo procedimiento en cada uno de los sitios que tengamos. Por lo menos, tenemos que hacerlo una vez más.

CONFIGURACIÓN DEL SISTEMA

Es importante mencionar que en cada sitio donde instalamos SRM, debemos instalar un **plugin** para vCenter para acceder a la consola de SRM desde vSphere client.



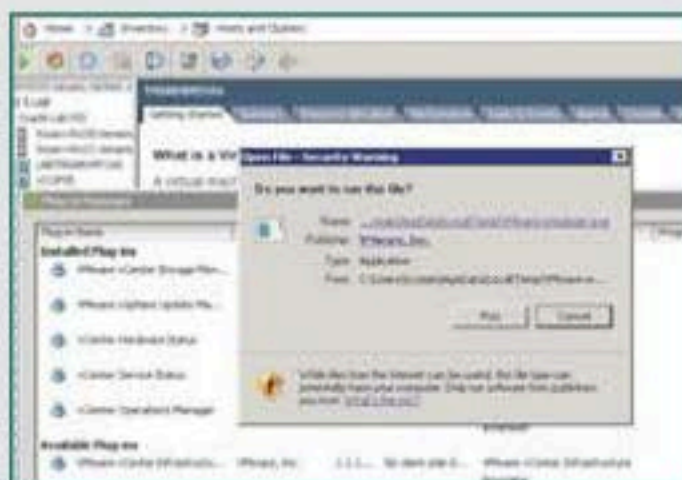
CONTRATO SLA

SLA es un contrato que el consumidor de un servicio de infraestructura hace con la empresa que ofrece el servicio. En él se detallan la cantidad de tiempo que un servicio puede caerse, el tiempo de respuesta y reparación, entre otros.

PASO A PASO /7

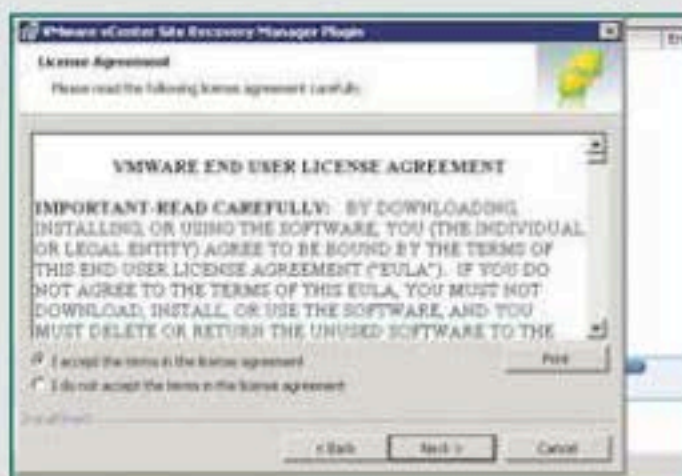
Configuración del plugin de SRM en vCenter

1



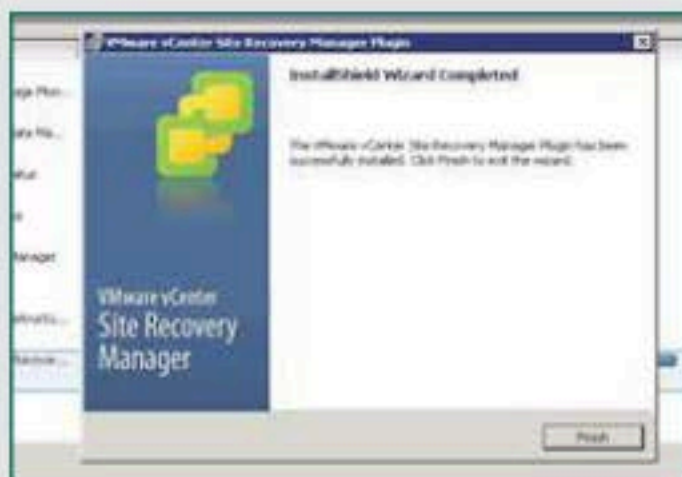
Vaya a la consola de vCenter y, en el menú superior, seleccione **Plug-ins**. Verifique que haya una nueva opción de **VMware Site Recovery Manager** y pulse **Download and Install**. En la ventana que se abre, presione **Run**.

2



En la ventana de bienvenida al asistente de instalación, pulse **Next**. A continuación, acepte el contrato de licenciamiento y presione **Next**.

3



Para comenzar la instalación, pulse **Install**. Una vez que haya finalizado, presione **Finish**.

PASO A PASO /7 (cont.)

4



Acceda a la consola desde **Home/Solution and Applications/Site Recovery**.

Como segundo paso, lo que debemos hacer es conectar el sitio de recuperación con el sitio de protección.

Es muy importante tener en cuenta que los dos sitios deben tener el sistema SRM 5 instalado junto con su plugin correspondiente en cada vCenter.

Vale aclarar que no es necesario que los vCenters estén en modo **Link**, ya que en la consola de SRM 5 esto no importa.

Es posible administrar ambos sitios por más que estos no se encuentren interconectados. Cuando hablamos de conectar los sitios, en esta oportunidad, hacemos referencia a la conexión de los vCenters con la consola de SRM y no entre las consolas del vCenter.

Esto quiere decir que, por más que conectemos ambos sitios de SRM, no podremos visualizar los dos vCenters desde la consola de vCenter. Para ello, haría falta utilizarlos en modo **Link**.

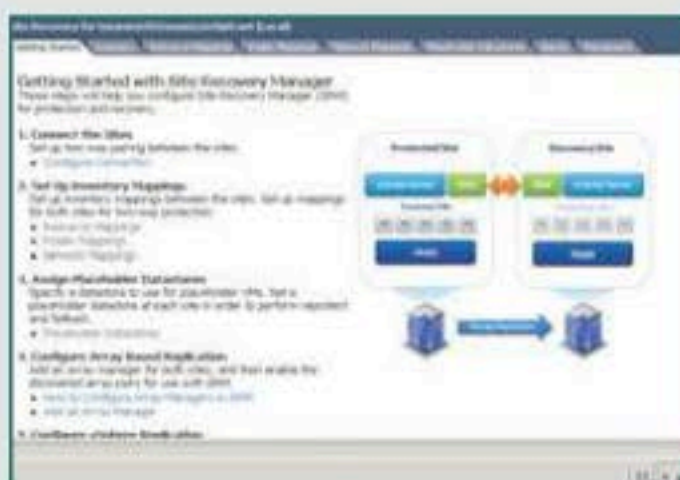
FQDN

Full Quality Domain Name es el nombre único de un servidor en una red dentro de una organización. Es el nombre de DNS que tiene el servidor para ser reconocido en combinación con su dirección IP.

PASO A PASO /8

Interconectar los sitios de SRM

1



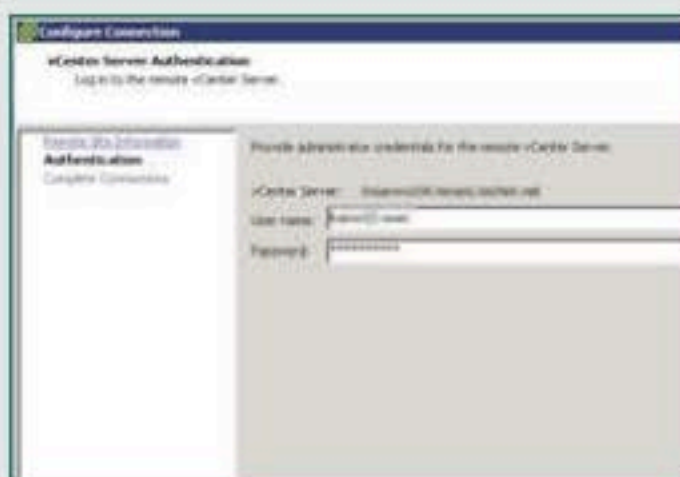
Diríjase a la consola de SRM del sitio de protección. Complete los datos de usuario y contraseña para conectarse. En el lado derecho de la pantalla, haga clic sobre **Configure Connection**.

2



En la ventana emergente, escriba la dirección del servidor de recuperación. Deje el puerto **80**, si no cambió las conexiones por defecto. Pulse **Next>**.

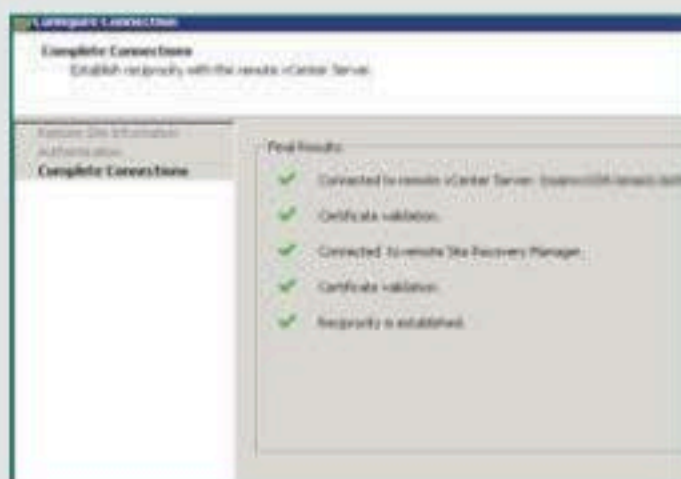
3



Se mostrará un certificado que debe aceptar, pulse **OK**. A continuación, complete el nombre de usuario y la contraseña que se usará para conectarse con el otro vCenter. (Luego lo podrá cambiar). Pulse **Next>**.

PASO A PASO /8 (cont.)

4



Nuevamente se mostrará un detalle del certificado del sitio remoto, pulse **OK**. A continuación, verifique que en ninguno de los 5 puntos de configuración se genere un error, y presione **Finish**.

5



Complete otra vez el nombre de usuario y contraseña para conectarse al sitio remoto, una vez que la conexión entre los sitios SRM se haya realizado.

Debemos repetir esta tarea para el sitio de recuperación. De esta forma, podremos administrar los dos sitios desde cualquiera de las dos consolas de SRM 5. Como tercer paso, debemos configurar las siguientes variables de mapeo de SRM:

- **Resource Mappings:** debemos marcar, dentro del vCenter en el que estemos trabajando, los recursos que serán asignados al sistema de SRM. Por ejemplo, tendremos 5 clusters creados en vCenter,

DATASTORE Y GRUPOS DE PROTECCIÓN

Por una cuestión de orden y de rendimiento, necesitaremos armar un grupo de protección distinto por cada datastore replicado. Conviene que las máquinas que se correspondan con un sistema que vamos a proteger estén dentro del mismo datastore replicado.

aunque solo utilizaremos uno para la recuperación de servidores.

- **Folder Mappings:** son las carpetas dentro del vCenter en donde ubicaremos los servidores recuperados.
- **Networks Mappings:** son las redes dentro de la infraestructura que utilizaremos de un lado y del otro para los servidores recuperados.

Como cuarto paso, tenemos que establecer la ubicación que SRM utilizará para los **placeholder**. Estos son archivos de marcación de posición de los servidores virtuales que se van a recuperar. Por lo tanto, tendremos que configurarlos en el sitio de recuperación. Si queremos proteger servidores en los dos sitios para que el otro sitio remoto oficie de sitio de recuperación en algún momento, debemos configurar los placeholder en los dos sitios.

Los placeholder son unos pequeños archivos que se generan en el datastore y que reservaremos para almacenar los datos de las máquinas virtuales que se van a recuperar. Indican al administrador de VMware que, en esos recursos van a almacenarse las máquinas recuperadas.

También informan al administrador de SRM que los servidores están protegidos realmente. De este modo, las máquinas se verán dentro del inventario de vCenter, pero no podrán encenderse. Estos archivos no se podrán ubicar dentro de los datastores que utilizarán los servidores protegidos, el storage replicado, ya que no se verán hasta que se ejecute el plan de recuperación. Deben estar almacenados en los discos locales del ESXi o en alguna otra ubicación que se comparta entre los servidores intervinientes del cluster de recuperación. Una vez ejecutado el plan de recuperación y recuperados los servidores, se deberán borrar.

En la versión 5 de SRM, disponemos de una ayuda extra para ubicar los equipos replicados, ya que se ven a simple vista mediante otro icono dentro del árbol de administración. Un error muy evidente de versiones anteriores era que, al buscar un servidor protegido por SRM, se lo encontraba dos veces y no se podía establecer cuál era el productivo y cuál su réplica, hasta que no entrábamos en la consola de administración y sus detalles.

Sigamos estos simples pasos para ubicar los placeholder en un datastore.

MAPPING

Hace referencia a los mapeos que se deben establecer entre el sitio de protección y el de recuperación. Permite que el sistema sepa que deberá mover los servidores desde una red a otra, desde un cluster a otro, desde un datastore a otro, etcétera.

PASO A PASO /9

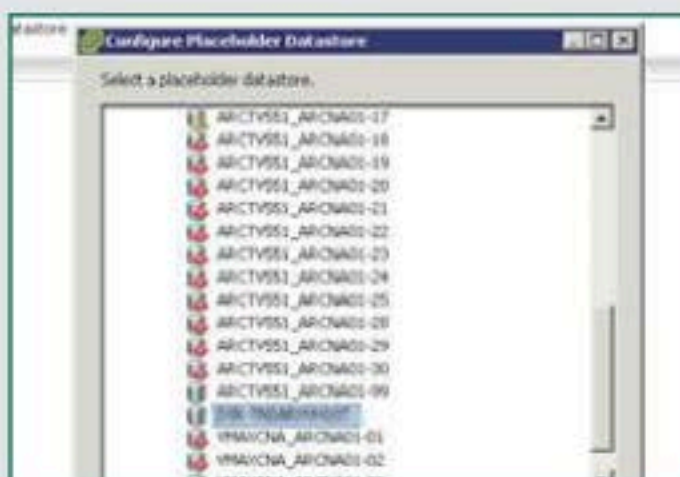
Ubicar los placeholder

1



Vaya a la consola de SRM y pulse **Placeholder Datastores**.

2



En la consola, haga clic en **Configure Placeholder Datastore**. Esto abrirá una ventana emergente, en la cual deberá elegir el datastore en cuestión. Luego, pulse **OK**.

El quinto paso consiste en configurar la replicación de los datastore. Esto dependerá de la elección de storage que hayamos tomado antes.



RESUMEN

En este capítulo, vimos dos de las más importantes herramientas de VMware: VMware vCenter Operations, un sistema extraordinario de monitoreo y estadísticas, y Site Recovery Manager, un sistema de DRP para toda la infraestructura.

CONTENIDO

1. Introducción a la virtualización de servidores

Conceptos
Historia

2. Soluciones de virtualización en el mercado

Diferentes tecnologías
Virtualización de servidores y escritorios

3. VMware como herramienta de virtualización

Por qué VMware
vSphere, ESXi y vCenter
Cluster vSphere, Datacenters y Linked Mode
HA, DRS, VMotion y Storage VMotion
Snapshots, VMware FT y vApps

4. Herramientas sobre plataforma VMware

VMware Operations
VMware SRM, solución de DRP de VMware
VMware Navigator
VMware Chargeback
VMware Configurations

VIRTUALIZACIÓN

En este libro el lector conocerá las ventajas y desventajas de esta revolucionaria tecnología mediante un acercamiento a las soluciones disponibles en el mercado en materia de virtualización. Conocerá VMware en detalle, con una descripción minuciosa de sus características y funciones. También las herramientas que operan sobre plataformas VMware, como Operations, SRM, Navigator, Chargeback y Configurations. Además, todo sobre plataformas de virtualización para workstations y servidores, clusters y data centers.



EXCLUSIVO PARA LECTORES

Profesores en línea:
profesor@redusers.com

Servicios para lectores:
usershop@redusers.com



9 789871 857791