UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA SOLUCIÓN DE ALTA DISPONIBILIDAD Y RECUPERACIÓN ANTE DESASTRES PARA CENTROS DE DATOS BASADA EN TECNOLOGÍAS DE REPLICACIÓN DE DATOS Y VIRTUALIZACIÓN DE SERVIDORES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

GUNTER NÚÑEZ GALINDO

PROMOCIÓN

2007-II

LIMA-PERÚ

2013

A mi familia:

Mis padres Edmundo y Magda,

Mi hermano Ismael

SUMARIO

En el presente trabajo se describe la virtualización de servidores, sistemas de almacenamiento inteligentes, red de área de almacenamiento (SAN), replicación y recuperación ante desastres. Estas tecnologías se complementan entre si y requieren el uso de hardware y software nuevos actuales de última generación para mejores resultados y beneficios.

Esta solución permite a las empresas un mejor uso de los recursos de hardware, reducción de costos de inversión, reducción de costos operacionales, contar con alta disponibilidad y afrontar con éxito los planes de recuperación ante desastres de la información y la reanudación de las operaciones.

La solución implica la utilización de equipamiento de hardware y software en dos centros de datos ubicados en dos ubicaciones geográficas distantes entre sí. El sitio principal alberga al centro de datos de producción y el sitio secundario alberga un centro de datos preparado para entrar en producción ante un desastre parcial o total en el sitio principal.

El marco teórico presenta un resumen de los aspectos relacionados a la virtualización, sistemas de almacenamiento inteligentes, redes SAN, replicación y recuperación ante desastres a fin de que se pueda comprender la solución propuesta en el presente informe.

ÍNDICE

INTRODUCCIÓN

La última década ha sido una época de un rápido incremento de la cantidad e importancia de la información almacenada en los centros de datos empresariales.

La movilidad y la portabilidad de los dispositivos de computo personales tales notebooks, tablets, smartphones han acelerado la demanda de servicios de IT de las empresas como e-commerce, aplicaciones multimedia, y operaciones criticas empresariales como banca, salud, transporte. Así como la cantidad de información crece de manera exponencial, su importancia también crece significativamente.

Aplicaciones de tipo bancario, salud, transporte requieren un alto grado de seguridad y disponibilidad de la información para asegurar que esta sea accesible cuando se necesite. En el sector bancario existen normativas orientadas a la salvaguarda de la información que incrementan la importancia de la protección y continuidad de la infraestructura IT y dan mayor relevancia a la calidad de los niveles de servicio.

Dado que los requerimientos de disponibilidad y performance continúan creciendo, los costos y complejidad para proteger y proporcionar esa información durante un escenario de desastre también aumentan. Los costos y complejidad son un obstáculo para la mayoría de empresas y como resultado se tienen planes de recuperación ante desastres inexistentes o poco confiables.

La rápida adopción y crecimiento de infraestructuras virtualizadas han permitido a las empresas mejorar la eficiencia del uso de recursos computacionales, reducir el consumo de energía en los centros de datos, mejorar la disponibilidad de las aplicaciones y recuperar la información ante desastres.

El presente informe presenta una propuesta de solución que permite mejorar el uso de los recursos de hardware, tener alta disponibilidad de las aplicaciones y protección de la información en caso de desastres en el centro de datos.

Las fuentes bibliográficas utilizadas en el informe, para la explicación de la virtualización se basan principalmente en el fabricante de software de virtualización VMware. Adicionalmente, se usaron documentos relacionados fabricantes de hardware de servidores y sistemas de almacenamiento tales como HP, DELL, y EMC.

El trabajo está organizado en tres capítulos principales:

Capítulo I "Planteamiento de ingeniería del problema".- Estableciendo las

necesidades y objetivos, así como precisando los alcances y una síntesis del trabajo.

Capítulo II "Marco Teórico Conceptual".- Organizado en tres partes: Virtualización de servidores x86 (tipos, arquitectura, beneficios), Sistemas de Almacenamiento (tipos, arquitectura, replicación, beneficios), y Continuidad de Negocio y Recuperación ante Desastres (Causas de la falta de disponibilidad de la información, RTO, RPO, soluciones).

Capítulo III "Metodología para la Solución del Problema".- Evaluación de alternativas (Recuperación ante Desastres con Tecnologías de Virtualización y Replicación, Ventaja de la solución propuesta), topología y funcionalidad de la solución.

Capítulo IV "Presupuesto y Cronograma".- Análisis de costo y relación de tareas y tiempos.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema, para ello primeramente se describe el problema y luego se expone el objetivo del trabajo, también se evalúa el problema y se precisan los alcances del informe, para finalmente presentar una síntesis del diseño presentado.

1.1 Descripción del problema

En el Perú, gran parte de los centros de datos empresariales de todo tamaño aun cuentan con tecnologías antiguas y obsoletas que complican el crecimiento y disponibilidad de las operaciones propias del negocio. Entre las principales consecuencias del uso de tecnología obsoleta en los centros de datos se tiene:

Proliferación de servidores: Los centros de datos albergan una cantidad considerable de servidores antiguos con el agravante de tener un servidor por cada aplicación que tiene o requiera la empresa. Este tipo de enfoque ya es obsoleto en la actualidad.

Gastos Operativos: El tener varios servidores encendidos para mantener las aplicaciones (software) siempre disponibles conlleva a tener una administración descentralizada que implica mayor inversión en cantidad de horas hombre.

Alto consumo de energía: A mayor cantidad de servidores encendidos, mayor es el consumo de energía para mantenerlos encendidos, mayor es el consumo de energía para el enfriamiento de los equipos, y mayor es el consumo de baterías en los UPS.

Aplicaciones dependientes del hardware: Las aplicaciones instaladas en PCs o servidores están atadas al hardware. Si ocurre una falla grave en el hardware, podría tomar horas o días restaurar la información en otro servidor y en ciertas ocasiones se pierde la información.

Alta disponibilidad compleja (clustering a nivel de SO, clustering a nivel de aplicaciones, etc.): Gran parte de las empresas no cuentas con una solución de alta disponibilidad para sus aplicaciones. Esto debido a la complejidad y costos que implica tener este tipo de solución.

Los cambios y mantenimientos requieren cortes de servicio: Para poder realizar operaciones de mantenimiento tales como cambio de partes, agregar CPU, memoria,

disco, etc. es necesario apagar los servidores. Esto implica también cortar servicios propios del negocio tales como acceso a archivos compartidos, correo, impresión, acceso a aplicaciones CRM, ERP, etc. perjudicando así la productividad del negocio.

Planes de recuperación ante desastres complejos y costosos: La gran mayoría de las empresas no poseen estrategias de continuidad de negocio, debido a lo complejo y costoso de esta solución. Incluso si poseen una solución de recuperación ante desastres, es casi imposible poder realizar ensayos de recuperación ante desastres para verificar que la solución funcionará correctamente ante un desastre real.

1.2 Objetivos del trabajo

El presente informe tiene como objetivo lo siguiente:

Explicar los fundamentos teóricos del uso de servidores como la base de la adopción de la virtualización.

Explicar los aspectos teóricos sobre la virtualización de servidores, sus capacidades y beneficios para las empresas.

Explicar los aspectos teóricos sobre el uso de sistemas de almacenamiento, su funcionamiento y beneficios.

Explicar los aspectos teóricos sobre la Continuidad de Negocio y Recuperación ante desastres.

Presentar una propuesta de solución con alta disponibilidad y recuperación ante desastres para los centros de datos mediante el uso de la virtualización de servidores y replicación de datos entre sistemas de almacenamiento.

1.3 Evaluación del problema

En el presente informe se presenta una propuesta de solución orientada a empresas que poseen una infraestructura tradicional de servidores (sin virtualización) las cuales necesitan contar con una solución que proporcione alta disponibilidad para sus aplicaciones y a la vez permita afrontar con éxito una situación de recuperación ante desastres en un sitio secundario ante la pérdida parcial o total del centro de datos del sitio principal.

1.4 Alcance del trabajo

El presente trabajo se enfoca en describir un diseño respecto a servidores, virtualización, sistemas de almacenamiento, y replicación de los datos. No abarca el diseño de redes LAN, soluciones de backup, diseño de aplicaciones, seguridad perimetral, sistemas de energía, construcción de sitio principal y sitio secundario.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen los conceptos y términos básicos para la compresión del tema desarrollado en el presente informe. Su objetivo es tener en claro los aspectos teóricos de la virtualización de servidores y replicación de sistemas de almacenamiento como tecnologías que permiten el uso eficiente de los recursos, alta disponibilidad y recuperación ante desastres en los centros de datos.

2.1 Virtualización de Servidores x86

En términos generales, la virtualización es la tecnología que permite abstraer los recursos físicos tales como procesamiento, almacenamiento y red para hacerlos aparecer como recursos lógicos.

En la virtualización de servidores x86 se agrega una capa de virtualización entre el hardware y el sistema operativo (Figura 2.1). Esta capa de virtualización permite ejecutar múltiples instancias de sistemas operativos de manera concurrente en un solo servidor físico.

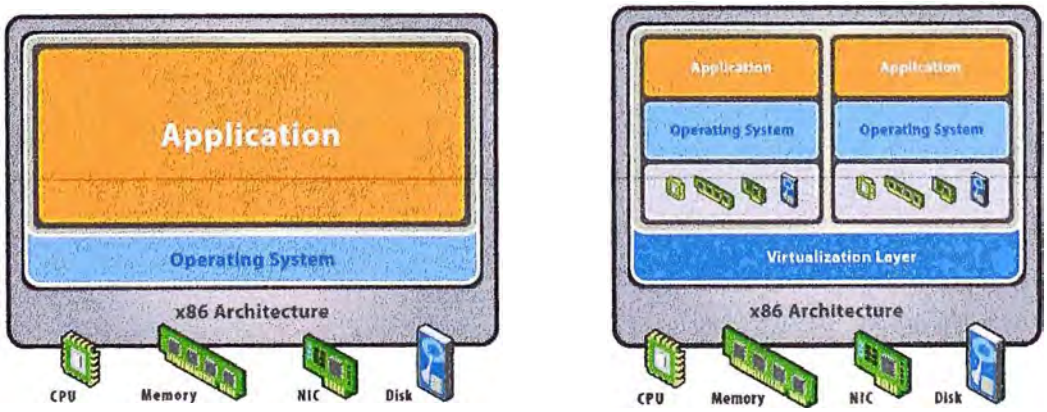


Figura 2.1 Capa de virtualización x86

Como consecuencia, la virtualización permite unir recursos físicos y proporcionar un conjunto agregado de capacidades de los recursos físicos (Figura 2.2).

En la actualidad existen tres marcas líderes en el mercado de la virtualización de servidores x86: VMware, Microsoft, y Citrix. La Figura 2.3 muestra el Cuadrante Mágico de Gartner (Junio 2013) para Virtualización de Servidores x86.

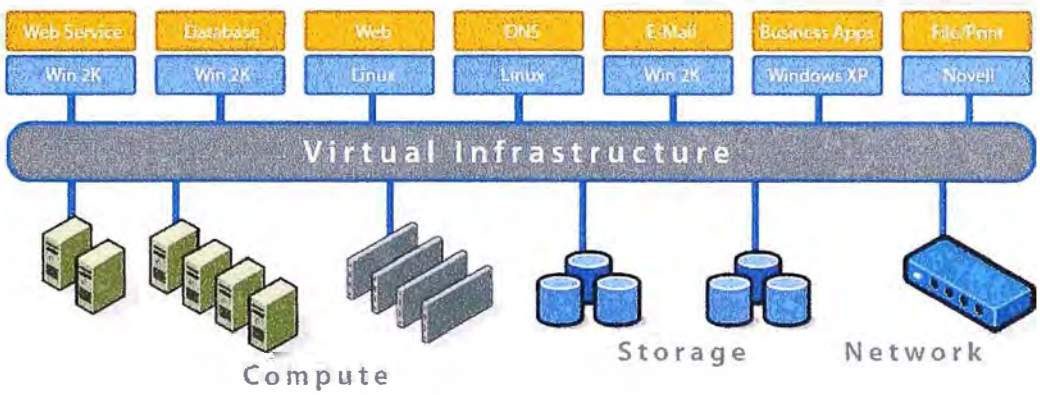


Figura 2.2 Infraestructura virtualizada

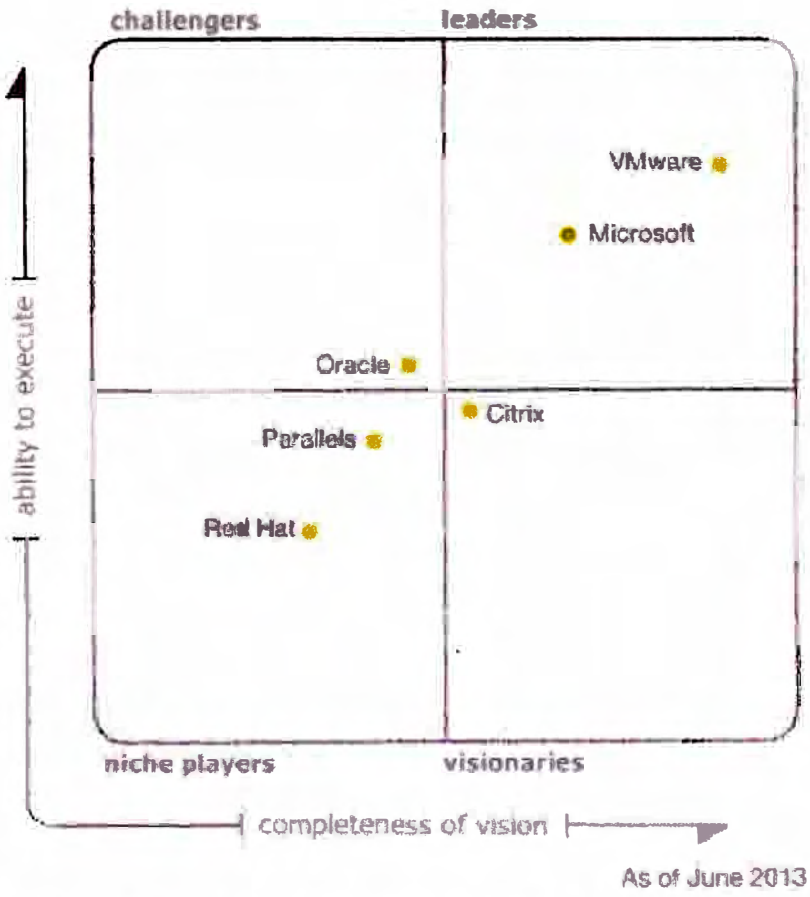


Figura 2.3 Cuadrante Mágico de Gartner para Virtualización de Servidores x86 (Junio 2013)

A continuación se presentan los conceptos y términos usados comúnmente en la virtualización de servidores x86.

2.1.1 Host

Es un servidor x86 el cual está conformado principalmente por CPU, memoria, discos, dispositivos I/O (NICs y HBAs) y software (sistema operativo, sistema de archivos, LVM, drivers de dispositivos, etc.) los cuales permiten realizar las operaciones de cómputo.

El software se ejecuta sobre un host y permite el procesamiento de datos de entrada y salida (I/O).

En la figura 2.4 se presenta los principales componentes de un servidor x86.

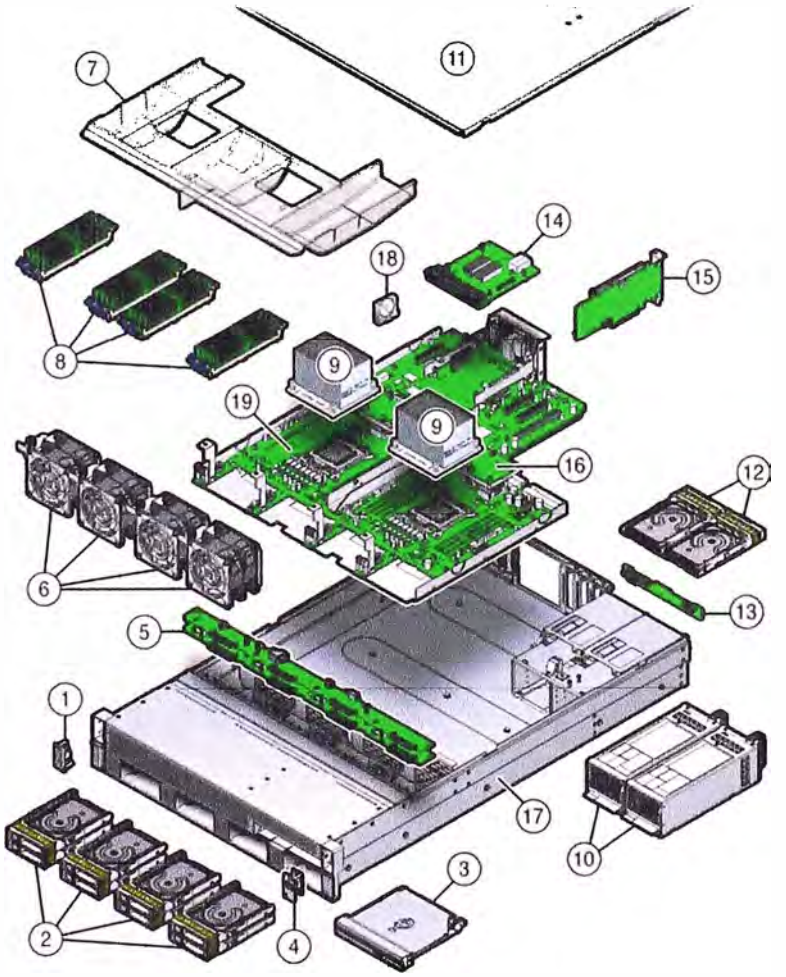


Figura 2.4 Componentes de un servidor x86

Leyenda:

1 Módulo indicador LED izquierdo

2 Unidades de disco

3 Unidad DVD

4 Módulo indicador LED derecho

5 Backplane frontal de unidades de discos

6 Módulos de ventilación

7 Deflector de aire

8 Ranuras DIMM

9 Procesadores and disipadores de calor

10 Fuentes de poder

11 Cubierta superior

12 Unidades de discos traseros

13 Backplane posterior de unidades de discos

14 Módulo expander SAS

15 Tarjeta PCIe

16 Mezzanine board

17 Chasis de sistema

18 Batería de sistema

19 Motherboard

En la actualidad existen diversas marcas de servidores x86, entre los cuales se encuentran principalmente HP, IBM, Dell, Cisco y Oracle. Estas marcas ofrecen 3 tipos de servidores según su factor de forma:

a) Tipo Torre: No necesita una ambiente especial para su funcionamiento. No se pueden apilar y ocupan espacio (Figura 2.5).

Figura 2.5 Servidor tipo torre Dell PowerEdge T320

b) Tipo Rack: Requieren un ambiente con enfriamiento de precisión ya que son colocados apilados en gabinetes especiales junto con sistemas de almacenamiento y dispositivos de red. Al ser instalados apilados en rack, se requiere de accesorios adicionales para el ordenamiento del cableado LAN, SAN y de energía (Figura 2.6).

Figura 2.6 Servidor tipo rack Oracle Sun Server X3-2L

c) Tipo Blade: Requieren un ambiente con enfriamiento de precisión. Son colocados en un chasis especial ya que son pequeños y delgados. El chasis proporciona energía, ventilación, conectividad LAN y SAN lo cual reduce el cableado en un 87%. Ocupan poco espacio y consumen menos energía. (Figura 2.7)

Figura 2.7 Servidores tipo blade HP ProLiant BL460c G7

2.1.2 Hipervisor

Es una capa de software que generalmente proporciona capacidades de particionamiento el cual se ejecuta directamente sobre el servidor.

Esta capa de virtualización permite ejecutar múltiples instancias de sistemas operativos con sus aplicaciones instaladas de manera concurrente dentro de "máquinas virtuales" en un solo servidor particionando y compartiendo dinámicamente la disponibilidad de recursos físicos tales como CPU, memoria, almacenamiento y

dispositivos de entrada y salida.

En un servidor físico se pueden crear varias máquinas virtuales dependiendo de las capacidades del servidor físico.

Existen dos tipos de hipervisores en el mercado:

a) Hipervisor Tipo 1: Es un hipervisor que se ejecuta directamente sobre el servidor físico. Por este motivo se le conoce comúnmente como hipervisor bare-metal: Ej.: VMware ESXi, Microsoft Hyper-V 2012, Citrix XenServer, Oracle VM.

   Este tipo de hipervisor es el más usado en centros de datos, destacando VMware ESXi por ser el más avanzado y confiable para entornos de producción críticos.

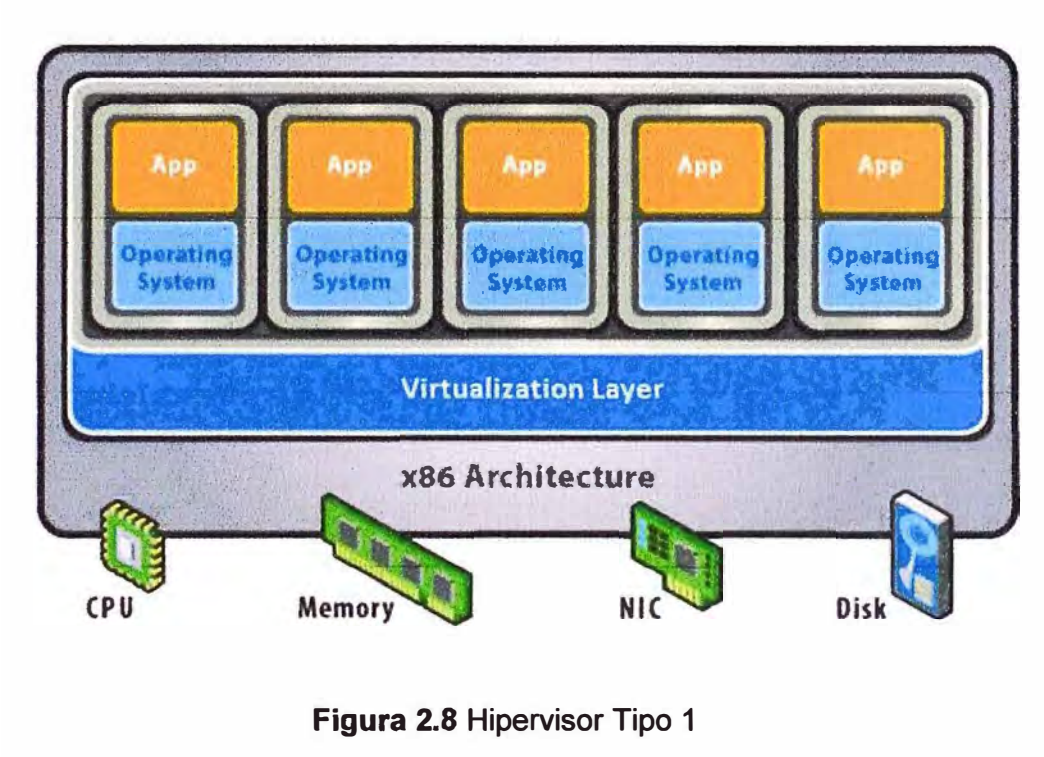


Figura 2.8 Hipervisor Tipo 1

b) Hipervisor Tipo 2: Es un hipervisor que se ejecuta como una aplicación sobre un sistema operativo existente. Ej.: VMware Workstation, Oracle VirtualBox y Microsoft Virtual PC (Figura 2.9).

   Este tipo de hipervisor generalmente se usa en entornos de prueba y para fines académicos.

2.1.3 Máquina Virtual

Una máquina virtual es una entidad lógica que se presenta como un servidor físico al sistema operativo, con sus propio CPU, memoria, NIC, y discos. De este modo, en un servidor físico, todas sus máquinas virtuales comparten los mismos recursos de hardware físico subyacente de manera aislada (Figura 2.10).

Desde el punto de vista del hipervisor una máquina virtual es un conjunto de archivos

discretos entre los que se encuentran: archivos de configuración, archivos de datos, etc.

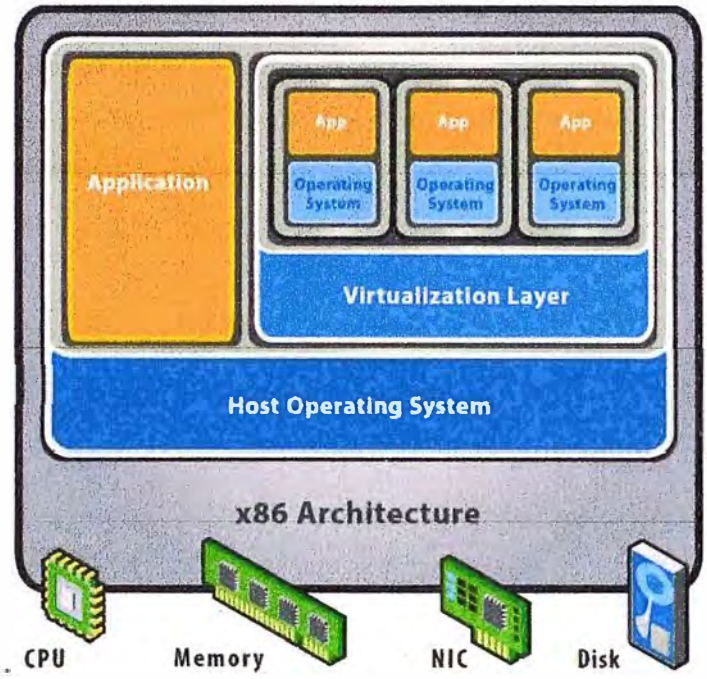


Figura 2.9 Hipervisor Tipo 2

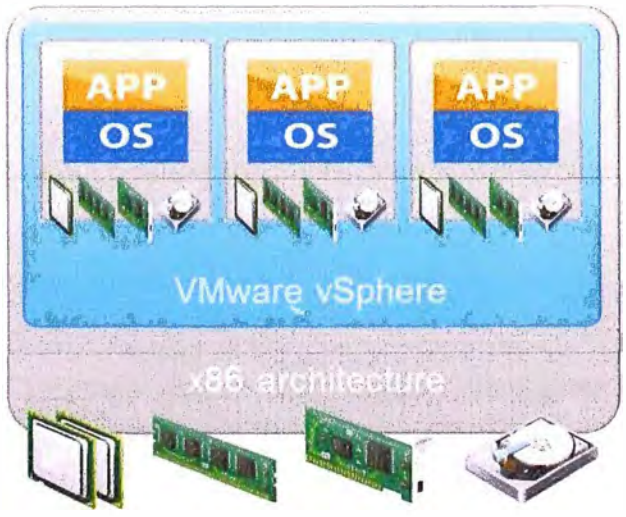


Figura 2.10 Máquinas virtuales

Una máquina virtual usa hardware virtual. El sistema operativo instalado en una máquina virtual reconoce los dispositivos de hardware virtual y no detecta que estos sean virtuales.

En una máquina virtual se pueden configurar dispositivos virtuales como: CPUs, RAM,

discos duros, controladoras de red (NICs), unidades de CD/DVD, unidades floppy y dispositivos SCSI.

Se pueden conectar dispositivos USB tales como discos duros y llaves de seguridad a una máquina virtual que reside en un host al cual se le conectó el dispositivo USB. Un dispositivo USB solo puede ser accedido por una máquina virtual. Se tiene que remover el dispositivo USB de una máquina virtual para luego conectarlo a otra máquina virtual que este ejecutándose en el mismo host.

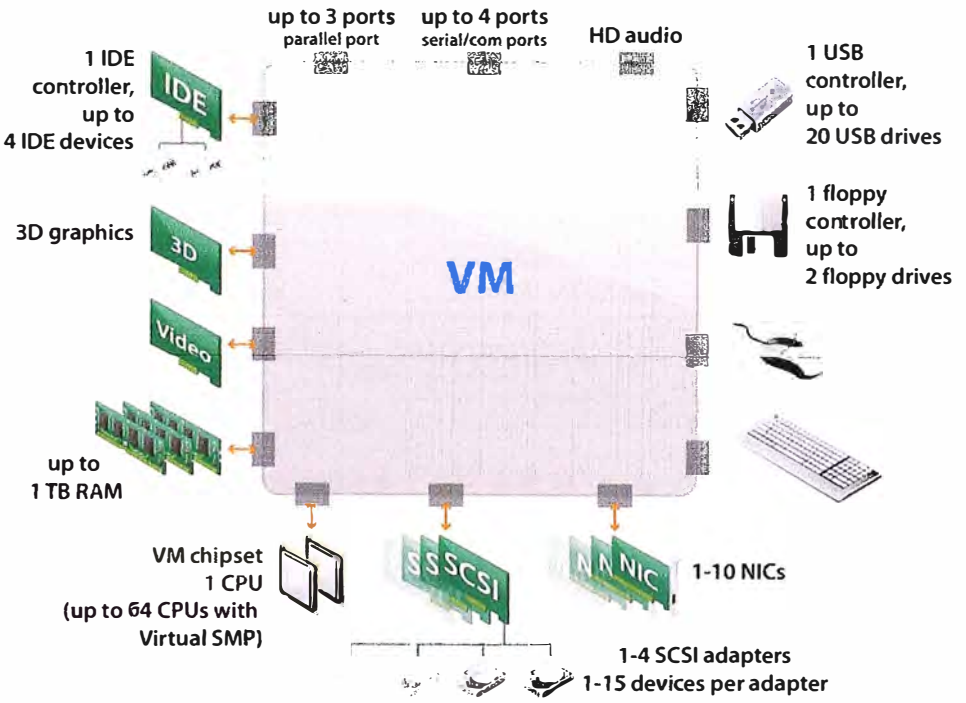


Figura 2.11 Hardware virtual de una máquina virtual

En la actualidad es posible crear máquinas virtuales con las siguientes capacidades máximas:

Tabla 2.1 Capacidades máximas de una máquina virtual

ITEM	Máximos
CPUs vituales	64
RAM virtual	1 TB
Discos duros virtuales	60
Tamaño de disco duro virtual	62 TB
NICs virtuales	10

CPU Virtual (vCPU): La asignación de CPUs virtuales a una máquina virtual está relacionado con la cantidad de CPUs Lógicos que tenga el host.

En un servidor de 2 CPUs (con 6 cores por CPU) y con hyperthreading activado se tendría 24 CPUs lógicos (LCPUs). Esto permitiría crear máquinas virtuales de hasta 24 vCPUs.

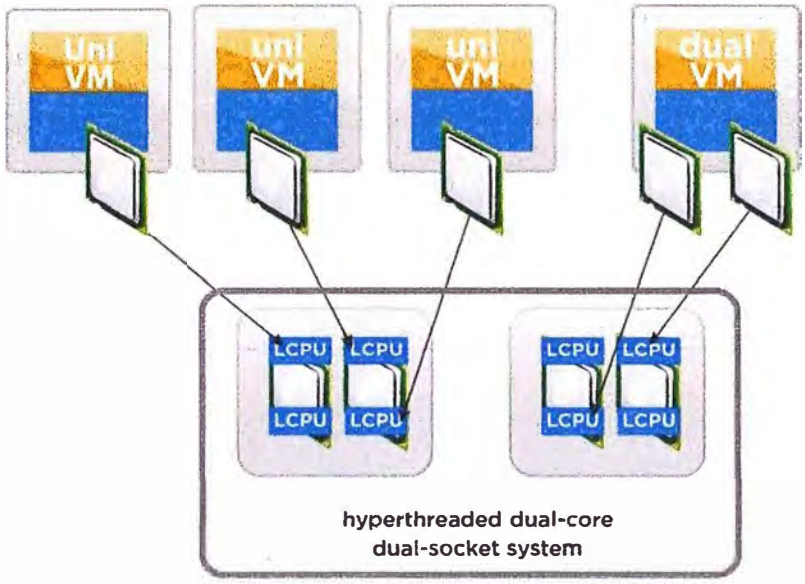


Figura 2.12 CPU Virtual

Memoria Virtual (vRAM): Memoria RAM que se asigna a una máquina virtual. La suma de la memoria virtual asignada a cada una de las máquinas virtuales no debe exceder a la memoria física instalada en el host. Sin embargo, el hipervisor tiene la capacidad de entregar más memoria de la que dispone el host. Esta característica se le conoce como sobresuscripción de memoria.

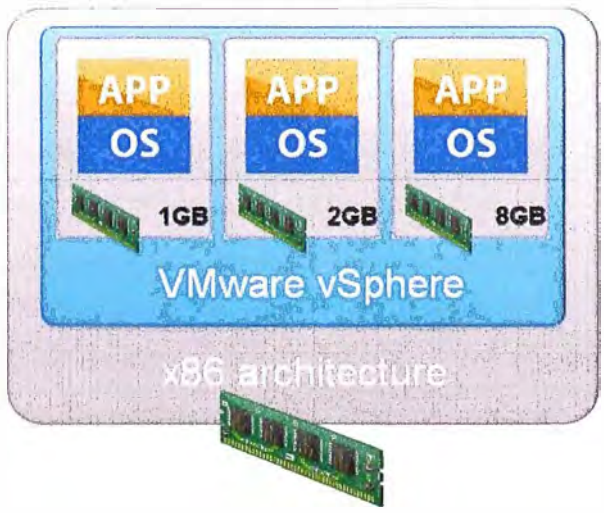


Figura 2.13 Memoria Virtual

Disco Virtual (vDisk): Una máquina virtual es un conjunto discreto de archivos que

pueden ser movidos, copiados y usados como una plantilla. El disco virtual junto con los demás archivos que conforman una máquina virtual son almacenados en un directorio sobre un sistema de archivos de tipo clúster llamado Virtual Machine File System (VMFS). VMFS es un sistema de archivos tipo clúster optimizado para alojar máquinas virtuales. Mientras un sistema de archivos convencional permite que un servidor tenga acceso de lectura/escritura al mismo sistema de archivos en un determinado instante, VMFS proporciona almacenamiento compartido para permitir que múltiples hosts lean y escriban al mismo almacenamiento concurrentemente.

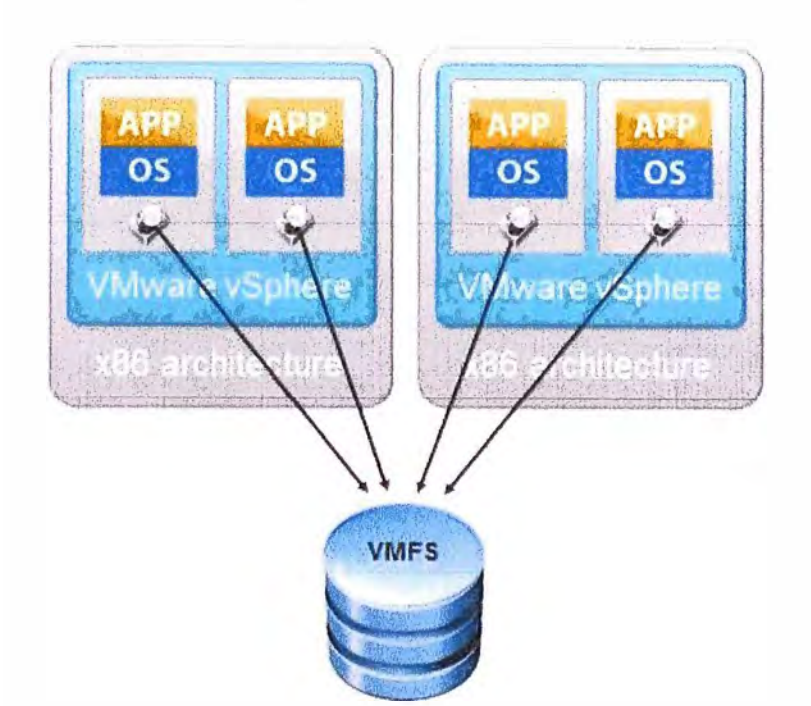


Figura 2.14 Disco Virtual

NIC Virtual (vNIC): Una máquina virtual puede ser configurada con una o más adaptadores de red virtuales (**vNICs**) de manera similar a un servidor físico. Estos adaptadores de red virtuales permiten a la máquina virtual comunicarse con la red de datos. Para lograr esta comunicación, los adaptadores de red virtuales de las máquinas virtuales son conectados "virtualmente" a los "switches virtuales".

Los switches virtuales se ejecutan dentro del hipervisor emulando un switch de red Ethernet tradicional enviando tramas en la capa de enlace de datos. Se pueden configurar varios switches virtuales con más de 1000 puertos virtuales dentro de un host.

Los switches virtuales permiten comunicar a las máquinas virtuales conectadas con la red de datos física a través de los puertos físicos del servidor. Estos puertos de red físicos del servidor, que forman parte del switches virtual, son conectados a los switches físicos de la red de datos.

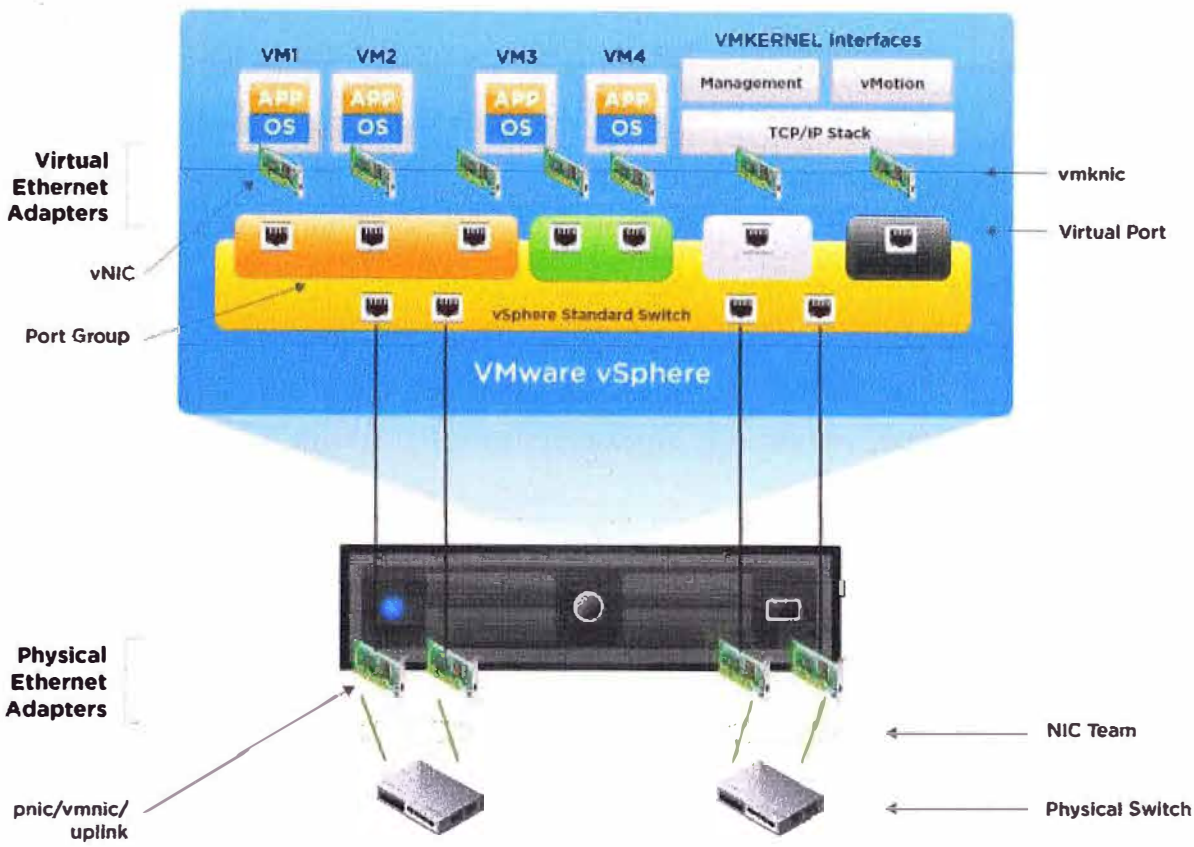


Figura 2.15 Tarjetas de red virtuales (vNIC) y switches virtuales

2.1.4 Arquitectura de un Entorno Virtualizado

La virtualización permite a los administradores crear un data center virtual el cual es administrado de manera centralizada por servidores de administración ya sea vía un software cliente, interface Web, terminal, etc.

Un data center virtualizado está conformado principalmente por servidores x86, sistemas de almacenamiento, switches para redes LAN, switches para redes SAN, servidores de administración centralizada y desktop cliente.

Servidores: En entornos virtualizados se les conoce comúnmente como hosts. Generalmente estos hosts se encuentran configurados en un agrupamiento llamado clúster el cual permite dar un conjunto de recursos de manera agregada a las máquinas virtuales, alta disponibilidad y balanceo de carga.

Los hosts son los encargados de proporcionar vCPU, vRAM y vNIC a las máquinas virtuales que se ejecutan sobre ellos.

Sistemas de almacenamiento: Permiten almacenar las máquinas virtuales que se ejecutan en los hosts de manera centralizada. Los sistemas de almacenamiento

generalmente son conectados a la red SAN mediante tecnologías tales como Fibre Channel (FC), iSCSI y FCoE

Red SAN: Es una red de switches dedicados que permiten la comunicación entre los host y los sistemas de almacenamiento.

Red LAN: Es una red de switches que permite la comunicación de los usuarios hacia los servicios y aplicaciones alojadas en los servidores.

Administración: Conformado generalmente por servidores dedicados con aplicaciones de administración instaladas. Permiten configurar, desplegar y monitorear la infraestructura virtual a través de consolas de administración gráficas.

Clientes de escritorio: Son computadores que tienen acceso restringido a la administración de la infraestructura virtual.

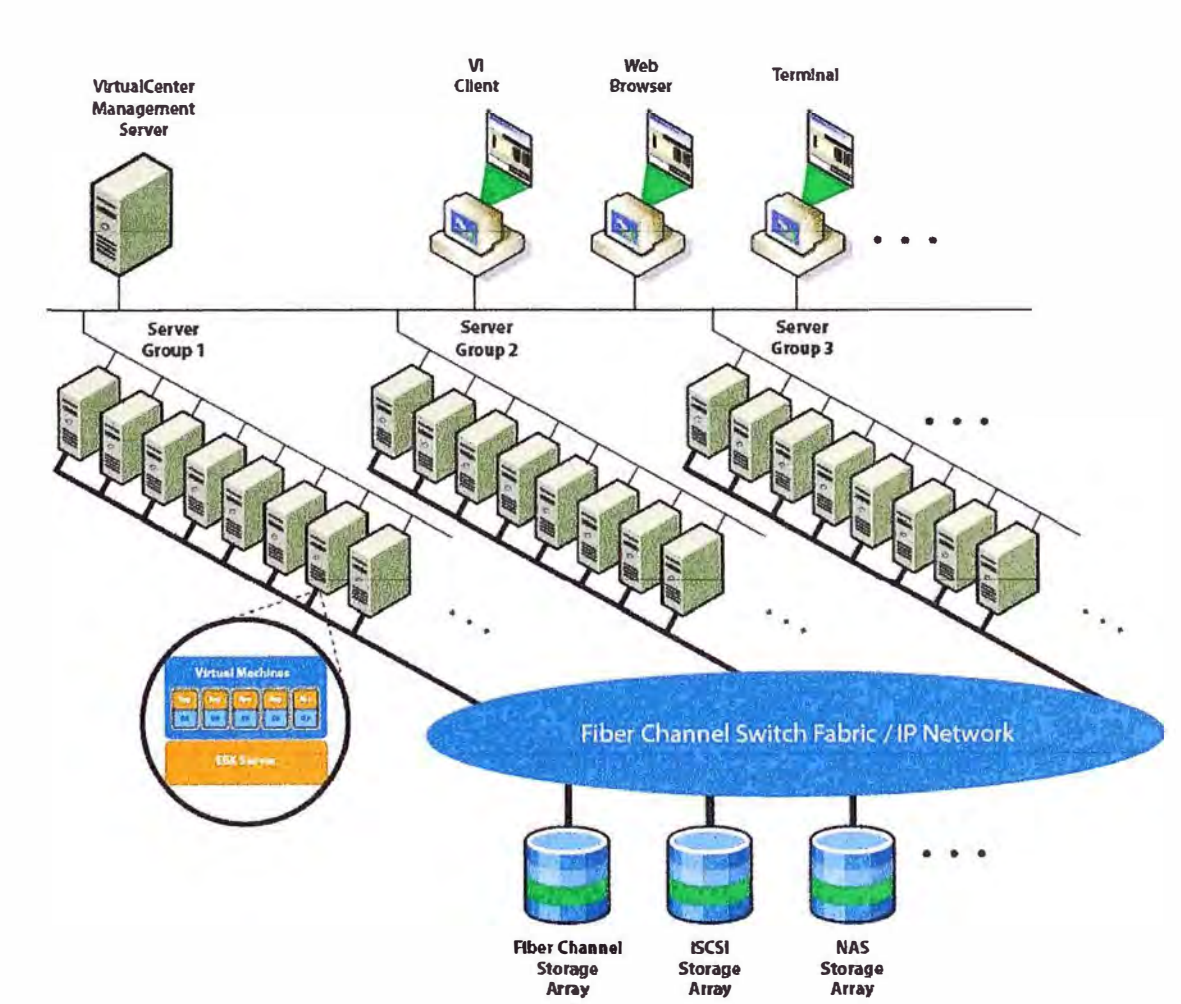


Figura 2.16 Data Center Virtual

2.1.5 Funcionalidades

La virtualización además de permitir la reducción de la cantidad de servidores mediante la consolidación, permite el uso de tecnologías que permiten la optimización del

uso de recursos, balanceo de carga, alta disponibilidad, escalabilidad entre otros.

En el presente informe se tomara como referencia el software de virtualización líder a nivel mundial, VMware vSphere.

VMware vSphere es una plataforma de virtualización que permite la construcción de infraestructuras virtuales (nubes). Permite cumplir acuerdos de niveles de servicio (SLAs) para las aplicaciones más críticas y a la vez conseguir el menor costo total de propiedad (TCO).

Las principales funcionalidades que brinda VMware vSphere son:

VMware ESXi: Es un hipervisor de alta performance, robusto y confiable para centros de datos con entornos críticos. Permite que varias máquinas virtuales puedan compartir los recursos físicos del host.

VMware vCenter Server: Es la consola de administración. Permite configurar máquinas virtuales, servidores ESXi asi como monitorear la infraestructura virtual.

Virtual Symmetric Multiprocessing (vSMP): Permite que las máquinas virtuales puedan escalar hasta 64 vCPUs.

Virtual Machine File System (VMFS): Sistema de archivos de tipo clúster propietario de VMware diseñado para almacenar máquinas virtuales. A la unidad de almacenamiento con formato VMFS se le conoce como datastore.

vMotion: Permite la migración de máquinas virtuales encendidas de un host hacia otro.

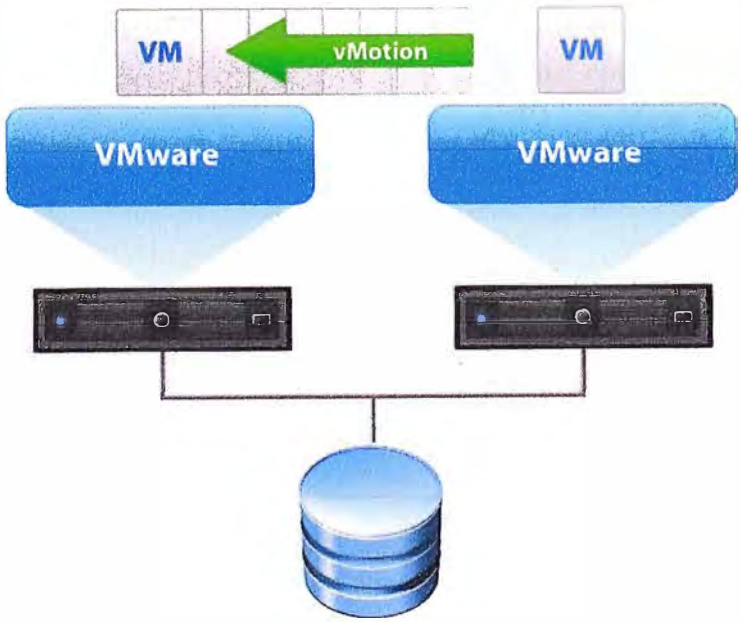


Figura 2.17 Migración de máquinas virtuales mediante vMotion

High Availability (HA): Permite el reinicio automático de máquinas virtuales que se

apagan debido a una falla en el hardware del host. Las máquinas virtuales son reiniciadas automáticamente en otros hosts del clúster.

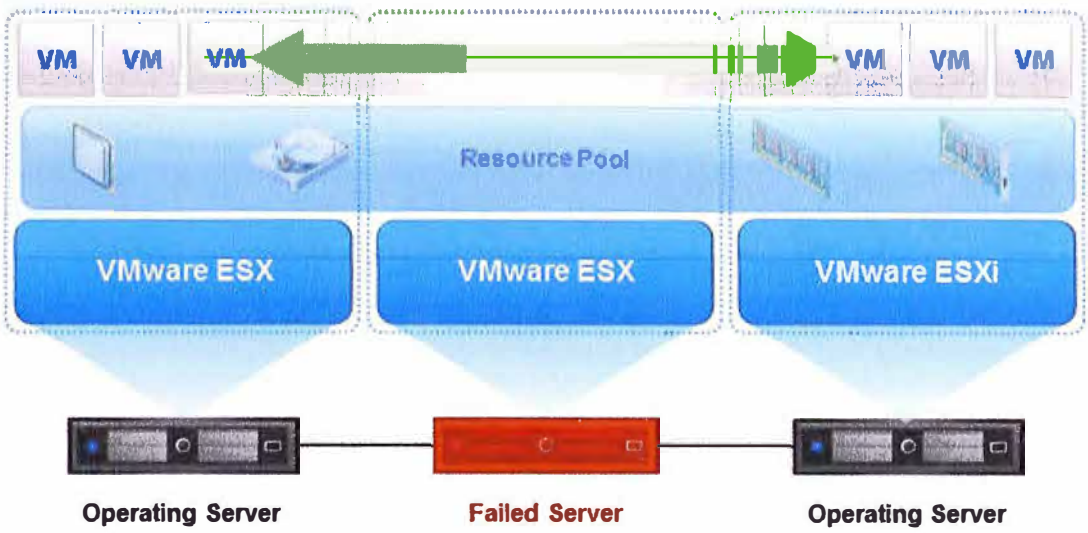


Figura 2.18 Alta disponibilidad de máquinas virtuales mediante High Availability (HA)

Fault Tolerance (FT): Permite proporcionar disponibilidad continua de una máquina virtual y sus aplicaciones creando una máquina virtual duplicada secundaria que está siempre sincronizada con la primaria.

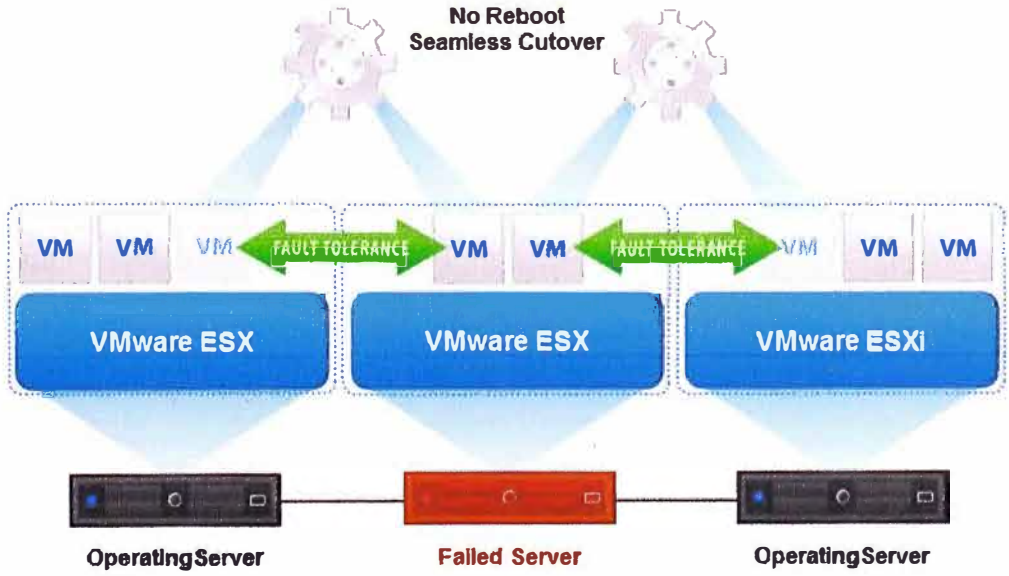


Figura 2.19 Disponibilidad continua de máquinas virtuales mediante Fault Tolerance (FT)

Distributed Resource Scheduler (DRS): Permite el balanceo de carga automático del uso de CPU y memoria RAM de los host del clúster. Realiza migraciones automáticas de máquinas virtuales por vMotion hasta lograr un balanceo en uso de recursos en todos

los hosts del clúster.

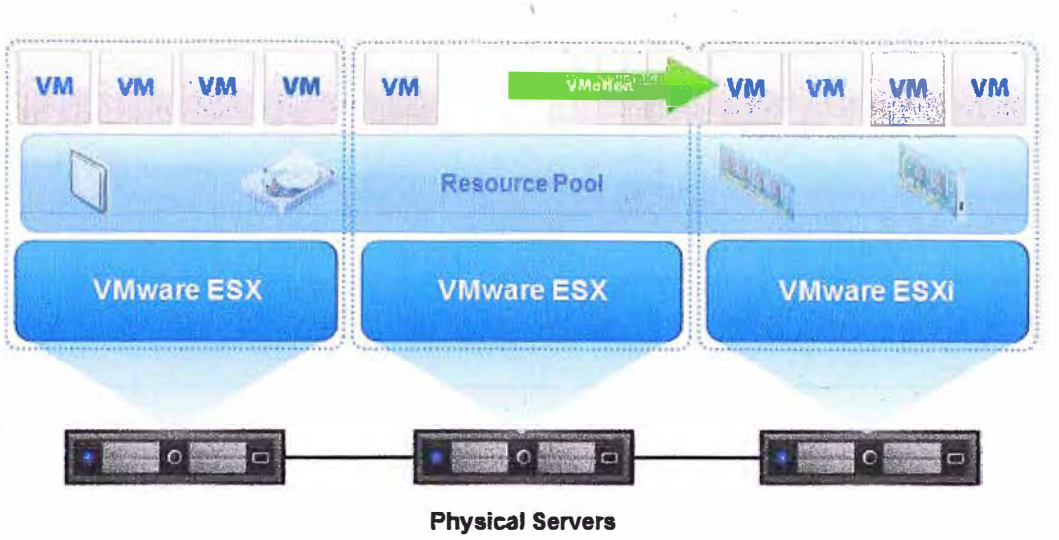


Figura 2.20 Balaceo de carga de máquinas virtuales mediante Distributed Resource Scheduler (DRS)

Distributed Power Management (DPM): Permite el ahorro de energía al redimensionar dinámicamente la capacidad total de un clúster de hosts de acuerdo a la demanda de recursos de las máquinas virtuales. DPM apagará hosts cuando el consumo de CPU y memoria del clúster bajen y encenderá hosts del clúster cuando el consumo se eleve.

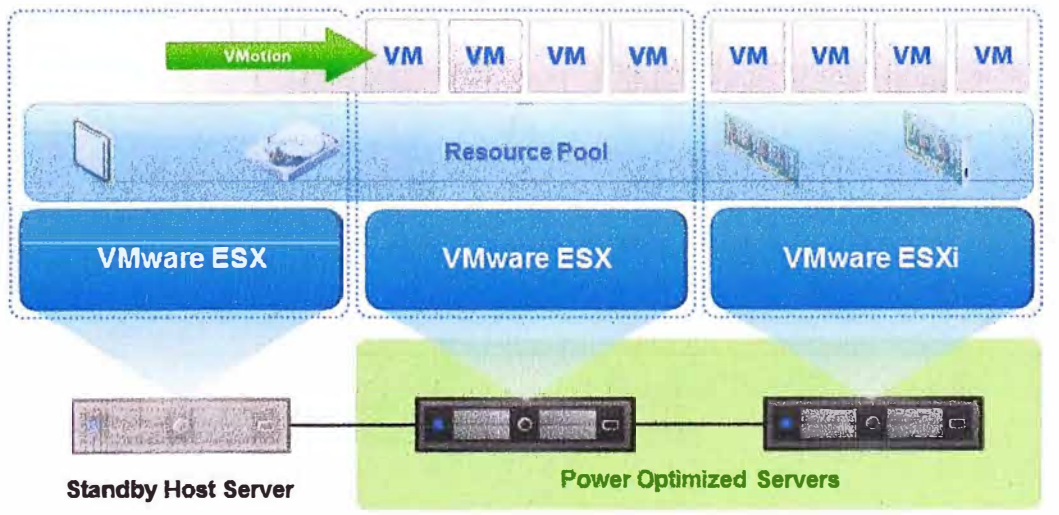


Figura 2.21 Administración del consumo de energía de hosts mediante Distributed Power Management (DPM)

Storage vMotion: Permite la migración de máquinas virtuales encendidas de un

sistema de almacenamiento a otro sin ninguna interrupción manteniendo la integridad de los datos.

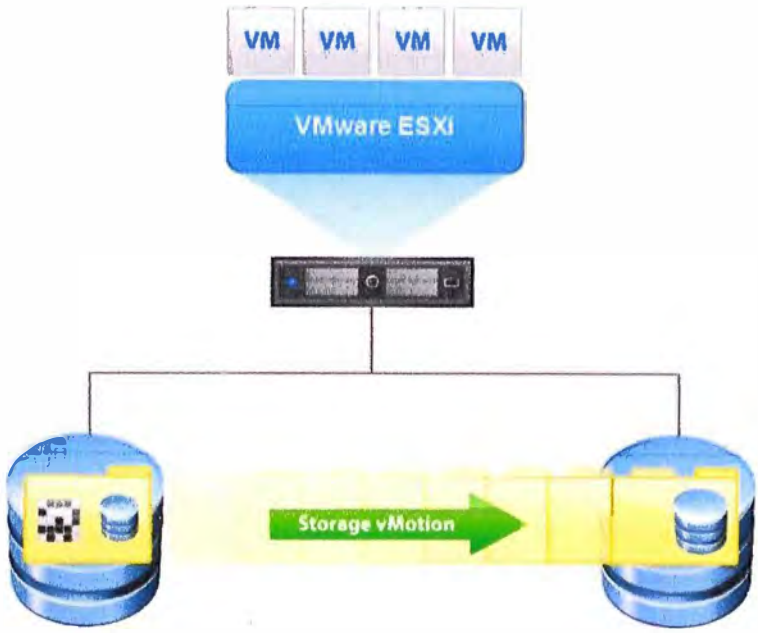


Figura 2.22 Migración de máquinas virtuales mediante Storage vMotion

Storage DRS: Permite el balanceo de carga de utilización de I/O y consumo de espacio en un clúster de datastores determinando la mejor ubicación para almacenar a las máquinas virtuales permitiendo así la reducción de cuellos de botella de utilización de I/O.

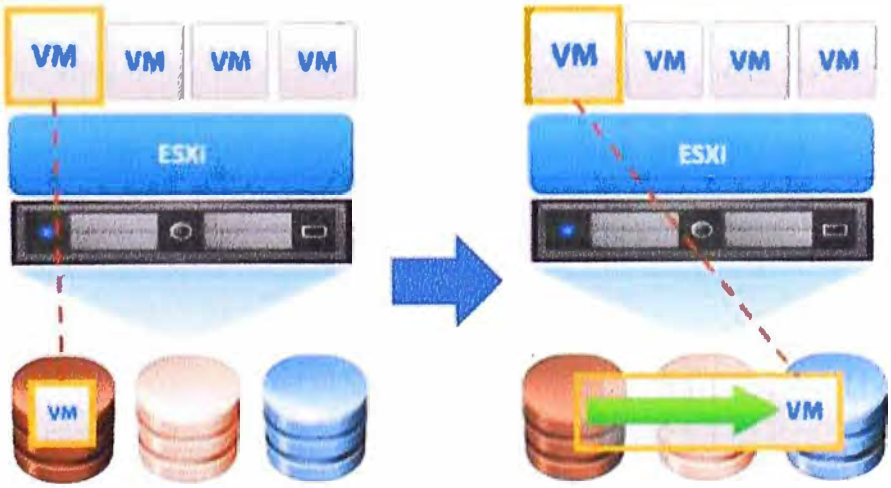


Figura 2.23 Balaceo de carga de almacenamiento mediante Storage DRS

Thin Provisioning: Permite que la capacidad de disco duro virtual asignada no sea reservada en el datastore. A medida que se incrementa la información almacenada en el disco virtual, dinámicamente se consume espacio en el datastore.

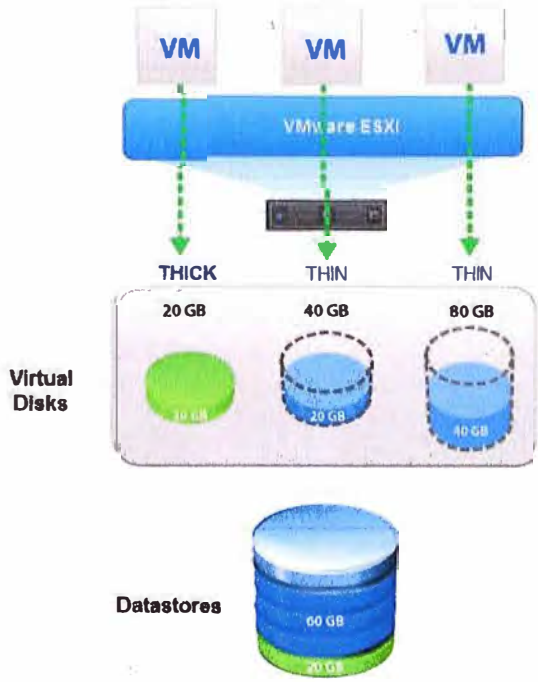


Figura 2.24 Consumo disco virtual mediante Thin Provisioning

Network I/O Control (NIOC): Permite configurar políticas a nivel de máquina virtual y asegurar que los recursos de tráfico de red estén siempre disponibles para las aplicaciones más críticas (QoS). Cada vez que se detecta congestión, NIOC automáticamente reasigna recursos a las aplicaciones de más alta prioridad según las reglas definidas.

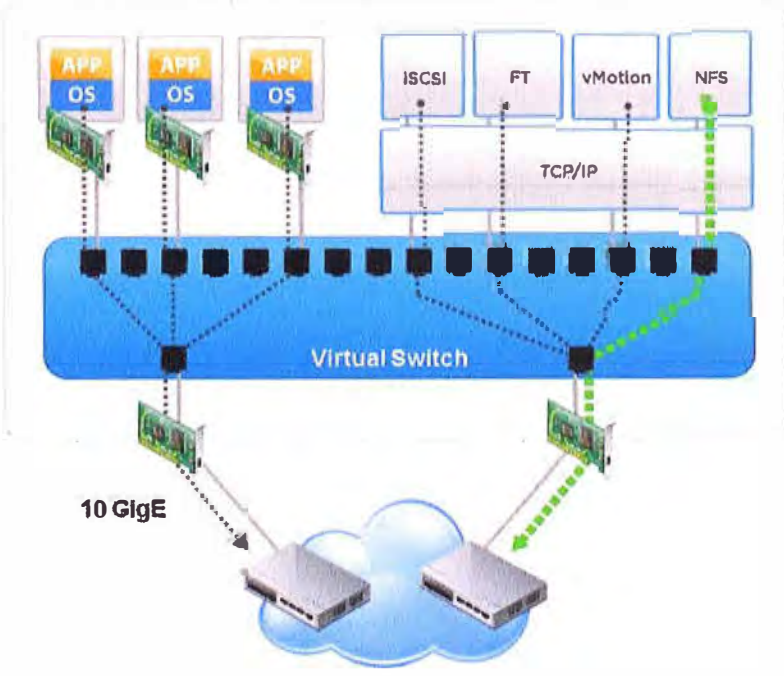


Figura 2.25 Control de utilización de red mediante Network I/O Control (NIOC)

Storage I/O Control (SIOC): Permite configurar políticas a nivel de datastore y asegurar que los recursos de I/O estén siempre disponibles para las máquinas virtuales más críticas. SIOC automáticamente reasigna recursos a las aplicaciones de más alta prioridad según las reglas definidas.

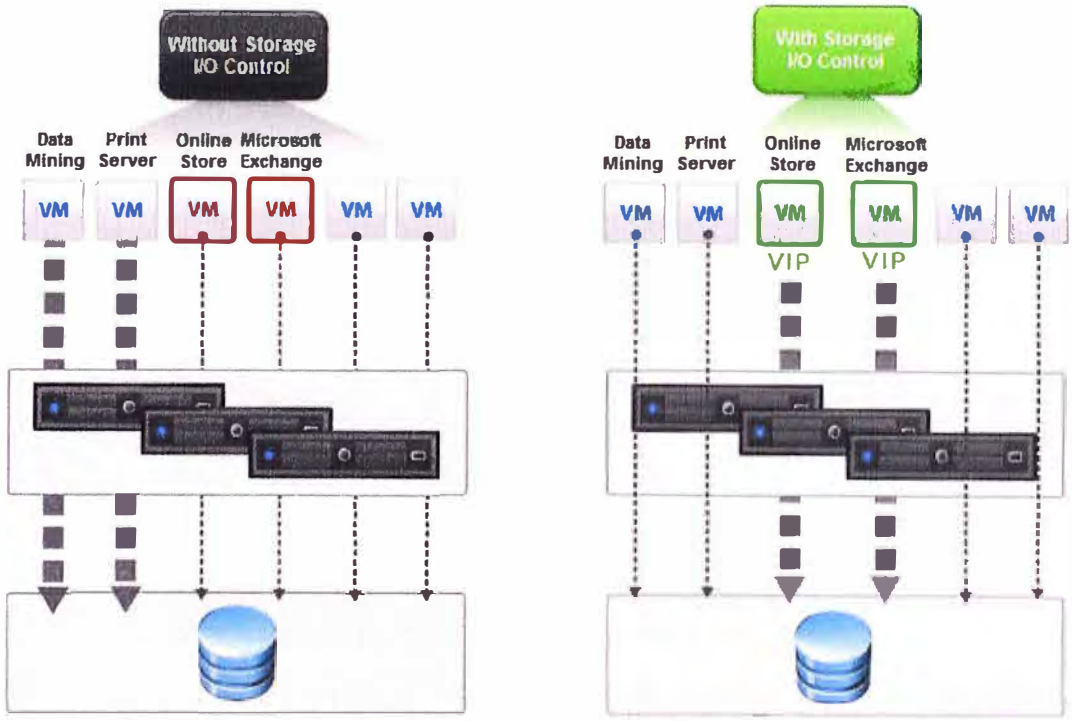


Figura 2.26 Control de utilización de almacenamiento mediante Storage I/O Control (SIOC)

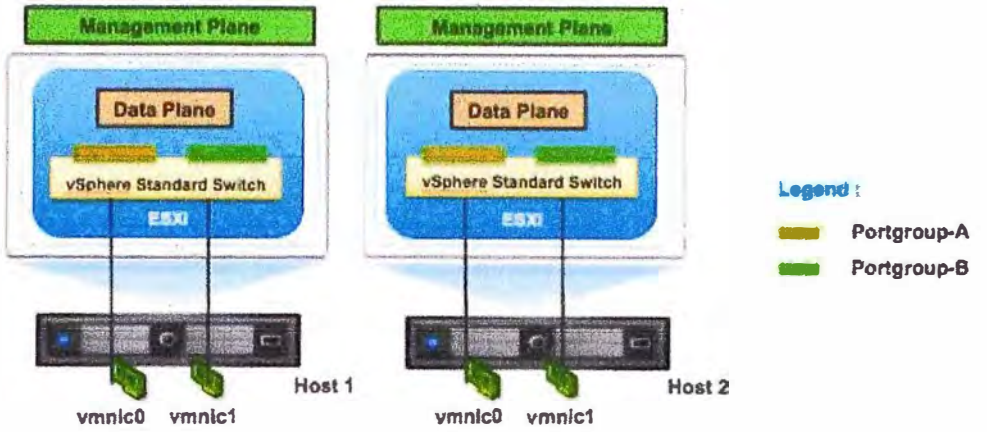
Virtual Standard Switch (vSS): Permite la comunicación de las máquinas virtuales con el entorno red de datos física. Se configura y administra a nivel de host (Figura 2.27).

Virtual Distributed Switch (vDS): Similar al vSS, pero funciona como un único switch a través de todos los host. Se configura y administra a nivel de la consola vCenter Server (Figura 2.28).

Existen productos adicionales que permiten extender los beneficios de VMware vSphere, entre ellos tenemos:

VMware Horizon View: Es una solución de infraestructura de escritorios virtuales (VDI) que permite la administración simplificada de los escritorios los cuales se entregan a los dispositivos de los usuarios finales (PCs, laptops, tablets, smartphones) a través de la red LAN o WAN. Los escritorios virtuales (máquinas virtuales con sistema operativo cliente) son administrados y almacenados de manera centralizada usando al infraestructura virtual VMware vSphere. La figura 2.29 muestra la arquitectura de esta

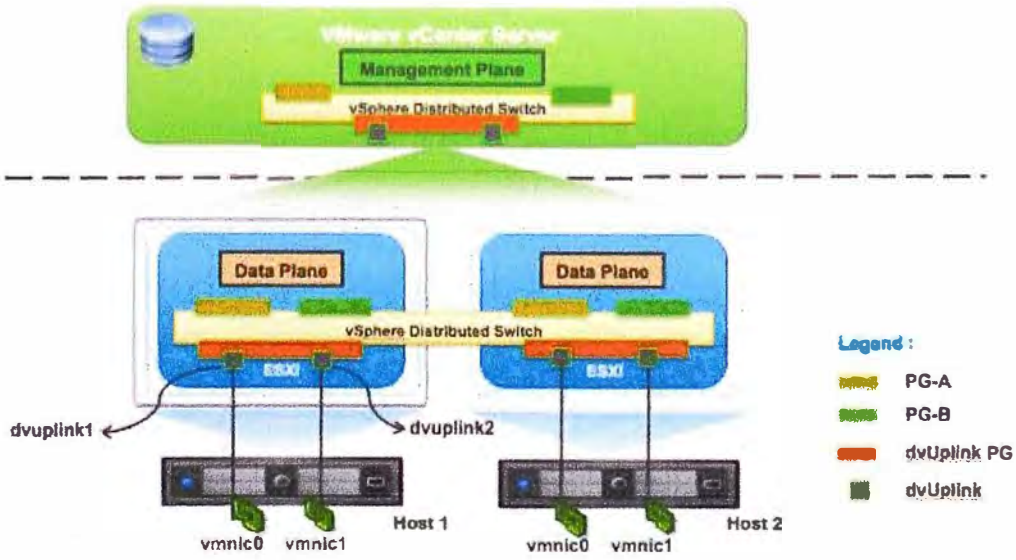
solución.



Management Plane : Allows to configure various parameters of the virtual switch

Data Plane : Handles the packet switching function

Figura 2.27 Switch virtual Estándar (Virtual Standard Switch)



One Management Plane : Allows to configure various parameters of the distributed switch

Data Plane : Handles the packet switching function

Figura 2.28 Switch virtual distribuido (Virtual Distributed Switch)

VMware vCenter Site Recovery Manager (SRM): Es una solución recuperación ante desastres que garantiza protección contra incidentes planeados y no planeados en el sitio principal de producción. Permite la administración centralizada de los Planes de Recuperación ante Desastres (DRPs) de la infraestructura virtual y automatiza el reinicio de las máquinas virtuales de producción en el sitio de recuperación. SRM permite realizar pruebas de failover y failback en cualquier momento sin causar impacto alguno en el sitio

principal. La figura 2.30 muestra la arquitectura de esta solución.

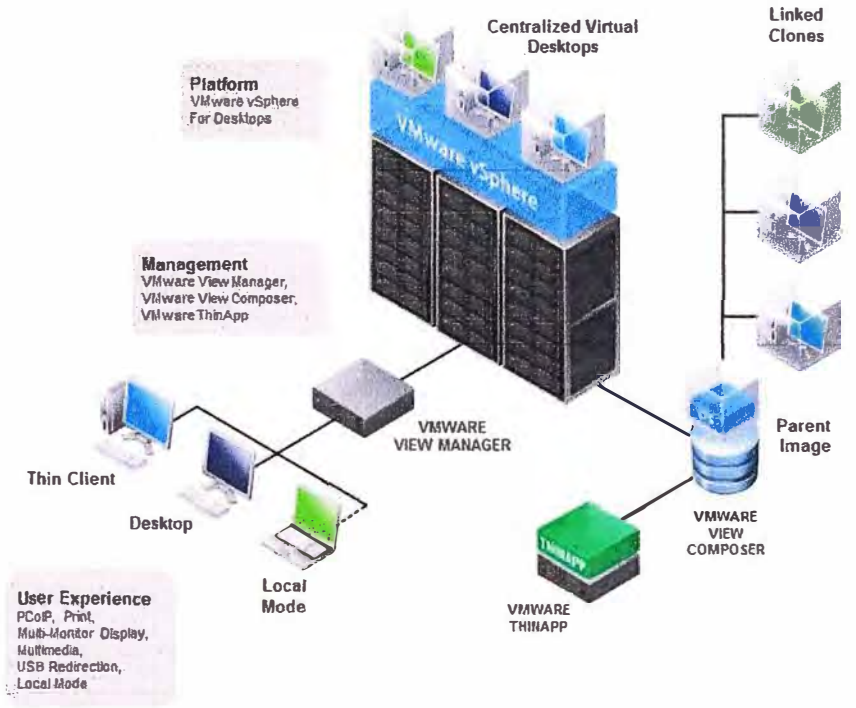


Figura 2.29 Virtualización de escritorios con VMware Horizon View

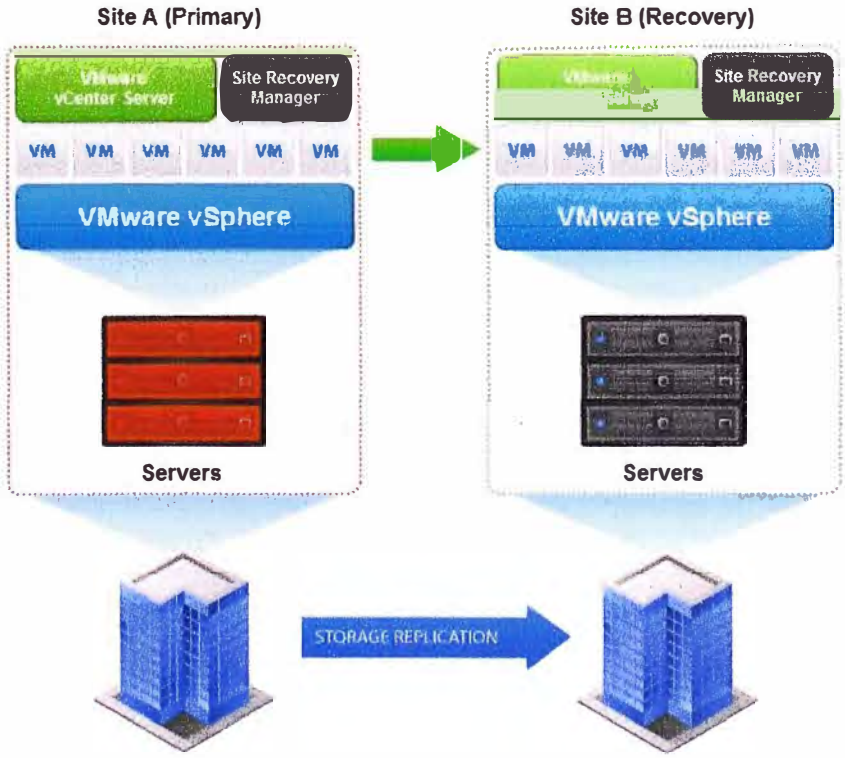


Figura 2.30 Recuperación ante desastres de entorno virtual con VMware Site Recovery Manager

2.1.6 Beneficios de la Virtualización

La virtualización de servidores ofrece beneficios directos importantes, siendo los principales los siguientes:

Consolidación de servidores: Se reduce la proliferación de servidores al usar varias máquinas virtuales por servidor físico.

Optimización de uso de recursos de hardware: La virtualización incrementa la utilización de recursos a través de la operación de múltiples cargas de trabajo en un solo servidor. El uso de recursos se incrementa de 5%-15% (sin virtualización) hasta 60%-80% (con virtualización).

Reducción de costos: La reducción de costos es la mayor preocupación de las empresas. La virtualización es la principal manera de reducir el gasto de capital (CAPEX) y gastos operativos (OPEX). Menor cantidad de servidores en el centro de datos significa menor inversión, bajos costos de mantenimiento, menor uso de espacio (m2), bajo consumo de energía eléctrica y enfriamiento.

Ambientes de desarrollo y pruebas: Permite la rápida creación, modificación y eliminación de nuevas máquinas virtuales al reusar imágenes maestras de máquinas virtuales sin afectar a las máquinas virtuales de producción.

Alta disponibilidad de Sistemas Operativos y Aplicaciones: Mediante funcionalidades como HA y FT se reducen los tiempos de interrupción de servicios por fallas de hardware.

Flexibilidad: La virtualización acomoda las necesidades de crecimiento al permitir agregar nuevos recursos físicos sin necesidad de interrumpir los servicios que brindan las máquinas virtuales.

Fácil administración y manejo de recursos: La administración de un entorno virtualizado se realiza de manera centralizada desde una consola de administración que permite entregar los recursos según las necesidades de recursos de las máquinas virtuales.

Recuperación ante desastres: Reduce los costos y complejidad de la Continuidad de Negocio (alta disponibilidad y recuperación ante desastres) al encapsular máquinas virtuales en simples archivos que pueden ser replicados y restaurados en otros servidores minimizando así los tiempos de interrupción de los servicios en sitios locales o remotos.

2.1.7 Migración de un Entorno Físico a un Entorno Virtual

La adopción de la virtualización además de consistir de un despliegue, instalación y configuración de hardware y software preparado para crear máquinas virtuales nuevas,

requiere también de herramientas que faciliten la migracion de una infraestructura tradicional de servidores ya existente a un entorno virtualizado.

A estas herramientas se les conoce como convertidores P2V (Physical to Virtual). En la actualidad, VMware proporciona un producto convertidor P2V llamado vCenter Converter Standalone el cual permite convertir servidores físicos a máquinas virtuales y además cuenta con capacidades de importar máquinas virtuales o imágenes de otros fabricantes.

Los pasos que realiza vCenter Converter Standalone para convertir un servidor físico encendido con sistema operativo Windows Server son los siguientes:

vCenter Converter Standalone instala un agente en el servidor físico que se desea convertir y toma un snapshot (Figura 2.31).

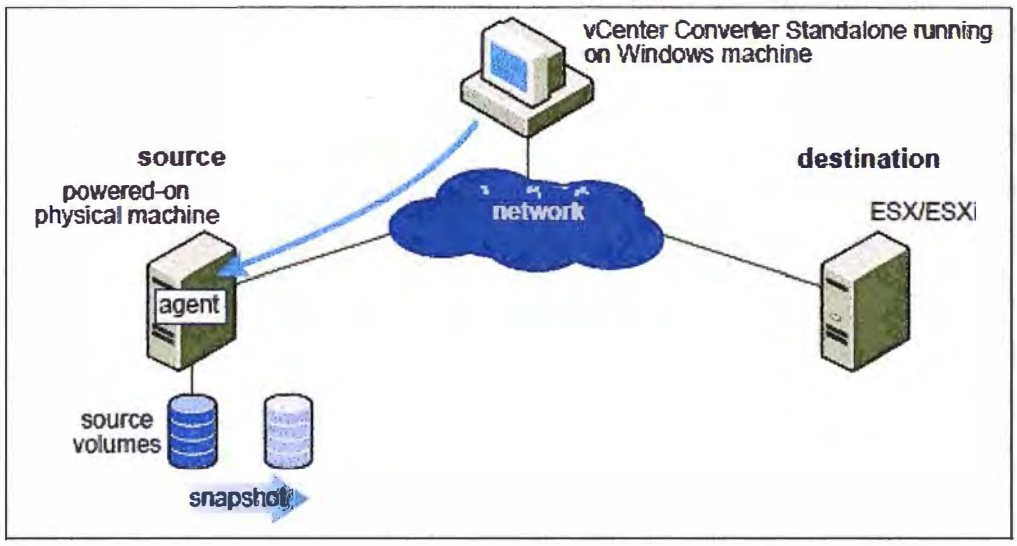


Figura 2.31 Instalación de agente de conversión

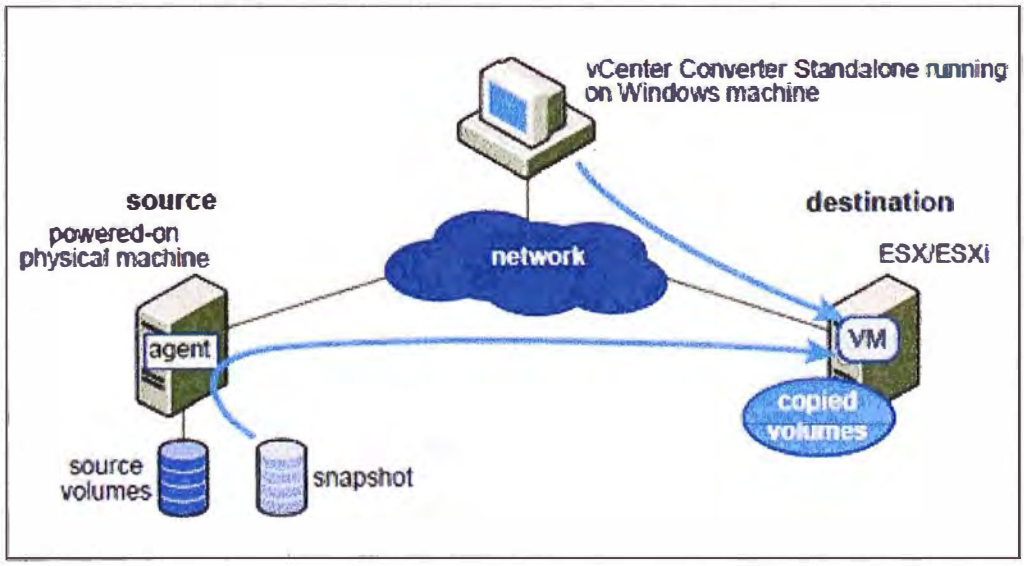


Figura 2.32 Creación de máquina virtual

vCenter Converter Standalone crea una máquina virtual en el host ESX destino y el agente copia la información de los volúmenes de datos desde el servidor origen hacia la máquina virtual (Figura 2.32).

El agente instala los drivers en la máquina virtual resultante para que inicie desde el nuevo hardware virtual (Figura 2.33).

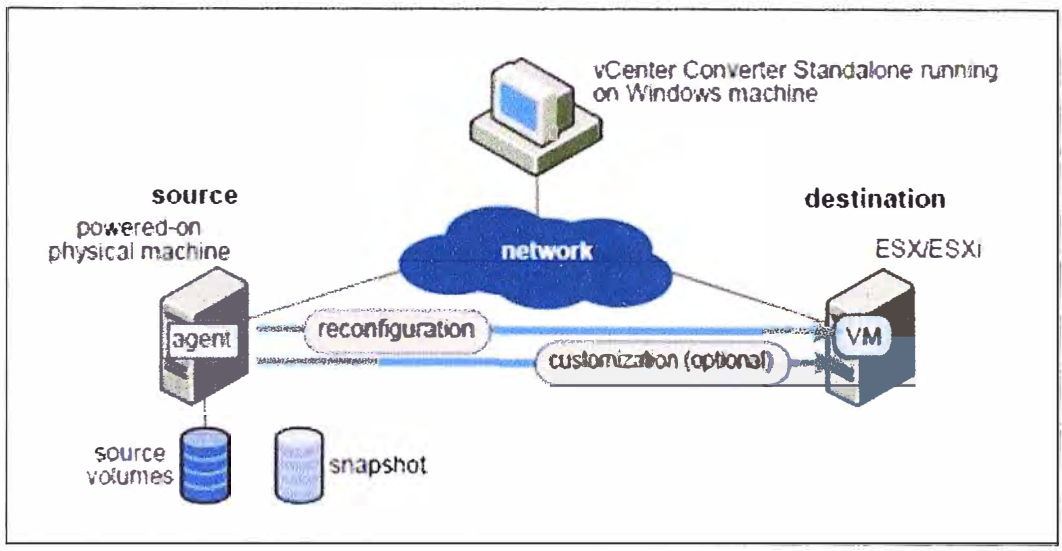


Figura 2.33 Reconfiguración de máquina virtual

2.1.8 Cloud Computing

La definición de Cloud Computing ampliamente adoptada viene del National Institute of Standards and Technology (NIST) de EE.UU:

"Cloud Computing es un modelo que permite el acceso bajo demanda a la red de manera cómoda y desde cualquier parte a un conjunto compartido de recursos de cómputo configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser aprovisionados y presentados de manera rápida con el menor esfuerzo administrativo e interacción con el proveedor de servicios." (Figura 2.34)

Cloud Computing permite a las empresas y consumidores obtener y aprovisionar recursos de tecnología de información como un servicio a través de internet. Cloud Computing permite a los usuarios navegar y seleccionar servicios de nube tales como computación, software, almacenamiento o una combinación de estos a través de un portal. La computación en la nube automatiza la entrega de servicios de nube requeridos a los usuarios.

Características Esenciales

Una infraestructura de cómputo usada para servicios en la nube debe tener ciertas capacidades o características. De acuerdo con el NIST, la infraestructura de nube debe

tener cinco características esenciales:

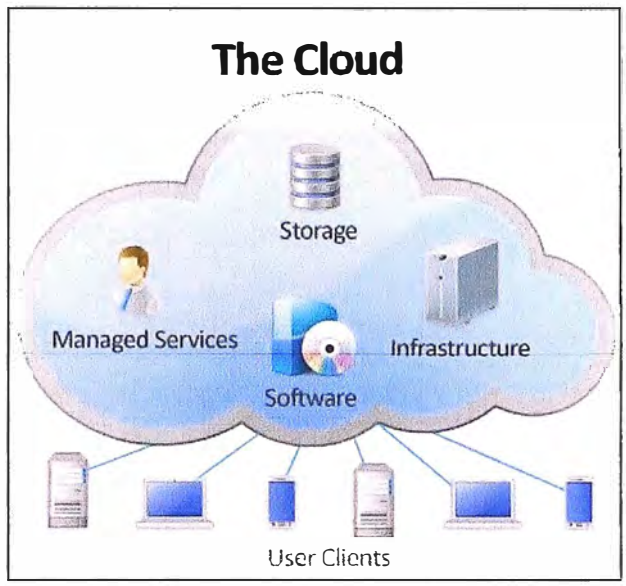


Figura 2.34 Cloud Computing

a) **Autoservicio bajo demanda:** El consumidor puede unilateralmente aprovisionar capacidades computacionales tales como servidores Windows y/o Linux y almacenamiento en la red cuando se necesite automáticamente sin requerir intervención del proveedor de servicio. El proveedor de servicio de nube publica sus catálogos de servicios los cuales incluyen información de los atributos, costos y procesos de solicitud vía web.
b) **Amplio acceso a la red:** Las capacidades están disponibles en la red y son accedidas por mecanismos standard que promueven el uso de plataformas heterogéneas (smartphones, tablets, PC, laptops, etc.).
c) **Recursos mancomunados:** Los recursos computacionales del proveedor son mancomunados para dar servicio a múltiples consumidores usando un modelo multiusuario con recursos físicos o virtuales asignados o reasignados de acuerdo a la demanda del consumidor. Ejemplos; procesamiento, memoria, velocidad de red.
d) **Elasticidad rápida:** Las capacidades pueden ser elásticamente aprovisionadas y presentadas, en algunos casos de forma automática, para escalar interna o externamente de acuerdo con la demanda. Para el consumidor, las capacidades disponibles para el aprovisionamiento a menudo parecen ser ilimitadas y pueden ser apropiadas en cualquier cantidad en cualquier momento. Ejemplo: una empresa puede requerir duplicar la cantidad de servidores web por un tiempo determinado y luego volver a la cantidad de servidores web contratados
e) **Medición de servicios:** Los sistemas de nube controlan y optimizan

automáticamente el uso de recursos mediante el aprovechamiento de la capacidad de medición en cierto nivel de abstracción adecuado para el tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda, y cuentas de usuario activas). El uso de recursos puede ser monitoreado, controlado, y reportado, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Modelos de Servicio

De acuerdo al NIST, las ofertas de servicios de nube se clasifican en tres modelos principales

a) **Infrastructure as a Service (IaaS):** La capacidad ofrecida al consumidor es de provisionar procesamiento, almacenamiento, redes y otros recursos fundamentales de computación en los que consumidor es capaz de desplegar y ejecutar software arbitrario, entre los que se puede incluir sistemas operativos y aplicaciones. El consumidor no administra o controla la infraestructura de nube subyacente pero tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, y posiblemente control limitado de componentes de red seleccionados (Ej: firewall de host).

   IaaS es la capa base del stack de servicios de nube. Sirve de base para las capas de SaaS y PaaS.

   Ejemplos de nubes IaaS: Amazon Elastic Compute Cloud (Amazon EC2), Rackspace, GoGrid, Microsoft, Terramark, AT&T, Google Compute Engine (GCE),

b) **Platform as a Service (PaaS):** La capacidad ofrecida al consumidor es la de desplegar sobre la infraestructura de nube aplicaciones creadas o adquiridas del consumidor usando lenguajes de programación, bibliotecas, servicios y herramientas soportadas por parte del proveedor. El consumidor no administra o controla la infraestructura de nube subyacente incluyendo la red, servidores, sistemas operativos, almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente configuraciones para el entorno de alojamiento de aplicaciones.

   PaaS también se usa como un entorno de desarrollo de aplicaciones, se ofrece como un servicio por parte del proveedor de servicios de nube. El consumidor puede utilizar estas plataformas para codificar sus aplicaciones y luego desplegar las aplicaciones en la nube. Debido a que la carga de trabajo de las aplicaciones desplegadas varía, la escalabilidad de los recursos informáticos suele estar garantizada por la plataforma informática, de forma transparente.

   Ejemplos de nubes PaaS: Google App Engine y Microsoft Windows Azure Platform

c) **Software as a Service (SaaS):** La capacidad ofrecida al consumidor es el uso de las aplicaciones del proveedor que se ejecutan en una infraestructura de nube. Las

aplicaciones son accesibles desde diferentes dispositivos cliente ya sea desde una interfaz de un thin client, como un navegador web (por ejemplo, correo basado en web), o desde una interfaz de un programa. El consumidor no administra ni controla la infraestructura de cloud subyacente incluyendo la red, servidores, sistemas operativos, o incluso capacidades específicas de una aplicación a excepción de algunas configuraciones de aplicación específicas de usuario.

En un modelo SaaS, aplicaciones tales como la gestión de relaciones con clientes (CRM), e-mail y mensajería instantánea (IM), se ofrecen como un servicio por los proveedores de servicios de nube. Los proveedores de servicios de nube administran exclusivamente la infraestructura informática y el software necesarios para soportar estos servicios. Los consumidores pueden estar autorizados para cambiar algunas opciones de configuración de una aplicación para personalizar las aplicaciones.

Ejemplos de nubes SaaS: Salesforce, Blackboard, Google, Microsoft, Zuora

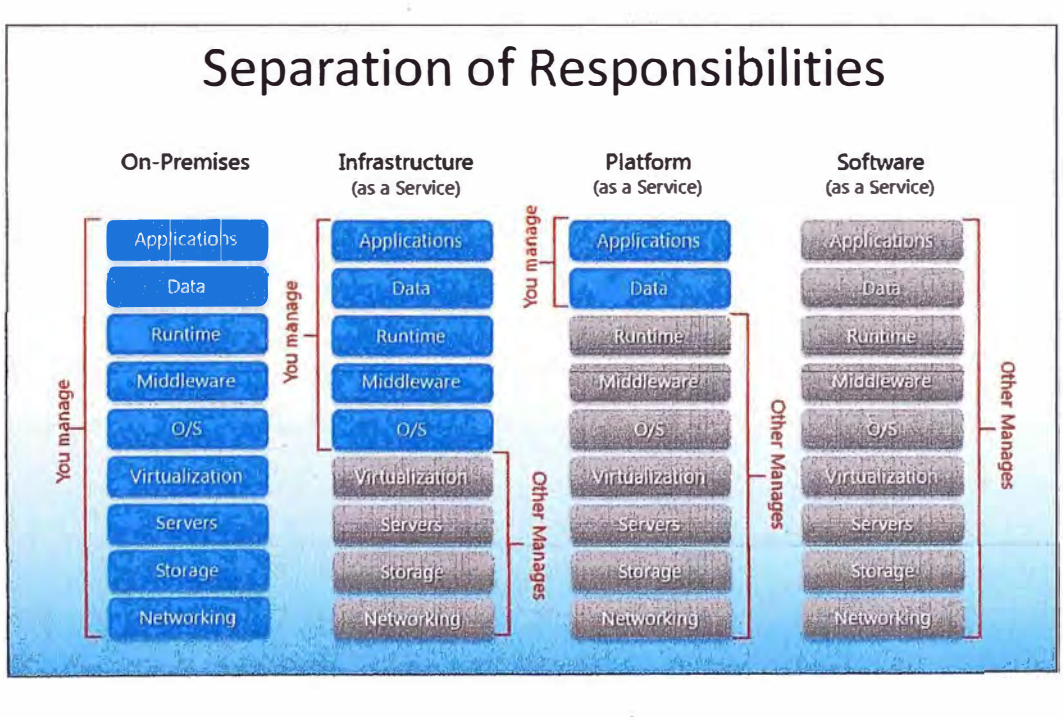


Figura 2.35 Modelos de servicio en la nube

Modelos de Despliegue

Según el NIST, el Cloud Computing se clasifica en cuatro modelos de despliegue que constituyen la base de cómo se consumen y se construyen las infraestructuras de nube.

a) **Nube Privada:** La infraestructura de la nube está preparada para el uso exclusivo de una sola organización que comprende múltiples consumidores (por ejemplo, unidades de negocio). Puede ser propia, administrada y operada por la organización, un

tercero, o una combinación de ellos, y que pueden existir dentro o fuera de las instalaciones.

Figura 2.36 Nube Privada

b) **Nube Comunitaria:** La infraestructura de la nube está preparada para el uso exclusivo de una comunidad específica de consumidores de organizaciones que tienen asuntos en común (por ejemplo, misión, requisitos de seguridad, política, y consideraciones de cumplimiento). Puede ser propia, administrada y operada por una o más de las organizaciones de la comunidad, un tercero, o una combinación de ellos, y que puede existir dentro o fuera de las instalaciones.

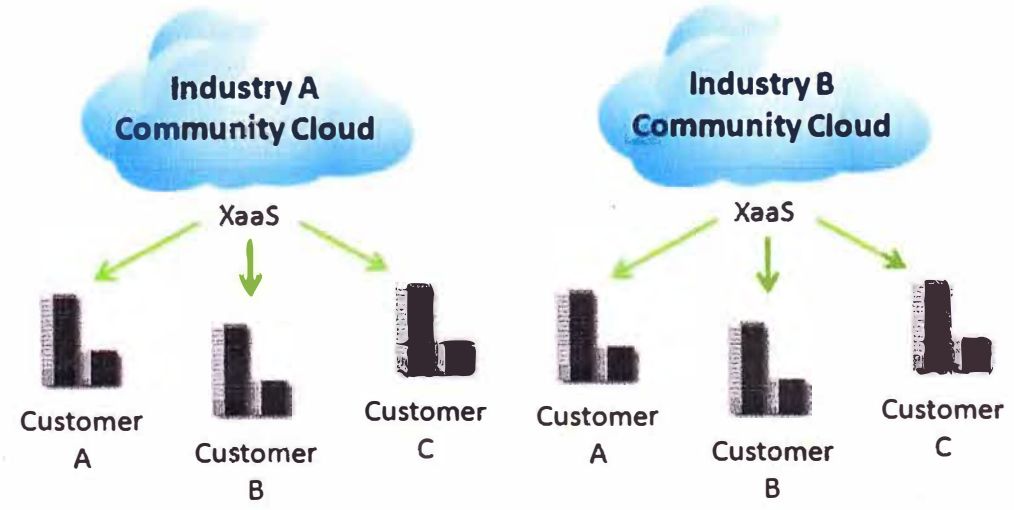


Figura 2.37 Nube Comunitaria

c) **Nube Pública:** La infraestructura de la nube está preparada para el uso abierto del

público en general. Puede ser propia, administrada y operada por una organización comercial, académica, o de gobierno, o una combinación de estas. Existe en las instalaciones del proveedor de nube.

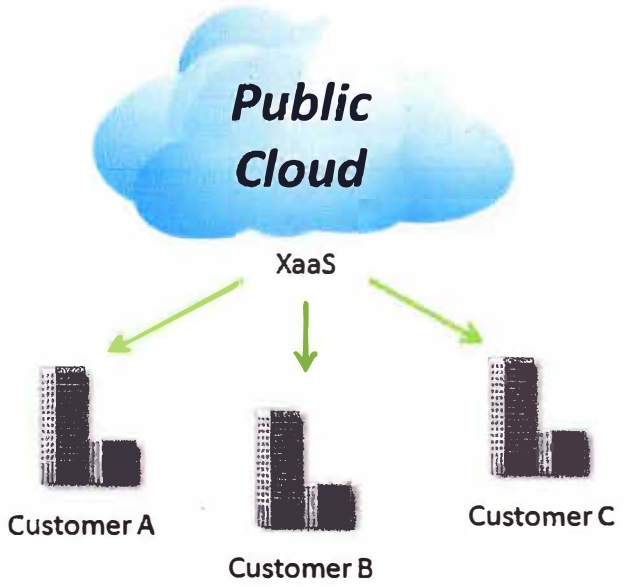


Figura 2.38 Nube Pública

d) **Nube Hibrida:** La infraestructura de la nube es una composición de dos o más infraestructuras de nube distintos (privada, comunitaria o pública) que permanecen como entidades únicas, pero que están unidos por la tecnología estandarizada o propietaria que permite la portabilidad de los datos y de las aplicaciones (por ejemplo, el cloud bursting para el equilibrio de carga entre nubes).

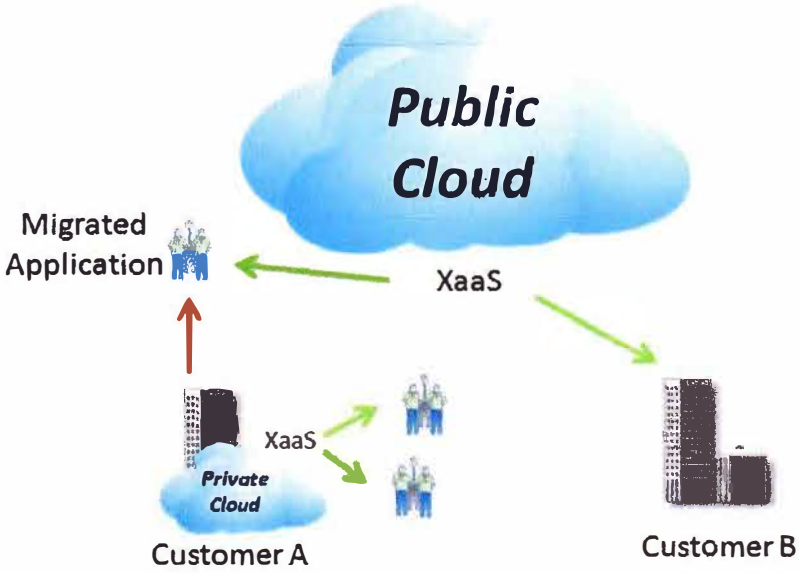


Figura 2.39 Nube Hibrida

2.2 Sistemas de Almacenamiento

La importancia, dependencia, y el volumen de información para el mundo de las empresas siguen creciendo a un ritmo asombroso. Las empresas dependen de un acceso rápido y fiable a la información crítica para su éxito. Ejemplos de procesos de negocio y sistemas que se basan en información digital incluyen reservas de vuelos aéreos, la facturación de las empresas de telecomunicaciones, el comercio por Internet, banca electrónica, procesamiento de transacciones de tarjetas de crédito, comercio de capitales y acciones, procesamiento de atención de la salud, etc. La dependencia cada vez mayor de las empresas en la información incrementó los desafíos en el almacenamiento, la protección y gestión de datos. Las obligaciones legales, reglamentarias y contractuales respecto a la disponibilidad y protección de datos se añaden a estos desafíos.

2.2.1 Almacenamiento de la Información

Datos

Los datos son una colección de hechos en bruto de los que se puedan extraer las conclusiones.

Cartas escritas a mano, un libro impreso, una fotografía, libros de contabilidad de un banco, son ejemplos que contienen datos.

Antes de la llegada de las computadoras, los métodos utilizados para la creación e intercambio de datos se limitaban a meros formularios, como el papel y cinta. Hoy en día, los mismos datos se pueden convertir en formas más convenientes, como un correo electrónico, un ebook, una imagen digital, o una película digital. Estos datos se pueden generar usando una computadora y ser almacenados como cadenas de números binarios (0 y 1). Estos datos son denominados datos digitales que son accesibles solo si la computadora los procesa.

Otros factores que elevaron la generación y compartición de datos: avances en el procesamiento y almacenamiento de los datos, el bajo costo del almacenamiento digital, tecnologías de comunicación cada vez más rápidas y la proliferación de dispositivos móviles inteligentes.

La importancia y el valor de los datos varían con el tiempo. La mayoría de los datos que se crean tiene un significado por un corto plazo, pero se vuelven menos valiosos con el tiempo. Esto toma importancia en el tipo de soluciones de almacenamiento de datos utilizados. Normalmente, los datos recientes que tiene mayor uso se almacenan en un almacenamiento más rápido y caro. A medida que pasa el tiempo, se pueden mover a un almacenamiento más lento, menos caro, pero fiable.

Algunas empresas manejan datos de miles o millones de clientes y garantizan la seguridad e integridad de los datos durante un largo período de tiempo. Esto requiere de dispositivos de almacenamiento de alto rendimiento y de alta capacidad con una mayor seguridad y cumplimiento que puedan conservar los datos durante un largo período.

Tipos de datos

Los datos pueden ser clasificados como estructurados o no estructurados en base a la forma en que se almacenan y administran.

Los datos estructurados se organizan en filas y columnas en un formato estrictamente definido por lo que las aplicaciones pueden recuperar y procesar de manera eficiente. Los datos estructurados se almacenan típicamente usando un sistema de gestión de bases de datos (DBMS).

Los datos son no estructurados si sus elementos no se pueden almacenar en filas y columnas, lo que hace que sean difíciles para consultar y recuperar por las aplicaciones.

Los datos, sean estructurados o no estructurados, no cumplen un propósito para las empresas a menos que se presenta en una forma significativa. La información es la inteligencia y el conocimiento derivado de los datos.

Las empresas analizan los datos en bruto para identificar tendencias significativas. En base a estas tendencias, una empresa puede planificar o modificar sus estrategias.

Almacenamiento

Los datos generados por las empresas deben ser almacenados de modo que sean fácilmente accesibles para su posterior procesamiento. En un entorno de computación, los dispositivos diseñados para el almacenamiento de datos se denominan dispositivos de almacenamiento o simplemente de almacenamiento. El tipo de almacenamiento usado varía basándose en el tipo de datos y en la velocidad con los que se crean y usan. Dispositivos, tales como una tarjeta de memoria en un teléfono celular o cámara digital, DVD, CD-ROM y unidades de disco en las computadoras personales son ejemplos de dispositivos de almacenamiento. Las empresas tienen varias opciones disponibles para el almacenamiento de datos, incluyendo los discos duros internos, arreglos de discos externos, y cintas.

2.2.2 Evolución de la Arquitectura de Almacenamiento

Históricamente, las organizaciones tenían ordenadores centralizados (mainframes) y dispositivos de almacenamiento de información (carretes de cinta y paquetes de discos) en sus centros de datos. La evolución de los sistemas abiertos, su accesibilidad y facilidad de despliegue hicieron posible que las unidades de negocio/departamentos tengan sus propios servidores y almacenamiento.

En las primeras implementaciones de los sistemas abiertos, el almacenamiento era típicamente interno en el servidor. Estos dispositivos de almacenamiento no podían ser compartidos con otros servidores. A este enfoque se le conoce como la arquitectura de almacenamiento centrada en el servidor. En esta arquitectura, cada servidor tiene un número limitado de dispositivos de almacenamiento y las tareas administrativas, como el mantenimiento del servidor o el aumento de la capacidad de almacenamiento pueden resultar en la indisponibilidad de la información. La proliferación de servidores departamentales en una empresa dio como resultado islas de información sin protección, no administrados, fragmentadas y el aumento de los gastos operativos y de capital.

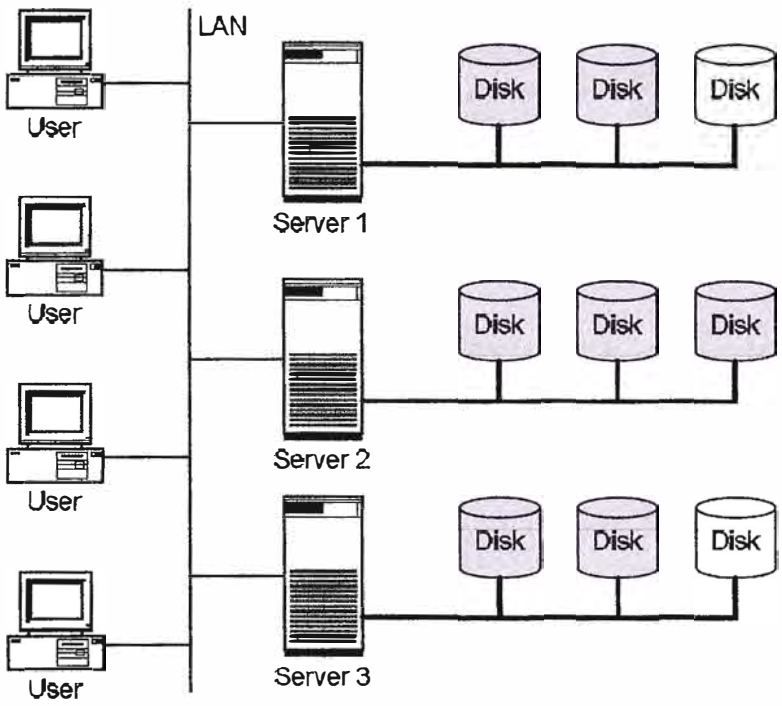


Figura 2.40 Arquitectura de almacenamiento centrado en el servidor

Para superar estas limitaciones, el almacenamiento evolucionó de la arquitectura centrada en el servidor a la arquitectura centrada en la información. En esta arquitectura, los dispositivos de almacenamiento se gestionan de manera centralizada e independiente de los servidores. Estos dispositivos de almacenamiento administrados centralizadamente son compartidos con múltiples servidores. Cuando se implementa un nuevo servidor, se asigna almacenamiento desde los mismos dispositivos de almacenamiento compartido a este servidor. La capacidad de almacenamiento compartido se puede aumentar dinámicamente añadiendo más dispositivos de almacenamiento sin afectar a la disponibilidad de información. En esta arquitectura, la

gestión de la información es más fácil y rentable.

Actualmente las tecnologías de almacenamiento y su arquitectura siguen evolucionando, lo que permite a las organizaciones consolidar, proteger, optimizar y aprovechar sus datos para lograr el mayor rendimiento de los activos de información.

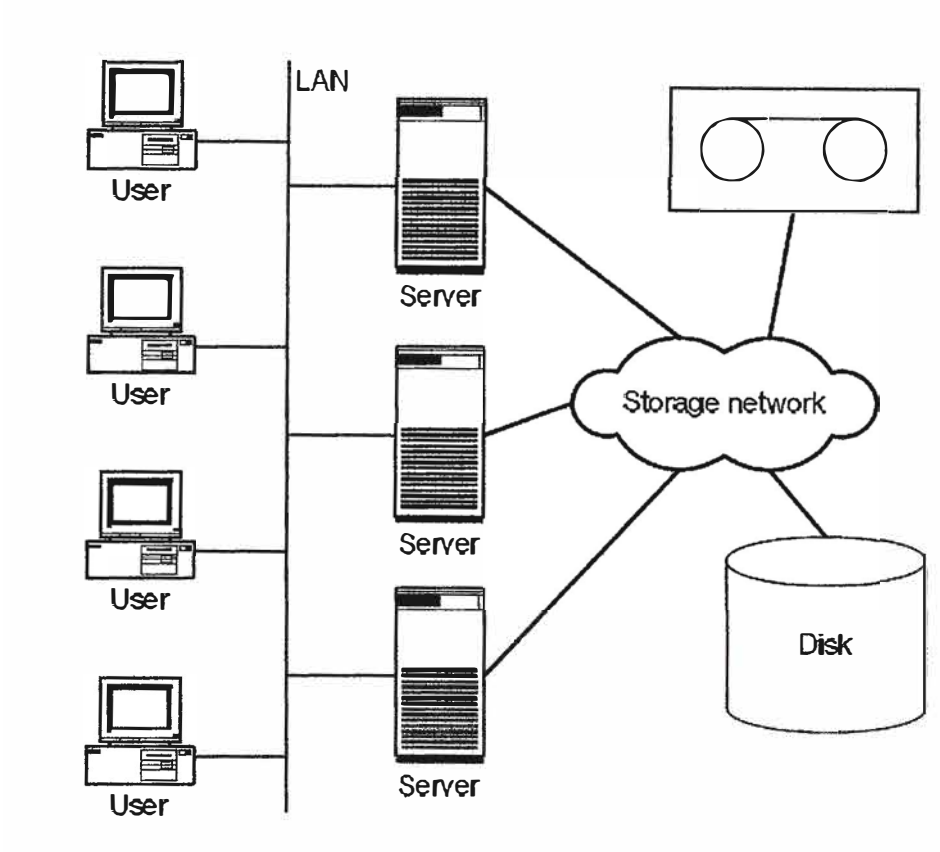


Figura 2.41 Arquitectura de almacenamiento centrada en la información

2.2.3 Conectividad

Los componentes físicos de conectividad son elementos de hardware que conectan al host con el almacenamiento. Los tres componentes físicos que permiten la conectividad entre el host y el almacenamiento son: la HBA, el puerto y el cable.

La HBA (Host Bus Adapter) es una tarjeta ASIC (Application-Specific Integrated Circuit) que realiza funciones de interfaz de I/O entre el host y el almacenamiento, liberando al CPU de carga de trabajo adicional de procesamiento de I/O. Un host suele tener múltiples HBAs

Un puerto es una toma especializada que permite la conectividad entre el servidor y los dispositivos externos. Una HBA puede tener uno o más puertos para conectar el host al dispositivo de almacenamiento.

Los cables conectan los hosts a los dispositivos internos o externos usando cobre o fibra óptica.

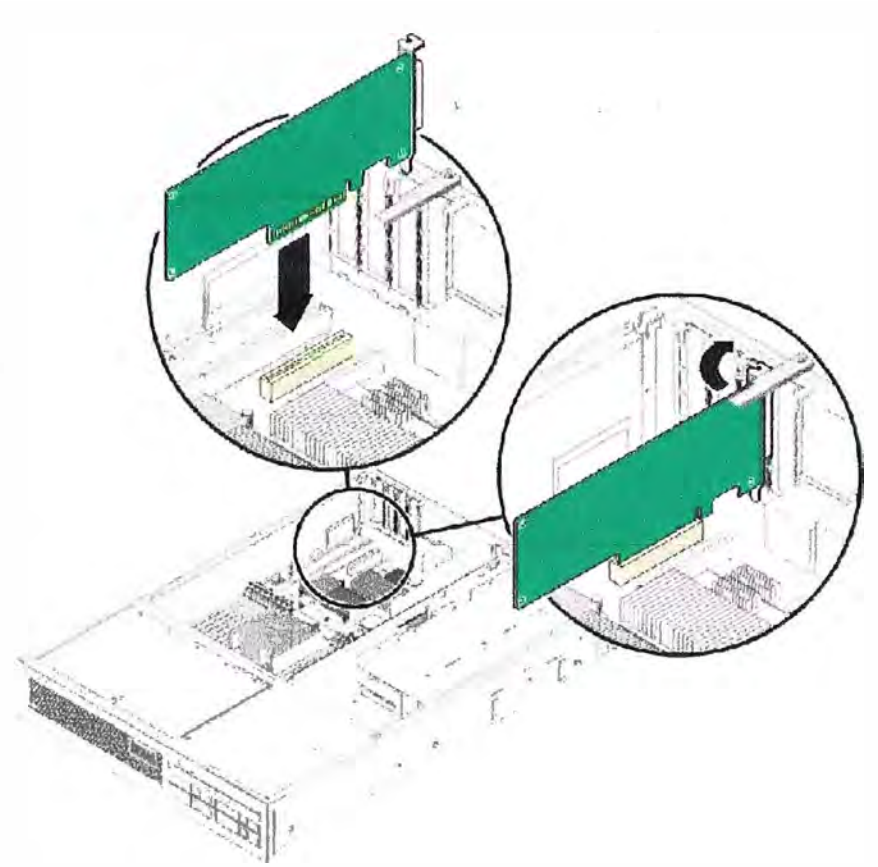


Figura 2.42 Instalación de tarjeta HBA en servidor

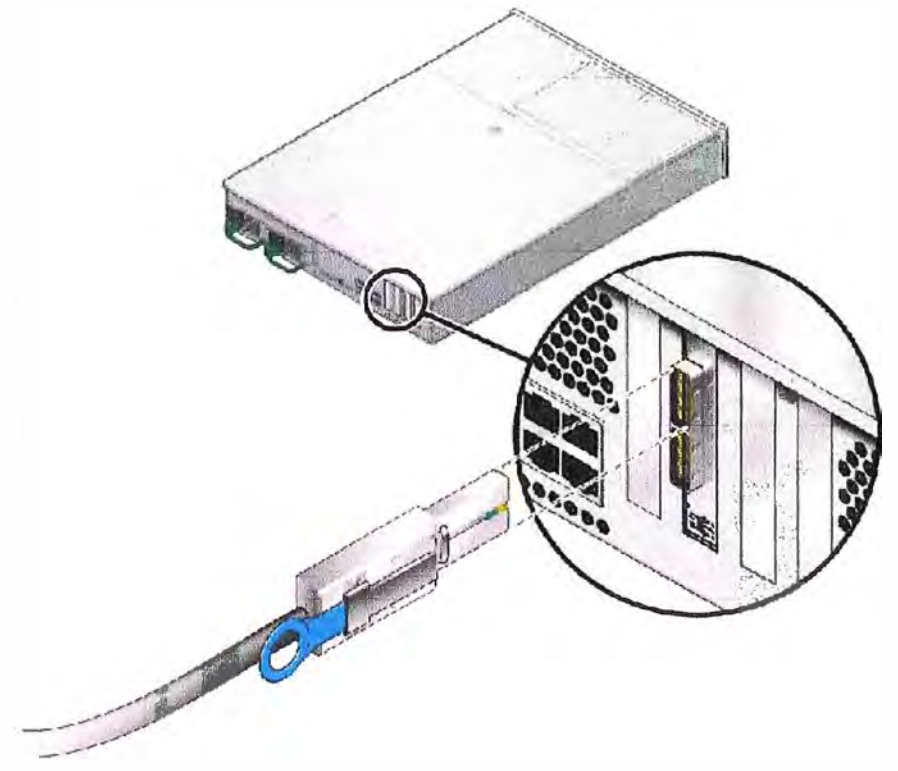


Figura 2.43 Conexión de cable de cobre con puerto de una HBA

Protocolos de Interfaz

Los protocolos populares para la conectividad entre los host y los dispositivos de almacenamiento son Integrated Device Electronics/Advanced Technology Attachment (IDE/ATA), Small Computer System Interface (SCSI), Fibre Channel (FC) y Internet Protocol (IP).

IDE/ATA y Serial ATA: IDE/ATA es un protocolo de interfaz estándar de usado para la conexión de dispositivos de almacenamiento, como discos duros y unidades de CD-ROM. Este protocolo soporta transmisión paralela por lo que también se conoce como ATA paralelo (PATA) o simplemente ATA. IDE/ATA tiene una variedad de normas y nombres. La versión Ultra DMA/133 de ATA soporta una capacidad de 133 MB por segundo. En una configuración maestro-esclavo, una interfaz ATA admite dos dispositivos de almacenamiento por cada conector.

Sin embargo, si el rendimiento de la unidad de almacenamiento es importante, no se recomienda compartir un puerto entre dos dispositivos.

La versión serie de este protocolo soporta la transmisión en serie de un bit y es conocida como Serial ATA (SATA). El alto rendimiento y bajo costo de SATA ha sustituido a PATA en los sistemas actuales. La versión 3.0 de SATA proporciona una velocidad de transferencia de hasta 6Gb/s.

SCSI y Serial SCSI: SCSI es el protocolo de conectividad preferido para equipos de gama alta.

El protocolo SCSI permite transmisión paralela y ofrece un mejor rendimiento, escalabilidad y compatibilidad en comparación a ATA. Sin embargo, el alto costo de SCSI limita su popularidad entre los usuarios de escritorio de casa o personales.

A través de los años, SCSI ha sido mejorado y ahora incluye una amplia variedad de tecnologías y estándares. SCSI permite el uso de hasta 16 dispositivos en un solo bus y proporciona velocidades de transferencia de datos de hasta 640MB/s (versión Ultra-640).

Serial Attached SCSI (SAS) es un protocolo serial punto a punto que proporciona una alternativa al SCSI paralelo. Una nueva versión de SCSI serial (SAS 2.0) permite una velocidad de transferencia de hasta 6Gb/s.

Fibre Channel (FC): Fibre Channel es un protocolo ampliamente utilizado para la comunicación de alta velocidad hacia un dispositivo de almacenamiento. La interfaz Fibre Channel proporciona una velocidad de red gigabit. Proporciona una transmisión de datos serial en cables de cobre y fibra óptica. La última versión de la interfaz FC permite la transmisión de datos de hasta 16Gb/s.

Internet Protocol (IP): IP es un protocolo de red que se ha utilizado tradicionalmente para el tráfico host a host. Con la aparición de las nuevas tecnologías, la red IP se ha

convertido en una opción viable para la comunicación del host con el almacenamiento. IP ofrece varias ventajas en términos de costo y madures lo que permite a las organizaciones aprovechar su red IP existente. Protocolos como iSCSI y FCIP son ejemplos comunes que aprovechan IP para la comunicación del host con el almacenamiento.

Las unidades de disco son accedidas a través de protocolos predefinidos, como ATA, Serial ATA (SATA), SAS (Serial Attached SCSI), y FC. Estos protocolos están implementados en los controladores de interfaz de disco. Los controladores de interfaz de disco modernos están integrados en las unidades de disco, por lo tanto, las unidades de disco son conocidos por el interfaz de protocolo que soportan, por ejemplo disco SATA, disco SAS, disco FC, etc.

2.2.4 Direct-Attached Storage (DAS)

DAS es una arquitectura en la cual el almacenamiento se conecta directamente a los hosts. La unidad de disco interna de un host y una unidad de almacenamiento externo directamente conectada son algunos ejemplos de DAS. Aunque la implementación de tecnologías de redes de almacenamiento está ganando popularidad, DAS se ha mantenido vigente para el acceso de datos en ambientes pequeños. DAS se clasifica como interno o externo, en base a la ubicación del dispositivo de almacenamiento respecto al host (Figura 2.44).

En las arquitecturas DAS internas, el dispositivo de almacenamiento está conectado internamente al host por un bus serie o paralelo. El bus físico tiene limitaciones de distancia y se puede mantener sólo a una distancia corta para una conectividad de alta velocidad. La mayoría de buses internos solo soporta un número limitado de dispositivos, y ocupan espacio dentro del host, lo que hace difícil el mantenimiento de otros componentes.

Por otro lado, en las arquitecturas DAS externas, el host se conecta directamente al dispositivo de almacenamiento externo, y se accede a los datos a nivel de bloque. En la mayoría de los casos, la comunicación entre el host y el dispositivo de almacenamiento se lleva a cabo sobre protocolo SCSI o FC. En comparación con el DAS interno, un DAS externo supera la distancia y las limitaciones de cantidad de dispositivos y proporciona una gestión centralizada de los dispositivos de almacenamiento.

2.2.5 Redundant Array of Independent Disks (RAID)

RAID es una tecnología que permite usar varias unidades de disco como un conjunto el cual proporciona protección de datos contra fallas de disco. En general, el uso de RAID

también mejora el rendimiento del sistema de almacenamiento al entregar I/Os de múltiples discos de manera simultánea. Los arreglos modernos con unidades flash también se benefician en términos de protección y rendimiento mediante el uso de RAID.

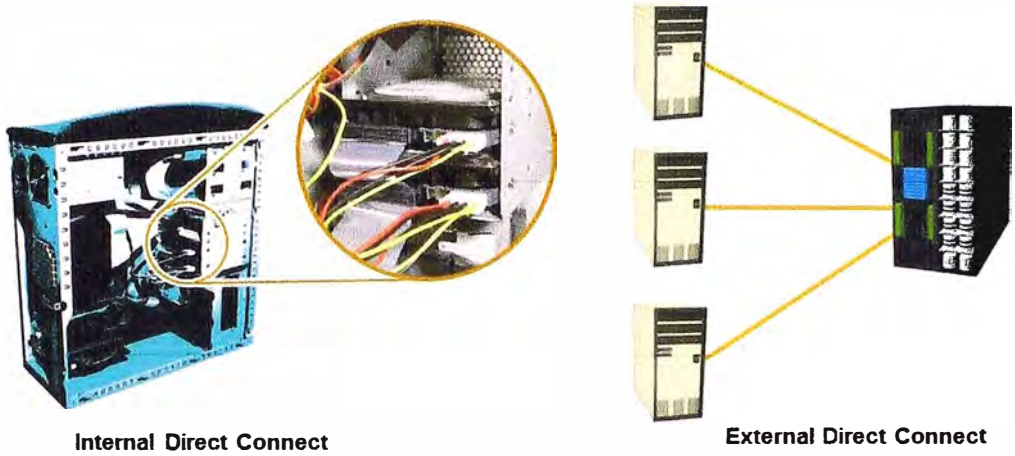


Figura 2.44 Conexión de dispositivos DAS internos y externos

Métodos de implementación de RAID

Los dos métodos de implementación de RAID son por hardware y por software. Ambos tienen sus ventajas y desventajas.

a) **RAID por software:** El RAID por software utiliza software basado en host para proporcionar funciones RAID. Se lleva a cabo a nivel del sistema operativo y no utiliza un controlador en hardware dedicado para administrar el arreglo RAID.

   Las implementaciones de RAID por software ofrecen beneficios tanto en costo como en simplicidad en comparación al RAID por hardware. Sin embargo, tienen las siguientes limitaciones:

   Rendimiento: El RAID por software afecta el rendimiento general del sistema. Esto es debido a los ciclos de CPU adicionales necesarios para realizar cálculos RAID.

   Funcionalidades soportadas: El RAID por software no soporta todos los niveles de RAID.

   Compatibilidad del sistema operativo: El RAID por software está atado al sistema operativo host, por lo que las actualizaciones al RAID por software o al sistema operativo deben ser validados para la compatibilidad. Genera inflexibilidad en el entorno de procesamiento de datos.

b) **RAID por hardware:** En implementaciones de RAID por hardware, se instala un controlador en hardware especializado en el host o en el arreglo de discos.

   La tarjeta controladora de RAID es una implementación de RAID por hardware

basado en host en la que un controlador RAID especializado es instalado en el host y las unidades de disco son conectadas a él. Los fabricantes también integran controladores RAID en las motherboard. Un controlador RAID basado en host no es una solución eficiente en un entorno de centro de datos con un gran número de hosts.

El controlador RAID externo es un RAID por hardware basado en arreglo de discos. Actúa como una interfaz entre el host y los discos. Presentan los volúmenes de almacenamiento al host y el host administra estos volúmenes como discos físicos.

Las principales funciones de los controladores RAID son:

- Gestión y control de las agrupaciones de discos.
- Traducción de las solicitudes de I/O entre los discos lógicos y discos físicos.
- Regeneración de datos en caso de fallas de disco.

Técnicas de RAID

Las técnicas de RAID tales como striping, espejado y paridad constituyen la base para la definición de los niveles de RAID. Estas técnicas determinan la disponibilidad y características de rendimiento de un conjunto de discos en RAID.

a) Striping: El striping es una técnica que distribuye los datos en varias unidades de disco para utilizar las unidades de disco en paralelo. Todos los cabezales de lectura y escritura trabajan de manera simultánea, lo que permite procesar más datos en un tiempo más corto y aumentar el rendimiento, en comparación con la lectura y escritura de un solo disco.

Dentro de cada disco en un conjunto de discos en RAID, un número predefinido de bloques de disco direccionables contiguos se definen como un strip. Al conjunto de strips alineados que se extienden sobre todos los discos dentro del conjunto de discos en RAID se le denomina un stripe.

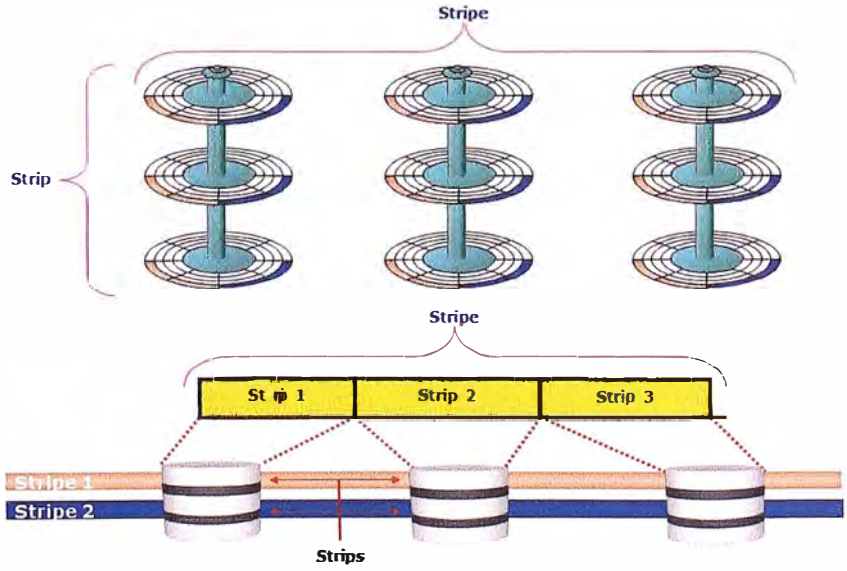


Figura 2.45 Conjunto de discos en RAID con stripes

b) **Mirroring:** El mirroring es una técnica mediante la cual los mismos datos son almacenados en dos unidades de disco diferentes, produciendo dos copias de los datos. Si se produce una avería en una unidad de disco, los datos están intactos en el disco sobreviviente y el controlador sigue atendiendo las solicitudes de datos del host desde el disco sobreviviente de un par de discos en mirroring.

Cuando se sustituye el disco averiado por uno nuevo, el controlador copia los datos del disco sobreviviente del par de discos en mirroring. Esta actividad es transparente para el host.

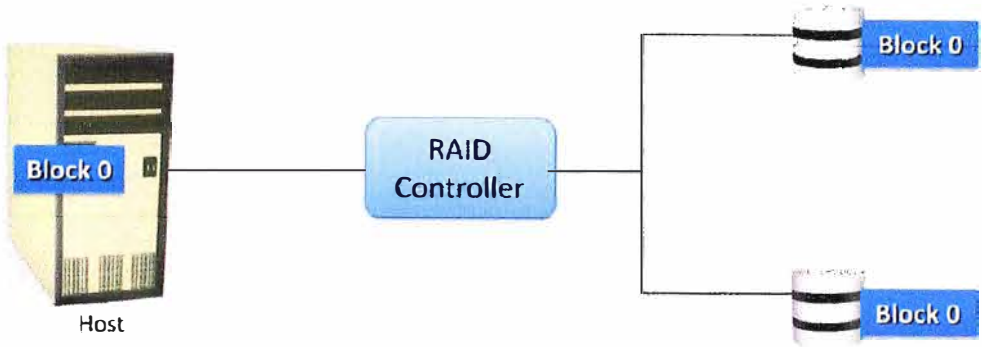


Figura 2.46 Par de discos en mirroring

c) **Paridad:** La paridad es un método para proteger los datos en striping contra la falla de unidad de disco sin el alto costo del mirroring. Se agrega una unidad de disco para mantener la paridad, una construcción matemática que permite la re-creación de los datos perdidos. La paridad es una técnica de redundancia que asegura la protección de los datos sin necesidad de mantener un conjunto completo de datos duplicados. El cálculo de la paridad es una función del controlador RAID.

La información de la paridad se puede almacenar en unidades de disco dedicadas, o distribuida en todos los discos en un conjunto de discos en RAID.

Niveles de RAID

a) **RAID 0:** La configuración RAID 0 utiliza las técnica de striping de datos, donde los datos están en strips en todos los discos en un conjunto de discos en RAID. Por lo tanto, utiliza la capacidad de almacenamiento total de un conjunto de discos en RAID. Para leer los datos, todos los strips son colocados juntos por el controlador.

Cuando el número de unidades de disco en el conjunto de discos en RAID aumenta, el rendimiento mejora porque más datos pueden ser leídos o escritos simultáneamente. RAID 0 es una buena opción para las aplicaciones que requieren un alto rendimiento de I/O. Sin embargo, si estas aplicaciones requieren alta

disponibilidad durante fallas de disco, RAID 0 no proporciona protección de datos ni disponibilidad.

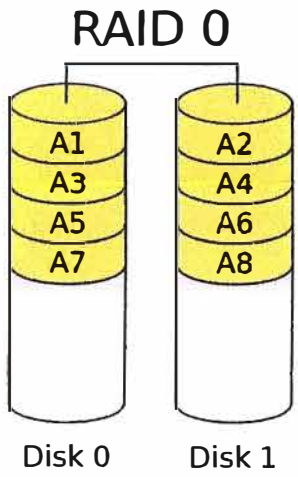


Figura 2.47 Conjunto de discos en RAID 0

b) RAID 1: RAID 1 se basa en la técnica de mirroring. En esta configuración RAID, los datos se duplican para proporcionar tolerancia a fallos. Un RAID 1 está compuesto por dos unidades de disco y cada escritura es escrita en ambos discos. El mirroring es transparente para el host. Durante la falla de un disco, el impacto en la recuperación de datos en RAID 1 es el menor entre todas las implementaciones RAID. Esto es debido a que el controlador RAID utiliza la unidad de disco en mirroring para la recuperación de datos. RAID 1 es adecuado para aplicaciones que requieren alta disponibilidad y en las que el costo no es una limitación.

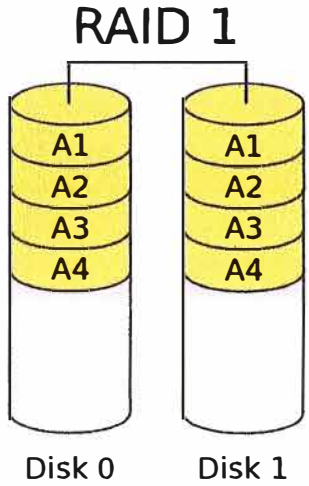


Figura 2.48 Conjunto de discos en RAID 1

c) **RAID 10 y RAID 01:** La mayoría de los centros de datos requieren redundancia de datos y rendimiento en sus arreglos en RAID. RAID 1+0 y RAID 0+1 combinan los beneficios del rendimiento de RAID 0 con los beneficios de la redundancia de RAID 1. Utilizan las técnicas de striping y mirroring y combinan sus beneficios. Estos tipos de RAID requieren un número par de discos, siendo el mínimo de cuatro (Figura 2.49).

RAID 1+0 es también conocido como RAID 10. Del mismo modo, RAID 0+1 también se conoce como RAID 01. RAID 1+0 funciona bien para cargas de trabajo pequeñas, aleatorias, de I/Os de escritura intensiva. Algunas aplicaciones que se benefician de RAID 1+0 son las siguientes: OLTP (Online Transaction Processing) con transacciones de altas velocidades, instalaciones de mensajería grandes y aplicaciones de bases de datos con cargas de trabajo de acceso aleatorio de escritura intensivas.

Un error común de concepto es considerar que RAID 1+0 y RAID 0+1 son lo mismo. En condiciones normales, los niveles de RAID 1+0 y 0+1 ofrecen beneficios idénticos. Sin embargo, las operaciones de reconstrucción en caso de falla de disco difieren entre los dos.

RAID 1+0 también se le conoce como striping sobre mirroring. El elemento básico de RAID 1+0 es un par de discos en mirroring, lo que significa que a los datos primero se les aplica mirroring y luego a las dos copias de los datos se les aplica striping en varios pares de unidades de disco en el conjunto de discos en RAID. Al sustituir una unidad de disco averiada, sólo el par en mirroring realiza la reconstrucción.

RAID 0+1 se conoce también como mirroring sobre striping. El elemento básico de RAID 0+1 es el stripe. Esto significa que el proceso de striping de datos en las unidades de disco se realiza primero, y luego todo el stripe se coloca en mirroring. En esta configuración, si un disco falla, entonces ocurre una falla en todo el stripe. La operación de re-construcción copia todo el stripe, copiando los datos de cada disco en un stripe operativo hacia un disco equivalente en el stripe averiado. Esto produce una carga mayor e innecesaria de I/O en los otros operativos y hace que el conjunto de discos en RAID sea más vulnerable a una segunda falla de disco.

d) **RAID 5:** RAID 5 usa striping de datos y usa paridad para la tolerancia a fallos (Figura 2.50). En RAID 5, la paridad se distribuye sobre todos los discos de modo que los datos se pueden reconstruir si una unidad de disco falla en un conjunto de discos en RAID.

RAID 5 es bueno para aplicaciones con I/O de lectura aleatoria intensa, y preferido para mensajería, data mining, servicios de media de mediano rendimiento y en implementaciones de sistemas de gestión de bases de datos relacionales (RDBMS),

en las cuales los administradores de bases de datos (DBA) optimizan el acceso a los datos.

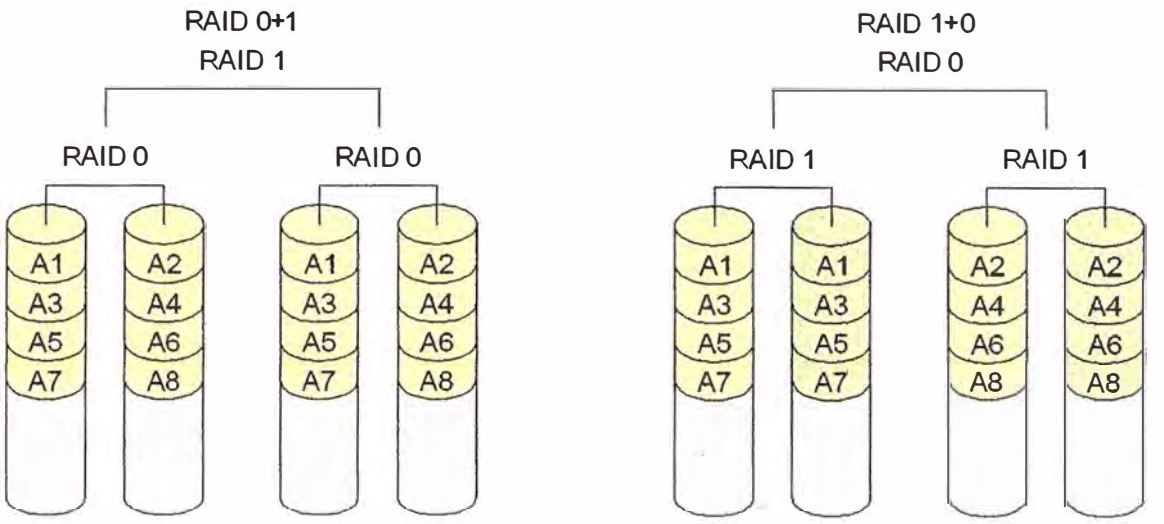


Figura 2.49 Conjunto de discos en RAID 0+1 y RAID 1+0

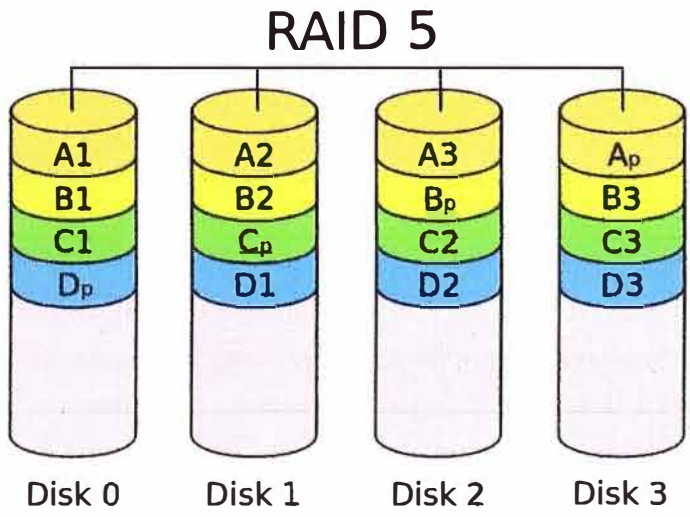


Figura 2.50 Conjunto de discos en RAID 5

e) **RAID 6:** RAID 6 funciona de la misma manera como RAID 5, excepto que RAID 6, incluye un segundo elemento de paridad para permitir la supervivencia si se producen dos fallas de disco en un conjunto de discos en RAID (Figura 2.51). Por lo tanto, una implementación de RAID 6 requiere al menos cuatro discos. RAID 6 distribuye la paridad a través de todos los discos. La penalidad en la escritura en RAID 6 es mayor que en RAID 5, por lo tanto, las escrituras de RAID 5 son de mejor rendimiento que en RAID 6. La operación de reconstrucción en RAID 6 puede tomar más tiempo que

en de RAID 5 debido a la presencia de dos conjuntos de paridad.

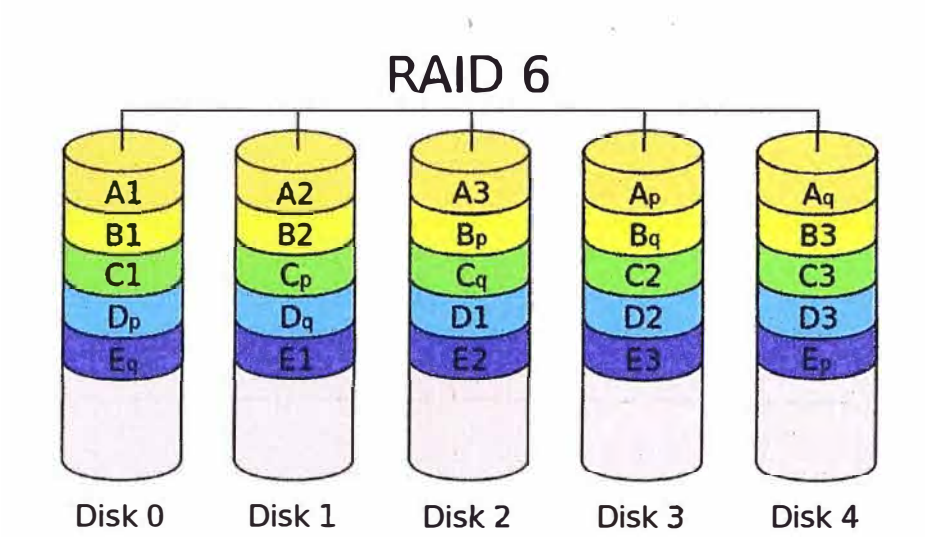


Figura 2.51 Conjunto de discos en RAID 6

Hot Spares

Un hot spare es una unidad de repuesto en un arreglo en RAID que reemplaza temporalmente un disco averiado al adoptar de la identidad de la unidad de disco averiada (Figura 2.52). Se tienen dos métodos de recuperación de datos mediante el uso de hot spare en función de la implementación de RAID:

- Si se usa la paridad de RAID, los datos se re-construye en el hot spare usando la paridad y los datos en las unidades de disco que sobreviven en el conjunto de discos en RAID.
- Si se usa mirroring, se utiliza los datos del mirror sobreviviente para copiar los datos en el hot spare.

Cuando se añade una nueva unidad de disco en el sistema, los datos del hot spare se copian en la nueva unidad de disco. El hot spare vuelve a su estado en espera, listo para reemplazar a la siguiente unidad de disco que falle. Alternativamente, el hot spare sustituye a la unidad de disco que ha fallado de forma permanente. Esto significa que ya no es un hot spare, y se debe configurar un nuevo hot spare en el arreglo de discos.

2.2.6 Sistemas de Almacenamiento Inteligentes

Las aplicaciones críticas de negocio requieren altos niveles de rendimiento, disponibilidad, seguridad y escalabilidad. La unidad de disco es el elemento central de almacenamiento la cual rige el rendimiento de cualquier sistema de almacenamiento. Algunas tecnologías de arreglos de discos antiguas no podían superar las limitaciones de rendimiento debido a las limitaciones de las unidades de disco y sus componentes

mecánicos. La tecnología RAID hizo una importante contribución a la mejora en el rendimiento de almacenamiento y la fiabilidad, pero las unidades de disco, incluso con una implementación RAID, no pueden cumplir con los requerimientos de rendimiento de las aplicaciones actuales.

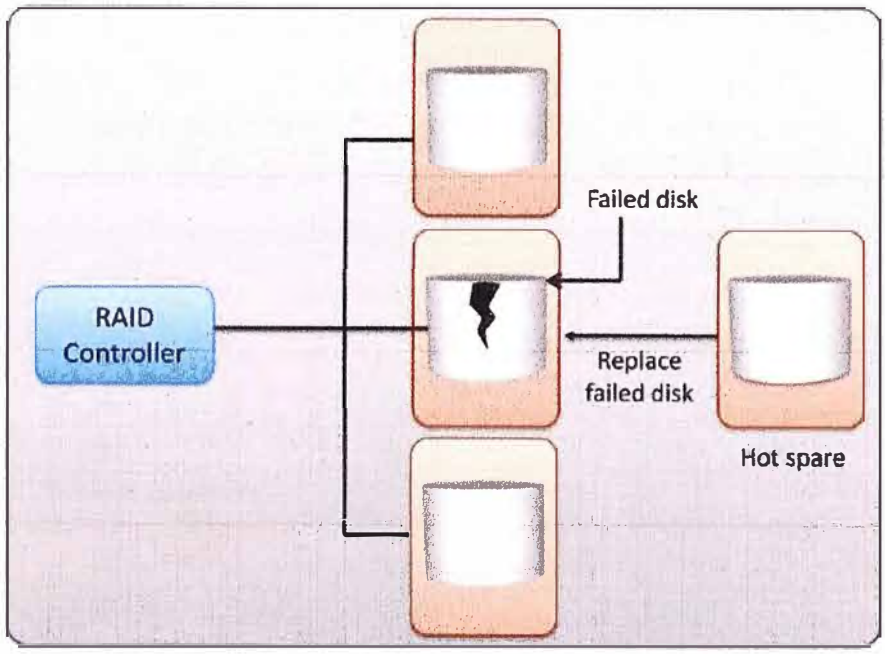


Figura 2.52 Unidad de repuesto Hot Spare

Con los avances en la tecnología, una nueva generación de soluciones de almacenamiento, conocidos como sistemas de almacenamiento inteligente, ha evolucionado. Estos sistemas de almacenamiento inteligentes son ricos en funcionalidades de arreglos RAID, que ofrecen capacidades de procesamiento de I/O altamente optimizado. Estos sistemas de almacenamiento están configurados con una gran cantidad de memoria (llamada memoria caché), con múltiples rutas de I/O y utilizan sofisticados algoritmos para satisfacer los requerimientos de las aplicaciones sensibles al rendimiento. Estos arreglos tienen un entorno operativo que inteligentemente y de manera óptima se encarga de la administración, asignación y utilización de los recursos de almacenamiento. El soporte de unidades flash y otras tecnologías de hoy en día, tales como el aprovisionamiento de almacenamiento virtual y el almacenamiento por niveles automatizado, han añadido una nueva dimensión al sistema de almacenamiento en rendimiento, escalabilidad y disponibilidad.

En esta sección se cubrirá los componentes de los sistemas de almacenamiento inteligentes, junto con el aprovisionamiento de almacenamiento a las aplicaciones.

Componentes de un sistema de almacenamiento inteligente

Un sistema de almacenamiento inteligente consta de cuatro componentes principales: el front-end, la caché, el back-end y los discos físicos. En la figura inferior se ilustra estos componentes y sus interconexiones. Una solicitud de I/O recibida desde el host en el puerto front-end es procesada a través de la caché y el back-end, para permitir el almacenamiento y la recuperación de los datos desde el disco físico. Una petición de lectura puede ser atendida directamente desde la memoria caché si el dato solicitado se encuentra en la memoria caché. En los sistemas de almacenamiento inteligente modernos, el front-end, la caché y back-end se integran normalmente en una sola tarjeta (llamada procesador de almacenamiento o controlador de almacenamiento).

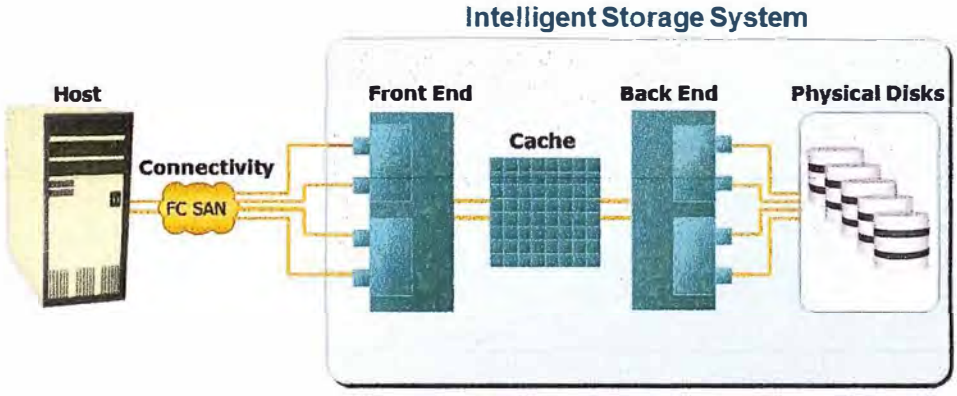


Figura 2.53 Sistema de almacenamiento inteligente

Front-end: El front-end proporciona la interfaz entre el sistema de almacenamiento y el host (Figura 2.54). Consta de dos componentes: los puertos front-end y los controladores front-end. Por lo general, un front-end tiene controladores redundantes en alta disponibilidad, y cada controlador tiene varios puertos que permiten que un gran número de hosts se conecten al sistema de almacenamiento inteligente. Cada controlador front-end tiene una lógica de procesamiento que ejecuta el protocolo de transporte apropiado, tales como Fibre Channel, iSCSI, FICON, o FCoE para conexiones de almacenamiento.

Los controladores front-end enrutan datos desde y hacia la memoria caché a través del bus de datos interno. Cuando la caché recibe los datos de escritura, el controlador envía un mensaje de confirmación al host.

Caché: La caché es una memoria de semiconductores donde los datos se colocan temporalmente para reducir el tiempo requerido para atender a las solicitudes de I/O desde el host (Figura 2.55).

La cache mejora el rendimiento del sistema de almacenamiento al aislar a los hosts de los retrasos mecánicos asociados a los discos giratorios o unidades de disco duro (HDD). Los discos giratorios son el componente más lento de un sistema de almacenamiento inteligente. El acceso a los datos en discos giratorios suele tardar varios milisegundos debido tiempo de búsqueda y latencia rotacional. El acceso a los datos de la memoria caché es rápido y normalmente toma menos de un milisegundo. En los arreglos inteligentes, los datos de escritura se colocan primero en caché y luego se escriben en disco.

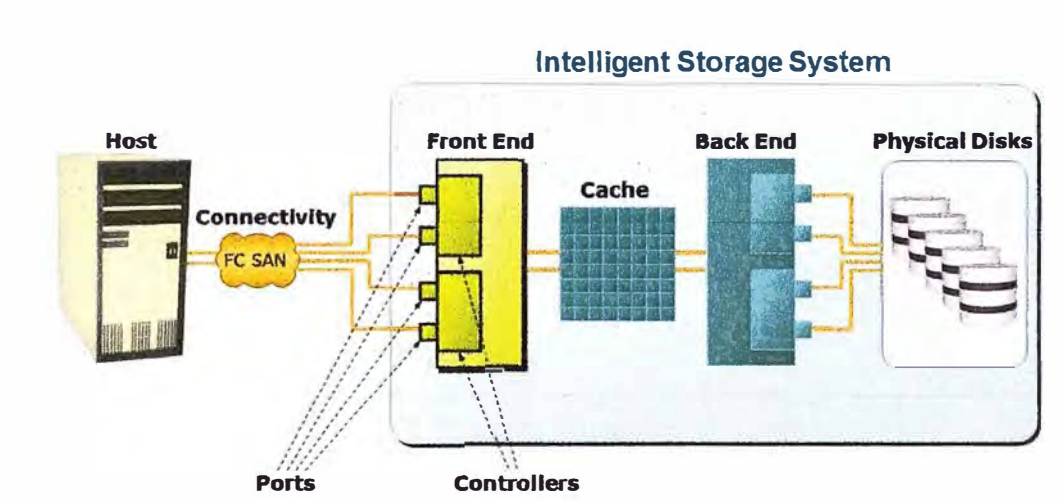


Figura 2.54 Interface de conectividad Front-end

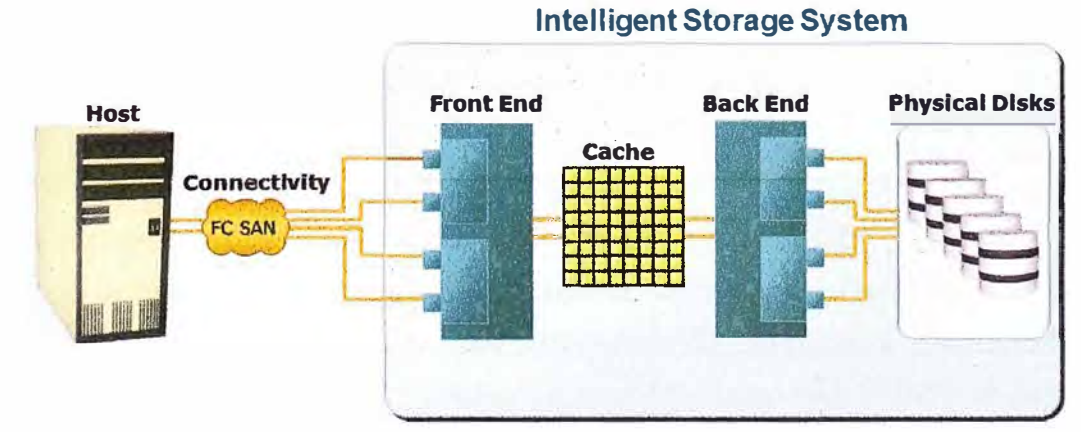


Figura 2.55 Módulo de memoria Caché

Back-end: El back-end proporciona una interfaz entre la caché y los discos físicos. Consta de dos componentes: los puertos back-end y los controladores back-end. El back-end controla las transferencias de datos entre la cache y los discos físicos. De la caché,

los datos se envían al back-end y luego enrutados al disco de destino.

Los discos físicos están conectados a los puertos back-end. El controlador back-end se comunica con los discos al realizar lecturas y escrituras y también proporciona adicionalmente almacenamiento temporal limitado de datos. Los algoritmos implementados en los controladores back-end proporcionan detección y corrección de errores, junto con la funcionalidad RAID.

Para una alta protección de datos y alta disponibilidad, los sistemas de almacenamiento están configurados con controladores duales con varios puertos. Tales configuraciones ofrecen una ruta alternativa a los discos físicos si se produce una falla en el controlador o en el puerto. Esta fiabilidad es aún mayor si los discos son también de dos puertos. En ese caso, cada puerto del disco se puede conectar a un controlador separado. El uso de múltiples controladores también facilita el equilibrio de carga.

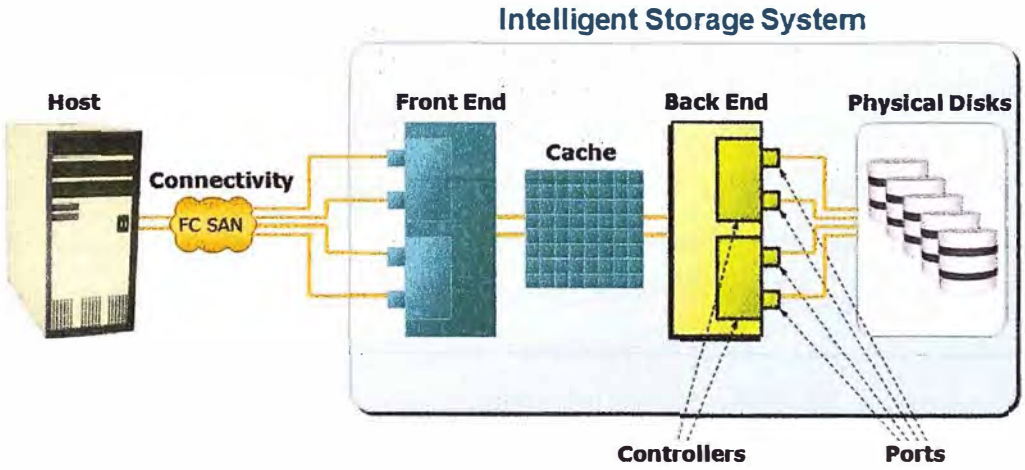


Figura 2.56 Interface de conectividad Back-end

Discos físicos: Los discos físicos se conectan a la controladora de almacenamiento back-end y proporcionan un almacenamiento de datos persistente (Figura 2.57). Los sistemas de almacenamiento inteligentes modernos soportan una variedad de unidades de disco con diferentes velocidades y tipos, tales como FC, SATA, SAS y unidades flash. También soportan el uso mixto de unidades de disco FC, flash, SAS y SATA en el mismo arreglo.

Aprovisionamiento de almacenamiento

En el aprovisionamiento de almacenamiento, los discos físicos se agrupan juntos de manera lógica y se les aplica un nivel de RAID deseado para formar un conjunto, llamado conjunto de discos en RAID. El número de unidades en el conjunto de discos en RAID y el nivel de RAID determinan la disponibilidad, la capacidad y el rendimiento del conjunto

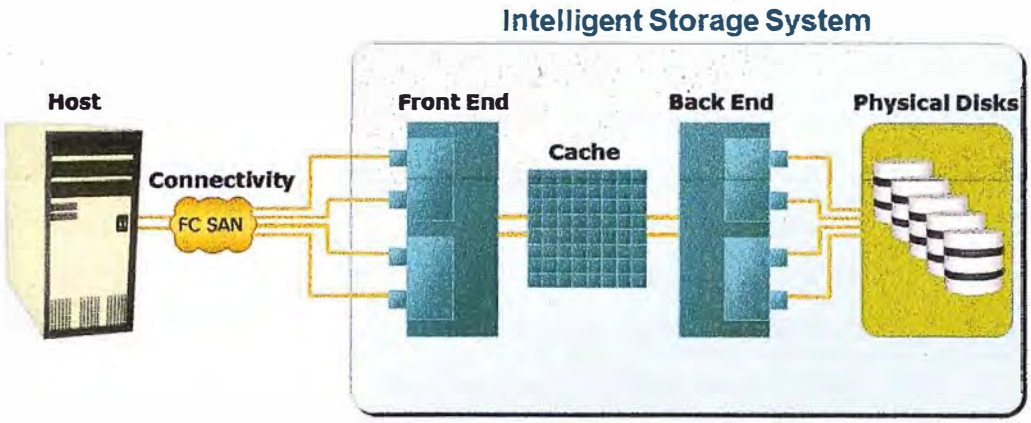


Figura 2.57 Discos físicos

de discos en RAID. Se recomienda que el conjunto de discos en RAID se genere a partir de unidades de disco del mismo tipo, velocidad y capacidad para garantizar la máxima capacidad utilizable, confiabilidad y consistencia en el rendimiento. Por ejemplo, si se mezclan unidades de disco de distintas capacidades en un conjunto de discos en RAID, la capacidad de la unidad de disco más pequeña se usara como referencia en cada disco en el conjunto para generar la capacidad total del conjunto de discos en RAID. La capacidad restante de las unidades de disco más grandes permanecerá inutilizada. Del mismo modo, mezclar discos de altas revoluciones por minuto (RPM) con discos de RPM bajas reduce el rendimiento total del conjunto de discos en RAID.

Los conjuntos de discos en RAID usualmente tienen una gran capacidad ya que combinan la capacidad total de las unidades de disco individuales en el conjunto. A partir de los conjuntos de discos en RAID se crean las unidades lógicas mediante el particionamiento de la capacidad disponible en unidades más pequeñas. Estas unidades son posteriormente asignadas al host en base a sus requerimientos de almacenamiento.

Las unidades lógicas se esparcen sobre todos los discos físicos que pertenecen al conjunto. A cada unidad lógica creada a partir del conjunto de discos en RAID se le asigna un ID único, llamado un Logical Unit Number (LUN). La LUN oculta la organización y la composición del conjunto de discos en RAID a los host.

La figura inferior muestra un conjunto de discos en RAID que consta de cinco discos que han sido particionados, en dos LUNs: LUN 0 y LUN 1. Estas LUNs son asignadas a los hosts Host1 y Host2 para sus necesidades de almacenamiento.

Cuando una LUN está configurada y se le asigna a un host no virtualizado, se requiere una escaneo de bus para identificar a la LUN. Esta LUN aparece como un disco en bruto para el sistema operativo. Para hacer este disco utilizable, el disco es formateado con un sistema de archivos y luego el sistema de archivos es montado.

En un entorno de host virtualizado, la LUN es asignada al hipervisor, el cual la reconoce como un disco en bruto. El disco es configurado con el sistema de archivos del hipervisor y luego sobre él se crean máquinas virtuales con sus respectivos discos virtuales. Los discos virtuales son archivos en el sistema de archivos del hipervisor. Los discos virtuales son asignados a las máquinas virtuales y aparecen como discos en bruto para ellas. Para hacer que el disco virtual sea utilizable para la máquina virtual, se siguen pasos similares como en un entorno no virtualizado. Aquí, el espacio de la LUN puede ser compartido y accedido simultáneamente por varias máquinas virtuales.

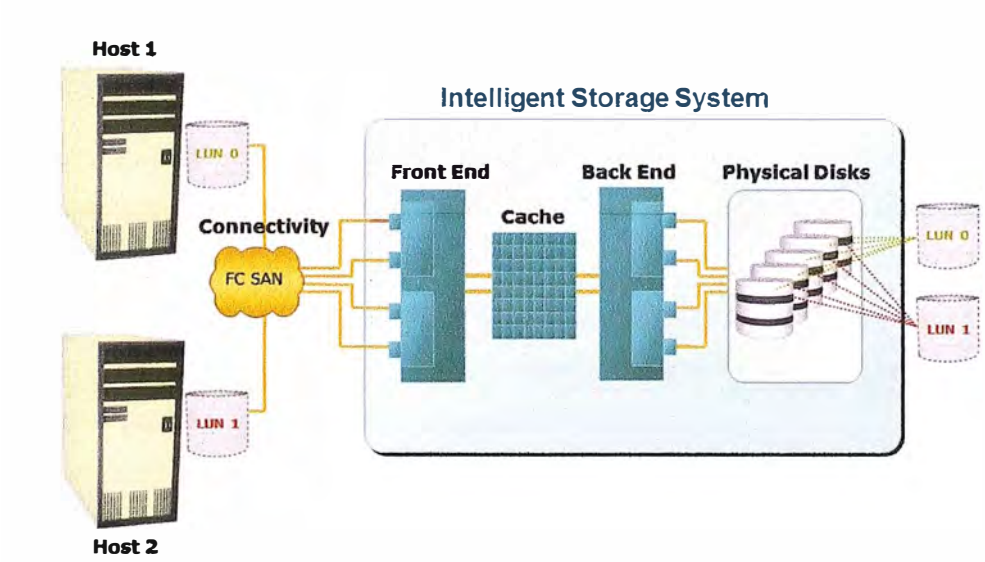


Figura 2.58 Conjunto de discos en RAID y unidades lógicas de almacenamiento LUNs

Tipos de sistemas de almacenamiento inteligente

En la actualidad se tienen dos categorías de sistemas de almacenamiento inteligentes: sistemas de almacenamiento de gama alta y sistemas de almacenamiento de gama media.

Tradicionalmente, los sistemas de almacenamiento de gama alta se implementaban con una configuración activo-activo, mientras que los sistemas de almacenamiento de gama media se implementaban con una configuración activo-pasivo. Las distinciones entre estas dos implementaciones son cada vez más insignificantes.

Sistemas de almacenamiento de gama alta: Los sistemas de almacenamiento de gama alta, conocidos como arreglos activo-activo, generalmente están dirigidos a grandes aplicaciones empresariales. Estos sistemas están diseñados con un gran número de controladores y memoria cache. Un arreglo activo-activo implica que el host puede realizar I/O a su LUN a través de cualquiera de los controladores disponibles.

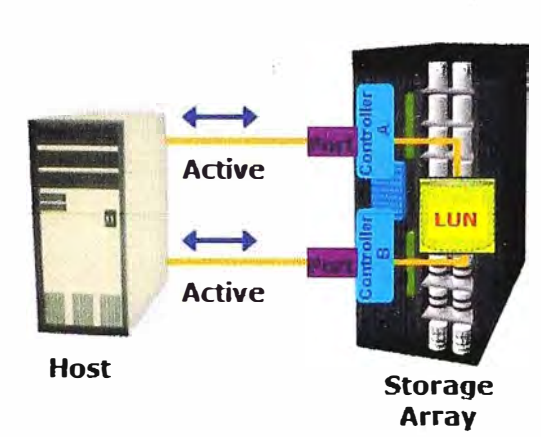


Figura 2.59 Arreglo activo-activo

Para hacer frente a las necesidades de almacenamiento empresarial, estos arreglos proporcionan las siguientes capacidades:

Gran capacidad de almacenamiento.

Grandes cantidades de memoria caché para atender I/Os de host de forma óptima.

Arquitectura con tolerancia a fallos para mejorar la disponibilidad de datos.

Conectividad para mainframe y hosts de sistemas abiertos.

Disponibilidad de múltiples puertos front-end y de protocolos de interfaz para atender a un gran número de hosts.

Disponibilidad de múltiples controladores back-end para administrar el procesamiento de disco.

Escalabilidad para soportar una mayor conectividad, rendimiento y requerimientos de capacidad de almacenamiento.

Capacidad para manejar grandes cantidades de I/Os concurrentes de varios hosts y aplicaciones.

Soporte de replicación de datos local y remota basada en arreglos.

Además de estas características, los sistemas de gama alta poseen algunas características únicas que se requieren para las aplicaciones de misión crítica.

Sistemas de almacenamiento de gama media: Los sistemas de almacenamiento de gama media también se les conoce como arreglos activo-pasivo y son los más adecuados para aplicaciones de pequeñas y medianas empresas. También ofrecen soluciones óptimas de almacenamiento a un menor costo. En un arreglo activo-pasivo, un host puede realizar I/Os a un LUN sólo a través del controlador que posee la LUN. Como se muestra en la figura inferior, el host puede realizar lecturas o escrituras sobre la LUN sólo a través de la ruta hacia el controlador A ya que el controlador A es el dueño de esa LUN. La ruta hacia el controlador B permanece pasiva y ninguna actividad de I/O se lleva

a cabo a través de esta ruta. Los sistemas de almacenamiento de gama media se diseñan con dos controladores, cada uno de los cuales contiene interfaces de host, caché, controladores RAID, y una interfaz para unidades de disco.

Los arreglos de gama media están diseñados para satisfacer los requerimientos de aplicaciones de pequeñas y medianas empresas, por lo tanto, albergan menos capacidad de almacenamiento y de caché que los arreglos de almacenamiento de gama alta. Poseen también un menor número de puertos de front-end para la conexión a los hosts. Sin embargo, aseguran una alta redundancia y alto rendimiento para aplicaciones con cargas de trabajo predecibles. También soportan la replicación local y remota basada en arreglos.

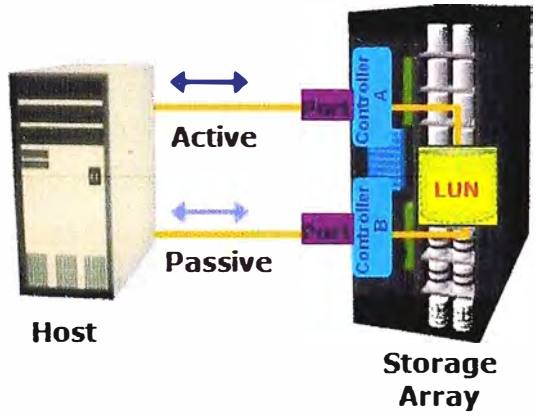


Figura 2.60 Arreglo activo-pasivo

2.2.7 Tecnologías de Redes de Almacenamiento

La SAN es una red de alta velocidad, dedicada para la comunicación de servidores y dispositivos de almacenamiento compartido. Una SAN proporciona la consolidación del almacenamiento y facilita la administración de datos centralizada. Cubre las demandas de almacenamiento de manera eficiente y también proporciona mantenimiento y protección de datos efectiva de los datos.

Las implementaciones de SAN comunes son la SAN Fibre Channel (SAN FC) y la SAN IP. La SAN FC utiliza el protocolo Fibre Channel para el transporte de datos, comandos e información de estado entre los servidores (o hosts) y dispositivos de almacenamiento. La SAN IP utiliza protocolos basados en IP para la comunicación.

a) Fibre Channel Storage Area Network (SAN FC)

Fibre Channel es una tecnología de red de alta velocidad que opera en cables de fibra óptica de alta velocidad y cables de cobre seriales. La tecnología FC fue desarrollado para satisfacer la demanda de mayores velocidades de transferencia de datos entre servidores y sistemas de almacenamiento masivo. El Technical Committee T11, el cual

es el comité en el International Committee for Information Technology Standards (INCITS), es responsable de las normas de interfaz de Fibre Channel.

La alta velocidad de transmisión de datos es una característica importante de la tecnología de redes FC. La implementación inicialmente ofrecía un rendimiento de 200 MB/s (equivalente a una velocidad de bits en bruto de 1 Gb/s), la cual fue mayor que las velocidades de Ultra SCSI (20 MB/s), comúnmente utilizado en entornos DAS. En comparación con Ultra SCSI, FC es un salto significativo en la tecnología de redes de almacenamiento. Las últimas implementaciones de FC de 16 GFC (Fibre Channel) ofrecen una capacidad de 3200 MB/s (velocidad de bits en bruto de 16 Gb/s), mientras que Ultra640 SCSI está disponible con un rendimiento de 640 MB/s. La arquitectura de FC es altamente escalable, y en teoría, una única red FC tiene capacidad de 15 millones de dispositivos aproximadamente.

Componentes

La SAN FC es una red de servidores y dispositivos de almacenamiento compartidos. Los servidores y los dispositivos de almacenamiento son los dispositivos finales (o "nodos") en la SAN. La infraestructura SAN FC está compuesta de puertos de nodo, cables, conectores, dispositivos de interconexión (como switches FC o hubs), y el software de administración de SAN.

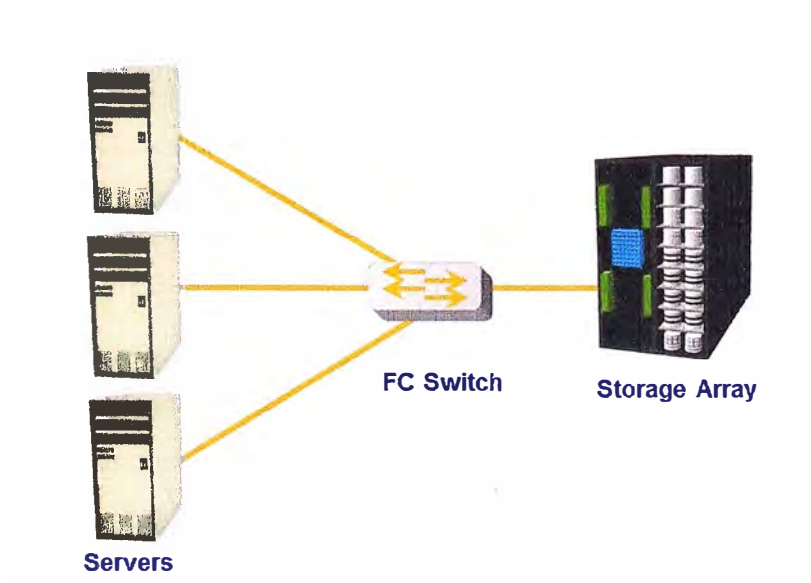


Figura 2.61 Red de área de almacenamiento Fibre Channel (SAN FC)

Puertos de nodo: En una red Fibre Channel, a los dispositivos finales tales como hosts, arreglos de almacenamiento y librerías de cinta, se les denomina nodos (Figura 2.62). Cada nodo es el origen o destino de la información para uno o más nodos. Cada nodo requiere uno o más puertos para proporcionar una interfaz física para la

comunicación con otros nodos. Estos puertos son componentes integrados de los adaptadores de host, tales como HBAs y adaptadores front-end de almacenamiento. En un entorno FC un puerto opera en el modo de transmisión de datos full dúplex con un enlace de transmisión (Tx) y un enlace de recepción (Rx).

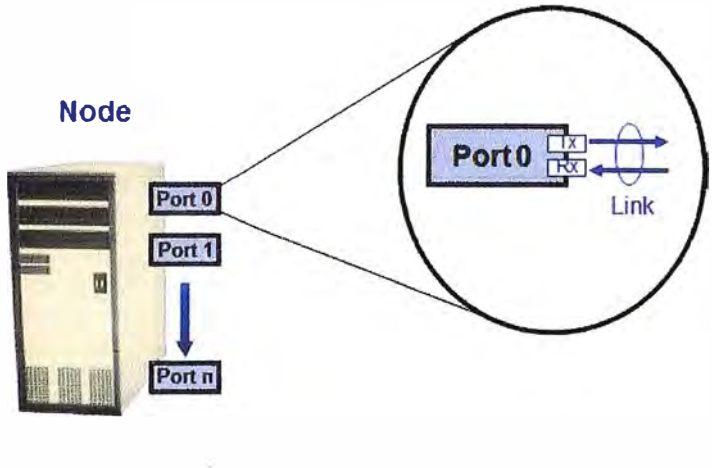


Figura 2.62 Puertos de nodo

Cables y Conectores: Las implementaciones SAN utilizan cableado de fibra óptica. El cobre puede ser utilizado para distancias más cortas, ya que proporciona una relación señal a ruido aceptable para distancias de hasta 30 metros. Los cables de fibra óptica transportan datos en forma de luz. Hay dos tipos de cables ópticos: monomodo y multimodo. El cable de fibra multimodo (MMF) transporta varios haces de luz proyectados desde distintos ángulos al mismo tiempo en el núcleo del cable. Basado en el ancho de banda, las fibras multimodo se clasifican como OM1 (62.5µm), OM2 (50µm), y OM3 de laser optimizado (50µm). En una transmisión MMF, los múltiples haces de luz que viajan en el interior del cable tienden a dispersarse y chocan. Esta colisión debilita la fuerza de la señal después de que se desplaza una cierta distancia - un proceso conocido como dispersión modal. Un cable de MMF se utiliza normalmente para distancias cortas debido a la degradación de la señal (atenuación) por la dispersión modal.

La fibra monomodo (SMF) transporta un solo rayo de luz que se proyecta en el centro del núcleo. Estos cables están disponibles en diámetros de núcleo de 7 a 11 micras; el tamaño más común es de 9 micras. En una transmisión SMF, un único haz de luz viaja en línea recta a través del núcleo de la fibra. El núcleo pequeño y la única onda de luz ayudan a limitar la dispersión modal. Entre todos los tipos de cables de fibra, monomodo proporciona atenuación mínima señal sobre la máxima distancia (hasta 10 km). Un cable monomodo se utiliza para tendidos de cable de larga distancia, y la distancia por lo general depende de la potencia del láser en el transmisor y sensibilidad del receptor.

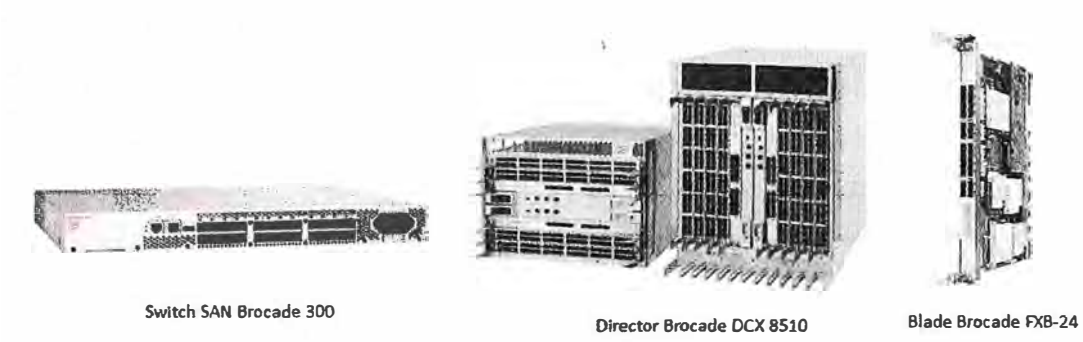


Figura 2.64 Switches modulares y Directores

recursos desde una consola central.

Proporciona funciones de gestión importantes, incluyendo el mapeo de dispositivos de almacenamiento, switches y servidores, supervisión y generación de alertas para dispositivos detectados.

b) IP Storage Area Network (SAN IP)

La SAN tradicional permite la transferencia de I/O de bloques sobre Fibre Channel y ofrece un alto rendimiento y escalabilidad. Estas ventajas de la SAN FC vienen con el costo adicional de comprar componentes, tales como HBAs FC y switches FC. Las organizaciones suelen tener una infraestructura basada en Internet Protocol (IP), la cual podría ser aprovechada para redes de almacenamiento.

Los avances en la tecnología han permitido que IP pueda ser utilizado para el transporte de I/O de bloques sobre la red IP. Esta tecnología de transporte de I/O de bloques sobre IP se le conoce como SAN IP. IP es una tecnología madura, y el uso de IP como una opción de red de almacenamiento ofrece varias ventajas. IP ofrece una administración más fácil y mejor interoperabilidad. Cuando el I/O de bloques opera sobre IP, la infraestructura de red existente puede ser aprovechada, lo cual es más económico que la inversión en una nueva infraestructura SAN FC. Además, hay muchas opciones de seguridad robustas y maduras que están ahora disponibles para las redes IP.

Muchas soluciones de recuperación de desastres (DR) de larga distancia, ya están aprovechando las redes basadas en IP. Con la SAN IP, las organizaciones pueden ampliar el alcance geográfico de su infraestructura de almacenamiento.

Los dos protocolos principales que aprovechan IP como mecanismo de transporte son Internet SCSI (iSCSI) y Fibre Channel sobre IP (FCIP). iSCSI es el encapsulamiento de I/O SCSI sobre IP. FCIP es un protocolo en el que una entidad FCIP como un gateway FCIP se utiliza para generar túneles FC a través de una red IP. En FCIP, las tramas FC

están encapsulados en la carga útil de IP.

1) Protocolo iSCSI

iSCSI es un protocolo basado en IP que establece y gestiona las conexiones entre el host y el almacenamiento sobre IP. iSCSI encapsula los comandos SCSI y datos en un paquete IP y los transporta a través de TCP/IP . iSCSI es ampliamente usado para la conexión de los servidores con el almacenamiento ya que es relativamente barato y fácil de implementar, especialmente en entornos en los que una SAN FC no existe.

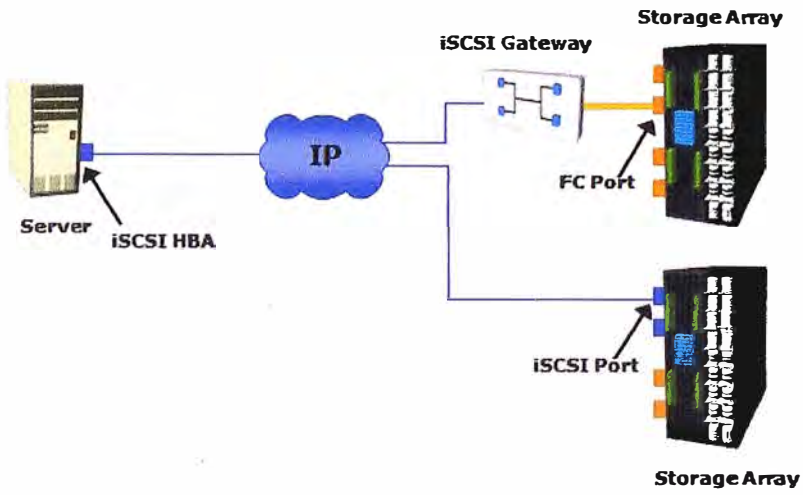


Figura 2.65 Implementación iSCSI

Componentes de iSCSI

Los componentes principales de iSCSI son: el initiator (host), el target (almacenamiento o gateway iSCSI), y una red basada en IP. Si se implementa un arreglo de almacenamiento con soporte iSCSI, entonces un host con el initiator iSCSI puede comunicarse directamente con la arreglo de almacenamiento sobre IP. Sin embargo, en una implementación que utiliza un arreglo de almacenamiento FC existente, para la comunicación iSCSI, se utiliza un gateway iSCSI. Los gateways iSCSI realizan la traducción de los paquetes IP a tramas FC y viceversa, permitiendo así la conectividad entre los entornos IP y FC.

Conectividad iSCSI para Host

Exiten tres opciones de conectividad iSCSI para host: Una NIC estándar con initiator iSCSI por software, una NIC TOE (TCP Offload Engine) con initiator iSCSI por software y un HBA iSCSI. La función del initiator iSCSI es para enrutar los comandos SCSI sobre una red IP.

Una NIC estándar con initiator iSCSI por software es la opción de conectividad más sencilla y de menor costo. Es fácil de implementar debido a que la mayoría de los

servidores vienen con al menos una, y en muchos casos dos NICs incorporadas. Sólo se requiere un iniciador por software para la funcionalidad iSCSI. Debido a que las NICs proporcionan la funcionalidad IP estándar, las tareas de encapsulamiento SCSI en paquetes IP y des encapsulamiento son llevadas a cabo por el CPU. Esto supone una sobrecarga adicional al CPU. Si se utiliza una NIC estándar en situaciones de carga de I/O pesada, el CPU del host puede convertirse en un cuello de botella. La NIC TOE ayuda a aliviar esta carga. La NIC TOE libera al host de la carga de las funciones de gestión TCP y deja sólo la funcionalidad iSCSI al CPU del host. El host pasa la información iSCSI a la tarjeta TOE, y la tarjeta TOE envía la información al destino mediante TCP/IP. Aunque esta solución mejora el rendimiento, la funcionalidad iSCSI está siendo manejada por un initiator por software que requiere ciclos de CPU del host.

Un HBA iSCSI proporciona beneficios en el rendimiento ya que libera la carga al CPU del host de todo el procesamiento iSCSI y TCP/IP. El uso de una HBA iSCSI también es la forma más sencilla de bootear los host desde la SAN por iSCSI. La funcionalidad de un HBA iSCSI es similar a la funcionalidad de un HBA FC.

Topologías iSCSI

Las dos topologías de implementaciones iSCSI son la nativa y la puente. La topología nativa no tiene componentes FC. Los initiators pueden ser conectados directamente a los targets o conectados a través de la red IP. La topología puente permite la coexistencia de FC con IP al proporcionar la funcionalidad puente iSCSI a FC. Por ejemplo, los initiators pueden existir en un entorno IP, mientras que el almacenamiento permanece en un entorno FC.

Conectividad iSCSI nativa: No se requieren componentes FC para la conectividad iSCSI si se implementa un arreglo de almacenamiento con soporte iSCSI. El arreglo de almacenamiento tiene uno o más puertos iSCSI configurados con una dirección IP y está conectado a un switch Ethernet estándar (Figura 2.66).

Después de que un initiator se conecta a la red, éste puede acceder a la LUN disponible en el arreglo de almacenamiento. Un único puerto del arreglo puede atender a múltiples hosts o initiators, siempre y cuando el puerto del arreglo pueda manejar la cantidad de tráfico de almacenamiento que los hosts generen.

Conectividad iSCSI puente: Una implementación iSCSI puente incluye componentes FC en su configuración. En este caso, el arreglo de almacenamiento no tiene ningún puerto iSCSI. Por lo tanto, se debe utilizar un dispositivo externo, denominado gateway o router multiprotocolo para facilitar la comunicación entre el host iSCSI y el almacenamiento FC (Figura 2.67). El gateway convierte los paquetes IP a tramas FC y viceversa. Estos dispositivos puente contienen puertos FC y Ethernet para facilitar la

comunicación entre los entornos FC e IP.

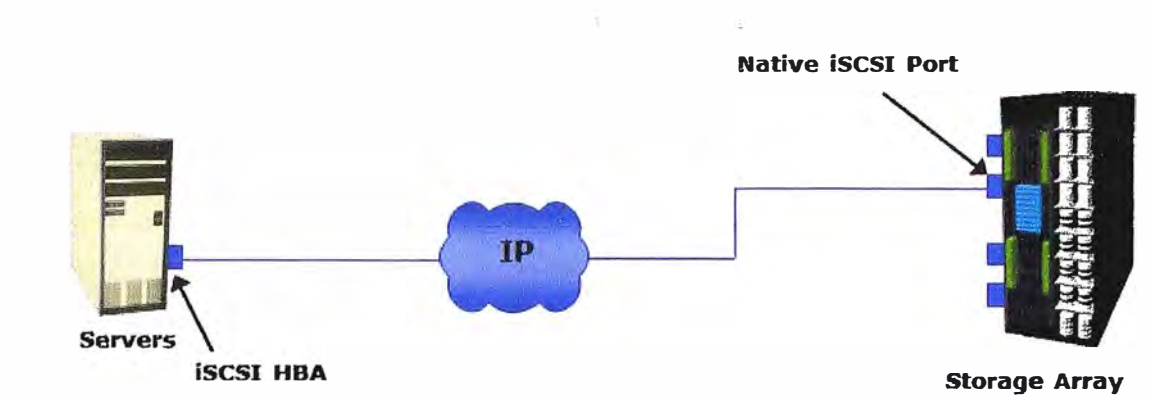


Figura 2.66 Conectividad iSCSI nativa

En una implementación de iSCSI puente, el initiator iSCSI está configurado con la dirección IP del gateway como su target destino. En el otro extremo, el gateway está configurado como un initiator FC hacia el arreglo de almacenamiento.

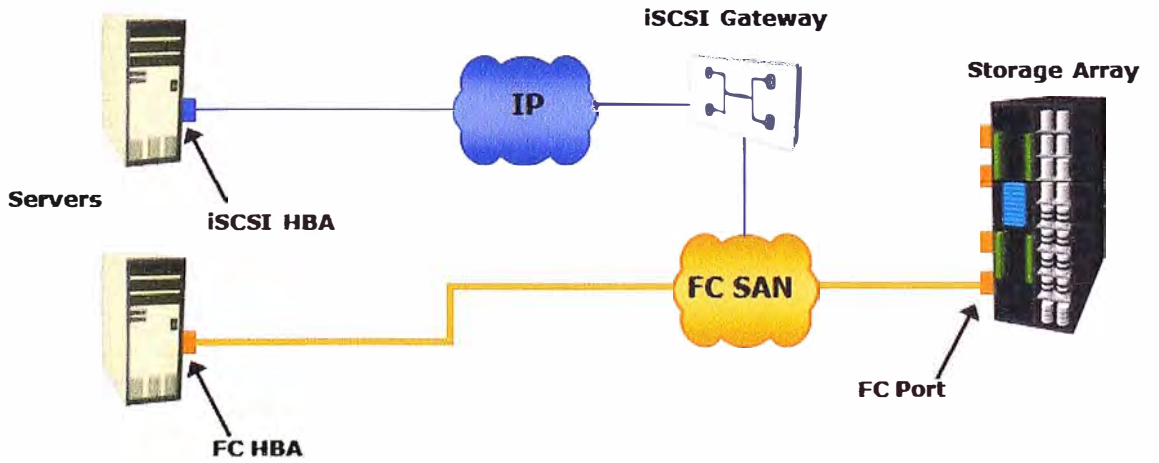


Figura 2.67 Conectividad iSCSI puente

2) Protocolo FCIP

Una SAN FC proporciona una infraestructura de alto rendimiento para el movimiento de datos localizados.

Las organizaciones ahora están buscando maneras de transportar datos a larga distancia entre sus SANs en múltiples ubicaciones geográficas. Una de las mejores maneras de lograr este objetivo es interconectar redes SAN dispersas geográficamente a través de enlaces fiables y de alta velocidad. Este enfoque implica el transporte de los datos de los bloques FC sobre la infraestructura IP. FCIP es un protocolo de túnel que

permite la interconexión de islas SAN FC distribuidas sobre redes IP existentes.

La norma FCIP ha ganado rápidamente la aceptación como una forma manejable, rentable para combinar lo mejor de dos mundos: la SAN FC y la infraestructura IP ampliamente implementada. Como resultado, las organizaciones ahora tienen una mejor manera de almacenar, proteger y mover sus datos mediante el aprovechamiento de las inversiones en sus infraestructuras IP existentes. FCIP se utiliza ampliamente en las implementaciones de recuperación de desastres en las cuales los datos se duplican en un almacenamiento situado en un sitio remoto.

Topología FCIP

En un entorno FCIP, un gateway FCIP está conectado a cada red SAN FC. El gateway FCIP en un extremo de la red IP encapsula las tramas FC en paquetes IP. El gateway en el otro extremo elimina la envoltura IP y envía los datos de FC a la otra red SAN FC. Después de establecer la conectividad IP entre los gateways, los nodos en las redes SAN independientes pueden comunicarse entre sí.

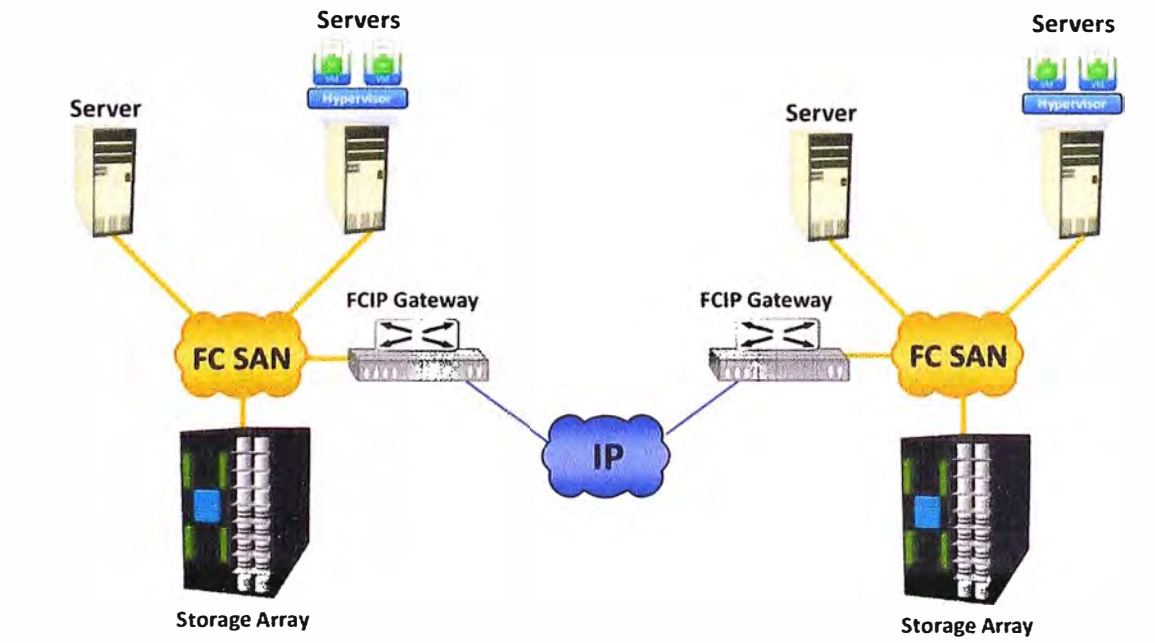


Figura 2.68 Topología FCIP

2.2.8 Replicación Remota

En el entorno empresarial actual, para una organización es imperativo proteger los datos de misión crítica y reducir al mínimo el riesgo de interrupción del negocio. Si se produce un corte local o desastre, la restauración rápida de los datos y el reinicio es esencial para asegurar la Continuidad del Negocio (BC). Una de las formas de asegurar la BC es la replicación. La replicación es el proceso de crear una copia exacta (réplica) de los datos. Estas copias réplicas se utilizan para restaurar y reiniciar las operaciones en

caso de pérdida de datos.

La replicación remota es el proceso de crear réplicas de la información en sitios remotos. La replicación remota ayuda a las organizaciones a mitigar los riesgos asociados con interrupciones resultado de desastres naturales o causados por el hombre. Durante los desastres, la carga de trabajo se puede mover a un sitio remoto para asegurar la operación continua del negocio.

Figura 2.69 Replicación Remota

Modos de replicación remota

Los dos modos básicos de replicación remota son síncronas y asíncronas.

En la replicación remota síncrona, las escrituras deben ser cometidas en el origen y en la réplica remota (o destino), antes de acusar la "escritura completada" hacia el host. No se pueden realizar escrituras adicionales en el origen hasta que cada escritura anterior haya sido completada y acusada (Figura 2.70). Esto asegura que los datos sean idénticos en el origen y en la réplica en todo momento. Además, las escrituras se transmiten al sitio remoto exactamente en el orden en que se reciben en el origen. Por lo tanto, se mantiene un orden de escritura. Si se produce una falla en el sitio origen, la replicación remota síncrona proporciona un Recovery Point Objetivo (RPO) cero o cercano a cero.

Sin embargo, el tiempo de respuesta de una aplicación se incrementa con la replicación remota síncrona porque escrituras deben ser cometidas tanto en el origen como en el destino antes de enviar el acuse de "escritura completada" hacia el host. El grado de impacto en el tiempo de respuesta depende principalmente de la distancia entre los sitios, ancho de banda, y la calidad de servicio (QoS) de la infraestructura de conectividad de red. La figura 2.71 muestra el requerimiento de ancho de banda para la replicación síncrona. Si el ancho de banda proporcionado para la replicación remota síncrona es menor que la carga de trabajo máxima de escritura, habrá momentos durante el día en el que el tiempo de respuesta podría ser excesivamente largo, provocando que el tiempo de espera de las aplicaciones se agote. Las distancias a las que la replicación

síncrona se puede implementar dependen de la capacidad de la aplicación de tolerar demoras en el tiempo de respuesta. Por lo general, se realizan implementaciones para distancias inferiores a 200 Km (125 millas) entre los dos sitios.

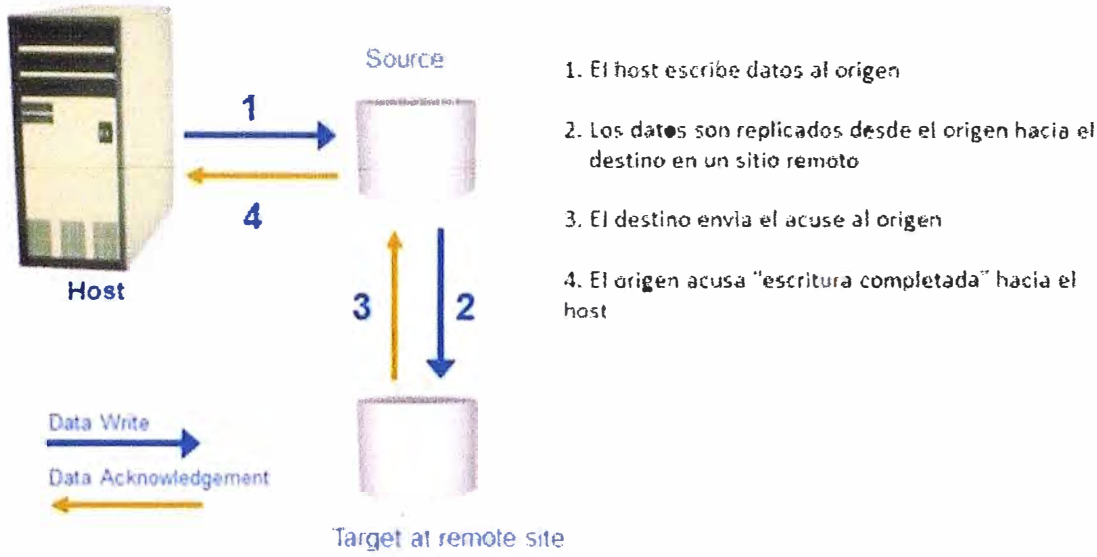


Figura 2.70 Replicación síncrona

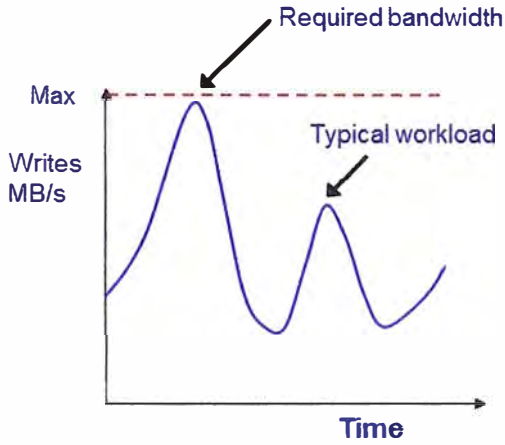


Figura 2.71 Ancho de banda para replicación síncrona

En la replicación remota asíncrona, una vez que la escritura se ha cometido en el origen, inmediatamente es acusada hacia el host. De este modo, los datos se almacenan en buffer en el origen y son transmitidos al sitio remoto posteriormente (Figura 2.72).

La replicación asíncrona elimina el impacto en el tiempo de respuesta de la aplicación, ya que las escrituras son acusadas inmediatamente al host origen. Esto permite la implementación de la replicación asíncrona a distancias que van desde varios cientos a varios miles de kilómetros entre los sitios primarios y remotos. La figura 2.73

muestra el requerimiento de ancho de banda para la replicación asincrónica. En este caso, se puede proporcionar un ancho de banda igual o mayor que la carga de trabajo de escritura promedio. Los datos pueden ser almacenados en buffer durante tiempos en que el ancho de banda no es suficiente y movidos posteriormente al sitio remoto. Por lo tanto, se debería proporcionar una capacidad de buffer suficiente.

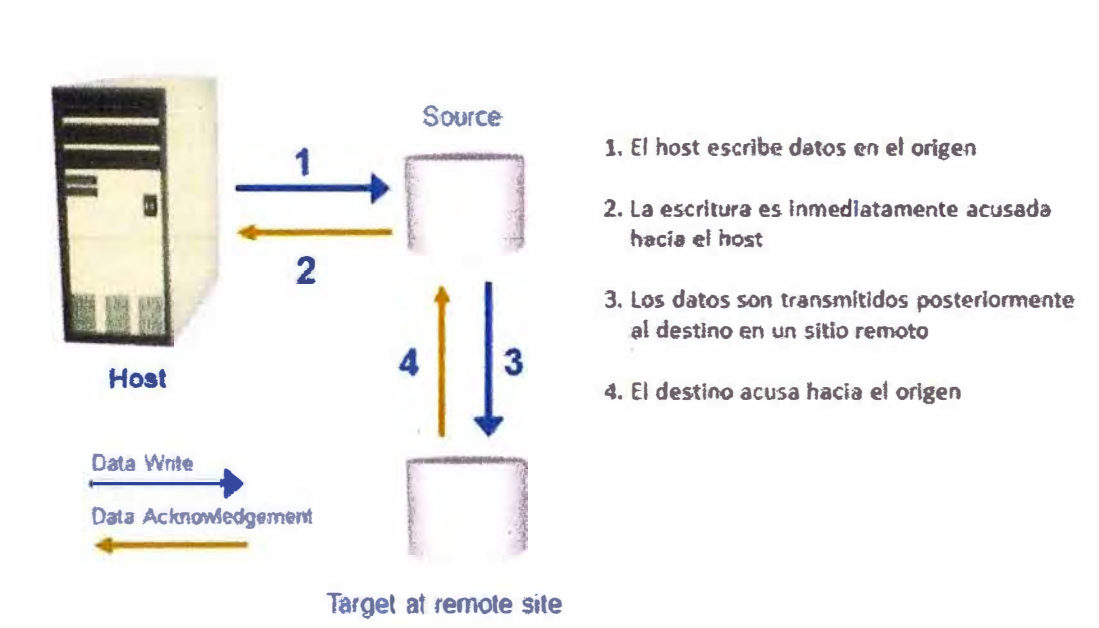


Figura 2.72 Replicación asíncrona

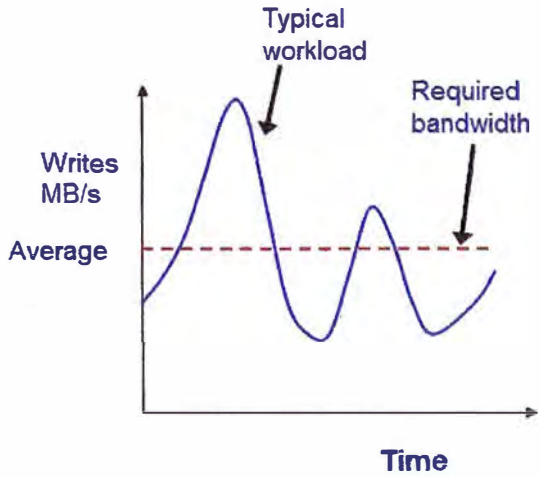


Figura 2.73 Ancho de banda para replicación asíncrona

En la replicación asíncrona, los datos en el sitio remoto estarán atrasados respecto al origen en por lo menos el tamaño del buffer. Por lo tanto, la replicación remota asíncrona

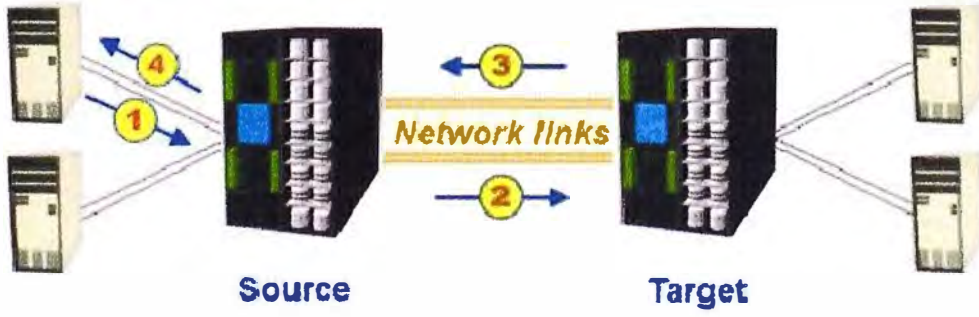
proporciona una solución de recuperación de desastres con RPO finito (distinto de cero). El RPO depende del tamaño del buffer, el ancho de banda de red disponible y la carga de trabajo de escritura en el origen.

En los modos de replicación síncrona y asíncrona, sólo las escrituras en el origen son replican; las lecturas aún se realizan en el origen.

Replicación Remota basada en Arreglos de Almacenamiento

En la replicación remota basada en arreglos de almacenamiento, el entorno operativo y recursos del arreglo realizan y gestionan la replicación de datos. Esto alivia la carga sobre el CPU del host, el cual puede ser mejor utilizado para aplicaciones que se ejecutan en el host. El dispositivo origen y su réplica residen en arreglos de almacenamiento diferentes. Los datos son transmitidos del arreglo de almacenamiento origen hacia el arreglo de almacenamiento destino sobre una red compartida o dedicada. La replicación entre arreglos puede llevarse a cabo en modo síncrono o asíncrono.

Modo de replicación sincrónica: En la replicación remota síncrona basada en arreglo, las escrituras deben ser cometidas en el origen y el destino antes de acusar "escritura completada" hacia el host de producción. No se pueden realizar escrituras adicionales en el origen hasta que cada escritura anterior haya sido completada y acusada. La figura 2.74 muestra el proceso de replicación remota síncrona basada en arreglo.



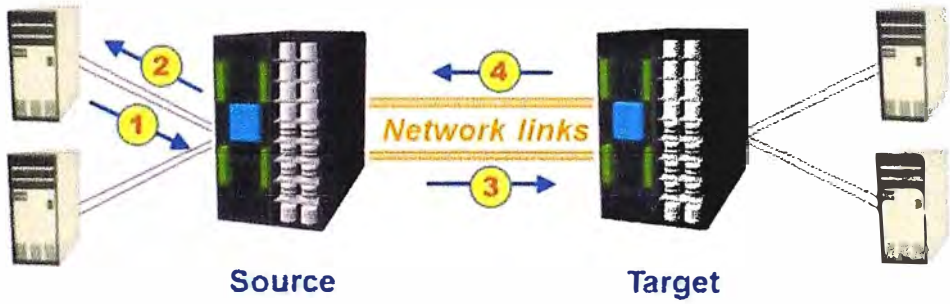
1. El host de producción envía una escritura al arreglo de almacenamiento origen.
2. La escritura luego es transmitida al arreglo de almacenamiento remoto.
3. El arreglo de almacenamiento remoto envía el acuse al arreglo de almacenamiento origen.
4. El arreglo de almacenamiento origen notifica "escritura completada" al host de producción.

Figura 2.74 Replicación remota síncrona basada en arreglo

En el caso de la replicación remota síncrona, para optimizar el proceso de replicación y minimizar el impacto en el tiempo de respuesta de las aplicaciones, la escritura se almacena en la cache de los dos arreglos. Posteriormente los arreglos de almacenamiento inteligentes almacenan estas escrituras en los discos apropiados.

Si los enlaces de red fallan, la replicación se suspende, sin embargo, el trabajo de producción puede continuar sin interrupción en el arreglo de almacenamiento origen. El entorno operativo del arreglo mantiene un registro de las escrituras que no se transmiten al arreglo de almacenamiento remoto. Cuando los enlaces de la red se restablecen, los datos acumulados se transmiten al arreglo de almacenamiento remoto. Si durante el tiempo en que permanece interrumpido el enlace de red se produce un corte de servicio en el origen, se perderán algunos datos, y el RPO en el objetivo no será cero.

Modo de replicación asíncrona: En el modo de replicación remota asíncrona basada en arreglo, como se muestra en la figura 2.75, la escritura se comete en el origen e inmediatamente es acusada al host. Los datos se almacenan en buffer en el origen y posteriormente se transmiten al sitio remoto. Los dispositivos origen y destino no contienen datos idénticos todo momento. Los datos del dispositivo destino están atrasados respecto al origen, por lo que el RPO en este caso no es cero.



1. El host de producción escribe en el arreglo de almacenamiento origen.
2. El arreglo origen inmediatamente acusa al host de producción.
3. Las escrituras son luego transmitidas al arreglo destino.
4. Luego que las escrituras son recibidas en el arreglo destino, éste envía un acuse al arreglo origen.

Figura 2.75 Replicación remota asíncrona basada en arreglo

Al igual que en la replicación sincrónica, en la replicación asincrónica las escrituras se almacenada en cache en los dos arreglos y posteriormente son almacenados en los discos correspondientes.

En algunas implementaciones de replicación remota asíncrona se mantienen un orden de escritura. A cada escritura se le adjunta un timestamp y un número de secuencia cuando es recibida por el origen. Las escrituras se transmiten luego al arreglo remoto, en el cual son cometidas en la réplica remota en el mismo orden en que fueron almacenadas en buffer en el origen. Esto garantiza implícitamente la consistencia de los datos en las réplicas remotas. Otras implementaciones garantizan la consistencia, aprovechando el principio de escritura dependiente inherente en la mayoría de las bases

de datos. En la replicación remota asíncrona, las escrituras se almacenan en buffer durante un periodo de tiempo predefinido. Al final de este periodo, el buffer se cierra, y un nuevo buffer se abre para las siguientes escrituras. Todas las escrituras en el buffer cerrado se transmiten juntas y son cometidas hacia la réplica remota.

La replicación remota asíncrona proporciona ahorro de costos en el ancho de banda de red debido a que el ancho de banda requerido es menor que la carga de trabajo de escritura pico. En momentos en que la carga de trabajo de escritura supera el ancho de banda promedio, se debe configurar suficiente espacio de buffer en el arreglo de almacenamiento origen para mantener estas escrituras.

2.3 Continuidad de Negocio y Recuperación ante Desastres

En la actualidad, el acceso continuo a la información es una necesidad para el buen funcionamiento de las operaciones del negocio. El costo de la falta de disponibilidad de la información es mayor que antes, y las interrupciones en las principales industrias cuestan millones de dólares por hora. Hay muchas amenazas para la disponibilidad de la información, como los desastres naturales, los incidentes no planificados, y los incidentes planeados, que podrían resultar en la falta de acceso a la información. Por lo tanto es muy importante para las empresas definir una estrategia adecuada que les pueda ayudar a superar esas crisis. La continuidad del negocio es un proceso importante para definir y poner en práctica estas estrategias.

La Continuidad de Negocio (BC) es un proceso integrado y para toda la empresa, que incluye todas las actividades (internas y externas a IT) que una empresa debe realizar para mitigar el impacto del tiempo de inactividad planificado y no planificado. La BC implica la preparación, la respuesta y la recuperación de una interrupción del sistema que afecta negativamente a las operaciones de negocio. Involucra medidas proactivas, tales como análisis de impacto en el negocio, evaluaciones de riesgo, implementación de soluciones de tecnología de BC (backup y replicación), y medidas reactivas, como la recuperación ante desastres y reinicio, que deben invocarse en el caso de una falla. El objetivo de una solución de BC es asegurar la "disponibilidad de la información" necesaria para llevar a cabo operaciones vitales de negocio.

En un entorno virtualizado, las soluciones de tecnología de BC necesitan proteger los recursos, tanto físicos como virtuales. La virtualización simplifica considerablemente la implementación de las estrategias de BC

2.3.1 Causas de la falta de Disponibilidad de la Información

Varios incidentes planificados y no planificados resultan en la falta de disponibilidad

de información. Las interrupciones planificadas incluyen la instalación, integración, mantenimiento de un nuevo hardware, actualizaciones de software y parches, realizar backups, restauración de aplicaciones y datos, operaciones sobre instalación (renovación y construcción), la actualización y migración de un entorno de prueba a producción. Las interrupciones no planificadas incluyen fallas causadas por errores humanos, corrupción de bases de datos, y fallas de los componentes físicos y virtuales.

Otro tipo de incidente que pueda causar falta de disponibilidad de los datos son los desastres naturales o provocados por el hombre, tales como inundaciones, incendios, terremotos y contaminación. Como se muestra en la figura 2.76, la mayoría de interrupciones son planeadas. Las interrupciones planificadas son esperadas y son programadas, pero aun así causan que los datos no estén disponibles. Estadísticamente, la causa de la falta de disponibilidad de información debido a desastres imprevistos es menos de 1 por ciento.

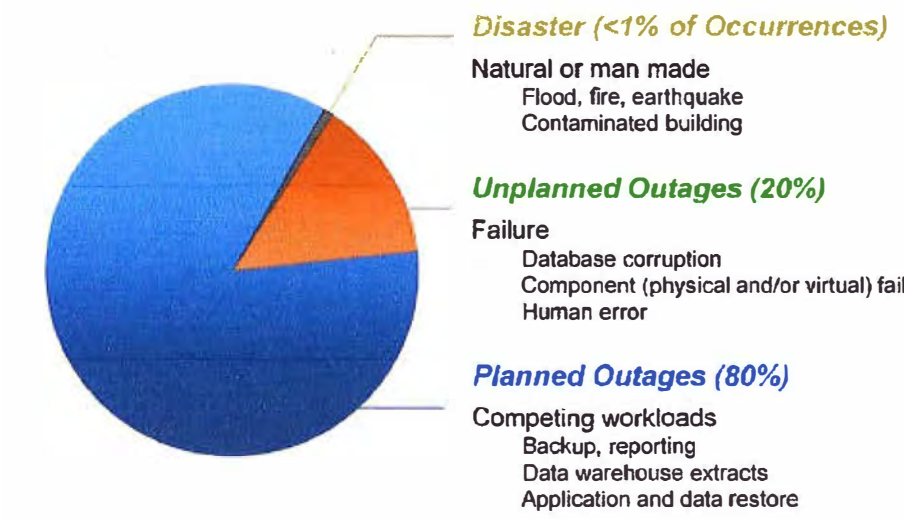


Figura 2.76 Interrupción de la disponibilidad de la información

2.3.2 Consecuencias de la Inactividad

La falta de disponibilidad de información o tiempo de inactividad resultan en la pérdida de productividad, pérdida de ingresos, bajo rendimiento financiero, y daños a la reputación. La pérdida de productividad incluye reducción de la producción por unidad de mano de obra, equipamiento y capital. La pérdida de ingresos incluye la pérdida directa, pagos compensatorios, pérdida de ingresos futuros, pérdida de facturación, y la pérdida de la inversión. El bajo rendimiento financiero afecta el reconocimiento de ingresos, flujo de efectivo, descuentos, garantías de pago, calificación crediticia, y precio de las acciones. Los daños a la reputación pueden resultar en una pérdida de confianza y credibilidad con los clientes, proveedores, mercados financieros, bancos y socios de

negocios. Otras posibles consecuencias de la inactividad incluyen el costo de alquiler de equipos adicionales, horas extras, y el envío adicional.

2.3.3 Terminología BC

La recuperación de desastres: Es el proceso coordinado de restauración de los sistemas, datos, e infraestructura necesario para soportar las operaciones del negocio en curso después de que ocurra un desastre. Es el proceso de restauración de una copia anterior de los datos y registros aplicables u otros procesos necesarios para que esa copia sea llevada a un punto de consistencia conocida. Una vez completados todos los esfuerzos de recuperación, los datos son validados para asegurar que sean los correctos.

Recovery Point Objective (RPO): Este es el punto en el tiempo en que los sistemas y los datos deben ser recuperados después de una interrupción. Define la cantidad de datos perdidos que una empresa puede tolerar. Un gran RPO significa una alta tolerancia a la pérdida de información en una empresa. En base al RPO, las organizaciones planifican la frecuencia con que se deben realizar el backup o réplica. Por ejemplo, si el RPO es de 6 horas, los backups o réplicas deben hacerse por lo menos una vez cada 6 horas. La figura 2.77 muestra varios RPO y sus correspondientes estrategias de recuperación ideales. Una organización puede planificar una solución de tecnología de BC apropiada basándose en el RPO que necesita.

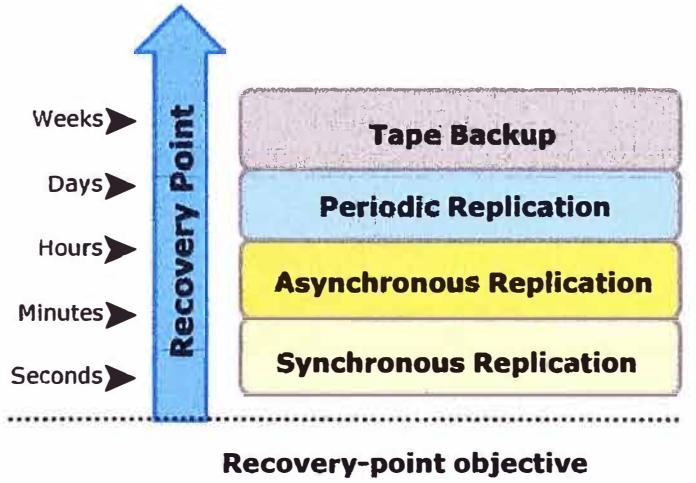


Figura 2.77 Estrategias RPO

Recovery Time Objective (RTO): El tiempo en el cual los sistemas y las aplicaciones se deben recuperar después de una interrupción. Define el tiempo de inactividad que una empresa puede soportar y sobrevivir. Las empresas pueden optimizar los planes de recuperación ante desastres después de definir el RTO para un sistema dado. Por

ejemplo, si el RTO es de 2 horas, se requiere un backup basado en disco, ya que permite una restauración más rápida que una un backup en cinta. Sin embargo, para un RTO de 1 semana, el backup en cinta podría cumplir con este requerimiento. La figura 2.78 muestra algunos RTOs y sus estrategias de recuperación.

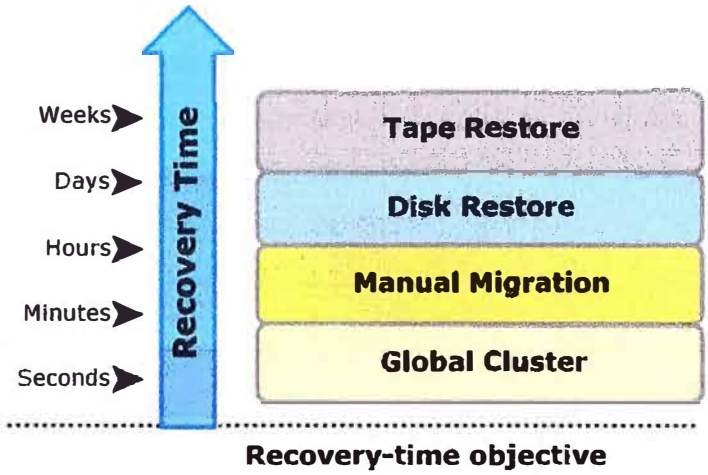


Figura 2.78 Estrategias RTO

2.3.4 Punto Único de Falla

Para mitigar los puntos únicos de falla, los sistemas se diseñan con redundancia, de tal manera que el sistema sólo falle si todos los componentes del grupo de redundancia fallan. Esto asegura que la falla de un solo componente no afecte a la disponibilidad de datos. Los centros de datos siguen pautas estrictas para poner en práctica la tolerancia a fallos para la disponibilidad ininterrumpida de la información. Un cuidadoso análisis se realiza para eliminar cualquier punto único de falla. En la figura inferior se muestra una infraestructura con componentes redundantes que mitigan los puntos únicos de falla.

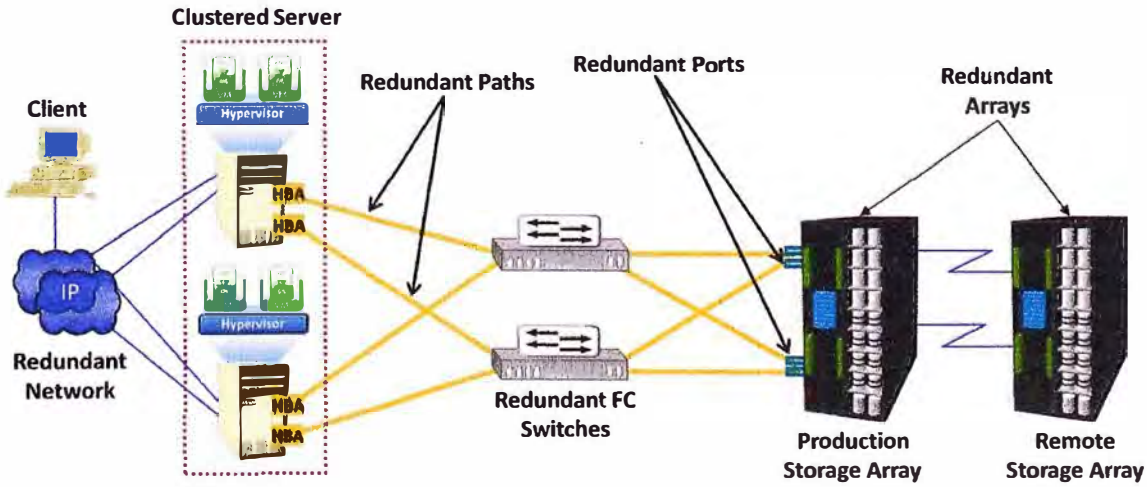


Figura 2.79 Infraestructura con componentes redundantes

- Configuración de HBA redundantes en un servidor para mitigar la falla de una única HBA.
- Configuración de NIC teaming en el servidor permite la protección contra falla de una única NIC. Se permite la agrupación de dos o más tarjetas de red físicas y tratarlos como un único dispositivo lógico. Con NIC teaming, si una de las tarjetas de red físicas subyacentes falla o el cable se desconecta, el tráfico se redirige a otra tarjeta de red física en el team. Por lo tanto, el NIC teaming elimina el punto único de falla asociado con una sola tarjeta de red física.
- Configuración de switches redundantes para soportar la falla de un switch.
- Configuración de múltiples puertos de arreglo de almacenamiento para mitigar la falla de un puerto.
- Configuración de RAID y hot spare para asegurar la operación continua en caso de falla en disco.
- Implementación de un arreglo de almacenamiento redundante en un sitio remoto para mitigar la falla en el sitio local.
- Implementación de clustering de servidores, un mecanismo de tolerancia a fallas mediante el cual dos o más servidores de un clúster tienen acceso al mismo conjunto de volúmenes de datos. Los servidores clusterizados intercambian heartbeats para informarse mutuamente acerca de su salud. Si uno de los servidores o hipervisores falla, el otro servidor o hipervisor puede tomar la carga de trabajo.
- La implementación de un mecanismo de tolerancia a fallos VM asegura BC en el caso de una falla en el servidor. Esta técnica crea copias duplicadas de cada máquina virtual en otro servidor de manera que cuando se detecta un fallo de máquina virtual, la máquina virtual duplicado se puede utilizar para la conmutación por error. Las dos máquinas virtuales se mantienen en sincronización con los demás con el fin de realizar la conmutación por error con éxito.

2.3.5 Soluciones de Tecnología de BC

Después de analizar el impacto de una interrupción en el negocio, el siguiente paso es el diseño de las soluciones adecuadas para recuperarse de una falla. Una o varias copias de los datos se mantienen utilizando cualquiera de las siguientes estrategias para que los datos puedan ser recuperados o las operaciones de las empresas pueden reanudarse mediante una copia alternativa:

Backup: El backup de los datos es el principal método para asegurar la disponibilidad

de datos. La frecuencia de los backups se determina en base al RPO, RTO, y frecuencia con la que cambian los datos.

Replicación Local: La información se replica en una ubicación separada dentro del mismo arreglo de almacenamiento. La réplica se utiliza de forma independiente para otras operaciones de negocio. Las réplicas también se pueden utilizar para las operaciones de restauración de si se produce una corrupción de datos.

Replicación Remota: Los datos en un arreglo de almacenamiento se replican en otro arreglo de almacenamiento que se encuentra en un sitio remoto. Si el arreglo de almacenamiento se daña debido a un desastre, las operaciones del negocio pueden iniciarse desde el arreglo de almacenamiento remoto.

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capitulo se realizara la evaluación de alternativas de solución que permita a las empresas contar con una solución de alta disponibilidad y recuperación ante desastres para sus centros de datos. Se describirán los criterios tomados en consideración para la elección y diseño de la implementación de la solución.

Finalmente se presentara la arquitectura y funcionalidades de la solución propuesta

3.1 Evaluación de Alternativas

En la actualidad se cuenta con diversos enfoques y tecnologías que permiten a los centros de datos tener alta disponibilidad y recuperación ante desastres. Estas soluciones permiten reducir la interrupción de las operaciones ocasionadas por fallas de hardware, proteger la información y reanudar operaciones en el sitio remoto en el menor tiempo posible.

Entre las alternativas típicas que permiten alta disponibilidad y/o recuperación ante desastres se tiene:

Backup en cinta: Permite respaldar datos estructurados y no estructurados en medios externos como cintas magnéticas. El backup en cinta es usado generalmente para recuperar datos de manera granular como un archivo, un mensaje de correo, alguna tabla de base de datos, etc.

Los propósitos principales del backup en cinta son: recuperación granular de datos, archivado de información histórica y recuperación ante desastres.

La utilización del backup en cintas como una opción ante desastre es viable pero con la principal desventaja de tener un RTO muy elevado. Recuperar información de varios servidores a partir de backup en cinta puede tomar días e incluso semanas debido a que se tiene que preparar nuevos host, reinstalar los sistemas operativos y aplicaciones y luego restaurar los datos a partir de las cintas.

Sin embargo, se recomienda siempre tener una solución de backup en cintas ya que es el último recurso ante alguna posible corrupción o pérdida de datos específicos luego de una recuperación ante desastres.

Replicación basada en host: En esta opción, se instala un software de replicación

sobre el sistema operativo del servidor (físico o virtual) en el origen y en el destino y no depende ni requiere componentes de hardware adicionales para su funcionamiento. La replicación basada en host agrega carga de procesamiento al CPU del host. Los recursos de CPU en el servidor origen son compartidos entre la tarea de replicación y la aplicación. Esto podría causar degradación del rendimiento e inestabilidad para las aplicaciones que se ejecutan en el host. El costo de licenciamiento y la administración se incrementan cuando se necesita replicar varios servidores (físicos o virtuales) por lo que este tipo de solución esta mayormente orientado a pequeñas y medianas empresas que no pueden optar por una replicación basada en almacenamiento.

La replicación basada en host tiene mayor soporte y compatibilidad con sistemas operativos Windows que sistemas operativos Linux.

La replicación remota basada en host es asíncrona

Replicación basada en almacenamiento: En esta opción la tarea de replicación remota es llevada a cabo por el sistema de almacenamiento. No se consumen recursos de CPU del host para la replicación por lo que los recursos host son dedicados para la aplicación. La replicación basada en almacenamiento es transparente para el host e independiente del sistema operativo ya sea Windows, Linux, Unix, mainframe, etc.

Las principales ventajas son que en la mayoría de sistemas de almacenamiento de gama media soportan replicación síncrona y asíncrona. Es la mejor opción para entornos críticos ya que permiten RPOs y RTOs muy bajos comparados a otras soluciones.

Las principales desventajas son el alto costo de los sistemas de almacenamiento que soportan replicación los cuales deben ser de la misma marca y modelo. Por tal motivo, esta solución está orientada a medianas y grande empresas en las que la alta disponibilidad y la continuidad del negocio son muy importantes para sus actividades productivas.

Recuperación ante Desastres en la Nube: Es una solución nueva en estos días que está comenzando a tener valor para las empresas que no cuentan con los recursos económicos para desplegar un sitio remoto. La principal ventaja radica en que no se requiere de inversión en hardware, software y ni costos operacionales en un sitio remoto ya que se está optando por un servicio de nube pública de un proveedor de servicios.

Una de las principales desventajas está relacionada a la seguridad y ubicación real de la información. Debido a políticas internas de seguridad de la información, las grandes empresas prefieren no colocar en la nube pública información sensible del negocio.

Otra desventaja es que se tiene que poseer y manejar tecnologías de hardware y software compatibles con las utilizadas por el proveedor de servicios.

3.2 Propuesta de solución

En la presente propuesta de solución se diseñará una arquitectura que cumplirá con los necesidades de uso eficiente de los recursos del servidor, alta disponibilidad y recuperación ante desastres mediante el uso de la virtualización de servidores x86, sistemas de almacenamiento centralizado con tecnología de replicación, y software de recuperación ante desastre que permita la automatización de la recuperación ante desastres mediante la integración con el sistema de almacenamiento y el software de virtualización. Esta propuesta permitirá reducir el RPO y el RTO ante un desastre que produzca la pérdida parcial o total de la información en el sitio principal.

Para dimensionar la solución, se tomara como referencia el siguiente escenario típico de implementación:

Una mediana empresa de 800 usuarios que cuenta con una infraestructura tradicional de servidores con una antigüedad de 4 años aproximadamente. No se tiene implementada una solución de alta disponibilidad ni se tiene protección ante un desastre en el centro de datos. Todos los equipos tienen 5 años de antigüedad y ya no cuentan con soporte ni garantía.

A continuación se presentan los datos técnicos necesarios a tener en cuenta para el diseño:

- 20 servidores x86 físicos de 2 sockets (con CPUs Quad-Core). De los cuales 16 servidores son de carga moderada en CPU y 4 servidores de alta carga en CPU.
- Los 16 servidores tienen 6GB de memoria RAM instalada y 4 servidores cuentan con 12GB de RAM.
- La capacidad total de la información almacenada en los 20 servidores es de 4.5TB.
- Cada servidor cuenta con 1 puerto de red Gigabit.
- Se cuenta con una oficina remota con conexión dedicada de 4Mbps.

Las necesidades de la empresa son:

- Reducir costos de adquisición de nuevos servidores.
- Alta disponibilidad para todos los servidores.
- Balanceo de carga de CPU y memoria a nivel de servidores.
- Balanceo de carga de uso de almacenamiento.
- Contar con una solución de recuperación ante desastres para todos los servidores.
- Escalabilidad a nivel de servidores y almacenamiento. Dimensionado para crecimiento a 3 años, con una proyección de crecimiento de 30%.

Diseño de componentes de la solución

La solución propuesta consistirá en reducir al máximo la cantidad de servidores a adquirir. Por tal motivo se virtualizarán todos los servidores físicos.

a) Hosts

El dimensionamiento de la cantidad de servidores y sus características está en función de la cantidad de máquinas virtuales que se alojaran y la proyección de crecimiento.

- Cantidad de CPUs

  La cantidad de vCPU necesarios para alojar las 20 máquinas virtuales está dado por:

  - 16 máquinas virtuales de 2 vCPU (carga moderada): 32 vCPU
  - 4 máquinas virtuales de 4 vCPUs (alta carga): 16 vCPU

  Si proyectamos crecimiento de máquinas virtuales en un 30% en 3 años, se tiene lo siguiente:

  - 21 máquinas virtuales de 2 vCPU (carga moderada): 42 vCPU.
  - 6 máquinas virtuales de 4 vCPUs (alta carga): 24 vCPU.

  Según las buenas prácticas de VMware se puede colocar de 2 a 4 vCPUs por core físico para máquinas virtuales de carga moderada, y 1 vCPU por cada core físico para máquinas virtuales de alta carga.

  - Para las 21 máquinas virtuales se necesitarían de 11 a 21 cores físicos (asumiremos 21 cores físicos).
  - Para las 6 máquinas virtuales se necesitarían 24 cores físicos.

  Serán necesarios por lo menos 45 cores físicos para poder ejecutar 27 servidores virtualizados (máquinas virtuales) en nuevos servidores de mayor rendimiento.

  Esto equivale a tener que considerar 3 servidores de 2 CPU físicos con 8 cores por CPU. Como se desea tener alta disponibilidad de hosts (tolerancia a falla de un host) que alojaran máquinas virtuales, se necesitara un host adicional a la cantidad de host necesarios (configuración N+1).

  Finalmente, para este escenario serían necesarios 4 servidores de 2 CPU físicos de 8 cores para virtualizar 27 máquinas virtuales.

- Memoria RAM

  La cantidad de memoria RAM necesaria para las 27 máquinas virtuales es la siguiente:

  - 21 máquinas virtuales de 6GB de vRAM (carga moderada): 126GB de vRAM
  - 6 máquinas virtuales de 12GB de vCPUs (alta carga): 72GB de vRAM

  Por lo tanto serán necesarios 198GB físicos distribuidos en 4 servidores físicos.

- Puertos de red

  La mayoría de servidores actuales traen cuatro puertos de red 1Gb integrados lo que es suficiente para este escenario ya que se tiene en promedio 8 máquinas

virtuales por servidor físico.

Por razones de redundancia se suele colocar una tarjeta de red de cuatro puertos adicional ante una posible falla de los puertos integrados. Se considerara para el diseño una tarjeta de cuatro puertos de 1Gb adicional para los cuatro servidores.

- Discos internos

  Para la instalación del hipervisor se necesita de 4 a 5 GB como mínimo en almacenamiento. Se considerara un arreglo de dos discos en RAID 1

  No se requiere más discos internos ya que las máquinas virtuales estarán alojadas en un sistema de almacenamiento externo.

- HBA

  Los cuatro servidores necesitaran acceso al sistema de almacenamiento. Para este escenario se consideran HBAs Fibre Channel de 8Gb de dos puertos (por redundancia).

b) Sistema de almacenamiento

El dimensionamiento de la capacidad en TB está en función a la capacidad de la información total actual más el crecimiento proyectado (30%). Para este escenario se tiene 4.5TB de información total. La capacidad necesaria a dimensionar considerando el crecimiento a 3 años de 30% seria de 6TB.

En ambientes virtualizados se tiene también que considerar espacio adicional para operaciones propias de la virtualización como: almacenamiento para snapshots de las máquinas virtuales, almacenamiento para memoria swap de máquinas virtuales (equivalente a la memoria física de los hosts) y espacio libre para migraciones de máquinas virtuales de LUN a LUN para balanceo de carga. El cálculo de la capacidad total necesaria es la siguiente:

Capacidad Total = [Capacidad de los datos] + [Capacidad de memoria física total de los servidores] + [Capacidad para los snapshots (20%)] + [Capacidad libre para operaciones (30%)]

Reemplazando valores:

$$Capacidad\ Total = 6TB + 0.198TB + 1.2TB + 1.8 = 9.2TB$$

Existen diversas opciones de marcas y modelos que pueden proporcionar los 9.2TB necesarios. Para este caso son necesarias las siguientes características adicionales cuando se trabaja con virtualización y recuperación ante desastres.

- Controladores redundantes: Se seleccionan de acuerdo al protocolo de conectividad hacia la SAN. Existen controladores con puertos integrados SAS, iSCS y FC.
- Cache: Las controladoras incluyen memoria cache que permite mejorar el rendimiento al acelerar las tareas de escritura de los servidores en el sistema de almacenamiento.
- Discos: Los sistemas de almacenamiento soportan discos SATA, SAS, y SSD. Los discos SATA (7200 RPM) son usados generalmente para crear LUNs que almacenan datos no estructurados como archivos o información histórica ya que no son accedidos con mucha frecuencia, los discos SAS (10000 RPM o 15000 RPM) se usan para crear LUNs que almacenan datos estructurados como bases de datos y máquinas virtuales ya que generan más accesos de lectura y escritura. Las unidades SSD son unidades de almacenamiento basado en flash y no en discos magnéticos como los SATA y SAS. Estos discos son mucho más rápidos y caros que los discos SAS.
- Opción de Thin Provisioning en las LUNs: La tecnología de Thin Provisioning permite generar LUNs con una capacidad determinada pero esta capacidad no es reservada en el sistema en almacenamiento. A medida que se almacenan datos en la LUN, se va consumiendo capacidad en el sistema de almacenamiento. Esta funcionalidad permite el uso eficiente de la capacidad total de sistema de almacenamiento.
- Opción de snapshots de LUNs: Permite la generación de snapshots o copias en el tiempo de LUNs. Esta funcionalidad permite revertir cambios y realizar pruebas de recuperación ante desastres.
- Opción de replicación remota de LUNs síncrona y/o asíncrona: Sera necesario que el sistema de almacenamiento soporte replicación síncrona y/o asíncrona.

c) Switches SAN

Son necesarios para conectar los servidores al sistema de almacenamiento. Serán necesitan 2 switches FC de 8Gb (por redundancia).

d) Software de virtualización

Se propone usar VMware vSphere Enterprise Edition para los 8 servidores ya que permitirá el uso de las siguientes tecnologías:

vMotion: Migración de máquinas virtuales encendidas de un servidor físico a otro. Esta funcionalidad permite balancear carga de CPU y memoria RAM y realizar mantenimientos.

Storage vMotion: Migración de máquinas virtuales encendidas de una LUN a otra.

Permite balancear la carga de I/O en las LUNs y colocar máquinas virtuales en LUNs con mayor espacio.

High Availabilty (HA): Realiza el reinicio automático de máquinas virtuales en otros servidores del clúster debido a una falla de hardware en el servidor que las alberga.

DRS: Permite que las tareas de vMotion sean automáticas y administradas por la consola de administración VMware vCenter Server.

DPM: Permite ahorrar consumo de energía al apagar host que tienen baja carga de CPU y memoria. La consola de administración VMware vCenter migra automáticamente máquinas virtuales mediante vMotion hasta liberar un host para luego apagarlo. Cuando la carga de CPU y memoria empieza a subir, la consola enciende el host y retorna las máquinas virtuales hacia el host.

Se propone también el uso de software de recuperación ante desastres VMware vCenter Site Recovery Manager que permite automatizar las tareas de recuperación ante desastres mediante la integración con la consola de administración VMware vCenter Server y el sistema de almacenamiento HP 3PAR StoreServ 7200.

Beneficios de la solución propuesta

Las principales ventajas de la solución propuesta son:

- Disminución en la adquisición de servidores nuevos. No serán necesarios adquirir ni administrar 54 servidores, sino 8 servidores
- Menor consumo de energía. El consumo de energía en servidores se reducirá en 86% debido a un mejor uso de los recursos cuando se opta por la virtualización.
- Centralización de la información. Todas las máquinas virtuales están almacenadas en un sistema de almacenamiento central. Permitirá una administración centralizada de las máquinas virtuales.
- Las máquinas virtuales no son dependientes de un servidor específico. Las máquinas virtuales pueden ser migradas o reiniciadas en otros hosts del clúster
- Balanceo de carga de uso de CPU y memoria RAM. Si alguna máquina virtual comienza a consumir más recursos de CPU o memoria RAM de un host, ésta será migrada a otro host con más recursos de manera automatizada sin necesidad de apagarla.
- Alta disponibilidad de máquinas virtuales. La solución propuesta reducirá los tiempos de interrupción de servicios ante la caída de un host. Si un host fallara, todas sus máquinas virtuales serán reiniciadas automáticamente en los demás hosts del clúster.

- Fácil mantenimiento. Si se desea apagar un host por motivos de mantenimiento, sólo será necesario migrar las máquinas virtuales encendidas que se ejecutan en él hacia otros host.
- Replicación remota a través de sistemas de almacenamiento. Los sistemas de almacenamiento además de almacenar información de manera centralizada, permite replicar toda la información en un sitio remoto, protegiendo así la información ante la pérdida parcial o total del sitio principal debido a un desastre.
- Recuperación ante desastres automatizado. La virtualización permite automatizar las tareas de recuperación en un sitio remoto mediante el uso de VMware vCenter Site Recovery Manager el cual realizara todas las reconfiguraciones necesarias en las máquinas virtuales replicadas en el sitio secundario. El RTO será prácticamente el tiempo que las máquinas virtuales toman en reiniciar, aproximadamente 2 minutos por cada máquina virtual.

3.3 Topología y funcionalidad de la solución

La propuesta de solución consta de los siguientes componentes de hardware y software:

a) 8 servidores x86 para Virtualización (4 unidades por sitio)
Modelo: HP ProLiant DL360p Gen8

Figura 3.1 Servidor tipo rack HP ProLiant DL360p Gen8

b) 4 Switches SAN FC (2 unidades por sitio)
Modelo: HP 8/8 Base SAN Switch

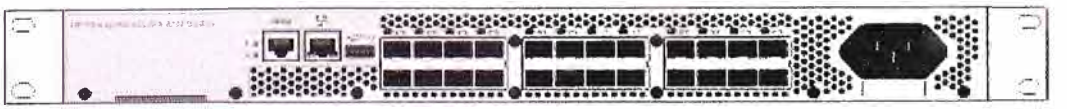


Figura 3.2 Switch Fibre Channel HP 8/8 Base SAN Switch

c) 2 Sistemas de Almacenamiento (1 unidad por sitio)
Modelo: HP 3PAR StoreServ 7200

Figura 3.3 Sistema de almacenamiento HP 3PAR StoreServ 7200 (10TB)

d) Software de Virtualización

Licencias VMware

16 licencias VMware vSphere Enterprise Edition

2 licencias VMware vCenter Server Standard Edition

2 licencias de VMware vCenter Site Recovery Manager para replicación de 25 máquinas virtuales

Figura 3.4 Licencias VMware

En la figura 3.5 se muestra el diagrama lógico de la solución propuesta como servidores, sistema de almacenamiento, red SAN, máquinas virtuales y replicación ente sistemas de almacenamiento

En la figura 3.6 se muestra la distribución física de los equipos que forman parte de la solución propuesta, así como el detalle de la conectividad LAN y SAN en el sitio principal y en el sitio secundario

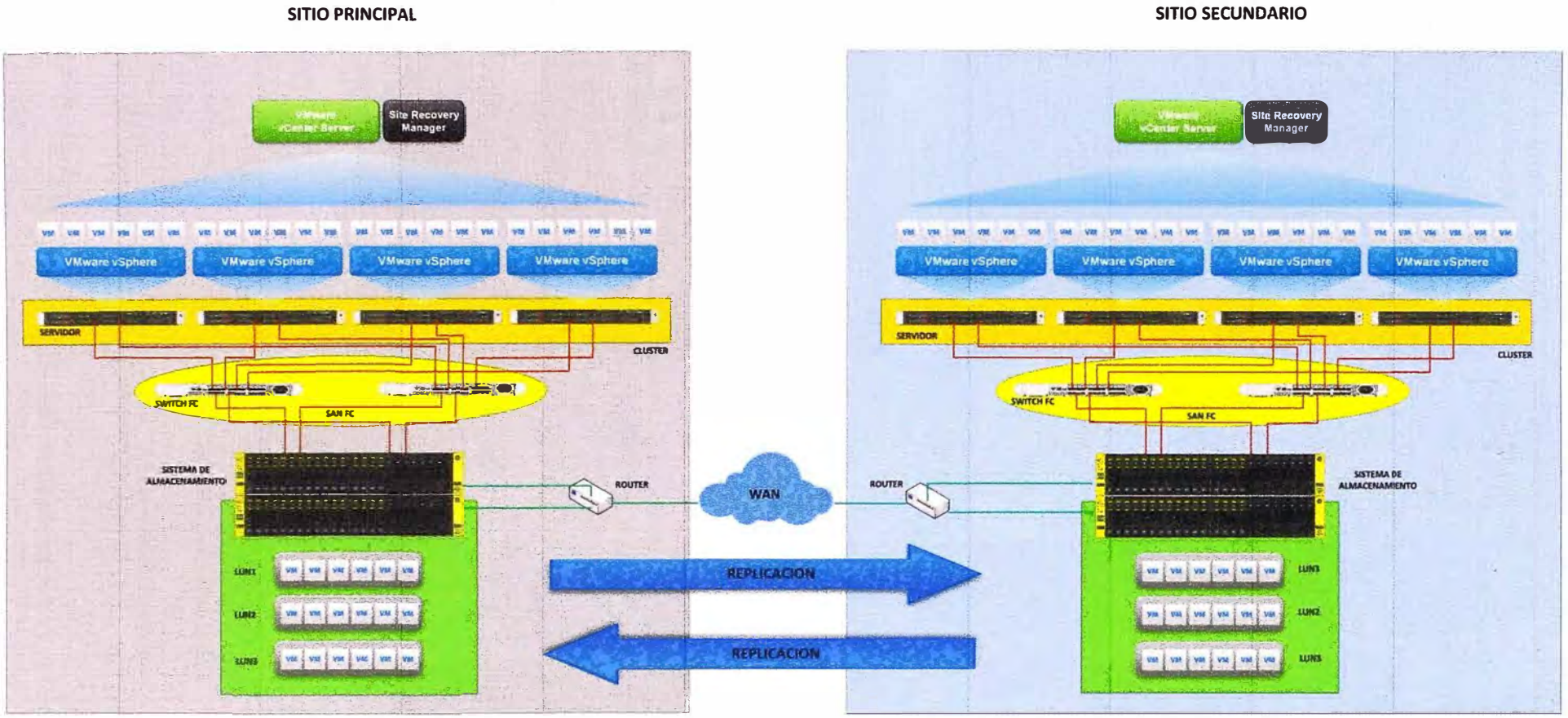


Figura 3.5 Esquema lógico de la solución propuesta

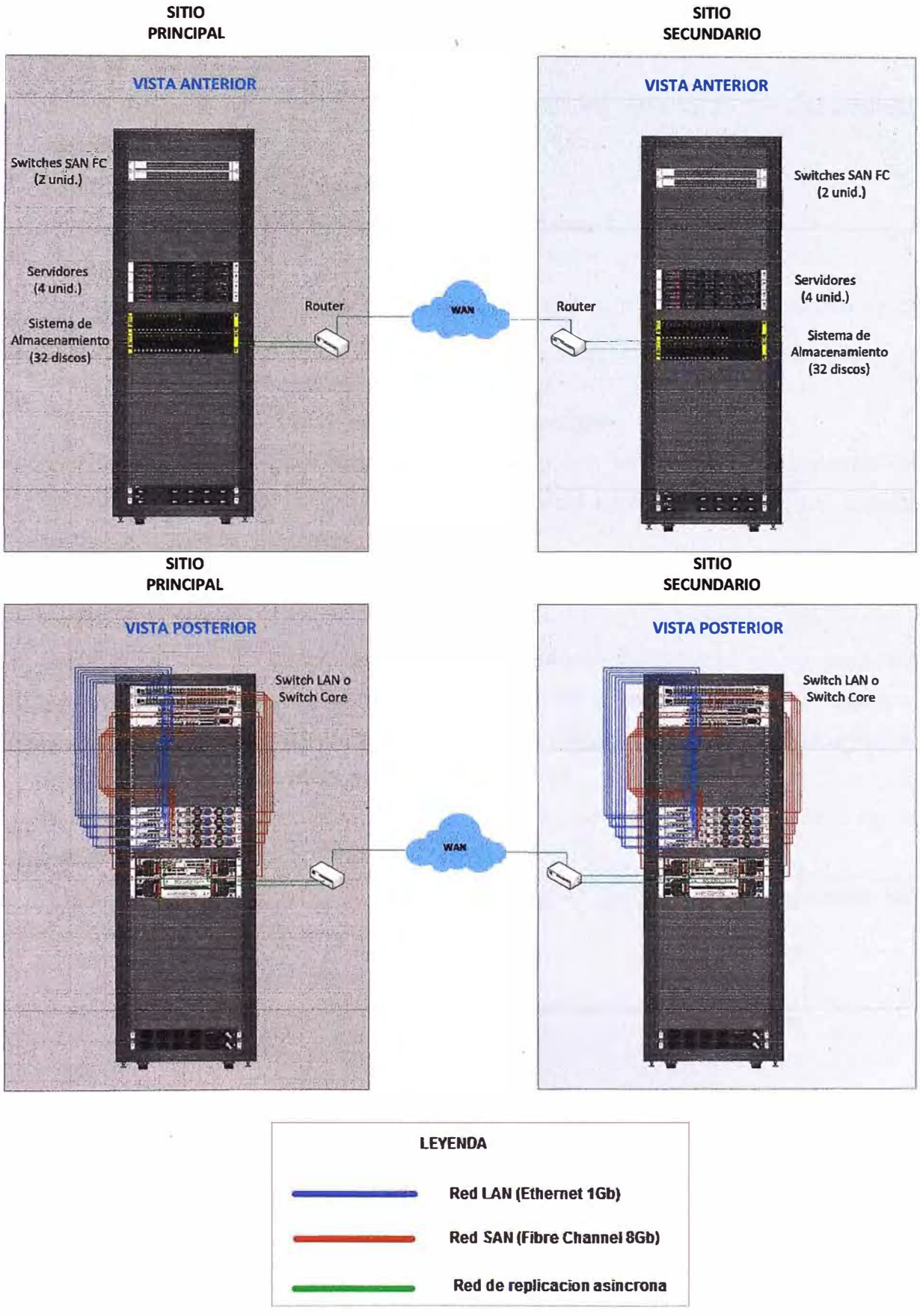


Figura 3.6 Distribución física de equipos y conectividad

3.4 Instalación de la solución

Los requerimientos para la instalación de la solución propuesta son:

- En el sitio principal

  Un (1) gabinete para montaje de equipos (servidores, sistema de almacenamiento, switches SAN).

  Dos (2) tomas eléctricas de 30A.

  Dieciséis (16) puertos Gigabit en switch core principal.

- En el sitio secundario

  Un (1) gabinete para montaje de equipos (servidores, sistema de almacenamiento, switches SAN).

  Dos (2) tomas eléctricas de 30A.

  Dieciséis (16) puertos Gigabit en switch core secundario.

- Enlace LAN o WAN para replicación asíncrona que interconecte los sistemas de almacenamiento de ambos sitios con un ancho de banda de 1Mbps (que permite transmitir 128MB de datos replicados en 18min).

  El RPO en replicación asíncrona cada 18 min seria de 128MB usando un enlace dedicado de 1Mbps.

Luego de colocar las partes en los equipos, instalarlos físicamente en los gabinetes apropiados, y realizar el cableado LAN y SAN se inician la configuración de los equipos, instalación y configuración del software de virtualización, migración de servidores físicos a máquinas virtuales y finalmente la replicación.

A continuación se presentan algunas capturas de pantalla referenciales de la instalación y configuración de la solución propuesta.

- Instalación de componentes (discos, memoria, CPU, NICs, HBA) en servidores HP ProLiant DL360p Gen8

Figura 3.7 Instalación de componentes en servidor

- Configuración de dos discos en arreglo de discos en RAID 1 en cada servidor para la instalación de hipervisor

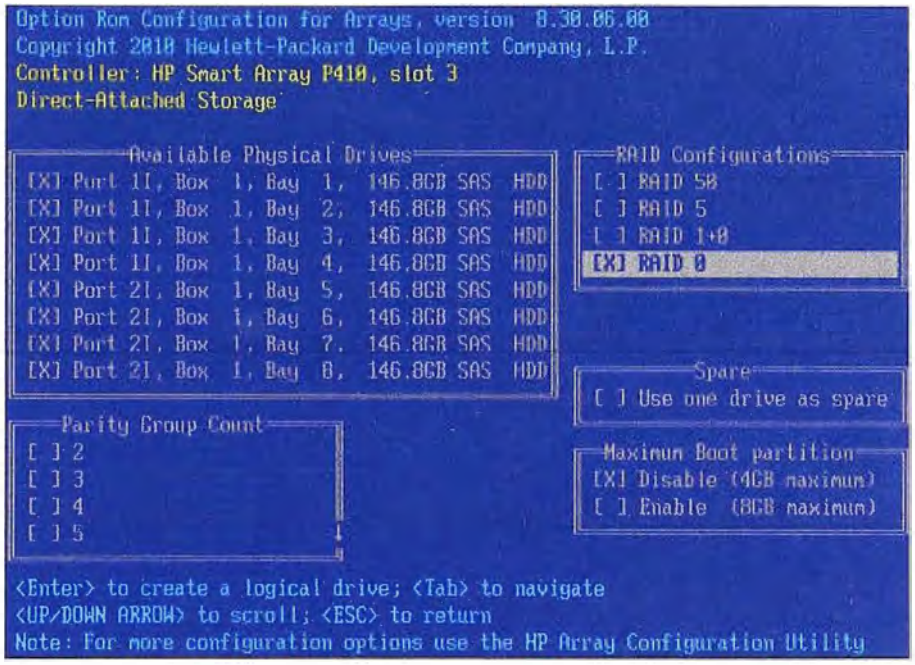


Figura 3.8 Configuración de arreglo de discos en RAID 1 en servidor

- Activación de la opción Virtualization Technology en los procesadores de los servidores.

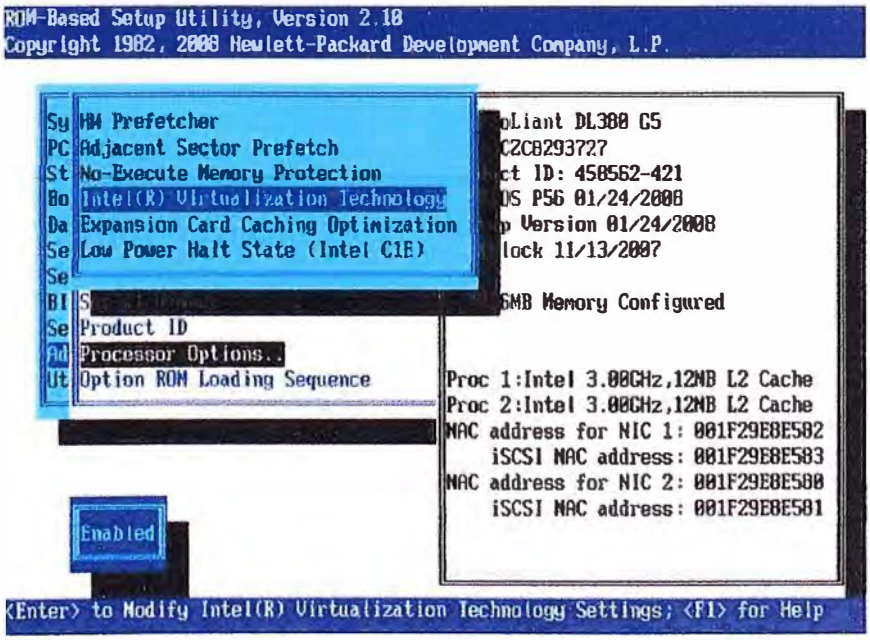


Figura 3.9 Activación de Virtualization Technology en servidores

- Instalación de sistema de almacenamiento HP 3PAR StorServ 7200

Figura 3.10 Controladores FC del sistema de almacenamiento

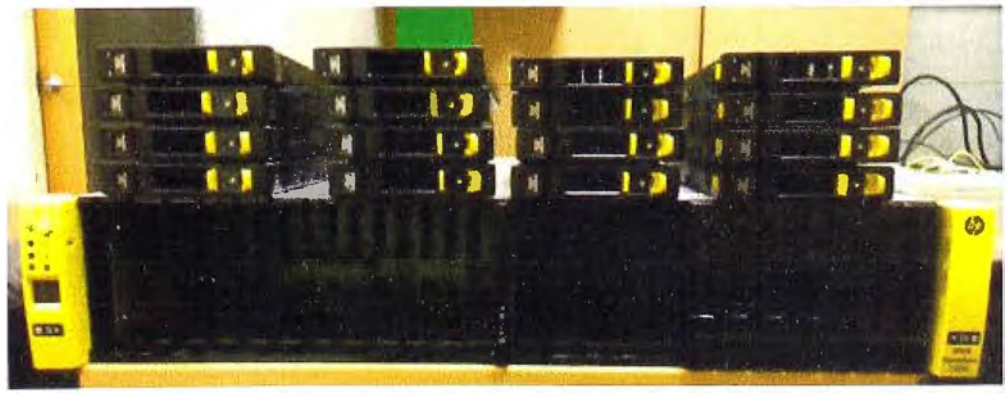


Figura 3.11 Discos SAS

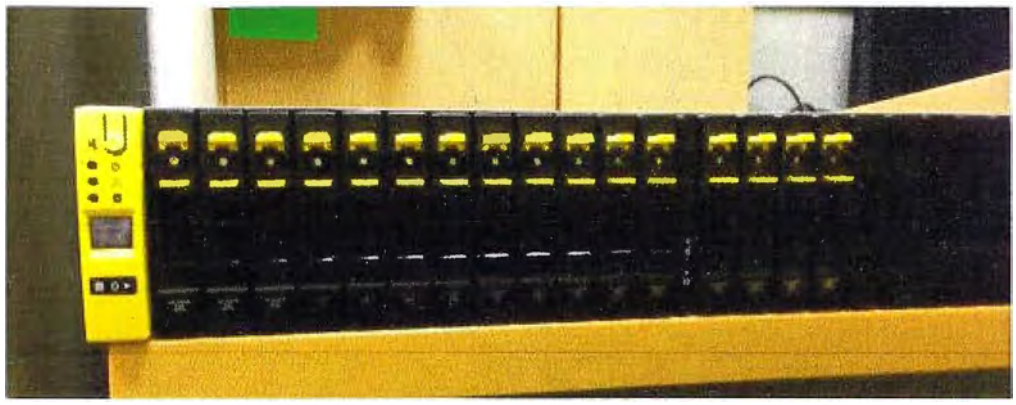


Figura 3.12 Enclosure de discos

Instalación de switches HP 8/8 SAN

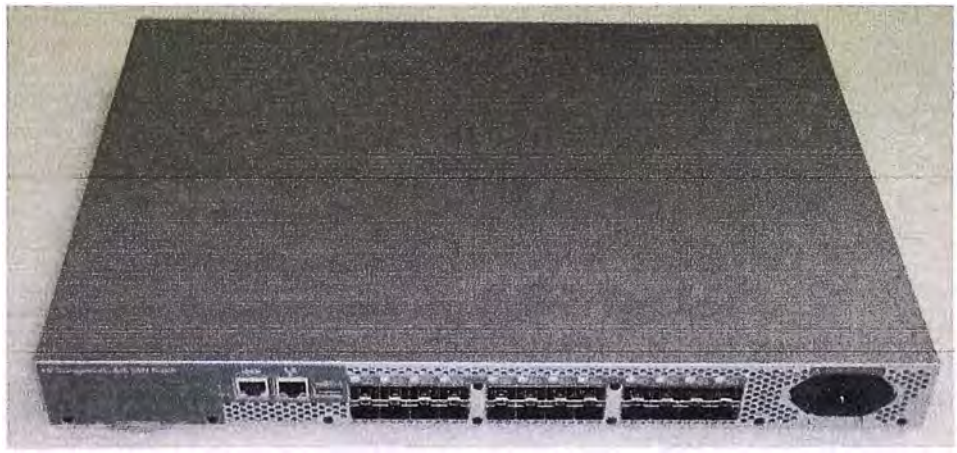


Figura 3.13 Switch HP 8/8 Base SAN

Configuración de switches SAN

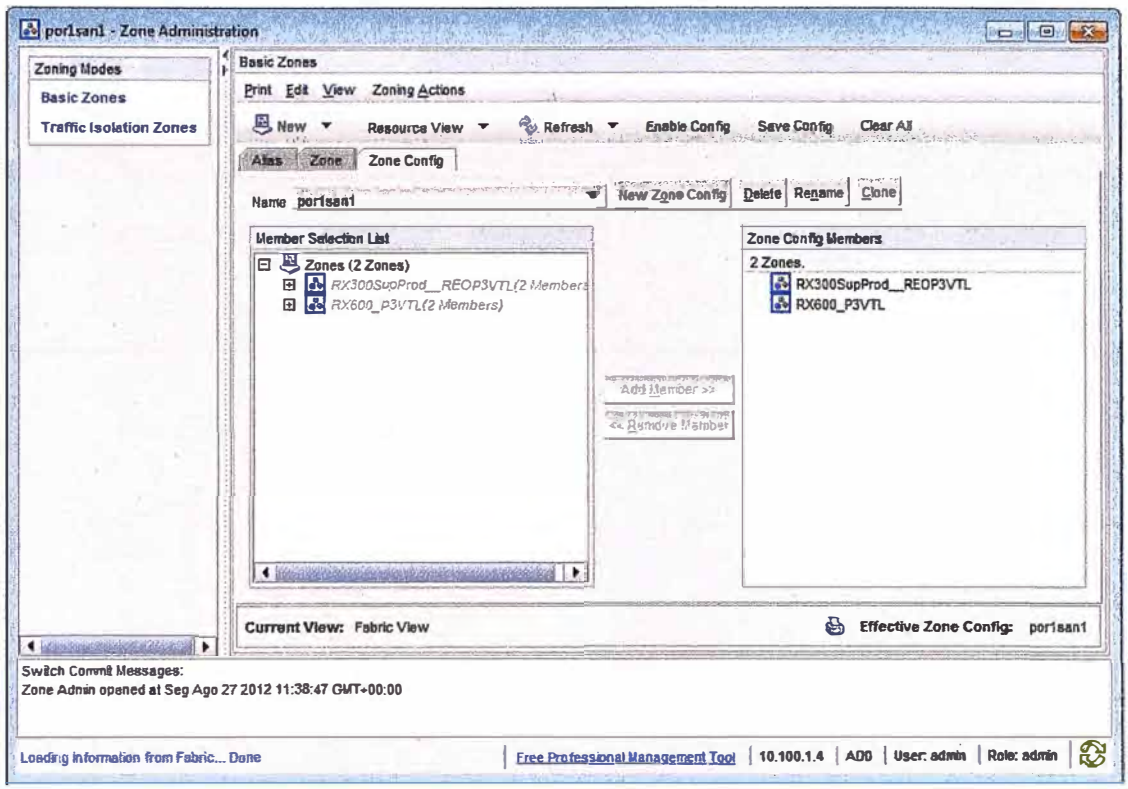


Figura 3.14 Configuración de Switch HP 8/8 Base SAN

Configuración de LUNs para los servidores

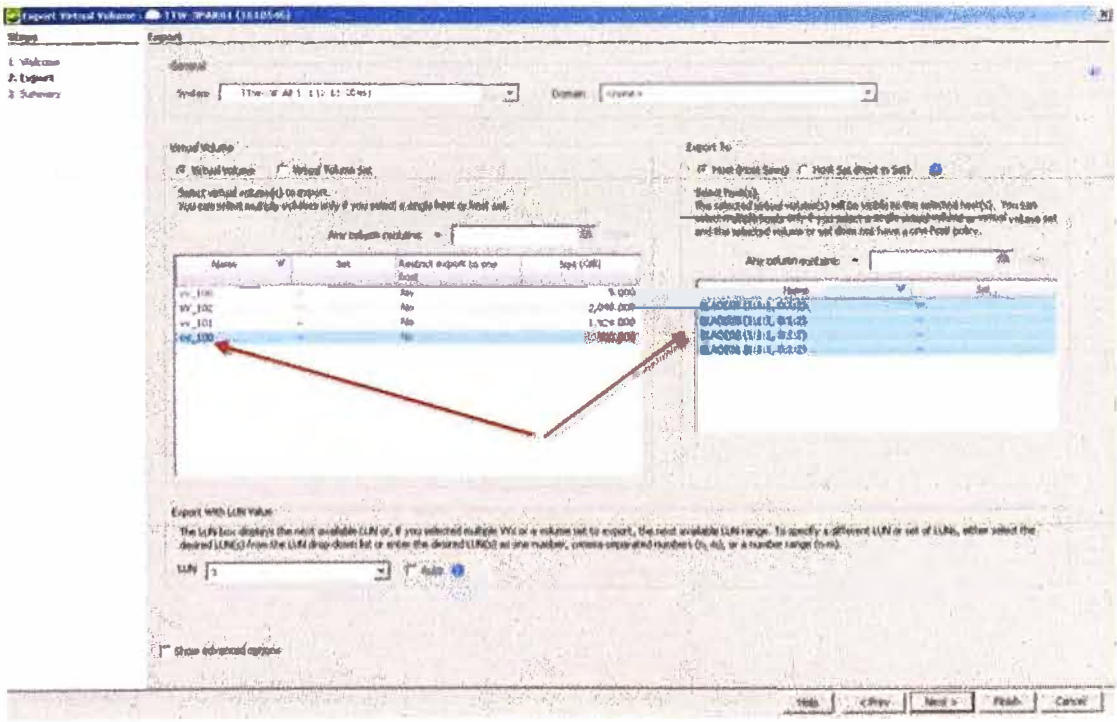


Figura 3.15 Configuración de LUNs en HP 3PAR StoreServ

Instalación y configuración de software de virtualización VMware vSphere 5

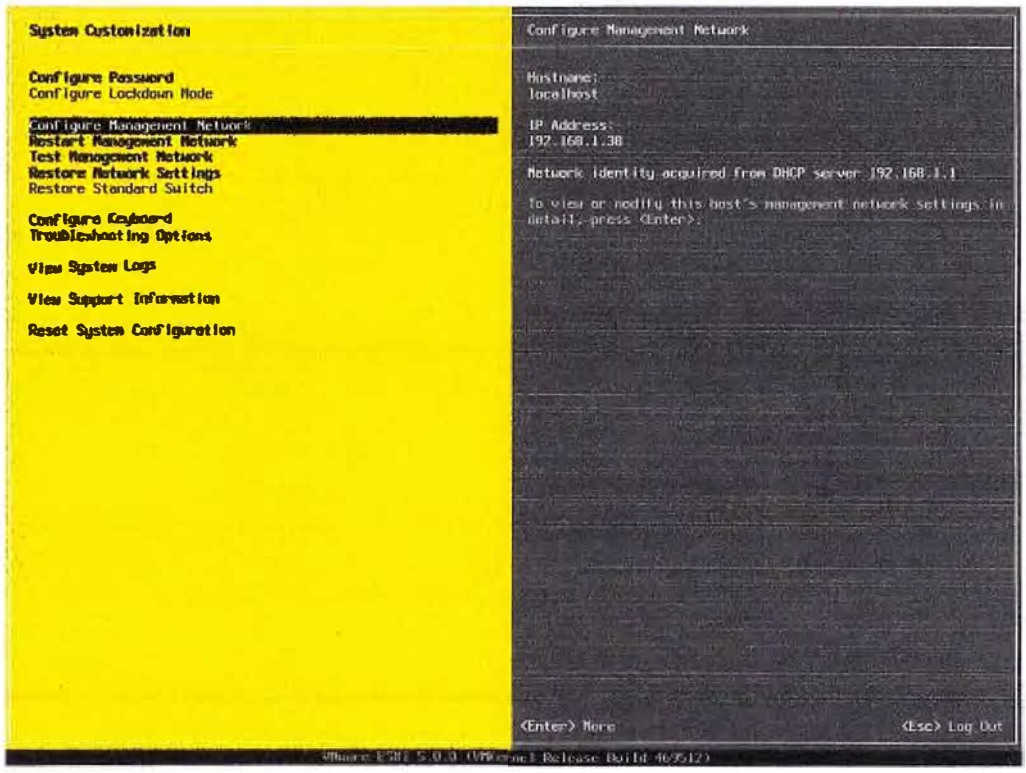


Figura 3.16 Configuración de hipervisor VMware ESXi 5

Instalación de consola de administración VMware vCenter Server 5

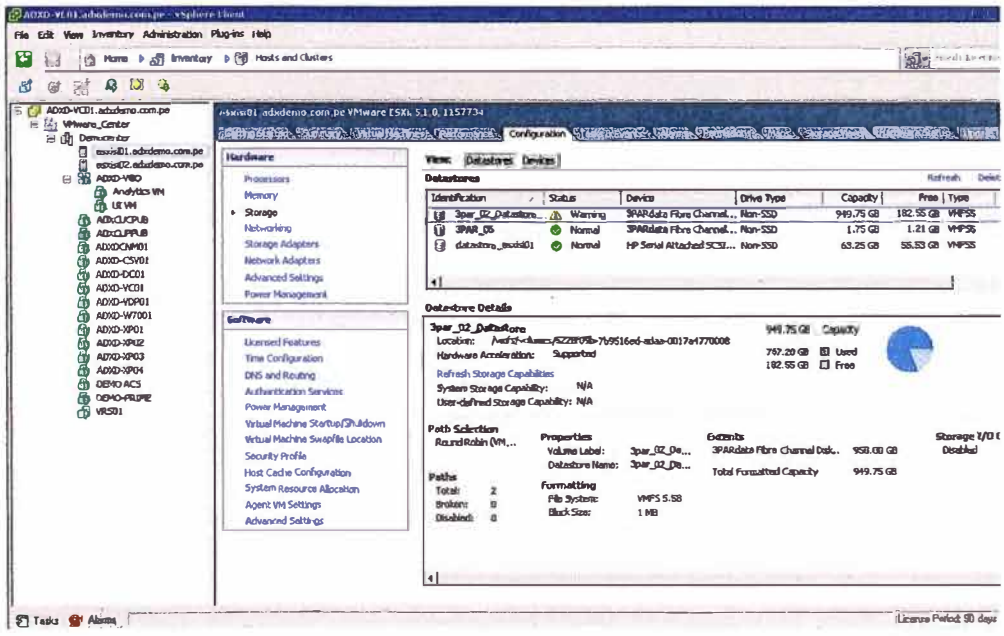


Figura 3.17 Consola de administración VMware vCenter 5 Server

Migración P2V de servidores físicos a máquinas virtuales

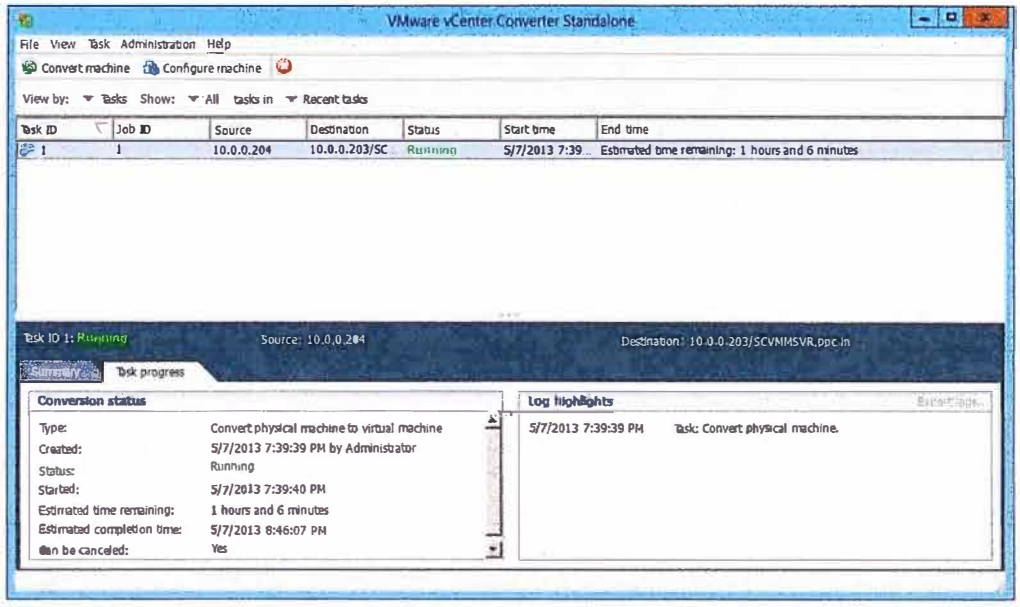


Figura 3.18 Migración P2V de servidores físicos a máquinas virtuales VMware

Configuración de replicación entre sistemas de almacenamiento HP 3PAR StoreServ 7200 de los sitios principal y secundario

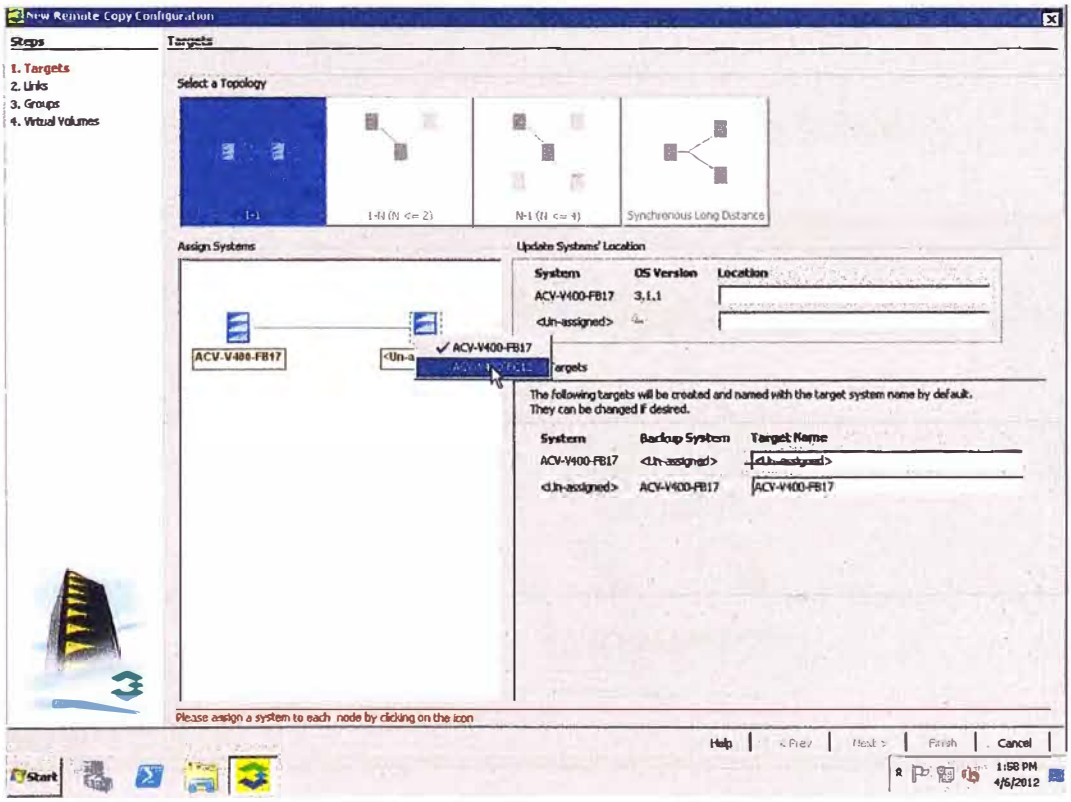


Figura 3.19 Configuración de replicación entre sistemas de almacenamiento HP 3PAR

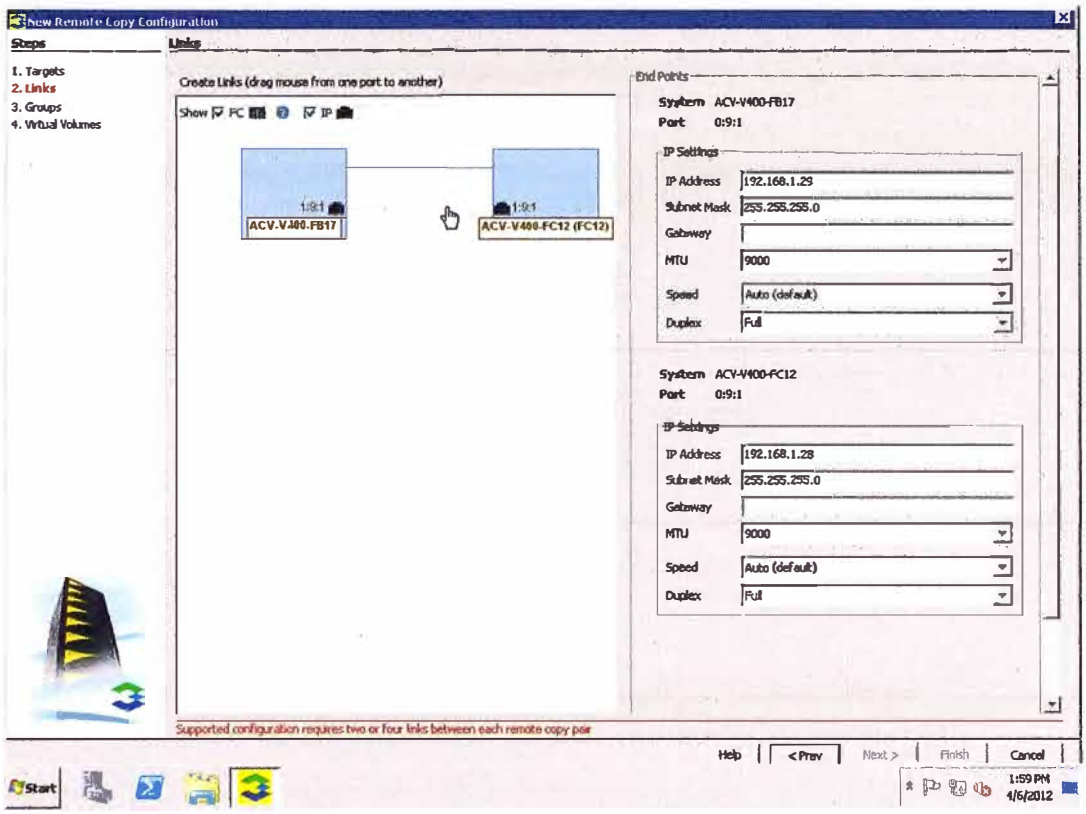


Figura 3.20 Configuración de replicación por Remote Copy de 3PAR

Instalación y configuración de VMware vCenter Site Recovery Manager

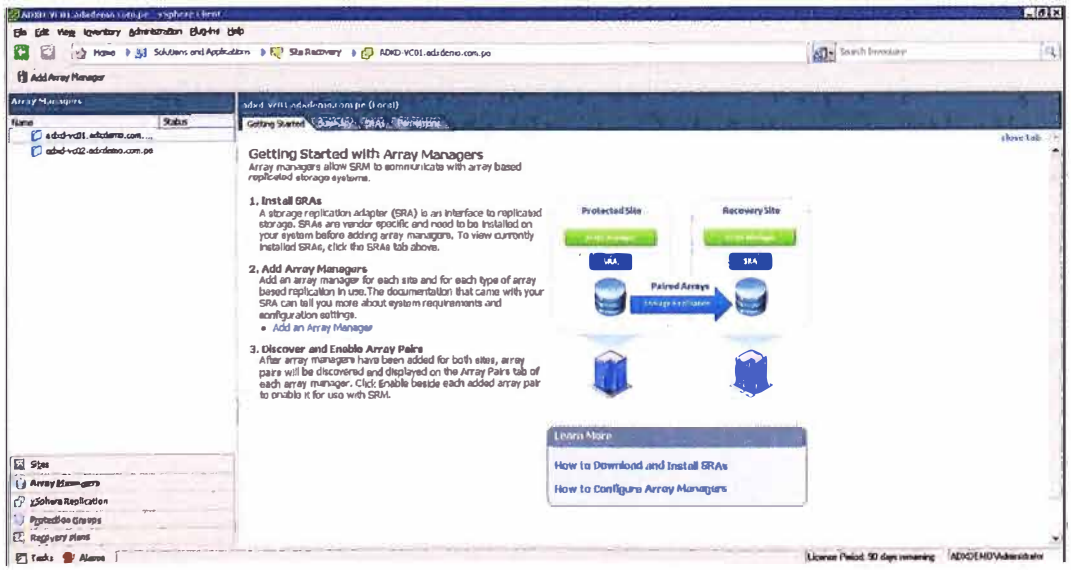


Figura 3.21 Consola VMware Site Recovery Manager

Integración de VMware vCenter Site Recovery Manager con sistemas de almacenamiento HP 3PAR StoreServ 7200

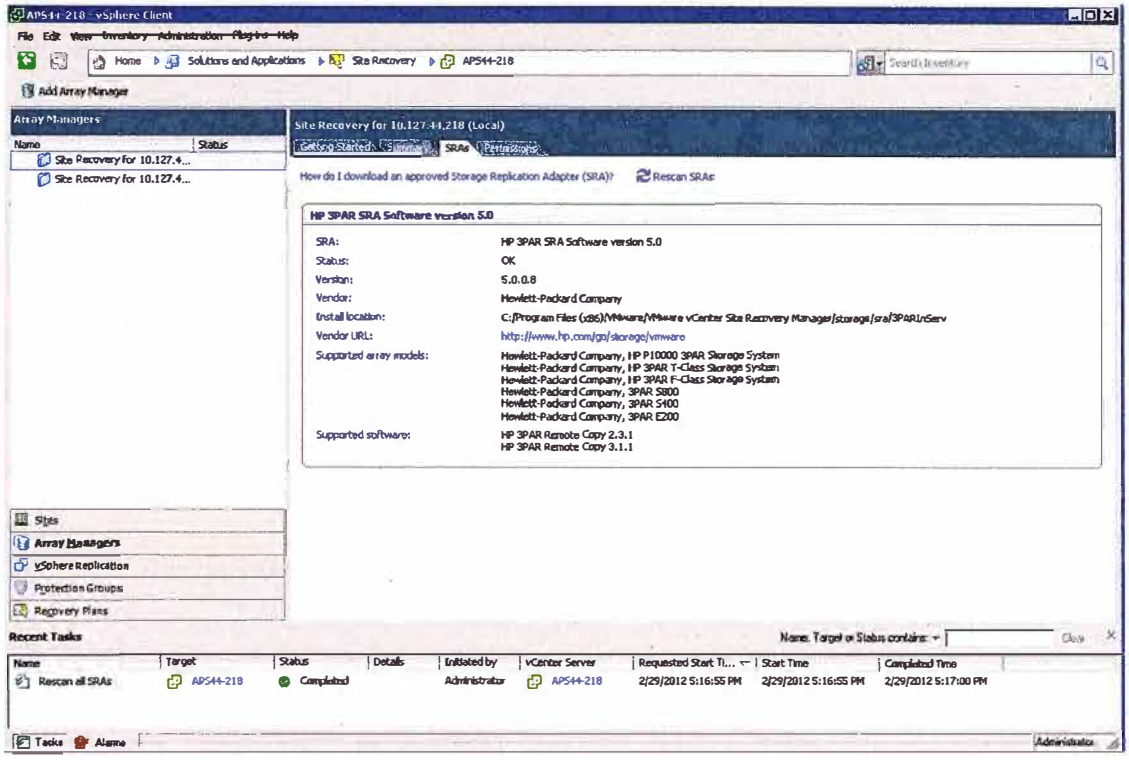


Figura 3.22 Integración de consola VMware Site Recovery Manager con sistemas de almacenamiento HP 3PAR StoreServ

Inicio de recuperación ante desastres de máquinas virtuales de sitio principal hacia sitio secundario

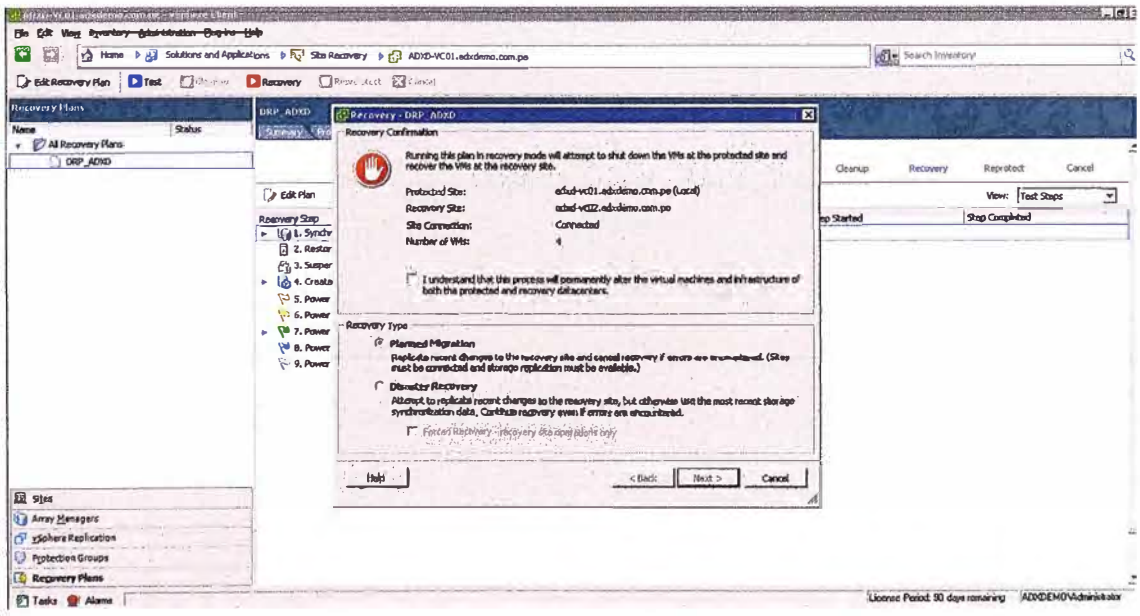


Figura 3.23 Inicio de recuperación ante desastre hacia sitio secundario

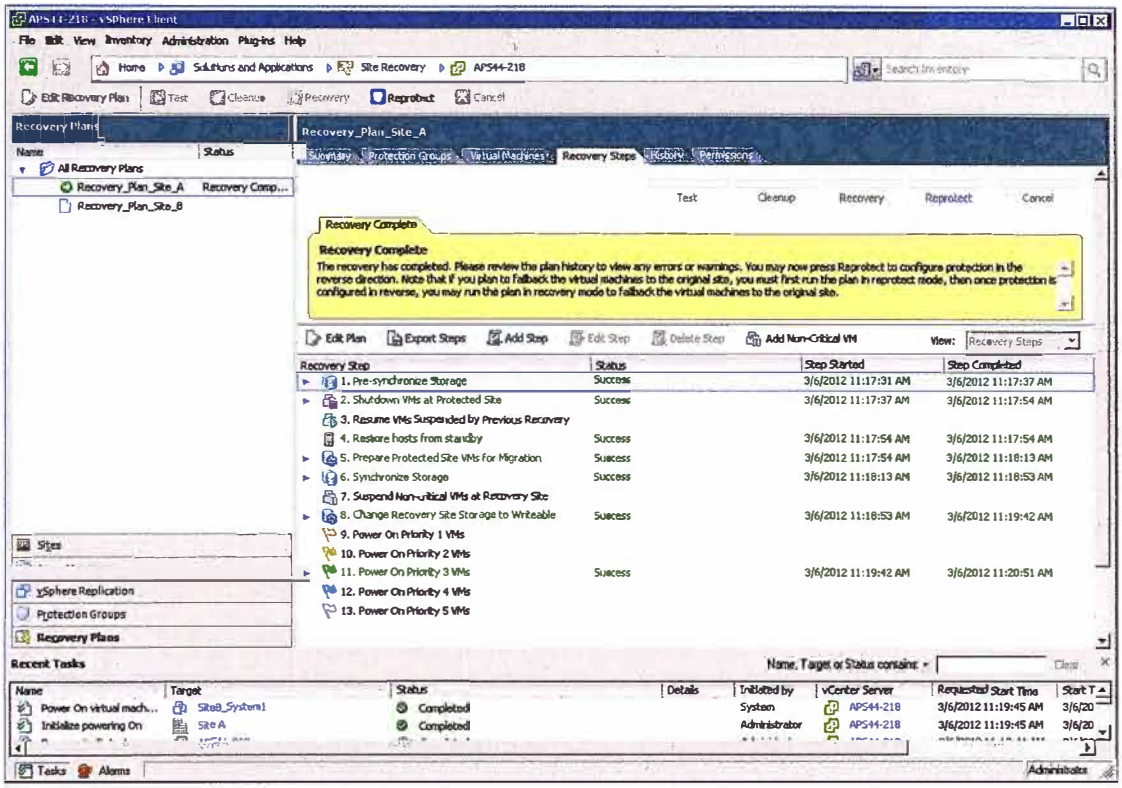


Figura 3.24 Recuperación ante desastres finalizado

CAPÍTULO IV
PRESUPUESTO Y CRONOGRAMA

En el presente capítulo se presenta el detalle del hardware y software que forman parte de la solución propuesta y así como el cronograma de implementación.

En la solución propuesta se incluye hardware como servidores x86 nuevos, switches SAN FC nuevos, sistema de almacenamiento FC y software de virtualización.

4.1 Relación de equipamiento

La solución propuesta incluye los siguientes componentes de hardware y software

a) Servidores x86 para Virtualización (4 unidades por sitio)

Se propone 8 servidores HP ProLiant DL360p Gen8, 4 por cada sitio. Cada servidor tiene las siguientes características técnicas:

- 2 CPUs de 8 cores c/u. 2.5GHz
- 56GB RAM
- 2 Discos duros 146GB SAS 15K
- 8 puertos de red 1GbE
- 2 Puertos Fibre Channel 8Gb
- 2 fuentes de poder redundante 460W
- 1 Lectora DVD RW
- Soporte Hardware HP 3años, 4 horas de tiempo de respuesta, 24x7

Tabla 3.1 Lista de componentes de servidores HP ProLiant DL360p Gen8

Cantidad	Part Number	Detalle
8	646902-001	HP DL360p Gen8 E5-2640 Base US Svr
1	HA104A3	HP 3y 4h 24x7 HW Support
8	HA104A3 7G2	HP Proliant DL36x(p) HW Support
8	745717-B21	HP DL360p Gen8 E5-2640 SDHS Kit
16	672631-B21	HP 16GB 2Rx4 PC3-12800R-11 Kit
16	647893-B21	HP 4GB 1Rx4 PC3L-10600R-9 Kit
16	652605-B21	HP 146GB 6G SAS 15K 2.5in SC ENT HDD
8	652241-B21	HP 9.5mm SATA DVD RW Jb Kit
8	647594-B21	HP Ethernet 1Gb 4-port 331T Adapter
8	AP770B	HP 82B PCIe 8Gb FC Dual Port HBA
8	656362-B21	HP 460W CS Plat PL Ht Plg Pwr Supply Kit

b) Switches SAN FC (2 unidades por sitio)

Dos switches SAN FC en redundancia por cada sitio con las siguientes características técnicas:

HP 8/8 Base SAN Switch

- 24 Puertos Fibre Channel 8Gb
- 8 Puertos Licenciados
- 8 transceiver SFP+
- 8 Cables LC/LC de 5m
- Soporte Hardware HP 3años, 4 horas de tiempo de respuesta, 24x7

Tabla 3.2 Lista de componentes de switches HP 8/8 Base SAN Switch

Cantidad	Part Number	Detalle
4	AM866B	HP 8/8 Base (0) e-port SAN Switch
4	AM866B ABA	U.S. - English localization
1	HA104A3	HP 3y 4h 24x7 HW Support
4	HA104A3 9LJ	HP B-Series 8/8 and 8/24 Switch Support
32	QK734A	HP Premier Flex LC/LC OM4 2f 5m Cbl
32	AJ716B	HP 8Gb Short Wave B-Series SFP+ 1 Pack

c) Sistemas de Almacenamiento (1 unidad por sitio)

Dos sistemas de almacenamiento HP 3PAR StoreServ 7200 de 10TB cada uno con licenciamiento para replicación síncrona o asíncrona (Tabla 3.3) con las siguientes características:

- 2 Controladores de discos
- 24GB Cache
- 32 Discos 450GB SAS 10K
- 4 Puertos Fibre Channel
- Replicación (Licenciado)
- Reportes (Licenciado)
- Soporte Hardware/Software HP Proactive 3años, 4 horas de tiempo de respuesta, 24x7

d) Software de Virtualización

Se consideran licencias VMware para todos los servidores, licencias para administración y licencias de recuperación ante desastres para máquinas virtuales (Tabla 3.4). Son necesarias las siguientes licencias:

- 16 licencias VMware vSphere Enterprise Edition. Incluye las siguientes funcionalidades licenciadas: vMotion, Storage vMotion, High Availability, Fault

Tolerance, Distributed Resources Scheduler (DRS) y Distributed Power Management (DPM)

- 2 licencias VMware vCenter Server Standard Edition
- 2 licencias de VMware vCenter Site Recovery Manager para replicación de 25 máquinas virtuales
- Soporte software VMware 3años, 24x7

Tabla 3.3 Lista de componentes de sistema de almacenamiento HP 3PAR StoreServ

Cantidad	Part Number	Detalle
2	QR482A	HP 3PAR StoreServ 7200 2-N Storage Base
32	C8R59A	HP M6710 450GB 6G SAS 10K 2.5in Encr HDD
2	QR490A	HP M6710 2.5in 2U SAS Drive Enclosure
2	HA114A1	HP Installation and Startup Service
2	HA114A1 5TP	HP Startup 3PAR 7200 2-Nd Strg Base SVC
2	HA114A1 5TV	HP Startup 3PAR 7000 2U SAS Enclosre SVC
32	C8R59A	HP M6710 450GB 6G SAS 10K 2.5in Encr HDD
2	BC745AAE	HP 3PAR 7200 OS Suite Base E-LTU
64	BC746AAE	HP 3PAR 7200 OS Suite Drive E-LTU
2	BC747AAE	HP 3PAR 7200 Replication Ste Base E-LTU
64	BC748AAE	HP 3PAR 7200 Replication Ste Drive E-LTU
2	BC767AAE	HP 3PAR 7200 Reporting Suite E-LTU
2	H1K92A3	HP 3Y 4 hr 24x7 Proactive Care SVC
2	H1K92A3 RD0	HP 3PAR 7200 OS Suite Base LTU Supp
2	H1K92A3 RD1	HP 3PAR 7200ReplicationSuiteBaseLTU Supp
2	H1K92A3 RDB	HP 3PAR 7200 Reporting Suite LTU Supp
64	H1K92A3 S6L	HP 3PAR 7200 OS Suite Drive LTU Supp
64	H1K92A3 S6M	HP 3PAR 7200 Replic Suite Drive LTU Supp
64	H1K92A3 WUS	HP 3PAR 7000 Drives under 1TB Support
2	H1K92A3 WUW	HP 3PAR 7000 Drive Enclosure Support
2	H1K92A3 WVB	HP 3PAR 7200 2-node Storage Base Supp
2	HA124A1	HP Technical Installation Startup SVC
2	HA124A1 5TM	HP Startup 3PAR 7000 Reporting Ste SVC

Tabla 3.4 Lista de licencias VMware

Cantidad	Part Number	Detalle
16	VS5-ENT-C	VMware vSphere 5 Enterprise for 1 processor
16	VS5-ENT-3P-SSS-C	Production Support/Subscription for VMware vSphere 5 Enterprise for 1 processor for 3 years
2	VCS5-STD-C	VMware vCenter Server 5 Standard for vSphere 5 (Per Instance)
2	VCS5-STD-3P-SSS-C	Production Support/Subscription for vCenter Server 5 Standard for vSphere 5 for 3 years
2	VC-SRM5-25S-C	VMware vCenter Site Recovery Manager 5 Standard (25 VM Pack)
2	VC-SRM5-25S-3P-SSS-C	Production Support/Subscription for VMware vCenter Site Recovery Manager 5 Standard (25 VM Pack) for 3 years

4.2 Estimación de costos

Los costos de hardware, software, soporte 24x7, garantía 3 años y servicios de implementación son los siguientes:

Tabla 3.5 Lista de precios aproximados

Cantidad	Part Number	Detalle	Costo Aproximado (USD)
8	646902-001	HP DL360p Gen8 E5-2640 Base US Svr	$80,000.00
1	HA104A3	HP 3y 4h 24x7 HW Support	
8	HA104A3 7G2	HP Proliant DL36x(p) HW Support	
8	745717-B21	HP DL360p Gen8 E5-2640 SDHS Kit	
16	672631-B21	HP 16GB 2Rx4 PC3-12800R-11 Kit	
16	647893-B21	HP 4GB 1Rx4 PC3L-10600R-9 Kit	
16	652605-B21	HP 146GB 6G SAS 15K 2.5in SC ENT HDD	
8	652241-B21	HP 9.5mm SATA DVD RW Jb Kit	
8	647594-B21	HP Ethernet 1Gb 4-port 331T Adapter	
8	AP770B	HP 82B PCIe 8Gb FC Dual Port HBA	
8	656362-B21	HP 460W CS Plat PL Ht Plg Pwr Supply Kit	
4	AM866B	HP 8/8 Base (0) e-port SAN Switch	$30,000.00
4	AM866B ABA	U.S. - English localization	
1	HA104A3	HP 3y 4h 24x7 HW Support	
4	HA104A3 9LJ	HP B-Series 8/8 and 8/24 Switch Support	
32	QK734A	HP Premier Flex LC/LC OM4 2f 5m Cbl	
32	AJ716B	HP 8Gb Short Wave B-Series SFP+ 1 Pack	
2	QR482A	HP 3PAR StoreServ 7200 2-N Storage Base	$70,000.00
32	C8R59A	HP M6710 450GB 6G SAS 10K 2.5in Encr HDD	
2	QR490A	HP M6710 2.5in 2U SAS Drive Enclosure	
2	HA114A1	HP Installation and Startup Service	
2	HA114A1 5TP	HP Startup 3PAR 7200 2-Nd Strg Base SVC	
2	HA114A1 5TV	HP Startup 3PAR 7000 2U SAS Enclosre SVC	
32	C8R59A	HP M6710 450GB 6G SAS 10K 2.5in Encr HDD	
2	BC745AAE	HP 3PAR 7200 OS Suite Base E-LTU	
64	BC746AAE	HP 3PAR 7200 OS Suite Drive E-LTU	
2	BC747AAE	HP 3PAR 7200 Replication Ste Base E-LTU	
64	BC748AAE	HP 3PAR 7200 Replication Ste Drive E-LTU	
2	BC767AAE	HP 3PAR 7200 Reporting Suite E-LTU	
2	H1K92A3	HP 3Y 4 hr 24x7 Proactive Care SVC	
2	H1K92A3 RD0	HP 3PAR 7200 OS Suite Base LTU Supp	
2	H1K92A3 RD1	HP 3PAR 7200ReplicationSuiteBaseLTU Supp	
2	H1K92A3 RDB	HP 3PAR 7200 Reporting Suite LTU Supp	
64	H1K92A3 S6L	HP 3PAR 7200 OS Suite Drive LTU Supp	
64	H1K92A3 S6M	HP 3PAR 7200 Replic Suite Drive LTU Supp	
64	H1K92A3 WUS	HP 3PAR 7000 Drives under 1TB Support	
2	H1K92A3 WUW	HP 3PAR 7000 Drive Enclosure Support	
2	H1K92A3 WVB	HP 3PAR 7200 2-node Storage Base Supp	
2	HA124A1	HP Technical Installation Startup SVC	
2	HA124A1 5TM	HP Startup 3PAR 7000 Reporting Ste SVC	
16	VS5-ENT-C	VMware vSphere 5 Enterprise for 1 processor	$100,000.00
16	VS5-ENT-3P-SSS-C	Production Support/Subscription for VMware vSphere 5 Enterprise for 1 processor for 3 years	
2	VCS5-STD-C	VMware vCenter Server 5 Standard for vSphere 5 (Per Instance)	
2	VCS5-STD-3P-SSS-C	Production Support/Subscription for vCenter Server 5 Standard for vSphere 5 for 3 years	
2	VC-SRM5-25S-C	VMware vCenter Site Recovery Manager 5 Standard (25 VM Pack)	
2	VC-SRM5-25S-3P-SSS-C	Production Support/Subscription for VMware vCenter Site Recovery Manager 5 Standard (25 VM Pack) for 3 years	
1	SERV. PROFESIONALES	Implementación de la solución	$15,000.00

La inversión total asciende aproximadamente a $ 295,000.00

4.3 Cronograma

El resumen de actividades

Tabla 3.6 Lista de actividades

ACTIVIDADES	DIA 1	DIA 2	DIA 3	DIA 4	DIA 5	DIA 6	DIA 7	DIA 8	DIA 9	DIA 10	DIA 11
Instalación y puesta en marcha de 8 servidores HP DL360 *Gen8*	x										
Instalación de partes en servidores (Procesador, memorias, discos, tarjetas NIC, tarjetas HBA)											
Instalación de servidores y accesorios en rack standard											
Actualización de firmware											
Configuración de arreglos de discos											
Conexión de patch cords hacia switch core											
Instalación y puesta en marcha de 2 sistemas de almacenamiento HP 3PAR 7200		x									
Instalación de controlador de discos											
Instalación de enclosure de discos											
Configuración de módulo de administración											
Creación y presentación de LUNs para 4 servidores											
Instalación y puesta en marcha de 4 switches SAN			x								
Instalación de switches											
Conexión de cables de fibra hacia servidores y sistema de almacenamiento											
Configuración de zonas											
Instalación y configuración VMware vSphere 5			x								
Instalación y configuración de hipervisor VMware ESXi 5 sobre 8 servidores											
Creación de 2 máquinas virtuales para administración (una por sitio)											
Instalación de sistema operativo sobre 2 máquinas virtuales de administración (una por sitio)											
Instalación y configuración de 2 consolas de administración VMware vCenter 5 (una por sitio)											
Configuration de Cluster, vMotion, High Availability, DRS y DPM en 2 sitios											
Pruebas de funcionalidades y puesta en producción											
Migración P2V											
Migración por conversión P2V de 20 servidores físicos hacia Infraestructura Virtual. Afinamiento de VMs convertidas				x	x	x	x	x			
Configuración de replicacion									x		
Configuración de Remote Copy vía RCIP											
Instalación y configuración VMware vCenter Site Recovery Manager 5									x	x	x
Instalación de SRM en 2 sitios											
Instalación de SRA de 3PAR en 2 sitios											
Conexión de SRM entre 2 sitios											
Configuración de Protection Groups para todas las máquinas virtuales											
Configuración de Recovery Plans											
Pruebas de funcionamiento de failover y failback y puesta en producción											

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La virtualización de servidores x86 permite reducir significativamente la inversión en nuevo equipamiento mediante la consolidación de varias máquinas virtuales en un solo servidor físico. Con la virtualización se aprovecha de manera más eficiente el uso de recursos de CPU y memoria del servidor físico.
2. La virtualización permite ahorrar costos de consumo de energía y enfriamiento. Al tener menor número de servidores encendidos, menor es el consumo de energía y menores son los requerimientos de enfriamiento en el centro de datos.
3. La virtualización permite independizar las máquinas virtuales unas de otras. Las máquinas virtuales ya no están atadas al servidor físico, esto permite la movilidad de las máquinas virtuales. Las máquinas virtuales pueden ejecutarse en cualquier servidor físico.
4. La virtualización permite tener alta disponibilidad de máquinas virtuales. Si se produce una falla de hardware en un host del clúster, las máquinas virtuales que se ejecutaban en él serán reiniciadas automáticamente en los hosts restantes del clúster. Esto permite reducir los tiempos de inactividad por fallas de hardware.
5. La virtualización permite escalabilidad tanto en servidores como en almacenamiento sin necesidad de apagar máquinas virtuales de producción. Si se necesita agregar más hosts o más almacenamiento, no se necesita apagar ninguna máquina virtual.
6. La virtualización también permite simplificar las tareas de recuperación ante desastres ya que se aprovechan las tecnologías de replicación de los sistemas de almacenamiento para replicar grupos de máquinas virtuales hacia un sitio secundario.
7. Con la virtualización de servidores, la replicación basada en almacenamiento y su integración con la automatización de la recuperación ante desastres que ofrece VMware vCenter Site Recovery Manager, los RTO y RPO se reducen a tiempo de reinicios de máquinas virtuales (RTO) y ancho de banda para replicación para transferir datos (RPO).

Recomendaciones

1. En el presente informe se presenta una solución basada en virtualización de servidores y replicación de sistemas de almacenamiento como tecnologías que permiten reducir costos y proteger la información ante un desastre. Es importante también considerar como parte de una solución total de Continuidad de Negocio la implementación de redes, acceso a internet, firewalls, VPNs y seguridad en el sitio secundario.

2. Para completar la solución de recuperación ante desastres es recomendable el uso de backup en cintas. Este permitirá la recuperación granular de archivos o datos estructurados como bases de datos y a la vez retener información histórica. La recuperación ante desastres no es una solución de backup de información sino una solución que permite la restauración de las operaciones de los sistemas.

3. Es importante también considerar en el sitio secundario infraestructura que permita a los usuarios trabajar de manera temporal. Una de las opciones es virtualización de escritorios y/o virtualización de aplicaciones las cuales permiten a los usuarios acceder desde cualquier parte y desde cualquier dispositivo a sus escritorios y aplicaciones alojadas en el sitio secundario de manera remota incluso sin necesidad de VPNs ya que estas tecnologías ya encriptan la información.

4. Es importante el dimensionamiento de un enlace para la replicación de la información. El ancho de banda asignado para la replicación asíncrona afectara en el RPO de la información. A menor ancho de banda mayor será la información que se pierda. Implementaciones de replicación asíncrona son comunes a distancias superiores a los 200 Km.

5. Para distancias menores a 200 Km es posible implementar replicación síncrona. Esto permitirá un RPO cercano a cero, es decir, sin pérdida de información.

ANEXO A
GLOSARIO DE TÉRMINOS

Activo-activo
Es una arquitectura diseñada para una alta disponibilidad en la que todos los componentes están activos y disponibles para llevar a cabo una tarea si otro componente falla.

Activo-pasivo
Es una arquitectura diseñada para una alta disponibilidad en la que los componentes redundantes están inactivos y están a la espera de realizar una tarea si un componente activo falla.

Alta disponibilidad
Asegura que no se pierdan datos en caso de desastre en el origen

Aplicación
Un programa de computadora que proporciona la lógica para las operaciones de computación.

Application Specific Integrated Circuit (ASIC)
Un circuito integrado diseñado para realizar una función específica.

Archivado
Permite almacenar información de contenido fijo en un repositorio para retención a largo plazo.

Arreglo / arreglo de discos / arreglo de almacenamiento
Un grupo de unidades de disco duro que trabajan juntos como una unidad.

Buffer
Área de almacenamiento temporal, por lo general en la RAM.

Cache
Es una memoria semiconductora donde los datos se colocan temporalmente para reducir el tiempo necesario para atender las solicitudes de I/O desde el host.

Centro de Datos
Proporciona capacidades de procesamiento de datos centralizada para las empresas. Sus elementos principales son las aplicaciones, bases de datos, sistemas operativos, redes y almacenamiento.

Continuidad de negocio (BC)
Es la preparación, respuesta y recuperación ante una interrupción que pueden afectar negativamente las operaciones del negocio.

Controlador RAID
Hardware especializado que realiza todos los cálculos RAID y presenta volúmenes de disco al host

Datos estructurados
Datos que pueden ser organizadas en filas y columnas, y por lo general se almacenan en una base de datos u hoja de cálculo.

Datos no estructurados
Datos que no tienen estructura inherente y por lo general se almacenan como diferentes tipos de archivos.

Destino
Un dispositivo SCSI que ejecuta un comando para llevar a cabo la tarea recibida desde un iniciator SCSI.

Director (Switch)
Clase de dispositivo de interconexión que posee un gran número de puertos y componentes redundantes para requerimientos de de conectividad de clase empresarial

Failback
Es una operación que permite la reanudación de las operaciones normales del negocio en el sitio de origen. El failback se invoca después del failover iniciado.

Failover
Cambio automático de una función hacia un componente redundante en caso de fallo de un componente activo.

Fibre Channel (FC)
Es una interconexión que soporta múltiples protocolos y topologías. Los datos se transfieren en serie en una variedad de enlaces de cobre u ópticos a alta velocidad.

Hipervisor
Es una plataforma de virtualización que permite que múltiples sistemas operativos se ejecuten simultáneamente en un host físico. El hipervisor es responsable de interactuar directamente con los recursos físicos del host.

Host o Servidor
Una plataforma de cómputo que ejecuta aplicaciones y bases de datos.

Hot spare
Una unidad de disco inactivo que reemplaza una unidad que ha fallado en un grupo RAID protegido.

Internet Small Computer System Interface Protocol (iSCSI)
Protocolo basado en IP construido sobre SCSI. Transporta los datos a nivel de bloque sobre redes IP tradicionales.

Máquina virtual (VM)
Una imagen de software de un equipo que se comporta como una máquina física. Se presenta a la red como si fuera una máquina física. Se pueden ejecutar varias máquinas virtuales en una misma máquina física.

National Institute of Standards and Technology (NIST)
Una agencia federal no reguladora dentro de U.S. Commerce Department's Technology Administration. La misión de NIST es desarrollar y promover la medición, los estándares y la tecnología para mejorar la productividad, facilitar el comercio y mejorar la calidad de vida.

Online Transaction Processing (OLTP)
Un sistema que procesa las transacciones en el instante en que el equipo los recibe y actualiza los archivos principales inmediatamente.

P2V (Physical to Virtual)
Es la migración de servidores físicos a máquinas virtuales.

Paridad
Una construcción matemática que permite la re-creación de un segmento de datos faltante.

Partición
Una división lógica de la capacidad de un disco físico o lógico.

Peripheral Component Interconnect (PCI)
Un bus estándar para la conexión de dispositivos de I/O en un ordenador personal.

Plan de Recuperación de Desastres (DRP)
Un plan para hacer frente a la pérdida inesperada o repentina de acceso a los datos con un enfoque a la protección de los datos. Forma parte de la planificación de la continuidad del negocio.

Protocolo
Un conjunto de reglas o normas que permite la comunicación entre sistemas o dispositivos.

Proveedor de servicios de nube
Es una persona, organización o entidad responsable de mantener un servicio siempre disponible para los consumidores de la nube.

Random Access Memory (RAM)
Memoria volátil que permite el acceso directo a cualquier posición de la memoria .

Recuperación de desastres
Son un conjunto procesos, políticas y procedimientos para restaurar las operaciones críticas para la reanudación del negocio, incluyendo la recuperación del acceso a los datos.

Red de área de almacenamiento (SAN)
Una red dedicada de alta velocidad de servidores y dispositivos de almacenamiento compartido.

Redundancia
Es la inclusión de componentes adicionales (por ejemplo, unidad de disco, HBA, un enlace o datos) que permite un funcionamiento continuo si cualquiera de los componentes de trabajo falla.

Redundant Array of Independent Disks (RAID)
Es la inclusión de un conjunto de múltiples unidades de disco independientes en un arreglo de unidades de discos, el cual presenta un rendimiento superior a la de un único disco grande más costoso.

Small Computer System Interface (SCSI)
Una interfaz de almacenamiento popular usada para conectar un dispositivo periférico a

un ordenador y transferir datos entre ellos.

Snapshot
Es una copia del archivo de disco (.vmdk) de una máquina virtual en un punto dado en el tiempo. Los snapshots proporcionan un registro de cambios para el disco virtual y se utilizan para restaurar una máquina virtual a un punto determinado en el tiempo cuando se produce un error de fallo o sistema.

Solid-State Drive (SSD) / Flash drive
Un dispositivo de almacenamiento de datos que utiliza memoria de estado sólido para almacenar datos de manera persistente.

Strip
Un grupo de bloques direccionables contiguos dentro de cada disco de un conjunto de discos en RAID.

Stripe
Un conjunto de strips alineados que se extiende por todos los discos en un conjunto de discos en RAID.

Striping
Es la división y la distribución de datos a través de múltiples unidades de disco.

Switches
Dispositivos más inteligentes que los hubs, los switches conmutan directamente los datos de un puerto físico a otro.

Tarjeta de interfaz de red (NIC)
Hardware de computadora diseñada para que las computadoras se comuniquen a través de una red IP.

Topología puente
Una topología que proporciona conectividad entre la red FC y la red IP.

Tolerancia a fallos
Describe a un sistema o componente diseñado de tal manera que si se produce un falla, un componente de respaldo o procedimiento puede tomar su lugar inmediatamente sin pérdida de servicio.

Trama
Es un flujo de datos que se ha codificado por una capa de enlace de datos para la transmisión digital a través de un enlace de nodo a nodo.

Unidad de disco
Un dispositivo de almacenamiento no volátil que almacena datos mediante rotación rápida de discos con superficies magnéticas.

BIBLIOGRAFÍA

1. VMware, "Virtualization Overview" - VMware Inc. - USA, 2006
2. VMware, "VMware Virtual Networking Concepts" - VMware Inc. - USA, 2006
3. VMware, "VMware vSphere: Install, Configure, Manage V5.0", VMware, Inc. - USA, 2012
4. VMware, "VMware vSphere 5 Building a Virtual Datacenter", VMware, Inc. - USA, 2013
5. Forbes Guthrie and Scott Lowe," VMware vSphere Design", John Wiley & Sons, Inc. - USA 2013
6. Ulf Troppens, Rainer Erkens, Wolfgang Muller, "Storage Networks Explained", John Wiley & Sons, Inc. - Germany, 2004
7. EMC Corporation, "EMC Unified Storage System Fundamentals for Performance and Availability" - EMC Corporation - USA, 2011
8. Gartner, "Magic Quadrant for x86 Server Virtualization Infrastructure", Gartner, Inc. - USA 2013
9. VMware, "VMware vCenter Converter Standalone 5.0 User's Guide" - VMware Inc. - USA, 2013
10. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, - USA, 2011