Universidad de las Ciencias Informáticas

Título: Propuesta de Implementación del Centro de Resguardo de Datos de 5ta B.

Trabajo de Diploma para optar por el título de

Ingeniero en Ciencias Informáticas

Autores:

Yamir Acosta Lozada

Román Gilberto Álvarez Sutrimina

Tutor:

Deivis Leyva Velázquez

Ciudad de la Habana, 12 de Junio de 2009

"En la capacidad nuestra y de nuestros hijos está la posibilidad de adquirir en el futuro una capacidad técnica que nos permita figurar entre los países desarrollados del mundo."

Ché

Datos de contacto

Tte. Ingeniero en Ciencias Informáticas Deivis Leyva Velázquez:

Ingeniero en Ciencias Informáticas, graduado de la Universidad de las Ciencias Informáticas curso 2007-2008. Se ha capacitado como Arquitecto de Software en la tecnología J2EE y .NET. Actualmente se desempeña como Ingeniero en Sistemas de la Dirección de Informática y Comunicaciones, donde se especializa en tecnologías Oracle y Sistemas Operativos.

Agradecimientos

De Yamir:

A la Revolución y a Fidel por darnos la oportunidad de estudiar en esta Universidad.

A mis padres por darme confianza y seguridad a lo largo de mi vida. Millón de gracias para ustedes.

A mi hermano Vladimir por ser ese ejemplo a seguir desde que era un muchacho, gracias por ser ese modelo para mí.

A mi sobrinita Jessie Aimeé por ser tan cariñosa conmigo y quererme mucho.

A mi familia por darme ese apoyo que necesita cualquier futuro profesional.

A mi querida Tía Erenia, a Yiya, Tío Reinaldo, a Yusnier y a tía Zulia por darme desde pequeño la dicha y los consejos para seguir siempre adelante, los quiero mucho.

A mis amigos de infancia Haimert, Alexey, Dailiovis, Yoinicer, a Yoania , el Villo y Elinor por haber confiado en mí siempre. Gracias.

A mi amiga Alicia Lisset Fernández Silva por esos buenos consejos en los años que estuvo junto conmigo en la universidad que aunque no sigue aquí me sigue ayudando.

A mi tutor por brindarnos consejos y ayuda que demasiada es todavía muy poco para todo lo que hizo por nosotros en este trabajo de diploma. Muchas gracias.

A todos mis amigos de la universidad que son muchos pero muy especial a Román, Daniel, Kenny, Oreste, Yori, Héctor, Noslen, Janiel, Julito, René, Aldo, Alberto, Máximo. En fin a todos esos amigos que de una

forma u otra compartieron junto conmigo los años tan especiales de la universidad y que muchos no están. Gracias a Todos.

Agradecer a las niñas del 8502 y las del antiguo grupo 4.

De Roman:

A nuestra Revolución y a nuestro siempre Comandante en Jefe Fidel Castro por darnos la oportunidad.

A mis padres por su apoyo incondicional en todo lo largo de mi vida.

A mi querida Yadira por su confianza, comprensión y cariño a lo largo de mi carrera pese a todas las dificultades y la distancia, gracias por estar siempre a mi lado.

A mi niña Liena que a pesar de su corta edad me ha brindado cariño, madurez y seguridad, un besote mi chiquitica.

A mis abuelos María y Gaspar por toda esa preocupación.

Al tutor Deivis Leiva que con tanto esfuerzo y dedicación supo guiarnos en el desarrollo de este trabajo.

A mi amiga Ginisleisi que siempre me aconsejo en los momentos más difíciles.

A mis amigos y compañeros de la universidad Yamir, El locho, Lissuan, El piquete Red Slime, Kenny, Daniel, Ariam , El chino, EL Salvaje, El Mulo, Yoisell, El Rodo, Marlon, Hector, Felipao, en fin a todos que son tantos que han compartido conmigo, que me han ayudado a seguir adelante.

Dedicatoria

A Adis Lozada mi querida madre, a Jorge Acosta mi excelente padre, a mi sobrinita Jessie Aimeé y a mi hermano Vladimir Hidalgo.

A los amigos de la Universidad.

A mi amigo y compañero de Tesis Román G. Álvarez.

Yamir Acosta Lozada

A mis padres, Elena Sutrimina y Gilberto Álvarez por el empeño y dedicación con que me han conducido en la vida para lograr este resultado....

A mi futura esposa Yadira Martínez y madre de mi niña Liena Álvarez las cuales siempre han confiado en mí, gracias a ellas he obtenido lo logrado…

A mi gran amigo Yamir Acosta por haberme ayudado y apoyado en todos estos años.

Román Gilberto Álvarez Sutrimina

Índice

Índice de Figuras

Índice tablas

Resumen

El trabajo de diploma tiene como tema “Propuesta de Implementación para el Centro de Resguardo de Datos de 5ta B”, principalmente refiriéndose a incrementar la alta disponibilidad del sistema, tener una buena protección de los datos y poseer un plan de recuperación ante desastres en caso de una caída del sistema. En la actualidad en las bases de datos de nuestra entidad al ocurrir cualquier falla del sistema, un error humano, o un desastre natural los servicios se interrumpen y para poder recuperarse transcurre un tiempo lo suficientemente extenso. Actualmente se cuenta con un plan de recuperación ante estos eventos, así como la protección de los datos pero es necesario incrementar y tener asegurada la alta disponibilidad del servicio. Esta investigación pretende dar una solución para obtener un incremento de la alta disponibilidad, la rápida recuperación ante desastre y la protección de los datos utilizando las bases de datos standby físicas configuradas en un ambiente Data Guard de Oracle las cuales se encuentran ubicadas en servidores virtualizados con la tecnología VMware.

Palabras clave: Disponibilidad, interrupción, recuperación, protección, virtualización, base de datos.

Introducción

Desde hace mucho tiempo, en el sector empresarial, existe la necesidad de contar con sistemas que permanezcan disponibles el mayor tiempo posible, es decir, todo el día, todos los días de la semana, todo el año. Con el avance de las tecnologías en las redes de computadoras y la amplia gama de equipos de última generación, se ha logrado en gran medida que este problema de hace muchos años de antigüedad tenga solución.

¿Pero en qué medida, con estos avances, se ha logrado la disponibilidad y la continuidad de los sistemas?

Por ejemplo, cierta empresa brinda un determinado servicio en la red, dígase un centro de datos, donde tiene a disposición de los usuarios informaciones en el que es necesario estar accediendo a ella las 24 horas del día, los 7 días de las semanas , los 365 días del año. En cierto momento ocurre una falla eléctrica, una catástrofe de cualquier índole, un error humano, un ataque informático; o sucede una combinación de cualquiera de los sucesos anteriormente mencionados. Si este centro no cuenta con una configuración de alta disponibilidad, con una buena protección de los datos, y con un plan de recuperación ante desastre, la continuidad de los servicios se verá afectada y el tiempo de vuelta a brindarlos será relativamente alto. Además, hay que tener en cuenta que estos sucesos ocurren de forma imprevista y es de suma importancia estar preparado para lo peor.

Actualmente existen varios softwares, que en combinación con la arquitectura de hardware, pueden proponer un buen plan de alta disponibilidad, una excelente protección de los datos, y una guía para la recuperación ante desastres. Haciendo posible que una parada del servicio tenga consecuencias mínimas para los usuarios, los cuales podrán seguir trabajando de forma transparente a la falla ocurrida en el sistema.

Situación Problémica

En la actualidad no existe una completa alta disponibilidad y protección de los datos y además, se torna difícil poder recuperarse ante desastres en un tiempo relativamente corto y con el menor impacto posible sobre la disponibilidad de los sistemas que se encuentran en explotación en el Centro de Datos Ministerial.

En el presente trabajo de diploma, que lleva por título, “Propuesta de Implementación del Centro de Resguardo de Datos de 5ta B”, se pretende dar respuesta a la siguiente **interrogante científica** ¿Cómo

lograr alta disponibilidad, protección de los datos y recuperación ante desastres de las bases de datos del Centro de Datos Ministerial utilizando la tecnología Data Guard de Oracle y VMware? Siendo el **objeto de estudio** de la investigación las características presentes en Oracle Data Guard y en VMware que hacen posible elevar la alta disponibilidad, la protección de los datos y recuperación ante desastres. El **campo de acción** de la misma está constituido por: las características específicas de las tecnologías Oracle Data Guard y VMware, que permiten elevar la alta disponibilidad, la protección de los datos y la recuperación ante desastres en las bases de datos del Centro Ministerial.

Para solucionar el problema descrito se tiene como **objetivo general:** realizar una propuesta de implementación del Centro de Resguardo de Datos de 5ta B, utilizando tecnología Data Guard de Oracle y VMware que permita elevar la alta disponibilidad, protección de los datos y recuperación ante desastres de las bases de datos del Centro de Datos Ministerial. Con dicho objetivo, se pretende defender la siguiente **Idea:** obteniendo una propuesta de implementación del Centro de Resguardo de Datos de 5ta B utilizando tecnología Data Guard de Oracle y VMware, se puede asegurar alta disponibilidad, protección de los datos y recuperación ante desastres de las bases de datos del Centro de Datos Ministerial.

Para llevar a cabo la investigación se definieron las siguientes **Tareas Investigativas:**

- Realizar un estudio del Estado del Arte de la tecnología Data Guard.
- Realizar un estudio del Estado del Arte de la tecnología VMware.
- Asimilar la tecnología Data Guard de Oracle.
- Asimilar la tecnología VMware.
- Configurar un polígono de prueba para desplegar las tecnologías que se investigan.
- Describir los métodos y procedimientos para realizar la implementación y el despliegue de las tecnologías que se investigan.

Para el cumplimiento de las tareas investigativas se emplearon los métodos investigativos siguientes:

- Análisis-síntesis: Permitió el estudio del fenómeno en sus múltiples relaciones y componentes, así como el análisis de la bibliografía existente para poder sintetizar y obtener las características más generales y específicas para la solución de la investigación.
- Método histórico-lógico: Permitió analizar la trayectoria completa del fenómeno, su condicionamiento a los diferentes períodos de la historia, revela las etapas principales de

> desenvolvimiento y las conexiones históricas fundamentales, y puso de manifiesto la lógica interna de su desarrollo, de su teoría y el conocimiento más profundo de su esencia.3

El presente trabajo de diploma está compuesto por 3 capítulos, organizados de la manera siguiente:

Capítulo 1: Fundamentación Teórica. En este capítulo se dará una panorámica de los conceptos de alta disponibilidad, protección de los datos, lo que es un servidor, lo que es la virtualización, máquinas virtuales, las tecnologías de Oracle, Real Application Cluster, Stream, las posibles tecnologías de virtualización y una detallada caracterización de estas, para proporcionar elementos suficientes a la hora de realizar la selección de una en específico.

Capítulo 2: Características principales de Data Guard y VMware ESX Server. En este capítulo se definen las características esenciales de estas dos tecnologías, describiendo sus potencialidades a utilizar en aras de lograr soluciones de alta disponibilidad robustas. Se plasman criterios importantes a evaluar durante el análisis de las mismas para ser usadas en la implementación de un centro de resguardo de datos.

Capítulo 3: Concepción e Implementación del Entorno de Alta Disponibilidad. En este capítulo se describe la configuración que se debe llevar a cabo, así como los principales problemas a tener en cuenta a la hora de implementar un entorno de alta disponibilidad con Oracle Data Guard y VMware ESX Server.

Capítulo 1

Fundamentación Teórica

Introducción

Hoy en día el mundo informático revoluciona a una velocidad increíble, razón por la que cualquier apasionado podría dedicar gran parte de su vida a su estudio y análisis. El siguiente capítulo es el resultado de una minuciosa y breve investigación acerca de los conceptos esenciales asociados al dominio del problema, del software existentes asociados al campo de acción, las nuevas tecnologías en este campo, las tendencias existentes en el mundo y una breve reseña del proceso que se empleará para darle solución al problema planteado.

1.1 Estado del arte

1.1.1 Conceptos fundamentales

Alta disponibilidad

Consiste en que la infraestructura tecnológica esté siempre funcionando en términos de 24 horas al día, los siete días de la semana, los 365 días del año, la famosa ecuación 24x7x365, y los cinco nueves: 99.999% de confiabilidad. Este concepto se refiere a la disponibilidad del sistema y que esté el menor tiempo caído (downtime) o “fuera de línea”, lo que se traduce en que una aplicación y el hardware donde corre ésta van a funcionar en el momento que se necesite [1].

Para lograrlo, se requiere de integrar soluciones que se componen de energía, procesadores, discos duros, software, personal capacitado, consultoría y procesos detallados; además, ya en la operación, se requiere redundancia en componentes críticos.

Protección de los datos

Acción que se realiza en cualquier compañía para resguardar y proteger la información almacenada en sus bases de datos o equipos. Por lo que para asegurar una buena protección de los datos es necesario tener en cuenta los tres aspectos de la seguridad Informática: Confidencialidad, Integridad y Disponibilidad. Confidencialidad porque los datos tienen que ser accedidos por las personas autorizadas. Integridad

porque no puede ser modificados por otras personas que no tengan acceso a esa información y disponibilidad porque debería estar accesible en el momento requerido por la persona autorizada.

Recuperación ante desastres

Los recientes acontecimientos políticos y los desastres climatológicos en el mundo obligan a los ingenieros en sistemas y especialistas en Tecnologías de la Información (TI) a adoptar un enfoque nuevo y sólido con respecto a las estrategias de recuperación ante desastres. Para brindar protección contra fallas generales, las organizaciones deben construir centros de datos secundarios lo suficientemente lejos como para que no se vean afectados por ningún desastre que pueda afectar al centro de datos principal, o bien tener implementado un plan de recuperación ante desastre.

Un plan de recuperación ante desastres es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que una empresa o compañía pueda comenzar de nuevo sus operaciones en caso de un desastre natural o un problema causado por errores humanos.

Existen varias causas que hacen que cualquier negocio con manejo de datos tenga que tener un plan y una implementación para la recuperación de los datos ante desastres. Se mencionan a continuación algunas de ellas:

- Catástrofes.
- Fuego.
- Fallas de energía
- Virus Informáticos
- Error humano.
- Sistema y/o fallas de equipo.

Servidor

En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una computadora cuyo principal propósito es proveer datos de modo que otras PC puedan utilizar esos datos, es decir, un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor. Es

importante saber que los servidores se conectan a la red mediante una interfaz que puede ser una red verdadera o mediante conexión vía línea telefónica o digital. [2]

Sistema Gestor de base de datos

Los Sistemas de Gestión de bases de datos (SGBD) son un tipo de software muy específico, dedicado a servir de interfaz entre las bases de datos, el usuario y las aplicaciones que las utilizan. Una base de datos no es más que un conjunto de información relacionada que se encuentra agrupada o estructurada [3]. Desde el punto de vista informático, una base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulan ese conjunto de datos.

Virtualización

Es una tecnología de software que hace posible la ejecución simultánea de varios sistemas operativos y varias aplicaciones en el mismo ordenador, aumentando con ello la utilización y la flexibilidad del hardware, que básicamente, permite transformar hardware en software.

La virtualización permite crear una máquina virtual completamente funcional que puede ejecutar su propio sistema operativo y aplicaciones de la misma forma que lo hace un ordenador real. Varias máquinas virtuales comparten recursos de hardware sin interferir entre sí; de modo que es posible ejecutar simultáneamente y de forma segura varios sistemas operativos y aplicaciones en un único ordenador.

Máquina Virtual

Es un contenedor de software perfectamente aislado que puede ejecutar sus propios sistemas operativos y aplicaciones como si fuera un ordenador físico. Una máquina virtual se comporta exactamente igual a un ordenador físico; y contiene sus propios CPU, RAM, disco duro y tarjetas de interfaz de red virtuales. El sistema operativo de la máquina virtual no puede establecer una diferencia entre esta máquina virtual y una máquina física, ni tampoco lo pueden hacer las aplicaciones u otros ordenadores de una red. Incluso la propia máquina virtual considera que es un ordenador “real”. Sin embargo, una máquina virtual se compone exclusivamente de software y no contiene ninguna clase de componente de hardware. El

resultado de ello es que las máquinas virtuales ofrecen una serie de ventajas con respecto al hardware físico.

1.1.2 Estado actual

Actualmente, en el mundo, existen mecanismos y tecnologías que permiten implementar sistemas con características de disponibilidad prácticamente completas, contando con un nivel elevado de protección de sus datos, ya que, este es el renglón fundamental de un sistema. A continuación, se muestran algunas empresas a nivel mundial que constituyen la avanzada en el desarrollo de estas tecnologías.

Vision Solutions

Es el principal proveedor de soluciones de alta disponibilidad y recuperación ante desastres dentro de los mercados IBM Power Systems, cuenta con una innovadora tecnología nombrada EchoStream para la tecnología de Ejecución Interactiva Avanzada (*AIX, por sus siglas en ingles*), la cual tiene propiedades de replicación de datos con protección continua de datos (*CDP, por sus siglas en ingles*) [4]. Esta tecnología CDP permite a un sistema recuperar datos en cualquier momento y de una manera rápida y fácil; e incluso si fueron datos accidentalmente borrados o de otra manera corrompidos.

"EchoStream para AIX es absolutamente esencial para nuestra continuidad empresarial ya que nos brinda el poder de mantener datos importantes protegidos y disponibles en todo momento, sin el trabajo manual o las caídas temporales de las soluciones de respaldo de datos tradicionales",[1]

"Y debido a que funciona automáticamente en trasfondos, EchoStream para AIX no requiere un periodo de inactividad planificado previamente para que se realicen copias de respaldo, esto resulta ser perfecto para la estrategia de recuperación de desastres de DKSH". [2]

Con la ayuda de esta tecnología y las instalaciones de alojamiento IBM cercanas, el centro de datos ahora cuenta con capacidades de recuperación ante desastres muy sólidas. En el caso de cortes inesperados como faltas de energía o fallas en las líneas de comunicaciones o si Diethelm Keller Siber Hegner (*DKSH*

[1] Sr. MK Lee, gerente técnico y de operaciones de DKSH CSSC, Agosto 27/2008.

[2] El Sr. Richard Tee, director regional de ventas de Vision Solutions para el área del Pacífico Sur de Asia.

por sus siglas en ingles) experimenta pérdidas de datos accidentales o maliciosas, puede rápidamente recuperar y reanudar sus operaciones desde un espacio confiable de respaldo de datos. Los servidores del Centro de Servicios Corporativos Compartidos (*CSSC, por sus siglas en ingles*), brindan protección y respaldo de datos para los sistemas usados en Malasia, Singapur, Indonesia, Filipinas, Hong Kong, Taiwán, Tailandia, la Unión Europea, Japón y Holanda. Prácticas y ejercicios sobre recuperación ante desastres son llevados a cabo regularmente para asegurar una transmisión libre de problemas en el caso de cualquier crisis. [4]

EMC Corporation

Las soluciones de Affordable Disaster Recovery de EMC minimizan la exposición a pérdidas de datos ocasionadas por desastres y reducen el costo total de propiedad. Con estas soluciones se puede cumplir con los exigentes requerimientos de nivel de servicio, tiempo de recuperación y pérdida de datos de la actualidad. Además, se pueden reiniciar rápidamente las aplicaciones en caso de fallas y replicar información de manera asequible a ubicaciones remotas con tecnología que minimiza el ancho de banda y los costos de las redes. Además tienen soluciones para la protección de los datos con su Replicación de Datos Heterogénea (*HDR, por sus siglas en ingles*). [5]

Comprende varios productos para llegar a una solución:

- MirrorView: Ofrece espejo remoto sincrónico y asincrónico para garantizar que la información esté protegida contra fallas del sistema y del sitio.
- RecoverPoint: Se obtiene protección de datos rentable y continua, y replicación remota continua, a fin de permitir la recuperación y protección según demanda a cualquier punto en el tiempo.
- RecoverPoint/SE: Se garantiza la protección continua de datos y la replicación remota continúa de datos para su sistema de almacenamiento en red EMC CLARiiON.
- RepliStor: Proporciona replicación asincrónica local y remota basada en servidor para su entorno Microsoft Windows. Esta solución brinda continuidad del negocio de bajo costo para replicar, proteger, migrar y recuperar los datos.

AQB Corporation

La solución de Alta Disponibilidad de AQB considera una tecnología de software, fácil e inmediata para recuperación y protección de datos para Windows. Aumenta la disponibilidad de la información, al ofrecer réplicas en tiempo real a una o más ubicaciones, independientemente de donde se encuentren. Sus datos se pueden usar para protección de respaldo fuera de línea, recuperación ante desastres, distribución de datos y prueba de aplicaciones. La solución se integra con Volume Shadow Copy Service (VSS) de Microsoft, permite crear copias instantáneas consistentes con las aplicaciones, en un servidor secundario para asegurar la capacidad de recuperación y sin afectar al servidor principal. En la siguiente tabla se definen las principales características que brinda esta tecnología donde se puede distinguir sus principales funcionalidades y los beneficios que aporta.

Funcionalidades	Beneficios
Replicación sincrónica simple	Distribuye geográficamente conjuntos idénticos de datos de manera instantánea a uno o varios computadores.
Replicación de datos para Windows	Proporciona un conjunto secundario de datos que permiten tener acceso al sistema las 24 horas del día, los siete días de la semana en caso de un error o debido al mantenimiento del sistema.
Capacidad de recuperación asegurada	Recupera entornos Exchange luego de una interrupción compleja con integración de Volume Shadow Copy Service (VSS) de Microsoft.
Soporte de LAN, MAN y/o WAN	Protege datos y servidores de misión crítica contra desastres locales o en el sitio.
Consolidación centralizada del backup	Asegura que los datos estén disponibles desde la oficina remota para respaldo centralizado.

Tabla 1: Características de la solución de AQB.

Proporcionan funciones de alta disponibilidad dentro de múltiples sistemas operativos (UNIX, LINUX y Windows) para entornos en cluster de Oracle, Exchange y SQL Server. Administra el reinicio automatizado de las aplicaciones en un servidor alternativo, local o remoto, en caso de un desastre y/o una interrupción planificada o no planificada del servicio. Permite automatizar el failback de los servicios, aplicaciones y datos de manera rápida y eficiente, garantizando la continuidad del servicio. [6]

En el caso de entornos geográficamente dispersos, que requieren protección a través de la implementación de un clúster, soporta tecnologías de replicación con una óptima integración, los cuales se definen en la siguiente tabla.

Funcionalidades	Beneficios
Reinicio automático de las aplicaciones	Elimina el tiempo de inicio de los sistemas en otro servidor, en caso de haber downtime. En minutos recupera automáticamente las aplicaciones.
Integración de tecnologías de replicación	Asegura de que los datos se encuentren en el sitio de failover y su estado sea consistente para las aplicaciones.
Módulos de aplicaciones pre-configurados	Disminuye la complejidad de administrar la disponibilidad de las aplicaciones. Implementación más rápida de la solución de continuidad del negocio.
Aplicaciones soportadas	Brinda soporte para Microsoft® Exchange, SQL Server y Oracle.
Soporte para servidores heterogéneos	Administra fácilmente sus diversas aplicaciones y entornos de almacenamiento

de información.

Tabla 2: Características de la solución de AQB para entornos geográficamente dispersos.

1.2 Tecnologías para la solución

Existen numerosas tecnologías, así como, variantes de implementación que permiten implementar entornos de alta disponibilidad, protección de los datos y recuperación ante desastres. No obstante, a través del presente epígrafe se describirán las principales que presenta Oracle y VMware.

1.2.1 Tecnologías dentro de Oracle

Oracle desarrolla una gran gama de tecnologías para lograr las exigencias impuestas por los sistemas de alta disponibilidad, entre ellas se encuentran:

1.2.1.1 Real Application Clusters

Real Application Clusters (RAC) es una tecnología de Oracle que permite utilizar un cluster de servidores ejecutando múltiples instancias sobre una misma base de datos. Los archivos de base de datos quedan almacenados en discos física o lógicamente conectados a cada nodo, de modo tal que todas las instancias activas pueden leerlos o escribirlos. El software de RAC maneja el acceso a los datos, de modo tal que los cambios en los datos son coordinados entre las instancias y cada instancia ve imágenes consistentes de la base de datos. La interconexión del cluster permite que las instancias se intercambien entre ellas información de coordinación e imágenes de los datos. Esta arquitectura permite que los usuarios y aplicaciones se beneficien de la potencia de procesamiento de múltiples máquinas. La arquitectura RAC también ofrece redundancia; por ejemplo, en el caso de que un nodo quede inutilizado, la aplicación continuará accediendo a los datos vía el resto de las instancias disponibles [7].

Dado que todas las computadoras/instancias acceden a los mismos datos, el software de Oracle debe garantizar que los datos cambian en computadores diferentes de forma coordinada y que cuando un computador consulta datos recibe la versión actual, incluso si los datos fueron modificados recientemente por otro computador. Esta funcionalidad de Oracle RAC se llama Cache Fusion, la cual se encarga de

tratar las caches de datos en memoria en cada computador en una cache individual global. Cache Fusion esencialmente *funde* las caches separadas en una cache global. [7]

Beneficios

Cache Fusion transfiere los bloques de datos (la unidad de transferencia más pequeña en la base de datos) usando la red de interconexión de alta velocidad de la infraestructura. Antes de la fusión de cache, el disco se usa como un medio de transferencia de datos y que tiene desventajas evidentes. Dado que Oracle RAC permite a varias computadoras acceder a una base de datos individual, puede ser usado para dirigir varias áreas de gestión de base de datos. Estas áreas incluyen: Alta disponibilidad, Escalabilidad, Crecimiento Incremental, y Consolidación de base de datos. [7]

1.2.1.2 Oracle Recovery Manager (RMAN)

Una estrategia fiable para obtener alta disponibilidad y recuperación ante desastres requiere de una copia de seguridad de los datos, una restauración y algún procedimiento de recuperación. Oracle Recovery Manager (RMAN), es el método preferido de Oracle para realizar copias de seguridad de manera eficaz y recuperar su base de datos. RMAN está diseñado para trabajar estrechamente con el servidor, optimiza el rendimiento y se integra con Oracle Secure Backup y un tercer producto de gestión. [8]

RMAN se encarga de todas las bases de datos antes y después de los procedimientos de copia de seguridad o restauración, liberando la dependencia del sistema operativo y las secuencias de comandos SQL*Plus. Proporciona una interfaz común para las tareas de copia de seguridad a través de diferentes sistemas operativos de host, y ofrece características no disponibles a través de métodos usuario-administrado, tales como la paralelización del backup, recuperación de datos, archivos de copia de seguridad, políticas de retención, y la historia detallada de todas las copias de seguridad. A continuación se muestra una representación general de la tecnología.

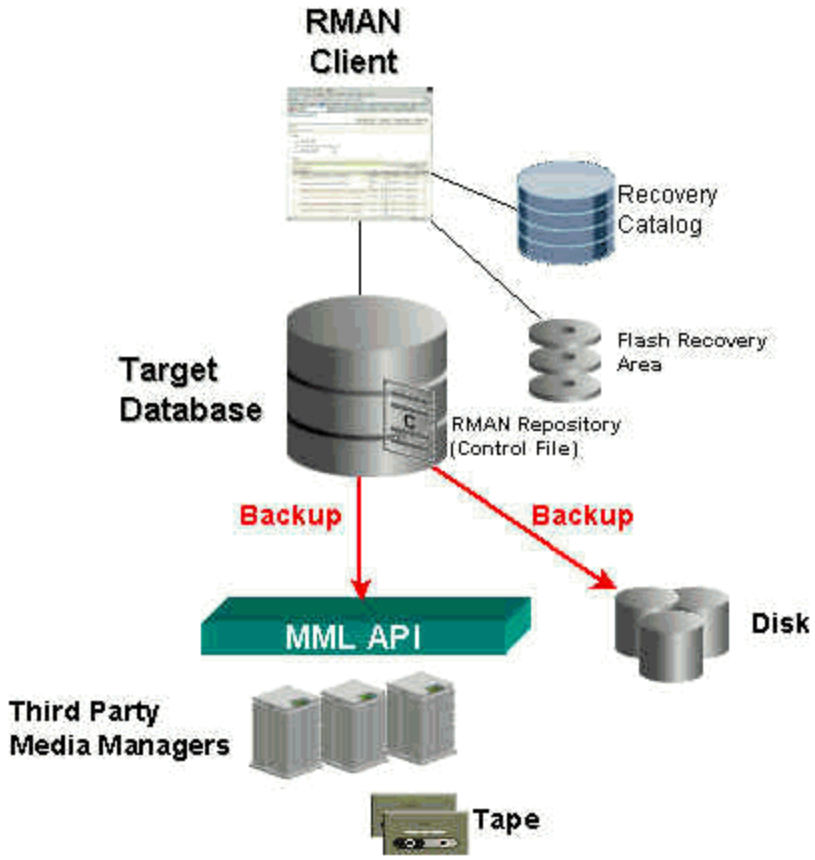

Figura 1: Representación general de la tecnología RMAN

La imagen anterior muestra los diferentes componentes que comprende RMAN, como:

- La base de datos de destino para la copia de seguridad
- El cliente RMAN (interpreta los comandos de copia de seguridad y recuperación).
- Un disco en la ubicación de la base de datos (para gestionar los archivos relacionados con el backup y la recuperación).
- Un software de gestión de los medios de comunicación.
- Un catálogo de recuperación de la base de datos.

Beneficios

RMAN puede realizar copias de seguridad o restaurar un único archivo en paralelo dividiendo el trabajo entre varios canales. Cada canal de copias de seguridad de un archivo de sección, que es una serie de bloques contiguos. Esto incrementa la seguridad global y restaura el rendimiento en caso de fallo. (Ídem).

1.2.1.3 Oracle Streams

Oracle Streams permite la propagación y gestión de datos, transacciones y sucesos en un flujo de datos, ya sea en una base de datos, o desde una base de datos a otra.. El resultado es una nueva característica que proporciona una mayor funcionalidad y flexibilidad que las soluciones tradicionales para la captura y gestión de eventos, y compartir los eventos con otras bases de datos y aplicaciones. [9]

Es una tecnología para compartir información. Detecta que información es relevante y quienes la utilizan. Esta tecnología es utilizada por Oracle para propagar los cambios en un ambiente replicado. Se basa en tres acciones aplicadas a la información, captura, almacenamiento y consumo. Para la replicación la captura se relaciona con un mecanismo que toma los cambios desde los ficheros redo log. El almacenamiento se vincula cuando los cambios capturados son enviados al área de almacenamiento, y luego estos cambios son propagados a las áreas de almacenamiento de los equipos remotos con réplicas. El consumo es la máquina que se encarga de aplicar los cambios almacenados a la base de datos en cada equipo con replicas. Las tablas replicadas pueden ser diferentes, Oracle Streams se encarga de transformar la información para ajustarla a la base de datos de cada sitio replicado. [9]

El proceso de captura configurado para recolectar cambios realizados, recupera los mismos desde el redo log, formatea la información como Registros de Cambio Lógicos (*LCR, por sus siglas en ingles*) y coloca los LCR en el área de almacenamiento de la base de datos local. Los LCR son entonces propagados desde el área o cola de almacenamiento de la base de datos origen, hacia las áreas de almacenamiento de las bases de datos destino de la replicación. [9]

1.2.1.4 Oracle Data Guard

Oracle Data Guard es una tecnología que garantiza alta disponibilidad, protección de los datos y recuperación ante desastres de los datos empresariales. El mismo brinda todo un conjunto de servicios

para crear, mantener, administrar y monitorear una o mas bases de datos en espera (standby), creadas a partir de una base de datos primaria o en producción, que permiten recuperar la base de datos de producción ante desastres o corrupción de los datos. Esta tecnología mantiene estas bases de datos standby como copias consistentes transaccionales de dicha base de producción. Oracle Data Guard puede ser usado como una técnica de salva, restaura y de cluster para suministrar un alto nivel de protección y disponibilidad de los datos.

Una configuración Data Guard está formada por una base de datos de Producción y una o más bases de datos en espera. Las bases de datos de una configuración Data Guard están conectadas mediante Oracle Net y pueden estar dispersas geográficamente. No existe ninguna restricción en cuanto al lugar donde estén ubicadas las bases de datos, mientras se puedan comunicar unas con otras. En la siguiente figura se muestra un entorno Data Guard donde se muestra una base de datos de producción o primaria conectada a través de Oracle Net con dos bases de datos standby.

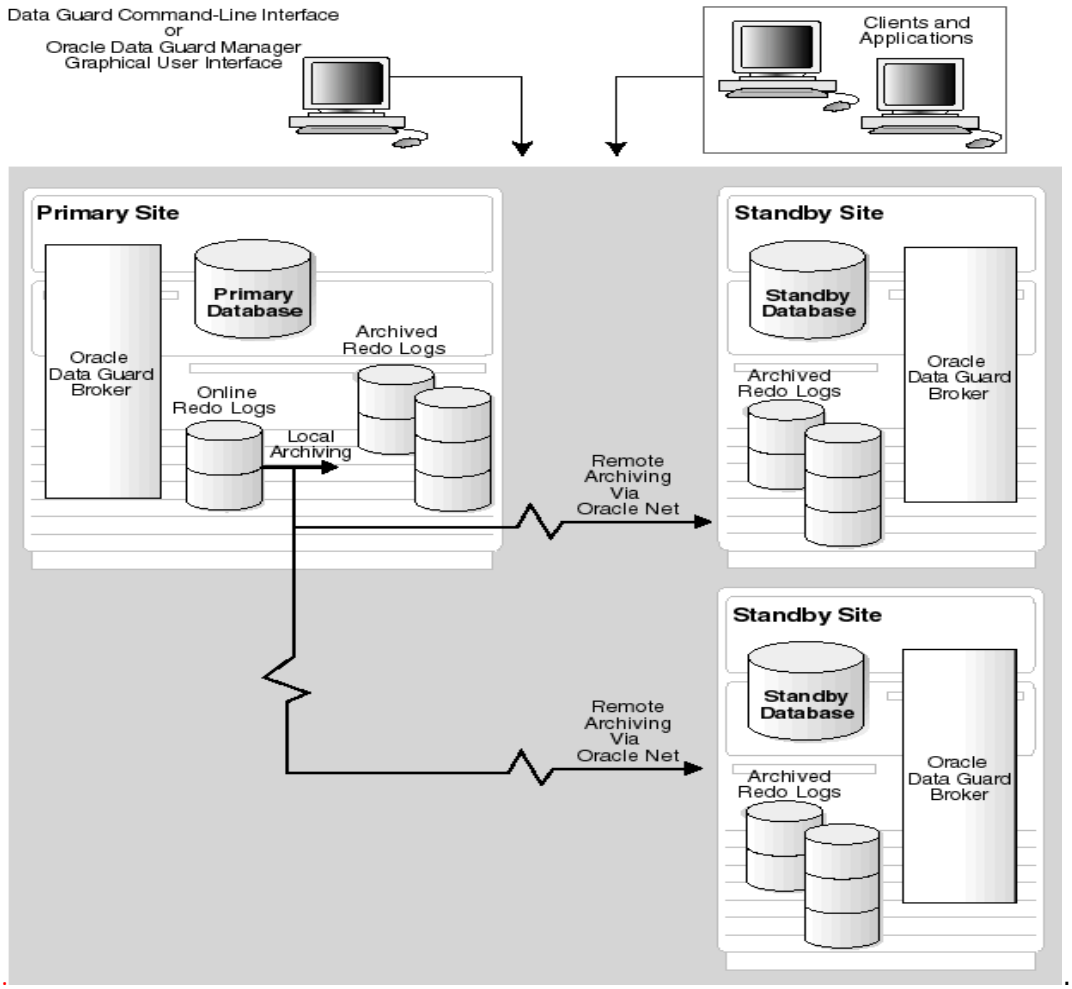

Figura 2: Representación de un entorno Data Guard

De una copia de la base de datos primaria se pueden obtener hasta nueve bases de datos standby. En una configuración Data Guard pueden coexistir 3 tipos diferente de bases de datos standby:

- Base de datos standby física
- Base de datos standby lógica.
- Base de datos standby snapshot.

La propuesta de implementación del centro de resguardo estará constituida por bases de datos standby del tipo física, teniendo estas bases de datos se puede contar con las características siguientes: constituyen

una copia físicamente idéntica de la base de datos primaria, sus estructuras en disco son idénticas, bloque a bloque, a las de la base de datos primaria, y su esquema de bases de datos, incluyendo los índices, es idéntico. Una base de datos standby física se mantiene sincronizada con la primaria mediante un proceso llamado Redo Apply el cual recupera los datos de redo recibidos de la base de datos primaria aplicándolos posteriormente en la base de datos standby física. A partir de Oracle11g a través de Active Data Guard una base de datos standby física puede recibir y aplicar los datos de redo recibidos de la base de datos primaria mientras se mantiene abierta en sólo lectura. El proceso de Redo Apply aplica de manera continuada los datos de redo recibidos de la base de datos primaria en la base de datos standby física usando los mecanismos de recuperación de bases de datos tradicionales conocidos desde versiones anteriores de Oracle. Por lo tanto, estas características mencionadas anteriormente provocan que las bases de datos standby físicas tengan las ventajas que se describen a continuación.

Ventajas de una base de datos standby física.

- Recuperación ante desastres y alta disponibilidad.

Una base de datos standby física constituye una forma eficiente y robusta de recuperación ante desastres, así como una solución de alta disponibilidad. Las facilidades de administración para la conmutación, permiten un fácil intercambio de roles entre la base de datos primaria y las bases de datos standby físicas, minimizando el tiempo de parada de la base de datos primaria ante cualquier tipo de interrupción que pueda ocurrir.

- Protección de los datos.

Una base de datos standby física puede prevenir la pérdida de datos incluso en el caso de desastres imprevistos. Ellas soportan todos los tipos de datos y todas las operaciones del lenguaje de definición de datos (*DDL por sus siglas en ingles*) y del lenguaje de manipulación de datos (*DML por sus siglas en ingles*) que pueden ser realizados sobre la base de datos primaria. De igual manera proporcionan una salvaguarda contra corrupciones en los datos y errores de usuarios. Una corrupción al nivel del almacenamiento físico en la base de datos primaria no se propagará hacia las bases de datos standby físicas, así mismo, las corrupciones de tipo lógico o los errores de usuario que de otra manera significarían la pérdida de los datos pueden ser resueltos fácilmente.

- Reducción de la sobrecarga en la base de datos primaria.

RMAN puede usar una base de datos standby física para ejecutar las salvas de la base de datos primaria disminuyendo la sobrecarga de trabajo que pueda existir en esta. De igual manera, una base de datos

standby física puede ser encuestada mientras el servicio de aplicación de redo (Redo Apply) está activo, esto permite que las consultas sean transferidas desde la base de datos primaria hacia la standby, reduciendo también cualquier sobrecarga de trabajo que pueda existir.

- Rendimiento (Performance)

La tecnología de Redo Apply usada en las bases de datos standby físicas es el más eficiente mecanismo para mantener actualizada una base de datos standby con los cambios realizados en la base de datos primaria porque aplica los cambios usando los mecanismos de recuperación de la base de datos de bajo nivel evitando toda la capa de código al nivel de las sentencias SQL.

1.2.2 Tecnologías para la Virtualización

Con el desarrollo cada vez mayor del hardware, es imprescindible utilizar tecnologías que permitan aprovechar al máximo sus capacidades; elevando considerablemente los niveles de prestaciones de los servicios que se brindan. Actualmente, se pueden encontrar diferentes tecnologías y productos desarrollados con este fin. El liderazgo a nivel mundial se encuentra entre las soluciones que serán mencionadas a continuación.

1.2.2.1 Xen

Es un software de código abierto que permite implementar máquinas virtuales. Su finalidad es la ejecución de distintos sistemas operativos a partir de cualquier hardware y, para ello, utiliza una técnica llamada paravirtualización que permite incrementar el nivel de rendimiento con respecto a los resultados que ofrecen las técnicas tradicionales de virtualización. [10]

Algunas aplicaciones de la virtualización con Xen son:

- Consolidación de servidores.
- Independencia del hardware.
- Housing virtual.
- Recuperación ante desastres.
- Reducción de costos

Entre sus beneficios están:

- Permite ejecutar instancias de sistemas operativos paravirtualizados (Linux, NetBSD, FreeBSD).
- Agrega dispositivos en caliente (Hard Disk Drive (HDD por sus siglas en ingles), etc.)), migrar máquinas virtuales.
- Xen permite alcanzar virtualización de alto rendimiento.(Ídem)
- Presenta características como:
- Un excelente rendimiento (entre 0.1% y 3% de sobrecarga).
- Tiene soporte de hasta 32 procesadores en paralelo (SMP).
- Soporta PAE (Physical Address Extension) para servers de 32 bits con más de 4Gb de memoria RAM.
- Tiene soporte para hardware de virtualización Intel VT y AMD Pacifica. [11]

1.2.2.2 Virtual Box

VirtualBox es un software de virtualización para arquitecturas x86. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como “guest”, dentro de otro sistema operativo “host”, cada uno con su propio ambiente virtual. Provee funcionalidades, como la ejecución de máquinas virtuales de forma remota, por medio del Protocolo de Escritorio Remoto (*RDP, por sus siglas en ingles*) y soporte para iSCSI.

En cuanto a la emulación de hardware, los discos duros de los sistemas invitados son almacenados en los sistemas anfitriones como archivos individuales en un contenedor llamado Imagen de Discos Virtuales (*VDI, por sus siglas en ingles*), incompartible con los demás software de virtualización. Otra de las funciones que presenta es la de montar imágenes ISO como unidades virtuales de CD o DVD, o como un disco floppy [12]. Ahora, es importante aclarar que estas características antes mencionadas no son exclusivas de Virtual Box, sino que están presentes en la mayoría de las soluciones de virtualización.

1.2.2.3 Parallels Virtuozzo

Parallels Virtuozzo crea múltiples entornos virtuales independientes (también conocidos como Servidores Privados Virtuales (*VPS, por sus siglas en ingles*)) en un solo servidor físico.

Características:

- Virtuozzo puede crear decenas o centenares de VPS en un solo servidor debido a su forma de funcionamiento y realizar la virtualización a nivel de sistema.
- Está disponible para las plataformas Linux y Windows.
- Virtualiza a nivel del sistema operativo y no a nivel del hardware.
- Permite administrar un alto rendimiento.
- Permite desarrollar la alta disponibilidad. [13]

1.2.2.4 VMware

Esta herramienta inserta directamente una capa de software en el hardware del ordenador o en el sistema operativo host. Esta capa de software crea máquinas virtuales y contiene un monitor de máquina virtual o "hipervisor" que asigna recursos de hardware de forma dinámica y transparente, para poder ejecutar varios sistemas operativos de forma simultánea en un único ordenador físico. VMware ofrece una sólida plataforma de virtualización que puede ampliarse por cientos de dispositivos de almacenamiento y ordenadores físicos interconectados para formar una infraestructura virtual completa.

Entre las ventajas que permite VMware están:

- Consolidación de servidores y optimización de infraestructuras.
- Disminución de los costes de infraestructura física.
- Flexibilidad operativa y una capacidad de respuesta rápida.
- Amplia disponibilidad de aplicaciones y continuidad de los servicios.
- Capacidad de gestión y seguridad.

Para la virtualización de empresas y centros de datos es recomendado usar el ESX server debido a que presenta numerosas características que en el capitulo 2 de este trabajo se explicarán.

1.2.2.4.1 ESX Server

La versión 3.5 del software de virtualización ESX Server constituye un verdadero Sistema Operativo (SO), lo que significa que para su ejecución no es necesario contar con un SO que se encargue de su gestión, por lo tanto su instalación se realiza directamente sobre el hardware. Con ESX Server se puede:

- Aumentar la utilización de las herramientas de hardware y disminuir considerablemente los costos operacionales y de capital al compartir recursos de hardware a través de un gran número de máquinas virtuales que funcionan en paralelo en el mismo servidor.
- Mejorar los niveles de servicio incluso para las aplicaciones que consumen más recursos con las funcionalidades avanzadas de administración de recursos, alta disponibilidad y seguridad.
- ESX Server ofrece los más altos niveles de rendimiento, escalabilidad y solidez que necesitan los entornos de TI empresariales.[14]

ESX Server 3.5 es el producto software de virtualización optimizado, rigurosamente probado y certificado de todas las ofertas completas de TI de servidores, almacenamiento de información, sistemas operativos y aplicaciones de software que permiten una estandarización a nivel empresarial.[14]

Además ESX server permite:

- Interoperabilidad ya que está certificado con servidores blade, de torre y montados en rack líderes de la industria de Dell, Fujitsu Siemens, HP, IBM, NEC, Sun Microsystems y Unisys.
- El Performance y la Escalabilidad porque pueden virtualizarse hasta las aplicaciones de producción que hacen un uso más intensivo de los recursos, como las bases de datos, los sistemas de planificación de recursos de la empresa (ERP, por sus siglas en ingles) y la administración basada en la relación con los clientes (CRM, por sus siglas en ingles).
- Una fácil administración de las máquinas virtuales mediante una amigable interfaz de usuario.
- Optimización de recursos distribuidos debido a que permite distribuir los recursos del hardware dinámicamente.
- Alta Disponibilidad: porque permite el almacenamiento compartido y asigna a cada máquina virtual de la red un failover de la Interfaz de la Tarjeta de Red (*NIC, por sus siglas en ingles*) incorporado y un equilibrio de carga para permitir una tolerancia a fallas.

1.3 ¿Por qué usar Virtualización?

Oracle permite crear varias instancias en un mismo servidor. Esta podría ser una solución para mantener sobre una misma infraestructura de hardware varios sistemas Oracle que sean utilizados como bases de datos standby dentro de una configuración Data Guard. Ahora, el problema se produciría, si el sistema dónde están desplegadas estas instancias, le ocurre una falla; ya que, sería necesario volver a instalar el Sistema Operativo y crear todas las diferentes instancias con sus configuraciones pertinentes. De esta forma es imposible recuperarse en un tiempo relativamente corto, además de que todas las consultas realizadas a partir del momento de la interrupción no se atenderán y el costo en recuperación sería muy alto.

Con virtualización el problema anteriormente mencionado se soluciona eficazmente, ya que esta tecnología permite el almacenamiento centralizado de máquinas virtuales, permitiendo mantener salvas de las máquinas virtuales que en caso de un desastre del sistema, estas, estando almacenadas en otra localización, sería bastante rápido recuperar el sistema al estado anterior de haber ocurrido la falla. Siendo esta características muy importante para el mantenimiento, continuidad de los servicios y la protección de los datos. Por ejemplo, el sistema donde se tiene instalado el ESX Server, tiene un fallo, el tiempo de recuperación es mucho más corto pues como se tienen las salvas de estas máquinas virtuales, con un simple procedimiento de montaje, las máquinas virtuales nuevamente estarán disponibles con su Sistema Operativo y el Oracle instalados. A partir del cual simplemente bastaría una recuperación de las bases de datos standby, procedimiento que es realizado automáticamente por la tecnología Data Guard.

Otra de las razones es que no se cuenta con la cantidad de recursos suficientes para tener una base de datos standby física de un sitio primario en relación uno a uno con el hardware. Al contar en el Centro de Datos con equipamiento de explotación bastante potente (tecnología Blade Server), se podría optimizar su uso creando un entorno virtual para alojar los sitios standby en máquinas virtuales.

Además de contar con las siguientes características presentes en la virtualización con ESX Server, como son:

- Existe una consolidación de servidores y la optimización de infraestructuras.
- Disminución de los costes de infraestructura física.

- Capacidad de gestión y seguridad.

Conclusiones

A través del capítulo se realizó un estudio minucioso de las principales herramientas y tecnologías que se deben valorar y tener en cuenta cuando se pretenden elevar los niveles de disponibilidad, protección de los datos y recuperación ante desastres en un data center. Después de haberse realizado un profundo estudio del estado del arte de estas tecnologías y analizado cada una de sus ventajas y desventajas, se llega a la conclusión de que el uso de la tecnología Data Guard de Oracle conjunto con ESX Server constituyen una buena selección para dar solución al problema planteado, ya que, Data Guard puede ser usado como una técnica de salva, restaura y de cluster para suministrar un alto nivel de protección y disponibilidad de los datos, brinda todo un conjunto de servicios que garantizan alta disponibilidad, protección de los datos y recuperación ante desastres, además la virtualización provee una consolidación de servidores y optimización de infraestructuras, una disminución de los costes de infraestructura física, flexibilidad operativa y una capacidad de respuesta rápida, y una amplia disponibilidad de aplicaciones y continuidad de los servicios.

Capítulo 2

Características principales de Data Guard y VMware ESX Server

Introducción

Después de analizar en el capítulo anterior algunas de las tecnologías de Oracle que permiten incrementar la alta disponibilidad, la protección de los datos y la rápida recuperación ante desastre; así como analizar de forma rigurosa las tecnologías de virtualización se dará paso durante el transcurso de este capítulo a describir las principales características y potencialidades de las tecnologías Oracle Data Guard y VMware ESX Server. También, se definirán los principales elementos a tener en cuenta para su configuración e implementación.

2.1 Características Generales de Oracle Data Guard

Oracle Data Guard es una tecnología que garantiza alta disponibilidad, protección y recuperación ante desastres de los datos de una base de datos. Permite crear y administrar una o más bases de datos standby, creadas a partir de una base de datos primaria, cuyo principal objetivo es permitir recuperar la base de datos de producción ante cualquier desastre o corrupción de los datos. Data Guard mantiene estas bases de datos standby como copias consistentes transaccionales de dicha base de producción.

Además, Oracle Data Guard puede ser usado como una técnica de salva, restaura y de cluster para suministrar un alto nivel de protección y disponibilidad de los datos. La administración de las bases de datos primarias y standby se puede realizar usando la interfaces de líneas de comandos SQL o las interfaces del Data Guard Broker, incluyendo una interface de línea de comando DGMGRL y una interfaz gráfica que es integrada al Oracle Enterprise Manager.

2.1.1 Arquitectura de Oracle Data Guard

A continuación se muestra la representación general de una configuración Data Guard donde se muestra una base de datos primaria, varias bases de datos Standby, la conexión a través del Oracle Net, los diferentes Servicios que intervienen y el Data Guard Broker, los cuales serán explicados durante el transcurso de este capitulo.

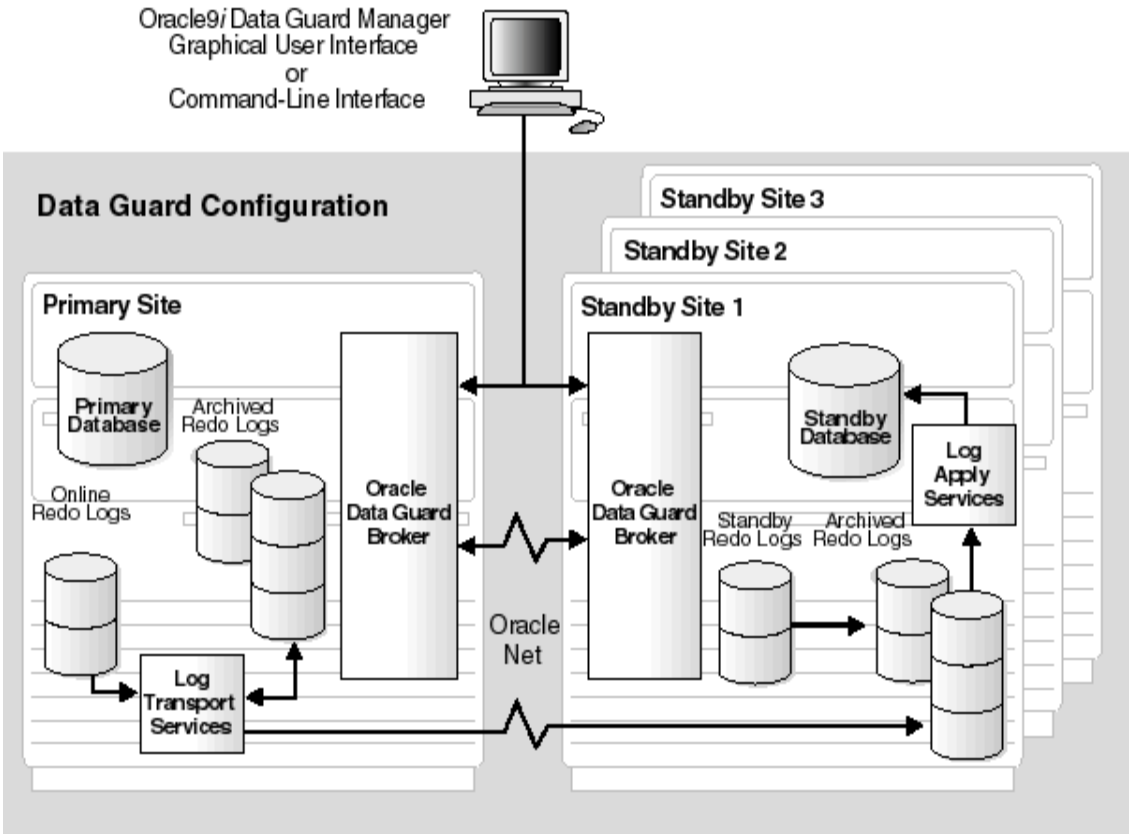

Figura 3: Configuración Data Guard.

2.1.1.1 Base de datos primaria

- Es una base de datos en producción, la cual es usada para crear la base de datos standby.
- La base de datos primaria puede ser una base de datos Oracle de una sola instancia o una base de datos en un Oracle Real Application Cluster.
- Cada base de datos primaria puede soportar múltiples bases de datos standby.
- Los redologs asociados con la base de datos primaria son enviados para ser aplicados hacia cada sitio standby.

2.1.1.2 Base de datos standby

- Es una base de datos de réplica consistente, transaccional, creada a partir de una base de datos primaria.
- Se pueden crear hasta 9 bases de datos standby de una base de datos primaria.
- Una base de datos standby está asociada con una y solo una base de datos primaria.
- Similar a una primaria, una base de datos standby puede ser una base de datos Oracle de una instancia o una base de datos Oracle Real Application Cluster.
- Una base de datos standby puede ser una base de datos standby física, una standby lógica o una snapshot.

A continuación se describen las principales características que definen a cada uno de los tres tipos de bases de datos standby que pueden encontrarse en un entorno Data Guard.

- Una base de datos standby física es una copia idéntica de la primaria a nivel de bloque a bloque, con las mismas estructuras de base de datos que la primaria, con los mismos esquemas e índices. La cual se sincroniza a través del servicio “Redo Apply”, el cual recibe todos los datos redo desde la primaria y los aplica en la base de datos standby física. A partir de la versión Oracle11g Release 1, una base de datos standby física puede recibir y aplicar redo mientras se encuentra abierta en solo lectura.
- Una base de datos standby lógica contiene la misma información lógica que la base de datos de producción, aunque la organización física y estructura de los datos sea diferente. Esta base de datos standby es sincronizada con la base de datos primaria a través del servicio “SQL Apply”, el cual transforma los datos de redo recibidos en instrucciones SQL y luego ejecuta estas instrucciones en la base de datos standby. Esta permite realizar actualizaciones del software de bases de datos Oracle y aplicar parches sin tener que desactivarla.
- Una base de datos snapshot no es mas que una base de datos standby actualizable que es creada por la conversión de una base de datos standby física en una base de datos standby snapshot. Al igual que las anteriores recibe y guarda los redo de datos desde la base de datos primaria, los

cuales son aplicados cuando la base de datos snapshot es convertida nuevamente en una base de datos física, deshaciendo todos los cambios realizados a la base de datos durante el periodo en que se encontraba como snapshot.

2.1.1.3 Configuración de la red

La base de datos primaria está asociada a una o más bases de datos standby remotas a través del Oracle Net.

Oracle Net es un componente de software que reside en el cliente y en el servidor Oracle y se encarga de establecer y mantener las conexiones entre los clientes y el servidor de base de datos, usando para el intercambio de mensajes protocolos de comunicación Standard (TCP/IP). Su configuración depende de los ficheros **`listener.ora`** y el **`tnsnames.ora`**. El listener es un proceso que corre en el servidor que es el encargado de escuchar las solicitudes clientes para atenderlas; cuando este recibe una solicitud verifica que la información ofrecida por el cliente en el descriptor de conexión coincide con la información que aparece configurada en el fichero **`listener.ora`** localizado en **`$ORACLE_HOME/network/admin`** y solo en este caso es autorizada la conexión hacia el servidor de datos. El cliente puede definir los parámetros para el descriptor de conexión en el fichero **`tnsnames.ora`** de la máquina cliente.

2.1.1.4 Servicios del Data Guard

2.1.1.4.1 Servicio de transporte de Redo

Controla la transferencia automática de datos redo desde una base de datos primaria a uno o más sitios standby. Para ello realiza las siguientes tareas:

- Transmitir los redo de datos desde el sistema primario al sistema standby.
- Administrar el proceso que resuelve cualquier salto (gap) en los ficheros redologs archivados provocados por un fallo de red.
- Garantizar los modos de protección de la base de datos.
- Automáticamente detectar ficheros redologs corruptos u omitidos en un sistema standby y recibir los ficheros redologs de reemplazo desde el sitio primario o desde otro sitio standby.

2.1.1.4.2 Servicio de aplicación de redo

- Aplica los redo de datos en la base de datos standby para mantener la sincronización transaccional con la base de datos primaria. Los redo de datos pueden ser aplicados desde los ficheros redolog archivados, o, si la aplicación en tiempo real esta activa (Real-time Apply), entonces directamente desde los ficheros redologs standby cuando se hayan llenado, sin necesidad de que sean almacenados primeramente en la base de datos standby.

- Existe diferencia entre la manera en que se aplican los redo de datos archivados entre una standby física y lógica. En la física, Data Guard usa la tecnología Redo Apply, la cual aplica los redo de datos en la base de datos standby usando las técnicas de recuperación estándares de Oracle como se muestra en la siguiente figura.

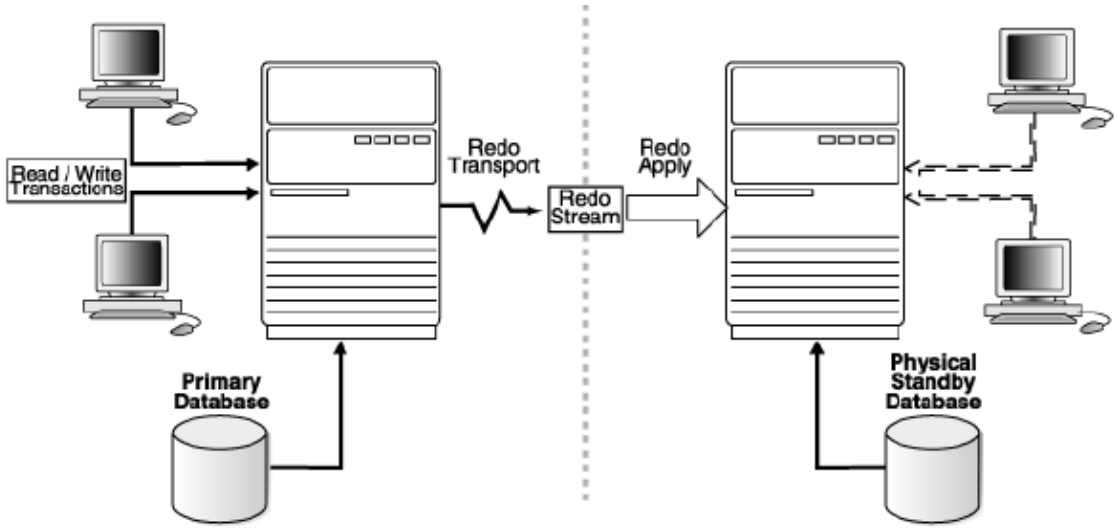

Figura 4: Aplicación de los redo de datos en una base de datos Standby física.

En la figura siguiente se muestra como en la base de datos standby lógica el Data Guard usa la tecnología SQL Apply, la cual, a diferencia de Redo Apply, transforma los redo de datos recibidos en instrucciones SQL antes de ser aplicados y luego ejecuta dichas instrucciones en el sitio standby.

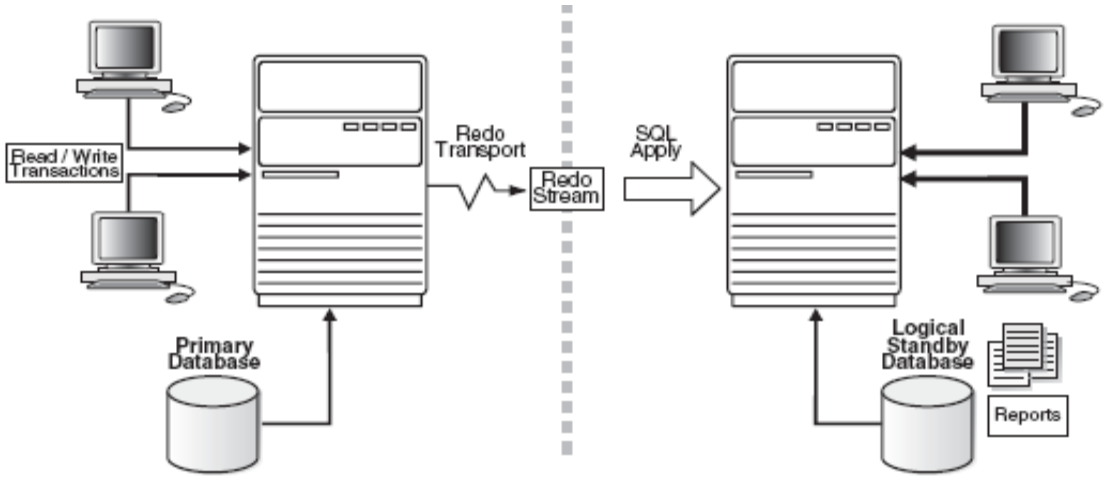

Figura 5: Aplicación de los redo de datos en una base de datos Standby lógica.

Los Servicios Apply automáticamente aplican redo a las standby para mantener la sincronización con la base de datos primaria y permitir transaccionalmente acceso consistente a los datos. Por defecto los Servicios Apply esperan a que lleguen todos los redolog archivados a la standby para después aplicarlos sobre la misma. Aunque también se puede realizar una configuración habilitando la propiedad real-time apply como se menciona anteriormente, para que los relog sean aplicados una ves llegado al sitio standby.

2.1.1.4.3 Servicio de transición de roles

- Una base de datos Oracle opera en uno de los siguientes roles exclusivamente: primario o standby. El servicio de transición de roles es el encargado de controlar los cambios de roles de las bases de datos que conforman la configuración Data Guard. Esta operación se lleva a cabo utilizando dos operaciones básicas, un **switchover** o un **failover**.

- Un switchover es la operación que permite invertir los roles entre una base de datos primaria y alguna de sus standby, es importante destacar que esta operación ocurre sin pérdida de datos alguna. Generalmente es realizado para ejecutar un mantenimiento al sistema primario. Esta transición ocurre sin tener que volver a crear ninguna de las dos bases de datos.

- Un failover, en cambio ocurre cuando la base de datos primaria no esta disponible. Esta es realizado solo ante eventos catastróficos de la base de datos primaria y el resultado es una transición de una base de datos standby a primaria.

2.1.1.5 Data Guard Broker

- Es el componente de administración y monitoreo, distribuido como un marco de trabajo de administración, que ayuda a crear, controlar y monitorear las configuraciones de Data Guard.
- Automatiza todo el proceso manual de configuración y una vez creada la configuración, monitorea la actividad y disponibilidad de todos los sistemas en la configuración.
- Simplifica las operaciones de failover y switchover permitiendo que sean invocados desde un simple clic en el Enterprise Manager o un simple comando en el DGMGRL.
- Cuando la característica fast-start failover es habilitada, el Data Guard Broker determina si es necesario un failover y lo inicia automáticamente sin necesidad de un administrador.

Observador (Observer)

Para que se inicie un failover a través del fast-start failover es necesario tener iniciado un observador (observer), el cual está integrado al componente del lado del cliente DGMGRL y típicamente corre sobre una infraestructura diferente donde se encuentra la base de datos primaria o standby. El observador constantemente monitorea el entorno fast-start failover para asegurar que el sitio primario esté disponible, el principal objetivo del observer es mejorar la alta disponibilidad reduciendo el tiempo de una intervención humana para realizar un failover manual.

Propiedades para poder habilitar el fast-start failover

FastStartFailoverTarget = 'base de datos standby': Donde se especifica cual será la base de datos standby que pasará a ocupar el rol primario en caso de falla.

LogXptMode = SYNC | ASYNC: Esta propiedad permite cambiar el servicio de transporte de redo de a SYNC o ASYNC.

- **ASYNC:** Especifica que se van a generar los redo de datos por una transacción después que se haga un commit.
- **SYNC:** Especifica que se van a generar los redo de datos por una transacción antes que se haga un commit.

FastStartFailoverThreshold = seg: Especifica la cantidad de segundos que el observador esperara cuando el sitio primario está inhabilitado para poder iniciar un failover.

FastStartFailoverPmyShutdown = true | false: Si se especifica True el sitio primario hará un shutdown cuando se terminen los seg definidos en **`FastStartFailoverThreshold`**.

Para que la característica Fast-Start failover sea activada satisfactoriamente el observador debe estar iniciado.

2.1.2 Modos de protección del Data Guard

En algunas situaciones una empresa o entidad importante no puede permitirse el lujo de perder sus datos independientemente de las circunstancias. En otras situaciones, la disponibilidad de la base de datos puede ser más importante que cualquier posible pérdida de datos en el caso improbable de un fallo múltiple. Por último, algunas aplicaciones necesitan de un máximo rendimiento de sus bases de datos, y por lo tanto, puede tolerar una pequeña pérdida de datos si cualquier componente falla. A continuación se describen los tres modos de protección de los datos que brinda Data Guard.

- **Protección máxima:** Dictamina que las modificaciones que se realizan en la base de datos primaria tienen que estar disponibles en al menos una de las bases de datos standby. Garantiza que no ocurra ninguna pérdida de datos ante un fallo de la base de datos primaria, para ello los redo tienen que ser escritos en el redolog online local y en el redolog standby de al menos una base de datos standby antes de hacer efectiva la transacción (commit). Si no existe comunicación con ninguna de las bases de datos standby o por alguna causa la escritura de los redo no puede efectuarse, entonces se descarga (shutdown) la instancia primaria.
- **Máxima disponibilidad:** Dictamina al igual que la anterior, que las modificaciones que se realizan en la base de datos primaria tienen que estar disponible en al menos una de las bases de datos

standby. Pero en este caso ante un fallo de la comunicación o la escritura de los redo la base de datos primaria continúa disponible, ocurriendo una transición del modo de protección de máxima disponibilidad hacia la de máximo rendimiento hasta que el fallo se corrija y todos los gap en los ficheros redologs sean resueltos; después de ello entonces la base de datos primaria vuelve al modo de máxima disponibilidad.

- **Máximo rendimiento:** Dictamina que las modificaciones que se realizan en la base de datos primaria estarán disponible en el sitio standby si la red esta activa. Este modo garantiza el mayor nivel de protección de los datos sin afectar el rendimiento de la base de datos primaria. Este permite que una transacción se haga efectiva una vez que los redo se hayan escrito al menos en el redolog online local; la escritura hacia los sitios standby se realiza asincrónicamente. Cuando el enlace de red tiene buen ancho de banda y confiabilidad, este modo proporciona un nivel de protección cercano al de máxima disponibilidad con un mínimo impacto en el rendimiento de la base de datos primaria.

2.1.3 Consideraciones sobre la estructura de directorio en una Base de datos standby

La estructura de directorio de las distintas bases de datos standby es importante, dado que determina el camino donde se encuentran los ficheros de datos, los ficheros redologs archivados y los ficheros redologs standby. Si es posible, las bases de datos standby y la base de datos primaria deben tener el mismo nombre y la misma estructura de directorio para los ficheros de datos, los ficheros redologs y los controlfiles, en correspondencia con la Optima Arquitectura Flexible (*OFA, por sus siglas en ingles*).

Si no se desea tener la misma estructura de directorio, entonces se tienen que definir los parámetros de conversión de nombre de fichero (filename) o renombrar los datafile. A continuación se describen tres casos diferentes:

1. Una base de datos standby en el mismo sitio que la primaria usando una estructura de directorio diferente a la del sitio primario. Las consecuencias para este caso son las siguientes:
    - Establecer el parámetro de inicialización **`DB_UNIQUE_NAME`**.
    - Renombrar los datafiles de la Base de datos primaria en el controlfile de la base de datos standby. Este proceso se puede ejecutar manualmente o automáticamente definiendo el

parámetro de inicialización **DB_FILE_NAME_CONVERT** y el parámetro de inicialización **LOG_FILE_NAME_CONVERT**.

- En este caso, la standby no protege contra desastres que destruyan el sistema en el cual residen ambas, pero posibilita el switchover para mantenimientos planificados.

1. Una base de datos standby en un sitio separado que usa la misma estructura de directorio que la del sitio primario.
   - No se necesitan renombrar ya sea manualmente, ni automáticamente los datafiles.
   - Localizando la standby en un medio físico separado, se salvaguardan los datos de la primaria contra desastres que destruyan el sistema primario.
2. Una base de datos standby en un sitio separado que usa una estructura de directorio diferente a la del sitio primario.
   - Establecer el parámetro de inicialización **DB_UNIQUE_NAME**.
   - Renombrar los datafiles de la Base de datos primaria en el controlfile de la standby. Este proceso se puede ejecutar manualmente o automáticamente estableciendo el parámetro de inicialización **DB_FILE_NAME_CONVERT** y además el parámetro de inicialización **LOG_FILE_NAME_CONVERT**.
   - Localizando la standby en un medio físico separado, se salvaguarda los datos de la primaria contra desastres que destruyan el sistema primario.

La figura 6 representa una base de datos standby en el mismo sitio que la primaria usando una estructura de directorio diferente a la del sitio primario, otra base de datos standby en un sitio separado que usa la misma estructura de directorio que el sitio primario, y por ultimo una base de datos standby en un sitio separado que usa una estructura de directorio diferente al del sitio primario.

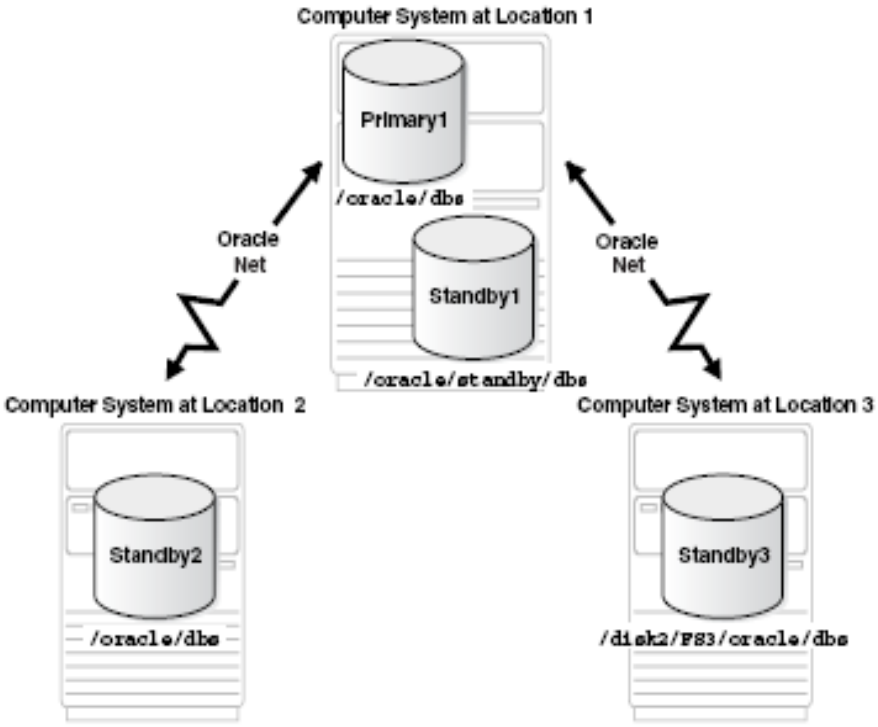

Figura 6: Localizaciones y estructuras de directorio.

2.1.4 Modo de operación de una base de datos standby

Data Guard mantiene una base de datos standby física mediante los servicios de Redo Apply. Cuando la base de datos no está realizando recuperación, puede ser abierta en modo solo lectura. Si está configurado Flashback (a partir del Oracle10), entonces la base de datos puede ser abierta temporalmente en modo de lectura y escritura.

- Modo de recuperación controlada (Manage Recovery Mode): Indica si los redo de datos están siendo aplicados desde los ficheros redolog archivados o directamente desde los ficheros redolog standby usando los mecanismos de recuperación de Oracle. La operación de recuperación aplica los cambios de los bloques redo a los bloques de datos usando las direcciones de los bloques de datos

- Modo abierto en solo lectura: Una base de datos standby puede ser abierta en modo solo lectura. Mientras está abierta, la base de datos standby puede continuar recibiendo redo de datos, pero la aplicación de los mismos desde los ficheros log es diferido hasta que la base de datos pase a modo de recuperación controlada.

- Modo abierto en lectura/escritura: Una base de datos standby puede también ser abierta en lectura/escritura con propósitos de desarrollo, prueba, ejecución de reportes, etc. Mientras se encuentra en este modo, la misma no recibe datos redo desde la base de datos primaria y no puede proveer protección ante desastres. Cuando la base de datos es abierta, Data Guard guarda el punto en que se encuentra, y cuando la base de datos es retornada hacia el punto de origen, sincroniza la base de datos standby con la primaria, sin necesidad de volverla a crear.

2.1.5 Redologs Online, Redologs archivados y Redologs standby

Las estructuras más importantes para las operaciones de recuperación del Data Guard son los redologs online, los redologs archivados y los redolos standby. Los redo de datos transmitidos desde la base de datos primaria son recibidos por el proceso RFS en el sistema standby, en donde dicho proceso escribe los redo de datos en los ficheros logs archivados o en los ficheros redologs standby. La transmisión de redo es esencial para mantener la consistencia transaccional de la base de datos primaria y la standby y tanto los redologs online como los redologs archivados son requeridos en un ambiente Data Guard.

Redologs Online*:* Cada instancia de una base de datos primaria o standby lógica tienen que tener un redolog online para proteger la base de datos en caso de fallo. Las bases de datos standby físicas no lo usan, dado que estas no pueden operar en modo escritura/lectura.

Redologs archivados: Son requeridos dado que es el método usado para tener consistente transaccionalmente una base de datos standby con la base de datos primaria. Todos los tipos de bases de datos lo usan.

Redologs standby: Es similar a los redolos online, excepto que estos almacenan redo de datos recibidos desde otra base de datos. Estos son requeridos si se desean implementar:

- Los niveles de protección de datos máxima y de disponibilidad máxima.

- Aplicación en tiempo real.
- Destinaciones en cascada.

2.1.6 Arquitectura de los procesos en una base de datos standby física

Como se muestra en figura 7 Data Guard utiliza una serie de procesos de Oracle para lograr una alta disponibilidad y una buena recuperación ante desastres. En el sitio primario se podrá encontrar el servicio de transporte de redo y en el sitio standby se puede apreciar el servicio de aplicación, ambos utilizan una serie de procesos que seguidamente serán explicados.

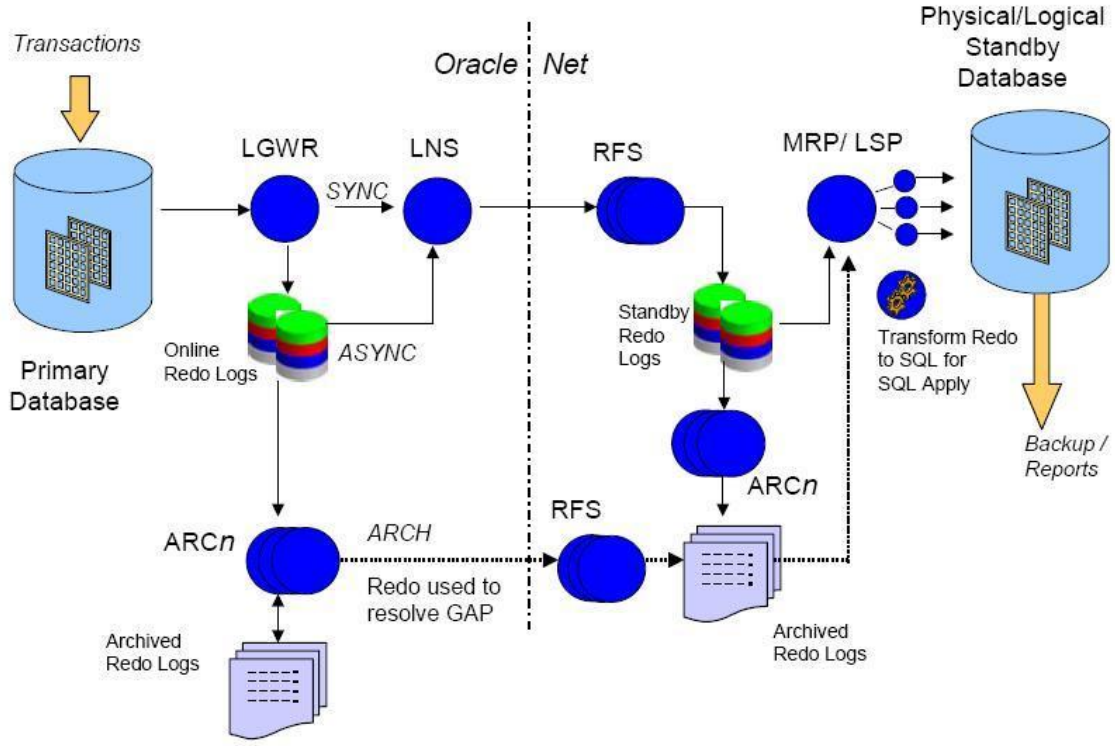

Figura 7: Procesos de servicios de transporte de redo y servicios de aplicación.

En el sitio primario el servicio de transporte de redo usa los siguientes procesos:

LGWR (log writer process): Colecciona todos los redo transaccionales y actualiza los redologs online. Este proceso además puede crear los redolog archivados localmente y transmitir los redo online a las bases de datos standby sincrónica o asincrónicamente a través del LNS.

LNS (Log Writer Network Server): Este proceso aisla al LGWR de la sobrecarga en la transmisión y las interrupciones de la red.

ARC (archiver process): Crea una copia de los redolog online ya sea para el sitio local o las bases de datos remotas standby de red

En el sitio standby el servicio de aplicación usa los siguientes procesos:

RFS (Servidor de fichero remoto): Es el proceso que recibe los redologs archivados desde la base de datos primaria.

ARC (archiver process): Archiva los redologs standby a ser aplicados por el proceso MRP.

MRP (manager recovery process): Aplica la información de los redologs archivados en la base de datos standby física.

LSP (Logical Standby Process): Aplica la información de los redologs archivados en la base de datos standby lógica a través de la traducción del SQL.

2.1.7 Parámetros de inicialización

Oracle en su configuración presenta una base de datos para almacenar toda la información y una instancia que contiene todo un conjunto de procesos que operan en los datos almacenados. Una instancia debe de estar iniciada para leer o escribir información en la base de datos, cuando una instancia no esta funcionando sus datos están seguros en la base de datos pero no pueden ser accedidos por ningún usuario ni aplicación.
Las instancias de Oracle utilizan varios parámetros de inicialización para poder arrancar. A continuación se muestran varios que son muy importantes para configurar el Data Guard.

DB_NAME: Se especifica un nombre de 8 caracteres.
DB_UNIQUE_NAME: Especifica el nombre único de cada base de datos. Este es el nombre que se mantiene con la base y no cambia independientemente del rol en que se desempeña.

LOG_ARCHIVE_CONFIG: Especifica el atributo DG_CONFIG donde se listan los nombres de las Bases de Datos primaria y standby en la configuración de Data Guard especificados en el parámetro de inicialización DB_UNIQUE_NAME de cada base de datos.

LOG_ARCHIVE_DEST_n: Este parámetro de inicialización define hasta 10 (donde n puede ser 1,…., 9, 10) destinos, cada uno debe especificar el lugar donde se archivaran los redo de datos. Se pueden establecer varios atributos para controlar diferentes aspectos como: el transporte de redo desde la base de datos de producción o primaria hacia un sitio standby y otros que se van a explicar seguidamente:

- **AFFIRM | NOAFFIRM:** Controla si o no el servicio de transporte de redo usa sincrónicamente o asincrónicamente para escribir los redo de datos hacia los archived_log o redolog archivados, por defecto esta en NOAFFIRM.
- **ALTERNATE = destino**: Especifica un archivo de destino alternativo para ser utilizado cuando el destino original falla.
- **ASYNC | SYNC**
    - **ASYNC:** Especifica que se van a generar los redo de datos por una transacción después que se haga un commit.
    - **SYNC:** Especifica que se van a generar los redo de datos por una transacción antes que se haga un commit.
- **COMPRESSION= {ENABLE | DISABLE}:** Indica si se va a comprimir la red o no.
- **DB_UNIQUE_NAME = nombre:** Se debe especificar un nombre único para la base de datos en este destino.
- **DELAY [=minutes]:** Especifica un lapso de tiempo entre el momento que se van a archivar y el momento que se van a aplicar los redo de datos en un sitio standby físico. No se puede establecer

este atributo para una base de datos standby lógica, si se especifica este atributo y no se le da un tiempo por defecto es 30 min.

- **DEPENDENCY=destino:** Define un archivo de destino para recibir los redo de datos en nombre de varios destinos.
- **LOCATION=directorio de disco local | SERVICE=nombre del servicio**
  - **LOCATION=directorio de disco local**: Especifica un destino o un directorio de un sistema de archivos locales o los grupos de discos del Administrador de Almacenamiento de Oracle que servirá como el área de recuperación flash(FLASH RECOVERY AREA).
  - **SERVICE=nombre del servicio**: Especificar un servicio de Oracle Net válido que identifica la instancia de base de datos Oracle remota para enviar los redo de datos. Cada destino debe especificar bien el lugar o el atributo SERVICIO. No hay ningún nombre de servicio de red por defecto.
- **MANDATORY:** Especifica que la transmisión de redo de datos hacia el destino debe tener éxito antes de que los online redo log puedan estar en disposición de ser reutilizados. Si no se especifica este atributo el destino es opcional.
- **MAX_CONNECTIONS:** Especifica el número máximo de conexiones de red que se utiliza para transmitir los redo de datos hacia el destino, por defecto es 1.
- **MAX_FAILURE:** Controla el número de veces consecutivas que el servicio de transporte de redo intenta restablecer la comunicación y transmitir los redo de datos hacia un destino fallido.
- **NET_TIMEOUT= segundos:** Especifica el número de segundos que el proceso Log Writer espera por el estado del proceso de servicio de red (LNSn) antes de dar por terminado el proceso de conexión de red. El valor predeterminado es 30 segundos.
- **NOREGISTER:** Indica que la ubicación de los redo log archivados no se registran en el destino correspondiente.

- **REOPEN [=segundos]:** Especifica el número mínimo de segundos antes de que el archivador procesos (ARCn) o el LGWR deben tratar de nuevo a acceder a un destino fallido, el valor por defecto es 300 segundos.
- **VALID_FOR=(redo_log_type, database_role):** Identifica cuando el servicio de transporte de redo puede transmitir los redo de datos hacia los destinos basado en los siguientes factores:
    - redo_log_type: Especifica que tipo(online redo log, standby redo log, o ambos)archivos logs quieres archivar en el destino.
    - database_role: Especifica para que rol(base de datos primaria o standby) quieres archivar los redo de datos en ese destino.

LOG_ARCHIVE_DEST_STATE_n: Específica ENABLE para permitir al servicio de transporte de logs a transmitir los redo de datos a la destinación especificada.

REMOTE_LOGIN_PASSWORDFILE: Indica que el usuario SYS tiene el mismo password tanto en la Base de Datos primaria como standby. Los valores recomendados son EXCLUSIVE o SHARED.

LOG_ARCHIVE_MAX_PROCESS: Especifica la cantidad máxima de procesos archivadores (ARCs) que se desean que sean invocados inicialmente por el Oracle. El valor implícito es 4.

FAL_SERVER: Indica el nombre del servicio Oracle Net del servidor FAL (normalmente la base de datos que se encuentra corriendo en el rol primario). Este parámetro indica que cuando la base de datos que originalmente estaba cumpliendo un rol primario se encuentra en el rol standby, este usa el servidor FAL que se ejecuta en la base de datos que paso que ser la de producción.

FAL_CLIENT: Especifica el nombre del servicio Oracle Net del servidor de base de datos donde se copiaran los files redologs archivados perdidos en la Base de Datos standby.

STANDBY_FILE_MANAGEMENT: Si se Indica AUTO cuando los ficheros de datos sean creados o eliminados de la Base de Datos primaria, los correspondientes cambios sean hechos automáticamente en la Base de Datos standby.

2.2 Características Generales de ESX Server

ESX Server inserta directamente una capa de software en el hardware del ordenador o en el sistema operativo host. Esta capa de software crea máquinas virtuales y contiene un monitor de máquina virtual o "hipervisor" que asigna recursos de hardware de forma dinámica y transparente, para poder ejecutar varios sistemas operativos de forma simultánea en un único ordenador físico. VMware ofrece una sólida plataforma de virtualización que puede ampliarse por cientos de dispositivos de almacenamiento y ordenadores físicos interconectados para formar una infraestructura virtual completa.

Arquitectura al nivel más bajo de hardware

ESX Server inserta una sólida capa de virtualización directamente en el hardware del servidor para brindar un rendimiento casi nativo de la máquina virtual, además de confiabilidad y escalabilidad, como se muestra en la Fig. 8

Figura 8 Representación de ESX Server en bajo nivel.

Virtualización de la CPU

Hace posible que aumente la utilización del servidor sin arriesgarse a que servicios críticos se vean expuestos a la falta de recursos de la CPU. ESX Server utiliza una programación inteligente de procesos y balanceo de carga a través de los procesadores disponibles a fin de administrar la ejecución del procesamiento de la máquina virtual.

2.2.1 Virtualización para el almacenamiento de información

Aprovecha el almacenamiento de información compartido de alto rendimiento para centralizar el almacenamiento de archivos de la máquina virtual a fin de brindar mayor capacidad de administración, flexibilidad y disponibilidad.

Archivos de disco virtual

Simplifica la administración del almacenamiento de información de la máquina virtual. Las máquinas virtuales ven sus propios archivos de disco virtual privado. Sin embargo, fuera de la máquina virtual, los discos virtuales son simplemente archivos de gran tamaño a los cuales no se les puede hacer respaldo ni se pueden copiar, mover ni archivar con la misma facilidad que cualquier otro archivo.

Filesystem de cluster VMFS

Almacena archivos de discos virtuales en almacenamiento de información compartido de alto rendimiento, como Fibre Channel o SAN iSCSI. VMFS es un filesystem de cluster que permite que múltiples instalaciones de ESX Server tengan un acceso rápido y concurrente al mismo almacenamiento de máquina virtual. Dado que las máquinas virtuales son independientes del hardware y pueden trasladarse entre servidores, VMFS asegura que los servidores individuales no sean puntos únicos de falla y permite el balanceo de los recursos entre diversos servidores.[14]

Como se muestra en la fig. 9 se puede analizar cómo es el almacenamiento en Filesystem de cluster VMFS.

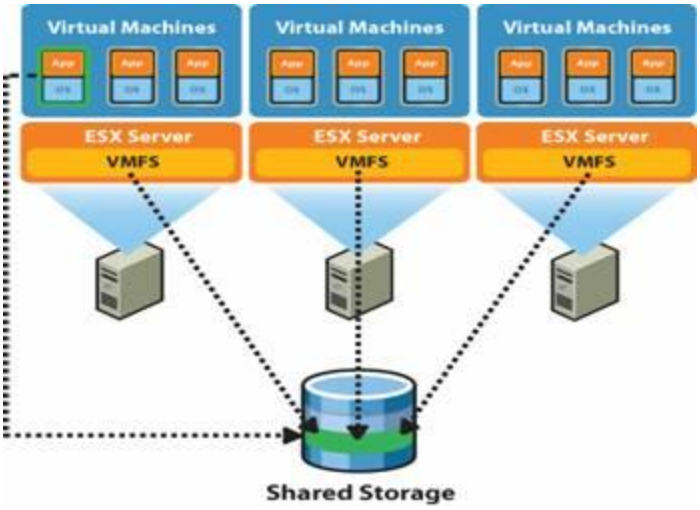

Figura 9 Almacenamiento en Filesystem de cluster VMFS.

Administrador de volúmenes lógico

Administra la interacción entre los arreglos de discos de almacenamiento físico y VMFS con flexibilidad y confiabilidad. Permite la modificación de tamaño de volúmenes dinámicos, donde agrega múltiples discos de almacenamiento de información a un solo volumen VMFS y cambia el tamaño de los LUNs y agrega nuevos LUNs heterogéneos a un volumen VMFS de forma inmediata. También hace posible el cambio de firma de volumen automático. Simplifica el uso de la tecnología de copia instantánea basada en el arreglo de discos. El cambio de firma reconoce automáticamente los volúmenes VMFS de copia instantánea. Al igual que permite la operación parcial en línea donde los volúmenes siguen funcionando a pesar de la pérdida de algunos LUNs.

Mapping de dispositivos raw

De manera opcional, es posible hacer mapping de LUNs SAN directamente a una máquina virtual con el fin de permitir el clustering de aplicaciones y la tecnología de copias instantáneas basadas en el arreglo de discos, mientras se aprovecha los beneficios que brinda la capacidad de administración de VMFS.

Consolidación de HBAs Fibre Channel

Comparte componentes costosos de almacenamiento de información entre varias máquinas virtuales mientras mantiene la tolerancia a las fallas de hardware.

I/O de escritura

Garantiza la recuperación precisa de máquinas virtuales en el caso de una falla del servidor. Las I/Os de escritura permiten que las máquinas virtuales tengan las mismas características de recuperación que un sistema físico que ejecuta el mismo sistema operativo.

Inicio desde SAN

Realiza configuraciones sin disco de servidores en módulo (blade) y montados en rack mediante el inicio desde SAN. Simplifica los respaldos y la recuperación ante desastres al eliminar la necesidad de hacer respaldos separados de los discos locales del servidor conectado.

Herramientas del VMware (VMware Tools):

Son un paquete de programas que permiten el mejor rendimiento de las máquinas virtuales, ya que este paquete se instala en los sistemas operativos de las máquinas virtuales. Es casi obligatorio la instalación de estas herramientas aunque si no se instala en los PC virtualizadas no sucede nada, solamente se pierde rendimiento y funcionalidad en ellas.

Dentro del paquete se encuentran los siguientes programas:

- Servicios: Este permite la sincronización se los sistemas operativos de las máquinas virtuales con el sistema del Host. Para clientes Windows se nombra VMwareService y para clientes Linux se nombra VMware-guestd al igual para clientes Solaris.
- Drivers VMware: Conjunto de drivers como el vmxnet, el SVGA, Bus Logic SCSI, drivers de mouse de VMware, driver para el control eficiente de la memoria de las máquinas virtuales y el driver sync.
- Panel de control: Permite que se conecten o desconecten dispositivos virtuales, así como la modificación de algunas propiedades.
- Proceso de Usuario de VMware: Permite copiar y pegar textos entre las máquinas virtuales y el host. Para clientes Windows es el VMwareUser y para clientes Linux es el VMware-user.

2.2.2 Virtualización para redes

Conecta en red máquinas virtuales como si fueran máquinas físicas. Crea redes complejas dentro de un solo ESX Server para implementaciones de producción o para fines de desarrollo y pruebas.

NICs virtuales

Hace posible la configuración de cada máquina virtual con uno o más NICs virtuales. Cada una de estas interfaces de red puede tener su propia dirección IP e incluso su propia dirección MAC. Como resultado, no es posible distinguir entre las máquinas virtuales y las máquinas físicas desde el punto de vista de la red. Dentro de las posibilidades de NICs virtuales que brinda ESX Server, se encuentran:

Vmxnet

Permite la interacción directamente con el VMkernel. Permite que el uso de CPU sea mínimo con respecto al otro dispositivo virtualizado: VLANCE.

Ventajas de usar Vmxnet.

- Es un dispositivo de alto rendimiento que optimiza la Red dentro de las Máquinas Virtuales.
- Recomendado a la hora de tener máquinas virtuales con una conectividad elevada y rápida.

Desventajas de Usar Vmxnet

- Requiere la instalación del paquete de VMware Tools.
- No todos los sistemas Operativos soportan este hardware virtual.

Vlance

Es una pieza compatible para hardware virtual sobre la arquitectura AMD PCNET-32 y que esta soportada por casi todos los Sistemas Operativos que se hospeden en las máquinas virtuales creadas por ESX Server.

Ventajas de usar Vlance. [15]

- Es compatible con los dispositivos AMD PCNET-32

- Presenta una alta compatibilidad con la mayoría de los Sistemas Operativos.
- Se instala por defecto en el Sistema Operativo Invitado.

Desventajas al usar Vlance.

- Menor rendimiento comparado con vmxnet.
- Uso mayor del CPU comparado con vmxnet.

Flexible

Es soportado en las máquinas virtuales creadas en servidor de ESX 3.0 o posterior y este corre en sistemas operativos de huésped de 32-bit. El adaptador flexible funciona como un adaptador de Vlance si las herramientas de VMware no son instaladas en la máquina virtual, y como un adaptador de red de Vmxnet si las herramientas de VMware son instaladas en la máquina virtual.

E1000

Un adaptador virtual que emula una tarjeta de red de E1000. Es el tipo de adaptador implícito para las máquinas virtuales creadas en servidor de ESX 3.0 o posterior y que corren sistemas operativos de huésped de 64 bit.

Enhanced Vmxnet

Una versión mejorada del adaptador de Vmxnet. Requiere que las herramientas de VMware son instaladas en la máquina virtual.

Switches virtuales

Esta característica presente en ESX Server, permite crear una red simulada con switches virtuales capaces de conectar máquinas virtuales. Estos switches virtuales permiten construir cualquier cantidad de puertos de 8 hasta 1016, y el número máximo de switches que se pueden construir es 248.

En la siguiente figura se expone claramente el funcionamiento de los Switch Virtuales en ESX Server. Cada Switch virtual estará conectado a las Tarjetas de Red Físicas del servidor, en el cual se había instalado el ESX Server, o a su vez lo puede estar en una Tarjeta de Red Virtualizada. La conectividad del

entorno de virtualización dependerá de la forma en que se configuren las Máquinas Virtuales y los switches.

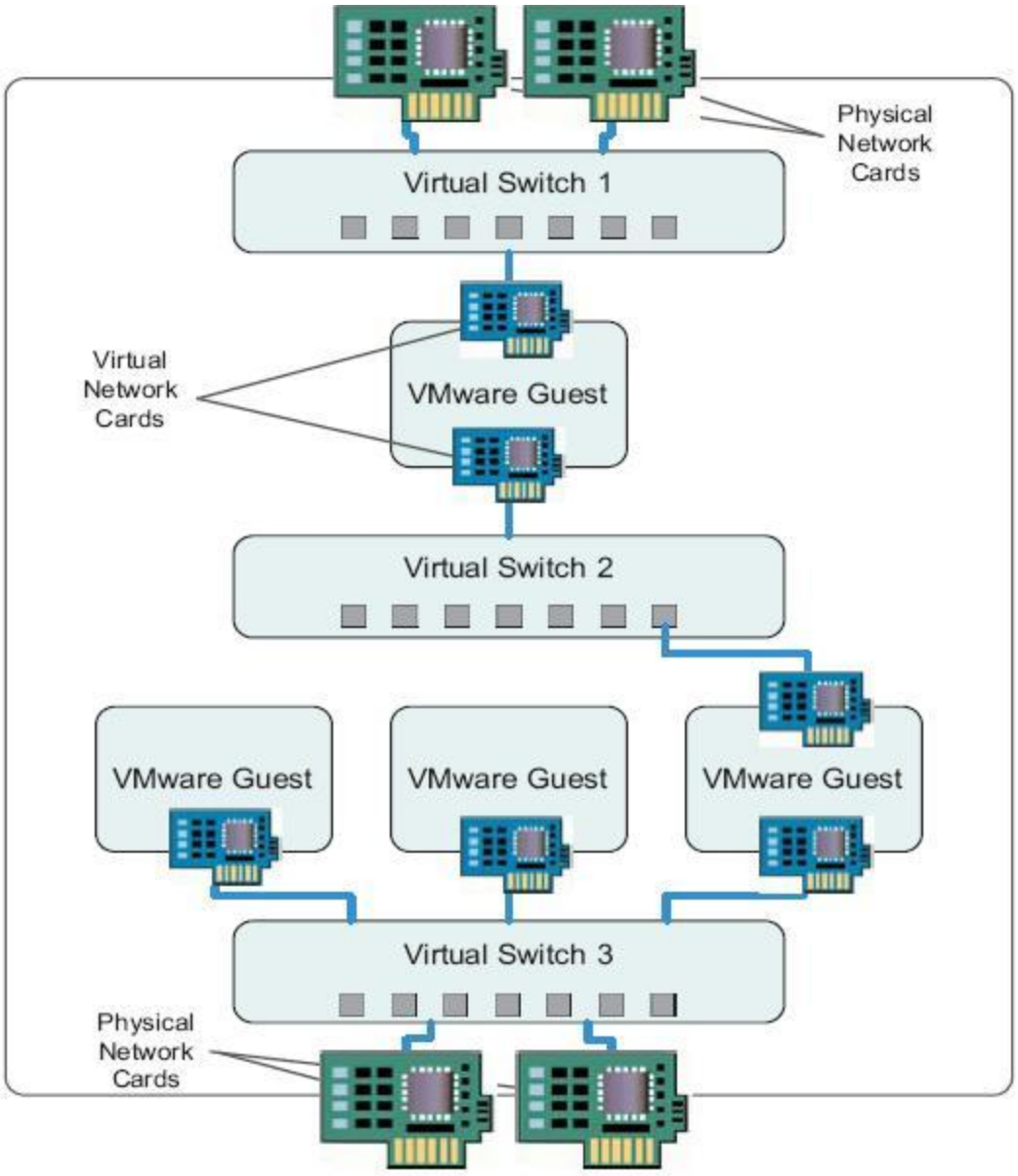

Figura 10. Representación de cómo ESX Server Usa los Switch Virtuales.

Políticas ampliadas de configuración de puertos

Simplifica la configuración de puertos al utilizar un solo objeto de configuración a través de un gran grupo de puertos. El objeto de configuración especifica toda la información necesaria para habilitar un puerto: Política de formación de equipos NIC por puerto, etiquetado de VLAN, seguridad de Nivel 2 y manejo de tráfico.

VLAN

Hace posible la creación de una VLAN donde superpone una LAN lógica sobre las LANs físicas para aislar el tráfico de la red y así aumentar la seguridad y la segregación de carga. Las VLANs son compatibles con las implementaciones de VLAN estándar de otros proveedores. Además se puede modificar las configuraciones de red sin tener que cambiar las configuraciones de switch y cableado reales. Las VLANs mantienen el tráfico de transmisión limitado a la VLAN, disminuyendo la carga de red de los paquetes de transmisión en otros switches y segmentos de la red.

2.2.3 Rendimiento y Escalabilidad

ESX Server 3 ofrece rendimiento y escalabilidad sin precedentes. Es posible virtualizar incluso aplicaciones de producción que consumen grandes cantidades de recursos, tales como bases de datos, ERP y CRM.

Rendimiento mejorado de la máquina virtual

Las mejoras en el rendimiento de ESX Server se logran a través de lo siguiente:

- Escalabilidad de varias máquinas virtuales.
- Manejo mejorado de la unidad de administración de memoria (MMU).
- Significativas mejoras a la conexión en red.
- Soporte de Native Posix Thread Library (NPTL) de Linux.

Administración avanzada de la memoria

- Aumento forzado de RAM.

- ESX Server aumenta la utilización de la memoria al configurar memoria de la máquina virtual que supera en forma segura la memoria física del servidor. Por ejemplo, la suma de la memoria de todas las máquinas virtuales que se están ejecutando en un servidor con 8 GB de memoria física puede ser de 16 GB. [14]

- Uso compartido transparente de páginas.

  Utiliza la memoria disponible en forma más eficiente al almacenar una sola vez páginas de memoria idénticas entre varias máquinas virtuales. Por ejemplo, si varias máquinas virtuales están ejecutando Windows Server 2003, tendrán muchas páginas de memoria idénticas. El uso compartido transparente de páginas consolida esas páginas idénticas en una sola ubicación en la memoria.

- Aumento de memoria.

  Intercambia memoria en forma dinámica entre máquinas virtuales inactivas y activas. El aumento de memoria induce en forma artificial presión de memoria dentro de las máquinas virtuales inactivas, forzándolas a utilizar sus propias áreas de paginación y a liberar memoria para las máquinas virtuales activas. [14]

Administración de energía mejorada

Disminuye la cuenta de servicios del centro de datos al mejorar la administración de la energía. ESX Server ingresa a un estado de “detención” de bajo consumo de energía cuando una CPU no está programada.

Virtual SMP de 4 vías

Permite que una sola máquina virtual utilice hasta cuatro procesadores físicos en forma simultánea. ESX Server amplía esta característica única de dos a cuatro procesadores. Con Virtual SMP de 4 vías, es posible virtualizar incluso las aplicaciones de software con mayor uso del procesador, como servidores de mensajería y bases de datos.

RAM de 16 GB para máquinas virtuales

Ejecuta las cargas de trabajo que consumen la mayor cantidad de memoria en máquinas virtuales con una memoria limitada ampliada hasta 16 GB.

Soporte para poderosos sistemas de servidores físicos

Aprovecha la ventaja de sistemas de servidores de gran tamaño con hasta 32 CPUs lógicas y 64 GB de RAM para proyectos de recuperación ante desastres y consolidación de servidores a gran escala.

Soporte para hasta 128 máquinas virtuales encendidas

Aprovecha grandes sistemas de servidores para la consolidación y contención de servidores de clase empresarial. La cantidad máxima de máquinas virtuales encendidas es de 128.

Activación en LAN

Hace posible mayores niveles de consolidación al permitir que las máquinas virtuales ingresen al modo de espera cuando no están en uso.

2.2.4 Interoperabilidad en ESX Server

ESX Server es un software de virtualización optimizado, probado rigurosamente y certificado en la gama completa de servidores, almacenamiento de información, sistemas operativos y aplicaciones de software de TI, permitiendo la estandarización en toda la empresa.

Hardware

ESX Server ha sido certificado con los racks, torre y servidores blade líderes en la industria de fabricantes como Dell, HP, IBM, Fujitsu Siemens, NEC, Sun Microsystems y Unisys. [14]

Tiene soporte para sistemas de hardware Sun Microsystems y Unisys, para especificaciones estándar de Intel White-Box y para procesadores de doble núcleo como AMD e Intel.

Almacenamiento de información

ESX Server está certificado con una amplia gama de sistemas de almacenamiento de información de EMC, Dell, HP, IBM y Network Appliance. [14].

- Arreglos de discos de almacenamiento de información heterogéneos donde utiliza una amplia variedad de dispositivos de almacenamiento de información heterogéneos en el mismo volumen VMFS.
- Asume soporte para NAS y SAN iSCSI. Que permite dar soporte para almacenamiento de información compartido de menor costo y más fácil de administrar, ESX Server disminuye aún más el costo total de propiedad de los entornos de TI. Las avanzadas funcionalidades de VMware, como VMotion y VMware HA cuentan con soporte completo en entornos NAS e iSCSI.
- Soporte para SAN Fibre Channel de 4 GB.

Sistemas operativos

ESX Server es la única plataforma de virtualización que soporta una amplia gama de sistemas operativos no modificados, incluidos Windows, Linux, Solaris y Novel NetWare.

Presenta soporte experimental para sistema operativo cliente de 64 bits, y para sistema operativo Solaris 10.

Aplicaciones de software

Ejecuta aplicaciones de software de más de 250 proveedores de software en máquinas virtuales VMware.

Soporte para otros formatos de máquina virtual

Puede ejecutarse en máquinas virtuales creadas en formatos diferentes a VMware. Al usar VMware Virtual Machine Importer, los usuarios pueden ejecutar máquinas virtuales de Symantec® LiveState Recovery, Microsoft® Virtual Server y Virtual PC en ESX Server.

Capacidad de Administración en ESX Server

Las funcionalidades avanzadas de capacidad de administración y uso en ESX Server 3 permiten la administración de la totalidad del entorno de TI virtualizado.

Interfaces de administración compatibles con SMI-S

Monitorizacion del almacenamiento de información virtual usando cualquier herramienta de administración de almacenamiento de información estándar que cumplen SMI-S.

Cliente de infraestructura virtual

En ESX Server se puede administrar máquinas virtuales y VirtualCenter Server con una interfaz de usuario común, una interfaz Web simple donde en versiones anteriores de la herramienta era conocido como Management User Interface o MUI.

Accesos directos a las máquinas virtuales

Con ESX Server se puede configurar la autoayuda para usuarios finales con acceso directo a las máquinas virtuales a través de un explorador Web.

2.2.5 Optimizaciones de Recursos Distribuidos en ESX Server

Administración de recursos para máquinas virtuales

Permite la definición de políticas avanzadas de asignación de recursos para máquinas virtuales a fin de mejorar los niveles de servicio de las aplicaciones de software. Establece los niveles mínimo, máximo y proporcional de usos compartidos de recursos para la CPU, memoria, disco y ancho de banda de la red. Modifica, además, las asignaciones mientras las máquinas virtuales continúan funcionando. Permitiendo que las aplicaciones adquieran más recursos en forma dinámica para adecuar el nivel de rendimiento máximo.

Asignación de prioridades para la capacidad de la CPU

La capacidad de la CPU se asigna a las máquinas virtuales según un “uso compartido justo” y los controles de recursos de la CPU también permiten que se proporcione un nivel mínimo absoluto de

capacidad de la CPU a las máquinas virtuales críticas. Con una asignación de prioridades de tráfico de I/O del almacenamiento de información, ESX Server asegura que las máquinas virtuales críticas reciban acceso prioritario a los dispositivos de almacenamiento de información. Se puede asignar prioridad al tráfico de I/O desde las máquinas virtuales a los discos basándose a un "uso compartido justo".

Con la herramienta **Network Traffic Shaper** asegura que las máquinas virtuales críticas reciban acceso prioritario al ancho de banda de la red. Se puede asignar prioridad al tráfico de la red desde las máquinas virtuales basándose a un "uso compartido justo". Network Traffic Shaper administra el tráfico de red de las máquinas virtuales para satisfacer el ancho de banda máximo, el ancho de banda promedio y las restricciones de los tamaños de ráfaga.

Presentando la opción de un Depósitos de Recursos (resource pool) se puede agregar colecciones de recursos de hardware virtualizados a recursos lógicos unificados que se pueden asignar a máquinas virtuales según la necesidad. Los depósitos de recursos aumentan la flexibilidad y la utilización de las herramientas de hardware.

2.2.6 Alta Disponibilidad en ESX Server

Brinda alta disponibilidad de clase centro de datos para máquinas virtuales donde:

- Almacenamiento de información compartido.

  Elimina los puntos únicos de falla al almacenar los archivos de las máquinas virtuales en almacenamiento de información compartido, como Fibre Channel, SAN iSCSI o NAS. Utiliza funcionalidades de espejado y replicación de SAN para mantener copias actualizadas del disco virtual en los sitios de recuperación ante desastres.

- Transparencia de SAN.

  Usa almacenamiento de información SAN nativo para máquinas virtuales con la misma facilidad y flexibilidad de los archivos de discos virtuales. El mapping de dispositivos raw permite que las máquinas virtuales usen almacenes de datos de LUN SAN estándar además de los LUNs con formato VMFS con fines especiales para archivos de discos virtuales. Descarga el respaldo y la replicación a nivel de archivo de los datos de máquinas virtuales a utilidades basadas en SAN.

Configura fácilmente clusters de máquinas virtuales y físicas con almacenamientos de datos SAN compartidos para obtener una alta disponibilidad rentable.

- Múltiples paths de acceso al almacenamiento de información incorporados.

  Garantiza la disponibilidad del almacenamiento de información compartido con múltiples paths SAN para Fibre Channel o SAN iSCS, y formación de equipos NIC para NAS.

- Formación de equipos NIC mejorada.

  Brinda a cada máquina virtual en red failover de NIC incorporado y balanceo de carga que proporciona una mayor disponibilidad de hardware y tolerancia a fallas. Las nuevas políticas de formación de equipos NIC permiten a los usuarios configurar múltiples adaptadores activos y en espera. La configuración de formación de equipos puede ser diferente para distintos grupos de puertos en el mismo switch virtual y distintos grupos pueden incluso seleccionar diferentes algoritmos de formación de equipos para el mismo equipo.

Seguridad en ESX Server

- Compatibilidad con las prácticas de seguridad de SAN.

  Aplicación de políticas de seguridad con LUN zoning y LUN masking.

- Etiquetado de VLAN.

  Mejora la seguridad de la red al etiquetar y filtrar el tráfico de la red en las VLANs. Limita el alcance de los dominios de transmisión (broadcast).

- Políticas de seguridad de red de nivel 2.

  Impone la seguridad para las máquinas virtuales en el nivel de Ethernet que no está disponible con los servidores físicos. No permite el sniffing de modo descontrolado del tráfico de la red, cambios de dirección MAC y transmisiones MAC de origen falsificado.

Conclusiones

A lo largo del capítulo se estuvieron mencionando y analizando las principales características de las Bases de Datos standby, sus parámetros de inicialización, la manera que Data Guard protege los datos y otras que son de vital importancia a la hora de configurar un entorno Data Guard. También se mencionaron características principales y específicas del software de virtualización ESX Server, como la manera que se emula las máquinas virtuales, la forma en que se almacenan todo lo referente a las PC virtualizadas, la seguridad, el comportamiento de las herramientas del software, entre otras. Estas características de ambas tecnologías, son precisas a la hora de realizarla configuración de un entorno de alta disponibilidad, rápida recuperación ante desastre y buena protección de los datos.

Capítulo 3

Concepción e Implementación del Entorno de Alta Disponibilidad

Introducción

Para poder implementar un entorno donde se logre altos niveles de alta disponibilidad de los datos, así como una buena protección de los mismos; y a su vez tener una rápida recuperación, es necesario configurar primeramente, el entorno de virtualización. Una vez configurado, se pueden crear máquinas virtuales, sobre las cuales puede ser instalado un Sistema Operativo cualquiera.

Durante el desarrollo de este capitulo se exponen los principales elementos de configuración e implementación de un entorno de virtualización sencillo utilizando ESX Server 3.5, así como, la concepción del ambiente Oracle Data Guard para lograr la protección de los datos.

3.1 Configuración de ESX Server 3.5

A la hora de instalar ESX Server 3.5, es necesario hacerlo sobre hardware para servidor, también se tendrán en cuenta los principales requerimientos de hardware que se muestran a continuación: [14]

- Tener más de 2 procesadores de cualquiera de estas tecnologías:
    - Procesador Intel Xeon a 1.5 GHz (o superior) o AMD Opteron (en modo de 32 bits).
    - Procesador Intel Viiv a 1.5. GHz o procesador AMD A64 x2 dual core.
- Memoria RAM mínima de 1GB.
- Presentar dispositivos SCSI, Fibre Chanel o RAID interno.
- Una o más tarjetas de red de cualquiera de estas arquitecturas: Tarjeta de Red Intel PRO/100 o Tarjeta de Red Broadcom NetXtreme 570x gigabit.

Para obtener un buen rendimiento y una mayor seguridad, es recomendado usar tarjetas de red diferentes para la Consola de Sistema Operativo (*COS, por sus siglas en ingles*) y para las máquinas virtuales que se creen sobre ESX Server.

Una vez cumplidos los requerimientos anteriores, se describen a continuación los pasos a seguir para implementar el entorno de virtualización.

ESX Server se puede instalar tanto en modo gráfico, como en modo texto. Para los que tienen pocos conocimientos del trabajo con SO Linux es recomendado usar el modo gráfico que es mucho menos complejo.

Luego de realizar las primeras opciones de instalación, por ejemplo, la de configurar el idioma del teclado y el tipo de mouse, se procede al formateado de las particiones necesarias para llevar a cabo la instalación. El ESX Server requiere como mínimo 3 particiones; por defecto el asistente de instalación crea 3 particiones (/boot, /root y /swap) y añade una 4ta partición extendida, sobre la cual se crean las particiones lógicas (/var/log, /vmfs). Se puede especificar que las 3 primeras particiones (primarias) sean de la capacidad que se estime conveniente siempre que antes se analice cual es la capacidad mínima y la máxima soportada de estas particiones.

Las particiones que crea el ESX server son las mostradas en la siguiente figura y además son las recomendadas:

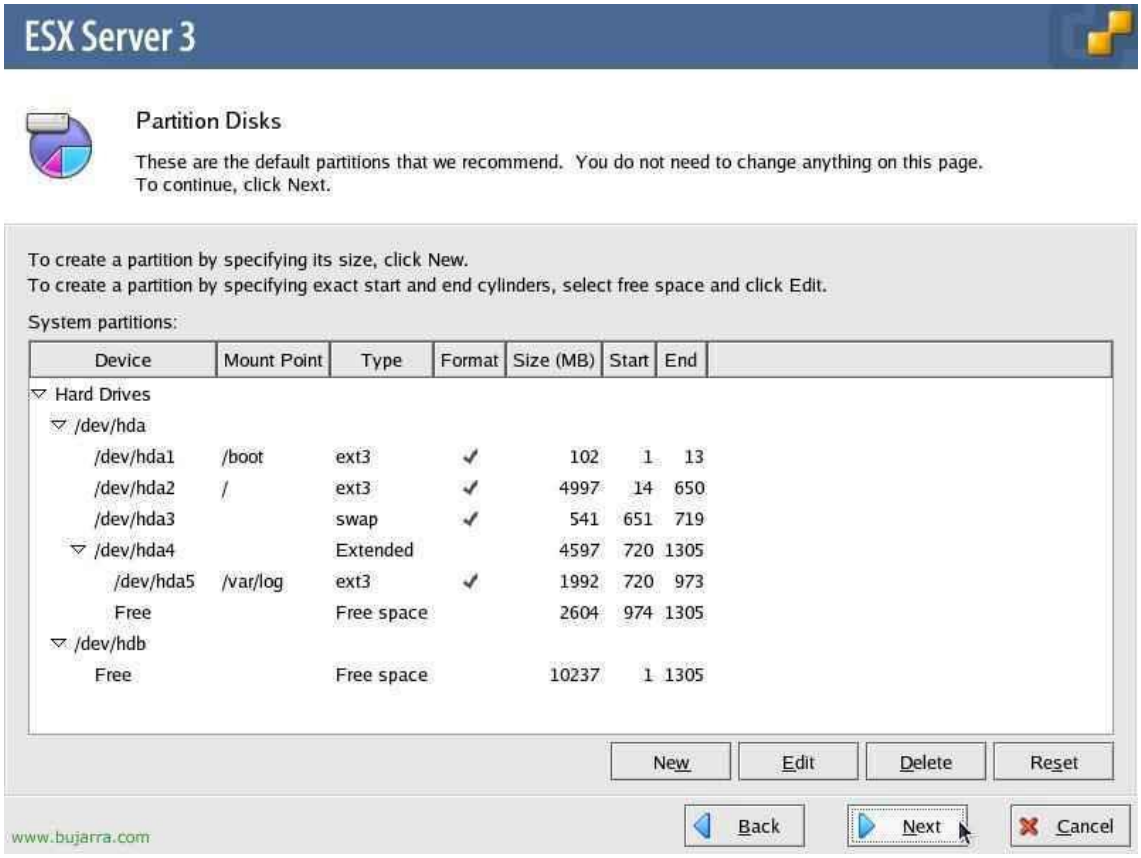

Figura 11: Pantalla particiones del ESX Server.

A continuación se define el tamaño mínimo que debe comprender cada partición:

- **boot:** es la partición dónde estará el arranque del sistema instalado y será del tamaño que se estime conveniente donde la capacidad mínima recomendada para esta es de 100Mb.
- **root**: partición donde se alojará el sistema instalado, es decir, donde estará ubicada la instalación del ESX Server. Para obtener una buena optimización de funcionalidad es importante asignarle como espacio minino 5.0 GB.
- **swap:** partición utilizada para el área de intercambio, es recomendado proporcionarle un tamaño superior a 544 MB.

- **/var/log:** partición que permite el almacenamiento de los archivos Log. El tamaño mínimo es de 2 GB. [15]
- **vmfs:** partición donde se almacenan todos los discos virtuales de las máquinas virtuales y que no permite dentro de él subdirectorios ni almacenamiento que no sean estos archivos. ESX Server recomienda no realizar estas particiones en discos IDE, debido a que no son compatibles. [15]

El paso siguiente es configurar la red para el COS. En la siguiente figura se muestra la pantalla presentada por el asistente de instalación para realizar la configuración:

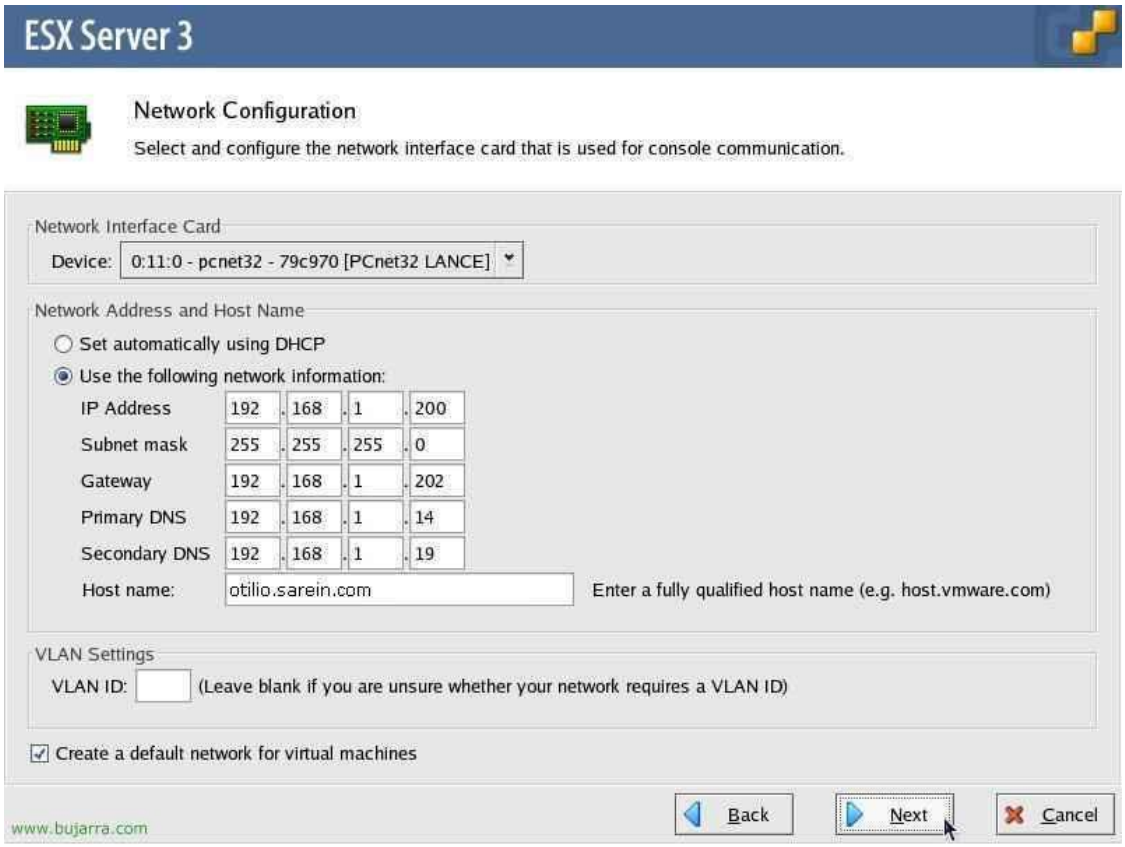

Figura 12: Configuración de la Red del ESX Server

Al configurar la red, se puede hacer asignándole una dirección IP a cualquiera de las tarjetas de red del hardware, por DHCP o manualmente. Se recomienda como buena práctica la asignación de una dirección IP estática. Al darle un IP estático, también se le debe dar la configuración correspondiente a la máscara

de red (Subnet mask), la puerta de enlace (gateway), el Servidor de Nombres de Dominio (*DNS, por su siglas en ingles*) primario y secundario, y por ultimo el nombre de host. En caso de que la red esté dividida en VLANs se le asignará un identificador según la VLAN correspondiente.

Para concluir la instalación de ESX Server, es necesario especificar el nombre de usuario administrador (root) y su contraseña.

Después de haber instalado el ESX Server se puede conectar a través del protocolo HTTP a la dirección del servidor (*http://direccionIPServidor*) (ver Figura 13), desde cualquier PC con acceso al ESX Server. Por el acceso Web se tiene acceso a una página de administración, desde donde se pueden realizar la mayoría de las funciones administrativas del entorno virtual.

También, utilizando el protocolo SSH se puede acceder directamente al COS para desarrollar tareas administrativas. Esta vía de administración se torna un poco más compleja, pero también se pueden crear máquinas virtuales, realizar su administración y todo lo referente a sus configuraciones, al igual que a la configuración del propio ESX Server.

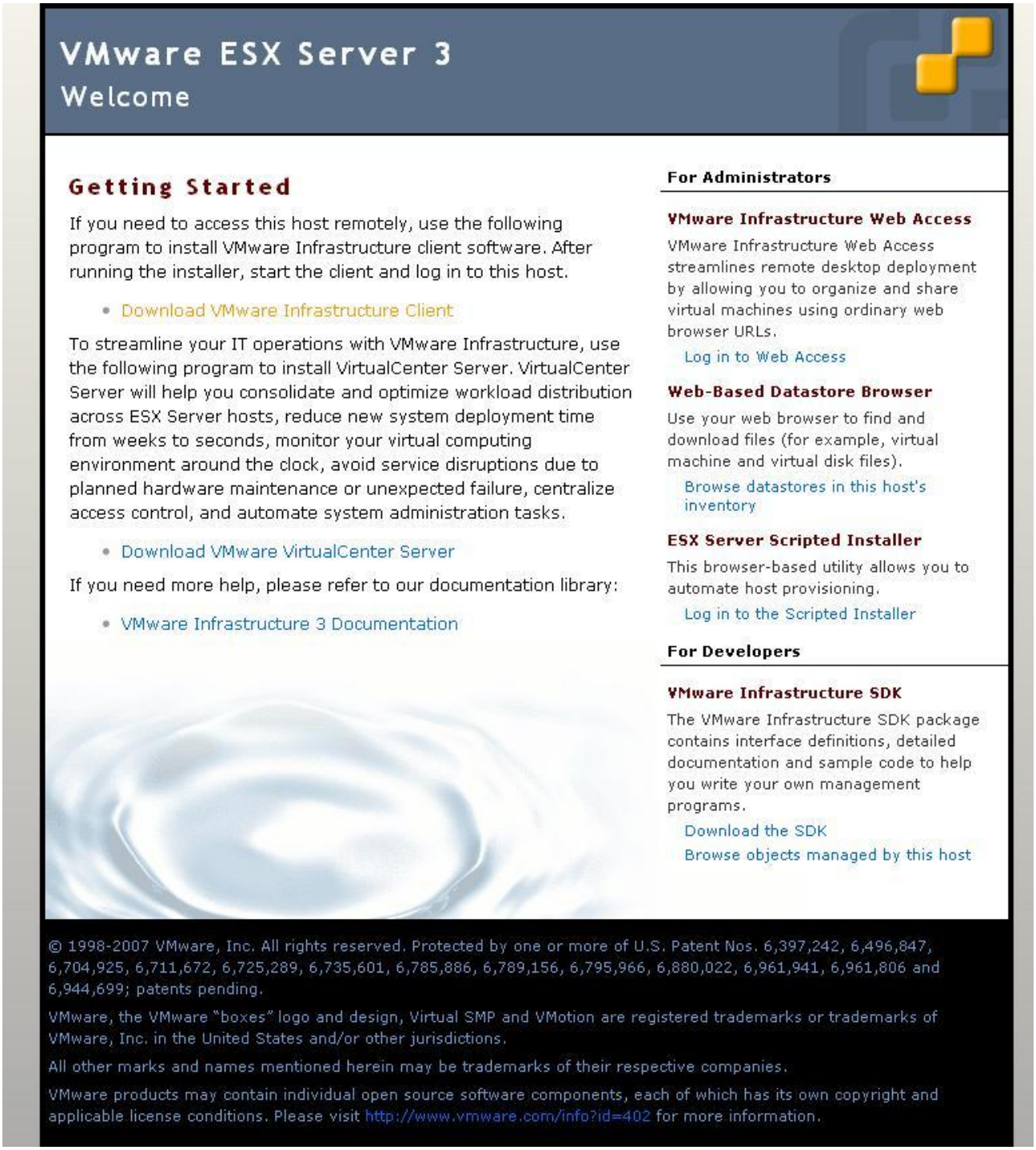

Figura 13. Vista del Acceso Web.

Otra forma de administración del ESX Server se puede lograr utilizando el VMware Infrastructure Client (VIC). Este se puede descargar desde el servicio de administración Web. Con esta herramienta brinda la posibilidad de construir máquinas virtuales, administrarlas, analizar su rendimiento, ver los eventos que están ocurriendo en el servidor ESX, su configuración, los grupos y los usuarios que pueden acceder al ESX Server, etc… de forma fácil y flexible.

En la figura 14 se muestra la pantalla de login del VIC.

Figura 14: Pantalla de login

Después de suministrar un usuario y contraseña correcto, entonces aparecerá la pantalla con los diferentes accesos predefinidos según el rol del usuario utilizado. Ejemplo, figura 15:

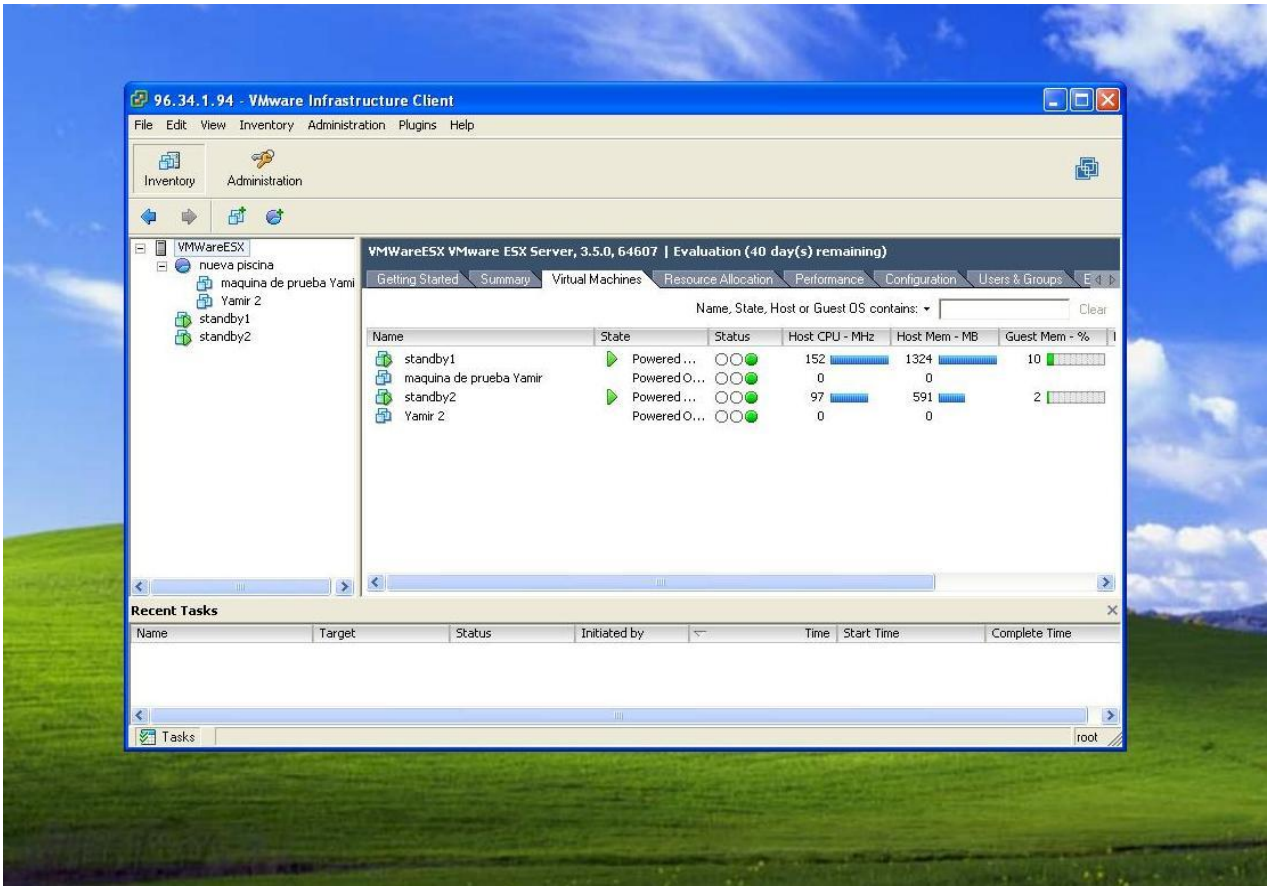

Figura 15: Pantalla de configuración y administración del entorno virtual

A través del VIC se crearán las máquinas virtuales, que utilizando el sistema operativo SuSE Linux y a través de Oracle serán configuradas permitiendo la implementación de los sitios standby para cada sistema primario que se incluya en el entorno de respaldo y recuperación de datos; logrando de esta forma un mayor aprovechamiento del hardware, y una centralización de las bases de datos standby. El valor agregado por el entorno de virtualización está dado por las potencialidades de alta disponibilidad presentes en la tecnología VMware ESX Server.

Cualquier cambio que se desee realizar específicamente para el entorno virtual, se puede hacer desde el VIC, accediendo a la pestaña de configuración, desde aquí se pueden añadir dispositivos de almacenamiento, crear nuevos switches virtuales, nuevas redes virtuales, así como también, habilitar la

opción HiperThreading, configurar el apagado y encendido de las máquinas virtuales, designar si los archivos *swap* se almacenaran en los discos de las máquinas virtuales. *Ver Anexo 1.*

3.2 Configuración de las máquinas Virtuales

Antes de empezar a crear las máquinas virtuales es necesario tener en cuenta los requerimientos de procesamiento que serán asignados al sistema virtual. En la siguiente tabla se muestra las limitaciones a las que están sometidas las máquinas virtuales[16]:

Dispositivos	Cantidad Máxima
Dispositivos SCSI por máquina virtual	**4**
Dispositivos por SCSI	**15**
Dispositivos por máquina virtual para el Sistema Operativo Windows	**60**
Dispositivos por máquina virtual para el Sistema Operativo Linux	**60**
Capacidad del disco SCSI	**2TB**
Número de CPUs virtuales por máquina virtual	**4**
Memoria RAM por máquina virtual	**65532MB (64GB - 4MB)**
Tarjetas de RED (NICs) por máquina virtual	**4**
Dispositivos IDE por máquina virtual	**4**
Dispositivos Floppy por máquina virtual	**2**
Puertos paralelos por máquina virtual	**3**

Puertos en Serie por máquina virtual	**4**
Tamaño del archivo SWAP por máquina virtual	**65532MB**
Dispositivos PCI virtuales: NICs, SCSI, Dispositivos de audio (solo para VMware Server), Tarjeta Videos (una por máquina virtual), VMI-ROM.	**6**
Consolas Remotas por máquina virtual	**10**

Tabla 3: Máxima configuración para las máquinas virtuales. [16]

A través del VIC se puede crear un depósito de recursos (Resource Pool), donde se podrán tener un rango de recursos para crear las máquinas virtuales. Este depósito permite la limitación de uso de la memoria y del CPU del Host. A la hora de crear un depósito de recursos como se muestra en la Figura 16, se le asigna la capacidad a reservar y si se le limitara o no, ejemplo, el uso del CPU o la memoria RAM a las diferentes máquinas dentro del entorno virtual comprendido por el depósito de recursos.

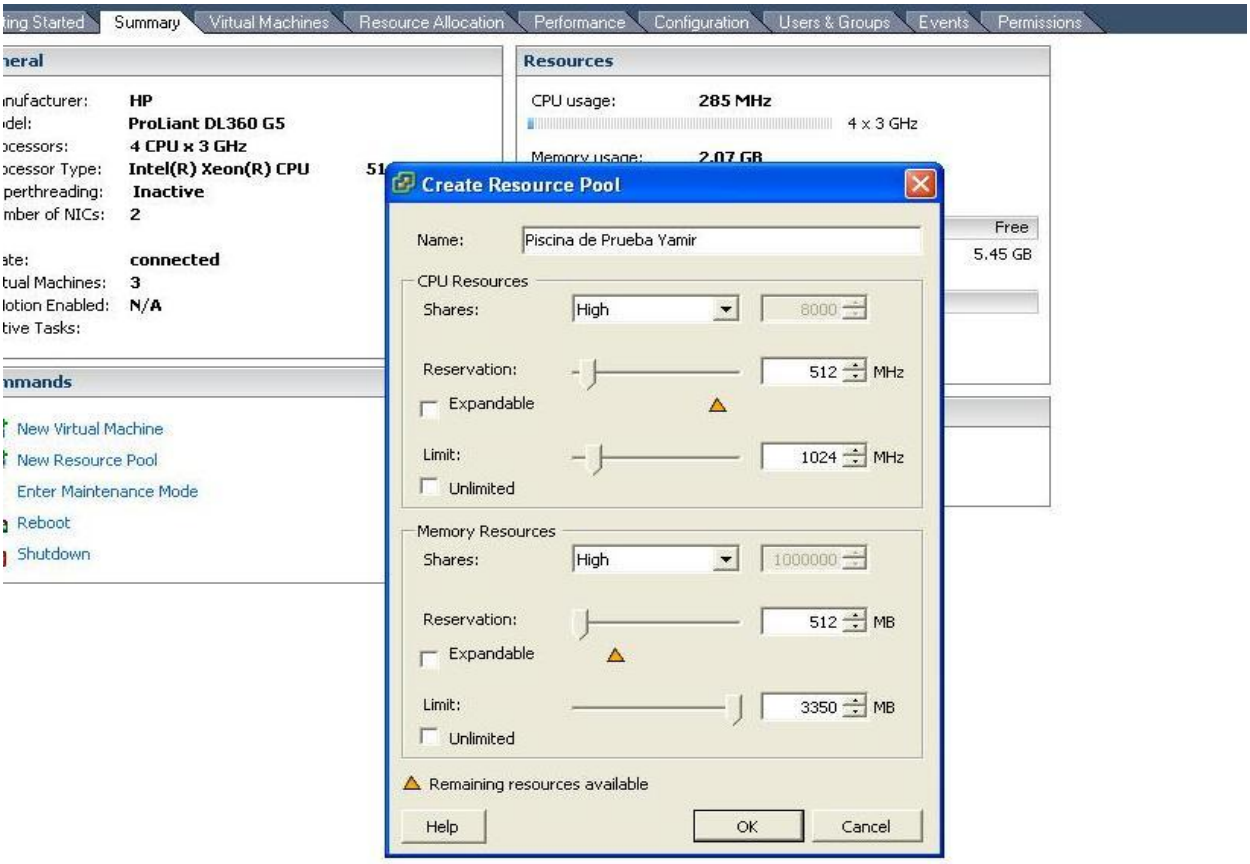

Figura 16: Creación de un Depósito de Recursos

Se debe tener en cuenta lo siguiente:

- **Shares (Prioridad):** prioridad de esa máquina respecto a otras cuando haya que competir por el recurso.

- **Reservation (Reservación):** cantidad mínima de recursos que la máquina virtual va a tener garantizados. Por ejemplo, al asignar a una máquina virtual 512 MB de RAM y una reserva de 128. Se garantizara que 128 MB van a ser de memoria física pero el resto puede ser swap o RAM en función de las necesidades y de la disponibilidad. Esto permite evitar la degradación completa del entorno virtual por el uso indiscriminado de recursos del sistema.

- **Limit (límite):** Máximo de recursos de los que va a disponer una máquina virtual. Por ejemplo, al utilizar un máximo de memoria a utilizar, una vez superado el límite especificado el sistema comenzara a realizar swapping.

Es importante conocer que ESX Server expone un prototipo de PC con las siguientes características de hardware para las máquinas virtuales a crear, las características de este hardware son las siguientes:

- Procesador virtual: Intel Pentium II o superior (dependiendo de los procesadores del Host)
- Uno, dos, o cuatro procesadores por máquina virtual.
- Chip set virtual: Intel 440BX basado en una motherboard con chip NS338 SIO.
- BIOS virtual: PhoenixBIOS 4.0 version 6.

En el siguiente paso, se le asigna un nombre a la máquina virtual y se especifica el lugar donde será almacenada y luego se escoge el Sistema Operativo que se instalará sobre la misma. El Sistema Operativo a instalar en las máquinas virtuales creadas será SuSE Linux Enterprise Server 10 SP2. Es necesario tener en cuenta que sobre ESX Server para poder crear máquinas virtuales de 64 bits es necesario activar la opción del BIOS, Intel Virtualization Technology.

Después de haber realizado lo anteriormente mencionado se procede a designar la cantidad de procesadores y la memoria RAM que se destinaran para el procesamiento de la máquina virtual. Es recomendado para mejor rendimiento, crear máquinas virtuales que tengan como máximo de procesadores la cantidad exacta de los que tiene el host. Nunca la máquina virtual puede superar la cantidad de procesadores que tiene el host, ya que esto provocaría una degradación del rendimiento del sistema. Luego se deciden cuántas tarjetas de red tendrá la maquina virtual que se está creando, a que red virtual estarán conectadas (en caso de tener más de 1) y qué tipo de adaptador de red, como se muestra en la figura:

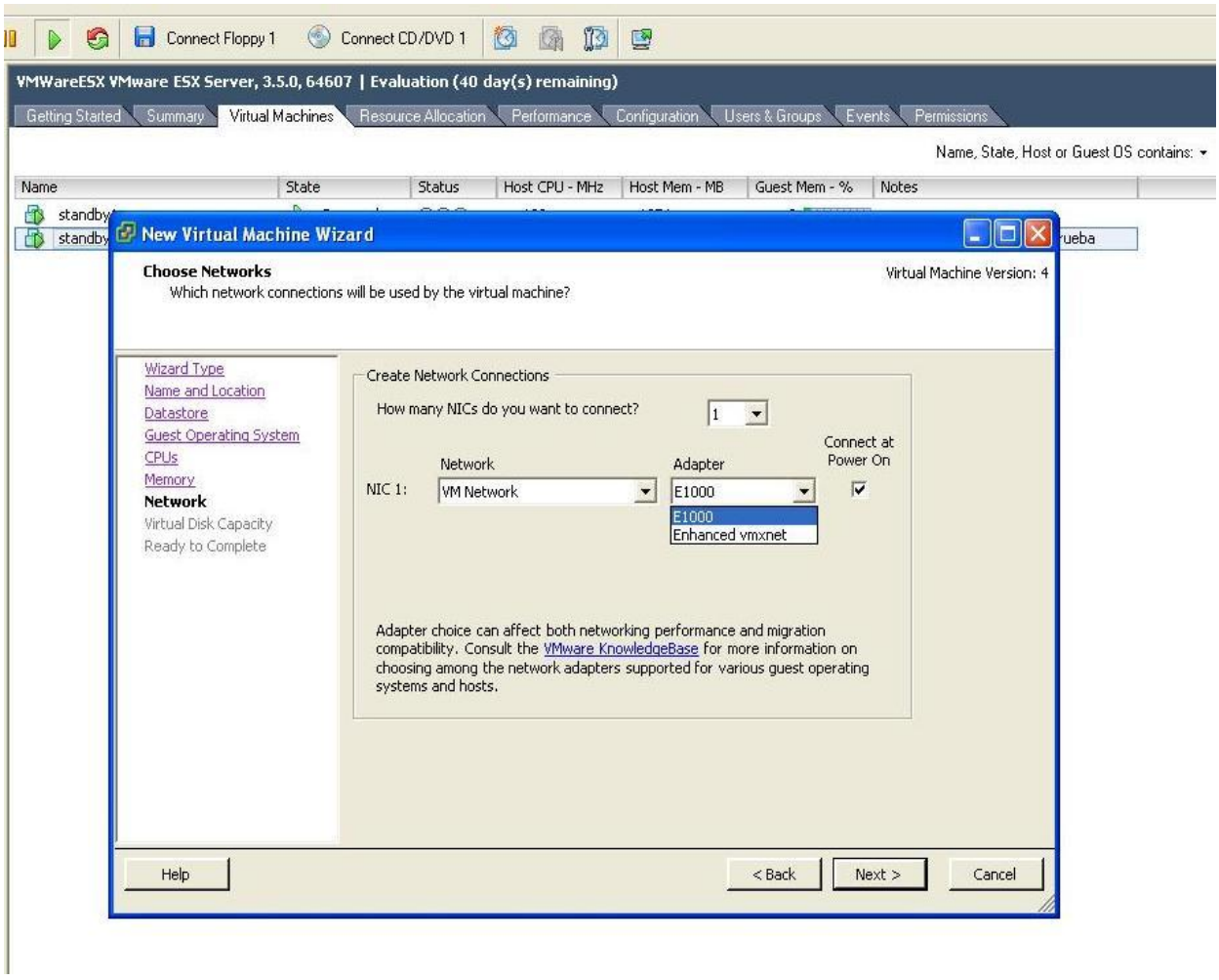

Figura 16. Configuración de la red para las máquinas virtuales

Después de haber realizado esta configuración de red, se procede entonces a la asignación de la capacidad del disco virtual, podría ser en un disco ya existente o se puede crear uno nuevo. Durante esta fase, se decide la capacidad de almacenamiento y también se define si se desea que los cambios que ocurran en la máquina virtual se almacenen de forma persistente o no persistente en el disco virtual de la maquina. Si se selecciona persistente, entonces se guardaran todos los cambios; sino ninguno de los cambios realizados serán guardados. La opción recomendada y seleccionada por defecto en el asistente de instalación de ESX Server es la persistente.

Luego de haber realizado todos estos pasos, la máquina virtual ya se encontrará creada y se encontrara lista para instalar sobre ella el sistema operativo especificado durante su creación; en este caso, SuSE Linux Enterprise Server 10.

3.3 Configuración del entorno Data Guard

Después de tener configurado el entorno de virtualización y creadas las maquinas virtuales que serán destinadas como sitios standby; es necesario pasar a la configuración del ambiente Data Guard, el cual estará conformado por una base de datos origen o primaria y una base de datos en espera o standby física de este sitio primario. La variante propuesta para crear estos sitios standby está basada en la funcionalidad de RMAN para duplicar una base de datos Oracle activa.

Para crear una base de datos standby con el comando **DUPLICATE** de RMAN, se deberá primeramente conectarnos como **TARGET** a la base de datos primaria, especificando la opción **FOR STANDBY**. Hay que tener presente que, no es posible crear una base de datos standby adicional a partir de la base de datos standby inicialmente creada. Durante el proceso de creación de la standby, RMAN necesita restaurar y montar un fichero de control, por lo tanto, es necesario para ello contar con una salva del fichero de control de la base de datos primaria.

Además, es preciso conocer que una base de datos en un ambiente Data Guard es identificada mediante el parámetro de inicialización **DB_UNIQUE_NAME**, este parámetro debe ser único entre todas las bases de datos con el mismo **DBID** (y el mismo **DB_NAME**) que integran el entorno Data Guard, de forma tal que RMAN las pueda identificar correctamente.

A continuación se describirán los pasos a seguir para lograr el entorno Data Guard.

3.3.1 Configuración de la base de datos de producción o primaria

Partiendo de que la base de datos primaria, cuenta con 3 grupos de discos administrados por una la instancia de Administración de Almacenamiento Automático (*ASM, por sus siglas en ingles*):

- **+BD1**, donde se encontrarán todos los ficheros principales de la base de datos.
- **+BD2,** utilizado para duplicar los redolog online y los ficheros de control.
- **+DATOS,** donde se encontrarán todos los tablespaces de los sistemas desarrollados por los usuarios.

Es importante considerar que en algún momento la base de datos origen puede pasar a cumplir un rol standby, ya sea por un failover automático o por un switchover manual. Por tanto, es necesario que la base de datos primaria cuente también con varios grupos de ficheros redolog standby. Es recomendado contar siempre con al menos uno más que la cantidad de ficheros redolog online del sitio que cumplirá el rol de primario durante su permanencia como standby. En el caso propuesto, como solo se tiene una base de datos standby, entonces la cantidad de ficheros redolog standby debe ser al menos uno más que la cantidad de ficheros redolog online del sitio standby. Ademas, estos ficheros redolog standby deberían ser del mismo tamaño que los redologs online.

Hay que tener en cuenta, que en todo momento que se adicione un grupo de redolog a la base de datos primaria también deberá ser añadido uno la base de datos standby, estando la base de datos standby en el modo de transporte de redo síncrono. Si no se hace de esa forma entonces una base de datos corriendo en el modo de protección de datos de Máxima Protección realizara un shutdown, y una base de datos corriendo en el modo de Máxima Disponibilidad se cambiará automáticamente al modo de Máximo Desempeño.

Antes de crear los ficheros redolog standby, primeramente, es necesario crear las estructuras de directorio siguientes dentro de los grupos de discos de ASM. Para ello se podría auxiliar del utilitario **asmcmd**.

```
+BD1/bdm1/standbylog
+BD2/bdm1/standbylog
```

1. Antes de ejecutar la sentencia SQL para adicionar un redolog standby a la base de datos primaria, se recomienda eliminar, si existen, grupos de redolog standby anteriores. Ejemplo:

```
SQL> ALTER DATABASE DROP LOGFILE GROUP 4;
SQL> ALTER DATABASE DROP LOGFILE GROUP 5;
SQL> ALTER DATABASE DROP LOGFILE GROUP 6;
SQL> ALTER DATABASE DROP LOGFILE GROUP 7;
```

2. Después de haber ejecutado las instrucciones SQL anteriores se procede a crear los grupos de redolog standby:

```
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 4
('+BD1/bdm1/standbylog/standredo_41', '+BD2/bdm1/standbylog/standredo_42')
  SIZE 50M;
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 5
('+BD1/bdm1/standbylog/standredo_51', '+BD2/bdm1/standbylog/standredo_52')
  SIZE 50M;
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 6
('+BD1/bdm1/standbylog/standredo_61', '+BD2/bdm1/standbylog/standredo_62')
  SIZE 50M;
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 7
('+BD1/bdm1/standbylog/standredo_71', '+BD2/bdm1/standbylog/standredo_72')
  SIZE 50M;
```

3. Se coloca la base de datos de producción en modo archivelog (si no lo está), ya que es necesario para los propios mecanismos de funcionamiento de Oracle Data Guard:

```
SQL> SHUTDOWN IMMEDIATE;
SQL> STARTUP MOUNT;
SQL> ALTER DATABASE ARCHIVELOG;
SQL> ALTER DATABASE OPEN;
```

Se puede verificar si la base de datos ya se encontraba en este estado, realizando la siguiente consulta SQL:

```
SQL> SELECT LOG_MODE FROM V$DATABASE;
```

Se fuerza la generación de redo de todas las estructuras de la base de datos (al fin y al cabo esta es la manera en la que se garantizará una sincronización perfecta entre el sitio primario y el sitio standby) mediante:

```
SQL> ALTER DATABASE FORCE LOGGING;
```

Para verificar si la base de datos se encuentra ya en este modo se puede ejecutar:

```
SQL> SELECT FORCE_LOGGING FROM V$DATABASE;
FOR
---
YES
```

4. Se definen los parámetros de inicialización en la base de datos primaria que controlan el servicio de transporte de redo mientras la base de datos está en el rol primario y también los parámetros necesarios para el control de la recepción de los datos de redo y el servicio de aplicación cuando la base de datos primaria se convierta en standby.

Existen 2 tipos de ficheros de parámetros de inicialización los PFILE que son ficheros de inicio en texto los cuales se pueden modificar mediante un editor de texto y los SPFILE que son ficheros de inicio en binarios los cuales no se pueden modificar. Si la instancia de la base de datos ha sido iniciada desde un SPFILE, entonces se debe construir un PFILE de dicho SPFILE, para luego editar los parámetros correspondientes a la configuración Data Guard:

```
SQL> CREATE PFILE FROM SPFILE;
```

Una vez ejecutada la instrucción SQL anterior, será creado en el directorio **`$ORALCLE_HOME/dbs/`** un fichero llamado **`init$ORACLE_SID.ora`**. Y entonces, los parámetros a modificar serán los siguientes:

```
*.DB_UNIQUE_NAME=bdm1
*.LOG_ARCHIVE_CONFIG='DG_CONFIG= (bdm1, bdm2)'
*.LOG_ARCHIVE_DEST_1='LOCATION=+BD2/TRAZAS/ VALID_FOR= (ALL_LOGFILES, ALL_ROLES)
  DB_UNIQUE_NAME=bdm1'
*.LOG_ARCHIVE_DEST_2='SERVICE=bdm2 ASYNC VALID_FOR= (ONLINE_LOGFILES, PRIMARY_ROLE)
  DB_UNIQUE_NAME=bdm2'
*.LOG_ARCHIVE_FORMAT=%t_%s_%r.arc
*.LOG_ARCHIVE_MAX_PROCESSES=30
*.FAL_SERVER=bdm2
*.FAL_CLIENT =bdm1
*.STANDBY_FILE_MANAGEMENT=AUTO
*.DG_BROKER_START=TRUE
```

Si durante el proceso de configuración de la base de datos, se seleccionó la opción FLASH RECOVERY AREA, entonces no es necesario añadir los parámetros que siguen, pues ya deben aparecer en el fichero de inicialización, de lo contrario se deberán incluir teniendo cuidado de que los valores usados se ajusten a la configuración del sistema operativo:

```
DB_RECOVERY_FILE_DEST_SIZE=2G

DB_RECOVERY_FILE_DEST='/salva/area_recupera'
```

Luego es necesario reconstruir el SPFILE:

```
SQL> CREATE SPFILE FROM PFILE;
```

5. Configuración de las salvas de RMAN en la base de datos primaria, especialmente cuidar de configurar el autobackup de los controlfile, es necesario ejecutar una salva de RMAN, preferiblemente de nivel 0, si no se tiene alguna reciente, o de un nivel que nos actualice las salvas.

3.3.2 Preparación de la instancia que asumirá el rol de base de datos standby

6. Configuración de la instancia ASM y creación de los grupos de discos idénticos a los de la base de datos primaria, es decir:

+BD1, +BD2 y +DATOS

- Se crean los directorios:

```
+BD1/BDM2/CONTROLFILE
+BD1/BDM2/STANDBYLOG
+BD2/BDM2/CONTROLFILE
+BD2/BDM2/STANDBYLOG
+BD2/TRAZAS
```

De existir estructuras de directorio dentro del grupo de discos +DATOS, se tienen que crear también.

- Crear en **$ORACLE_HOME/dbs** el fichero de parámetros de inicialización **init$ORACLE_SID.ora** solamente con la línea:

```
DB_NAME = primaria
```

- Levantar la instancia NO MONTADA, si existe el fichero **spfile$ORACLE_SID.ora** debe borrarse.
- Crear el directorio en el sistema operativo para el área de recuperación con un espacio suficientemente grande como para contener a todos los datafiles de la base de datos, se propone no menos de 2Gb, debiendo corresponderse con lo declarado en el paso 4.
- Copiar desde la base de datos primaria la estructura de directorios que se encuentra debajo de **/opt/oracle/admin** con el nombre de la instancia principal, es decir en este ejemplo se debe copiar el directorio **/opt/oracle/admin/primaria** con todos sus subdirectorios. También, en vez de hacer lo anterior se puede redefinir el parámetro de inicialización **AUDIT_FILE_DEST**, el cual es posible modificar mediante la cláusula **PFILE** del comando **DUPLICATE**.

7. Establecer la conectividad con la instancia auxiliar mediante Oracle Net. La instancia auxiliar debe estar disponible mediante Oracle Net debido a que se duplicará una base de datos activa mediante un cliente RMAN en un host distinto al de destino. Es decir, cuando se realiza el duplicado de una base de

datos activa, en primer lugar se debe garantizar la interconexión como **SYSDBA** entre la base de datos fuente y la base de datos auxiliar por medio de nombres de servicio de red.

La instancia de la base de datos fuente a la cual RMAN se conectará como **TARGET**, usa este nombre de servicio de red para conectarse directamente a la instancia de la base de datos auxiliar. En el directorio **$ORACLE_HOME/network/admin** se debe crear los ficheros **listener.ora** y el **tnsnames.ora**, a través de ellos se configura el Oracle Net para lograr la conexión entre las bases de datos. En el **tnsnames.ora** deben existir la misma cantidad de servicios declarados que la cantidad de bases de datos comprendidas en el entorno Data Guard, según la propuesta dos. A continuación se describe la configuración correspondiente a los ficheros **tnsnames.ora** y **listener.ora** respectivamente.

```
# TNSNAMES.ORA Network Configuration
BDM1 =
    (DESCRIPTION =
       (ADDRESS_LIST =
          (ADDRESS = (PROTOCOL = TCP) (HOST = dbserver1.das.cites) (PORT = 1521))
          (ADDRESS = (PROTOCOL = TCP) (HOST = dbserver1.das.cites) (PORT = 1526))
        )
       (CONNECT_DATA =
          (SERVER = DEDICATED)
         (SERVICE_NAME = primaria.das.cites)
        )
     )
BDM2 =
    (DESCRIPTION =
       (ADDRESS_LIST =
           (ADDRESS = (PROTOCOL = TCP) (HOST = standby1.das.cites) (PORT = 1521))
           (ADDRESS = (PROTOCOL = TCP) (HOST = standby1.das.cites) (PORT = 1526))
        )
        (CONNECT_DATA =
          (SERVER = DEDICATED)
          (SERVICE_NAME = primaria.das.cites)
         )
      )
```

```
# LISTENER.ORA Network Configuration
LISTENER =
       (DESCRIPTION_LIST =
         (DESCRIPTION =
              (ADDRESS = (PROTOCOL = TCP) (HOST = dbserver1.das.cites) (PORT = 1521)
          )
         (DESCRIPTION =
              (ADDRESS = (PROTOCOL = TCP) (HOST = dbserver1.das.cites) (PORT = 1526)
          )
       )
SID_LIST_LISTENER =
     (SID_LIST =
         (SID_DESC =
             (GLOBAL_DBNAME = primaria.das.cites)
             (ORACLE_HOME = /opt/oracle/product/11g)
             (SID_NAME = primaria)
          )
          (SID_DESC =
              (GLOBAL_DBNAME = bdm1_DGMGRL.das.cites)
              (ORACLE_HOME = /opt./oracle/prodcut/11g)
              (SID_NAME = primaria)
          )
       )
```

Estos dos ficheros deben ser editados en ambos sistemas, tanto el sitio primario como el standby, cambiando solamente los nombres de host.

8. Creación del fichero de contraseñas de Oracle para la instancia auxiliar. Este fichero, ubicado en **$ORACLE_HOME/dbs/orapw$ORACLE_SID**, es absolutamente necesario debido a que se va a duplicar una base de datos activa. Cuando es usada la opción **FROM ACTIVE DATABASE**, la instancia de la base de datos origen, a la cual se conecta RMAN como **TARGET**, necesita conectarse de inicio directamente a la instancia de la base de datos auxiliar. Esta conexión requiere de un fichero de contraseñas con idéntica contraseña

SYSDBA, este fichero debe existir ya en el directorio dado del sitio primario, solamente sería necesario copiarlo hacia el sitio standby.

Adicionalmente, se debe tener presente también que si se usa la sentencia SQL, **ALTER USER**, para modificar la contraseña del usuario SYS, también se modificará el fichero de contraseñas. Luego durante el proceso de duplicación de la base de datos activa este fichero será sobrescrito, pero inicialmente es absolutamente necesario crearlo en el lado auxiliar para que RMAN pueda conectarse a la instancia del sitio standby. Una manera sencilla de comprobar si la autenticación funciona correctamente mediante el fichero de contraseñas sería, tratar de conectarse desde la base de datos primaria hacia la standby, ejemplo:

```
oracle@dbserver1: ~> sqlplus sys/manager@bdm2 as sysdba
```

Y desde la standby hacia la primaria:

```
oracle@dbserver1: ~> sqlplus sys/manager@bdm1 as sysdba
```

Es importante saber que, implícitamente, RMAN no recupera la base de datos standby después de haberla creado. Esto quiere decir, que después de terminado el duplicado de la base de datos primaria, la nueva base de datos (standby) queda montada, pero sin ponerla en modo de recuperación manual o administrada. RMAN se desconecta y no ejecuta la recuperación de la base de datos standby.

Si se quiere que RMAN recupere la base de datos standby después de haberla creado, entonces el fichero de control de la standby debe estar disponible para la recuperación. Por tanto, las siguientes condiciones deben cumplirse:

- La hora final de recuperación de la base de datos standby debe ser mayor o igual al checkpoint SCN del fichero de control de la standby.
- Un fichero de redo log archivado conteniendo el checkpoint SCN del fichero de control de la standby debe estar disponible para ejecutar la recuperación.

Una manera de asegurar que estas condiciones se cumplan es usando la sentencia **ALTER SYSTEM ARCHIVE LOG CURRENT** y después ejecutar la salva del fichero de control en la base de datos primaria. Esta sentencia archiva los ficheros redo log online de la base de datos primaria. Entonces, luego de ejecutado lo anterior, se debe salvar el fichero redo log archivado con RMAN o se traslada los ficheros redo log archivados al sitio standby.

Ejecutar la sentencia:

```
SQL > ALTER SYSTEM ARCHIVE LOG CURRENT;
```

9. Conectarse a las dos instancias, primaria y standby, con la siguiente cadena de RMAN:

```
oracle@dbserver1: ~> $ORACLE_HOME/bin/rman TARGET / AUXILIARY sys/manager@bdm2
LOG='/opt/oracle/Data Guard/salidas/ejemplo_crear_standby.log'
```

Después de estar conectarnos al sitio primario como **TARGET** y al sitio standby como **AUXILIARY** se debe mandar a ejecutar el siguiente script de RMAN:

```
DUPLICATE TARGET DATABASE FOR STANDBY
  DORECOVER
  FROM ACTIVE DATABASE
  NOFILENAMECHECK
  SPFILE
     SET DB_UNIQUE_NAME = "bdm2"
     SET LOG_ARCHIVE_CONFIG='DG_CONFIG= (bdm2, bdm1)'
     SET LOG_ARCHIVE_DEST_1='LOCATION=+BD2/TRAZAS/
        VALID_FOR= (ALL_LOGFILES, ALL_ROLES)
          DB_UNIQUE_NAME=bdm2'
     SET LOG_ARCHIVE_DEST_2="SERVICE = bdm1 ASYNC
        VALID_FOR = (ONLINE_LOGFILES, PRIMARY_ROLE)
          DB_UNIQUE_NAME=bdm1)"
     SET FAL_SERVER = 'bdm1'
     SET FAL_CLIENT = 'bdm2'
     SET CONTROL_FILES='+BD1/bdm2/controlfile/control01.ctl',
     '+BD2/bdm2/controlfile/control02.ctl';
```

10. Crear los ficheros standby redolog en la BD standby en el directorio ASM siguiente:

```
+BD1/bdm2/standbylog y +BD2/bdm2/standbylog
```

Para ello:

```
SQL> ALTER DATABASE DROP LOGFILE GROUP 4;
SQL> ALTER DATABASE DROP LOGFILE GROUP 5;
SQL> ALTER DATABASE DROP LOGFILE GROUP 6;
SQL> ALTER DATABASE DROP LOGFILE GROUP 7;
```

```
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 4
('+BD1/bdm2/standbylog/standredo_41', '+BD2/bdm2/standbylog/standredo_42')
  SIZE 50M;
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 5
('+BD1/bdm2/standbylog/standredo_51', '+BD2/bdm2/standbylog/standredo_52')
  SIZE 50M;
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 6
('+BD1/bdm2/standbylog/standredo_61', '+BD2/bdm2/standbylog/standredo_62')
  SIZE 50M;
SQL> ALTER DATABASE ADD STANDBY LOGFILE GROUP 7
('+BD1/bdm2/standbylog/standredo_71', '+BD2/bdm2/standbylog/standredo_72')
  SIZE 50M;
```

Luego de tener configurada la base de datos standby es necesario colocarla en modo de recuperación administrado utilizando además la característica de Data Guard, Real-Time Apply.

```
SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING CURRENT LOGFILE
DISCONNECT FROM SESSION;
```

Cuando se tiene activa la propiedad Real-Time Apply del Data Guard prácticamente el entorno se encuentra sincronizado. Existen varias vistas o procedimientos para verificar que los redo log se están transportando y aplicando en el sitio en espera o standby. Si se ejecuta **ARCHIVE LOG LIST** en el sitio primario, se obtendrá una lista de elementos a través de los cuales se puede conocer la secuencia de log actual, la próxima, entre otras características; ejecutando esta misma sentencia en el sitio standby, permite saber (en caso de que coincidan), si el sitio standby esta sincronizado con respecto al sitio primario. A continuación se muestra el procedimiento.

```
SQL> ARCHIVE LOG LIST
Database log mode              Archival Mode
Automatic archival             Enabled
Archive destination            +BD2/trazas/
Oldest online log sequence     862
Next log sequence to archive   863
Current log sequence           863
```

Con el procedimiento anterior se obtendrán los log archivados pero no se puede conocer si están aplicados, si no se tiene por alguna razón el Real-Time Apply activado primeramente se archivaran los redo de datos y luego se aplicarán. Existe otra vista para comprobar la sincronización entre la base de datos primaria y la standby, es la recomendada, se puede consultar a través de los campos **SEQUENCE#** y **APPLY** de la vista **V$ARCHIVED_LOG** en el sitio primario y luego en el standby y comparar los log.

```
SQL> SELECT SEQUENCE#, APPLY FROM V$ARCHIVED_LOG;

SEQUENCE#              APP
_ _ _ _ _              _ _ _
850                    YES
851                    YES
852                    YES
853                    YES
SEQUENCE#              APP
_ _ _ _ _              _ _ _
863                    YES
806 rows selected.
```

Una vista que podría ayudar mucho a la hora de verificar que todos los procesos que actúan para lograr el transporte de redolog en la base de datos primaria y el recibo en el sitio standby no presentan errores es la **V$DATAGUARD_STATUS**, si se describe representaría los siguientes campos.

```
SQL> describe v$dataguard_status
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------
 FACILITY                                           VARCHAR2(24)
 SEVERITY                                           VARCHAR2(13)
 DEST_ID                                            NUMBER
 MESSAGE_NUM                                        NUMBER
 ERROR_CODE                                         NUMBER
 CALLOUT                                            VARCHAR2(3)
 TIMESTAMP                                          DATE
 MESSAGE                                            VARCHAR2(256)
```

El campo **MESSAGE** de esta vista que se muestra a continuación describe el proceso de transporte de cada secuencia hacia el sitio standby si se esta trabajando sobre el sitio primario.

```
SQL> SELECT MESSAGE FROM V$DATAGUARD_STATUS;
MESSAGE
--------------------------------------------------------------------------------
LGWR: Standby redo logfile selected to archive thread 1 sequence 864
LGWR: Standby redo logfile selected for thread 1 sequence 864 for destination LO
G_ARCHIVE_DEST_2

LNS: Standby redo logfile selected for thread 1 sequence 864 for destination LOG
_ARCHIVE_DEST_3
256 rows selected.
```

En el caso contrario se describe el proceso de llegada de los redolog en la base de datos standby, como se muestra seguidamente.

```
SQL> SELECT MESSAGE FROM V$DATAGUARD_STATUS;
MESSAGE
--------------------------------------------------------------------------------
Primary database is in MAXIMUM AVAILABILITY mode
Standby controlfile consistent with primary
Media Recovery Waiting for thread 1 sequence 863 (in transit)
RFS[1]: Successfully opened standby log 7: '+BD1/bdm2/standbylog/standredo_71'
210 rows selected.
```

11. Durante este paso se definirá la configuración para la herramienta de control, administración y configuración del Data Guard conocida como Broker. Al mismo se puede acceder a través de la línea de comando utilizando el utilitario **dgmgrl**:

```
DGMGRL> CONNECT sys/manager
DGMGRL> CREATE CONFIGURATION 'Ejemplo' AS PRIMARY DATABASE IS 'bdm1' CONNECT
IDENTIFIER IS bdm1.das.cites;
DGMGRL> ADD DATABASE 'bdm2' AS CONNECT IDENTIFIER IS bdm2.das.cites MAINTAINED AS
PHYSICAL;
DGMGRL> ENABLE CONFIGURATION;
```

Para verificar si la configuración se ha ejecutado correctamente se puede ejecutar:

```
DGMGRL> SHOW CONFIGURATION VERBOSE;
```

En el estado de la configuración aparecerán estos elementos:

```
Configuration
  Name:                Ejemplo
  Enabled:             YES
  Protection Mode:     MaxPerformance
  Databases:
    bdm1 - Primary database
    bdm2 - Physical standby database

Fast-Start Failover: DISABLED

Current status for "Ejemplo":
SUCCESS
```

Si el estado de la configuración informa que se presentan algunos errores en las bases de datos entonces se puede ejecutar la siguiente sentencia para verificar el estado individual de cada base de datos.

```
DGMGRL> SHOW DATABASE bdm1;
Database
  Name:            bdm1
  Role:            PRIMARY
  Enabled:         YES
  Intended State:  TRANSPORT-ON
  Instance(s):
  primaria

Current status for "bdm1":
SUCCESS
```

Si la respuesta es SUCCESS en cualquiera de los casos, entonces se puede ejecutar un switchover hacia la standby, utilizando el Broker y de esta forma validar que la configuración del entorno Data Guard está completamente correcta:

```
DGMGRL> SWITCHOVER TO bdm2;
```

De producirse correctamente, entonces:

```
DGMGRL> SWITCHOVER TO bdm1;
```

Al haber ejecutado el comando **SHOW CONFIGURATION VERBOSE** se puede apreciar que no está habilitada la característica de Fast-Start Failover. A continuación se describirán los pasos a llevar a cabo para habilitar esta capacidad, permitiendo que cuando ocurra alguna falla del sistema automáticamente se realice un cambio de rol entre las bases de datos presentes en el entorno Data Guard.

- Primeramente, es necesario determinar cuál es la base de datos standby óptima para que pase a cumplir un rol primario en caso de falla.
- Especificar a través de la propiedad **FastStartFailoverTarget** cuál será la base de datos standby que asumirá el rol.

Si la configuración Data Guard solamente presenta una sola base de datos standby física, entonces se puede omitir este paso, ya que automáticamente el Broker hará un cambio de rol en la configuración entre el sitio primario y el standby, detectando la base de datos standby y realizándole la transición de rol hacia primaria.

Si en cambio, están presentes más de un sitio standby, entonces se debe configurar la propiedad de la siguiente forma. Por ejemplo, se especifica que bdm2 pasará a cumplir un rol primario en caso de falla, y si ocurre otra falla estando bdm2 como base de datos de producción entonces bdm1 pasará nuevamente a cumplir su rol.

```
DGMGRL> EDIT DATABASE 'bdm1' SET PROPERTY FastStartFailoverTarget = 'bdm2';
DGMGRL> EDIT DATABASE 'bdm2' SET PROPERTY FastStartFailoverTarget = 'bdm1';
```

- Determinar cual tipo de protección será la correcta.

Si la protección escogida será la de máxima disponibilidad entonces se hará lo siguiente:

```
DGMGRL> EDIT DATABASE 'bdm1' SET PROPERTY LogXptMode=SYNC;
DGMGRL> EDIT DATABASE 'bdm2' SET PROPERTY LogXptMode=SYNC;
DGMGRL> EDIT CONFIGURATION SET PROTECTION MODE AS MaxAvailability;
```

- Configurar la propiedad **FastStartFailoverThreshold**.

```
DGMGRL> EDIT CONFIGURATION SET PROPERTY FastStartFailoverThreshold = 45;
```

- Existen otras propiedades y condiciones opcionales que se le pueden configurar al fast-start failover, las cuales traen un valor por defecto.
- Se habilita el fast-start failover utilizando el DGMGRL:

```
DGMGRL> ENABLE FAST_START FAILOVER;
```

- Por último, se inicia el observer.

```
DGMGRL> START OBSERVER;
```

- Verificar el estado del fast-start failover.

```
DGMGRL> SHOW FAST_START FAILOVER;

Fast-Start Failover: ENABLED
  Threshold:          45 seconds
  Target:             bdm2
  Observer:           observer.foo.com
  Lag Limit:          30 seconds (not in use)
  Shutdown Primary:   TRUE
  Auto-reinstate:     TRUE
Configurable Failover Conditions
  Health Conditions:
  Corrupted Controlfile       YES
  Corrupted Dictionary        YES
  Inaccessible Logfile         NO
  Stuck Archiver               NO
  Datafile Offline            YES
Oracle Error Conditions:
  (none)
```

3.3.3 Resolución de conflictos en la configuración Data Guard

1. Renombrar los datafiles utilizando la instrucción **ALTER DATABASE.**

Si el parámetro de inicialización **STANDBY_FILE_MANAGEMENT** es establecido al valor **AUTO** no se pueden renombrar los datafiles en un sitio standby, por lo tanto el uso de las siguientes instrucciones SQL no está permitido:

- **ALTER DATABASE RENAME**
- **ALTER DATABASE ADD/DROP LOGFILE**
- **ALTER DATABASE ADD/DROP STANDBY LOGFILE MEMBER**
- **ALTER DATABASE CREATE DATAFILE AS**

Si se intenta usar alguna de estas instrucciones en la base de datos standby, entonces un error será generado. Por ejemplo:

```
SQL> ALTER DATABASE RENAME FILE '/disk1/oracle/oradata/payroll/t_db2.log' to
'dummy';
alter database rename file '/disk1/oracle/oradata/payroll/t_db2.log' to 'dummy'
*
ERROR at line 1:
ORA-01511: error in renaming log/datafiles
ORA-01270: RENAME operation is not allowed if STANDBY_FILE_MANAGEMENT is auto
```

2. El sitio standby no puede recibir datos redo desde el sitio primario.

En el caso que los datos redo no se estén recibiendo en el sitio standby, se puede consultar la vista **V$ARCHIVE_DEST** y revisar los mensajes de error relacionados con el problema que está ocurriendo. Por ejemplo, se puede ejecutar la siguiente instrucción SQL:

```
SQL> SELECT DEST_ID "ID",
  2> STATUS "DB_status",
  3> DESTINATION "Archive_dest",
  4> ERROR "Error"
  5> FROM V$ARCHIVE_DEST WHERE DEST_ID <=5;

ID DB_status Archive_dest                    Error
-- --------- ------------------------------ --------------------------------
 1  VALID    /vobs/oracle/work/arc_dest/arc
 2  ERROR    standby1  ORA-16012: Archivelog standby database identifier mismatch
 3  INACTIVE
 4  INACTIVE
 5  INACTIVE
5 rows selected.
```

Si la salida resultado de la ejecución de la instrucción SQL anterior no brinda referencia suficiente para detectar lo que esta ocurriendo, entonces se pueden chequear los siguientes elementos. Si alguna de las condiciones siguientes está presente, los servicios de transporte de redo fallarían a la hora de transmitir los datos redo hacia el sitio standby:

- El nombre de servicio para la base de datos standby no se encuentra configurado correctamente en el fichero **`tnsnames.ora`** en el sitio primario.
- El nombre de servicio de Oracle Net especificado en el parámetro **`LOG_ARCHIVE_DEST_n`** para el sitio primario es incorrecto.
- El parámetro **`LOG_ARCHIVE_DEST_STATE`** para el sitio standby no está definido con el valor **`ENABLE`**.
- El fichero **`listener.ora`** no ha sido configurado correctamente en el sitio standby.
- El listener no ha sido iniciado en el sitio standby.
- La instancia standby no está iniciada.
- Se ha añadido un destino de archivado standby al SPFILE o PFILE del sitio primario, pero aun no se ha habilitado el cambio.

3. No se puede montar la base de datos física

Si el problema consiste en que no se puede montar la base de datos, se debe revisar y tener en cuenta que el fichero de control para el sitio standby haya sido creado utilizando la instrucción SQL, **ALTER DATABASE CREATE STANDBY CONTROLFILE**, o utilizando un comando de RMAN. No es posible utilizar los siguientes tipos de salvas del fichero de control:

- Una salva creada con el sistema operativo.
- Una salva creada usando una instrucción **ALTER DATABASE** sin la opción **PHYSICAL STANDBY.**

4. Fallas en el destino de los ficheros redolog.

Si se especifica **REOPEN** para un destino de redologs **MANDATORY**, los servicios de transporte de redo provocaran un impacto sobre la base de datos primaria cuando los datos redo no pueden ser transmitidos satisfactoriamente hacia el sitio standby. Por tanto, es requerido utilizar el atributo **REOPEN** cuando se usa también el atributo **MAX_FAILURE**.

En el siguiente ejemplo se muestra como se define un tiempo para volver a tratar enviar los datos redo de 5 segundos y con un límite de tres intentos.

```
LOG_ARCHIVE_DEST_1='LOCATION=/arc_dest REOPEN=5 MAX_FAILURE=3'
```

También se puede utilizar el atributo **ALTERNATE** para especificar un destino de archivado alternativo, de esta forma el sitio primario utilizaría este destino de archivado en caso de no poder transmitir los datos redo hacia la base de datos standby.

Si por otro lado, la transmisión de redo falla y el atributo **REOPEN** no fue especificado o el valor del atributo **MAX_FAILURE** ha sido excedido, entonces los servicios de transporte de redo intentaran transmitir hacia el destino archivado alternativo cuando ocurra una nueva operación de archivado.

A continuación se muestra como realizar la configuración de un destino de redologs archivado utilizando el parámetro **ALTERNATE**.

```
LOG_ARCHIVE_DEST_1='LOCATION=/disk1 MANDATORY ALTERNATE=LOG_ARCHIVE_DEST_2'
LOG_ARCHIVE_DEST_STATE_1=ENABLE
LOG_ARCHIVE_DEST_2='LOCATION=/disk2 MANDATORY'
LOG_ARCHIVE_DEST_STATE_2=ALTERNATE
```

3.3.4 Problemas a la hora de realizar un switchover en una base de datos standby

El switchover falla porque los datos redo no han sido transmitidos

Si un switchover no es terminado satisfactoriamente, se puede realizar una consulta al campo **SEQUENCE#** en la vista **V$ARCHIVED_LOG** para ver si el último dato de redo transmitido desde el sitio primario original fue aplicado en la base de datos standby. Si este no ha sido transmitido aun hacia el sitio standby, se puede copiar el fichero redolog archivado que contiene el último dato redo manualmente en la base de datos standby y será aplicado automáticamente. Luego se debe realizar una consulta al campo **SWITCHOVER_STATUS** de la vista **V$DATABASE**. Si el resultado de la consulta es **TO PRIMARY** entonces es posible continuar el switchover normalmente.

```
SQL> SELECT SWITCHOVER_STATUS FROM V$DATABASE;

SWITCHOVER_STATUS

-----------------

TO PRIMARY

1 row selected
```

El switchover falla porque existen sesiones SQL que aún permanecen activas

Si al ejecutar un switchover a través de SQL, no se especifica la clausula **WITH SESSION SHUTDOWN** como parte de la instrucción **ALTER DATABASE COMMIT SWITCHOVER TO PHYSICAL STANDBY**, el switchover no ejecutará satisfactoriamente si existen sesiones activas en la base de datos. Cuando esto acurre, el intento de realizar un switchover falla mostrando el siguiente mensaje:

```
SQL> ALTER DATABASE COMMIT TO SWITCHOVER TO PHYSICAL STANDBY;

ALTER DATABASE COMMIT TO SWITCHOVER TO PHYSICAL STANDBY *

ORA-01093: ALTER DATABASE CLOSE only permitted with no sessions connected
```

Para resolver este error, es recomendable consultar la vista **V$SESSION** para determinar cuáles son los procesos que están podrían provocar el error. Por ejemplo:

```
SQL> SELECT SID, PROCESS, PROGRAM FROM V$SESSION
  2> WHERE TYPE = 'USER'
  3>  AND SID <> (SELECT DISTINCT SID FROM V$MYSTAT);
SID         PROCESS    PROGRAM
---------   --------   -------------------------------------------------
        7       3537   oracle@nhclone2 (CJQ0)
       10
       14
       16
       19
       21
 6 rows selected.
```

En el ejemplo anterior, la columna **PROCESSES** corresponde al PID del proceso de la cola de trabajos (jobs) CJQ0. Como este es un proceso de usuario, es contado y tratado como una sesión SQL; mientras este proceso este activo no se puede realizar un switchover de la base de datos. Se pueden verificar la cantidad de procesos activos de la siguiente forma:

```
SQL> SHOW PARAMETER JOB_QUEUE_PROCESSES;

NAME                              TYPE      VALUE

------------------------------ -------   --------------------

job_queue_processes               integer   5
```

Ahora, para lograr realizar el switchover sin problemas se debe establecer el valor de este parámetro a 0 de la siguiente forma:

```
SQL> ALTER SYSTEM SET JOB_QUEUE_PROCESSES=0;

Statement processed.
```

Se debe tener en cuenta que `JOB_QUEUE_PROCESSES` es un parámetro dinámico, por lo tanto su valor puede ser modificado y hecho efectivo sin necesidad de reiniciar la instancia.
A continuación se presenta una tabla que muestra los principales procesos que pueden impedir realizar un switchover.

Tipo de Procesos	Descripción	Acción para corregir el problema
CJQ0	Proceso del programador de la cola de jobs.	Cambiar el valor del parámetro `JOB_QUEUE_PROCESSES` a 0.
QMN0	Administrador avanzado de la programación de tiempo de la cola.	
DBSNMP	Agente administrador del Enterprise Manager.	

Tabla 4. Procesos que pueden impedir realizar un switchover

El switchover falla porque aun existen sesiones de usuarios activas

Si al realizar un switchover ocurre el error ORA-01093 "*Alter database close with no sessions connected*"; este error ocurre usualmente porque la instrucción `ALTER DATABASE COMMIT TO SWITCHOVER` al ser ejecutada cierra la bases de datos implícitamente, por tanto al tratar de ejecutarla con sesiones de usuario actualmente activas esta fallará. La solución para resolver este tipo de error esta en desconectar todas las sesiones de usuario que permanecen activas, para ellos se puede consultar la vista `V$SESSION` de la siguiente forma:

```
SQL> SELECT SID, PROCESS, PROGRAM FROM V$SESSION;
```

Los datos redo no se aplican en el sitio standby después de haber realizado el switchover

Este error puede ocurrir debido a que varios parámetros de inicialización no fueron propiamente establecidos después de haberse ejecutado el switchover. En este caso, las acciones a seguir para eliminar el error deberían ser:

- Chequear el fichero **tnsnames.ora** en el sitio primario y el **listener.ora** en el sitio standby. Deben existir entradas para el listener en la standby y los servicios deben sestar correctamente descritos en el sitio primario.
- Iniciar el listener en el sitio standby si no está iniciado.
- Revisar si el parámetro de inicialización **LOG_ARCHIVE_DEST_n** ha sido definido correctamente para trasmitir datos redo desde el sitio primario hacia el sitio standby. Para ver esto se puede realizar una consulta a la vista **V$ARCHIVE_DEST** como se muestra a continuación:

```
SQL> SELECT DEST_ID, STATUS, DESTINATION FROM V$ARCHIVE_DEST;
```

Si después de realizada la siguiente consulta no existe una entrada correspondiente para enviar datos redo hacia el sitio standby, entonces es necesario establecer los parámetros **LOG_ARCHIVE_DEST_n** y **LOG_ARCHIVE_DEST_STATE_n.**

- Definir los parámetros **STANDBY_ARCHIVE_DEST y LOG_ARCHIVE_FORMAT** correctamente en el sitio standby, de tal manera que sean aplicados correctamente en la localización destino.
- En el sitio standby, definir los parámetros **DB_FILE_NAME** y **LOG_FILE_NAME_CONVERT**. También, establecer el parámetro **STANDBY_FILE_MANAGEMENT** al valor **AUTO** si desea que la base de datos standby adicione automáticamente nuevos datafiles que sean creados en el sitio primario.

Realizar un rollback después de un switchover insatisfactorio

Para las bases de datos standby físicas, y en ocasiones donde un error ocurre durante el switchover, es posible revertir la base de datos a su estado inicial como primaria.

Conectarse a la nueva base de datos standby (primaria vieja) y ejecutar la siguiente instrucción SQL:

```
SQL> ALTER DATABASE COMMIT TO SWITCHOVER TO PRIMARY;
```

Si la instrucción anterior se ejecuta satisfactoriamente, entonces se debe realizar un shutdown (si es necesario) de la base de datos e iniciarla otra vez. Una vez iniciada, la base de datos volverá a correr bajo el rol primario.

Conclusiones

Durante el transcurso de este capítulo se describió paso por paso la propuesta de configuración e implementación con el objetivo de lograr un entorno de alta disponibilidad utilizando VMware ESX Server y Oracle Data Guard. Por tanto, se puede apreciar cómo la utilización de un entorno de virtualización ayuda a aprovechar al máximo las características y potencialidades del hardware, así como a elevar considerablemente los niveles de disponibilidad del sistema implementado. También, se describen aspectos importantes acerca de la monitorización del buen funcionamiento de un configuración Data Guard, principales errores a los que se podría enfrentar y cómo solucionarlos. Es importante destacar, que se ha demostrado que es viable utilizar ESX Server para construir una capa de virtualización para soportar sitios standby de un entorno Data Guard; observándose buen rendimiento de los sistemas standby y un uso bastante eficiente de los recursos de hardware utilizados.

Conclusiones Generales

A lo largo de la investigación se realizó un análisis de las características presentes en Oracle Data Guard y VMware que permiten el incremento de la alta disponibilidad en un Centro de Datos.

Al concluir el presente trabajo, con el fin de lograr una propuesta de implementación para el incremento de alta disponibilidad, protección de los datos y una rápida recuperación de los datos en un Centro de Datos, se arribó a la conclusión de que un entorno de virtualización, al presentar numerosas ventajas como: consolidación de servidores y optimización de infraestructuras, disminución de los costes de infraestructura física, flexibilidad operativa y capacidad de respuesta rápida, además de una amplia disponibilidad de aplicaciones y continuidad de los servicios; constituye un pilar fundamental en la consolidación de las características de alta disponibilidad de un Centro de Datos.

Después de tener concebido el entorno de virtualización se pudo constatar que el mismo brinda las potencialidades necesarias para sostener sistemas de bases de datos standby físicas comprendidos dentro de una configuración Oracle Data Guard, logrando un ambiente de alta disponibilidad y excelente protección de los datos. Ofreciendo una rápida recuperación ante desastres.

Como resultado de la investigación, se obtuvo una documentación actualizada que permite la comprensión y valoración de las tecnologías Oracle Data Guard y ESX Server, así como, una guía para la implementación y despliegue de estas.

Recomendaciones

Luego de concluir la investigación, se recomienda lo siguiente:

- Tener en cuenta las tecnologías VMware ESX Server y Oracle Data Guard en la implementación de un entorno de alta disponibilidad, protección de los datos y recuperación ante desastres.
- Continuar el estudio de las características que comprende ESX Server para consolidar una alta disponibilidad del entorno de virtualización.
- Utilizar e implementar la propuesta realizada en el Centro de Resguardo de Datos.

Referencia Bibliográfica

(1).El Semanal. [Online] [Cited: 01 10, 2009.] http://www.juniper.net/techpubs/software/screenos/screenos5x/translated/CE_v8_SP.pdf

(2).Desarrollo Web Alicante. [Online] [Cited: 01 15, 2009.] http://www.masadelante.com/faq-servidor.html

(3).Monografias. [Online] [Cited: 01 19, 2009.] http://www.monografias.com

(4).IconoCast. [Online] [Cited: 01 22, 2009.] http://www.iconocast.com/B000000000000032/W1/News3.htm

(5).EMC. [Online] [Cited: 01 22, 2009.] http://mexico.emc.com/solutions/business-need/business-continuity-availability/affordable

(6).AQB. [Online] [Cited: 01 22, 2009.] http://www.aqb.cl/soluciones.php?pag_codigo=2

(7).Oracle. [Online] [Cited: 01 26, 2009.] http://oracleracnotes.wordpress.com/2008/02/20/que-es-oracle-real-application-clusters

(8).Oracle Corporation. [Online] [Cited: 01 27, 2009.] http://www.oracle.com/technology/deploy/availability/htdocs/rman_overview.htm

(9). Oracle Corporation. [Online] [Cited: 01 27, 2009.] http://www.oracle.com/technology/products/dataint/htdocs/streams_fo.html

(10).Open System. [Online] [Cited: 01 28, 2009.] http://www.opensistemas.com/soluciones/sistemas_y_seguridad/paravirtualizacion_con_Xen

(11).Whyfloss. [Online] [Cited: 01 28, 2009.] http://www.whyfloss.com/pages/conference/static/editions/bsas07/charla10.pdf

(12). Abox. [Online] [Cited: 01 28, 2009.] http://www.abox.com/productos.asp?pid=676

(13).Parallels Virtualizacion. [Online] [Cited: 02 03, 2009.] http://www.parallels.com/screen_costum?/pag_?=4

(14).VMware. [Online] [Cited: 02 9, 2009.] http://www.VMware.com/lasp/pdf/

Bibliografía

VMware.[Online] [Cited: 02 05, 2009]
http://www.VMware.com/pdf/vi3_35/esx_3/r35u2/vi35_guideAdmin.pdf

VMware.[Online] [Cited: 09 05, 2009]
http://www.VMware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_config_max.pdf

Oracle.[Online][Cited: 15 12, 2008] http://www.oracle.com/index.html

Documentation Library.[Online][Cited: 01 15, 2009] http://www.oracle.com/pls/db111/homepage

Oracle® Data Guard Concepts and Administration.[Online][Cited: 02 20, 2009]
http://download.oracle.com/docs/cd/B28359_01/server.111/b28294/toc.htm

Oracle® Data Guard Broker.[Online][Cited: 04 10, 2009]
http://download.oracle.com/docs/cd/B28359_01/server.111/b28295/toc.htm

Oracle Data Guard 11g.[Online][Cited: 02 20, 2009]
http://www.oracle.com/technology/deploy/availability/pdf/twp_Data Guard_11gr1.pdf

David Marshall, Stephen S. Beaver, and Jase McCarty. *VMware ESX Essentials in the Virtual Data Center.* Paris : Ausbarch Publication, 2009. 978-1-4200-7027-9.

Tc. Gilberto Arias Izaguirre. *El Guardian de los Datos en Oracle 11g*. 2008.

Glosario de Términos

Fibre Channel : Canal de fibra, , es una tecnología de red utilizada principalmente para redes de almacenamiento.

iSCSI : (Internet SCSI) es un estandar que permite el uso del protocolo SCSI sobre redes TCP/IP.

HTTP : (HyperText Transfer Protocol) Es el protocolo de transferencia de hipertexto usado en cada transacción de la Web (WWW).

SSH : (Secure SHell) intérprete de órdenes seguro sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos y usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible.

SAN : (Storage Area Network en inglés) red de área de almacenamiento, es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte.

RAID : (Redundant Array of Independent Disks en inglés), arreglo redundante de discos independientes a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos.

LUN : *Logical unit number* es una dirección para una unidad de disco duro y por extensión, el disco en sí mismo.

NIC : (Network Interface Card en inglés)Tarjeta de Interfaz de Red , permite la comunicación entre diferentes aparatos conectados entre si y también permite compartir recursos entre dos o más equipos.

VLAN : Acrónimo de Virtual LAN, 'red de área local virtual' es un método de crear redes lógicamente independientes dentro de una misma red física.

CPU: (Central Processing Unit en inglés) la unidad central de procesamiento.

BIOS: (Basic Input-Output System en inglés) Sistema Básico de Entrada/Salida es un código de software que localiza y carga el sistema operativo en la RAM.

Dell: Compañía multinacional estadounidense establecida en Round Rock (Texas) que desarrolla, fabrica, vende y da soporte a computadores personales, servidores, switches de red, programas informáticos, periféricos y otros productos relacionados con la tecnología.

HP (Hewlett-Packard) Es la mayor empresa de tecnologías de la información del mundo. Fabrica y comercializa hardware y software además de brindar servicios de asistencia relacionados con la informática.

IBM: International Business Machines es una empresa que fabrica y comercializa herramientas, programas y servicios relacionados con la informática.

Fujitsu Siemens: es una marca de productos electrónicos para los mercados de Europa, Oriente Medio y África. Fabrica servidores Unix, ordenadores portátiles, de sobremesa, periféricos y ordenadores de bolsillo o PDA.

NEC: Nippon Electric Company es una compañía multinacional de tecnología y comunicaciones. La compañía está dividida en tres principales ramas: Soluciones IT, Soluciones de Comunicaciones y Dispositivos Electrónicos.

Sun Microsystems: Sun Microsystems es una empresa informática de Silicon Valley, fabricante de semiconductores y software.

TIC : Las tecnologías de la información y la comunicación son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

Anexos

Anexo 1

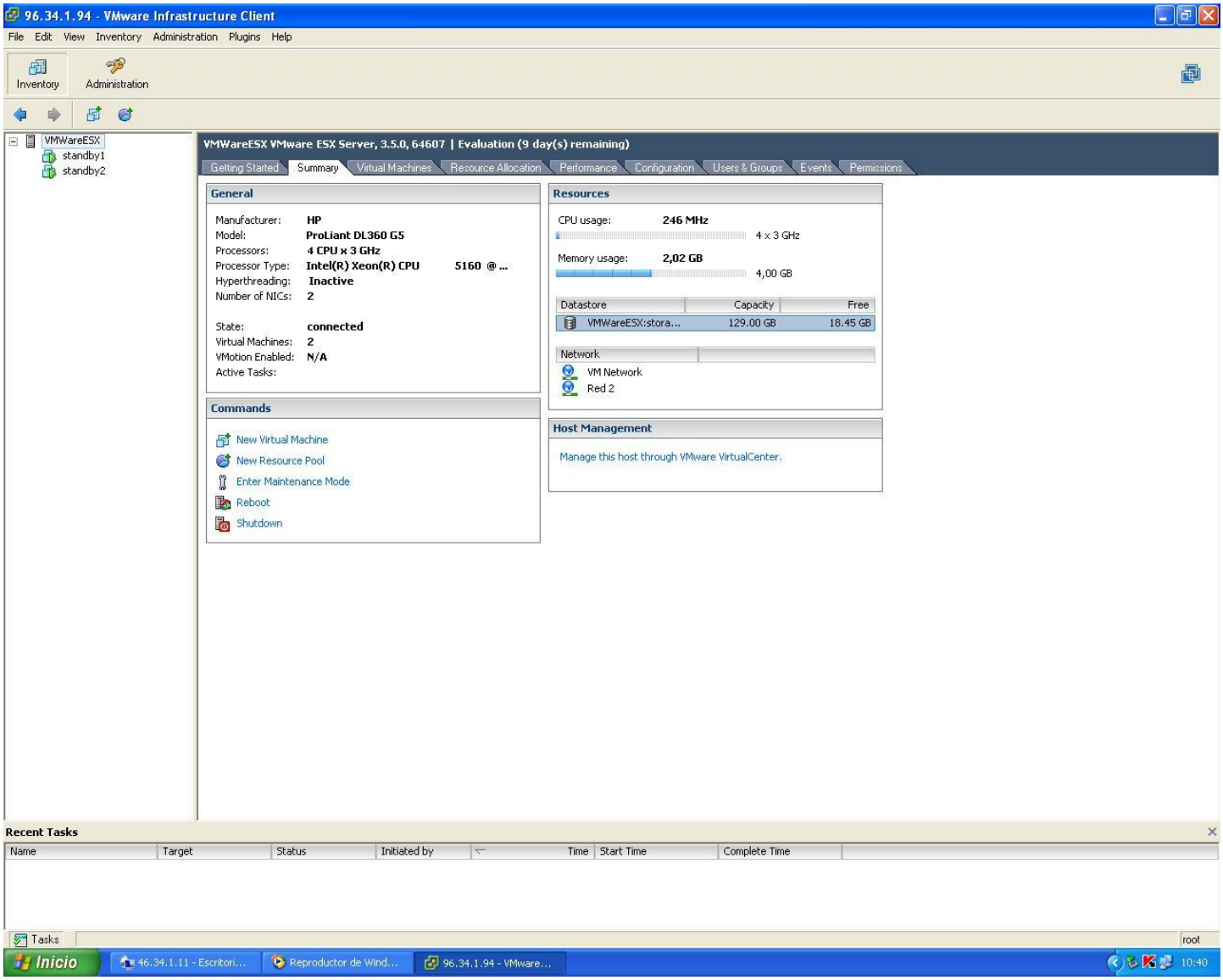

Imagen 1 : Pantalla de la vista general de la configuración del ESX Server

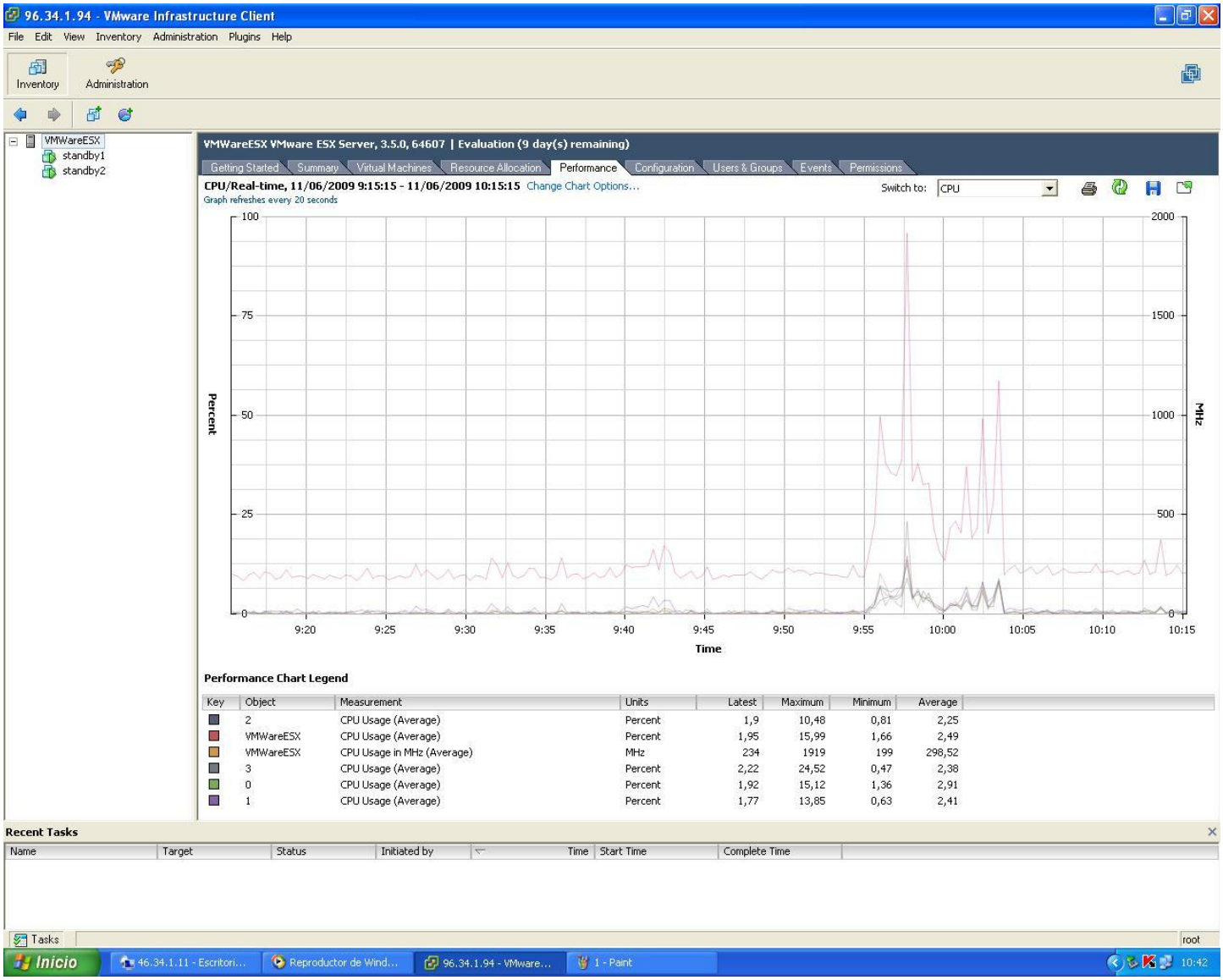

Imagen 2 : Pantalla del rendimiento del ESX Server

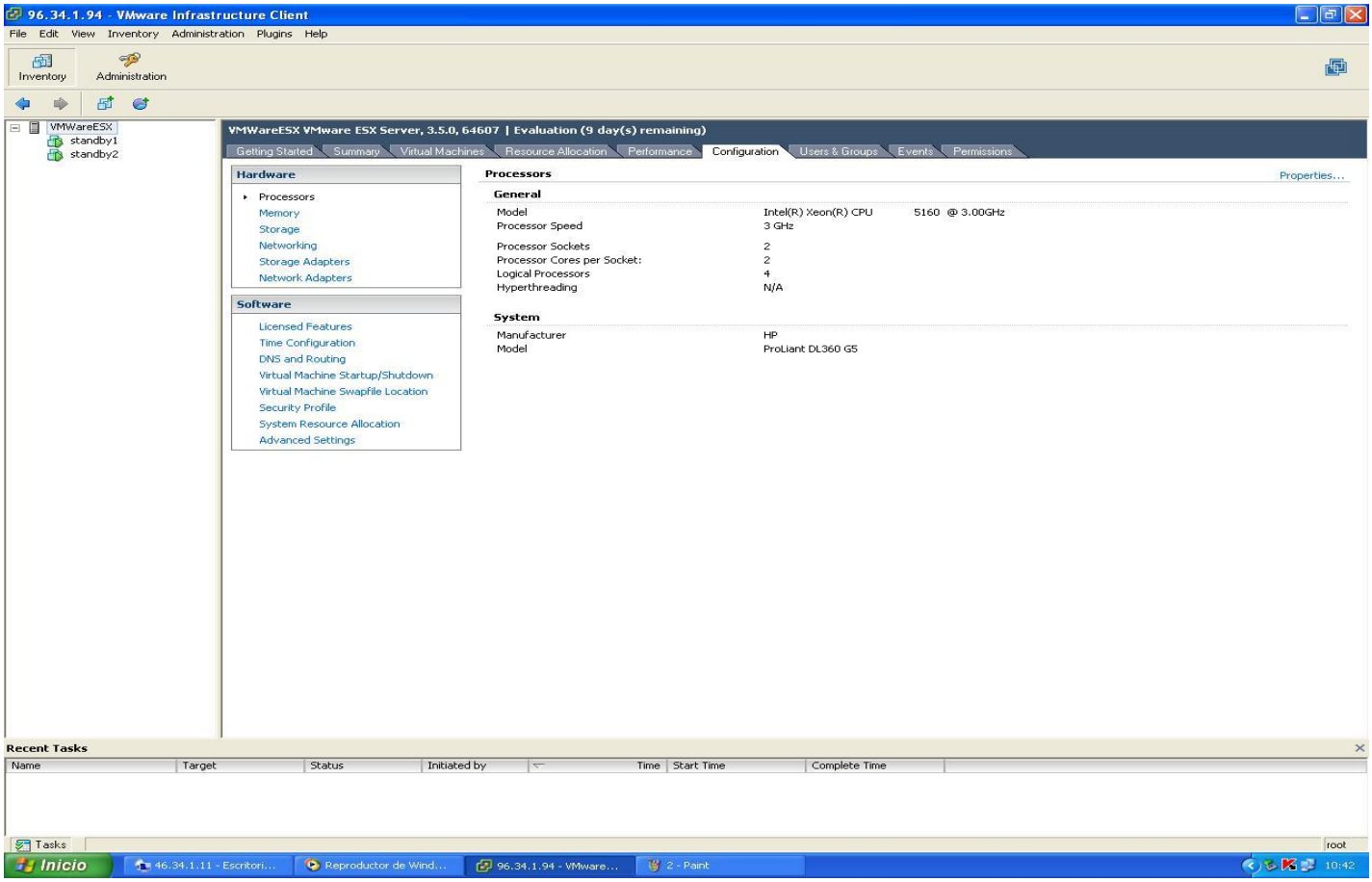

Imagen 3: Pantalla de las opciones de configuraciones del ESX Server

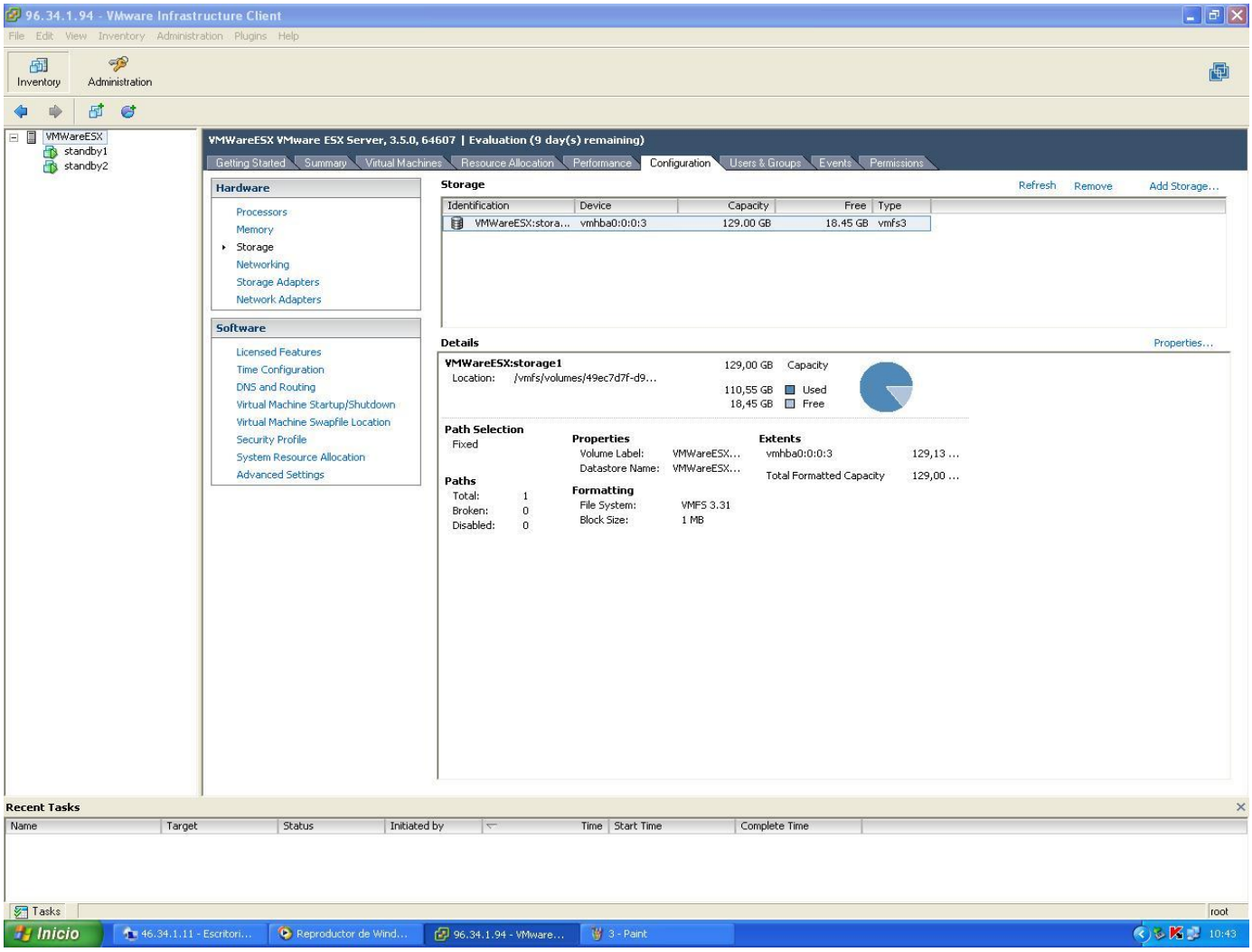

Imagen 4 : Pantalla de administración del almacenamiento

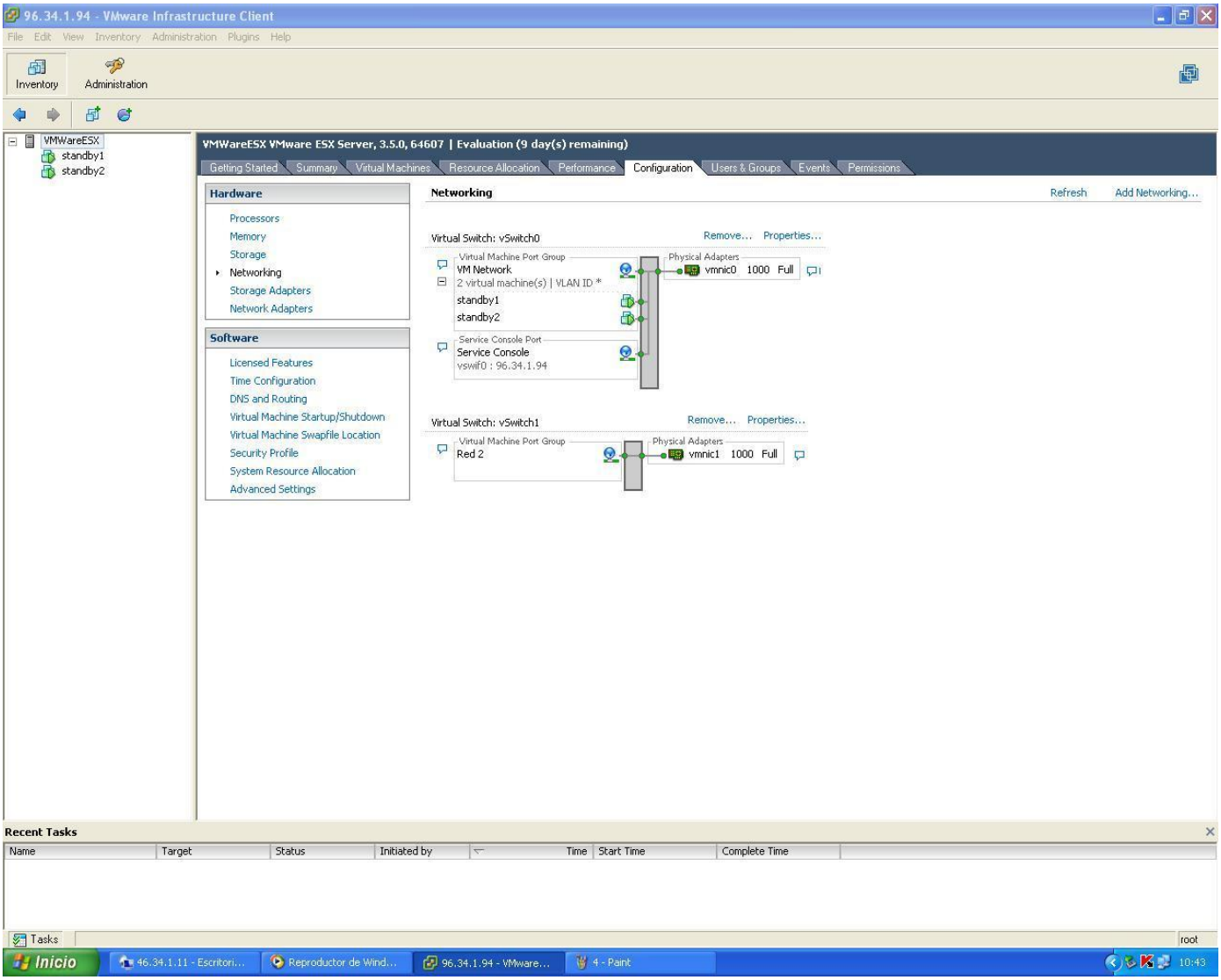

Imagen 5 : Pantalla opciones de redes

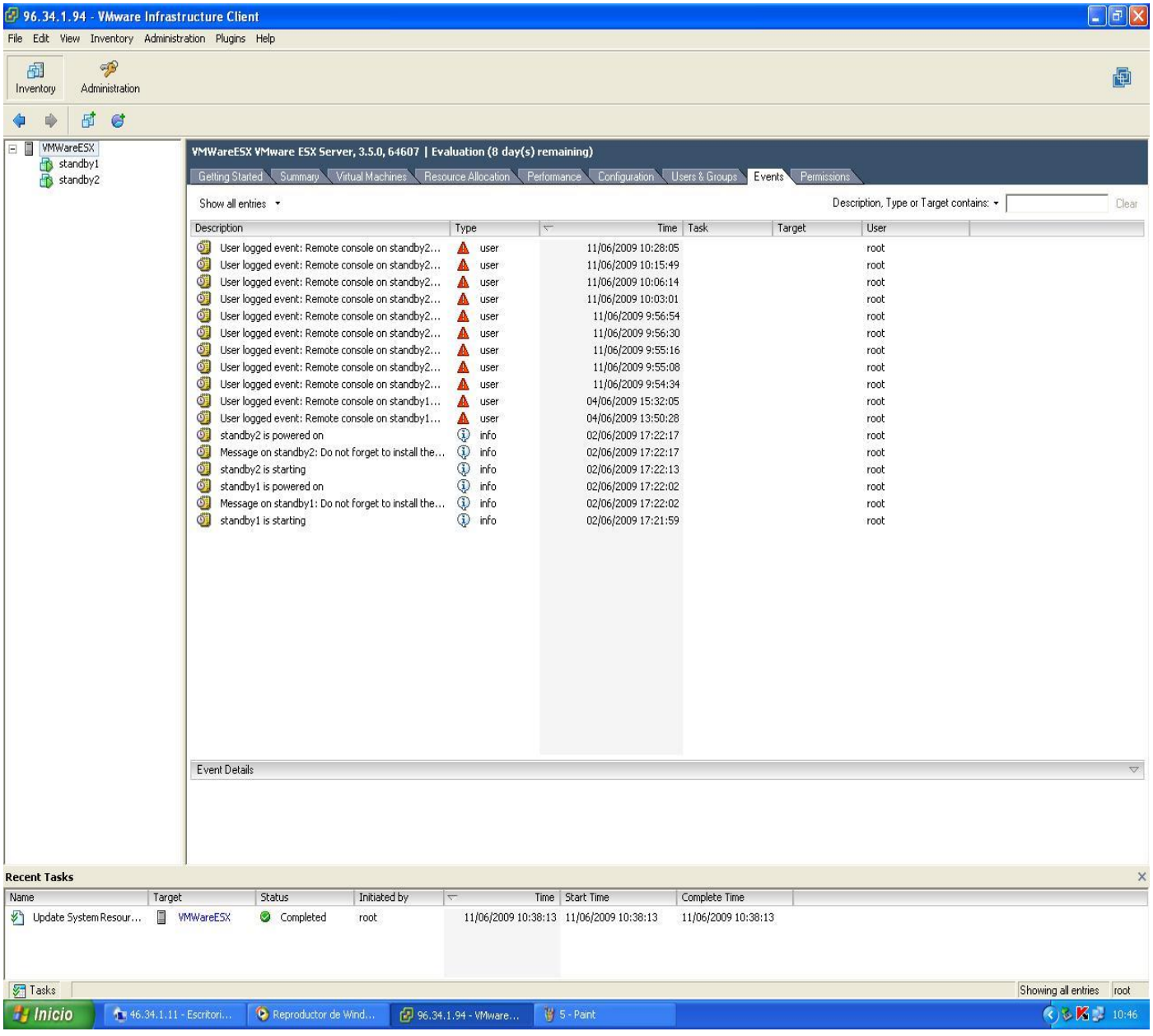

Imagen 6 : Pantalla de los log de Eventos que Ocurren

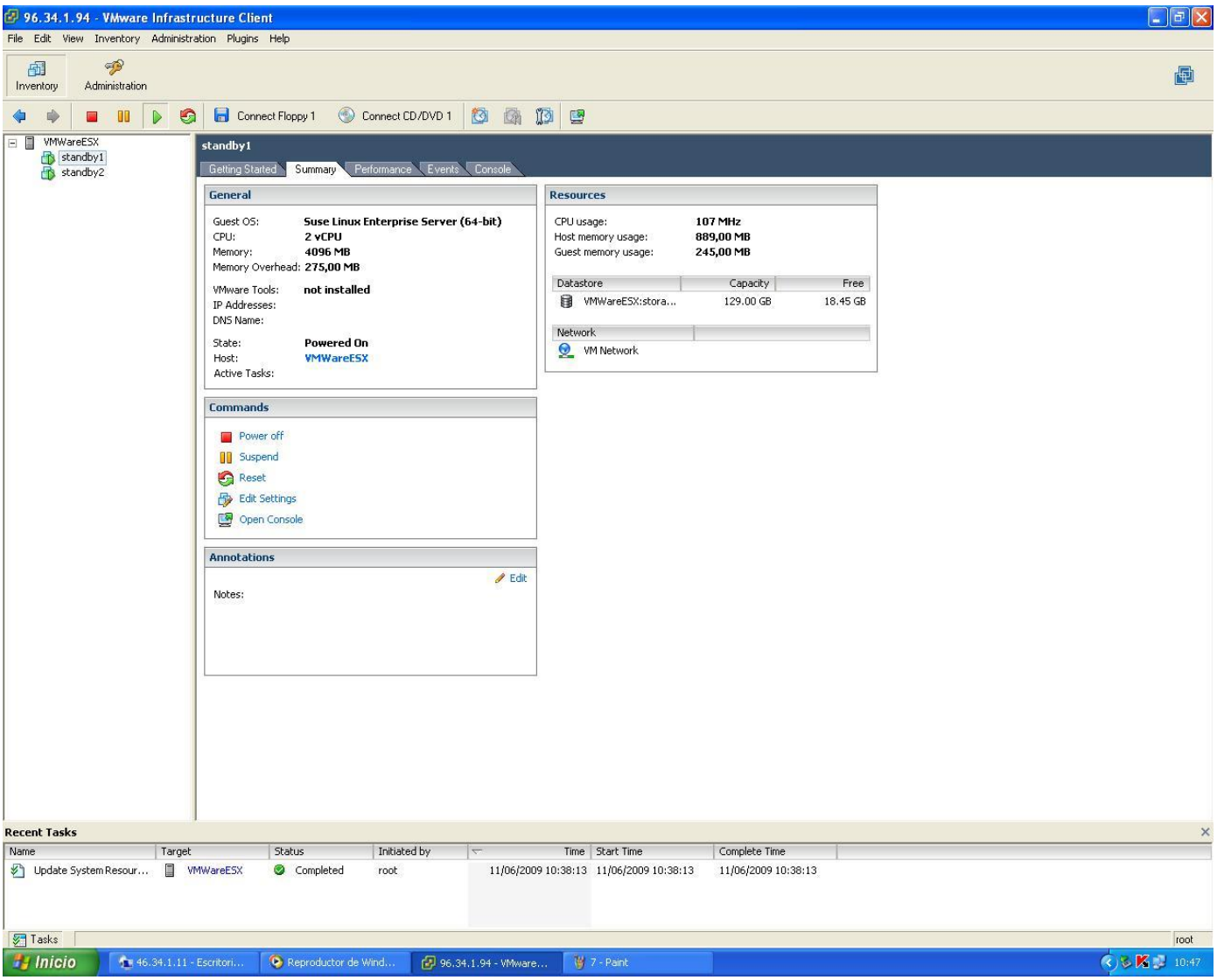

Imagen 7 : Pantalla de visión General de una Máquina Virtual

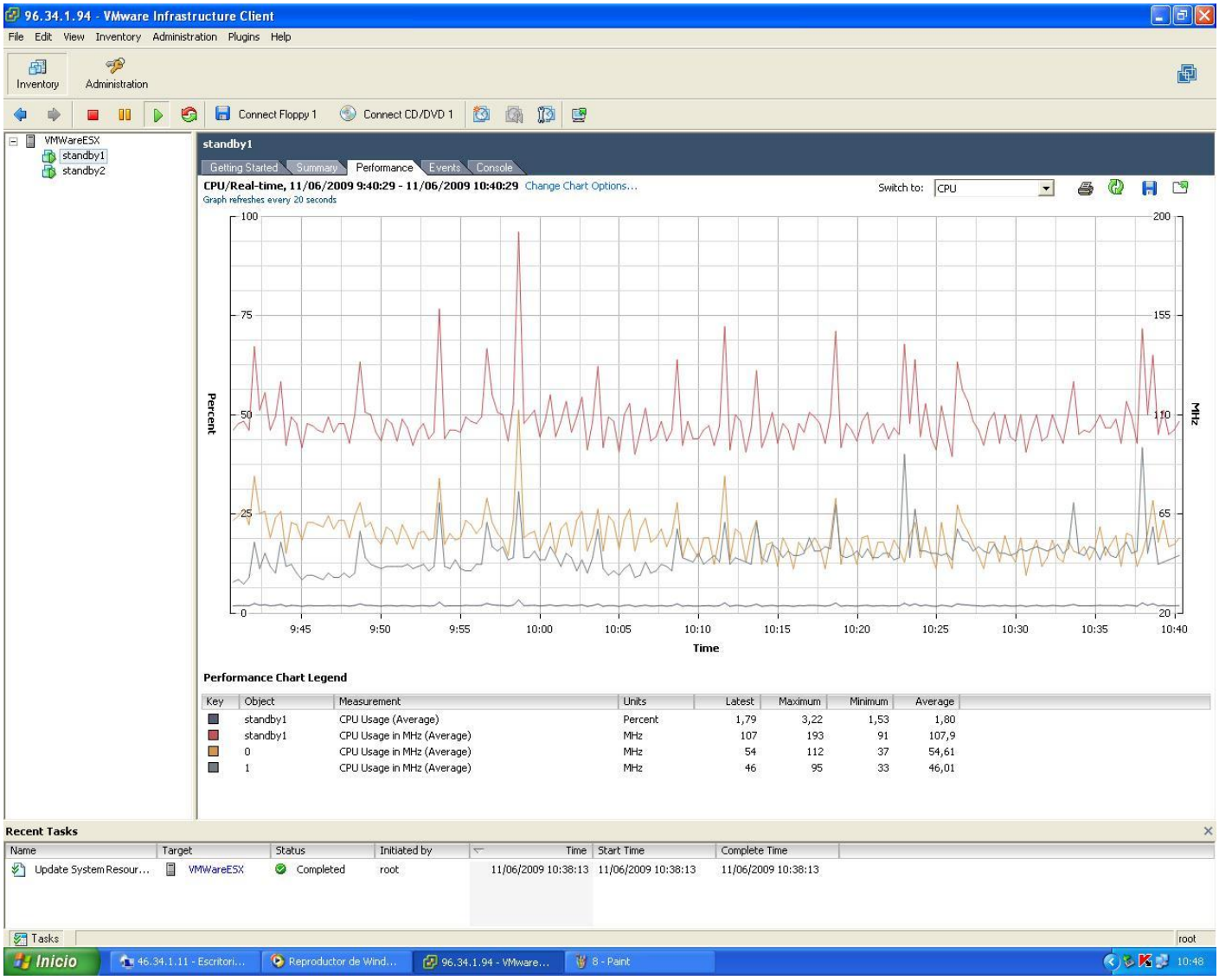

Imagen 8: Pantalla del rendimiento del CPU de una maquina Virtual