UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE CONTADURIA PUBLICA
Y ADMINISTRACION

TESIS

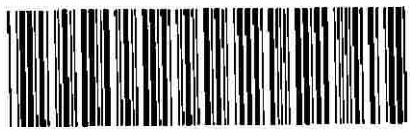
ANALISIS Y EVALUACION DE LOS ESQUEMAS DE ALTA DISPONIBILIDAD DE SISTEMAS PARA UNA OPERACION CONTINUA

POR

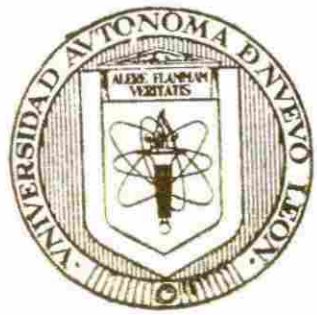
JESUS CABRAL RODRIGUEZ

COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE MAESTRIA EN INFORMATICA ADMINISTRATIVA

CD. UNIVERSITARIA MARZO DEL 2002



UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE CONTADURIA PUBLICA
Y ADMINISTRACION



TESIS

ANALISIS Y EVALUACION DE LOS ESQUEMAS DE ALTA DISPONIBILIDAD DE SISTEMAS PARA UNA OPERACION CONTINUA

POR

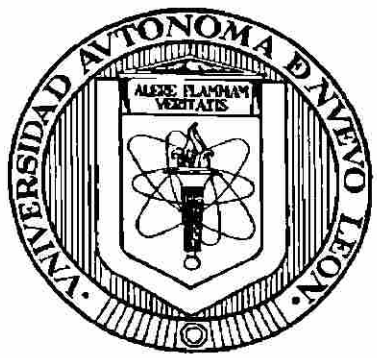
JESUS CABRAL RODRIGUEZ

COMO REQUISITO PARCIAL PARA OBTENER EL
GRADO DE MAESTRIA EN INFORMATICA
ADMINISTRATIVA

CD. UNIVERSITARIA MARZO DEL 2002

UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE CONTADURÍA PÚBLICA Y ADMINISTRACIÓN



T E S I S

ANÁLISIS Y EVALUACIÓN DE LOS ESQUEMAS DE ALTA DISPONIBILIDAD DE SISTEMAS PARA UNA OPERACIÓN CONTINUA

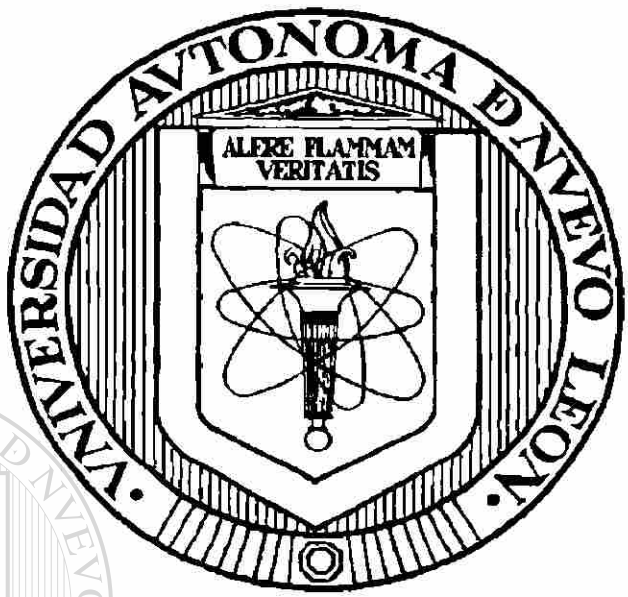
Por

JESÚS CABRAL RODRÍGUEZ

Como requisito parcial para obtener el Grado de

MAESTRIA EN INFORMATICA ADMINISTRATIVA

F e b r e r o, 2 0 0 2



RECTOR
DR. LUIS GALAN WONG

SECRETARIO GENERAL
ING. JOSE ANTONIO GONZALEZ TREVIÑO

SECRETARIO ACADEMICO
DRA. MA. ELIZABETH CÁRDENAS CERDA

DIRECTOR GENERAL DE ESTUDIOS DE POSTGRADO
DR. UBALDO ORTIZ MENDEZ

AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento al maestro director de tesis: Lic. MIA. Enrique Hernández Hernández, quién dedicó parte de su valioso tiempo para guiarme en el desarrollo de esta tesis, así como aconsejarme para definir más claramente mis objetivos.

Al M.S. Humberto Martínez Jiménez y M.A. Fernando Gutierrez Peón, por el tiempo dedicado a la revisión y evaluación de la presente tesis, así como por las acertadas recomendaciones que me permitieron reforzarla.

Al Subdirector de Informática de 7 Eleven México, Ing. Gustavo Treviño por permitirme participar en su proyecto de SAN y Alta Disponibilidad de Sistemas, aún cuando no pueda referir datos específicos al mismo (por confidencialidad), me ha sido útil como base para establecer los pasos a seguir para un proyecto de este tipo.

DEDICATORIA

A mi Esposa Irma Leticia Flores Padilla quién me apoyó durante el curso de la maestría, y me ofreció su comprensión durante el desarrollo de esta tesis. A mis hijos Iliana Mayté e Iván Jesús, que representan la luz de mi vida.

A mi madre Teresa Rodríguez Chaires, quien me enseño a luchar por salir adelante, y que siempre me exigió más en mi estudios iniciales, se esforzó en apoyar a la familia, y logró que esta fuera de bien para la sociedad.

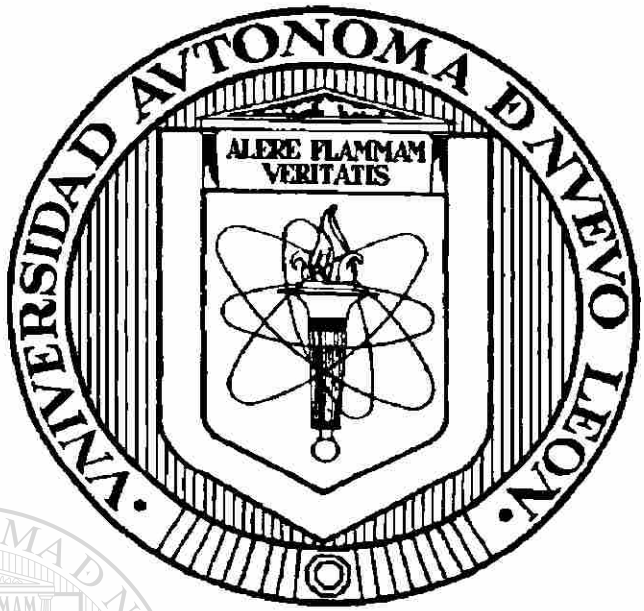


TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Capitulo

1 INTRODUCCIÓN

La era informática se ha ido desarrollando a pasos agigantados, llegando a ofrecer soluciones de alto nivel de desempeño, sin embargo, muchas veces existe aun la dependencia de elementos humanos que deben intervenir para activar un sistema o iniciar un proceso de recuperación en caso de falla. La alta disponibilidad de Sistemas define que en caso de que un sistema computacional falle, sus datos deben ser recuperados en una cantidad de tiempo razonable. La definición de "Razonable" varía ampliamente dependiendo del tipo de industria que esta operando. Sin embargo es de alta relevancia que el concepto sea aplicado en toda empresa que le dé importancia a su información.

Hubo un tiempo en que los conceptos de alta disponibilidad se asociaban con los bancos, y equipos mainframe fault-tolerant de precios excesivos para una empresa mediana o pequeña. Hoy las organizaciones pueden recibir el mismo nivel de disponibilidad a un costo mucho menor haciendo uso de sistemas abiertos.

La alta disponibilidad se basa en una mezcla de soluciones concertadas para remediar fallas en discos, aplicaciones, redes, sistemas operativos, y computadoras que afecten el flujo de información y operaciones que componen la base de una compañía.

Conforme se hacen diversos análisis, podremos ver que hay soluciones que pueden tomarse como obvias, pero que mientras no se haga este listado de posibles causas de fallas, no han sido visibles para nadie. Por ejemplo, puede ser obvio que mi red de área local puede fallar en

cualquier momento por lo que debería tener instalaciones alternas de red con tarjetas alternas y duplicar nodos de conexión, sin embargo, esto no se contempló en un principio por el costo que podria haber representado.

Una empresa especifica puede tener diseñados planes de contingencia que le permitan continuar con las operaciones teniendo los sistemas fuera de servicio (por fallas, mantenimientos, o respaldos), con un costo en la productividad Sin embargo, estos planes de contingencia que siempre deben existir deben ser lo últimos en aplicarse, siempre debe existir una solución de alta disponibilidad de sistemas, aunque esto puede implicar adquisición de más equipos y personal más preparado.

Para que una solución de Alta Disponibilidad tenga éxito en un largo plazo, se requiere del compromiso de las Gerencias y del personal de Sistemas de Información para ir evolucionando en su ambiente operacional, enfocando los esfuerzos en las personas, procesos y la tecnología. Además la empresa debe establecer métricas que indiquen el cumplimiento del requerimiento de Alta Disponibilidad: ¿Será suficiente que el sistema garantice su operación al 96%? ¡Esto sería aproximadamente 2 semanas al año sin servicio por fallas!

Es importante tener bien claro las necesidades propias de la empresa o sector para determinar como proporcionarle una solución real y factible Si tus operaciones dentro de la empresa son de enfoque científico, muy difícilmente podrás hallar una solución de alta disponibilidad

1.1 Hipótesis

"No existe una metodología establecida para el desarrollo de proyectos de alta disponibilidad, por lo que basado en mi experiencia, y con el fin de apoyar futuros proyectos de Alta Disponibilidad propondré como parte de mis conclusiones una metodología para el desarrollo de los proyectos de alta disponibilidad"

1.2 Objetivos del Proyecto

Se pretende hacer un análisis de los distintos conceptos de alta disponibilidad que existen actualmente, investigando requerimientos tecnológicos, humanos y económicos requeridos para su aplicación.

Basándose en estos conceptos, se presenta un ejemplo de evaluación costo / beneficio de la implementación de un proyecto de alta disponibilidad.

Clarificar que la alta disponibilidad no significa que el sistema este operando el 100% del tiempo

Que impacto tiene para una empresa de comercio electrónico el que su sistema de comercialización en línea este fuera de servicio.

El crecimiento de los costos de implementación y administración de un sistema en alta disponibilidad según se incrementa el porcentaje de disponibilidad ofrecido

El tiempo máximo al año que un sistema en alta disponibilidad puede estar fuera de servicio según el porcentaje de disponibilidad esperado Algunos niveles de disponibilidad no podrán ser garantizados aún con la tecnología actual

Mostrar que partes de un sistema impactan más en la disponibilidad del mismo.

La importancia que la alta administración este involucrada y consciente del costo que implica para la empresa el no tener un sistema en alta disponibilidad

Los sistemas se deben organizar de acuerdo al nivel de disponibilidad esperado, no todos los sistemas se deben configurar con el mismo nivel de disponibilidad, deberán clasificarse por nivel de impacto dentro del negocio contra el costo de la inversión a realizar.

Explicar que un esquema de recuperación de desastres es un nivel de Disponibilidad Continua y Alta Disponibilidad más avanzado y que implica requerimientos más complejos los cuales no son el enfoque de esta tesis

1.3 Alcance

Esta es una la evaluación de los esquemas de alta disponibilidad en el manejo de cluster On-Site: Los esquemas de recuperación de desastres y operación de Sites Remotos pertenecen a un rubro de estudio por si mismos, por lo que fueron excluidos de este material.

Se presenta un procedimiento general que podría seguirse para la implementación de un esquema de alta disponibilidad La información técnica solo se detalla lo necesario para enfocar el tema y clarificar los pasos usuales que deben seguirse para esta implementación Este procedimiento general es solo una posible guía de apoyo para iniciarse en el tema.

Debido a la alta dinámica de los mercados de aplicaciones y software, los productos aquí mencionados pudieran haber quedado desactualizados con respecto a la fecha en curso Por la misma causa, los productos mencionados no son todos los que existen, pero si nos ayudan a ubicar las áreas comunes entre ellos así como las diferencias básicas entre los mismos

Como existe suficiente material sobre cada producto como para definir un proyecto por si solo, el material presentado prescinde de profundidades altamente técnicas, principalmente para poder hacer una revisión rápida de las semejanzas y diferencias entre los productos, tal que nos ayude a formar una idea más clara de los conceptos de alta disponibilidad.

1.4 Antecedentes

¿Quién puede necesitar de una Alta Disponibilidad en sus Sistemas? La respuesta es todo aquel que se precie de darle importancia a su negocio. Todo negocio que trabaje en un esquema de 7x24 o que no pueda sufrir de cortes de servicio por un tiempo mayor de 2 minutos o hasta un máximo de 30 minutos (según la definición de alta disponibilidad que tenga la empresa)

En 1995 dos investigaciones llevadas a cabo por Oracle Corporation y por Datamation mostraron que los negocios habían perdido en promedio entre 80,000 y 350,000 dólares por hora debido a fallas no planeadas En 1993 la bomba que se colocó en el World Trade Center provocó que 145 de los 350 negocios que se ubicaban en este edificio cerraran por no contar con una infraestructura redundante de Sistemas que les permitiera continuar las operaciones o recuperar la información de sus transacciones.

Con base en estos datos, es claro que el configurar y mantener una infraestructura redundante de Sistemas es un bajo precio comparado contra la pérdida del negocio por no haber hecho este esfuerzo Además, habrá de considerarse que los tiempos fuera (downtime) de los sistemas pueden deberse a fallas no planeadas así como a mantenimientos preventivos. Si contamos con esquemas de Alta Disponibilidad, estos mantenimientos se podrán realizar sin afectar la continuidad de los servicios en ningún momento

Conforme las empresas de todos los tipos continúan implementando sistemas de mayor complejidad y poderío, la disponibilidad de las aplicaciones, hacia los usuarios a través de la organización, se ha convertido en algo importante

La ecuación de disponibilidad involucra un número de elementos que deben funcionar como parte de un todo. La red, la plataforma de hardware, sistema operativo, y software de aplicaciones. Históricamente, los responsables de los departamentos de Sistemas se han enfocados en la plataforma de hardware, sin evaluar que, sin un desempeño confiable del sistema, la disponibilidad de la aplicación sería imposible. Al mismo tiempo, conforme las infraestructuras de redes se convierten en parte vital de las organizaciones, se incrementa la atención prestada al desempeño de ruteadores, hubs y elementos específicos de la red.

Investigaciones realizadas por IDC (International Data Corporation) muestran que las organizaciones de clientes y usuarios están volviéndose más conscientes de que un sistema con mayor tiempo de operación y una red más confiable no garantizan por sí solo la disponibilidad máxima de la aplicación.

Existen varios detonantes que presionan para lograr mejores esquemas de alta disponibilidad

La Internet – Quizás uno de los mayores detonantes de los requerimientos de alta disponibilidad, ha empujado a muchas organizaciones de todos los tamaños y de todas las industrias hacia una dependencia de los servicios de información y tecnología en un esquema 7x24x365 (Las 24 horas de la semana y los 365 días del año.) Hoy con la revolución del e-comerce que está cambiando *literalmente* los modelos de negocio hacia negocios que operen por la noche, los clientes buscan proveedores que operen bajo la WWW (World Wide Web) Muchas empresas que tienen cierto número de clientes en el día (en América) probablemente lograrán otro número nuevo de clientes por la noche (En Europa y Asia) . Esto no solo se aplica a empresas comerciales, sino también empresas de manufactura que pueden recibir pedidos via Internet de productos de "materia prima" para procesamiento adicional por parte de un cliente, ciertamente en estos casos primero habrá una negociación previa para que el cliente y el

proveedor puedan abrir una línea de crédito, pero una vez establecida, será una muy natural forma de levantar pedido, aún cuando el personal laboral de la empresa no esté en oficinas en ese momento, muchos sistemas de pedidos, basándose en los datos preconocidos del cliente enrutan y programan pedidos para su procesamiento en forma automática.

Integración de los procesos de negocio a la tecnología de información. Al igual que las necesidades de disponibilidad para Internet, los procesos de negocio se integran más y más a la tecnología de información, hasta niveles en que no se distingue entre el proceso y la aplicación que lo habilita. Por ejemplo, la habilidad de la organización de almacenar y recuperar la información de los clientes. Anteriormente se manejaban los legajos y gabinetes, ahora es mediante herramientas de datawarehouse y minería de datos que se ha logrado una transformación total de está actividad. Adicionalmente con esta transformación, la importancia de esta actividad se ha incrementado, hasta niveles en los cuales, una implementación pobre, puede llevar a una compañía a una perdida competitiva real.

Globalización de los mercados y negocios. Otro de los factores que están demandando de mejores niveles de disponibilidad, es la rápida globalización de los negocios y las organizaciones. En la actualidad, muchos negocios tienen sistemas de información distribuidos, un sistema de servicio de intranet cuyo servidor este ubicado físicamente en Hong Kong al fallar puede afectar las operaciones de la compañía en lugares como París, Nueva York, o Los Ángeles. Tal nivel de impacto era impensable hace algunos años, cuando aún las compañías multinacionales realizaban instalaciones de sistemas en forma regional, local o nacional, concentrando posteriormente la información mediante procesos de consolidación.

Las nuevas tecnologías requieren de la mas alta disponibilidad de los sistemas y aplicaciones de la compañía para garantizar la competitividad. Uno de los factores más impactantes es el mercado electrónico el ***e*-business**, es precisamente en esta nueva área tecnológica donde él

dejar de ofrecer servicio, a causa de un sistema fuera (downtime) que, implica grandes pérdidas. No solamente se pierde un cliente que llega al sitio de Internet a buscar un producto que comprar, sino que además este cliente seguramente se irá a un competidor, si este le dio un buen servicio, seguramente este cliente ya nunca regresará. Pero además, si este cliente comenta como adquirió ese producto y como **nuestro** sitio no le dio el servicio, y como el competidor inmediatamente lo atendió, seguramente hemos perdido al menos otras 10 ventas. Multipliquemos esto por el número de clientes que no pudieron acceder a nuestro sitio en este mismo momento.

Algunas investigaciones han mostrado que las empresas están invirtiendo en combinaciones de sistemas de alta disponibilidad con sistemas identificados de misión crítica. Se espera que para finales del 2002 la demanda de servicios de alta disponibilidad se incremente. En Estados Unidos de Norteamérica, se ha presentado el siguiente comportamiento.

Rubro	1997	1998	1999	2000	2001	2002
Hardware						
Inversion en Soporte de Hardware de mision critica	646	719	774	857	926	995
Inversion total en hardware	12,663	12,399	12,288	12,240	12,187	12,133
Porcentaje de la inversion en Mision Critica	5.1%	5.8%	6.3%	7.0%	7.6%	8.2%
Software						
Gastos de soporte en software de mision critica	553	702	885	1,101	1,348	1,626
Gasto total en software	8,782	10,172	11,806	13,591	15,674	17,869
Porcentaje de la inversión en mision critica	6.3%	6.9%	7.5%	8.1%	8.6%	9.1%
Total						
Inversion total en soporte a la mision critica	1,199	1,421	1,660	1,958	2,274	2,621

Total invertido	21,445	22,571	24,094	25,831	27,861	30,002
Porcentaje de la inversión en misión crítica	5.6%	6.3%	6.9%	7.6%	8.2%	8.7%

Tabla 1. Inversiones para el soporte de aplicaciones de misión crítica:[1]
Nota. Estos gastos no incluyen las inversiones hechas en infraestructura y dispositivos de alta disponibilidad en servicios específicos de redes (millones de dólares.)

Los vendedores de hardware han realizado inversiones cuantiosas para proporcionar servicios de alta disponibilidad, pero con tecnología propietaria Con la llegada de nuevos sistemas operativos como ocurre con Windows NT, los proveedores de hardware (HP, IBM, Compaq y otros) se han visto forzados a desarrollar soluciones de alta disponibilidad que no nacen en sus plataformas y que no son desarrollados por ellos mismos Ahora esta ocurriendo que estos proveedores de hardware son empujados a competir entre ellos, con un sistema operativo que es elaborado por un tercero (Microsoft)

Existen productos de terceros que en forma independiente del sistema operativo Windows NT 2000, pero basándose en asociaciones estratégicas han desarrollado métodos de ofrecer soluciones de alta disponibilidad, uno de estos ejemplos, es la solución ofrecido por Oracle con su producto "Real Application Clusters", el cual pretende ofrecer una solución de disponibilidad continua con recursos propios, no dependientes directamente del S O

[1] **International Data Corporation** high availability Not just for hardware anymore an IDC whitepaper

Capitulo

2 MARCO TEÓRICO

2.1 Conceptos de alta disponibilidad y requerimientos para su funcionalidad

Se hará una referencia a las definiciones y conceptos básicos que nos permitirán profundizar en el tema de la alta disponibilidad.

2.1.1 ¿Que es la Alta Disponibilidad?

Minimización del número y duración de ocurrencias planeadas o no planeadas de suspensión de servicio de los sistemas que soportan la operación de una compañía, por mantenimientos preventivos, o por fallas de los mismos

Nivel de Servicio es el periodo esperado de servicio disponible y tiempo aceptable de servicio no disponible.

2.1.2 Definición de Alta Disponibilidad

Un sistema que es diseñado, puesto en práctica y desplegado con componentes suficientes para satisfacer las exigencias funcionales del sistema, pero el que también tiene la redundancia suficiente en componentes (el hardware, el software y procedimientos) para enmascarar ciertas fallas definidas, tiene Alta Disponibilidad (HA) Esta definición es ambigua. los

términos(condiciones) "suficientes", "enmascarar" "ciertas" requieren una clarificación más profunda En vez de hacer esto, sin embargo, debemos enfatizar que debido a esta ambigüedad, existe un gran número y clases de configuraciones que con esta definición pueden ser clasificadas como de "Alta Disponibilidad".

Definamos ahora con más detalle los términos(condiciones) ambiguos

- **El Enmascaramiento** de una falta implica el proteger de la observación externa de la falla. Este acercamiento es el equivalente computacional del adagio filosófico " Si un árbol se cae sin nadie para oírlo, este no hace ningún sonido ". El enmascaramiento es una técnica "de juego de manos" para asegurar no el hecho de que la falta ocurra, sino que esta no sea observable

  Recordemos que las faltas son definidas como una desviación inesperada del comportamiento especificado El enmascaramiento de una falla significa que ninguna desviación (o más precisamente que las desviaciones definidas) del comportamiento especificado ocurre Esto invariablemente se logra mediante un mecanismo de réplica apropiado al componente, una estrategia de redundancia. Cuando un componente falla, el componente redundante lo sustituye El grado de transparencia en la que este reemplazo ocurre puede conducir a una amplia variación de los sistemas que se llaman de "Alta Disponibilidad" Tenemos el siguiente espectro de enmascaramiento existentes:

  - **Manual Masking: Enmascarado Manual(MM)**. Después de una falla de un componente, se requiere alguna acción manual para poner el componente redundante en servicio, durante este tiempo el sistema no estará disponible para el su uso La expectativa usual es que la HA implica una recuperación automatizada

De ahí, los sistemas que usan "el enmascaramiento manual" generalmente no son considerados HA)

- **Cold Standby (CS) réplica parcial (o sustituto en frió)** Después que un componente falla, los usuarios del componente son desconectados y pierden cualquier trabajo en progreso (esto es, ellos regresan la transacción operada a un pasado consistente, y estable de su trabajo) Un mecanismo automático de detección de falla y recuperación descubre la falla, y ponen en servicio el componente redundante Este componente redundante ha permanecido inactivo y deberá ser inicializado para entrar en servicio. Una vez que esto es hecho, los usuarios son capaces de continuar su proceso desde el punto hasta donde se regresó su transacción Típicamente el tiempo requerido para que el proceso de detección de fallas descubra esta falla e invoque el componente redundante es bastante bajo (decenas de segundos) Sin embargo, el tiempo requerido para la inicialización del componente redundante puede ser mucho más largo. Este tiempo de recuperación es dependiente de la aplicación, pero por lo general implica la limpieza de los filesystems, bases de datos y otros recursos persistentes hacia un estado consistente de información, que fácilmente puede tomar decenas de minutos.

- **Warm Standby (WS) réplica en Caliente (o sustituto parcial).** Después de que un componente falla, los usuarios del componente son desconectados y pueden perder parte de su trabajo en progreso. El mecanismo automático de detección y recuperacion de fallas descubre la falla y notifica al componente redundante para que asuma la operación. Este componente redundante ha estado corriendo activamente y esta parcialmente inicializado Además, este puede ya estar compartiendo algo del estado de procesamiento de su par fallado. De ahí, no

necesariamente deberá reiniciarse todo el trabajo en progreso. Los clientes del componente todavía deben unirse activamente al nuevo componente redundante Los tiempos de detección de falla para los sistemas en Warm Standby son similares a los que tienen los sistemas en Cold Standby, pero los Tiempos de recuperación son dramáticamente más cortos que en el CS (típicamente algunas decenas de segundos), debido a la inicialización parcial y estado operacional compartido.

- **Hot Standby (HS)/Active Replication(AR) Réplica en Caliente/Replicación Activa (o Sustituto en Caliente/Replicación Activa)**. Los Componentes activos y Redundantes están fuertemente acoplados en grupos y son (lógicamente) indistinguibles a los usuarios del grupo de componentes En realidad, el usuario no "ve" el grupo sino sólo el comportamiento requerido del componente. El Estado de Procesamiento es compartido activamente y completamente entre los componentes de grupo. Después de una falla de uno de los componentes del grupo, los usuarios del componente no son desconectados y no observan la falla de ningún modo El trabajo en progreso sigue con el(los) componente(s) en redundancia que restan en el grupo que proporciona la funcionalidad del componente En este modelo, el enmascaramiento es completo y transparente - los clientes del sistema no son interrumpidos

Los tiempos de recuperación son instantáneos – con más exactitud, el concepto de tiempos de recuperación no se aplicaría, puesto que desde la perspectiva del cliente no hay ninguna recuperación El término "Réplica Activa" se prefiere sobre "Reserva en Caliente", puesto que éste último hace referencia a una relación asimétrica entre un componente "Activo" y uno "De reserva" (o en espera) concepto utilizado en los términos "Reserva en Frío" y "Reserva Parcial" El término

"Réplica Activa" refleja mejor, sin embargo, la simetría entre las replicaciones. Vamos a referirnos a esto como Reserva en Caliente/Replicación Activa (HS/AR).

- **La Suficiencia** es una reflexión de las exigencias del sistema para la Alta Disponibilidad (¡una definición recurrente!) Por ejemplo, un sistema diseñado para apoyar la tolerancia de fallas de hardware sólo podría enmascarar fallas de hardware, pero no fallas de software. Esto sería "suficiente" para las exigencias de aquel sistema, y tal sistema no enmascararía fallas de aplicación

  La práctica Aceptada, sin embargo, es usar el término " Tolerancia a Fallas " (Fault-Tolerance) para tales sistemas de solo-enmascarado-de-hardware, mientras el término " Alta Disponibilidad " es reservado para el sistema que enmascara fallas en el hardware, en el software y en los procesos Siguiendo esta convención, " la redundancia suficiente " en la definición de Alta Disponibilidad anterior implica que deben enmascararse tanto las fallas del hardware, del software y de los procesos

  Además de la determinacion de que las fallas son enmascaradas, La Suficiencia también refleja cuantas veces son enmascaradas Por ejemplo, un acercamiento de par-empatado reproduce cada componente exactamente una vez, esto es "suficiente" para soportar(resistir) un solo punto de falla Por otra parte, un sistema en el que cada componente tiene n>2 replicaciones puede sobrevivir más fallas simultáneas (donde "simultáneo" implica que las fallas ocurren dentro de la ventana de reparación del primer componente que falló)

- **La Certeza**, como se usa en la definición de HA, se reconoce del hecho que no todas las faltas pueden ser enmascaradas, por esta razón se debe establecer con certeza que fallas si son enmascaradas, cualquier otra falla no establecida con certeza, no sería enmascarada

definitivamente Por ejemplo, algunos errores de diseño, y que son reproducibles, raras veces son enmascarados. Así un sistema que se supone, autentifica a un usuario antes de permitir el acceso, pero cuyo diseño no lo estableció correctamente, bajo ningún nivel de replicación se corregirá esta falta, y con algunos intentos repetidos los usuarios hostiles podrán fácilmente exponer la falta y lograr el acceso.

Existen técnicas como la programación n-way para poder atacar esta clase de faltas, sin embargo, estas técnicas raras veces se usan debido a su complejidad y costo. De ahí que se reduce el juego de fallas que serán compensadas en un sistema Alta Disponibilidad. Este conjunto de restricciones, puede conducir a una amplia variación de sistemas que se llaman a sí mismos de "Alta Disponibilidad".

2.1.3 Acrónimos y Abreviaciones[2]

Existen términos, acrónimos y abreviaciones que se usan con frecuencia para referirnos a temas de alta disponibilidad, la tabla 2 menciona algunos de los mismos.

Acrónimo	Nombre	Definición
BA	Basic Availability Disponibilidad Básica	Un sistema cuya ingeniería ofrece un servicio funcional, pero que no hace ninguna prevencion para atrapar las fallas.
CA	Continuous Availability (Disponibilidad Continua)	Enmascara completamente los cortes de servicio planeados o no planeados La Alta Disponibilidad HA es un subconjunto de la disponibilidad continua (CA) La disponibilidad continua asume el uso estricto del modelo de replicación activa Hot Standby (Copia de Sustitución caliente)
HA	High Availability	Enmascarado automático de cortes de servicio no planeados, puede

[2] Acronyms And Abreviations from "A Modern Taxonomy of High Availability"

	(Alta Disponibilidad)	implementarse mediante replicación en frío, incremental o en caliente.
MM	Manual Masking (Enmascarado Manual)	Concepto de seudo disponibilidad (muy débil) que utiliza la replicación mediante rutinas dentro del sistema, pero que requiere detección manual y acciones de recuperación Debido a esto no cumple con las condiciones de HA (Alta Disponibilidad) de reactivación automática.
CS	Cold Standby (Sustituto en Frío)	Es la más débil forma de Alta Disponibilidad, se generan réplicas completas de la instalación, pero no se tiene la información actualizada, por lo que al presentarse una falla el servicio reinicia con una fuerte perdida de información.
WS	Warm Standby (Sustituto Parcial)	Forma moderada de alta disponibilidad, se generan réplicas de la información y se actualizan parcialmente, y pueden tener algunos estatus de procesamiento en preparación para una falla.
HS	Hot Standby (Sustituto en Caliente)	Esta es el modelo más fuerte de Alta Disponibilidad, las réplicas son copias en línea y que comparten el estatus con la instalación primaria. De hecho, no se puede diferenciar directamente entre la instalación primaria y la instalación de recuperación. Esto hace que el término "primario" sea más a forma de referencia que otra cosa.
AR	Active Replication (Replicación Activa)	Técnica usada para obtener la Disponibilidad proporcionada por la Replicación en Caliente (o Sustituto en Caliente) "Hot Standby".
LR	Passive (Lazy) Replication (Replicación Pasiva)	Técnicas aplicadas para obtener un Sustituto Parcial del sistema (Warm Standby).
MFP	Make Forward	Termino aplicado a sistemas con Replicación Activa (Hot Standby)

	Progress (Avanzar la Operación)	que acentúa que los clientes y usuarios de los sistemas en operación no pueden verse interrumpidos en sus operaciones o actividades en el evento de una falla, y que estos deben continuar operando normalmente sin perder un solo cambio de su operación.
RR	Rollback and Recover (Regreso y Recuperación)	Término aplicado a los sistemas con replicación parcial o en frío Warm/Cold Standby que enfatiza que los usuarios y clientes de un sistema que dejo de operar sufrirán una interrupción mínima de servicio, y deberán regresar algunas de sus operaciones hasta un estado de procesamiento que sea consistente antes de reiniciar el proceso de recuperación de la falla.
MTTF	Mean Time To Failure (tiempo medio para fallar)	Promedio de vida de un componente que operará hasta fallar.
MTTR	Mean Time To Restore (Tiempo medio de recuperación)	Tiempo promedio requerido para reparar un componente y reactivar el sistema, o tiempo promedio requerido para restaurar el servicio despues de una falla
MTBF	Mean Time Between Failures (Tiempo promedio entre fallas)	Es el tiempo transcurrido desde que se inicia el servicio hasta que se reinicia nuevamente el servicio MTBF MTTF+MTTR
	Availability (Disponibilidad)	A MTTF / (MTTR + MTTF)
HVAC	Heating, Venting and Air Conditioning	Equipo de calefacción, ventilación y enfriado

	equipment	
UPS	Uninterruptable Power Supply	Fuente ininterrumpible de poder

Tabla 2. Algunos acrónimos y abreviaciones de alta disponibilidad

2.1.4 Algunos términos

Cluster: Existen diversas definiciones de cluster, algunas son:

1) Conjunto de servidores configurados para proporcionar los servicios computacionales, y recibir la carga operacional en caso de que uno de los nodos falle.
2) Conjunto de servidores configurados para ofrecer servicios computacionales en grupo donde cada nodo ofrece un servicio específico y funcional, y el grupo ofrece un servicio total
3) Conjunto de servidores organizados para balancear la carga de trabajo entre ellos, y poder ofrecer servicios computacionales con un alto nivel de desempeño.
4) Arreglo de Servidores dedicados a atender peticiones específicas de operación, y servidores redundantes que se encuentran en estado de espera para soportar la carga de trabajo en caso que el servidor primario llegará a fallar

Los Tipos de cluster existentes serían:

- **Cluster Elástico y Escalable**: Servidores acoplados en forma sencilla, y que contiene múltiples sistemas unidos mediante un esquema de balanceo de cargas. Son cluster escalables horizontalmente. Los sistemas no interfieren ni consideran a otros sistemas en el mismo cluster. Las instancias de aplicación se administran en forma autónoma, con transacciones y juegos independientes de datos, que se replican a los nodos en forma individual a través de la

red, o vía un servidor NFS. Los nodos se administran en forma individual, apoyado mediante prácticas y procedimientos locales que facilitan su manejo.

- **Cluster para Performance** Este tipo de clusters es típico para sistemas computacionales de alto desempeño (HPC), que se enfocan en el desempeño y escalabilidad de sistemas al aplicar tantos procesadores (CPU) como sean posibles para resolver un problema o cálculo específico La mayoría de los clusters científicos usan alguna forma de procesamiento por lotes, o software de trabajo compartido Este tipo de clusters no tiene capacidad elástica, en caso de una falla de la aplicación o sistema, debe existir un sistema de verificación del nivel de avance y su mecanismo de recuperación, para poder reiniciar el procesamiento de los lotes que han fallado

- **Cluster para Alta Disponibilidad** Este tipo de clusters agrega capacidades de alta disponibilidad, al montarse sobre la infraestructura del sistema operativo. La disponibilidad se logra al usar scripts que monitorean la sanidad de los nodos individuales del cluster En caso de falla en los servicios (debido a fallas en discos, redes, o los servicios de la aplicación misma) los recursos y las aplicaciones serán asignados y reiniciados en otro nodo. Los nodos individuales del cluster, se administran principalmente en forma independiente uno del otro.

Failover Evento en el cual el cluster reubica una aplicación de un nodo que ha fallado hacia un nodo sano, perdiéndose las operaciones que se estaban llevando a cabo en el nodo fallado, el otro nodo del cluster adquiere el control de los recursos y levanta los servicios del nodo fallado para soportar los requerimientos operacionales Los clientes del cluster pueden ver una ligera interrupción en los servicios, pero no se deberán darse cuenta del cambio de servidor

Failback Evento donde el servidor primario de un cluster reinicia sus operaciones retomando nuevamente el control de los recursos y levanta los servicios que un nodo secundario estaba proporcionando a causa de un failover. Esto es, regresar los servicios al servidor que esta identificado como proveedor primario de los mismos.

Escalabilidad. Habilita que un servicio cumpla niveles crecientes de carga, al mismo tiempo que se entrega la misma calidad de servicio Una aplicación escalable hace uso de los múltiples nodos en un cluster al correr varias instancias de los mismos servicios de aplicación Permite así mismo que a un nodo se le incremente su capacidad (en una ventana de mantenimiento), mientras los otros nodos cubren el servicio que este nodo debe proporcionar, al terminarse el mantenimiento este nodo toma sus recursos y ofrece mejores niveles de servicio Al nivel aplicativo, la escalabilidad se proporciona mediante el paralelismo, donde las transacciones individuales pueden ejecutarse en paralelo en varios nodos del cluster a la vez, esto requiere que el software de la aplicación soporte el paralelismo y sea responsable de sincronizar los datos. Cada instancia de la aplicación seria responsable de atender

Elasticidad· Capacidad de la aplicación, o sistema de resistir las fallas, soportando la migración de actividades hacia otro nodo de un cluster, con el menor tiempo de corte de servicio, y con el menor efecto visible hacia el usuario de un sistema.

2.1.5 Como medir la Disponibilidad esperada[3]

En un nivel simple, la disponibilidad, ya sea alta, baja o media se puede medir como una parte del tiempo que un servicio se tiene operando normalmente Es decir, el período de tiempo que el

[3] Chapter II What is resiliency from Blueprints of High Availability 1st Edition, Marcus Evans & Halt Stern Editorial John Wiley & Sons, Inc

sistema está realmente disponible durante el tiempo que debería estar disponible, se puede expresar mediante la fórmula:

Disponibilidad = MTTF / (MTTF+ MTTR)

Donde MTTF es el tiempo transcurrido para fallar (mean time to failure) y MTTR es el tiempo promedio de resolución de la falla (mean time to restore).

Aquí podemos observar que.

1. Según el MTTR se acerque a cero, la disponibilidad se acercará al 100%.
2. Conforme el MTTF (Tiempo transcurrido para fallar) se incremente, el MTTR tendrá un impacto menor en la medida de Disponibilidad

Por ejemplo, si un sistema particular tiene un MTTF de 100,000 hora, y el MTTR es de 1 hora, esto nos da un nivel impresionante de Disponibilidad de 100,000/100,001, o un total de 99 999 por ciento. Si se reduce el MTTR a 6 minutos (o 1 décimo de una hora) la disponibilidad se incrementa a un 99.9999 por ciento. Pero para lograr este nivel de disponibilidad requerirías de componentes cuya duración real entre fallas fuera de 100,000 horas que es alrededor de 11.4 años Dicho de otra forma: para lograr un porcentaje de 99.9999 de disponibilidad, cualquier parte o componente especifico deberá durar al menos 11.4 años sin fallar y cuando falle solo dispondrás de un máximo de 31.5 segundos por año (o 6 minutos en 11 4 años) para recuperarte de la falla Pero estos 6 minutos sin servicio son para todo el sistema, no sólo para un componente específico Con la tecnología actual, esto es inalcanzable y no realista Quizás sea más realista pedir que los tiempos máximos de resolución de fallas sean de 10 minutos al año, lo cual nos da un total de 99 998 % de disponibilidad y lo cual sea probablemente más alcanzable. Pero será muy difícil subir de este valor

A continuación se muestra la relación[4] entre el nivel de disponibilidad (cuantos nueves) y el impacto de tiempo máximo fuera de servicio hasta recuperarse de la falla

Porcentaje de Disponibilidad	Porcentaje de Tiempo fuera	Tiempo Fuera x Año	Tiempo Fuera x Semana
98%	2%	7.3 Días	3 horas 22 minutos
99%	1%	3.65 Días	1 hora 41 minutos
99.8%	0.2%	17 horas 30 minutos	20 mins. 10 Segundos
99.9%	0.1%	8 horas 45 minutos	10 mins. 5 segundos
99.99%	0.01%	52 mins 30 segundos	1 minuto
99.999%	0.001%	5.25 minutos	6 segundos
99.9999%	0.0001%	31.5 segundos	0.6 segundos

Tabla 3. medida del nivel de disponibilidad

2.1.6 Términos Relevantes a la discusión de la Alta Disponibilidad

Para el tema que nos concierne es necesario definir algunos términos y así poder comprender el enfoque de la alta disponibilidad, y allanar el camino hacia el desarrollo de esta tesis

[4] Table 2 1/Chapter II Measuring Availability from Blueprints of High Availability 1st Edition, Marcus Evans & Halt Stern Editorial John Wiley & Sons, Inc

2.1.6.1 Sistema en Alta Disponibilidad[5]

Cuando nos referimos a un sistema en HA, hacemos mención no solo del programa de aplicaciones y operaciones que se utiliza, sino, a una amplia gama de componentes que lo conforman y que soportan el todo como una sola unidad, algunos de estos son tomados en cuenta para el diseño del modelo de HA y otros definitivamente no son involucrados en los mismos, ya sea por su complejidad, por su irrelevancia, o simplemente porque el factor costo / beneficio no es suficiente para justificarlo.

Los componentes usualmente incluidos como parte de un sistema en HA, muchas veces no fueron necesariamente hechos bajo el enfoque de HA (Alta Disponibilidad), pero que deberemos considerar en el diseño de un sistema en HA

1) Hardware del Servidor que se requiere bajo una implementación distribuida
2) Discos y dispositivos de almacenamiento asociados al servidor
3) Software de aplicaciones implementado como parte del ambiente configurado de servidor.
4) Software de Sistema Operativo y para servicios de comunicación, y dominios
5) Conexiones de Red (Lan y Wan) que permiten un ambiente distribuido,
6) El hardware de escritorio (Clientes PC o Workstations) usado en un ambiente de trabajo distribuido
7) El software de aplicaciones implementado en el hardware de escritorio
8) El software de sistema operativo y herramientas de soporte que se implementan como parte del ambiente del equipo cliente (Herramientas GUI, utilerías de acceso a la informacion, etc).

[5] Definitions from "A Modern Taxonomy of High Availability"

9) Comunidades de usuarios (personas) que utiliza las herramientas GUI para operar las aplicaciones existentes en el equipo servidor.
10) La comunidad administrativa(personas) que administran y mantienen el sistema implementado y a su comunidad de usuarios
11) Los procedimientos administrativos, las políticas y lineamientos de seguridad utilizados en un ambiente operacional (Respaldos, Almacenamiento histórico, administración de perfiles de usuario, etc.)

Los componentes que usualmente no son incluidos en el diseño de un sistema en HA son:

1) El ambiente para la construcción del modelo de HA, que se compone de los ambientes de definición y creación usados para configurar el comportamiento del sistema, pero que no formarán parte final del mismo cuando quede ya en producción, estos ambientes se consideran temporales y no se plantean como parte de la solución final
2) Sistemas heredados (o sistemas preexistentes) con los cuales el Sistema habrá de interactuar pero que no son parte de él per se Estos sistemas pueden tener sus propios diseños de HA pero no están coordinados con el diseño del Sistema actual
3) Elementos y comunidades de personas que no interactúan con el sistema Por ejemplo, clientes del negocio que interactúan con los usuarios de los sistemas pero que no tocan directamente al sistema directamente, así como las áreas de administración y planeación.

Ver la figura 1 para evaluar que es lo que si se incluye usualmente en los modelo de sistemas de Alta Disponibilidad, y que es lo que no se incluye usualmente en estos modelos

2.1.6.2 DownTime (El Corte de Servicio)

La definición de DownTime varía mucho desde una definición amable, hasta una definición estricta, y desde sencilla hasta compleja Una definición estricta puede implicar que se tiene un DownTime cuando la red esta lenta o el servidor tiene bajo desempeño, o simplemente cuando un sistema no esta operando

La mejor definición la dan Marcus Evans y Hal Stern en su libro "Blueprints of High Availability" y es la siguiente: ***Si un usuario no puede lograr hacer su(s) tarea(s) a tiempo a causa del sistema, entonces, el sistema esta abajo, o ha fallado (es decir, tenemos un Downtime).***

Figura 1. Las distintas causas de fallas de sistemas

Existen múltiples causas de Cortes de Servicio, como se muestra, sin embargo, de los cortes de servicio el 30% corresponde a mantenimientos y actualizaciones de aplicaciones, sistema operativo, software crítico, o quizás es readecuación de arreglos, reorganización de los datos, etc otras ocasiones corresponde a depuración de logs, directorios y archivos temporales y limpieza de memoria

Muchos de los mantenimientos de hardware con la tecnología de muchos proveedores, se pueden hacer en línea, sin dar de baja los servicios Arreglos con discos reemplazables en

caliente, algunas aplicaciones se pueden remplazar en línea. Algunas veces se mueve la operación a otro equipo en un esquema de cluster para la alta disponibilidad

Otro factor es el recurso humano, a veces el usuario no sabe como debe realizar alguna tarea especifica y comete algún error drástico que provoca la caída de la aplicación, la mejor forma de combatir estos errores es incluir en el diseño del sistema en HA un desarrollo amigable y sencillo de usar, así como un plan de educación y entrenamiento continuo sobre el manejo del sistema, así como el establecer como un rubro de este diseño, la necesidad de documentación solidamente preparada y siempre a la mano.

La parte más sorprendente en el DownTime es aquel relacionado con las fallas de Hardware. Este DownTime representa sólo el 10% del total de los cortes de servicios. Es decir, que con el mejor arreglo de discos (RAID) y un gran número de discos, tarjetas de red, y CPU's redundantes, así como el mejor hardware de redes del mundo, solamente estaríamos previniendo la ocurrencia del 10% de los cortes de servicio totales[6].

El factor de mayores causas de corte de servicio es el software de aplicaciones que esta operando, los bugs en el software de aplicaciones son los más difíciles de eliminar del sistema.

[6] Causes of Downtime, Chapter II What is resiliency, Blueprints of High Availability, Evans Marcus & Hal Stern

2.1.6.3 Faltas, Fallas y su relación con DownTime

Una falta es una desviación del comportamiento esperado de un sistema. Es decir, si el sistema

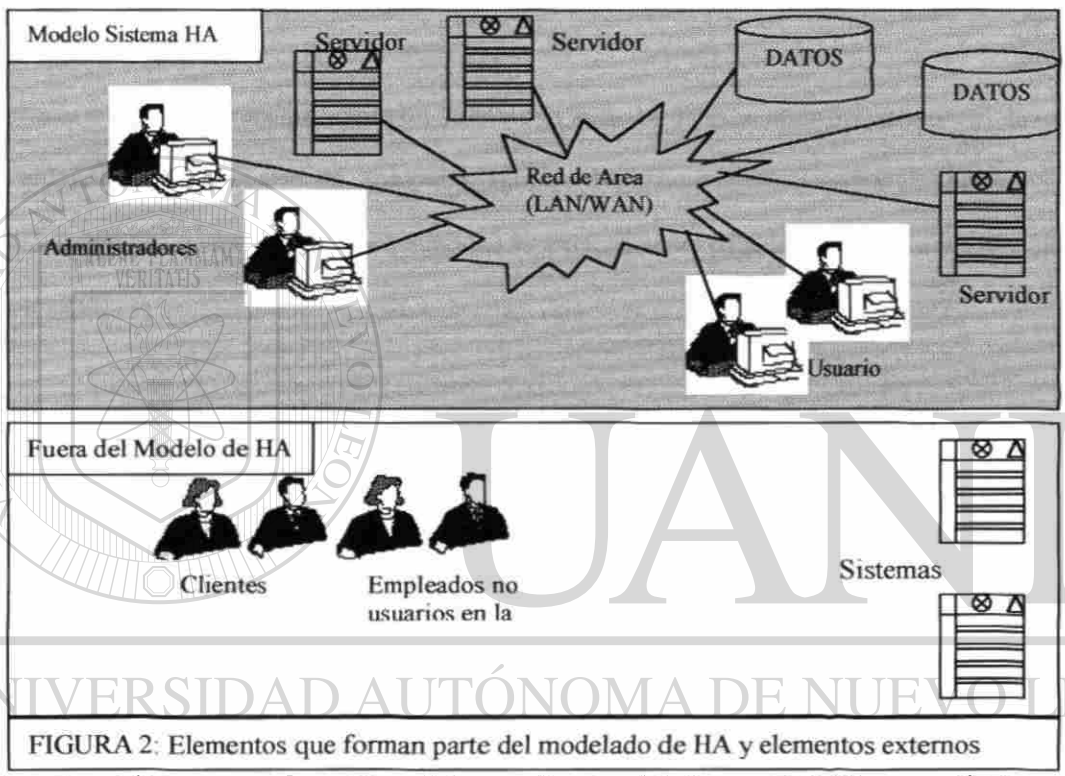


FIGURA 2: Elementos que forman parte del modelado de HA y elementos externos

está configurado para proporcionar y exhibir una funcionalidad muy específica, y en el proceso de ejecución el sistema produce una diferencia funcional que es palpable, entonces una falta ha ocurrido. El sistema proporciona la funcionalidad requerida mediante un procedimiento contenido en el software que se ejecuta en un hardware que involucra Equipos cliente, servidores, redes, almacén de datos, y otros periféricos Las faltas pueden presentarse en los procedimientos, software o hardware y pueden clasificarse como reproducibles o no reproducibles

Faltas Reproducibles: Un conjunto prescrito de pasos que lleva a observar la presentación de la falta en forma predecible.

Faltas no reproducibles La aparición de la falta se presenta en forma aleatoria o no determinada, o esta asociada a un origen o raíz que se encuentra fuera del sistema que se ha implementado.

Debemos siempre diferenciar entre una falta y una falla. La falta es el no-cumplimiento de una funcionalidad dentro del sistema, que puede ser palpable o no palpable externamente al usuario final La falla por su parte es aquella falta que es externamente palpable como una interrupción del servicio.

Ejemplos de faltas

- Error de diseño de la aplicación, la funcionalidad no es como se espera.
- El usuario debe ser validado pero esto no ocurre.
- El cálculo de un valor debe ser a+b pero se codificó para efectuar a−b
- Una falta es un acceso erróneo a un valor en memoria (siempre y cuando no provoque la caída del sistema)

Ejemplos de fallas

- La ocurrencia de una falta que efectúa una acceso erróneo a un valor en memoria y que provoca la caída del sistema.
- Una falla en un dispositivo de hardware Disco duro, tarjeta de red.
- Una falta de diseño que provoca que se sobrecargue de procesos un servidor, provocando una falla del sistema y caida del mismo

Las fallas se clasifican en diversos ramos, algunas se denominan fallas fuertes· Son fallas que al correr un conjunto de pasos se presentan en forma idéntica y en la misma forma. Otras se denominan fallas Suaves. Son fallas que al correr un conjunto de pasos pueden presentarse ocasionalmente y otras no. La alta disponibilidad es muy útil y permite atacar a las fallas suaves, pero no es tan eficiente con las fallas duras.

2.1.6.4 Disponibilidad Básica

Un sistema que es diseñado, puesto en práctica y desplegado con componentes suficientes (el hardware, el software y procedimientos) para satisfacer las exigencias funcionales del sistema, pero no más, tiene la Disponibilidad Basica (BA) Tal sistema entregará la funcionalidad correcta mientras que no ocurran faltas / fallas y no se realicen operaciones de mantenimiento, etc. Siempre que una falta ocurre o una operación de mantenimiento es realizada, sin embargo, se observa una interrupción del servicio. Los sistemas de Disponibilidad Típicamente Básicos son desplegados como simples sistemas (no reproducidos)

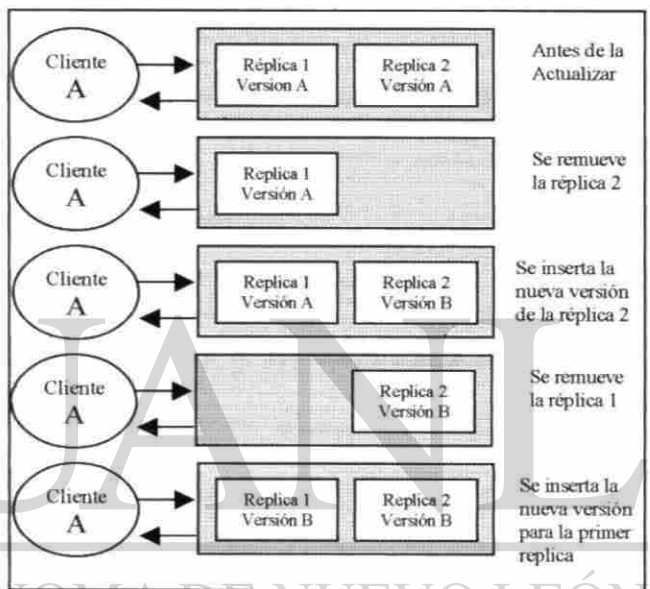


Figura 3: Pasos para lograr la disponibilidad básica

2.1.6.5 Disponibilidad Continua

La Disponibilidad Continua (CA) amplía la definición de Alta Disponibilidad, sobre fallas no planeadas, y lo aplica a interrupciones planeadas también. Consistiendo entonces en un sistema que enmascara ambas (interrupciones imprevistas así como interrupciones planeadas) Los

Sistemas Continuamente Disponibles deben tener una estrategia de enmascarar que se ocupa de interrupciones planeadas Implicando una definición más vigorosa, mientras que la HA permite una variedad de estrategias para enmascarar (reserva en frío, reserva parcial y reserva en caliente), el sistema CA se limita a operar exclusivamente con el modelo de "Reserva en Caliente / Réplica Activa" - el enmascaramiento transparente debe ser completo, no solamente para fallas, sino para interrupciones planeadas también.

Para reconocer las dificultades inherentes a esto, consideremos las implicaciones para una mejora de software:

- Al principio, dos procesos idénticos son las réplicas uno del otro.
- Para realizar una mejora, una réplica se saca de servicio, y se substituye con la nueva versión mejorada.
- Al ponerse en línea la nueva versión en la réplica 2 debe absorber el estado de procesamiento de la versión 1.
- Posteriormente el segundo par (la réplica 1) se da de baja y la réplica 2 con la nueva versión toma el control de los clientes.
- Finalmente, el sistema totalmente replicado se recrea con ambas copias actualizadas a la versión B. Por supuesto que para alcanzar esto, las versiones A y B deben ser lo suficientemente compatibles para compartir el estado de procesamiento entre ellos. También, los clientes (que típicamente tienen un ciclo operativo independiente,

representado como la Versión X), deben ser capaces de inter funcionar transparentemente a través de ambas versiones A y B de servidor.

Todas estas cuestiones de compatibilidad dependen del estado de procesamiento de la aplicación y el comportamiento esperado, no hay soluciones "fáciles" para estas exigencias. De hecho, si la actualización de la Versión A hacia la B es bastante significativa (por ejemplo una gran cantidad de nuevas funcionalidades adicionales se implementan en la Versión B), esto no será posible en lo absoluto

2.1.6.6 Dominios para la Alta Disponibilidad

La definición de los componentes que un sistema en alta disponibilidad debe contemplar, no implica que todos estos componentes se repliquen para poder obtener de ellos una disponibilidad alta o continua En su lugar, el sistema deberá decomponerse para identificar y establecer cuales componentes tendrán disponibilidad básica, alta o continua Adicional a esto, si el componente del sistema estará bajo el esquema de alta disponibilidad es necesario identificar si la replicación será con enmascaramiento manual, reserva en frío, reserva parcial, o reserva en caliente / replicación activa. De esta forma podremos seccionar los sistemas en HA en dominios de disponibilidad, por las siguientes razones

- Porque algunos tipos de componentes por su costo prohibitivo no son tan factibles para establecerse en disponibilidad continua, o aun en alta disponibilidad

- Porque algunos tipos de componentes por implicaciones (o inexistencia) de la tecnología no son tan factibles para la disponibilidad requerida

- Porque el desempeño global del sistema en HA a se vería tremendamente degradado si un componente específico se pone en disponibilidad alta o continua.

- Porque el diseño para soportar la disponibilidad requerida es demasiado complejo y la implementación puede acarrear riesgos adicionales de la operación

- Porque sólo se justifica disponibilidad continua para algunos componentes (como discos o arreglos de discos) y varias formas de alta disponibilidad (o aún disponibilidad básica) para otros componentes.

Las tareas para el diseño de la alta disponibilidad se orientarían entonces a

1 Identificar la tecnología a utilizar para cada una de las variaciones de disponibilidad MM, CS, WS, HS/AR, la disponibilidad básica o BA se asume que no requiere una tecnología adicional a la configuración misma del sistema.

2 Basándose en el criterio anterior, establecer cuales componentes del sistema en HA deberán estar en BA, MM, CS, WS, HS/AR (o CA)

3 Habremos de organizar los componentes en los dominios y ubicar las tecnologías que permiten soportar este dominio.

En la figura siguiente se trata de ejemplificar esto, vemos que para en el dominio de disponibilidad continua, solo puede haber componentes que estén todos bajo el rubro de disponibilidad continua. Sin embargo, para el dominio de alta disponibilidad, algunos componentes estarán en reserva en caliente, otros en reserva parcial, y algunos otros componentes proporcionarían la alta disponibilidad mediante el esquema de reserva en frío. En el dominio de disponibilidad básica, tenemos algunos componentes con enmascarado manual y otros que definitivamente no tienen forma de tener un par de reemplazo (o reserva).

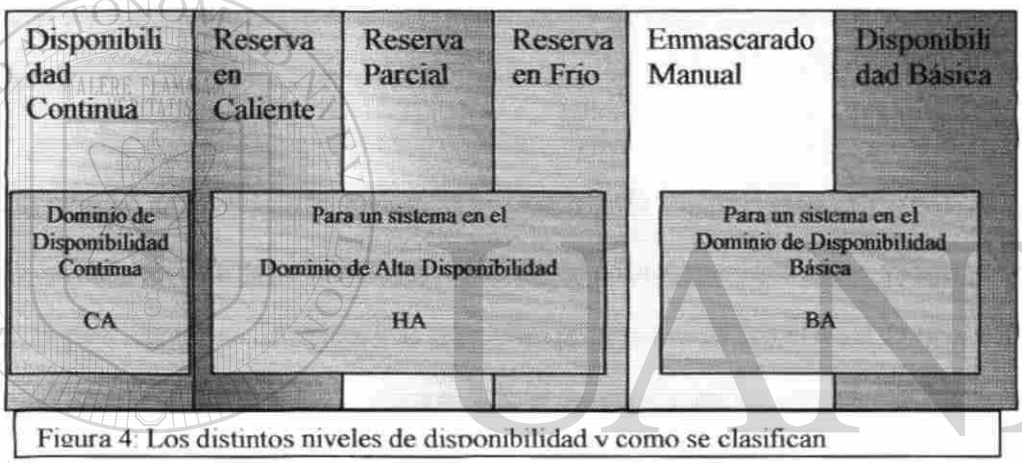


Figura 4: Los distintos niveles de disponibilidad y como se clasifican

2.1.6.7 La Replicación Activa

Anteriormente la replicación activa se manejaba como un sinónimo de la Reserva en Caliente, sin embargo, la Replicación Activa se usa también para describir el conjunto de técnicas que se utilizan para lograr implementar esta Reserva en Caliente, al compartir activamente el estado de procesamiento entre ambas réplicas Como el estado de procesamiento es un elemento dinámico en un ambiente distribuido, el compartir el estado de procesamiento entre las réplicas implica que no solo se transfiere información entre ambas, también deberán coordinar y sincronizar esta información Esto para que las réplicas puedan presentar hacia el exterior un estado estable, e internamente se procese en forma consistente

En general, los cambios de estado de procesamiento son no conmutativos, es decir, el aplicar dos cambios de estado de {A,B} a un momento de cambio S tal que: $S \rightarrow S_A \rightarrow S_{AB}$ lleva a un estado de procesamiento final distinto al obtenido si se aplican los dos cambios {B,A}: $S \rightarrow S_B \rightarrow S_{BA} <> S_{AB}$.

De aquí que el sincronizar un estado de cambio, en una réplica, significa que las operaciones deberán ser aplicadas en exactamente el mismo orden de procesamiento que se aplicaron a la copia maestra.

Así las técnicas de "Replicación Activa" están relacionadas principalmente con el ordenamiento de las operaciones para llevar una réplica de un estado de procesamiento a otro. Existen diversas técnicas para lograr este resultado, y se relacionan principalmente con el nivel de rigor con que se garantiza la replicación activa, y el impacto en el desempeño para el sistema en replicación.

Mientras más riguroso es un esquema de replicación, más degradado se verá el desempeño del sistema en alta disponibilidad.

Además de proporcionarse un vehículo para la transferencia ordenada de operaciones, los sistemas en Replicación Activa requieren mecanismos para soportar las nociones de grupos de replicas con servicios de membresía que identifiquen, en un sentido de distribución que procesos son miembros de un grupo en un momento dado del tiempo. Se requieren mecanismos adicionales que permitan a los miembros unirse a un grupo, atrapar el estado de procesamiento del mismo, y removerse ya sea en forma voluntaria o como respuesta a una falla detectada en un miembro. De aquí, los sistemas de Replicación Activa incluyen la detección de falla y

mecanismos heartbeat. Un mecanismo heartbeat es un método para estar censando un dispositivo y detectar si se pierde señal del mismo, lo que implica que ha fallado.

Los siguientes términos, son en su fondo sinónimos pero sus nombres hacen énfasis en los distintos aspectos de un mismo comportamiento:

Acrónimo	Término	Descripción
HS	Hot Standby	Acentúa la asociatividad de este modelo con otros métodos de Alta Disponibilidad que son menos exigentes. Un término mal aplicado, pues standby (reserva/sustituto) implica asimetría, siendo que este modelo especifica que debe ser replicación simétrica.
AR	Active Replication	Hace énfasis en su referencia al servidor, al indicar que la replicación que debe ocurrir requiere controlar el estado de procesamiento del servidor para lograr este objetivo. Este término es más descriptivo del mecanismo utilizado, que de la función que se espera que realice este mecanismo.
VS	Virtual Synchrony	Un término que acentúa el paradigma computacional general alcanzado cuando los grupos de procesos han garantizado el ordenamiento de mensajes entre ellos. La sincronización virtual enfatiza que el ordenamiento de procesamiento y la replicación son técnicas generales, donde la Alta Disponibilidad es sólo un (muy importante) uso de las mismas.
MFP	Make Forward Progress	Acentúa la visión de parte del cliente Se enfatiza más en la función esperada del sistema de Alta Disponibilidad, no en la forma en que se implementan los mecanismos de HA.

Tabla 4. Algunos términos sinónimos de replicación activa

2.1.6.8 La Replicación Pasiva

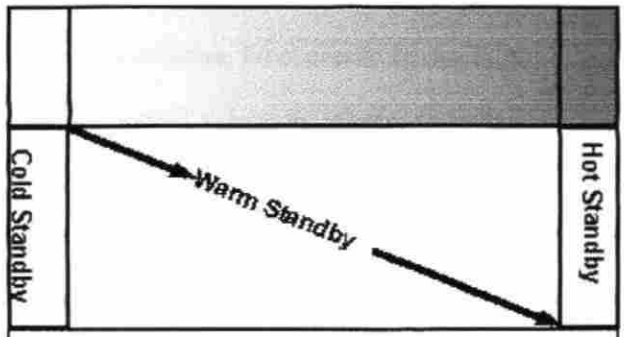


Figura 5. Espectro de Variación de modelos de alta disponibilidad, las soluciones Cold Standby y Hot Standby son puntos extremos, y en un amplio rango habrían implementaciones de tipo Warm Standby.

Describe el conjunto de técnicas usadas para lograr un modelo de Reserva Parcial (Warm Standby). Según la definición de WS, un sistema replicado con cierto nivel de inicialización y compartimiento del estado de procesamiento de la copia maestra con la réplica. En la práctica, las soluciones WS se usan como una forma relajada (menos rigurosa) de Reserva en Caliente para Alta Disponibilidad, puesto que la Replicación Activa puede ser muy costosa en términos de Performance y complejidad del diseño de la aplicación El nivel de relajamiento de los rigurosos modelos de Replicación Activa / reserva en Caliente (HS/AR), sin embargo, provoca que muchas implementaciones se definen a sí mismas como WS (Warm Standby), pero tienen una variación muy amplia entre los niveles de inicialización y estado compartido.

Algunos ejemplos válidos de Warm Standby son:

- Técnicas comunes de Replicación que se usan en algunas bases de datos, en las cuales una imagen maestra periódicamente (cada minuto/hora/noche) envía un log de transacciones a la imagen replicada, y aquí se aplican estos cambios Estas replicas pueden estar desincronizadas por el ultimo número de registros desde la última transferencia

- La imagen de procesos en memoria que se instancían (se activan) en los procesadores tanto activo como en reserva (espera) El proceso maestro administra todos los clientes que se conectan, mientras el otro procesador se mantiene a la expectativa. En el evento de una falla, todos los clientes se reconectan al proceso en reserva (espera), y deberán rehacer su trabajo desde que empezaron a trabajar en su último proceso.

- La imagen de procesos en memoria que se instancían en los procesadores activos y de espera El proceso maestro atiende los requerimientos de los clientes. Cuando el cliente indica cerrar la transacción (hacer commit), el proceso maestro envía un log (registro) de transacciones al proceso en reserva o en espera. En el evento de una falla, los clientes son desconectados y deberán reconectarse, una vez reconectados, están en un punto de sincronización igual a la última actividad realizada, y no será necesario reiniciar todo el proceso (excepto la última actividad desarrollada)

Existen muchas otras implementaciones de replicación que podemos calificar como Warm Standby. El término LR (Lazy Replication) frecuentemente se asocia al concepto "Rollback&Recover(RR)" –Deshacer y Recuperar Puesto que con ciertos mantenimientos del estado de procesamiento, los clientes se interrumpen cuando hay un evento de falla, y deberán reconectarse explícitamente a la réplica en reserva La siguiente tabla resume estos términos.

Acrónimo	Término	Descripción
WS	Warm Standby	Se centra en la parte media del espectro de HA, y el grado variable de inicialización del estado de proceso de la replica de reserva Termino que implica el compromiso entre las alternativas Hot Standby y Cold Standby
LR	Lazy Replicati on	Se centra en la vista desde el servidor, identificando la replicación que debe ocurrir en el estado de proceso del servidor para lograr el objetivo. Termino descriptivo del mecanismo de replicación, no de la función realizada por este

		mecanismo.
RR	Rollback & Recover	Se centra en la vista desde el lado del cliente. Término descriptivo del comportamiento de un cliente en un sistema en replicación parcial (Warm Standby), por ejemplo: Los efectos visibles y trastocados de una falla. Pero no define los mecanismos de implementación.

Tabla 5: Algunos sinónimos de replicación pasiva

2.1.6.9 El Balanceo de Cargas y la Alta Disponibilidad

Mecanismo usado para lograr escalabilidad, al distribuir el procesamiento y el trabajo a través de un pool de servidores De hecho, este término no tiene nada que ver con la replicación y la alta disponibilidad. En la práctica, sin embargo, estos conceptos se asocian frecuentemente a HA debido a la inversión hecha en la adquisición de sistemas redundantes para HA que no podrían justificarse si el equipo adicional se quedara inactivo, o simplemente duplicando el trabajo realizado en los servidores primarios En vez de esto, un requerimiento frecuente de los clientes es tener un pool de servidores replicados que estén preparados para sustituir a otro en el evento de una falla (rol de Alta Disponibilidad), pero que además se dividan la carga de los clientes en condiciones normales de operación (rol de Balanceo de Carga). Tal requerimiento, aunque común, puede complicar significativamente el diseño de ambos aspectos (HA y Balanceo de Cargas), puesto que la configuración computacional no puede optimizarse específicamente para un rol

En suma, deben considerarse las implicaciones funcionales de tan comprometedores diseños Si un sistema se afina para soportar una carga normal de clientes con un pool de N servidores para balanceo de cargas, y llega a sufrir la falla de un servidor, la carga debe ahora redistribuirse entre los N-1 servidores Esto claramente impactará el desempeño global del sistema, y por lo tanto no enmascarará apropiadamente la falla (pues se verá una degradación de desempeño) Por

supuesto, el sistema puede haber sido sobreprotegido con más de N servidores, lo cual permite que ocurra un número M de fallas antes de impactar al desempeño. Sin embargo, esto nos regresa al punto de partida de adquirir capacidad adicional que estará inactiva (en condiciones normales) En la mayoría de los casos, se usa N = 2, y se define el requerimiento de Balanceo de Cargas para distribuirse en ambos equipos El añadir un tercer servidor para protección no puede ser una opción.

Aquí podemos usar una analogía Consideremos una póliza de seguro de vida, con una cartera de beneficios acumulativos usables en vida. El propósito inicial de la póliza es proteger a la familia del asegurado en el evento de fallecimiento o catástrofe similar Sin embargo, la cartera de beneficios en la póliza puede usarse a discreción del asegurado, para solventar gastos normales de la vida diaria El peligro, por supuesto, es que al usar los recursos de la póliza durante la aseguranza en vida, sus beneficios pueden haberse reducido cuando realmente se requieren, al faltar el asegurado-

La Alta Disponibilidad (HA) y el diseño de software, puede pensarse como una póliza de seguros que tiene un balance de beneficios usables en vida. Por Ejemplo, la capacidad de procesamiento de los servidores redundantes. Al usar esta capacidad para balancear la carga durante operaciones normales, el beneficio de la HA se reduce al presentarse una falla.

2.1.6.10 La Disponibilidad y los Costos

2.1.6.10.1 El Costo de tener Alta Disponibilidad

La Disponibilidad Continua, y la Replicación Activa son un concepto agradable, sin embargo, el lograr aplicarlo conlleva un costo monetario, de desempeño y de complejidad que deberán

quedar claros si se desea implementar Necesitamos entender los requerimientos centrales de disponibilidad que deberá ofrecer el software del sistema, para poder entender el costo que tendrá el poder soportar el cumplimiento de estos requerimientos.

Es muy típico para una empresa que esta diseñando un sistema en alta disponibilidad, que los clientes del sistema definan sus requerimientos como 7x24, al cuestionarlos, siempre pedirán que "el sistema este operando a la hora que se requiera, es decir, debe ser 7x24", como si esto lo dijera todo, "Ningún dato se deberá perder nunca, y el sistema deberán permanecer activo y no se deberá presentar ninguna sensación perceptible de falla, los mantenimientos y actualizaciones de los sistemas no deberán interferir con el servicio y operación", esto es en verdad una gran expectativa.

Cuando no se está apropiadamente informado de los costos totales de adquisición, mantenimiento, e impuestos que implica el adquirir un Rolls Royce, es natural desear precisamente uno. Sólo que al darse cuenta que además del costo de adquisición, existe un costo adicional por el seguro, consumo de gasolina, partes de refacción, y costo del servicio calificado, entonces se tiene la suficiente información para decidir que opción elegir del rango de los modelos desde lujo hasta económico.

Igual que al evaluar productos de consumo final y automóviles, al evaluar las inversiones en sistemas complejos, es importante poder tener esta perspicacia y mente crítica que permita distinguir entre las nubes publicistas que pretenden vender productos como adecuadas soluciones para tareas que realmente no son capaces de hacer. Así también en el mercado de Alta Disponibilidad, existen una cantidad inmensa de folletos y mercadotecnia que se promocionan como "totalmente 7x24". Ni que decir, entonces, que los usuarios crean que este requerimiento es algo simple y sencillo que el sistema debe proporcionar

En suma, tanto los usuarios de sistemas computacionales, así como los desarrolladores y creadores de los mismos tienden a estar más interesados en especificar los requerimientos funcionales que debe tener: mas no que capacidades útiles realmente posee. Los temas de desempeño, escalabilidad, confiabilidad, etc. tienden a ser decididas en forma menos enfocada. Cuando muchas veces son estos requerimientos no asociados a la funcionalidad tan importantes como la utilidad global del sistema, pero si implican una complejidad igual o mayor que los requerimientos funcionales del sistema

Finalmente, es responsabilidad de los usuarios y los desarrolladores, el trabajar en equipo para lograr identificar claramente: (1) ¿Qué es realmente lo que requieren los usuarios? Contra lo que desean, (2) ¿Qué alternativas tecnológicas podemos usar para cumplir esas expectativas?, (3) Los costos monetarios, complejidad, algoritmos de replicación, protocolos para pertenecer a un grupo, degradación del desempeño causado por la solución.

2.1.6.10.2 El Costo que implica el NO TENER una Alta Disponibilidad

La única forma de convencernos de la importancia de la Alta Disponibilidad, es demostrando los costos que implica la ocurrencia de una falla y el efecto del downtime (o corte de servicio), pero desde una perspectiva de dólares y centavos

El costo más obvio de un downtime, no es necesariamente el costo más caro o impactante de todos Uno de los costos más obvios del downtime es que el usuario pierde productividad, pero el costo real depende de que tanto trabajo esta dejando de realizar el usuario del sistema afectado, y un costo aun mayor es: ¿Está afectando esto a la imagen de mi compañía?

Si los usuarios de un sistema fallado son desarrolladores, el costo puede no ser muy impactante en una empresa usuaria, pero si es una empresa de software, este costo si será grande Si un desarrollador tiene un costo de entre $400 a $1000 el día, es muy razonable que un grupo de 50 desarrolladores inactivos causarían un elevado costo de hasta $2,000,000 en la semana Si se trabaja por proyecto y existe un entregable, además de este costo, deberemos agregar las horas extras para poder salir a tiempo, si se retrasa el proyecto, entonces deberemos agregar las penalizaciones, además de un costo intangible que es la imagen.

En sistemas operacionales, el costo por un downtime puede identificarse por el costo por hora de los usuarios inactivos de los sistemas afectados, sin embargo, habrá que agregar los pedidos perdidos, las ventas no hechas, las inversiones no efectuadas, reaprovisionamiento de inventarios no realizados, etc. Otros costos son la pérdida de imagen ante clientes potenciales (principalmente en el comercio electrónico), o los nominados costos de oportunidad Imaginemos una firma de la casa de bolsa que no pudo realizar la puesta de acciones en el momento antes de que bajaran de precio, también pudo ocurrir que haya evitado vender acciones que subían de precio (ahorrándole dinero a la firma)

Muchos costos no son cuantificables, pero tratemos de poner una ejemplo Imaginemos que queremos comprar un CD de música o un libro en un negocio de ventas vía Internet, entramos al sitio y vemos la descripción del producto, pero cuando queremos levantar el pedido, nos responde con un mensaje indicando que en este momento el sistema no está operando, intente más tarde, pero yo quiero pedir ya este producto Entonces, busco otro sitio de Internet (ya se perdió una venta, pero además ayude a mi competencia), si además en este negocio me entregan el producto rápida y eficientemente, cuando quiera comprar otra cosa ¿donde lo pediré? Definitivamente en el segundo negocio (más pérdidas) Imaginemos que un amigo me dice, oye yo quería conseguir ese disco, y los centros comerciales no le he visto, seguramente le diré, mira

en Internet busca este sitio y ahí lo encontrarás (otra pérdida más), y si comentamos que en el primer sitio no es muy confiable ¿quién ganará más ventas? Y si esto lo platicamos en una reunión de amigos, ¿Cuantos clientes se han perdido?

2.1.6.10.3 Cuando es más impactante el costo de la disponibilidad.

La diferencia de efecto entre los cortes de servicio de un sistema interno a una empresa, y los cortes de servicio en un sistema de Internet es que mientras la falla de un sistema interno de una empresa puede ser cubierto por los empleados, la falla de un sistema externo vía Internet, impacta instantáneamente a los clientes y no puede ser cubierta la sensación de falla

El corte de servicio debe observarse desde la perspectiva del usuario, e incluye la inhabilidad para acceder o comprar productos o servicios desde él site (por cualquier razón), así como la aparición de problemas de desempeño

El desempeño es un atributo de la disponibilidad, y cuando el tiempo de respuesta toma más de lo que un usuario esta dispuesto a tolerar (típicamente un valor entre 6 a 10 segundos), estos habrán de considerar que los servicios de la empresa están fuera de operación y le abandonará.

En la nueva economía de redes, el costo de corte de servicio es usualmente mucho mayor que en los ambientes comerciales físicamente localizados Las pérdidas por corte de servicio, afectan a las ganancias reales (ventas perdidas durante los períodos de falla, que no se habrán de recuperar posteriormente), las posibles ganancias de clientes actuales y prospectos de cliente, debido a la publicidad negativa, y daños irreparables a la reputación empresarial La complejidad de la mayoría de las infraestructuras de aplicaciones Web, también dificulta el asegurar la consistencia de los servicios el 100% del tiempo operacional. Más aún, los costos de obtener mayores niveles

de disponibilidad se incrementa en forma exponencial. Para poder sostener y justificar las inversiones en disponibilidad, las empresas deben calcular un retorno de la inversión que garantice que el beneficio (la reducción de los costos por cortes de servicio) excede el costo mismo de la inversión.

2.1.7 Diferencia entre Fault-Tolerance y Alta Disponibilidad

El objetivo principal de un sistema Fault-Tolerance es tener la máxima exactitud de la información procesada durante el tiempo que el sistema este operando. Un sistema Fault-Tolerance no siempre esta disponible pero un sistema Fault-Tolerance siempre deberá ser exacto (recordemos los cajeros automáticos de los bancos, que hacen cortes de servicio cada cierto tiempo, pero no deben fallar al momento de realizar una transacción)

Un sistema en Alta Disponibilidad estará casi siempre en servicio, pero no siempre se requiere un procesamiento con nivel extremo de exactitud: por ejemplo, un Proveedor de Servicios de Internet siempre debe estar operando, aun cuando en ocasiones las imágenes que presenta el site se vean indefinidas o borrosas Otro caso es el de las consultas telefónicas de saldos, usualmente este tipo de servicio debe ser 7x24 aun cuando la información no siempre es exacta, pues el saldo será proporcionado a una fecha de corte (sin incluir los últimos movimientos de la cuenta).

La definición de un sistema Fault-Tolerance consiste de equipo y sistemas con tecnología propietaria de alto costo, y sistemas duplicados fuertemente acoplados. El manejo de fallas se integran y se convierten en parte de las funciones del sistema operativo. Estos sistemas tienen una respuesta automática y espontánea a las fallas de sistema y proporciona servicios continuos ininterrumpidamente

2.2 Esquemas de Alta Disponibilidad

Para todo negocio (principalmente si es de comercio electrónico) es impactante el nivel de competitividad que le da el tener un sistema siempre disponible, el cual permite atender los pedidos, y llamadas de clientes potenciales que al recibir un servicio eficiente (y a cualquier hora) se pueden convertir en clientes leales.

Definitivamente la alta disponibilidad tiene un costo, pero siempre será un costo que se estará dispuesto a pagar si logramos este nivel de servicio y si logramos garantizar la respuesta y funcionalidad del sistema aún en los momentos más críticos de operación (las horas pico)

El impacto más fuerte que puede tener una empresa al no usar esquemas de alta disponibilidad es bajo el rubro de imagen, ya que se pone en entredicho la credibilidad de una empresa que no puede garantizar el nivel servicio de los sistemas de primer contacto con el cliente.

2.2.1 Clustering

El concepto de cluster es tomar dos o más computadoras independientes(recién desempacadas), y organizarlas para trabajar en conjunto para proporcionar la más alta disponibilidad y escalabilidad que puede obtenerse al usar un solo sistema Cuando una falla ocurre en un cluster, los recursos pueden ser movidos a otro sistema en el cluster y la *recuperación* del trabajo perdido es posible mediante procedimientos de software. Al contrario, un sistema tolerante a fallas usa un hardware especial para correr múltiples computadoras en un modo *"paso a paso"* tal que se proporcione un servicio de computo que no se detenga al ocurrir una falla de algún componente. Los sistemas tolerantes a fallas son mucho más caros debido a el hardware de propósito especial que necesitan.

2.2.1.1 Beneficios de los clusters.

La arquitectura de cluster puede proporcionar tres principales beneficios hacia el usuario:

- **Mejora la Disponibilidad:** Al proporcionar un servicio continuo aún durante una falla de hardware o software. Cuando el servidor falla, la carga de trabajo es reasignada a los servidores restantes, la sensación es de un corto período sin servicio, tan corto que la expectativa es que no sea perceptible, excepto por aquellas transacciones que estaban en proceso justo en ese momento. El proceso de failover depende de la aplicación en uso.
- **Mejora la Escalabilidad:** Al permitir que se agreguen nuevos componentes conforme la carga del sistema se incrementa. Cuando la carga global excede las capacidades de los equipos en el cluster, se pueden agregar nuevos módulos (para esto el sistema del cluster debe ser capaz de redistribuirse en varios equipos a la vez). Se puede incrementar el poder de procesamiento al agregar más CPU's (un equipo a la vez). Adicionalmente, se puede incrementar aún más la capacidad de procesamiento al aumentar el número de servidores en el cluster
- **Una Administración Simplificada:** En los grupos de sistemas y sus aplicaciones, al permitir que los administradores gestionen los grupos completos de servidores y procesos como un solo sistema.

2.2.1.2 Limítrofes de la tecnología de clusters.

Los clusters pueden proteger contra fallas en el almacenamiento, fallas de hardware, fallas en un segmento de la red (enrutando los servicios por una red alterna), pero se requiere que el software de aplicaciones sea funcionalmente capaz de recuperarse de un evento de falla en un cluster

- **La tecnología de cluster** no puede proteger contra fallas inducidas por corrupción de software, o por fallas causadas por negligencia o descuido de la intervención humana. Si el sistema operativo del servidor se cae de tal forma que corrompe las definiciones de cluster, la recuperación de la información procesada por este miembro puede no ser recuperable por otros elementos del cluster.
- **La presencia de un virus** o una falla del software de aplicación causa que la estructura lógica de datos de la aplicación se corrompa, probablemente no será posible recuperar la aplicación mediante la operación normal del cluster, requerirá procedimientos avanzados de recuperación.
- **El borrar un archivo** con información importante en forma accidental del sistema, cuando el usuario esta operando, definitivamente no será recuperable (mediante principios del cluster), si es un archivo de cierto tiempo de vida, probablemente se tenga algún respaldo, pero requiere intervención manual Si el archivo se generó en el momento o como parte de la operación normal, entonces no existe respaldo y se puede considerar una perdida total

2.2.2 Sites Espejo

Este concepto es un nivel más avanzado de alta disponibilidad y esta enfocado a la recuperación de desastres La recuperación de desastres es el nivel máximo de alta disponibilidad, y se enfoca a tener un site remoto que es (o debe ser) un espejo de los sistemas y equipos de mayor importancia ubicados en el site principal, en caso de que este site principal llegará a sufrir una falla mayor: Un incendio, una bomba, terremoto, inundación, o caída de un edificio. El site remoto estará en posibilidad de retomar el control de las operaciones y lograr que el negocio continúe en la operación Un estudio efectuado por la Universidad de Texas acerca de las compañías que han sufrido una pérdida catastrófica de información, el 43% nunca volvió a operar, el 51% cerró en el transcurso de 2 años a partir de la fecha del desastre, y sólo 6 sobrevivieron Los sites espejo y los

planes para ponerlo en operación en caso de desastre, es decir, los Planes de Recuperación de Desastre son imperativos ya que una empresa no logrará recuperarse en caso de que no tenga establecido el suyo al momento de ocurrir un desastre mayor.

Adicionalmente, deberá existir una metodología para el traslado de cintas con los respaldos de la información desde un edificio a otro, tal que se tenga una fuente parcial de información en caso que el site remoto no logre operar adecuadamente

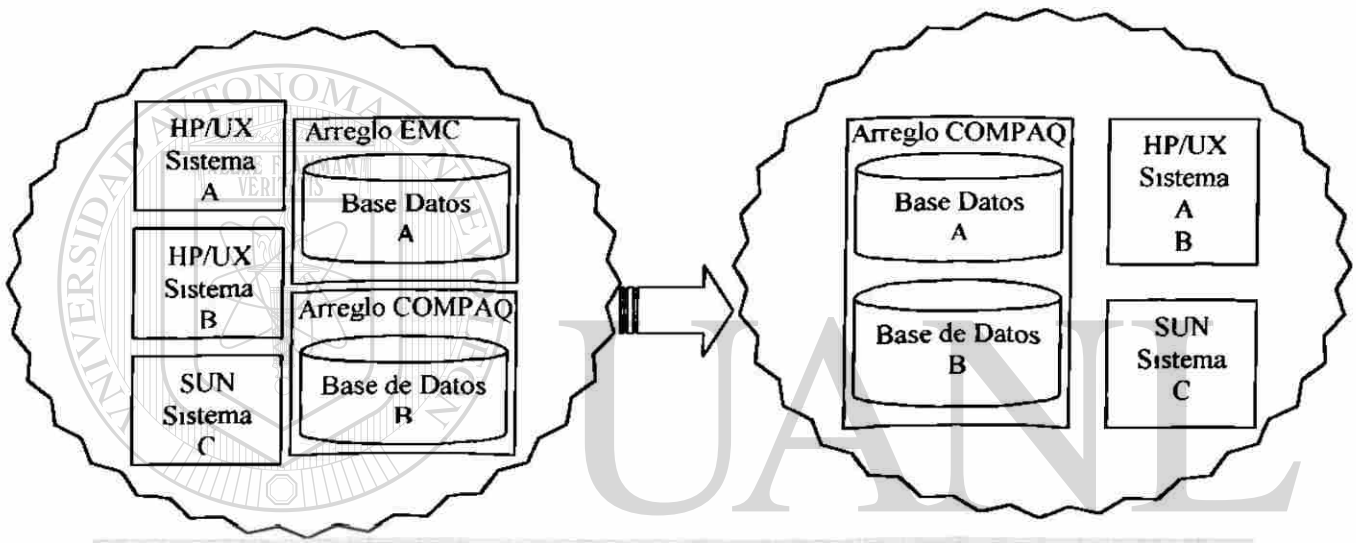
Existen diversas formas de lograr mantener la configuración de un site espejo, una es realizando una copia de cada una de las bases de datos del site principal, y posteriormente aplicando las operaciones en forma incremental. Otra forma es mediante hardware especial que proporciona replicación byte a byte de cada uno de los discos hacia un juego de discos remoto, en caso de falla, la copia de información de los discos estará actualizada hasta un momento muy cercano a la falla, con lo cual se podrá retomar la operación en el site remoto.

Un site remoto, no necesariamente debe ser una réplica exacta del site primario, pero si debe tener una copia de la información organizada de tal forma que la operación pueda ser retomada, aún cuando los equipos que se utilicen para tal efecto, no sean necesariamente de la misma capacidad que el site primario

El modelo de Recuperación de Desastres debe tener un plan de implementación, así como un plan para aplicarlo en caso de presentarse la necesidad, es un plan muy complejo, que debe contemplar desde las instalaciones eléctricas duplicadas, redes de comunicación duplicadas, arreglos de discos en replicación, equipos de computo adicionales, racks para soportar estos equipos, aire acondicionado alterno, sistema contra incendios, fuentes de energía, y si esto no fuera poco, esto

mismo deberá existir para el site remoto, con costos que deben calcularse adecuadamente y justificarse para poder lograr su aplicación.

En general, el esquema de recuperación de desastres y el manejo de Sites Espejo es un tema demasiado amplio por si mismo suficiente para dedicar una investigación propia al mismo. Por esta razón no se contempla profundizar más sobre este tema en este proyecto, sino mencionar que



Site Principal **Site Remoto**

El site remoto, no necesariamente es una copia fiel del site principal, sin embargo debe estar preparado para potestad recibir la carga y soportar la operación (tal vez un poco más lenta) pero que permita continuar las actividades del negocio.

Figura 6. Ejemplificación de un esquema de recuperación de desastres

existe y es el esquema de mayor protección que puede aplicar una empresa. Adicionalmente, ya existen algunas alternativas de solución a esta necesidad, y muchos proveedores ya son capaces de soportar esquemas de automatización para lograr eficientes implementaciones de los mismos

Capitulo

3 PROPUESTA DE ANALISIS Y EVALUACIÓN

3.1 Productos Comerciales para Alta Disponibilidad

3.1.1 HP MC/Service Guard

Es la tecnología primaria ofrecida por HP para esquemas de Alta Disponibilidad en plataformas medianas, solo soportado en HPUX Permite al software de aplicación organizarse en paquetes que se instalan en servidores HP en Cluster , típicamente en pares A un paquete se le asignan recursos de disco (Logical Volumes de HP), y recursos de red (una dirección IP). Estos recursos permanecen asignados al paquete, aun cuando ocurre una falla El ServiceGuard realiza una validación de heartbeat entre los equipos que forman el cluster, y si se detecta una falla, apaga el paquete y lo levanta en la maquina que esta operando correctamente, con la misma dirección IP que el paquete tenía en el otro equipo, y con los mismos recursos de disco que tenía previamente Logra la transparencia de red al mapear una dirección de red IP flotante, a la dirección IP fija asignada a los equipos Se logra la transparencia de los recursos de disco al conectar los discos vía múltiples puertos (F/W SCSI) a las máquinas participantes en el cluster. Un DLM (Distributed Lock Manager) garantiza que solo un servidor tendrá acceso de escritura, previniendo la corrupción de datos. Las actividades de iniciar y detener los paquetes de aplicaciones, así como cualquier actividad específica de activación y terminación que se requiera, se realiza mediante scripts en código shell que son escritos por los desarrolladores de aplicaciones

3.1.1.1 Dominio de Aplicabilidad

El HP ServiceGuard es la oferta de Alta Disponibilidad para las plataformas HP en un campo que tiene ofertas similares de competidores tales como IBM HACMP para los equipos RS/6000 de IBM, SunCluster HA para SUN. Todos estos productos son orientados hacia sistemas que desean un mecanismo sencillo de replicación en equipos Unix recién desempacados (A diferencia de los carísimos sistemas de tolerantes a fallas de Tandem o Stratus) con poco o ningún desarrollo aplicativo. HP ServiceGuard y sus competidores están diseñados para deslizarse por debajo de las aplicaciones existentes, tales como bases de datos, monitores de transacciones, servidores de aplicaciones, etc. con cero cambios al código. El único desarrollo requerido es crear los scripts en shell para gestionar las operaciones de activación y desactivación de aplicaciones.

Los clientes que intentan acceder sus servidores pueden permanecer en pleno desconocimiento de la plataforma de Alta Disponibilidad que soporta sus peticiones, y por tanto no requiere cambios al código, puesto que al ocurrir una falla estos clientes intentan resolver a la misma dirección de red, que se ha migrado al nuevo equipo que hospeda sus servicios. Esto es un comportamiento muy útil para Sistemas de software de terceros para los cuales no habrá necesidad de hacer ajustes para atarlas a un "inteligente" Sistema en Alta Disponibilidad, y los cuales se instalarán y configurarán con sus ejecutables binarios. Finalmente, al soportar definiciones arbitrarias de paquetes de operaciones, y permitiendo a estos paquetes que sean configurados sobre todos los nodos en el cluster de ServiceGuard, una forma limitada de balanceo de carga se podrá lograr

3.1.1.2 Características del MC/ServiceGuard

- Esta diseñado para proteger aplicaciones de misión crítica de una amplia gama de fallas en hardware y software

- Soporta hasta 16 equipos en cluster.

- Monitorea la actividad de cada nodo y responde rápidamente a las fallas en una forma que minimiza el tiempo de resolución de falla en procesadores, memoria, adaptadores e interfases de redes, procesos de aplicación.

- Requiere de tecnología RAID en discos para protección de la información y eliminar puntos básicos de falla.

- Requiere redes de área local múltiples para eliminar puntos básicos de falla en comunicaciones.

- Organiza los servicios soportados como paquetes y con esto permite que se muevan en forma semitransparente entre los nodos del cluster.

Beneficios	**Características**
Rápida deteccion de fallas, recuperacion automática de las aplicaciones	El MC/ServiceGuard monitorea los componentes de hardware y software, y puede detectar fallas en rangos de hasta 2 segundos (según la configuración) y responde moviendo los paquetes a otros nodos del cluster. El tiempo real de migración de los paquetes de aplicación variaran de acuerdo a los servicios de software usados por la aplicación, y el tiempo mismo de recuperación del software de aplicacion.
Elimina errores del operador de sistemas	Basándose en la configuración de secuencias de recuperacion, el proceso de detección de una falla y reactivacion es completamente automatico, no se requiere que el operador intervenga para levantar el

	sistema (eliminando posibilidades de que lo haga en un orden incorrecto)
Permite tener los servicios disponibles durante etapas de mantenimiento de software y hardware	Al permitir mover los paquetes de aplicación a otro(s) nodo(s) del cluster, se desconecta el nodo del cluster mientras se realizan labores de mantenimientos en este Una vez que el mantenimiento haya concluido simplemente se integra al cluster y se regresan los paquetes de aplicaciones al nodo nuevamente.
Arquitectura robusta de clustering	Usando evaluaciones dinámicas, el ServiceGuard puede mover y/o activar paquetes de aplicaciones entre uno o más nodos del cluster, al ser soportados por múltiples nodos puede moverse entre cada uno de ellos proporcionando un buen nivel de satisfacción.
Mezcla heterogénea de servidores HP	El ServiceGuard soporta hasta 16 servidores HP en el cluster. Estos servidores podrán ser todos uniprocesador, o todos SMP (symmetric massive processing), o una mezcla de servidores uniprocesador y servidores SMP. Esto permite utilizar equipos HP ya existentes y configurar cada nodo para recibir ciertos paquetes de aplicación empatándolos con los niveles de carga de los mismos.
Reducción de los tiempos planeados de cortes de servicio.	El MC/ServiceGuard permite reconfigurar/borrar/agregar un paquete de aplicaciones dentro del cluster mientras los otros paquetes continúan operando, permitiendo activar nuevas configuraciones con mayor rapidez.

Tabla 6.Consideraciones para el MC/ServiceGuard

Existen ciertas desventajas a la tecnología, siendo esto consecuencia de la simplicidad y conveniencia del ServiceGuard

- La falta de preservación de los estados operacionales a través de las réplicas: El ServiceGuard es un modelo puro de "Cancelar y Reiniciar", y los clientes notarán invariablemente una interrupción en el servicio El ServiceGuard ofrece un tiempo de

recuperación de aproximadamente un minuto para el paquete aplicativo, pero el tiempo total de recuperación es dependiente de la aplicación Especificamente para las aplicaciones que accedan grandes repositorios de datos, el tiempo requerido para efectuar actividades de sanidad y labores recuperativas de las bases de datos puede extenderse ampliamente (decenas de minutos). Este tiempo de recuperación se convierte en el factor decisivo en el factor MTTR del sistema total.

- El ServiceGuard es capaz de detectar y recuperarse de las fallas de hardware, de red, y de Sistema Operativo (las fallas de disco son atendidas y administradas por los dispositivos RAID o dispositivos bajo MirrorDisk) También puede proporcionar un nivel limitado de detección y recuperación de fallas de la aplicación, al actuar basándose en el código de terminación de los procesos. Pero no puede enmascarar fallas generalizadas de la aplicación, tales como bloqueo de los procesos, o comportamiento insano de proceso

- Debido a los requerimientos de discos con múltiples puertos, las maquinas en el cluster ServiceGuard deben localizarse en una muy cercana proximidad geográfica (típicamente en el mismo cuarto de sistemas) El ServiceGuard no puede resolver un cluster con una separación geográfica muy grande

- Solo se puede implementar en equipos HP El ServiceGuard se implementa con tecnología propietaria, que depende del kernel del sistema operativo HPUX , y de la arquitectura de red y hardware. No es una tecnología portable a ambientes diferentes de HP

3.1.1.3 Clasificación

Como se ha indicado, el ServiceGuard es un sistema en Alta Disponibilidad bajo el modelo de "Cancelar y Reiniciar" Coincide muy cercanamente al modelo "Cold Standby", o quizás una forma de modelos de Alta Disponibilidad Warm Standby of High Availability, puesto que hay

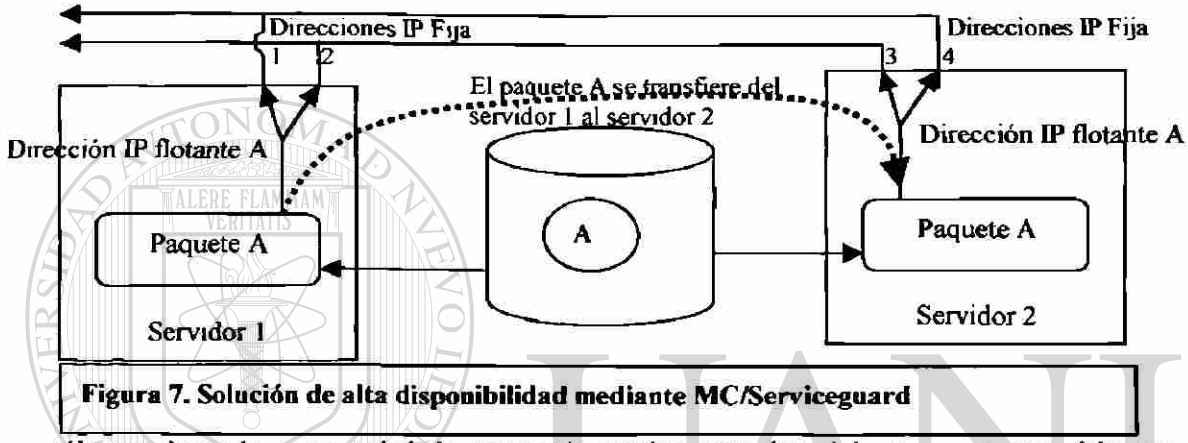


Figura 7. Solución de alta disponibilidad mediante MC/Serviceguard

sólo una limitada oportunidad de compartir estados entre las réplicas, y aun esto debe ser gestionado por la aplicación misma, a través de scripts de shell y espacios compartidos en disco, en vez que esto sea proporcionado por la plataforma tecnológica El MTTR (Tiempo de recuperación) que ofrece debido a los tiempos de recuperación de la aplicación, ubicaría a esta tecnología en la categoría de Disponibilidad Básica

3.1.2 HP ServiceGuard OPS Edition

Al igual que el MC/ServiceGuard permite organizar paquetes de aplicaciones, sin embargo este producto permite la integración del manejador de la base de datos ORACLE para soportar el Oracle Parallel Server, configuración que soporta el cluster de la base de datos levantando simultáneamente hasta 8 instancias (o copias) de la base de datos soportando la carga de trabajo en forma balanceada entre todos los servidores A diferencia del MC/ServiceGuard, bajo esta configuración se proporciona la más alta disponibilidad de los servicios, al estar levantadas

múltiples bases de datos de tal forma que si algún nodo llegará a fallar, los otros nodos del cluster recibirán la carga, y continuarán el procesamiento de base de datos del nodo fallado, por lo que sólo se verán afectados las aplicaciones que físicamente estuvieran ejecutándose sobre el nodo fallado, sin embargo, los usuarios externos a este nodo, y que estén accediéndole la base de datos serán enviados hacia los nodos y no sentirán ningún efecto en sus operaciones.

El ServiceGuard monitorea a los miembros del cluster y monitorea varios componentes dentro de cada nodo Permite habilitar una fiable coordinación y sincronización de lecturas y escrituras de datos compartidos entre los nodos del cluster. Esta versión de HP ofrece un administrador de configuraciones de red que permite recuperarse más eficientemente de las fallas en tarjetas y cables de la LAN. Además el administrador de volúmenes lógicos (Logical Volume Manager) permite la funcionalidad básica para compartir los discos y buses físicos entre los nodos del cluster

Beneficios	**Características**
Bases de Datos Altamente disponibles para aplicaciones de misión crítica.	El objetivo principal del ServiceGuard OPS Edition es asegurar que la base de datos ORACLE este siempre disponible a los usuarios finales Soporta hasta 8 nodos con 8 instancias de la misma base de datos. Si un nodo falla, las operaciones de base de datos de los usuarios son enrutados hacia otros nodos sin sentir la falla, los usuarios conectados a los otros nodos nunca sentiran la falla y continuarán laborando sin problemas, permitiendo un nivel de disponibilidad que puede llegar hasta el 99.99% en el acceso a los datos de aplicaciones críticas Sin embargo, si existen paquetes externos a la base de datos y uno de estos paquetes esta operando en el nodo fallado, este paquete deberá entrar a modo recuperacion

Rápida recuperación de fallas en la LAN	Monitorea los estados de señal de LAN que se reciben por cada uno de los nodos del cluster. El *ServiceGuard* detectará rápidamente las fallas y activaría una LAN sustituta dentro del mismo nodo. Esta detección y rápido reemplazo de una LAN alterna son completamente transparente a los usuarios de aplicaciones y base de datos. Eliminando los cortes de servicio por fallas en la LAN y refuerza la alta disponibilidad al no cortarse ni cancelarse el servicio para aplicaciones de misión crítica.
Integridad en la protección de los datos	Cuando el ServiceGuard detecta la falla de uno de los nodos, se elimina el acceso a la base de datos del nodo fallado. Esto previene al nodo bloqueado o que se ha reiniciado a sí mismo después de una falla de que intente inadvertidamente escribir datos sin control, sin esta garantía la integridad de los datos se vería comprometida. Los nodos que subsisten retoman el control, y le dan seguimiento a las operaciones del nodo fallado y efectúan actividades de recuperación del nodo fallado, todo esto sin cortar nunca el servicio de los otros nodos.
Failover automático de los paquetes de aplicación	El ServiceGuard detecta automáticamente los cortes de servicio en los nodos y paquetes de aplicaciones, entonces los transfiere y la propiedad de los paquetes y los levanta en otro nodo restableciendo los servicios computacionales rápidamente.
Reducción de costos de administración de bases de datos.	En lugar de tener múltiples bases de datos independientes en diferentes servidores, un cluster de Oracle Parallel Server reduce sustancialmente los costos de administración de las bases de datos al permitir que múltiples bases de datos se consoliden en una sola base con múltiples instancias Aún cuando existan 2 o más nodos accediendo a la base de datos al mismo tiempo, la base de datos se administra como una sola base de datos, permitiendo con esto simplificar el proceso de administración de la base de datos.
Configuración flexible que	Al poder utilizar cualquier servidor HP9000 excepto clase A se logra un

permite mezclar servidores HP9000, excepto clase A.	gran nivel de flexibilidad que permite crear cluster de costo efectivo. Sin embargo, no se podrán mezclar versiones de servidores HP en plataforma de 32 bits con versiones de 64 bits.

Tabla 7.Consideraciones para el ServiceGuard OPS Edition

Existen ciertas desventajas a la tecnología, siendo esto consecuencia de la dependencia del diseño de las aplicaciones más que de la configuración del cluster y de la base de datos en paralelo.

- La falta de preservación de los estados operacionales de las aplicaciones entre los nodos obliga a los usuarios ejecutando un programa en un nodo fallado a reiniciar sus operaciones, sin embargo, si existen usuarios conectados externamente a la base de datos dentro del nodo fallado, estos no se verán afectados y sus transacciones y conexiones serán transferidas hacia otros nodos.

- El ServiceGuard OPS Edition ofrece un tiempo de recuperación inmediato para el paquete aplicativo, pero el tiempo total de recuperación es dependiente de la aplicación (más no la base de datos que se mantiene operando sin verse afectada nunca). Este tiempo de recuperación se convierte en el factor decisivo en el factor MTTR del sistema total

- El ServiceGuard es capaz de detectar y recuperarse de las fallas de hardware, de red, y de Sistema Operativo (las fallas de disco son atendidas y administradas por los dispositivos RAID o dispositivos bajo MirrorDisk)

- Debido a los requerimientos de discos con multipuerto, las maquinas en el cluster ServiceGuard deben localizarse en una proximidad geográfica (típicamente en el mismo

cuarto de sistemas). El ServiceGuard no puede resolver un cluster con una separación geográfica muy grande.

- Solo se puede implementar en equipos HP9000, excepto HP9000 clase A. El ServiceGuard se implementa con tecnología propietaria d HP, que depende del kernel del sistema operativo HPUX , y de la arquitectura de red y hardware No es una tecnología portable a ambientes diferentes de HP.

3.1.2.1 Clasificación

Como se ve, el ServiceGuard OPS Edition es un sistema de Alta Disponibilidad con Replicación en Caliente, puede clasificarse como un modelo de Disponibilidad Continua en la parte que corresponde a los servicios de Base de Datos, pero en la parte que se refiere a los servicios de soporte a las aplicaciones, se implica el modelo de "Cancelar y Reiniciar" para un nodo fallado. El MTTR de este tipo de configuración es muy corto, sin embargo, los tiempos de recuperación de los paquetes de aplicación pueden alargarlo Se requiere que la aplicación sea ClusterAware para que pueda mejorarse el nivel de disponibilidad y garantizarse la disponibilidad continua

3.1.3 Arquitectura SunCluster 3

Tecnología que se integra con la plataforma Solaris de sistema operativo, y los equipos Sun Se enfoca en la unificación de las expectativas de alta disponibilidad, y facilidad de administración de la plataforma de entrega de servicios. Busca proporcionar un conjunto de servicios de sistema operativos orientados a la disponibilidad continua que habiliten la alta disponibilidad de todos los servicios de aplicación. El SunCluster 3 proporciona una vista de administración sencilla para todos los servicios, habilitando que el cluster se gestione como un todo

El cluster de Sun puede escalar en capacidad, al mismo tiempo que los costos incrementales por administración son más cortos. Este producto ofrece administrar los dispositivos, los filesystems y los servicios de redes a través de los nodos del cluster, y manteniendo compatibilidad total de para las aplicaciones existentes. Las operaciones de respaldo, aplicación de parches, actualización de software e instalación de nuevo hardware, podrían hacerse sin interrumpir la entrega de servicios.

El SunCluster ofrece que todos los nodos del cluster se presenten hacia el usuario final (o cliente del sistema) como un único sistema capaz de proveer servicios continuos de disponibilidad, aún cuando los nodos operan en forma independiente, ejecutando copias propias del sistema operativo, lo que proporciona un aislamiento de las fallas, de tal forma que no existe un solo punto básico de falla, que interrumpa los servicios de aplicación.

Este producto esta diseñado para ofrecer una plataforma continuamente disponible, que habilite los servicios de alta disponibilidad, o servicios de disponibilidad continua. Permite ofrecer servicios de disponibilidad escalable, o de disponibilidad mediante failover

Como sabemos existen diversos tipos de clusters:

- Clusters para escalabilidad y elasticidad a cambios, clusters acoplados libremente bajo el paradigma de balanceo de cargas, este tipo de clusters no permiten identificar los miembros y sistemas existentes dentro del cluster.
- Clusters para máximo desempeño, usados para procesamientos científicos, sin características elásticas para fallas de nodos, buscan utilizar la capacidad de procesamiento para cálculos científicos.

- Clusters para alta disponibilidad, añaden funcionalidad montándose sobre la infraestructura del sistema operativo, y mediante scripts que monitorean la operación de los módulos del sistema.

El SunCluster se identifica a si mismo como un **Cluster de propósito general,** que se enfoca en varios atributos clave para el centro de datos: Alta disponibilidad, Escalabilidad, Administrabilidad Este producto ofrece un cluster fuerte mente acoplado, donde los nodos tienen noción de su membresía al cluster, lo cual se requiere para lograr soportar la integridad de los datos Habilita a las instancias de la plataforma Solaris a ser vistas y administradas como un único ambiente operativo. Los recursos se comparten entre todos los nodos del cluster, habilitando a las aplicaciones para correr en cualquier servidor del cluster, con una visión consistente de estos recursos, aun en los momentos de falla. Las aplicaciones se pueden escalar mediante la replicación, logrando incrementar el desempeño, la capacidad productiva y elasticidad a las fallas.

El SunCluster permite que los mantenimientos al software o al hardware pueden realizarse sin interrumpir la entrega de servicios. En cuanto a la visión desde los procesos y los usuarios, se ofrece una visión administrativa que habilita a un administrador el realizar muchas tareas de mantenimiento en el cluster como si fuera un sistema computacional único. Por ejemplo, se puede agregar un disco a un nodo del cluster, y automáticamente estar disponible para el resto de los nodos Esto facilita la administración y reduce las posibilidades de un error humano Los niveles de entrega de los servicios aplicativos se maximizan al habilitar a las aplicaciones a correr en múltiples nodos concurrentemente Si un nodo se interrumpe , los otros nodos pueden continuar proporcionando el servicio esperado, evitando cualquier punto en el tiempo donde el servicio no este disponible.

De acuerdo a un reporte en cortes de servicio y grandes sistemas empresariales de uso final del Standish Group en 1999 este producto obtuvo el menor costo operacional para soportar la

ejecución de sistemas de misión crítica. Debido a su simplificada implementación. Además, como el SunCluster requiere menos personal que lo maneje, los costos operacionales son también menores. La tecnología de este producto proporciona simplicidad para administrar múltiples sistemas, reduciendo los costos operacionales asociados con el manejo de clusters.

Esta tecnología detecta en forma automática los dispositivos existentes, y habilita que los múltiples nodos los accedan y sean manejados todos como un ambiente de disponibilidad continua, administración unitaria y una plataforma completa para la instalación de las aplicaciones Habilita conceptos propios denominados Dispositivos Globales, Servicio Global de Archivos, Servicio Global de Redes que siempre estarán disponibles para los servicios que dependen de ellos.

Este producto ofrece además un servicio llamado Diskless Failover, donde los grupos de aplicaciones del nodo fallado se envían hacia otro nodo el cual, no requiere un disco o dispositivo de almacenamiento, sino que ha través de los conceptos de Dispositivos Globales, Servicio Global de Archivos, y Servicio Global de Redes, logra la abstracción de este concepto.

3.1.3.1 Características de Sun Cluster.

Depende de tecnología Sun para poder ofrecer estos niveles de disponibilidad. Requiere de dispositivo multipuertos de almacenamiento de datos.

Los nodos del cluster se comunican mediante una interconexión privada de cluster, propietaria de Sun, para lograr el envío de información de sanidad, heartbeats, información de membresía del cluster, datos aplicativos, tránsito de información del sistema de archivos, distribución y balanceo de cargas, asi como la administración de las IP's.

Hace uso de dispositivos compartidos de información, con conectividad dual de un nodo hacia el multipuertos del dispositivo, tal que si una vía de acceso a la información falla, el nodo pueda usar otra vía para este fin.

En conjunto con el Oracle Parallel Server, para los servicios de bases de datos, se logran niveles de disponibilidad continua de hasta el 99 999%, lo cual permite la sensación de tener un sistema tolerante a fallas, pero sin el costo del mismo.

Beneficios	**Características**
Mejores niveles de servicio	Los niveles de servicio se acentúan con la disponibilidad y predictibilidad de los servicios en sí. La predictibilidad incluye el nivel de desempeño, medido por la producción de los tiempos de respuesta, así como la integridad de datos, seguridad y consistencia de la interfase de usuarios
Incrementos en la Escalabilidad	Las aplicaciones que soportan las configuraciones de SunCluster permiten una alta escalabilidad al correr múltiples copias de la aplicación en diferentes equipos, de tal forma que al requerir mayor capacidad operacional basta con agregar un nuevo nodo al cluster.
Se incrementa la disponibilidad	En caso de que un nodo falle, otra instancia de la aplicación esta operando y ya tiene un acceso a los discos, de tal forma que no hay necesidad de esperar a que se reactiven los servicios, y algunas aplicaciones (como el Oracle Parallel Server) mantienen redundancia de las operaciones en proceso tal que nunca se pierde el estado operacional y se continúa operando en el mismo punto que en el

	momento de la falla.
Se mejora el desempeño	Los servicios de SunCluster proporcionan una infraestructura de comunicaciones memoria a memoria rápida y eficiente, para piezas de información que son de desempeño crítico para las aplicaciones.

Tabla 8.Consideraciones para el SunCluster

3.1.3.2 Clasificación.

Este producto ofrece servicios de disponibilidad cuasi continua, ofreciendo niveles de hasta 99.999% cuando las aplicaciones soportan la comunicación inter proceso, y niveles de paralelismo natural. El MTTR es mínimo cuando la aplicación esta preparada para inter operar con SunCluster, sin embargo, aun si la aplicación no soporta esta inter operación, este producto ofrece levantar instancias de la aplicación de tal forma que en caso de falla, solo se reinicie una pequeña sección del sistema, sin perder un gran número de operaciones. Pero si la aplicación es puramente secuencial, entonces en caso de una falla, no se podrá tener una recuperación inmediata, pues la estructura de operación de la aplicación no lo permitirá.

3.1.4 RS/6000 Cluster Technology y HACMP for AIX

EL RS/6000 Cluster Technology pretende ser una nueva tecnología de clustering y alta disponibilidad, orientado a plataformas de alta escalabilidad soportando hasta 128 nodos en cluster Este producto ofrece simplificar los esfuerzos requeridos para lograr que los programas proporcionen los mejores niveles de disponibilidad, al proporcionar la infraestructura para detectar fallas y coordinar acciones de recuperación. Busca soportar las fallas de hardware y software y lograr los niveles de recuperación para continuar la operación sin interrupción. Pretende soportar la recuperación de los subsistemas que son interdependientes. Ofrece un juego abierto de API's para fomentar su rápida explotación por los productos de software desarrollados.

Esta tecnología incluye sus tres componentes principales.

- Administrador de eventos,
- Grupos de servicios,
- Topología de servicios, un servicio interno explotado por los grupos de servicio.

Mediante un componente denominado administrador de eventos se logra un amplio monitoreo de recursos y mecanismo de detección y notificación Usando el administrador de eventos se puede establecer que ocurre en el sistema y se pueden establecer niveles de avisos a condiciones de sistema que pueden ocurrir Estos eventos pueden ser consultados por las aplicaciones ClusterAware y poder determinar las acciones a efectuar por el programa de aplicación para compensar los posibles problemas del sistema y/o explotar los recursos del sistema de alta disponibilidad Esta tecnología ofrece que se pueden configurar nuevos eventos y/o nuevos

grupos de servicios en línea sin afectar las operaciones en proceso. Mediante un conjunto de servicios de coordinación y sincronización, así como notificación de fallas de procesos o nodos.

Beneficios	**Características**
Simplifica esfuerzos para convertir los programas hacia la alta disponibilidad	Proporciona una infraestructura para detectar fallas y coordinar las acciones de recuperación. Logrando un soporte en la recuperación de fallas de software así como fallas de hardware. Soporta la recuperación de los subsistemas que son interdependientes.
Facilita la integración de aplicaciones ClusterAware	Al proporcionar un conjunto de herramientas y API's (Application Programming Interfaces) abiertas que promueva su explotación rápida por parte del software distribuido.
Soporta la escalabilidad	Permite una ejecución eficiente en configuraciones de hasta 128 nodos en cluster
Grupos de Servicios que comparten el estado de procesamiento.	Permiten a los programas que están operando en forma distribuida que se puedan comunicar y establecer sus alternativas de atención y ejecución de la estrategia de disponibilidad establecida Se mantiene un estado de procesamiento compartido para el grupo de servicios que permite establecer el nivel de mantenimiento requerido en caso de falla de uno de los elementos del grupo y la actividad de recuperación mediante un esquema de maquina de estados finitos. Se puede verificar que haya respuestas de los miembros de los grupos, permitiendo que otros miembros del grupo detecten un elemento fallado y efectuar actividades de compensación.
Detección de fallas en comunicaciones y	El componente de servicios de topologías proporciona un conjunto de servicios subyacentes que el administrador de eventos y los grupos de

determinación de vías alternas para proporcionar el servicio	servicios usan para determinar el estado de cada uno de los nodos y de las redes que los comunican. Mediante los servicios de heartbeat se monitorean los nodos y adaptadores de red contra posibles fallas. En caso de detectarse una falla se verifican múltiples vías alternas hacia el mismo nodo para determinar si el nodo esta fuera, si es un servicio de red, o si es el adaptador de red el fallido.
Facilidad de administración de los servicios y subsistemas del cluster	Mediante el uso de Monitores de recursos que recolectan información acerca del estado del sistema. Se ofrecen herramientas administrativas para detectar cambios en los estados de procesamiento y para responder apropiadamente a los mismos. Mediante la herramienta gráfica SP Perspectives se ofrece una interfase gráfica para el monitoreo de los cambios de estado del sistema. Sin efectuar cambios, puedes encontrar y solucionar rápidamente fallas de software.
Herramientas de monitoreo de fallas físicas en forma eficaz	El estado del hardware en sistemas de procesamiento simétrico puede ser detectado hasta niveles de variaciones de voltaje, advertencias de temperatura, o fallas en las fuentes de poder. Se vigila la sanidad de los nodos y adaptadores usados en el sistema. Se detectan cambios y/o fallas en los subsistemas de discos virtuales compartidos, y la situación operacional del producto de balanceo de cargas (LoadLeveler). Se controlan los recursos de los nodos bajo el sistema operativo AIX (RS/600 Unix) tales como CPU's, discos, volumegroups, filesystems, Adaptadores de red de area local, espacio de paginación, y colas de procesos. Se puede monitorear la sanidad hasta el nivel de procesos para determinar si un programa determinado esta operando.
Discos virtuales que	Mediante el producto IBM Virtual Shared Disk se ofrece esta

permiten acceder un mismo arreglo de datos desde nodos distintos, como si fuera local	funcionalidad, además de que se puede también seccionar la información a escribir y distribuirla en múltiples discos para que los accesos sean más eficientes, reducción cuellos de botella en el I/O, o picos de procesamiento.
Recuperación de discos en forma automática por fallas en nodo	El software IBM Recoverable Virtual Shared Disk (RVSD) ofrece una alta disponibilidad al recuperar la configuración e información de un VSD en un nodo secundario, con cero intervención humana. Este software toma ventaja de la información de los grupos de servicio, así como de las funciones de coordinación de los sistemas interdependientes de los grupos de servicios para coordinar las acciones a realizar para la recuperación.
Control más natural del cluster	Al ofrecer APIS que permiten a las aplicaciones obtener información acerca del estados del cluster y de otros miembros del mismo

Tabla 9: Características del RS/6000 Cluster Technology

El HACMP for AIX ó High Availability Cluster for Multiprocessing ofrece un método que permita reasignar los recursos que un equipo este usando y que presente una falla, moviéndolos hacia otro nodo predeterminado basándose en un juego de reglas. Esta herramienta detecta automáticamente fallas en el sistema y recupera los datos de los usuarios, y aplicaciones hacia un sistema de respaldo. Pretende ofrecer un ambiente de alta disponibilidad de aplicaciones a un bajo costo, y en caso de presentarse una falla, el HACMP para AIX proporciona una recuperación rápida y transparente. Ofrece una instalación, configuración y personalización fácil y rápida sobre una plataforma AIX. Ofrece flexibilidades al permitir al cliente configurar el nivel de desempeño deseado, mediante distintos equipos y capacidades de los mismos Los clientes pueden mezclar y empatar los adaptadores de red y subsistemas de discos que satisfagan las necesidades de desempeño, y almacenamiento esperadas El HACMP ofrece ventajas para recuperación en un

corto período de tiempo, si los dispositivos de almacenamiento pueden estar conectados a dos o más servidores al mismo tiempo, el HACMP puede reaccionar a fallas de un nodo al reasignar los dispositivos a otro servidor y reactivar la aplicación en otro sistema que sea apto para tomar el control de los mismos.

Beneficios	**Características**
Clusters a bajo costo	Ofrece que un servidor de alta capacidad 7 procesadores pueden ser respaldados en capacidad operacional por un procesador inactivo en espera , permitiendo continuar la operación cuando un procesador falle. Permite un método de recuperación a bajo costo que algunos clusters convencionales al permitir que los clientes enfoquen sus inversiones hacia componentes de hardware y software que son críticos para cumplir los requerimientos del negocio, y permitiendo que un servidor de menor capacidad pueda retomar el control para continuar el procesamiento en el caso extremo de una falla.
Procesadores rotantes de sustitución	Un servidor de hasta 8 procesadores un procesador sustituye a otro en un orden predeterminado de secuencia de contención.
Respaldo mutuo entre procesadores	Cada procesador sirve de respaldo a otro en un esquema de hasta 8 procesadores, al compartir entre ellos la carga de trabajo entre los mismos.
Acceso concurrente entre procesadores	Mediante una configuración adicional se permite que hasta 8 procesadores trabajen compartiendo la carga de trabajo y compartiéndose información entre los mismos y acceso a los datos que son operados por cada procesador

Tabla 10: Características del HACMP for AIX

Mediante el producto de IBM RS/600 Cluster Technology, el Cluster for Scalable Parallel Systems esta orientado a sistemas de procesamiento en paralelo que puedan escalarse fácilmente, es decir se configura un juego de nodos y conforme se requiera mayor capacidad de procesamiento se van agregando nodos, haciendo uso del HACMP (High Availability Cluster for Multiprocessing) en plataformas de misión crítica se lograr eliminar los puntos básico de falla entre los nodos del cluster.

3.1.4.1 HACMP/ES

Existe una versión denominada HACMP/ES (High Availability Cluster for Multiprocessing/Enhanced Scalability) la cual ofrece las caracteristicas del HACMP en combinación con las caracteristicas del RS/6000 Cluster Technology Tanto el HACMP como el RS/6000 Cluster technology son ambos productos de tecnología de clusters, cada uno se enfoca en diferentes pero importantes aspectos de manejo de clusters El HACMP se enfoca en mantener a las aplicaciones funcionando dentro del cluster a pesar de las fallas de hardware o software de los componentes del cluster, Sin embargo, no es fácilmente adecuable por parte del cliente para atacar nuevas clases de problemas que pudieran ser quizás menos catastróficas, pero que si implican interrupción a la operación de la aplicación El RS/6000 Cluster Technology permiten a las aplicaciones detectar y generar eventos, y coordinar las reacciones a estos eventos, sin embargo, este producto no proporciona respuestas reales a estos eventos

Por separado, estos dos productos atacan importante problemáticas de manejo de clusters, pero no explotan las capacidades especiales de la contraparte El HACMP/ES ofrece el acoplamiento del HACMP y del RS/6000 Cluster Technology, este producto acopla la robusta y amplia serie de reacciones predeterminadas a las fallas de software o hardware de los componentes del cluster,

con la interfase para la notificación de cualquier evento del cluster que ofrece el RS/6000 Cluster Technology. Este nuevo producto ofrece la funcionalidad típica del HACMP de hasta 32 nodos en cluster, en conjunto con la posibilidad de que los clientes puedan definir respuestas a nuevos eventos o a cualquier evento que pueda ser detectado a través de los grupos de servicios o administradores de eventos

3.1.4.2 Clasificación

Este producto puede ofrecer niveles de disponibilidad desde 95% hasta 99.9999% según el producto elegido para su implementación, así como el nivel de clusterización de la aplicación. Es decir, si la aplicación es ClusterAware, el nivel de disponibilidad se dispara al 99.9999% es decir Disponibilidad Continua

3.1.5 Microsoft Cluster Service Architecture and Microsoft Network load Balancing

El Cluster Service Architecture proporciona suporte de failover para aplicaciones centrales y servicios backend que requieren de alta disponibilidad e integridad de datos. Las aplicaciones backend son las que soportan las operaciones reales de las peticiones echas en una GUI por el usuario (las cuales son enviadas al proceso backend para su resolución). Entre las aplicaciones backend podemos mencionar los manejadores de bases de datos, los servidores de archivos, las aplicaciones ERP o Enterprise Resource Planning (como lo es SAP), y los sistemas de mensajería electrónica.

Este producto fue originalmente diseñado para Windows NT, pero ha avanzado y se ha mejorado para Windows 2000. Este producto habilita la interconexión de múltiples servidores hacia un servicio de Cluster que pretende proporcionar una alta disponibilidad y un fácil manejo de Programas de Aplicación y Datos que son procesados dentro del cluster.

El Cluster Service ofrece tres configuraciones de Tecnología de cluster

- **Disponibilidad Mejorada** al habilitar que los servicios y aplicaciones en el cluster puedan continuar proporcionando los servicios aún en caso de una falla de un componente de software o hardware o durante un mantenimiento planeado
- **Escalabilidad Ampliada** al soportar que los servidores puedan ser expandidos con más procesadores (hasta un máximo de 8 procesadores por servidor con Windows 2000 Advanced Server y hasta 32 procesadores en Windows 2000 DataCenter Server), y con

memoria adicional (hasta 8 gigabytes en Windows2000 Advanced Server y hasta 64Gb en Windows2000 DataServer)

- **Maniobrabilidad Mejorada** Al habilitar que los administradores manejen los dispositivos y recursos dentro del cluster completo como si fuera un sólo equipo o computadora.

El ClusterService es una de las 2 tecnologías que se complementan para lograr Clusters bajo Windows y que se proporcionan como una extensión del sistema operativo base de Windows 2000 y Windows NT.

Existe otra tecnología de Cluster para Windows. Microsoft Network Load Balancing, el cual es un complemento del Cluster Service Architecture al soportar un Cluster altamente disponible y escalable para aplicaciones y servicios de Front-End tales como Sites de Internet e intranet, Aplicaciones Web, y Servicios de Microsoft Terminal (terminales virtuales).

Cuando el Microsoft ClusterService hace referencia a los servidores que conforman un cluster, estos reciben el nombre de *nodo*, los conjuntos de componentes en cada nodo que realizan tareas específicas de operación del cluster se llaman *Servicios de Cluster*, y los componentes de software o hardware dentro del cluster que son administrados por los Servicios del Cluster son llamados *Recursos* El mecanismo usado por Microsoft Cluster Service para administrar los recursos del cluster, son las bibliotecas de recursos dinámicamente vinculadas (DLL de Recursos) Las DLLs de recursos definen las interfases de comunicación, las operaciones de administración a llevar, y una abstracción de recursos

El Microsoft ClusterService identifica a un recurso *online* cuando esta disponible y proporcionando servicios en el cluster Estos recursos son entidades lógicas o fisicas que tienen las siguientes características:

- Pueden ponerse en línea o fuera de línea en algún momento
- Pueden ser administrados por un cluster.
- Pueden pertenecer a un solo nodo en un momento del tiempo.

Algunos recursos de cluster son dispositivos físicos (como· Discos, Tarjetas de red) o elementos logicos (como. direcciones de Internet Protocol (IP), programas de aplicación, e instancias de bases de datos Cada nodo en el cluster tendrá sus propios recursos locales Sin embargo, en un cluster también existen recursos compartidos, como los arreglos de almacenamiento de datos, o red privadas del cluster (para el heartbeat). Éstos recursos compartidos son accesibles a cada nodo en el cluster. Adicionalmente se usa un recurso compartido especial llamado Recurso de quórum, un disco físico en el arreglo de discos compartidos que juega un role crítico en las operaciones del cluster Siempre debe existir para que cualquier operación de manejo de nodos ocurra (tales como formar un cluster, o unirse a un cluster).

Beneficios	**Características**
Fácil administración de discos y aplicaciones	Utiliza el modelo de cluster Shared-Nothing, que implica que cada nodo administra sus propios discos y recursos locales, en el caso de recursos compartidos como un arreglo de discos, el dispositivo se puede montar en sólo un nodo a la vez.
Cluster de bajo costo	No requiere de un cableado o aplicaciones especiales para entrar a operar en cluster
Conectividad estándar	Al conectar los dispositivos locales de almacenamiento y comunicación, el ClusterService utiliza los drivers estandar incluidos

	en Windows NT y Windows 2000, y los dispositivos externos compartidos requieren una interfase SCSI que puede ser PCI, o fibra óptica.
Manejo de servidores virtuales	Uno de los beneficios principales del Cluster Service es que las aplicaciones y servicios corriendo en un Servidor del Cluster, pueden exponerse hacia los usuarios y terminales de trabajo como Servidores virtuales. Los usuarios y clientes que se conectan a una aplicación o servicio corriendo como servidor virtual, aparenta ser el mismo proceso que si te conectas a un servidor físico único. De hecho, la conexión a un servidor virtual puede estar hospedada en cualquier nodo del cluster El usuario o cliente de la aplicación no sabrá cuál nodo está hospedando realmente el Servidor Virtual. Múltiples servidores virtuales pueden ser manejados en un solo cluster. No se requiere un Servidor Virtual para los servicios que corren directamente en el cluster y que no son accedidos en forma directa por un usuario o cliente del cluster
Rápido movimiento de un servidor virtual a otro nodo del cluster.	En caso de una falla de un servidor virtual por la caída de un nodo o dispositivo local al nodo huésped, este se mueve a otro nodo del cluster y se reactiva todo el servicio, el usuario o cliente reinicia la conexión al mismo servidor virtual (el no sabe que se cambio a otro nodo). Sin embargo la actividad actual se pierde (excepto si la aplicación sea fault tolerant).
Configuración Mínima	El Microsoft Cluster Service es una herramienta separada como tal, pero se integra al sistema operativo Windows NT o Windows 2000 con una configuración mínima requerida:

	• Soporte para la creación y borrado de nombres de red y direcciones • Modificación al sistema de archivos para habilitar el cerrado de archivos al desmontar discos. • Cambios al Subsistema de I/O para el intercambio de discos y volúmenes físicos entre nodos

Tabla 11: características del Microsoft Cluster Service

El producto **Microsoft Network Load Balance** ofrece un nivel de disponibilidad y escalabilidad de los servidores de servicios de Internet, tales como los usados en WebServers, FtpServers, virtual terminal servers, mail servers y otros servidores de misión crítica en Internet. Un servidor por si sólo no puede garantizar la confiabilidad y escalabilidad en el desempeño, sin embargo al combinar los recursos de dos o más computadoras en un cluster de servicios, este producto ofrece la confiabilidad y desempeño de los Web Servers. Con este producto, cada servidor corre una copia de los programas de servicios deseados y este producto se encarga de que los niveles de carga se distribuyan entre cada uno de los servidores. Algunos servicios como el de e-mail solo es atendido por uno de los servidores, en estos casos el producto enruta el tráfico hacia el servidor específico de e-mail, y desvía el tráfico hacia otro servidor solo cuando ocurre una falla

Los clusters de balanceo de carga de red unifican varias computadoras corriendo programas de servicio que usan el protocolo de red TCP/IP. El Microsoft Network Load Balance permite que todos las computadoras en el cluster se direccionen por el mismo cluster de direcciones IP (manteniendo su direccionabilidad usando direcciones IP únicas dedicadas). Este producto distribuye las peticiones entrantes de los clientes (en forma de trafico de red bajo protocolo TCP/IP) entre los servidores. Para lograr escalabilidad de servidores, el producto balancea el tráfico entrante hacia todos los servidores del cluster donde existe una copia de la aplicación

corriendo. Se puede lograr una escalabilidad agregando más servidores al cluster para una carga mayor de procesamiento El nivel de carga que cada servidor puede manejar se puede configurar según se requiera. Además, el software puede direccionar todo el tráfico hacia un sólo servidor preestablecido, llamado el servidor soporte de mandatos no atendidos, cuando se logra el nivel deseado de carga sea continua distribuyendo las nuevas peticiones.

El Network Load Balance administra el tráfico de TCP/IP logrando alta disponibilidad de programas de servicios, cuando un servidor falla, el Network Load Balance automáticamente reconfigura al cluster para direccionar las peticiones de los clientes hacia las computadoras restantes Una vez que se recupera el servidor fallado, este nodo se realinea al cluster y recibe su carga de trabajo.

Este producto complementa la Microsoft Cluster Service y en conjunto prometen lograr niveles de disponibilidad de hasta el 95% con aplicaciones típicas y hasta 99 99% con aplicaciones que son ClusterAware.

3.1.6 Legato Fulltime Cluster

Este producto a diferencia de los productos mencionados anteriormente, es principalmente un software de cluster de Failover, es decir, implemente el modelo de cluster Shared-Nothing, donde los recursos los tiene asignados un nodo a la vez, y en caso de falla de un Grupo de procesos (llamados ResourceGroup) este es migrado hacia otro nodo siguiendo un procedimiento de detención, migración de nodo y reactivación

En este producto se forman grupos de recursos los cuales involucran: Direcciones IP, Discos Fisicos, y Software de Aplicación Se define una serie de reglas en las cuales se establece la

secuencia en que pueden activarse los grupos de recursos en una lista de nodos, al fallar el grupo en un nodo, este grupo de recursos será migrado hacia otro nodo de la lista (discos, direcciones IP y procesos) Sin embargo, esto siempre conlleva un corte de servicio que puede prolongarse según el proceso de recuperación que requiera el Software de Aplicación que pertenece al ResourceGroup.

Este producto cuenta con implementación en diversas plataformas y sistemas operativos:

- Legato Cluster para HP-UX en HP9000 de HP
- Legato Cluster para Solaris en SunSparc de Sun
- Legato Cluster para Windows-NT o W2000 de Microsoft para equipos INTEL
- Legato Cluster para AIX en RS/6000 de IBM, Linux, }

Este tipo de productos es muy útil en negocios pequeños a medianos, en los cuales se desea contar con un mejor nivel de disponibilidad, tal que al fallar el servidor, al menos se pueda levantar el sistema en el menor tiempo posible en un equipo adicional que ya está instalado En negocios medianos a grandes pudiera ser también útil para sistemas de mediana importancia, y cuyo costo no justifique la adquisición de un producto de mayor nivel de protección. También es muy importante para aquellas empresas cuyos sistemas estén implementados en múltiples plataformas y sistemas operativos, donde el implementar una solución de alta disponibilidad implicaría instalar un software distinto en cada plataforma, y contar con un administrador especializado para cada cluster tecnología de cluster utilizado Al implementar soluciones de alta disponibilidad con este producto, podrá contarse con un único administrador especializado en Legato Cluster (sin importar la plataforma), reduciendo costos de personal, y de soporte.

El hecho de que este producto ofrezca un servicio de configuración de Cluster de Failover, permite ofrecer un cierto nivel de disponibilidad, pero este depende grandemente del nivel de

seguridad ofrecido por el software que esta corriendo con esta solución, pues cada vez que se presenta una falla física, el software de aplicación deberá realizar una labor de housekeeping y recuperación Sin embargo, como el Legato Cluster no esta integrado al sistema operativo, por lo mismo no puede garantizar que toda la información pudiera haberse escrito a disco lo cual pudiera ser causa de corrupción de información.

Es un producto ampliamente utilizado, pues requiere menor especialización en cada plataforma de cada sistema operativo. Un sólo experto me puede apoyar a implementar clusters en NT, HPUX, AIX y Solaris. Sin embargo el nivel de disponibilidad también es menor que un producto especializado a la plataforma específica.

Este producto complementa las plataformas de los diversos sistemas operativos con interfases estandarizadas y fáciles de manejar, aún cuando estos servicios no son nativos de la plataforma, debido a las APIS que tiene, se pueden lograr niveles de disponibilidad de hasta el 95% con aplicaciones típicas y hasta 99.99% con aplicaciones que puedan prepararse para interactuar con el producto

3.2 Que esperar de un proyecto de alta disponibilidad

Al momento de iniciar un proyecto de alta disponibilidad, es conveniente evaluar la posibilidad de que un proveedor externo experimentado en este tipo de proyectos pueda liderear el desarrollo del mismo, debido a que este tipo de proveedores ya tienen un know-how sobre estas soluciones, así como pueden ser partners integradores de proveedores, lo cual puede significar calidad en la entrega de la solución total Podremos exigir que este proveedor realice las tareas de investigación de compatibilidad, análisis de requerimientos de infraestructura, drivers de sistema operativo, así como planeación de las pruebas de funcionalidad Pero deberemos tener claro que esto podrá elevar el costo del proyecto mismo.

Si el proyecto lo dirige un proveedor externo, o un colaborador interno, es importante identificar que esperamos nos resuelva el mismo.

Debemos establecer y clarificar en la empresa cual es el significado de la alta disponibilidad, y dejar muy claro cuales son las expectativas de alta disponibilidad por parte de los clientes de los sistemas.

Como se menciona al principio de este documento, un usuario del departamento de sistemas puede creer que si SU sistema falla la operación total de la empresa se ve afectada de forma inmediata. Debemos identificar la realidad de este efecto, y establecer niveles de medición

Deberá generarse un documento mencionando las dependencias internas y los tiempos de entrega por parte de proveedores externos. Además, habrá necesidad de tener un registro de los tiempos actuales de retraso en solución de fallas, y evaluar el impacto real en la operación

Se habrá identificar cuales son los sistemas primordiales, y cuales son las expectativas de los esquemas de alta disponibilidad. Así como el efecto competitivo que puede significar el poder ofrecer un servicio continuo mediante sus sistemas de información.

Se deberá documentar el inventario total de sistemas de la empresa, así como calificarlos en nivel de prioridad y si es o no crítico para la empresa.

¿Se detiene la operación por falla del sistema, o se retrasa la toma de decisiones?

En esta empresa, ¿Qué efectos puede tener que tales sistemas dejen de operar por alguna falla determinada?

¿Cuánto tiempo estaría dispuesto a soportar sin que estos sistemas estén operando?

¿Ha considerado las pérdidas económicas que significa el tener estos sistemas sin operar?

¿Cuál es la plataforma operativa de sus sistemas computacionales? Esto es importante, pues dependiendo de las plataformas operativas es el tipo de solución comercial disponible para lograr la alta disponibilidad

¿Ha considerado la posibilidad de iniciar comercio electrónico?

¿Ha evaluado el impacto que puede tener en un comercio electrónico el hecho de que los servicios solicitados estén inhabilitados por mantenimiento o por falla?

3.3 La competitividad de las empresas con esquemas de Alta Disponibilidad

Al momento de mover los sistemas tradicionales hacia un esquema de alta disponibilidad, el nivel de competitividad se incrementa, al garantizar que el cliente de la empresa podrá recibir los productos y servicios sin retraso y en la calidad establecida

3.4 Análisis costo beneficio

En una investigación realizada por Qualix Group en el año de 1996, se encontraron los siguientes costos de incidentes por industria.[7]

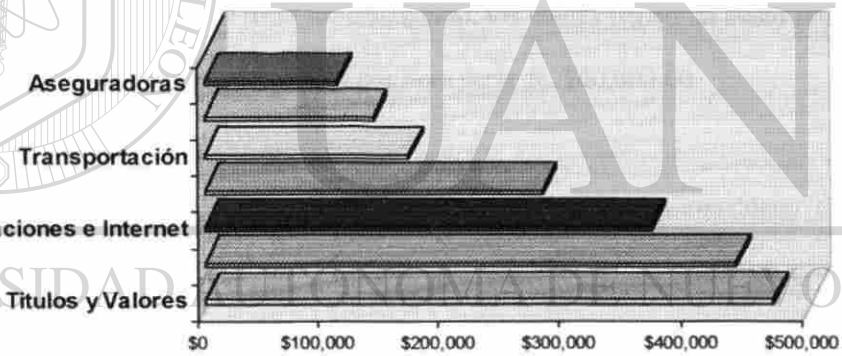


Figura 8. Promedio de perdidas por cada corte de servicio no planeado (US $)

Industria	Operación de Negocios	Costo Prom. x hora
Financiera	Operaciones de títulos	$6,450,000
Financiera	Tarjetas de Crédito / autorización de Ventas	$2,600,000
Medios de Comunicación	Pago por Evento	$150,000
Menudeo	Compras por televisión	$113,000
Menudeo	Compras de Casas por Catalogo	$90,000
Transportación	Reservaciones aéreas	$89,500

[7] Introduction to high availability and MC/ServiceGuard Bill Marmagas, Inotech , 1998

Medios de comunicación	Venta de Boletos por televisión	$69,000
Transportación	Envio de paqueteria	$28,000
Financiera	Rentas de Cajeros Automático	$14,500

Tabla 12. Costos por corte de servicio por hora según el tipo de industria[8]

Para calcular el costo de la pérdida por corte de servicios no planeados, en un valor aproximado, podríamos decir algo como:

(productividad) Número de usuarios promedio x Costo por usuario por hora +

(ventas) Número de clientes por hora x Costo promedio de operaciones del cliente +

(imagen) Costo de la imagen de mi empresa $$$$

Al menos el costo de la productividad podríamos calcularla, ya que sería la primera línea de la formula, si tenemos un total de 200 usuarios trabajando, los cuales tienen un costo promedio de 300 pesos la hora, la pérdida de productividad por hora sería de. $60,000 00

Si además queremos saber la perdida de productividad anual, debemos considerar el nivel de disponibilidad de nuestros sistemas. Por ejemplo, una plataforma que tenga un promedio de 97 5% de productividad, lo cual equivale a (100 97 5)x 24x365 = 219 horas al año, esto representa una pérdida anual de productividad de $13,140,000.00, si logramos subir la disponibilidad de los sistemas a un 99 86%, la pérdida de productividad se reduce a un valor de 12 26 horas que representa un costo de $735,600, una diferencia de $-12,404,400.00 (doce millones de pesos). El costo de una solución de alta disponibilidad posiblemente tenga un costo de un 10 a un 20% de este valor.

Se evaluamos lo anterior podremos ver con que facilidad podríamos justificar la implementación de un esquema de alta disponibilidad en aras de la productividad. Y si a esto aún hay que sumarle

el costo de ventas pérdidas y el costo de pérdida de la imagen pública, realmente la inversión en una solución de alta disponibilidad es muy baja, contra el nivel de pérdidas que pueden presentarse.

Existen diferentes niveles de disponibilidad, los cuales afectan definitivamente el costo de la solución deseada, por ejemplo:

- Una disponibilidad básica requiere que no hagas nada en especial, excepto activar la aplicación y ponerla a operar, mientras la aplicación opere, tendremos la misma disponible, es conveniente generar respaldo en ciertos periodos de tiempo para tener puntos de recuperación.
- Una disponibilidad mejorada implica proteger la información, aquí hacemos uso de arreglos de discos en RAID, y con una programación adecuada de respaldos, la eventualidad de pérdida de información se podrá evitar.
- La alta disponibilidad implica proteger al sistema, aquí requerimos al menos 2 servidores acoplados en forma relajada que conforman un cluster el cual a su vez puede estar bajo el esquema de failovers, ó de balanceo de cargas
- La recuperación de desastres implica proteger la organización al mantener al menos dos site de operación replicados entre ellos, o uno como réplica del otro. Aquí se hace uso también de los sistemas tolerantes a fallas, que son configuraciones especiales que tienen un uso muy especial (como sistemas bancarios, cajeros automáticos, etc.).

3.5 Pasos para un proyecto de Alta Disponibilidad.

Todo proyecto de alta disponibilidad debe ser ambicioso, establecer métricas específicas al negocio, objetivos a corto plazo y objetivos a largo plazo Un proyecto de alta disponibilidad

[8] Dataquest, perspective: Sept 1996

debe formar parte de un proyecto aún más ambicioso de Disaster Recovery y Remote Site Operation. Aun cuando este documento se enfocará a la Alta Disponibilidad y los pasos mínimos recomendados que debemos seguir, por supuesto algunos pasos podremos omitirlos(pero esto implicará posiblemente un costo en la disponibilidad o escalabilidad del proyecto).

No hay mejor proyecto de alta disponibilidad que el desarrollado por uno mismo. Bueno, los siguientes principios básicos del diseño de un proyecto nos servirán para planear mejor el nuestro[9]

3.5.1 Principios de Diseño para la Alta Disponibilidad

1) **Al disponer del presupuesto, no hacerlo a ciegas** La calidad es cara, sin embargo, en el área de sistemas y computación, la tendencia es usualmente inversa: Computadoras cada vez más poderosas a una fracción del costo del año pasado. Esto crea un concepto equivocado en los usuarios de que los niveles de disponibilidad pueden ser más baratos y fácules que como ocurría en el pasado, pero esto no es así; ya que la Alta Disponibilidad es un concepto de calidad. Es necesario hacer un buen análisis de costos y beneficios, así como un criterio de inversión y los plazos para lograr los niveles de disponibilidad esperada.
2) **No asumir compromisos sin información suficiente**. No hay absolutamente ningún producto de alta disponibilidad que venga empaquetado con tus sistemas. El lograr los niveles de disponibilidad deseados en sistemas finales requiere esfuerzos dirigidos a ingeniería de la redundancia, procesos para la administración, evaluación, integración y aceptación de los niveles de aplicación. Nada de esto te lo entrega un vendedor como producto recién desempacado. Nada puede ser simplemente instalado en un ambiente y esperar que nos dé la calidad y disponibilidad, sin una labor de ingeniería y de diseño

[9] Twenty Key System Design Principles from Blueprints for High Availability, Evan Marcus & Hal Stern

3) **Remover los puntos básicos de falla**. Un punto básico de falla es aquel componente (hardware, firmware, software, etc.) cuya falla causaría un cierto grado de corte de servicio Piensa de estos puntos como el eslabón más débil de la cadena, cuando se rompe ese eslabón, sin importar la calidad del resto de los elementos de la cadena, esta se romperá. Algunos puntos de fallas son obvios: Servidores, discos, tarjetas y dispositivos de red, cableado, usualmente estos se protegen contra fallas vía elementos redundantes. Siempre existirán segundos puntos básicos de falla: Es necesario recorrer toda la cadena operativa, desde la unidad de discos hacia la aplicación hacia la red hacia el usuario final del sistema, hasta identificar todo lo que pudiera fallar aplicaciones, respaldos, cintas, el servidor mismo, las instalaciones del edificio, servicios externos de comunicaciones, etc. Por ejemplo, si contratas un proveedor de comunicaciones para intercomunicar tus sistemas remotos, y proteges tu instalación contratando un segundo proveedor de comunicaciones como respaldo del primero; pero asegurarse que el segundo proveedor no este revendiendo los servicios sobre la infraestructura del primero, si falla el primero, ambos fallarán
4) **Garantizar los niveles de seguridad** El establecer los niveles suficientes de seguridad en el acceso a los sistemas, acceso a las instalaciones de los sistemas (sites), y niveles de acceso a la información.
5) **Consolidar la plataforma de servidores**. Con la baja en costos de equipos, muchos negocios se han llenado de diversas plataformas que soportan sistemas muy variados; esto ha significado costos ocultos como soporte, personal capacitado, contratos de mantenimiento con proveedores En vez de tener múltiples servidores, una forma de garantizar estabilidad (y por tanto estabilidad en los sistemas) es unificando y consolidando los sistemas en uno o más servidores de gran capacidad; con bases de datos en paralelo Esto reduce en demasia la complejidad de tus ambientes computacionales, menos equipos a respaldar, menos reboots y sobre todo, menos cosas que puedan fallar (menos puntos básicos de falla) El hecho no es poner todo en un solo servidor, sino en dos o más servidores configurados en cluster

6) **Automatizar tareas comunes**. Podemos ahorrarnos tiempo y dormir por las noches si logramos automatizar las tareas y procesos comunes. La automatización puede prevenir también los errores tipográficos, usualmente permiten que las tareas se realicen más rápido de lo que un operador humano puede hacerlo, además significa menos requerimientos humanos. Además la automatización nos permite enfocarnos en las áreas realmente relevantes del negocio. Podemos invertir en el desarrollo de herramientas que nos liberen de tareas repetitivas y de poco reto, así nuestros conocimientos no se estancan en un punto. La contraparte es que estaremos aceptando la responsabilidad de mantener y actualizar todas y cada una de estas herramientas en el momento en que empiezas a depender de ellas.

7) **Documentar todo.** Una documentación sólida nunca debe ser menospreciada La documentación proporciona caminos de auditoría que nos permitan analizar lo sucedido. Proporciona guías para que los futuros analistas puedan dominar los sistemas que existían antes de que ellos llegaran. Proporciona a los Analistas de sistemas y administradores con metas cumplibles. La documentación incluye manuales de ejecución, procedimientos departamentales, documentación del desarrollo, manuales de operación, guías de códigos de error de la aplicación, y todo aquello que un nuevo desarrollador o analista de sistemas requiera para poner el sistema en operación Nunca debemos asumir que el lector conocerá todos los temas; debemos explicar a fondo, buscando que hasta el elemento menos experimentado pueda comprender y resolver los problemas que pudieran presentarse Es importante que la documentación este en forma electrónica, pero más aun que contemos con ejemplares impresos y actualizados Debemos evitar una documentación errónea: en caso de una falla, los manuales se seguirán como un libro de fe, si algo no está bien documentado, esto provocará que las cosas vayan de mal en peor, la disponibilidad quedará completamente anulada.

8) **Establecer acuerdos de niveles de servicio.** Antes de que ocurra un desastre, es necesario establecer acuerdos por escrito con la comunidad de usuario para definir los niveles de

servicio que se proporcionarán, así como las penas que serán aplicables en caso de presentarse la falla y exceder el tiempo de resolución. Así como el nivel de evaluación y recompensa en caso de exceder en demasía los niveles de servicio acordados. Usualmente los niveles de servicio se enfocan hacia:

° **Niveles de disponibilidad.** Porcentaje del tiempo de operación en el cual los sistemas estarán realmente operando.

° **Horas de servicio.** ¿En cuales horas es realmente crítica la operación de los sistemas? ¿Qué días de la semana?

° **Ubicaciones de operación de los sistemas.** ¿Existen diversas oficinas, o instalaciones donde se hace uso del sistema? ¿Donde es prioritario que los sistemas continúen operando? ¿Esperan todos el mismo nivel de servicio?

° **Niveles de prioridad.** ¿Que sucede si dos o más sistemas están caídos al mismo tiempo? ¿Cuál tiene prioridad?

° **Políticas de escalación.** ¿Qué sucede si no se cumplen los acuerdos? ¿A quién se deberá avisar una vez que el tiempo mínimo establecido ha transcurrido?

Estos acuerdos son usualmente el resultado de considerables esfuerzos de negociación entre un proveedor de servicio y el representante del usuario. Siempre debemos tener cuidado estableciendo los niveles de servicio que realmente podremos cumplir No podemos garantizar los niveles de servicio midiéndolos desde la perspectiva del cliente cuando dependes de terceros o proveedores externos, a menos que tengas el nivel de autoridad y responsabilidad sobre cada uno de los componentes del sistema acordado Si al menos un componente esta fuera de tu control, si este falla, ¿quién lo corregirá? El responsable, ¿firmó un acuerdo de servicio contigo o con tus usuarios?

Un ejemplo de un acuerdo de servicio sería

Acuerdo de Nivel de Servicio esperado	**10-Jul-2001**

Área Usuaria (Dirección, Gerencia):	Gerencia de Facturación
Área de Servicios:	Gerencia de Soporte a la Operación

Objetivo Establecer un acuerdo en los niveles de servicio esperados, la calidad y tiempo de respuesta, así como las penalizaciones que aplicasen Definir las obligaciones y responsabilidades de las áreas involucradas.

1) La gerencia de Facturación. De ahora en adelante llamada el "Usuario", establece un requerimiento de servicio hacia la Gerencia de Soporte a la Operación, de ahora en adelante llamada el "Soporte"

2) El Usuario establece que requiere un nivel de servicio de calidad en la generación, calculo e impresión de las facturas del Cliente. El Soporte establece que cuenta con la capacidad para proporcionar este servicio de acuerdo a los lineamientos establecidos en este acuerdo, y según el nivel de prioridad definido de común acuerdo

3) El Usuario no es dueño de la información, sino su administrador y salvaguarda y por lo tanto es responsable de operar los sistemas dentro de los lineamientos y reglas documentados en los manuales mismos de operación y uso, tal que los datos y valores registrados dentro de los mismos sean verdaderos y den fe las operaciones realizadas con el Cliente y en representación de la empresa. Cualquier desviación en el correcto uso de estos servicios que implique fallas en la veracidad de la información será bajo la responsabilidad del Usuario, y no podrá ser imputable al Soporte.

4) El Usuario deberá cumplir los horarios de operación establecidos los cuales se definirán de común acuerdo con el Soporte, y en caso de requerir operar los sistemas fuera de los horarios previamente establecidos. Será responsabilidad del Usuario el avisar y acordar con el Soporte por la prestación de servicios fuera de estos horarios En caso de imposibilidad del Soporte de ofrecer

estos servicios fuera de los horarios previamente acordados y de ocasionar retraso en la operación, no será imputable al Soporte.

5) El Usuario se compromete a cumplir los acuerdos que como parte del servicio surjan debido a que el Soporte ha detectado un causal de baja en el servicio imputable al Usuario Demasiadas sesiones abiertas (el Soporte indicará cuantas podrá abrir en un momento dado), Consultas, Reportes o Jobs que exigen demasiados recursos (el Soporte recomendará los mejores horarios para efectuar este tipo de procesos) En caso de que el Usuario (todo o en alguno de sus elementos) se niegue a cumplir estas recomendaciones o acuerdos, el Soporte podrá evitar cualquier responsabilidad sobre el nivel de servicio.

6) Los horarios de uso de los sistemas se definen según el horario laboral para la empresa, que actualmente es de:

Periodos normales de trabajo

Lunes a Viernes: 8:00 horas hasta las 17.00 horas

Sábados y Domingos: No se opera.

Cierres de Mes (1,2 y 3 de cada mes)

Cualquier día de la semana 00:00 horas a 24 00 horas

Cualquier otro horario deberá ser acordado entre las partes

7) El Soporte deberá establecer las previsiones requeridas para poder ofrecer el nivel de servicio establecido Ya sea con la adquisición de inventarios o partes difíciles de obtener, o contratando con un tercero los servicios necesarios que solucionen el caso presentado. Adquiriendo el Hardware o Software mínimo necesario que logre garantizar el cumplimento del nivel de servicio esperado.

8) El Soporte se compromete a garantizar el 99 50% de disponibilidad de los sistemas durante los horarios de operación establecidos El Soporte ofrece un nivel de servicio de hasta el 90% durante

los horarios de operación acordados con el Usuario cuando estos horarios no estén dentro de los horarios de operación establecidos. En horarios fuera de los establecidos para la operación En caso de que el Soporte no pueda ofrecer el servicio a causa de mantenimientos o respaldos programados, o por disponibilidad del personal del Soporte, este podrá optar por negar el servicio al Usuario, o contratar personal externo con cargo al Usuario (mediante acuerdo escrito con el Usuario).

9) Existen tres tipos de servicios que el Soporte está obligado a ofrecer:

a) Soporte Crítico: La operación y actividades del Usuario se ven totalmente impedidos de continuar, no existe solución inmediata conocida. El Soporte deberá comunicarse con el Usuario y establecer un plan de acción en al menos 10 minutos dentro de los horarios de operación establecidos(o acordados), y de 40 minutos fuera de estos horarios. El Soporte se compromete a dar una respuesta y solución en un plazo no mayor a 24 horas.

b) Soporte Urgente. La operación se ve interrumpida en algunas partes, otras pueden continuar, existe alguna solución pero requiere detener la operación para su aplicación y no es fácil de aplicar. El soporte deberá comunicarse con el Usuario y establecer un plan de acción en al menos 1 hora en los horarios de operación establecidos (o acordados), y de hasta en 3 horas en otro horario. El soporte se compromete a dar una respuesta y solución en un plazo no mayor a 48 horas, y a través de un acuerdo con el Usuario sobre el momento de detener la operación para aplicar la solución

c) Soporte Básico: La aplicación o sistema opera normalmente, pero con lentitud palpable, el Soporte podrá evaluar la situación y responder al Usuario en un tiempo de al menos 2 horas en horarios establecidos (o acordados) y de hasta 5 horas fuera de horario. El Soporte deberá ofrecer una solución y acordar con el Usuario su aplicación (en caso de requerir costos extras) en un plazo no mayor a 5 días laborales

9) En caso de que el Soporte no cumpliese con los niveles de servicio establecidos

9) **Planear a futuro.** Estamos hablando de planear para emergencias y crisis; así como casos operacionales no cubiertos por tus herramientas automatizadas En algún punto, se podrían presentar múltiples y complejas fallas, que no se habían presentado en la operación del día a dia y las cuales requerirían intervención humana. Si has preparado un plan base de atención y seguimiento de las fallas, estarías en capacidad de seguir una guia para cada posible situación Si al contrario, pretendes resolver la situación priorizando y coordinando en tiempo real, dejarás la puerta abierta a miles de posibilidades de solución

10) **Probar todo.** Es necesario probar tanto los planes para emergencias y crisis como también las nuevas aplicaciones, cambios al software de sistemas, o cambios de hardware. Es recomendable que las pruebas sean tan próximas a los sistemas de producción como sea posible. De ser posible, las pruebas deben ser hechas por los mismos usuarios que en la operación normal. Existen herramientas de modelación y simulación de usuarios que pueden ser usados como medios de aseguramiento de calidad, pero usualmente es mucho mejor preparar un ambiente que se vea y sienta como en la vida real, aún antes de activar al sistema. También es importante hacer pruebas unitarias ¿qué pasa si falla una tarjeta de red?; ¿qué pasa si falla un arreglo de discos? Adicionalmente, las pruebas necesitan repetirse cada cierto tiempo Debemos adoptar una política de pruebas regulares; aún cuando esto no sea lo más popular dentro del departamento

11) **No mezclar ambientes operativos.** Debes mantener tu ambiente de desarrollo, de pruebas, entrenamiento y de producción independientes los unos de los otros No solamente los servidores sino también, dentro de lo posible, redes separadas y usuarios separados Los usuarios de desarrollo no deben tener acceso al equipo de producción, excepto durante los pocos días que exista la liberación de un nuevo modulo. Es conveniente que se procure tener un ambiente propio para pruebas de recuperación de desastres.

12) **Invertir en métodos de aislamiento de problemas.** El aislamiento de problemas significa que la aparición en un sistema o en un área de la empresa, no debe extenderse hacia otros

sistemas o áreas de la empresa. Debes tener la capacidad de identificar los problemas en el lugar donde se generan y detenerlos o solucionarlos antes de que se extiendan.

13) **Observa la historia de los sistemas.** Para poder ver que cambios hacer en los sistemas para hacerlos más elásticos, y estables, debes de observar la historia de operación reciente del sistema. ¿Por qué se ha caído el sistema? ¿Cuáles han sido las causas más comunes? El tener una bitácora actualizada de los sucesos más recientes dentro del sistema nos puede dar más información que si nos basáramos en historias anecdóticas Por ejemplo; si el sistema falla todos los días a las 3 de la mañana, hay que revisar las estadísticas operacionales, hay que detectar que sucede antes de las 3; que puede estar causando esta falla. Es necesario encontrar la raíz de la causa, y el momento real de la falla, quizás la falla no es a las 3 de la mañana sino a las 5:20; precisamente despues de que se lanzan los procesos de consolidación de información. Contabiliza cada incidente que ha causado fallas o corte de servicios, investiga los tiempos de recuperación (MTTR) ¿cuánto tardarón en llegar las partes falladas? No inviertas más esfuerzo del requerido en aquello que no es relevante; aplica la regla del 80/20 no dediques más esfuerzo.

14) **Construye para crecer.** Aunque en algún momento adquieras los recursos suficientes para tener capacidad de hasta el doble de operación, esto nunca es suficiente, pues el uso o abuso de los recursos se extenderá más allá de lo planeado originalmente terminando por consumir todos los recursos inicialmente adquiridos. Si segun la planeación, tus requerimientos serán de 4 CPUS, compra un servidor con capacidad de 8 CPUS, y 4 CPUS iniciales, dejando así espacio para ampliar la capacidad. Si compras el servidor con capacidad de 4 CPUS, al requerir incremento de capacidad, solo podrá hacerse con la adquisición de todo un nuevo servidor. Recuerda igualmente la capacidad de disco, si compras un servidor con cierta capacidad de discos, si quieres agregar más de los slots disponibles no podremos crecer de acuerdo a las nuevas necesidades.

15) **Usar software ya probado.** En el mercado hay muchos productos que están en operación, la regla que debemos seguir es buscar la utilización de software que este ampliamente probado y usado en múltiples instalaciones, no podemos justificar ser el conejillo de indias; la empresa es más importante que entrar en etapas de pruebas con nuestra plataforma de producción Sin embargo, si puedes tener capacidad para establecer áreas de pruebas y desarrollo, podrás también adquirir productos y probarlos, mientras tu operación continua con tus sistemas actuales. Esto te permitirá crecer sobre plataformas más eficientes y bien probadas. Adicionalmente, busca compañías sólidas y bien establecidas, quizás existe un proveedor de una herramienta de bases de datos digamos "SuperBase", que trae algunas funcionalidades que lo hacen más fácil de manejar y es más barato que Oracle o que Informix, sin embargo, este producto lo desarrollo un proveedor local que quizás tiene problemas financieros, ¿Pondrías tu empresa en sus manos? ¿Que sucede si en 2 meses desaparece el producto? ¿Cuantos expertos hay en el mercado que te puedan dar soporte? Sin embargo, el vendedor de SuperBase te ofrece un viaje a Cancún, crees que es tan importante arriesgar el futuro de tu compañía en un producto que no tiene suficientes bases financieras como para permanecer en el mercado Recordemos que aun cuando el producto sea de excelente calidad, se tiene que considerar la antigüedad de los proveedores y que permanencia tienen hacia un futuro cercano. Adicionalmente, los proveedores ampliamente establecidos tienen Grupos de Usuarios que tienen soluciones a problemas que ellos ya han vivido, existen Foros de discusión sobre características especiales del manejador, conferencias internacionales que te permiten empaparte de experiencias de otras profesionales, etc Siempre será más factible que puedas encontrar a alguien que haya desarrollado una solución o un workaround a un problema que te llegarás a presentar en el futuro sobre un producto que esta ampliamente presente y maduro.

16) **Elige hardware confiable y de fácil mantenimiento.** La información sobre el MTTF (tiempo entre fallas) puede ser difícil de obtener y en ocasiones el proveedor lo considera

confidencial, sin embargo, al adquirir nuevos equipos, debemos hacer un esfuerzo para lograr un dato comparativo del MTTF para distintos proveedores Debemos tener una idea de que tan frecuentemente fallarán las piezas del equipo a adquirir Por supuesto que al usar componentes de hardware más confiables se obtendrá un equipo más confiable y por tanto un sistema más confiable. Además de evaluar el MTTF, es necesario evaluar que tan fácil es remplazar un componente fallado pues esto afecta al MTTR, por ejemplo, es más fácil remplazar un disco si el arreglo es hot swap y los discos están por la parte externa del arreglo. Es necesario identificar que partes son más difíciles de adquirir en un periodo corto y establecer un inventario local base.

17) **Reutilicemos configuraciones.** Si haz logrado implementar una configuración cuyo uso haya sido exitoso, réplica esta configuración donde sea posible Es conveniente tener 2 o 3 configuraciones (pequeña, mediana, grande) perfectamente conocidas para los posibles requerimientos, el tener más configuraciones posibles implicaría posible desconocimiento en el comportamiento de las mismas Posiblemente tengamos que estar revisando y ajustando las configuraciones existentes, pero al limitar el total de las mismas tendremos:

Facilidad de manejo: Menos configuraciones implican menos combinaciones y permutaciones de software y hardware, menos situaciones que conocer, y menos cosas que pudieran fallar

Configuraciones probadas. Si exactamente la misma configuración se tiene instalada en 6, 8 o 10 instalaciones, el lograr una instalacion más requerirá un esfuerzo menor para garantizarla Sólo se tendrán que evaluar aquellos elementos que han sufrido cambios.

Alto nivel de confiabilidad en nuevos proyectos. Si tienes una configuración específica que ha operado en proyectos previos, es mucho más sencillo justificar su uso en futuros proyectos

Compras en paquete. Es más sencillo y barato el comprar un paquete de un componente que el hacer pequeñas compras en pequeñas cantidades de diversos componentes, especialmente cuando se involucran distintos proveedores.

Partes de repuesto. Al tener menos componentes distintos, esto significaría menos inventario de partes de repuesto, reduciendo uso de espacio de almacenamiento, y simplifica el proceso de inventario

Se reduce la curva de aprendizaje. Al hacer uso de configuraciones probadas, la curva de aprendizaje es dejada atrás rápidamente y permite a los Administradores enfocarse en menos tiempo hacia los objetivos de la compañía y se vuelven productivos más rápido

18) **Adquiere Servicios Profesionales.** Sin importar el tipo de problema que se desea resolver, o que productos se usen, probablemente alguien ya lo hizo anteriormente. Usualmente los vendedores de Software o Hardware cuentan con profesionales o socios consultores con experiencias y conocimientos similares que pueden ayudar, quienes por una tarifa visitarán tu site e implementarán la solución requerida o al menos estableceran las guías y lineamientos para implementarla. Sería conveniente que además de resolver la situación se negociara la transferencia de conocimientos hacia un recurso interno Si el proveedor ofrece entrenamiento es conveniente tomarlo antes de la implementación. Asiste a grupos de usuarios, documentos publicados, white papers, sitios en Internet, así como algún otro posible caso de estudio.

19) **Atiende un problema a la vez.** Los problemas complejos pueden tener varios causales o problemas secundarios Se debe enfocar a un causal a la vez, en ocasiones una solución para un causal, resolverá otros causales adicionales, sin embargo, habrá ocasiones que la solución de un problema o causal de problema podrá provocar otros problemas directa o indirectamente, como puede ser incompatibilidad con algún componente de hardware o módulo de software

20) **Simplicidad ante todo.** El hecho de estar implementando una solución compleja de alta disponibilidad, lo cual implica muchos causales posibles de falla, es necesario eliminar situaciones complejas artificiales, procura hacer uso de los elementos más sencillos, maneja configuraciones probadas, usa nomenclaturas fáciles de manejar, evita usar los servidores para fines distintos al establecido. Las soluciones de alta disponibilidad tienden a ser complejas, procurar no complicarlas más allá de lo naturalmente requerido nos ayudará en las labores de soporte y mantenimiento de las mismas.

3.5.2 Proyecto de Alta Disponibilidad.

Como todo proyecto y debido a la envergadura que puede tener un proyecto de este tipo, se deberán realizar todos los esfuerzos y seguir todos los procedimientos para lograr la justificación y éxito del mismo.

Antes que nada deberá identificarse la necesidad de tal proyecto. Así como informarse con documentación y material relevante al respecto (este documento puede ser un buen principio).

3.5.2.1 Identificar la necesidad del proyecto.

La situación más compleja de toda empresa, no es darse cuenta de que requiere un esquema de alta disponibilidad para un sistema que ha presentado una falla, pero hacerlo cuando los sistemas no han presentado tal falla y prepararse para ello Se requiere identificar los sistemas de mayor impacto a la operación de la empresa, y que afectarán en mayor cuantía en caso de fallar

Es necesario investigar y evaluar cada departamento, sus sistemas de apoyo, que sistemas sirven de eje para que fluya la información entre departamentos, así como el impacto que tendría en la operación global de la empresa el que uno de estos sistemas fallara Es necesaria una planeación de los sistemas del negocio (BSP) para identificar los procesos más rentables de la organización,

los sistemas involucrados en estos procesos, y el costo relativo en caso de que un proceso se detuviera a causa de una falla

Este paso debe involucrar tanto al personal administrativo de las áreas, a los elementos de IT que les proporcionan los servicios Entre las preguntas que pueden efectuarse tendríamos:

¿Si el sistema de pedidos dejará de operar entre las 08:00 y las 12:00 que impacto tendría a la empresa?

¿Existe la posibilidad de recuperar el número de transacciones que dejaron de realizarse en dicho período? ¿Debemos contratar personal adicional o requerirá tiempos extras?

¿Existe afectación directa al cliente de la empresa? ¿Hay un costo de imagen?

Si se logra restablecer el servicio pero con un desempeño inferior, ¿Se puede procesar bajo estas condiciones?, ¿Existe la posibilidad de generar lotes para todo cuando se logre reactivar el sistema al 100%?

¿Esta dispuesta la empresa a invertir en infraestructura para garantizar un mejor nivel de servicio?

La información siempre es el principal activo de cualquier empresa, los discos o equipos que tiene la empresa son realmente de bajo costo contra el valor de la información almacenado en ellos. ¿Se tiene la conciencia de este valor implícito? Muchas veces sera necesario iniciar una labor de concientización. ¿Se han presentado eventos de falla de los sistemas? ¿Cuando? ¿Que procedimiento se ha seguido para restablecer la operación? ¿Cuanto tiempo ha transcurrido para reactivar los sistemas?

En mi vida profesional he participado apoyando a diversas empresas a restablecer la operación de sus sistemas fallados, sin embargo, el costo que ha representado para ellos ha sido tremendo En una de estas empresas, el no tener un respaldo actualizado de la provoco un extenso tiempo de recuperación de la falla (MTTR), ya que falló el disco principal donde estaba el sistema operativo y los archivos de control de la información Fue necesario reinstalar el sistema operativo, reinstalar la aplicación, reinstalar el manejador de la base de datos, y recuperar el respaldo previo

de la base de datos. El proceso de recuperación de la información fue toda una odisea, el respaldo era anterior a unos cambios de configuración y el equipo donde se tenía la instalación era realmente arcaico: Se tuvo que ir a otros sistemas a extraer información para su reproceso, se tuvo que identificar los datos que habían cambiado, el proceso de cargar la información que se obtuvo de otros sistemas consumió aproximadamente 3 días debido a que el sistema era muy lento en la carga de información, y a que se tuvo que capturar información adicional Una vez que se logró la recuperación del total de la información disponible (no el total de la información perdida), se hizo un respaldo de toda la instalación lo cual consumió 8 horas aproximadamente.

Actualmente esta empresa está evaluando medios para reducir los tiempos entre cada respaldo, y mover su instalación hacia arreglos con redundancia, así como establecer planes de respaldo incrementales, sin embargo, es recomendable considerar la alternativa de una solución de Alta Disponibilidad.

3.5.2.2 Clasificar los procesos.

Dentro de la organización, es necesario encontrar aquellos procesos básicos que no pueden dejar de realizarse para llevar la organización adelante. Por ejemplo, sabemos que tenemos un sistema de contabilidad, sin embargo, si este sistema falla ¿Existe algún riesgo inmediato? ¿Detendrá la operación la empresa debido a su falta? La respuesta puede parecer obvia, pero muchas empresas invierten el mayor capital en estos sistemas que basicamente son los mismos entre cada empresa, aún de distinto ramo industrial, no significa que no les demos importancia a ellos. La empresa debe enfocarse hacia aquellos sistemas que le detendrán la operacion real de la misma Por ejemplo, si falla el sistema de manufactura Podremos fabricar las 150,000 piezas que teníamos programadas por entregar la proxima semana O si falla el sistema de inventarios¿que ocurre con todos los materiales requeridos para la fabricación de la siguiente remesa, o peor aún, por tener el inventario no actualizado debido a la falla, se fabricaron 275,000 piezas adicionales, y no sabemos donde almacenarlos, ni como venderlos ¿Que sucede si mi sistema de facturación no

opera? Podríamos pensar que no hay problema, puedo seguir entregando productos y ofreciéndolos para la venta, pero, y los ingresos, como puedo garantizar que mi empresa seguirá operando si no puedo facturar, y por lo mismo no puedo tener liquidez para el siguiente plan de producción. Que pasa si soy un comerciante a detalle, no puedo vender absolutamente nada, se detiene completamente mi operación, mis clientes se van inmediatamente a la competencia, ellos vienen a surtir su despensa, y no van a esperar a que yo me ponga a revisar porque no puedo cobrarles.

Para este punto, debemos tomar la información que surge de las preguntas antes mencionadas, adicionalmente debemos evaluar; si sabemos que un sistema determinado es el que tiene mayor impacto en el negocio, cual es el costo de brindarle protección al mismo Que infraestructura se cuenta actualmente para soportar el sistema. ¿Cuál es el costo de reemplazo de cada pieza? ¿Se puede mejorar la plataforma tecnológica?.

Definitivamente no será una buena idea empezar un proyecto si la empresa no esta conciente de que debe invertir en su infraestructura. Debemos recopilar la mayor cantidad de información disponible, organicemos estos datos, establezcamos costos por hora de operación para cada proceso, así como costo por hora adicional (tiempos extras)

3.5.2.3 Alcance del proyecto

Este es un rubro muy importante, debemos tener bien claro hasta donde llevaremos el proyecto, y las implicaciones que tendrá el llevarlo hasta ese alcance. Debemos analizar ¿Cantas plataformas de hardware tenemos?, Y ¿Cuantas de sistema operativo? Si deseo que todos mis sistemas estén bajo el esquema de alta disponibilidad, ¿Deberé adquirir un producto de clustering específico a cada plataforma? ¿Deberé adquirir un producto de clustering multiplataformas? Podríamos establecer primero un proyecto que estandarice la plataforma de hardware y Sistema operativo para todos mis sistemas, y entonces iniciar una segunda fase que sea la planeación para la alta disponibilidad.

Existen muchos elementos que intervienen en un proyecto de Alta Disponibilidad. ¿Que elementos podremos considerar?

Infraestructura eléctrica: No sólo es contratar la compañía de luz, ¿Tenemos posibilidades de adquirir al menos 2 fuentes de poder (UPS)? Si un UPS falla, cortando entonces la electricidad, tengo mi servidor de respaldo conectado al segundo UPS, algunas cuestiones parecen obvias, pero no siempre se plantean.

Infraestructura de redes. ¿Podremos justificar cuando menos dos redes para la operación? Si una falla la otra podrá garantizar que la operación continúe, debemos evaluar el costo de estas redes y el beneficio que perdemos en caso de no obtenerlas. Adicionalmente necesitamos una red para intercomunicar los equipos que formarán parte del cluster(esta es la red de heartbeat), de tal forma que estos sepan si el otro equipo esta respondiendo. ¿Que tipo de cableado usaremos? De cobre o fibra óptica, o haremos uso de redes inalámbricas, la respuesta depende del tipo de sistema que se va a implementar. Además cada uno tiene sus consideraciones, una instalación de fibra óptica sería ideal para instalaciones que cubren grandes distancias, y se necesitaría que complementar con instalaciones en cobre. Sin embargo, las instalaciones de cobre son propensas a inducciones magnéticas o eléctricas si no están perfectamente aisladas. La red es uno de los componentes más importantes de la infraestructura en el sentido de que sin red, no hay acceso a los sistemas, y si no tenemos una red adicional de heartbeat –o si ambas redes están alimentadas por una misma fuente de poder, en caso de falla, como los servidores que forman el cluster no pueden verse uno al otro, ambos pueden establecer que tienen el control de los arreglos de discos. Si esto ocurre, puede haber corrupción de datos si ambos escriben al arreglo al mismo tiempo.

Infraestructura de servidores: Requerimos al menos un servidor adicional para que tome control de los servicios en caso de que el servidor primario falle. Podremos justificar el tener un equipo que a la vista de todos no hace nada (solo esperar a que el otro falle)

Infraestructura de almacenamiento. Requerimos arreglos de discos que puedan ser accedidos por 2 o más servidores a la vez, ¿Tenemos forma de justificar un arreglo de discos que soporte

acceso simultáneo de dos o más servidores a la vez? Esto es importante pues en caso de fallar la red de heartbeat, ambos servidores querrán tomar el control del arreglo de discos ¿Podríamos configurar que un disco fuera usado como heartbeat entre servidores? Existe la posibilidad de llegar a implementar una Storage Area Network(SAN).

Software de Sistema Operativo: Soporta el S O en forma directa de operación bajo clustering, requiere un software adicional Invitemos al proveedor a que nos proporcione y recomiende alternativas.

Software de Aplicaciones y Base de datos: Que cambios requieren mis aplicaciones y mi base de datos para soportar el clustering. Invitemos al proveedor a que nos proporcione y recomiende alternativas.

Planeación de respaldos y casos de recuperación: Tenemos la infraestructura para respaldos, ¿Cómo se verá afectada esta infraestructura?, ¿Poseemos algún robot? ¿Algun Silus? Si es así, estará este control de respaldos por una SAN, si tenemos redes replicadas, ¿Tendremos acceso desde los servidores hacia el robot (o silus) a través de ambas redes? Si solo tenemos acceso por una red, ¿Cual es nuestro plan para administrar los respaldos en caso de falla de la red en juego?

Software de Clustering: Que producto usaré para el clustering, usaré un producto especifico para la plataforma que deseo instalar, o usaré un producto que opera en múltiples plataformas. Si recordamos la sección donde se mencionan algunos de los distintos productos que existen para clusters, aquellos productos que son específicos para una plataforma, son los más estables y con mayor escalabilidad y nivel de disponibilidad, sin embargo requiero de un experto específico para cada plataforma Por el otro lado un software multiplataformas, me permite tener un solo experto que podrá soportar las "N" plataformas diversas, sin embargo, este tipo de software no esta muy ligado a la plataforma y por lo tanto no proporciona el nivel total de disponibilidad que el especializado La recomendación es invitar a los proveedores de sistema operativo, usualmente estos ya tienen asociaciones con algún proveedor específico, o ellos mismos son proveedores de

la solución, adicionalmente podremos invitar a proveedores independientes de software de alta disponibilidad (ya sea multiplataforma o específico a una plataforma)

Direcciones IP y Servicios DNS: Es necesario que las direcciones IP's y los nombres de paquetes de servicios, se resuelvan en forma dinámica y puedan asignarse a un servidor o a otro en todo momento. Tengo mis servidores DNS en alta disponibilidad, si todos mis servicios se resuelven a través de nombres de servicios, que sucede si se cae mi servidor DNS y no hay otro para resolver la IP donde están montados los servicios.

Cuando hayamos identificado los alcances, podremos definir un plan general de acciones para lograr la implementación de este proyecto Diseñar la infraestructura de alimentación eléctrica, planeación de redes distribuidas, diseño de la solución de Alta Disponibilidad, etc.

3.5.2.4 Convenzamos a la alta dirección.

Para esto, requerimos más que nuestra buena voluntad, si vemos el punto anterior, se hablaba de lo que podría costar a la empresa el no poder ofrecer los servicios, o el detener su operación. Esta información debe complementarse con un buen análisis, cuanto le cuesta a la empresa cada hora de trabajo, cuanto se puede tardar el proveedor en tener un repuesto Quizás estos datos no son muy relevantes por si solos, pero si empezamos a sumar horas y costos, podremos llegar a un número bastante respetable que pueda realmente aclarar el costo para la empresa. No deberá mencionarse solamente aquello nos ha ocurrido o que nos pudiera ocurrir, hablemos casos de estudio, de sucesos documentados sobre otras industrias, quizás es muy impactante por su cercania, pero en el caso de los atentados a las Twin Towers, además del costo de aseguranza, Quizás no podrán sobrevivir algunas compañías (si alguna subsistió a la catástrofe) o reiniciar su operación si sus sistemas estaban en alguno de estos edificios, por supuesto esto es muy drástico y va más allá del alcance de este material, pero debemos buscar los argumentos que nos permitan convencer, en menor escala y con un alcance modesto, de implementar esquemas de Alta

Disponibilidad. Pensando en un futuro cercano en el caso mayor de un esquema de Recuperación de Desastres con replicación de sites.

Hablemos de un Sistema de punto de venta, en un negocio de ventas a detalle (Soriana, Walmart, Gigante, 7Eleven, Oxxo): Si no puedo vender ¿Cuánto se deja de ganar por una hora perdida? ¿Cuánto debo pagar de salarios sin recibir nada a cambio?, ¿Cuantas tiendas se ven afectadas? ¿Todas o sólo una? Si a esto le sumo el costo de reparación y restablecimiento de la operación: ¿Cuánto he perdido?. Podemos usar la fórmula aproximada mencionada en el punto 3.4 pero acentuemos algo más ¿Cuál es el costo de imagen pública? ¿Seremos el ridículo de la industria? O ¿Perderemos la confianza del cliente?.

En el año 1999 "Toys R'Us" ofertó que todas las compras navideñas por Internet tendrían entrega a domicilio el día de navidad y un buen descuento, fue una muy buena tecnica de mercadeo, pero no se contempló la penetración de la oferta ni la capacidad de sus equipos. Sus equipos de servicios por Internet se colapsaron, y hubo sobre demanda, todavía en enero de 2000 se estaban haciendo entregas de productos de la venta navideña, fueron enjuiciados por 1 5 millones de dólares, y ni hablar del costo de imagen pública[10]. En febrero del 2000 la compañía Proflowers Inc. Prometió entrega garantizada el 14 de febrero por una cuota de $10 dolares adicionales en el envío, sin embargo, esta compañía fallo también en la entrega de sus productos, debido a sobre demanda y caída de sus sistemas[11] Estos son casos reales y públicos, podremos hablar de los costos implicados para tales empresas, que significará no sólo los económicos directos, sino los de imagen pública

Debemos mencionar que siempre habrá factores externos e internos a la organización, nuestro trabajo consisten en identificarlos y buscar la forma de eliminarlos, si no los externos cuando

[10] Time to deliver the goods, By Paula Jacobs **eWEEK** 19 de nov de 2000

[11] Proflowers fails to deliver © Eugene R Quinn Jr (An expert in e-Commerce and Professor in law at Barry University School of Law at Orlando Florida)

menos los internos, si no podemos eliminarlos cuando menos reducir el nivel de impacto que esto implica.

Un buen proyecto de Alta Disponibilidad debe recibir el patrocinio y convencimiento de la alta dirección, esto es lo que determinará el éxito o fracaso de todo proyecto dentro de la empresa. En algunas organizaciones puede haber problemas para acceder a los ejecutivos de la alta administración y explicar los objetivos y resultados esperados de un proyecto de Alta Disponibilidad. Si esto ocurre, entonces se deben considerar las siguientes acciones:

- Agenda una visita ejecutiva a otros negocios que hayan hecho estudios y/o implementaciones exitosas sobre Alta Disponibilidad
- Invita a tu organización a los ejecutivos de las empresas expertas y proveedoras de servicios de Alta Disponibilidad.
- Planea y dirige una presentación ejecutiva de Alta Disponibilidad para tu alta dirección
- Proporciona un método formal y objetivo para que la administracion establezca las prioridades sin afectar intereses particulares.
- Procura enfocarte en los procesos de negocio que afectarian mayormente ala organización. Detecta los sistemas de información que intervienen para cada uno de estos procesos, busca aquellos que por lo menos garantizaran que la empresa seguirá existiendo después de una situación de falla mayor
- Si no se obtiene la aprobación de la alta dirección, regresa a recopilar más información y a reforzar tus estudios de soporte para buscar una nueva oportunidad más adelante.

3.5.2.5 Establece el equipo de trabajo.

Busca la participación en el equipo de trabajo de los elementos más representativos de cada una de las áreas involucradas. Definitivamente la Administración de Bases de Datos, la Administración de Sistemas Operativos, la Administración de Redes, de Monitoreo y Control, y

Desarrollo de Sistemas (Requeriremos que adecuen ciertos módulos, interfases y secciones criticas, etc.). Deberá definirse un lider administrador del proyecto y coordinador de avances. El desarrollo de una solución de alta disponibilidad no debe modificar la estructura básica de operación y funcionalidad de la aplicación, pero quizás requerirá cambios a algunos módulos, o desarrollo de algunas interfases, para poder determinar si la aplicación esta operando, así como para poder soportar el movimiento de los paquetes de procesos entre equipos. El área de usuario final, deberá estar informada, sin embargo, para garantizar la aceptación del proyecto de Alta disponibilidad y definición de las medidas de nivel de servicio.

3.5.2.6 Diseño del cluster.

El diseño de la solución de alta disponibilidad será nuestra base para desarrollar el proyecto. Este diseño depende mucho de las respuestas a los planteamientos definidos en el alcance del proyecto, al presupuesto autorizado, y a las soluciones disponibles para la plataforma elegida

Algunas de las posibles configuraciones, pero sin limitarnos a estas, son

Cluster Binodo Es la configuración más sencilla de configuración de un cluster de failover, y la más usualmente encontrada en las diversas empresas Consta de 2 servidores interconectados mediante dos redes dedicadas, el objetivo de estas redes es funcionar como heartbeat para que un nodo detecte si ha fallado el otro Es recomendable que el heartbeat esté en dos redes dedicadas, sin interconexión entre ellas, pues en caso de fallar una red de heartbeat la otra red proporcionará este servicio, aún en caso de fallar esta podríamos usar como alternativa la red pública (considerando los tiempos de confirmación de la señal) Si el heartbeat no esta en redes dobles independientes, en caso de presentar una falla en una red, pudiese ocurrir la llamada división de cerebros, donde al perder comunicación un servidor con el otro, ambos asumen que el otro falló e intentan tomar el control de los discos y administrar los procesos, accediendo los discos al mismo tiempo Esto puede provocar corrupción en la información y perdida masiva de informacion Como ambos servidores están conectados a un juego de discos en espejo, estos discos se dividen

idealmente mediante dos controladores y dos arreglos de disco separados, donde los datos son replicados de un controlador hacia el otro. Ambos servidores están conectados a la red pública, y comparten una o más direcciones IP, que se transfieren de un nodo al otro según la ocurrencia del failover, esta dirección IP se llama IP virtual, pues se asigna a un equipo según la función que hará el equipo. Con esta descripción, Si se desea reducir costos, eliminando algunas partes del proyecto, deberá evaluarse el impacto al nivel de elasticidad y capacidad de soporte a la disponibilidad.

De este tipo de configuraciones existen configuraciones Simétricas o Asimétricas.

- **Configuración asimétrica**: Existe un nodo maestro (primario) el cual ejecuta todas las transacciones criticas que el cluster debe ofrecer, mientras el segundo nodo(secundario)

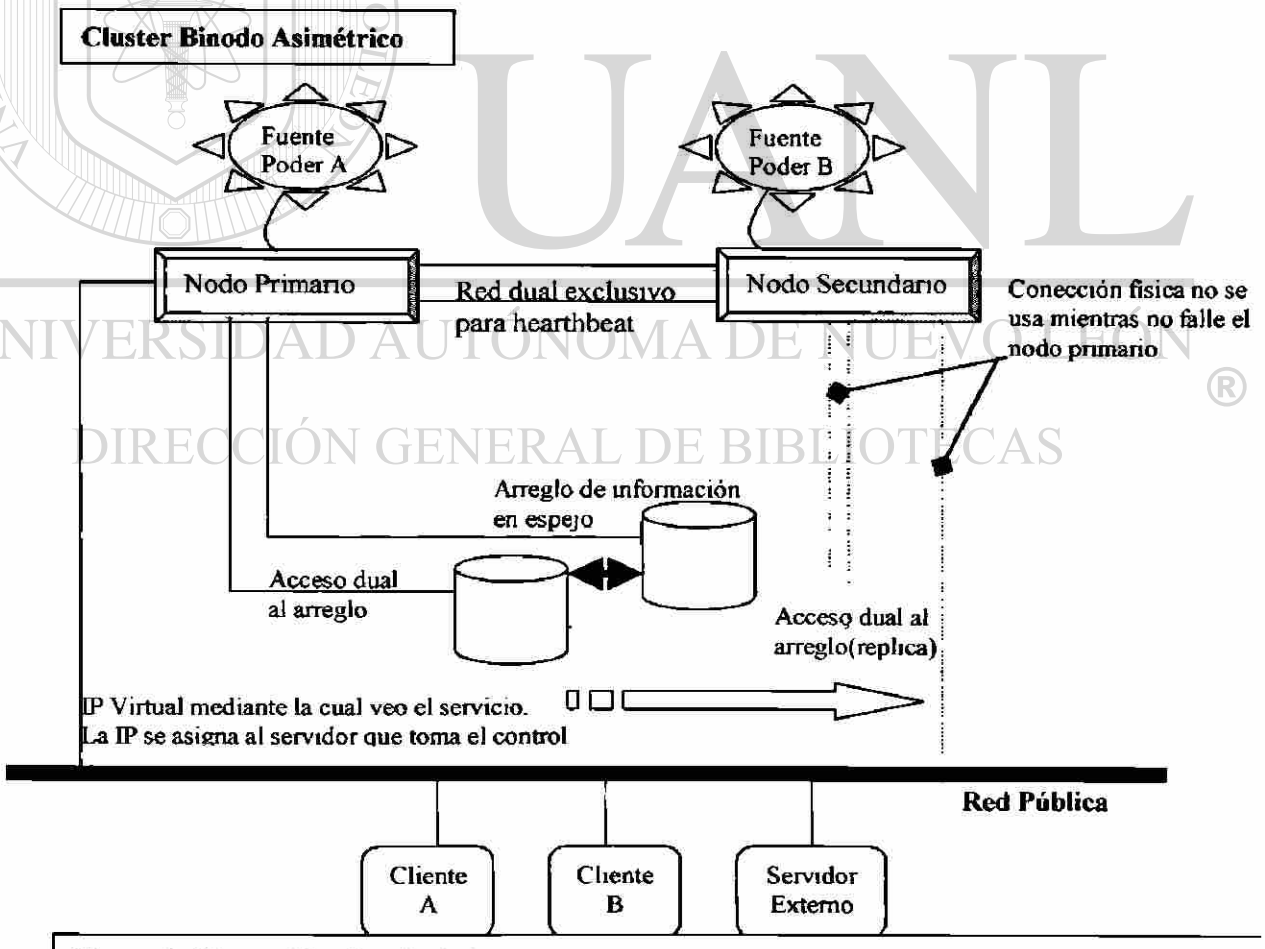


Figura 9. Cluster binodo asimétrico

esta encendido y en estado de espera, listo para recibir la carga de trabajo en caso de que el nodo primario falle.

En esta configuración, en el proceso de aprobación de presupuestos se cuestionará porque debemos pagar por un servidor que no está operando el 100% del tiempo, y que duplicará el costo de la inversión, y requerirá espacio de almacenamiento, y fuente de poder adicional, y redes duplicadas.

Podría buscarse algún tipo de actividad que pueda realizar este servidor, pero que no lo inhabilite para recibir la carga del nodo primario en caso de failover. Mas no debemos usar el nodo secundario para desarrollo, pues se introducirían bugs y condiciones que provocarían falla del cluster, ~~menos~~ se deberá permitir usar como equipo de laboratorios.

Si en algún momento se considera usar el nodo secundario para tener bases de datos de pruebas (esto porque las bases de datos encapsulan todo el desarrollo), deberás considerar que la asignación de recursos de memoria o procesador no debe impedir la recepción de la carga del nodo primario, y los servicios que pongas en el nodo secundario deberán ser factibles de quitarlos tan pronto ocurra el failover

Si el factor más importante de tu negocio es realmente la disponibilidad de los servicios, entonces podrás justificar sin ningun problema que exista un nodo secundario en espera, sin realizar absolutamente ninguna aplicación, mientras menos uso distinto al cluster le des a tu nodo secundario, menos factible es tener problemas al momento de requerir sus servicios

- **Configuración simétrica,** Es muy parecido a la configuración asimétrica, la diferencia estriba en que no hay nodo primario o secundario, ambos nodos están activos y operando, cada uno ejecutando un paquete de procesos distinto, y están preparado para recibir la carga del nodo asociado en caso de fallar este

  Desde la perspectiva del costo, la configuracion simétrica es la mejor forma de proceder, se hace un mejor uso de la inversión en hardware Podremos decir que, el único costo

adicional de inversión en hardware, sería de la infraestructura de redes para heartbeat y discos replicados, ya que ambos servidores serían parte de un proyecto normal sistemas. Sin embargo, si un paquete de procesos de aplicaciones utiliza todos los recursos del nodo donde operan, o si la configuracion de servidor o sistema operativo es distinta a la requerida por el otro paquete de procesos, entonces no podremos usar la configuración simétrica

Para usar efectivamente la configuración simétrica, ambos paquetes de procesos deberán usar menos del 45% de los recursos de ambos nodos, así en el failover podrán compartir el mismo nodo, pero el performance de los procesos se vería impactado, y el usuario final sentiría su efecto, podríamos tomar dos caminos Comprar más procesador y memoria en ambos servidores, o plantearlo como una característica del cluster "Garantizaremos la continuidad de la operación, aun cuando se disminuya la velocidad de procesamiento"

En un cluster simétrico, es de gran importancia que ninguno de los servidores sea cliente

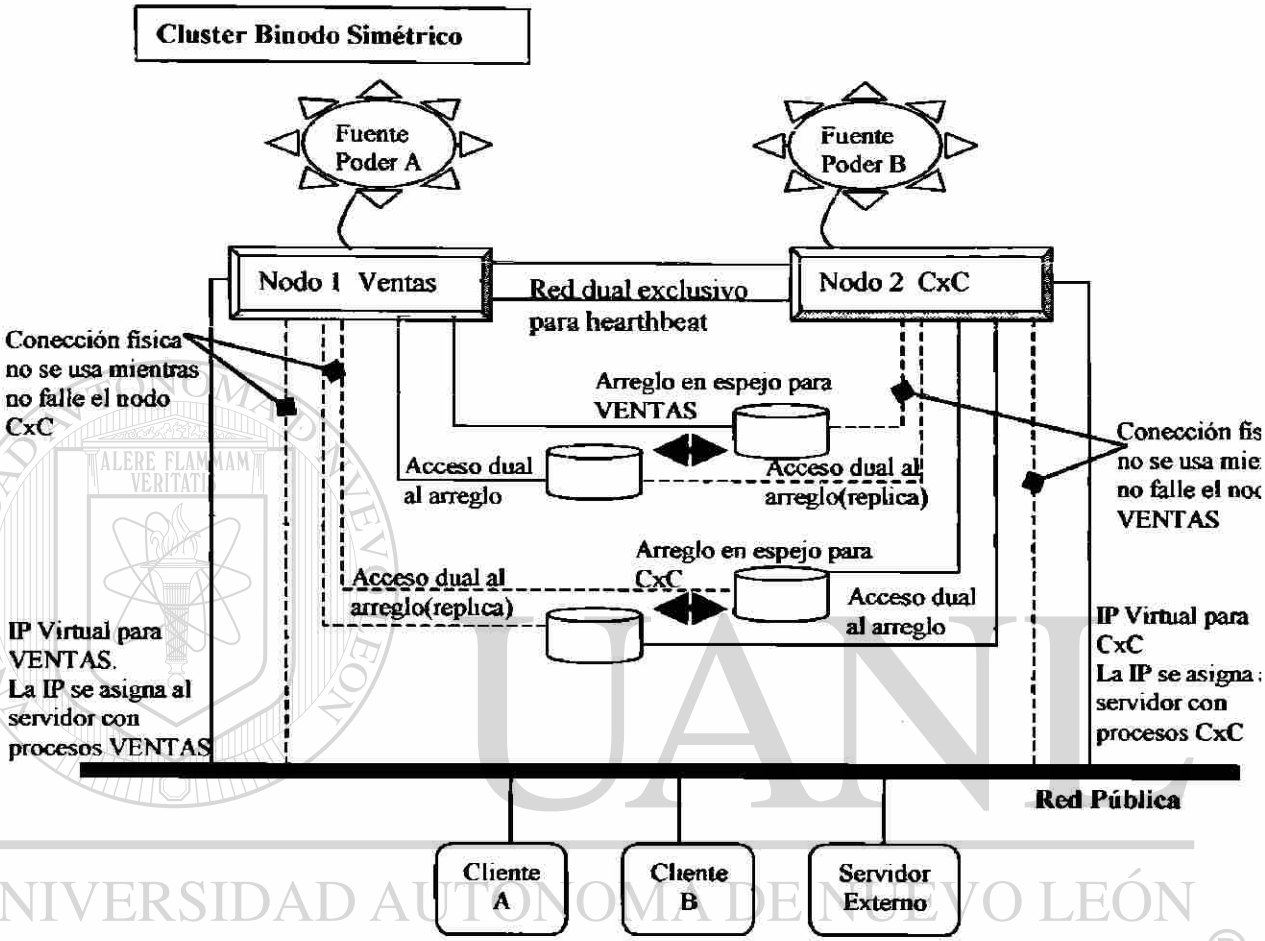


Figura 10. Cluster binodo simétrico

del otro, por ejemplo si hacemos uso de NFS, si falla el servidor propietario del FileSystem, el nodo cliente se quedará varado, pues no podrá resolver los servicios, y tampoco podrá tomar el control de los procesos del otro nodo, por intentar resolver el NFS, obteniendo así una perdida total de la disponibilidad.

Una variación de cluster binodo simétrico, es un cluster binodo multipaquetes de servicios, donde se definen grupos de servicios con su propia IP virtual y su propio juego de discos y procesos. Conforme los servidores se han vuelto más potentes y tienen mayor capacidad. Y mientras los recursos asociados a un grupo de servicios sean únicos y de

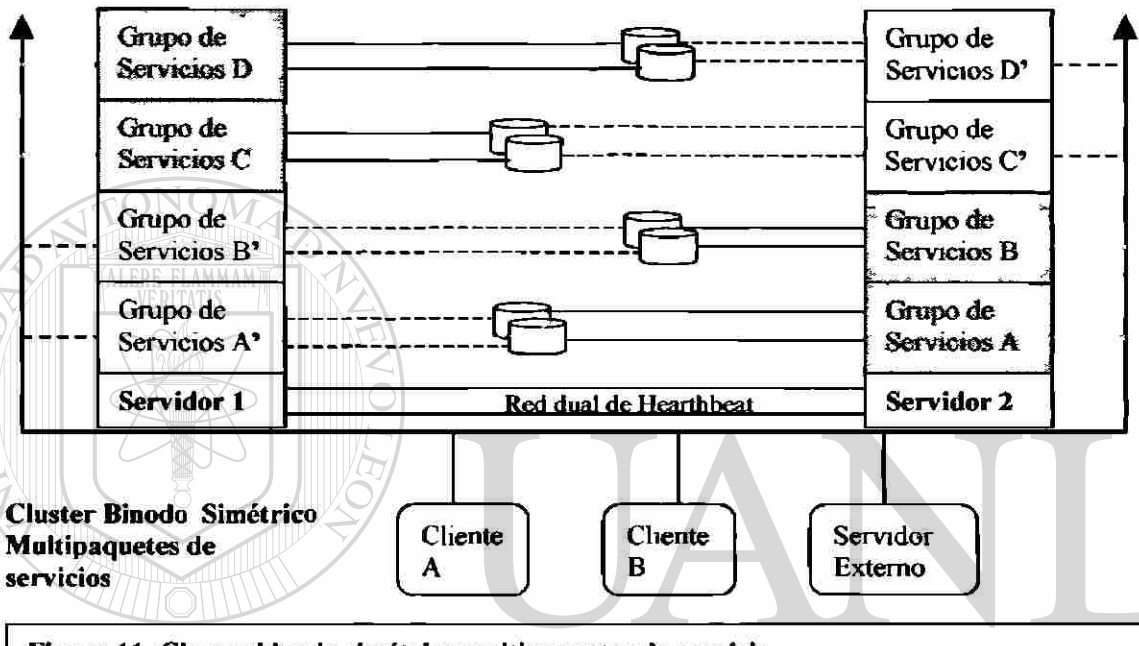


Figura 11. Cluster binodo simétrico multipaquetes de servicio

uso exclusivo para este grupo de servicios, entonces, los diversos grupos de servicios se pueden mover en forma independiente de un servidor hacia otro, sin embargo, si los procesos son dependientes entre ellos, entonces todos los recursos y procesos deben ser asociados en un solo grupo de servicios

Definitivamente, si podemos tener un cluster asimétrico, esto es mejor que uno simétrico, pero es menos costoso un cluster simétrico, y usualmente el nivel de riesgos de este es usualmente aceptable en comparación con el otro La configuración a utilizar depende de tu proyecto, y debemos considerar los pormenores, hagamos semejanzas a un seguro de vida, es bueno tenerlo y no usarlo que requerirlo y no tenerlo

Configuraciones complejas de Cluster. Existen configuraciones de cluster que por razones principalmente asociadas al costo involucran varios equipos en configuraciones complejas de

cluster, estos tipos de clusters no son muy recomendables, pues se agregan más puntos básicos de fallas y puede complicar la solución propuesta: muchas conexiones, cableados, posibles fallas, etc.

N a 1 varios equipos que tienen sus propios paquetes de servicios son configurados para hacer failover hacia un solo equipo en standby en una configuración asimétrica, o hacia un solo equipo el cual también esta efectuando alguna operación (configuración simétrica)

Networked Multihost este tipo de configuración implica que los paquetes de servicios se mueven en un orden preestablecido entre múltiples servidores, sin embargo, este tipo de configuración requerirá productos adicionales, entre ellos una SAN, que es lo que permitiría el movimiento de recursos de disco en forma transparente entre los diversos servidores Usualmente este tipo de configuraciones son más robustas que las configuraciones **N a 1** Permite mayor transparencia siempre y cuando el equipo receptor de los recursos tenga la capacidad y potencial para ofrecer los servicios.

3.5.2.7 Ejemplo de una Propuesta de Alta Disponibilidad

Todo proyecto debe ser planteado con formalidad para poder ser aceptado, e implementado con éxito, por favor refiérase a los anexos A y B para un ejemplo de un formato de propuesta de solución para un proyecto de alta disponibilidad. El Anexo B presenta un caso de una solución de bajo costo sin configuraciones especiales.

Capitulo 4 RESUMEN FINAL

De acuerdo al material presentado, podemos observar que para obtener un nivel de alta disponibilidad, el producto elegido está muy ligado al proveedor de sistema operativo, es decir, es se dificulta garantizar que se pueda configurar un cluster para alta disponibilidad cercana al servicio continuo, sin tener la capacidad que el mismo sistema operativo puede ofrecer.

Como vimos, los conceptos de alta disponibilidad son muy amplios y se puede caer en ambigüedades, por esto las soluciones de alta disponibilidad son muy variadas, de hecho, es posible, ofrecer soluciones de alta disponibilidad que no hagan uso de un software y configuración especial, al replicar los procesos en forma manual Por ejemplo

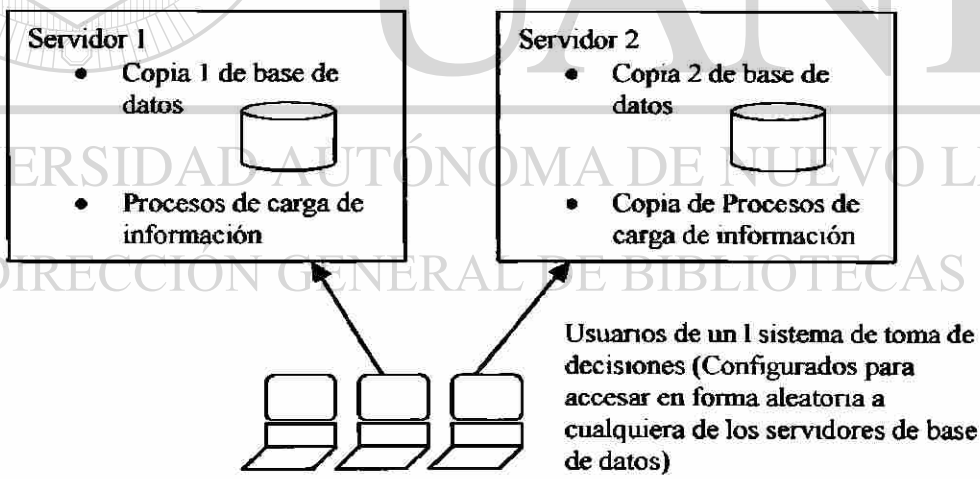


Figura 13. Ejemplo de una solución "sin costo" de alta disponibilidad

Esta solución es relativamente barata (sin costo) pues no se adquirió ningún software especial para configurarlo.

Existen otras alternativas para lograr servicios de failover, sin embargo, aquí no es tan factible el integrar funciones globales de paralelismo, y balanceo de carga automática, excepto si la aplicación misma ya lo soporta, algunos servicios como el manejador de base de datos, dependen grandemente de los servicios de sistema operativo, y hasta el día de hoy no soportan ni garantizan el paralelismo en proveedores externos al sistema operativo Más aún, aún la configuración para failover no garantiza la continuidad, pues como observamos, al efectuarse el failover, los servicios del nodo primario se interrumpen, y se mueven todos los recursos hacia el nodo secundario, donde se levantan nuevamente, lanzando un proceso de recuperación de la información (automático por la base de datos), donde el proveedor del manejador de las bases de datos indica que puede ocurrir corrupción de datos, aún cuando se intente la recuperación.

Con base en lo presentado en este material, se recomienda que el modelo de alta disponibilidad sea parte de un proyecto integral de sistemas donde se pueda plantear desde el nivel esperado de servicio, cual es el manejador de base de datos que proporcione el mayor nivel de soporte de clusters y alta disponibilidad, la plataforma tecnológica que requiere, cual es el software de cluster que el proveedor de esta plataforma ofrece, así como los costos que implicará la implementación misma de la aplicación y del servicio de cluster

En el caso de que la plataforma tecnológica de una empresa sea híbrida, la administración de los clusters (para cada proveedor) se convertiría en un elemento muy complejo tanto para administrar, configurar como para mantener Esto implicaría contar con un experto en clusters para cada plataforma

- un experto en McServiceGuard Ops Edition para HP,
- un experto en SunCluster 3.0,
- un experto en HACMP para equipos RS/6000 de IBM,

- un experto en Microsoft cluster para Sistemas operativos Windows. Etc.

En este tipo de ambientes, es necesario evaluar la conveniencia de:

- U una herramienta de alta disponibilidad de un tercero que opere en estas plataformas, aun y cuando no se ofrezca la capacidad total de paralelismo, y balanceo de cargas, pero si pueda tener servicios de failover, y automatizar los procesos de recuperación que permita que sea más transparente la operación del cluster
- Homogenizar las plataformas hacia un solo proveedor de hardware (esto podría ser costoso por aquellos productos que no se puedan transportarse o que tengan configuraciones especiales).

Toda empresa que pueda buscar la competitividad y que realmente planee su crecimiento futuro, deberá considerar dentro de su estrategia de negocio, proyectos que garanticen su continuidad Estos proyectos deberán considerar el costo por hora del recurso humano, costos fijos de servicios, y costos de recuperación de una falla (esfuerzo para restablecer los servicios, pagos por partes dañadas, etc.) Estos costos sumados a lo largo del año (o el cálculo promedio de los mismos) deberán compararse contra el costo de las alternativas de solución propuestas por los diversos proveedores.

Típicamente el costo de la solución es inferior al costo de operación pérdida, cuando esto no es así, entonces aún no es momento de buscar una solución de alta disponibilidad Esto puede deberse a varios factores:

- La solución propuesta no está bien soportada,
- El cálculo de los costos por pérdida de servicio no está incluyendo todos los factores que provocan pérdida.
- La herramienta propuesta no es la más apropiada para el nivel de disponibilidad buscado

- El sistema seleccionado no tiene un impacto directo sobre la operación, no es un sistema crítico, no es conveniente considerar este sistema en un proyecto de alta disponibilidad.

No es conveniente que el flujo de operaciones de un negocio se detenga por fallas en sus sistemas: Deben ofrecerse esquemas de Alta disponibilidad de Sistemas que permitan continuar la operación de la empresa, sin pérdida (o pérdida mínima) de la productividad. Sin embargo, esta conclusión, solo es aplicable a aquellas soluciones donde el costo de la misma sea inferior al costo anual de no tenerla. El mejor nivel de servicio se logrará al desarrollar un proyecto global de alta disponibilidad, donde se liste todo punto basico de falla y se realicen acciones para eliminarlos.

No existe un producto "out-of-the-box" en el mercado, que ofrezca la alta disponibilidad con solo instalarse en un equipo. Sin embargo, existen herramientas que en conjunto con un plan rigurosamente establecido, en el cual detalle cada posible situacion de falla, y su método de resolución. Con la partucipación de un experto integrador de soluciones puede desarrollar un proyecto de alta disponibilidad para la empresa como un paquete completo

Capitulo

5 CONCLUSIONES

La metodología de desarrollo e implementación de un proyecto de alta disponibilidad deber cumplir los siguientes puntos:

1 Identifica la necesidad del proyecto (refiérase al punto 3 5.2 1),

2 Establece los sistemas críticos de la empresa y clasificalos (ver el punto 3 2 y 3 5 2.2 para profundizar el tema),

3. Establece requerimientos mínimos del proyecto,

4. Define el alcance del proyecto (punto 3 5 2 3),

5 Prepara el documento de base del proyecto (ver el Anexo A), definiendo

a) Antecedentes (relación de oportunidades, necesidades y costos),

b) Objetivos (criterios de aceptación de proyecto),

c) Situación actual (fallas, necesidades, ventajas y desventajas)

d) Situación esperada (necesidades y expectativas, ventajas y desventajas),

e) Equipo de evaluación del proyecto (posibles candidatos que apoyarán el proyecto),

f) Descripción del proyecto,

g) Metodología del Proyecto,

h) Establece los Entregables (contra el cual se determinará el avance del proyecto)

i) Plan de implementación (involucrando actividades, fechas y responsables),

j) Requerimientos y especificaciones funcionales,

k) Diseño de la solución,

l) Desarrollo de la solución,

m) Pruebas funcionales, modulares e integrales,

n) Actividades para la Migración de datos,

o) Generación de la documentación de soporte,

p) Entrenamiento en herramientas elegidas,

q) Migración final de datos,

r) Pruebas de aceptación del usuario,

s) Arranque en producción

t) Relación de costos y beneficios esperados,

u) Resumen general del proyecto,

v) Relación de Riesgos al no realizarse el proyecto,

6 Adecua el documento para cumplir con los principios de diseño de alta disponibilidad (ver punto 3 5 1 donde se detallan estos principios)

a) Definir un presupuesto sensible y objetivo,

b) Obtener información antes de generar un compromiso,

c) Identifica los puntos básicos de falla y el método para eliminarlo,

d) Identifica los riesgos de seguridad en el acceso a la informacion,

e) Identifica las plataforma de hardware que utilizas en tu empresa y las acciones a tomar,

f) Previo a implementar un proyecto de HA, automatiza las tareas comunes,

g) Genera la documentación de soporte suficiente,

h) Negocia con el usuario final los acuerdos de nivel de servicio (SLA), enfocándote en:

i. Nivel de disponibilidad esperado,

ii. Horarios de servicio establecido,

iii. Ubicación de áreas de operación de los sistemas,

iv Niveles de prioridad entre sistemas,

v. Políticas de escalación de fallas,

a) Planea a futuro (toma este proyecto como tu base para nuevos proyectos)

b) Prueba todos las combinaciones de fallas posibles,

c) Procura no mezclar ambientes de desarrollo, pruebas y de producción para el desarrollo de una solución de alta disponibilidad,

d) Invierte en investigar como poder aislar todos los problemas,

e) Analiza los registros de fallas, esta es una fuente muy clara de posibles causas de las mismas,

f) Construye para crecer,

g) Enfocate hacia proveedores de software probado, no convertirse en ratón de laboratorio,

h) Invita sólo a los proveedores de hardware confiable y maduro,

i) Reutiliza las configuraciones hayas logrado implementar con exito,

j) Busca los servicios de un tercero con experiencia en estos proyectos,

k) Atiende un solo proyecto a la vez,

l) Busca que tu configuración sea lo más sencillo posible

7. Según el plan, invita a proveedores con experiencia en estas soluciones (ver Anexo A, Metodología de Implementación),

8. En base a la información y propuestas, fija el mejor diseño lógico del proyecto (Anexo A),

9 Selecciona al proveedor que mejor ataque el diseño lógico (Anexo A),

10 Invita a la alta dirección a conocer tu proyecto (ver punto 3 5 2 4)

11 Complementa la información sobre el proveedor final elegido y establece el equipo de trabajo definitivo, actualízalo el documento base del proyecto con las fechas finales (Anexo A),

12 Inicia el desarrollo del proyecto (en caso de ser necesario, programa una junta de Kick-Off): Una junta de Kick-Off es aquella donde se invita a los elementos clave del equipo de trabajo, y la alta dirección para hacer público el objetivo del proyecto, los alcances y fechas establecidas, buscando lograr el compromiso de los participantes en el éxito del proyecto Según el nivel de impacto que se desee lograr con el proyecto, sera la conveniencia usar esta herramienta de proyecto

13 Aplica el plan de implementación dándole seguimiento a los entregables y validando los resultados arrojados (Anexo A)

Esta metodología, es factible de sufrir cambios, reducciones o agregados, según el nivel de complejidad que se desee establecer en el proyecto de alta disponibilidad a desarrollar

6 BIBLIOGRAFÍA

"Blueprints for High Availability Designing Resilient Distributed Systems"
Evan Marcus, Hal Stern, First Edition Year 2000
John Wiley & Sons Inc

"Building the high-availability intranet. (Industry Trend or Event) "
Author/s Lynn Anderson
Computing Canada Issue Feb 23, 1998
http www findarticles com/m0CGC n7 v24 20367638 p1 article jhtml

"Linux High Availability HOWTO"
Harald Milz, hm@seneca.muc.de
Dec 22, 1998
http www ibiblio org pub Linux ALPHA linux-ha High-Ava labil ty-HOWTO html

"A Modern Taxonomy of High Availability"
Ron I Resnick , 1996
http www interlog com ~resnick ron html

"Sun™Cluster 3 Architecture A Technical Overview"
Sun Microsystems, 2000
http www sun c o n c t ters

"Hp Mc/ServiceGuard"
HP's UNIX High Availability program, 2000

http://www.hp.com.go/ha

"Hp ServiceGuard Ops Edition"
HP's UNIX High Availability program, 2000
http://www.hp.com/go/ha

"IBM's RS/6000 Cluster Technology: High Availability on a Larger Scale"
International Bussines Machines, 2001
http://www.rs6000.ibm.com/software.sp_products.pssp_pres.phoenix_main.html

"Windows 2000 Clustering Technologies Cluster Service Architecture"
Microsoft, 2001
http://www.microsoft.com.technet.treeview.default.asp?url=/TechNet/prodtechnol.windows2000serv.deploy/confeat/clustsrv.asp

ANEXO A

Se presenta un ejemplo de una propuesta de inicio de proyecto de Alta Disponibilidad, por supuesto que todo profesional tendrá sus propios lineamientos de control de proyectos, por lo que sus propuestas podrán variar y ser totalmente distintas en estilo y metodología

Proyecto: Alta Disponibilidad de Sistema de Facturación

Abstracto : *Implementar una solución que incremente el nivel de disponibilidad de los sistemas de facturación*

Confidencial : *Si*

Palabras Clave : *HA Facturación*

Comentarios : *El proyecto es de alta relevancia, requerimos garantizar la emisión de las facturas en tiempo para la entrega al cliente.*

Contenido

HISTORIA DEL DOCUMENTO

Versión	Autor(es)	Fecha	Razón del último cambio	Estatus	Aprobado por
1.0	*Administración de la Operación*	*22/10/01*	*Document Format*	*draft*	*Tecnologías de Información*

Lista de Distribución

Nombre	Departamento	Organización
	Dirección Administrativa	Materiales Industriales
	Tecnologías de Información, Director	Materiales Industriales
	Tecnologías de Información, Gerencia Operativa	Materiales Industriales
	Tecnologías de Información, Gerencia de Desarrollo	Materiales Industriales

Antecedentes

En Materiales Industriales contamos con los sistemas de compras, sistemas de pedidos, sistemas de inventarios, sistemas de facturación y sistemas de sistemas de cuentas por cobrar. En nuestra empresa se han presentado ocasionalmente fallas en la operación, donde al momento de intentar emitir la factura de las ventas realizadas, los equipos han dejado de operar, o se han presentado algunos problemas con los procesadores, o algunos recursos de memoria, este tipo de fallas no son cotidianas, sin embargo, algunas de las ocaciones que han fallado han impactado operaciones de gran cuantía, donde ha habido retraso de hasta 24 horas para concretar la operación deseada.

Debido a estrategias de nuestro negocio, es importante garantizar en primer instancia la continuidad del servicio en el sistema de facturación, y posteriormente evaluar las condiciones para implementar soluciones similares en otros sistemas.

Materiales Industriales requiere de una herramienta eficiente y flexible que le permita garantizar la continuación inmediata del servicio con los criterios establecidos para brindar nivel de alta calidad. Estos criterios son:

- Reducir o eliminar el tiempo de recuperación en caso de una falla de procesador, sim de memoria, o tarjetas de red moviendo los recursos hacia otro equipo evitando cualquier impacto a la operación.
- En caso de programar mantenimientos a los equipos, ofrecer una alternativa que permita continuar la operación, aún cuando el tiempo de mantenimiento se extienda más allá de lo planeado.
- Ofrecer un mejor nivel de desempeño de los sistemas involucrados en el proyecto.
- Evitar pérdidas por ventas no completadas en el momento requerido, que de acuerdo a un estudio realizado, el costo por hora de operación(desglosado) es de:
    - Personal inactivo en sistema (250 elementos): 328 dolares en promedio en salarios.
    - Horas extrar para recuperar los movimientos perdidos: 656 dolares en promedio
    - Costo de ventas no recuperables: 9,500 dolares en promedio.

Además, se requiere de una solución flexible que permita a Materiales Industriales adecuar la plataforma tecnológica a sus necesidades sin afectar los servicios indispensables, excepto en caso de afectar a la infraestructura física de operación. Actualmente esto no es posible debido a que cualquier cambio requerido, implica detener los servicios operacionales indispensables.

Pruebas realizadas con la infraestructura de Materiales Industriales y la experiencia con las plataformas tecnológicas permiten considerar como posible desarrollar una solución que permita cumplir con criterios de servicio y disponibilidad requeridos, que permitirá:

- Garantizar en un nivel mayor al 98% la operación del negocio, aun cuando llegará a fallar un servidor, procesador, tarjeta de red o disco.

- Programar los mantenimientos preventivos y/o correctivos sin afectar la operación del negocio al no detenerse los servicios de facturación
- Automatizar procesos de control que coordinen y para monitorear la operación, y tomando acciones correctivas en caso de falla y enviando aviso a los responsables de la operación en caso de falla mayor.

Objetivo

Este documento presenta la propuesta para el Proyecto: Alta Disponibilidad para el Sistema de Facturación, bajo los siguientes criterios de aceptación:

1. Garantizar la entrega de servicios del sistema de facturación en niveles superiores al 98%,
2. Reducir o eliminar el tiempo de recuperación en caso de falla,
3. Incrementar el tiempo entre fallas, al poder programar mantenimientos preventivos y actualización de hardware, software sin afectar a la operación.
4. Evitar pérdidas por ventas no completadas en el momento requerido.

Situación Actual

El sistema de facturación, ha presentado ocasionalmente cortes de servicio debido a fallas de CPU's, tarjetas de memoria, aun cuando este tipo de fallas no son continuas, algunas de estas fallas se han presentado en momentos en que se han estado efectuando transacciones de gran cuantía.

Las tareas de mantenimiento que se llevan acabo actualmente implican cortes de servicio en los sistemas involucrados, esto afecta que deben programarse horas extras y medios alternos para poder continuar operando aún sin el sistema operando, lo que implica costos administrativos y operativos. Por tal situación, siempre se busca reducir (sino eliminar) los cortes de servicio por mantenimientos programados, o actualización de hardware o software.

Ventajas

- El mantener la situación actual presenta la ventaja de cero inversión.
- El personal actual conoce la infraestructura y no requieren preparación adicional.

Desventajas

- El sistema no puede soportar fallas de hardware, tarjetas de red o del sistema operativo.
- Todo tipo de mantenimiento implican el corte de servicio.
- Las fallas pueden ocurrir en cualquier momento e implican largos periodos de recuperación, y puede afectar la ocurrencia de alguna transacción de importancia.
- La pérdida de servicio por hora puede alcanzar costos de $10,484 dólares la hora.

Situación Futura

Con la implementación de una solución de alta disponibilidad, podremos garantizar la continuidad de la operación, y se automatizarán el proceso de restablecimiento de la

operación, aún en caso de falla de algunos elementos de hardware, al moverse los procesos y recursos hacia otro equipo en el cual podrá continuarse la operación en el caso de un cluster, pudiendo remplazarse las partes afectadas sin efectuar cortes de servicio que detengan al negocio.

Esta solución permitirá ofrecer niveles de disponibilidad superiores al 98%. Al poder efectuar mantenimientos preventivos(mientras se mantiene la operación de los sistemas) los tiempos de recuperación por falla se reducirán acortando así los cortes de servicio. Este proyecto servirá como base para el desarrollo de proyectos similares en forma posterior.

Se establecerán acuerdos de nivel de servicio entre Tecnologías de Información y el departamento usuario, donde ambos se comprometen a cumplir lo ahí establecido tal que no se ponga en riesgo la operación.

Se establecerán claramente aquellos servicios que al tener dependencias de proveedores externos, solo podrán ofrecerse, mediante un contrato de servicios externos, los cuales se negociarán para lograr los menores tiempos de respuesta a fallas, y de soporte con los menores costos posibles.

Ventajas

- Se disminuye el tiempo de recuperación de fallas,
- Se incrementa el tiempo disponible entre cortes de servicio por fallas, al poder programar mantenimientos preventivos sin afectar los servicios del sistema, al mover los recursos hacia un nodo, mientras se da mantenimiento al otro nodo.
- Podremos identificar aquellas partes que son más susceptibles a fallas, y procurar la cantidad adecuada en spare (inventario) y no excesiva de los mismos,
- Identificar dependencias con proveedores externos tal que se establezca su factor en la valuación del nivel de servicio,
- Establecimiento de contratos de servicios externos estableciendo tiempos máximos de respuesta y de resolución de problemas para aquellos partes o servicios que por costo no podamos tener en forma local.
- La funcionalidad actual no sufre cambios, no requieres entrenamiento adicional del usuario final.
- Administración eficaz de cambios a plataformas, todo cambio estará registrado y podrá preverse el impacto a la configuración.

Desventajas

- Se hará una inversión adicional en infraestructura de hardware, redes, y discos protegidos
- Inversión adicional en software de alta disponibilidad.
- Requieres personal de Tecnologías de Información quien se especialice en clusters, o al menos entrenamiento a tu personal actual de T.I.

Equipo de evaluación

Área	Responsabilidades

Negociaciones Estratégicas	**Comercial** Servicios Profesionales Soporte y Mantenimiento Hardware **Precio**
Tecnologías de Información	**Aspecto Técnico** Infraestructura de Hardware y S.O. Software de Administración de Clusters Esquemas de Seguridad Auditoría y Registro de Actividades Tiempo de Implementación, Desarrollo y Metodología de Pruebas.
Finanzas	**Financiamiento**
Usuario	**Operación y funcionalidad** Pruebas de Funcionalidad (no afectación)

Roles y Responsabilidades

Rol	Nombre	Responsabilidades
Project Champion (Director IT/ Director Administrativo)		Presupuestos Aprobación de la propuesta
Project Prime		Administración global del proyecto
Equipo de Evaluación del Proyecto		Project Tracking Control de Cambios Situaciones administrativas
Comercial y Legal		Situaciones contractuales (en caso de existir)

Descripción del Proyecto

Este proyecto forma parte de un plan general de Sistemas en Alta Disponibilidad. Por esto se utilizará un producto comercial orientado hacia la Alta Disponibilidad que ofrezcan características estandarizadas de seguridad, estabilidad, y soporte, que nos permitan liberar la solución para el sistema de Facturación sobre una plataforma HP (HpUx), pero que nos permita contar con la posibilidad de implementar soluciones de alta disponibilidad similares en plataformas HP(HpUx), Pentium (Windows NT) e IBM (AIX). De esta manera podremos utilizar la experiencia adquirida, para planear cluster hacia los sistemas de Pedidos, CxC, etc., y contar con una fuente probada de soporte y experiencia en Alta Disponibilidad que nos garantizará la estabilidad de los mismos.

Requerimientos

Se requiere una solución tecnológica que permita lograr un nivel de servicio superior al 98%, es decir que en el transcurso del año la suma total de tiempos de corte de servicio no superen 7.3 días de operación para el Sistema de Facturación, en operación normal.

El nivel de servicio se refiere a garantizar en un 98% que la operación no se verá interrumpida debido a fallas de hardware, redes, base de datos o sistema operativo. Sin embargo, este nivel de servicio no podrá involucrar los cortes de servicio a causa de liberación de nuevas versiones del Sistema de Facturación, adecuación de los módulos del mismo o corrección de información del mismo.

La solución propuesta debe ser robusta y con suficiente estabilidad, debe existir soporte técnico local y foros de consulta con suficiente respaldo y fuentes de información que permitan resolución de problemas en forma inmediata y clara.

El producto seleccionado debe existir en versiones de Hp9000 HpUx, RS6000 Aix e intel con Windows NT/AS2000, tal que permita planear soluciones de Alta Disponibilidad para otros sistemas utilizados dentro de Materiales Industriales.

Metodología de la Implementación

Como parte del Análisis, deberán evaluarse aquellos productos de Alta Disponibilidad existentes en el mercado, que permitan ofrecer una solución directa para el sistema de facturación, sin embargo, un factor importante de esta propuesta es obtener información específica de aquellos que ofrezcan una alternativa estandarizada de solución para cada una de las plataformas donde operan los sistemas que soportan la operación de la compañía. Existen tres posibles soluciones:

- Utilizar un producto que tenga versiones para cada plataforma de sistema operativo (HPUX, AIX y Windows),
- Utilizar un producto especifico para cada plataforma.
- Rediseñar los sistemas moviéndolos hacia una plataforma única y estándar dentro de la compañía, y posteriormente elegir el producto base de alta disponibilidad para esta plataforma.

Sin embargo, es importante acentuar que la segunda y tercera alternativas no son una opción, debido a los altos costos que implican:

Alternativa 2:

- Costo mayor al adquirir los productos de vendedores diferentes,
- Costo de entrenamiento sobre productos distintos de HA, curva de aprendizaje doble,
- Personal adicional para administrar cada solución.

Alternativa 3:

- Alto costo para rediseñar todos los sistemas y moverlos hacia una plataforma única y estándar, lo cual no es el objetivo en el corto plazo.
- Esto impacta el objetivo original que es establecer una solución de alta disponibilidad para el sistema de facturación sobre la plataforma actual; si se desarrolla una solución en esta plataforma, pero posteriormente se debe migrar hacia otra distinta, es una inversión importante que se pierde.

En el diseño se deberá plantear los cambios de hardware, y software que deberán requerirse para poder soportar la alta disponibilidad. Las adecuaciones físicas al site deberán excluirse

sin embargo, deberá mencionarse el costo aproximado de las mismas, ya que al momento de aprobarse el proyecto deberá hacerse el planteamiento final de las mismas.

En la etapa de prototipo deberán establecer las adecuaciones necesarias para que la transformación sea lo más transparente posible, ya que el objetivo es no impactar al usuario final de los sistemas.

Etapa de pruebas, deberán establecer un plan de simulación de cada una de las fallas identificadas así como posibles combinaciones de las mismas y registrar el comportamiento esperado del sistema.

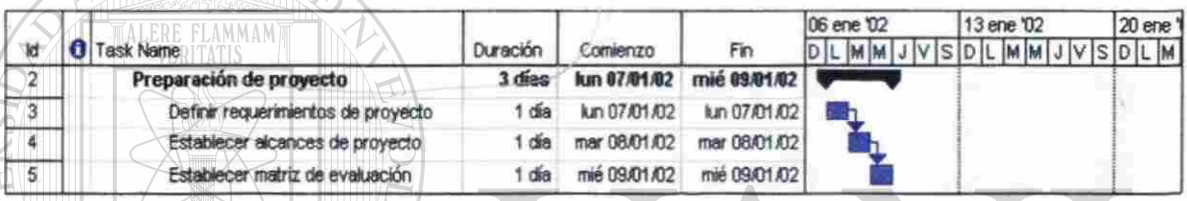
Entregables

Todos los entregables estarán sujetos a la aceptación de los usuarios. Estos entregables deberán estar claramente definidos y serán firmados una vez que lleguen a un acuerdo, y se autorice la continuación del proyecto.

Plan de Implementación

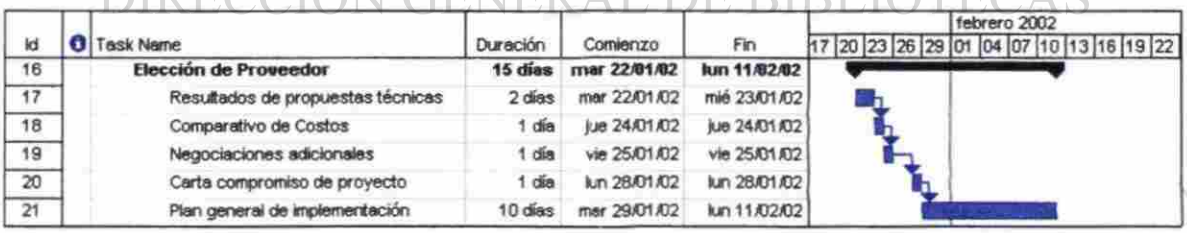
Se entregará un plan que contemplen todos los pasos, desde investigación de productos, evaluación, y desarrollo de prototipos, así como selección del proveedor y plan de configuración y pruebas funcionales. Este plan deberá presentarse en forma de gráfica de Gant; con fechas de inicio, fin y responsable claramente establecidos. Ejemplo:

Id	Task Name	Duración	Comienzo	Fin
1	**Proyecto de Alta Disponibilidad**	**98 días**	**lun 07/01/02**	**vie 10/05/02**
2	**Preparación de proyecto**	**3 días**	**lun 07/01/02**	**mié 09/01/02**
6	**Evaluación de Proveedores**	**11 días**	**lun 07/01/02**	**lun 21/01/02**
16	**Elección de Proveedor**	**15 días**	**mar 22/01/02**	**lun 11/02/02**
22	**Capacitación y Entrenamiento**	**16 días**	**mar 12/02/02**	**mar 05/03/02**
26	**Implementación de Solución**	**48 días**	**mié 06/03/02**	**vie 10/05/02**

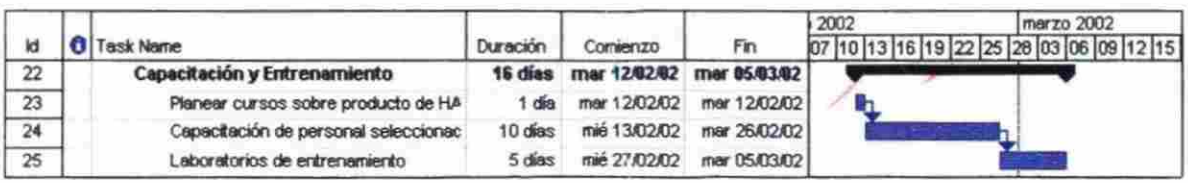


Id	Task Name	Duración	Comienzo	Fin
2	**Preparación de proyecto**	**3 días**	**lun 07/01/02**	**mié 09/01/02**
3	Definir requerimientos de proyecto	1 día	lun 07/01/02	lun 07/01/02
4	Establecer alcances de proyecto	1 día	mar 08/01/02	mar 08/01/02
5	Establecer matriz de evaluación	1 día	mié 09/01/02	mié 09/01/02

Id	Task Name	Duración	Comienzo	Fin
6	**Evaluación de Proveedores**	**11 días**	**lun 07/01/02**	**lun 21/01/02**
7	Invitar proveedores de AD	1 día	lun 07/01/02	lun 07/01/02
8	Firmar Contratos de confidencialidad	1 día	lun 07/01/02	lun 07/01/02
9	Evaluar requerimientos mínimos de so	2 días	mar 08/01/02	mié 09/01/02
10	Identif. cambios a infraestructura	3 días	jue 10/01/02	lun 14/01/02
11	Identif. cambios requeridos a aplicaci	2 días	mar 15/01/02	mié 16/01/02
12	Propuestas económicas	1 día	jue 17/01/02	jue 17/01/02
13	**Evaluar propuestas técnicas**	**2 días**	**vie 18/01/02**	**lun 21/01/02**
14	Comparativo de ventajas	1 día	vie 18/01/02	vie 18/01/02
15	Comparativo de desventajas	1 día	lun 21/01/02	lun 21/01/02

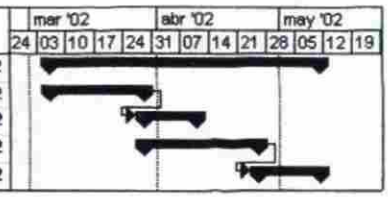


Id	Task Name	Duración	Comienzo	Fin
16	**Elección de Proveedor**	**15 días**	**mar 22/01/02**	**lun 11/02/02**
17	Resultados de propuestas técnicas	2 días	mar 22/01/02	mié 23/01/02
18	Comparativo de Costos	1 día	jue 24/01/02	jue 24/01/02
19	Negociaciones adicionales	1 día	vie 25/01/02	vie 25/01/02
20	Carta compromiso de proyecto	1 día	lun 28/01/02	lun 28/01/02
21	Plan general de implementación	10 días	mar 29/01/02	lun 11/02/02

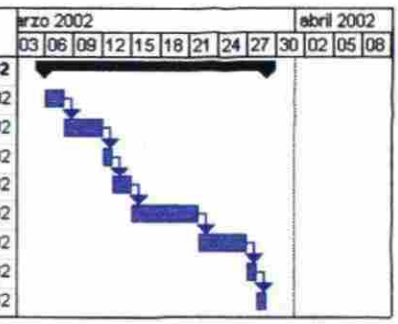


Id	Task Name	Duración	Comienzo	Fin
22	**Capacitación y Entrenamiento**	**16 días**	**mar 12/02/02**	**mar 05/03/02**
23	Planear cursos sobre producto de HA	1 día	mar 12/02/02	mar 12/02/02
24	Capacitación de personal seleccionac	10 días	mié 13/02/02	mar 26/02/02
25	Laboratorios de entrenamiento	5 días	mié 27/02/02	mar 05/03/02

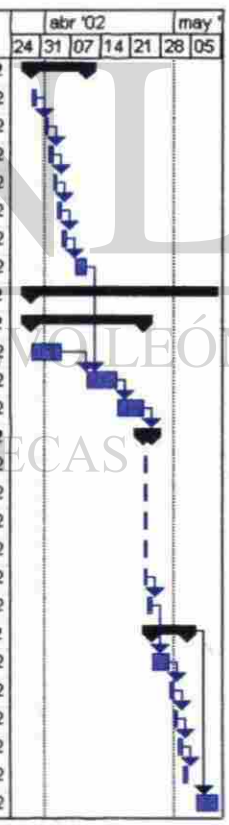
Id	Task Name	Duración	Comienzo	Fin
26	**Implementación de Solución**	**48 días**	**mié 06/03/02**	**vie 10/05/02**
27	**Diseñar modelo lógico de Alta Dis**	**17 días**	**mié 06/03/02**	**jue 28/03/02**
36	**Diseñar modelo físico de Alta Dis**	**9 días**	**vie 29/03/02**	**mié 10/04/02**
44	**Laboratorio de Alta Disponibilidad**	**20 días**	**vie 29/03/02**	**jue 25/04/02**
63	**Implementación de solución**	**11 días**	**vie 26/04/02**	**vie 10/05/02**



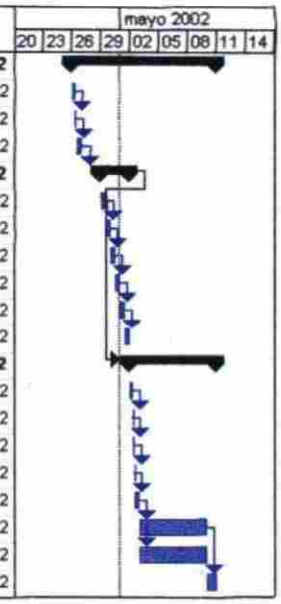
Id	Task Name	Duración	Comienzo	Fin
27	**Diseñar modelo lógico de Alta Dis**	**17 días**	**mié 06/03/02**	**jue 28/03/02**
28	Definición de procesos del sisten	2 días	mié 06/03/02	jue 07/03/02
29	Definición de monitores de proce	2 días	vie 08/03/02	lun 11/03/02
30	Definir IP's virtuales y nombres d	1 día	mar 12/03/02	mar 12/03/02
31	Definir Grupo de Servicios (proc	2 días	mié 13/03/02	jue 14/03/02
32	Identificar casos de falla(y medio	5 días	vie 15/03/02	jue 21/03/02
33	Definir reglas de recuperación(S	3 días	vie 22/03/02	mar 26/03/02
34	IP's de hearthbeat, discos base r	1 día	mié 27/03/02	mié 27/03/02
35	Modelado de solución lógica y re	1 día	jue 28/03/02	jue 28/03/02



Id	Task Name	Duración	Comienzo	Fin
36	**Diseñar modelo físico de Alta Disponibilidad**	**9 días**	**vie 29/03/02**	**mié 10/04/02**
37	Servidores requeridos (desarrollo y pruebas y producci	1 día	vie 29/03/02	vie 29/03/02
38	Infraestructura de redes internas	1 día	lun 01/04/02	lun 01/04/02
39	Arreglos de discos	1 día	mar 02/04/02	mar 02/04/02
40	Fuentes de poder (UPS)	1 día	mié 03/04/02	mié 03/04/02
41	Infraestructura de red pública	1 día	jue 04/04/02	jue 04/04/02
42	Espacio de SITES	1 día	vie 05/04/02	vie 05/04/02
43	Modelado de la solución física (distribución física)	3 días	lun 08/04/02	mié 10/04/02
44	**Laboratorio de Alta Disponibilidad**	**31 días**	**vie 29/03/02**	**vie 10/05/02**
45	**Preparar ambiente laboratorio**	**18 días**	**vie 29/03/02**	**mar 23/04/02**
46	Adquisición de equipos	5 días	vie 29/03/02	jue 04/04/02
47	Instalación de Software de Alta Disponibilidad	5 días	jue 11/04/02	mié 17/04/02
48	Instalación de software de aplicación(simular prod.)	4 días	jue 18/04/02	mar 23/04/02
49	**Configuración general**	**2 días**	**mié 24/04/02**	**jue 25/04/02**
50	Configuración de modelo de evaluación y laboratorio	1 día	mié 24/04/02	mié 24/04/02
51	Configuración de scripts de activación	1 día	mié 24/04/02	mié 24/04/02
52	Configuración de monitores de procesos	1 día	mié 24/04/02	mié 24/04/02
53	Configuración de servidores/discos e IP's para clust	1 día	mié 24/04/02	mié 24/04/02
54	Creación de paquetes de recursos	1 día	mié 24/04/02	mié 24/04/02
55	Scripts de Reglas y Triggers de producto	1 día	jue 25/04/02	jue 25/04/02
56	**Pruebas y validaciones**	**6 días**	**vie 26/04/02**	**vie 03/05/02**
57	Pruebas generales de fallas parciales	2 días	vie 26/04/02	lun 29/04/02
58	Pruebas puntuales de fallas de recursos y dispositi	1 día	mar 30/04/02	mar 30/04/02
59	Pruebas de falla general de servicios	1 día	mié 01/05/02	mié 01/05/02
60	Pruebas de failovers, y recuperación de fallas	1 día	jue 02/05/02	jue 02/05/02
61	Validación y ajustes a la configuración	1 día	vie 03/05/02	vie 03/05/02
62	Documentación de laboratorio	5 días	lun 06/05/02	vie 10/05/02



Id	Task Name	Duración	Comienzo	Fin
63	**Implementación de solución**	**11 días**	**vie 26/04/02**	**vie 10/05/02**
64	Respaldo total de la instalación	0.3 días	vie 26/04/02	vie 26/04/02
65	Configuración de hardware	0.3 días	vie 26/04/02	vie 26/04/02
66	Instalación de Software de Alta Disponibilidad	0.4 días	vie 26/04/02	vie 26/04/02
67	**Configuración de la solución**	**3 días**	**lun 29/04/02**	**mié 01/05/02**
68	Configuración de modelo de Alta Disponibilidad	0.5 días	lun 29/04/02	lun 29/04/02
69	Configuración de scripts de activación	0.5 días	lun 29/04/02	lun 29/04/02
70	Configuración de monitores de procesos	0.5 días	mar 30/04/02	mar 30/04/02
71	Configuración de servidores/discos e IP's para clust	0.5 días	mar 30/04/02	mar 30/04/02
72	Creación de paquetes de recursos	0.5 días	mié 01/05/02	mié 01/05/02
73	Scripts de Reglas y Triggers de producto	0.5 días	mié 01/05/02	mié 01/05/02
74	**Puesta en marcha**	**7 días**	**jue 02/05/02**	**vie 10/05/02**
75	Pruebas generales de fallas parciales	0.2 días	jue 02/05/02	jue 02/05/02
76	Pruebas puntuales de fallas de recursos y dispositi	0.2 días	jue 02/05/02	jue 02/05/02
77	Pruebas de falla general de servicios	0.2 días	jue 02/05/02	jue 02/05/02
78	Pruebas de failovers, y recuperación de fallas	0.2 días	jue 02/05/02	jue 02/05/02
79	Validación y ajustes a la configuración	0.2 días	jue 02/05/02	jue 02/05/02
80	Liberar instalación y estabilización de config.	5 días	vie 03/05/02	jue 09/05/02
81	Documentar infraestructura y paquetes de aplicacio	5 días	vie 03/05/02	jue 09/05/02
82	Firma de aceptación	1 día	vie 10/05/02	vie 10/05/02



Requerimientos y Especificaciones Funcionales

Definición de los alcances y limitantes del producto seleccionado:

- Identificación de los requerimientos mínimos de hardware:
  - Memoria,
  - Procesadores,
  - Discos,
  - Tipos de tarjetas de red, etc.
  - Tarjetas Fiber Optic,
  - Disk Arrays,
  - Cableado de fibra óptica, etc.
- Identificación de los requerimientos de software del producto seleccionado:
  - Sistema operativo, y parches de actualización.
  - Manejadores de bases de datos soportados.
  - Software de terceros que es requerido para operar.
  - Compiladores, bibliotecas de software.
  - Privilegios especiales y puertos de servicios requeridos.

Deberá llenarse los formatos para catalogar e identificar las Equipos, Bases de Datos, Volúmenes físicos y lógicos y como se distribuirán las aplicaciones en los equipos. Vea el Apéndice B para conocer estos formatos

Diseño

El diseño físico deberá incluir los detalles técnicos sobre los elementos físicos de la instalación, número de tarjetas, redes privadas de hearthbeat, discos protegidos, fuentes de poder (UPS's), servidores adicionales, cableado de cobre, fibra óptica, modificaciones al site, etc. Adicionalmente, deberá formar parte del diseño lógico, la identificación de procesos y grupos de proceso, paquetes de servicio, uso de las IP's para hearthbeat, monitores, tiempo de recuperación, tiempos para detección de la falla, procedimientos de recuperación, métodos de asignación de recursos, reglas de movimiento de paquetes entre servidores, etc.

Como parte de este diseño, y en base al producto seleccionado, deberá indicarse el tipo de Solución (Cluster binodo/multinodo, simétrico ó asimétrico), y plantearse las prioridades de los paquetes de procesos, identificando aquellos paquetes procesos que tienen la mayor prioridad y aquellos paquetes de procesos que pueden delegarse a un uso de recursos más restringido.

Desarrollo

En base al producto seleccionado, y en base a los paquetes de procesos identificados, deberán identificarse los scripts de monitoreo que permitirán detectar las fallas de un proceso o paquete de procesos. Asimismo como parte del proyecto, deberán establecerse las reglas de monitoreo, activación y de validación del Cluster. Cada una de estas reglas y scripts deberán estar identificados plenamente: su objetivo, lenguaje, temporización, propietario, etcétera. Por ejemplo:

- Regla de operación:
  - Existirán 2 paquetes de procesos, el paquete "Motor de la Base" y el paquete "Procesos de Aplicación", estos paquetes deberán operar como sigue.

- Al activarse el "Motor de la Base" se deberán montar los filesystems que componen la base de datos y el engine del manejador, adicionalmente se deberán activar el RDBMS y levantar la instancia de la base de datos.
- El paquete "Procesos de Aplicación" sólo podrá activarse si ya esta activo el paquete "Motor de la Base",
- El paquete "Procesos de Aplicación", deberá montar los filesystems que componen la aplicación y directorios de procesamiento temporal, así como se deberán ejecutar los programas de calculo de facturas los cuales están esperando nuevos registros para procesarlos,
- Preferentemente, el "Motor de la Base" deberá levantarse en el Nodo A, y el paquete "Procesos de Aplicación" deberá levantarse en el Nodo B, en caso que el nodo asignado previamente no pueda ser utilizado, deberán migrarse los servicios al nodo opuesto.
- Si el "Motor de la Base" sufre alguna falla y se desactiva a causa de esto, el paquete "Procesos de Aplicación" deberá desactivarse, y no se podrá reactivar hasta que el paquete "Motor de la Base" haya sido reactivado exitosamente en alguno de los nodos.

- Reglas de monitoreo:
  - En una operación normal, la base de datos se instanciará mediante el RDBMS (Oracle en este caso) y deberá abrirse al servicio al usuario final, para hacer esto el Producto de alta disponibilidad, deberá ofrecer la capacidad de llamar al sistema operativo y lanzar comandos con la cuenta propietaria del manejador, y con las cuentas propietarias de los módulos de aplicación, he aquí un ejemplo:
    - Levantar la BASE DE DATOS

```
####  SCRIPT /app/RDBMSCLUSTER startora.sh
if [ ! -f "/app/oracle/product" ] ; then
  # Debo verificar que esta montado filesystem del manejador
  echo "Filesystem de manejador ¡¡¡no esta montado!!!"
  exit
fi
if   ! -f "/dbs/FACTURAS/CONTROL" ] ; then
  # Debo verificar que esta montado filesystem de la base de datos
  echo "Filesystem de bases de datos ¡¡¡n  esta montado!!!"
  exit
fi
### CONFIGURAR VARIABLES DE AMBIENTE
.  app oracle product/SET ENVIRONMENT
ORACLE SID=FACTURAS
### LEVANTAR LA BASE DE DATOS  INSTANCIA)
svrmgrl <<!
connect internal
startup pfile=" app/oracle/admin/FACTURAS/pfile/init.ora"
exit
!
```

  - El producto de Alta disponibilidad debe ofrecer métodos para montar los filesystems, y monitorear que los mismos no se desactiven el acceso a los mismos.
  - Deberá ofrecer un medio para asignar la IP virtual al nodo que proporcionará el servicio, así como un método para migrar la misma de un nodo hacia otro (junto con los paquetes de servicios), y garantizar que la IP sigue respondiendo.
  - Este producto debe soportar monitoreo específico de las tarjetas de la red de hearthbeat, tal que se pueda detectar a tiempo la falla del nodo primario o espejo.

El formato para describir estas reglas y scripts deberá seguir un estándar que se utilizará para este y nuevos proyectos dentro de la compañía, el estándar se menciona en el anexo A:

Pruebas

Será necesario identificar y establecer los juegos de pruebas que habrán de realizarse para garantizar la operabilidad de la solución, estas podrían clasificarse como:

- Pruebas generales de fallas parciales
- Pruebas puntuales de fallas de recursos y dispositivos
- Pruebas de falla general de servicios
- "Pruebas de failovers, y recuperación de fallas"
- Validación y ajustes a la configuración

Este juego base de posibles pruebas deberán detallarse como parte del proyecto final y documentarse ampliamente tal que puedan usarse como soporte para futuras implementaciones.

Los escenarios posibles deberán establecerse claramente en conjunto entre los elementos que formen el equipo del proyecto. Deberá generarse un check list de evaluación de cada tipo de escenarios y documentar el comportamiento del sistema bajo estas pruebas.

Migración de Datos

No es requerido, pues la solución no afecta la funcionalidad de la aplicación.

Documentación

La documentación a entregar se compone de:

- Manuales técnicos y de usuario del producto de alta disponibilidad
- Documentación del modelo físico de la instalación, mencionando las adecuaciones y cambios realizados a las instalaciones, así equipo que forma parte del proyecto.
- Documentación del modelo lógico de la configuración, proceso, grupos de recursos, recursos disponibles, uso de IP's, bases de datos y sistemas operativos involucrados.
- Manual que documenta todas las reglas y procedimientos que regirán el comportamiento de la configuración, casos de falla identificados y el medio de solución que ofrecerá el producto.
- Manual de estándares que se usaron, y que determinarán el diseño e implementación para futuras instalaciones en Alta Disponibilidad.

Entrenamiento

No hay requerimiento de entrenamiento al usuario final, pues la aplicación no sufre cambios funcionales, por lo que los conocimientos operacionales actuales de la aplicación son suficientes y no requieres preparación adicional.

Migración final de datos

No es requerido, pues la aplicación no sufre cambios, y por lo tanto la información no deberá ser adecuada como parte de este proyecto. Sin embargo, deberá ser aclarado mediante una notificación al usuario final.

Pruebas de aceptación de usuarios

El usuario deberá ser invitado a validar la funcionalidad (que nunca debe ser afectada) de todo el sistema, una vez que se han configurado los paquetes de procesos y activado los servicios de Alta Disponibilidad. El usuario utilizará el sistema, como normalmente lo hace, y hará las observaciones sobre comportamiento anómalo, debiendo ajustarse todo aquello que afecte al proceso. Una vez que se hayan adecuado todos aquellas situaciones identificadas, el usuario deberá firmar un acuerdo donde se establece que la funcionalidad no esta sufriendo ninguna afectación y que por lo mismo la implementación del cluster no afecta en fallas funcionales (usualmente asociadas al uso o alimentación de informacion incompleta o incorrecta), excepto aquellas situaciones donde el sistema ha dejado de operar debido a que el paquete de procesos ha sido cancelado, suspendido, o retardado, como parte de una labor de mantenimiento previamente negociada.

Arranque en Producción

La fecha de arranque deberá ser establecida en base a los requerimientos definidos en esta propuesta, y los tiempos de configuración, desarrollo, pruebas, y fechas negociables con el area usuaria del sistema.

Costos y Beneficios

Actualmente, los cortes de servicio que se han observado dentro de el sistema, considerando el tiempo de recuperación del mismo, ha sido de 5 horas en promedio (tiempo para obtener la pieza faltante, y lanzar la recuperación del sistema), tomando el costo aproximado de $10,484dolares la hora, la pérdida de servicio por cinco horas representa un monto de $52,420 dólares. El nivel de disponibilidad actual es de aproximadamente 95% (sin cambios a la infraestructura), esto significa que al año los cortes de servicio significan hasta 18 dias de operación, el proyecto debe garantizar un nivel de disponibilidad de al menos un 98%, lo cual representa una diferencia de 3 puntos y 10.95 días con un costo que puede representar $2,755,195.20 dólares.

El producto seleccionado y la implementación de la instalación deberá tener un costo máximo no mayor a 3 días de operación, lo cual representa aproximadamente $754,848 dólares.

Costo de Corte de servicio por hora	Disp. 95%	Disp. 98%
1,000	18 días x 24 horas x 1000 = $432,000 anual	10.95 días x 24 horas x 1000 =$262,800 anual
10,484	18 días x 24 horas x 10,484 $4,529,088 anual	10 95 dias x 24 horas x 10,484 =$2,755,195.20 anual

Costos

El producto seleccionado y la implementación de la instalación no podrá tener un costo maximo equivalente a 3 días de operación, lo cual representa un monto de $754,848 dólares. La espectativa del proyecto es lograr subir el nivel de disponibilidad del 95% actual hacia un 98% o superior, es decir una diferencia de 3 puntos porcentuales.

El tiempo de recuperación esperado es de aproximadamente 4 meses, por lo siguiente:
Días del año: 365, nivel de disponibilidad actual = 95% que significa 18.25 días sin operación,
El nuevo nivel de disponibilidad esperado es 98% lo cual es 7.3 días sin operación por cortes de servicio, la diferencia es de 10.95 días adicionales con servicio en el año.

Actualmente en un periodo de 6 meses (6*30.5=182.5 días), con una disponibilidad del 95%: donde (100% - 95%)de 182.5 significa 9.125 días con fallas. Al mejorar la disponibilidad se espera lograr 5.475 días adicionales de operación sin fallas, es decir, en 6 meses ocurrirán solo 3.65 dias de fallas.

En base a este mismo formulamiento, Actualmente en un periodo de 4 meses (3*30.5= 122 días), y la disponibilidad del 95%: (100% - 95%) x 122 – 6.1 días con fallas. Al subir la disponibilidad a un 98% tendremos sólo 2.44 días (2%) con fallas, es decir 3.66 días adicionales de operación sin fallas.

Observando el proyecto: Al invertir 3 días de operación equivalente a $754,848 dólares en un proyecto de alta disponibilidad, logramos en cuatro meses reducir los cortes de servicio en 3.66 días equivalente a $920,914.56 dólares con una ganancia directa de 0.66 días equivalente a $166,066.56dolares.

Beneficios

- Se logrará mejorar el nivel de disponibilidad del sistema de facturación garantizando hasta un 98% de días de operación del año.
- Podrán programarse mantenimiento en los equipos relocalizando los recursos hacia otro servidor logrando de esta forma continuar ofreciendo los servicios del sistema donde mantenimientos preventivos, actualizaciones de hardware o software.
- Al lograr reducir los días de corte de servicio en aproximadamente 10.95 días al año, se podrán ofrecer y consumar mayor nivel de operaciones con un nivel de ingresos que puede representar hasta 9,500 dólares x hora con un monto de hasta $2,496,600 anuales por concepto de transacciones completadas.
- Se obtiene una plataforma base para implementar soluciones de alta disponibilidad en otros sistemas dentro de la compañia.

Resumen

La necesidad de implementar una solución de Alta Disponibilidad es urgente, el hecho de no planear y ofrecer esta alternativa significa que la compañia se encontrara en desventaja frente a competidores que podrán completar las ventas en el tiempo que no podremos operar por los cortes de servicio que ocurrieran, adicionalmente, nuestros clientes podrán optar por no regresar a nuestra empresa debido a la insatisfacción generada por los servicios ofrecidos

El monto de la inversión no es mayor a la 3 parte de lo que se pierde anualmente en cortes de servicio no programados. Se ofrece una plataforma estable 7x24 con niveles de disponibilidad del 98% y posibilidad de ofrecer una operacion continua en momentos que se realizan mantenimientos preventivos o de actualizacion sin afectar la operacion

Se contaría con una plataforma que ofrecería posibilidades de crecer la capacidad sin detener la operación (escalabilidad), al mover los recursos a un nodo mientras se "crece" o remplaza el otro

Se establecerá un procedimiento estándar para la implementación de soluciones de Alta Disponibilidad, que podremos utilizar para proyectos posteriores

Riesgos

En caso de no aprobarse este proyecto, los riesgos directos son:

- Las probabilidades de una falla en un momento de operación altamente transaccional,
- El tiempo de recuperación que consumiría,
- Las ventas no completadas que podrían correr el riesgo de no recuperarse.
- Una falla puede extenderse más allá de lo usual, por no tener piezas de recambio disponibles,
- Dependiendo de los tipos de contrato de soporte, existe una dependencia directa del proveedor, si existiese el cluster, la operación podría migrarse al otro nodo y continuarse mientras se dan servicios al nodo fallado.
- Las pérdidas por corte de servicio pueden ser superiores a $2,496,600 dólares anuales por concepto de transacciones no completadas.
- El costo por pérdida de imagen ante mis clientes directos.

Aprobación

Este documento, y los resultados de la evaluación, y negociaciones efectuadas, así como la carta compromiso del proveedor y el plan de implementación del proyecto, deberán de anexarse como información de soporte para que una vez presentado ante la alta dirección, se emita la autorización firmada para el desarrollo total del proyecto.

Se deberá firmar la autorización del proyecto y el presupuesto asociado al mismo, definiendo las fechas y los entregables que deberán ofrecerse para medir el avance del mismo.

Un taller de trabajo será llevado a cabo con los usuarios de cada área involucrada para la demostración del cumplimiento de la funcionalidad.

Soluciones de Negocio		Firma
Tecnologías de Información, Director		
Tecnologías de Información, Gerencia		
Tecnologías de Información, Gerencia de		
Director Administrativo		
Director General de Materiales Industriales		

Aprobación de los usuarios

Este tipo de proyectos, requiere una aprobación por parte de los usuarios en el sentido de que ellos aceptan la implementación de la herramienta, si esta garantiza que la operación podrá continuar sin efectos directos a la metodología de trabajo de los mismos, y sin afectar la especificación funcional del Sistema de Facturación. Sin embargo, no se requiere aprobación adicional del usuario, por ser un proyecto puramente interno al área de Tecnologías de Información. La aprobación deberá ser lograda por el Directorio de Tecnologías de Información y apoyada por el Director General de Materiales Industriales.

Usuario	Área	Firma
	Facturación	
	Administración	
	Embarques	

Apéndice A

Deberá anexarse el material de referencia acerca de los productos evaluados, así también referencias a las empresas donde está operando esta solucion. En caso de haber visitado los sitios de estas empresas, documentar la información recabada sobre el comportamiento de estos productos en las mismas. Los beneficios que se hayan obtenido directa e indirectamente por estas empresas.

Proveedores evaluados

Proveedor	
Herramienta Ofrecida	
Beneficios	
Desventajas	
Requerimientos mínimos	

Instalaciones Exitosas Visitadas

Fecha de Visita	
Empresa	
Director de Sistemas	
Contacto	
Producto implementado	
Tiempos de implementación	
Requerimientos mínimos	
Documentos de referencia	
Beneficios logrados	
Desventajas surgidas	

Apéndice B.

1. Identificación del cluster

Configuración del Cluster

Nombre del Cluster	HAFACT
Sistema operativo	HP/UX 11i
Base de Datos	Oracle 8i

Tiempos de control del cluster(microsegundos)

Intervalo del Heartbeat	5000000
Timeout del nodo	20,000,000
Tiempo de reactivación	600,000,000
Poleo de la red	2,000,000

Nodo primario

Nombre del nodo:	ASFABD
Numero de serie del equipo	
Equipo	HP9000 K360
Procesadores	PAx000
Memoria	2GB

Configuración de red:

Dirección IP	Subred	Gateway	Mascara de Red	Tarjeta interfase	Tipo de Tráfico
128.16.1.15	128.16.0.0	128.10.1.1	255.255.0.0	lan0	Usuarios
	0.0.0.0	128.10.1.1	255.255.0.0	lan5	Usuarios/Standby
128.17.1.15	128 17.0.0	128.10.1.1	255.255.0.0	lan4	Heartbeat
	0.0.0.0	128.10.1.1	255.255.0.0	lan2	Heartbeat/Standby
128.18.1.15	128.18.0.0	128.10.1.1	255.255.0.0	lan1	Heartbeat/datos
	0.0.0.0	128.10.1.1	255.255.0.0	lan3	Heartbeat/ datos/Standby

Nodo secundario:

Nombre del nodo:	HAFABD
Numero de serie del equipo	
Equipo	HP9000 K360
Procesadores	PAx000
Memoria	2GB

Configuración de red:

Direccion IP	Subred	Gateway	Mascara de Red	Tarjeta interfase	Tipo de Tráfico
128 16.1.15	128 16 0.0	128 10 1 1	255 255.0.0	lan0	Usuarios
	0.0.0.0	128.10.1.1	255.255 0.0	lan5	Usuarios/Standby
128.17.1.15	128.17.0.0	128.10.1.1	255.255.0.0	lan4	Heartbeat
	0 0 0.0	128.10.1.1	255.255.0 0	lan2	Heartbeat/Standby
128.18 1.15	128.18.0.0	128.10.1.1	255.255 0 0	lan1	Heartbeat/datos
	0.0.0.0	128.10.1.1	255.255.0.0	lan3	Heartbeat/ datos/Standby

Paquetes de Aplicación

Nombre de la aplicación:	GENFACT
Cuenta de instalación	ADMFACT
Nodo inicial de activación	HAFABD
Script de configuración del medio ambiente	$RAIZ_FACT Config_Fact.sh
Procedimiento para levantar el proceso	$RAIZ_FACT/Inicia_Fact.sh
Procedimiento para detener el proceso	$RAIZ_FACT/Termina_Fact.sh
Directorio de trabajo	app facturación/archivos_proceso

Sistema de archivos

Identificador de recurso	Grupo de volumen	volumen lógico	Punto de montaje	opciones de montaje
0.1.1	/dev/vg01	/dev/lv01	/app/facturacion/binarios	
0.1.2	/dev/vg01	/dev/lv02	/app/facturación/archivos_proceso	

Scripts de monitoreo y validación

Servicio	Procesos a verificar	Reintentos	Tiempo de reintento	Tiempo de detección de falla	Tiempo de terminación de proceso

Paquete de aplicación

Nombre de la aplicación:	BDFACT
Cuenta de instalación	ORACLE
Nodo inicial de activación	ASFABD
Script de configuración del medio ambiente	$RAIZ_BD/Config_Amb.sh
Procedimiento para levantar el proceso	$RAIZ_BD/Inicia_BD.sh
Procedimiento para detener el proceso	$RAIZ_BD/Termina_BD.sh
Directorio de trabajo	/app/oracle/

Sistema de archivos

Identificador de recurso	Grupo de volumen	volumen lógico	Punto de montaje	opciones de montaje
0.1.3	dev/vg03	dev/lv03	/app/oracle/product	
0.1.4	dev/vg03	/dev/lv04	dbs/BDFACT/DATOS	
0.1.5	dev/vg03	dev/lv05	/dbs/BDFACT/INDICES	
0.1.6	dev/vg03	dev/lv06	dbs/BDFACT CONTROL	

Scripts de monitoreo y validación

Servicio	Procesos a verificar	Reintentos	Tiempo de reintento	Tiempo de detección de falla	Tiempo para terminar proceso

ANEXO B

Se presenta un ejemplo de una propuesta alterna de inicio de proyecto de Alta Disponibilidad, para un proyecto con bajo presupuesto

Proyecto:
Implementación de Alta Disponibilidad para el Sistema de Apoyo a la Toma de Decisiones

Abstracto : *Implementar una solución que incremente el nivel de disponibilidad del sistema de apoyo a la toma de decisiones*

Confidencial : *Sí*

Palabras Clave : *HA DSS*

Comentarios : *El proyecto es de alta relevancia, requerimos garantizar el acceso a la información crítica de apoyo a la toma de decisiones para incrementar la competitividad de la empresa en su ramo.*

Contenido

Historia del Documento

Versión	Autor(es)	Fecha	Razón del último cambio	Estatus	Aprobado por
1.0	*Administración de la Operación*	*22 10 01*	*Document Format*	*draft*	*Tecnologías de Información*

Lista de Distribución

Nombre	Departamento	Organización
	Dirección Administrativa	"Empresa Comercial"
	Tecnologías de Información, Director	"Empresa Comercial"
	Tecnologías de Información, Gerencia Operativa	"Empresa Comercial"
	Tecnologías de Información, Gerencia de Desarrollo	"Empresa Comercial"

Antecedentes

En "Empresa Comercial" existe un sistema de apoyo a la toma de decisiones, el cual se basa en un servidor central de bases de datos y un cliente aplicativo instalado en el equipo del usuario final. En nuestra empresa se han presentado ocasionalmente fallas en la disponibilidad de los servicios de base de datos, lo cual ha provocado un impacto notorio hacia la alta dirección lo que ha generado una pérdida de la imagen de calidad que ofrece el departamento de Tecnologías de Información, debido a la crisis económica presente no es posible asignar un presupuesto elevado a la búsqueda de una solución de alta disponibilidad..

"Empresa Comercial" requiere de una solución de alta disponibilidad al menor costo posible, pero que permita recuperar el nivel de servicio esperado por la alta dirección en el acceso a la información de toma de decisiones. Este proyecto debe:

- Reducir o eliminar el tiempo de recuperación en caso de una falla de procesador, sim de memoria, o tarjetas de red moviendo los recursos hacia otro equipo evitando cualquier impacto a la operación.
- En caso de programar mantenimientos a los equipos, ofrecer una alternativa que permita continuar la operación, aún cuando el tiempo de mantenimiento se extienda más allá de lo planeado.
- Ofrecer un mejor nivel de desempeño de los sistemas involucrados en el proyecto.
- El costo de los altos ejecutivos es oneroso, por lo que deberá ofrecerse un servicio accesible en cualquier momento dentro del horario de labores de los mismos.

Además, se requiere que esta solución sea flexible y que permita a "Empresa Comercial" adecuar la plataforma tecnológica a sus necesidades sin afectar los servicios indispensables, excepto en caso de afectar a la infraestructura física de operación. Actualmente esto no es posible debido a que cualquier cambio requerido, implica detener los servicios operacionales indispensables.

Pruebas realizadas con la infraestructura de "Empresa Comercial" y la experiencia con las plataformas tecnológicas permiten considerar como posible desarrollar una solución que permita cumplir con criterios de servicio y disponibilidad requeridos, que permitirá:

- Garantizar en un nivel mayor al 98% la operación del negocio, aun cuando llegará a fallar un servidor, procesador, tarjeta de red o disco.
- Programar los mantenimientos preventivos y/o correctivos sin afectar la operación del negocio al no detenerse los servicios de facturacion

Objetivo

Este documento presenta la propuesta para el Proyecto Alta Disponibilidad para el Sistema de Apoyo a la Toma de Decisiones, bajo los siguientes criterios de aceptacion

1. Garantizar la entrega de servicios del sistema en niveles superiores al 98%,
2. Reducir o eliminar el tiempo de recuperación en caso de falla,
3. Incrementar el tiempo entre fallas, al poder programar mantenimientos preventivos y actualización de hardware, software sin afectar a la operación
4. Evitar pérdidas en la toma de decisiones orientadas a mejorar la competividad de la empresa.

Situación Actual

El Sistema de Apoyo a la Toma de Decisiones, ha presentado ocasionalmente cortes de servicio debido a fallas de CPU's y Discos dañados, aun cuando este tipo de fallas no son continuas, algunas de estas fallas se han presentado en momentos en que la alta dirección requiere el servicio en carácter de preponderante.

Como este sistema solo opera en horario de oficina, las tareas de mantenimiento se pueden realizar fuera de horario, sin implicar un cortes de servicio. Sin embargo, en el caso de una falla se ve afectada su uso total.

Ventajas

- El mantener la situación actual presenta la ventaja de cero inversión.
- El personal actual conoce la infraestructura y no requieren preparación adicional.

Desventajas

- El sistema no puede soportar fallas de hardware: disco, CPU's, o tarjetas de red o del sistema operativo.
- Las fallas pueden ocurrir en cualquier momento e implican largos periodos de recuperación, y puede afectar la ocurrencia de alguna transacción de importancia.

Situación Futura

Con la implementación de una solución de alta disponibilidad, podremos ofrecer un servicio casi continuo del sistema hasta un 98% de disponibilidad.

Se establecerán acuerdos de nivel de servicio entre Tecnologías de Información y el departamento usuario, donde ambos se comprometen a cumplir lo ahí establecido tal que no se ponga en riesgo la operación.

Se establecerán claramente aquellos servicios que al tener dependencias de proveedores externos, solo podrán ofrecerse, mediante un contrato de servicios externos, los cuales se negociarán para lograr los menores tiempos de respuesta a fallas, y de soporte con los menores costos posibles.

Se ha detectado la posibilidad, debido al tipo de sistema involucrado, de replicar la base de datos hacia un equipo semejante al actual, así como replicar los procesos de carga para que actualicen esta base de datos de replica. La observación de la tecnología disponible permite

configurar un medio de conectividad automático aleatorio para el acceso al servicio de base de datos (y secuencial en caso de fallar el acceso a la primer base de datos localizada)

Ventajas

- Se disminuye el tiempo de recuperación de fallas, al existir dos bases de datos replicas ofreciendo estos servicios,
- Se incrementa el tiempo disponible entre cortes de servicio por fallas, al poder programar mantenimientos preventivos sin afectar los servicios del sistema, al dar de baja una base de datos para mantenimiento, la "otra" podrá seguir respondiendo a las peticiones.
- No se requiere de un software o hardware especial de alta disponibilidad,
- La funcionalidad actual no sufre cambios, no requieres entrenamiento adicional del usuario final.
- Administración eficaz de cambios a plataformas, todo cambio estará registrado y podrá preverse el impacto a la configuración.

Desventajas

- Se hará una inversión adicional en infraestructura de hardware, y discos protegidos
- Esta solución requiere el doble de hardware, y Storage para ofrecer este servicio.
- Requieres configurar las réplicas de procesos de carga para garantizar que estos esten ocurriendo como se espera, en caso de modificar o agregar un proceso de carga, será necesario hacer la adecuación en el equipo réplica del proceso. El personal de Tecnologías de Información deberá tener especial consideración por esta configuración.

Equipo de evaluación

Área	Responsabilidades
Tecnologías de Información	**Aspecto Técnico** Infraestructura de Hardware y S.O. Software de Administración de Clusters Esquemas de Seguridad Auditoría y Registro de Actividades Tiempo de Implementación, Desarrollo y Metodología de Pruebas.
Finanzas	**Financiamiento en la adquisición del hardware adicional**
Usuario	**Operación y funcionalidad** Pruebas de Funcionalidad (no afectación)

Roles y Responsabilidades

Rol	Nombre	Responsabilidades
Project Champion (Director IT/ Director Administrativo)		Presupuestos Aprobación de la propuesta

Project Prime	Administración global del proyecto
Equipo de Evaluación del Proyecto	Project Tracking Control de Cambios Situaciones administrativas
Comercial y Legal	Situaciones contractuales (en caso de existir)

Descripción del Proyecto

Este proyecto forma parte de un plan alterno de Sistemas en Alta Disponibilidad.

Requerimientos

Se requiere una solución tecnológica que permita lograr un nivel de servicio superior al 98%, es decir que en el transcurso del año la suma total de tiempos de corte de servicio no superen 7.3 días de operación para el Sistema de Apoyo a la Toma de Decisiones, en una operación normal.

El nivel de servicio se refiere a garantizar en un 98% que la operacion no se verá interrumpida debido a fallas de hardware, redes, disco, base de datos o sistema operativo. Sin embargo, este nivel de servicio no podrá involucrar los cortes de servicio a causa de liberación de nuevas versiones del Aplicativo del Sistema (el cual va instalado en el cliente), adecuación de los módulos del mismo o corrección de información del mismo.

La solución propuesta debe ser robusta y con suficiente estabilidad, debe existir soporte técnico local y foros de consulta con suficiente respaldo y fuentes de información que permitan resolución de problemas en forma inmediata y clara.

Metodología de la Implementación

Como parte del Análisis, deberan evaluarse si existen productos de Alta Disponibilidad en el mercado, los cuales permitan ofrecer una solución directa y con el menor requerimiento de costo para el sistema y permitiendo una escalabilidad mayor, sin embargo, un factor importante de la propuesta es que debe permitir, a un bajo costo, la administración de la configuracion con el menor riesgo para la operación del sistema. Hasta el momento s ha identificado una posibilidad mediante la replicación de la base de datos y procesos de carga. Ubiquemos estas posibles soluciones

- Utilizar un producto de alta disponibilidad que ofrezca servicios de cluster paralelizados "a un bajo costo" y de fácil administración.
- Crear una replica del servidor de base de datos y configurar los procesos para que actualicen ambas bases de datos.

Sin embargo, es importante acentuar que la primera requiere de un producto altamente robusto, lo cual en el mercado actual tiene altos costos:

En el diseño se deberá plantear los cambios de hardware, y software que deberán requerirse para poder soportar la alta disponibilidad.

En la etapa de prototipo deberán establecer las adecuaciones necesarias para que la transformación sea lo más transparente posible, ya que el objetivo es no impactar al usuario final de los sistemas.

Etapa de pruebas, deberán establecer un plan de simulación de cada una de las fallas identificadas así como posibles combinaciones de las mismas y registrar el comportamiento esperado del sistema.

Entregables

Todos los entregables estarán sujetos a la aceptación de los usuarios. Estos entregables deberán estar claramente definidos y serán firmados una vez que lleguen a un acuerdo, y se autorice la continuación del proyecto.

Plan de Implementación

Debido a que el proyecto esta orientado en una forma directa a la replicación de la base de datos y sus procesos de carga en dos servidores, el plan de implementación se simplifica sobremanera:

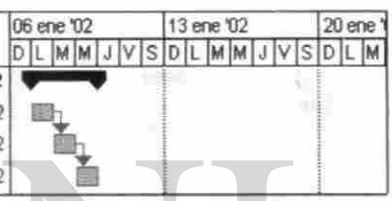
Proyecto de alta disponibilidad

Id	Task Name	Duración	Comienzo	Fin
1	**Proyecto de Alta Disponibilidad**	**90 días**	**lun 07/01/02**	**vie 10/05/02**
2	**Preparación de proyecto**	**3 días**	**lun 07/01/02**	**mié 09/01/02**
6	**Evaluación de Proveedores**	**11 días**	**lun 07/01/02**	**lun 21/01/02**
16	**Elección de Proveedor**	**15 días**	**mar 22/01/02**	**lun 11/02/02**
22	**Capacitación y Entrenamiento**	**16 días**	**mar 12/02/02**	**mar 05/03/02**
26	**Implementación de Solución**	**48 días**	**mié 06/03/02**	**vie 10/05/02**

Preparación del proyecto

Este punto se enfoca a justificar la necesidad mínima de adquirir el hardware adiciona, y los alcances esperados.

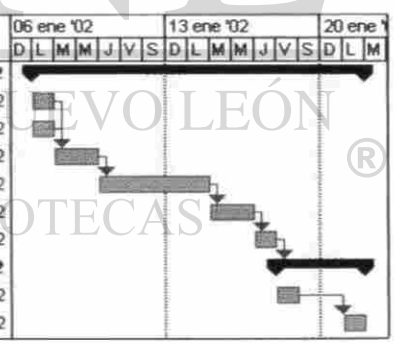
Id	Task Name	Duración	Comienzo	Fin
2	**Preparación de proyecto**	**3 días**	**lun 07/01/02**	**mié 09/01/02**
3	Definir requerimientos de proyecto	1 día	lun 07/01/02	lun 07/01/02
4	Establecer alcances de proyecto	1 día	mar 08/01/02	mar 08/01/02
5	Establecer matriz de evaluación	1 día	mié 09/01/02	mié 09/01/02



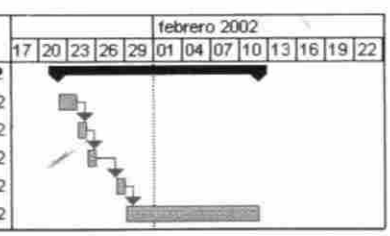
Evaluación y Elección de proveedores

Se reduce a evaluar si la base de datos réplica estará sobre la misma plataforma de hardware, o si es posible llevarla hacia otra infraestructura (Esto puede incrementar los costos de la solución "barata")

Id	Task Name	Duración	Comienzo	Fin
6	**Evaluación de Proveedores**	**11 días**	**lun 07/01/02**	**lun 21/01/02**
7	Invitar proveedores de AD	1 día	lun 07/01/02	lun 07/01/02
8	Firmar Contratos de confidencialidad	1 día	lun 07/01/02	lun 07/01/02
9	Evaluar requerimientos minimos de so	2 días	mar 08/01/02	mié 09/01/02
10	Identif. cambios a infraestructura	3 días	jue 10/01/02	lun 14/01/02
11	Identif. cambios requeridos a aplicaci	2 días	mar 15/01/02	mié 16/01/02
12	Propuestas económicas	1 día	jue 17/01/02	jue 17/01/02
13	**Evaluar propuestas técnicas**	**2 días**	**vie 18/01/02**	**lun 21/01/02**
14	Comparativo de ventajas	1 día	vie 18/01/02	vie 18/01/02
15	Comparativo de desventajas	1 día	lun 21/01/02	lun 21/01/02



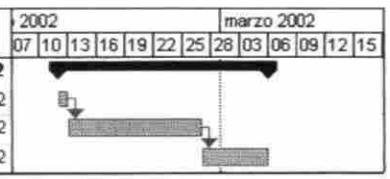
Id	Task Name	Duración	Comienzo	Fin
16	**Elección de Proveedor**	**15 días**	**mar 22/01/02**	**lun 11/02/02**
17	Resultados de propuestas técnicas	2 días	mar 22/01/02	mié 23/01/02
18	Comparativo de Costos	1 día	jue 24/01/02	jue 24/01/02
19	Negociaciones adicionales	1 día	vie 25/01/02	vie 25/01/02
20	Carta compromiso de proyecto	1 día	lun 28/01/02	lun 28/01/02
21	Plan general de implementación	10 días	mar 29/01/02	lun 11/02/02



Capacitación y Entrenamiento

Debido a la solución buscada este punto se basa en que el personal de TI deberá estar consciente de los cambios de configuración, así como la replica de procesos de carga y de la base de datos

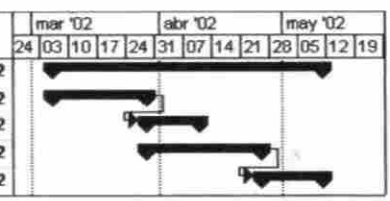
Id	Task Name	Duración	Comienzo	Fin
22	**Capacitación y Entrenamiento**	**16 días**	**mar 12/02/02**	**mar 05/03/02**
23	Planear cursos sobre producto de HA	1 día	mar 12/02/02	mar 12/02/02
24	Capacitación de personal seleccionac	10 días	mié 13/02/02	mar 26/02/02
25	Laboratorios de entrenamiento	5 días	mié 27/02/02	mar 05/03/02



Implementación de la Solución

Adquisición del hardware adicional (Servidores/Discos/CPU's y Memoria)
Adquisición de licencias adicionales de Base de datos y Sistema Operativo
Capacitación y Entrenamiento

Id	Task Name	Duración	Comienzo	Fin
26	**Implementación de Solución**	**48 días**	**mié 06/03/02**	**vie 10/05/02**
27	**Diseñar modelo lógico de Alta Dis**	**17 días**	**mié 06/03/02**	**jue 28/03/02**
36	**Diseñar modelo físico de Alta Dis**	**9 días**	**vie 29/03/02**	**mié 10/04/02**
44	**Laboratorio de Alta Disponibilidad**	**20 días**	**vie 29/03/02**	**jue 25/04/02**
63	**Implementación de solución**	**11 días**	**vie 26/04/02**	**vie 10/05/02**



Requerimientos y Especificaciones Funcionales

Definición de los alcances y limitantes del producto seleccionado:

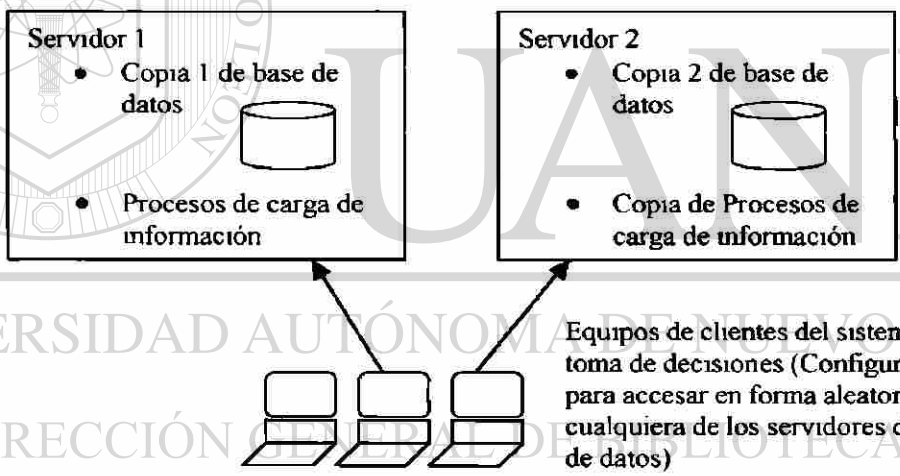
- Identificación de los requerimientos mínimos de hardware:
  - Memoria,
  - Procesadores,
  - Discos,
  - Tipos de tarjetas de red, etc.
  - Tarjetas Fiber Optic,
  - Disk Arrays,
    Cableado de fibra óptica, etc.
- Identificación de los requerimientos de software del producto seleccionado:
  - Sistema operativo, y parches de actualización.
  - Manejadores de bases de datos soportados.
  - Software de terceros que es requerido para operar.
  - Compiladores, bibliotecas de software.
  - Privilegios especiales y puertos de servicios requeridos.

Deberá llenarse los formatos para catalogar e identificar las Equipos, Bases de Datos, Volumenes físicos y lógicos y como se distribuirán las aplicaciones en los equipos. Vea el Apéndice B para conocer estos formatos

Diseño

El diseño fisico deberá incluir los detalles técnicos sobre los elementos fisicos de la instalación, número de tarjetas, redes privadas de hearthbeat, discos protegidos, fuentes de poder (UPS's), servidores adicionales, cableado de cobre, fibra óptica, modificaciones al site, etc. Adicionalmente, deberá formar parte del diseño lógico, la identificación de procesos y grupos de proceso, paquetes de servicio, uso de las IP's para hearthbeat, monitores, tiempo de recuperación, tiempos para detección de la falla, procedimientos de recuperación, métodos de asignación de recursos, reglas de movimiento de paquetes entre servidores, etc.

Como parte de este diseño, y en base al producto seleccionado, deberá indicarse el tipo de Solución (Cluster binodo/multinodo, simétrico ó asimétrico), y plantearse las prioridades de los paquetes de procesos, identificando aquellos paquetes procesos que tienen la mayor prioridad y aquellos paquetes de procesos que pueden delegarse a un uso de recursos más restringido.
En nuestro caso, la solución es un binodo simétrico, aunque el cluster no requiere software especializado.



Diseño de la solución "sin costo" de alta disponibilidad

Esta solución es relativamente barata (sin costo) pues no se adquirió ningún software especial para configurarlo.

Desarrollo

En base al producto seleccionado, y en base a los paquetes de procesos identificados, deberán identificarse los scripts de monitoreo que permitirán detectar las fallas de un proceso o paquete de procesos. Asimismo como parte del proyecto, deberán establecerse las reglas de monitoreo, activación y de validación del Cluster. Cada una de estas reglas y scripts deberán

estar identificados plenamente: su objetivo, lenguaje, temporización, propietario, etcétera. Por ejemplo:

- Regla de operación:
  - o Existirán 2 servidores con la misma capacidad de almacenamiento y procesamiento de información.
  - o Cada servidor contiene una instancia "independiente" de la base de datos para la toma de decisiones.
    Cada servidor contiene una copia del paquete de procesos de carga, asignados a la base de datos especifica dentro del servidor.
  - o Deberá configurarse el servicio de conectividad para permitir acceder en forma aleatoria a la base de datos, y en caso de no estar la primera BD elegida en operación, elegir la siguiente disponible. Ejemplo, si nuestra base de datos está basada en ORACLE, se configura el archivo TNSNAMES.ORA como sigue:

```
BASE DSS.WORLD- DESCRIPTION
(ADDRESS LIST (SOURCE_ROUTE=OFF)(FAILOVER-ON)
  (ADDRESS (PROTOCOL-TCP)(HOST EQUI_PRIMARIO)(PORT=1521))
  (ADDRESS (PROTOCOL TCP)(HOST-EQUI_ALTERNO)(PORT-1521))
  (ADDRESS=(PROTOCOL TCP)(HOST-EQUI_ALTERNO)(PORT=1521))
  (ADDRESS=(PROTOCOL TCP)(HOST=EQUI_PRIMARIO)(PORT=1521))
  )
     (CONNECT DATA=(SERVICE NAME-PRDSS))
)
```

- Reglas de monitoreo:
  - o En una operación normal, cada base de datos se instanciará mediante el RDBMS (Oracle en este caso) y deberá abrirse al servicio al usuario final, Cada servidor deberá tener posibilidad de hacer una llamada al servicio de base de datos existente en la réplica, si este servicio no responde deberá generar un aviso al administrador de la base de datos he aquí un ejemplo:
    - Detectar la BASE DE DATOS

```
###  C  T / p   M^  S   ta   . h
       A  t           P A
 t   SB  AR          \ "
  #   bo v r f  ar q e est  montad  f  esy tem de    ne  d r
  e h  "B    d  d '   ...     t  acr ba'!'"
        "    db "  "   t                    a       d "
  ' t
f
```


El formato para describir estas reglas y scripts deberá seguir un estándar que se utilizará para este y nuevos proyectos dentro de la compañía, el estándar se menciona en el anexo A:

Pruebas

Será necesario identificar y establecer los juegos de pruebas que habrán de realizarse para garantizar la operabilidad de la solución, estas podrían clasificarse como:

- Pruebas generales de fallas parciales
- Pruebas puntuales de fallas de recursos y dispositivos
- Pruebas de falla general de servicios
- "Pruebas de failovers, y recuperación de fallas"
- Validacion y ajustes a la configuración

Este juego base de posibles pruebas deberán detallarse como parte del proyecto final y documentarse ampliamente tal que puedan usarse como soporte para futuras implementaciones

Los escenarios posibles deberán establecerse claramente en conjunto entre los elementos que formen el equipo del proyecto. Deberá generarse un check list de evaluación de cada tipo de escenarios y documentar el comportamiento del sistema bajo estas pruebas.

Migración de Datos

No es requerido, pues la solución no afecta la funcionalidad de la aplicación.

Documentación

La documentación a entregar se compone de:

- Manuales técnicos y de usuario de la solución, estableciendo claramente las dependencias.
- Documentación del modelo físico de la instalación, mencionando las adecuaciones y cambios realizados a las instalaciones, así equipo que forma parte del proyecto.
- Documentación del modelo lógico de la configuración,.
- Manual que documenta todas las reglas y procedimientos que regirán el comportamiento de la configuración, casos de falla identificados y el medio de solución que ofrecerá el producto.
- Manual de estándares que se usaron, y que determinaran el diseño e implementación para futuras instalaciones en Alta Disponibilidad.

Entrenamiento

No hay requerimiento de entrenamiento al usuario final, pues la aplicación no sufre cambios funcionales, por lo que los conocimientos operacionales actuales de la aplicacion son suficientes y no requieres preparación adicional.

Migración final de datos

No es requerido, pues la aplicación no sufre cambios, y por lo tanto la información no deberá ser adecuada como parte de este proyecto. Sin embargo, deberá ser aclarado mediante una notificación al usuario final.

Pruebas de aceptación de usuarios

El usuario deberá ser invitado a validar la funcionalidad (que nunca debe ser afectada) de todo el sistema, una vez que se han configurado servicios de base de datos en Alta Disponibilidad. El usuario utilizará el sistema, como normalmente lo hace, y hará las observaciones sobre comportamiento anómalo, debiendo ajustarse todo aquello que afecte al proceso. Una vez que se hayan adecuado todos aquellas situaciones identificadas, el usuario deberá firmar un acuerdo donde se establece que la funcionalidad no esta sufriendo ninguna afectacion y que por lo mismo la implementación del cluster no afecta en fallas funcionales (usualmente asociadas al uso o alimentación de informacion incompleta o incorrecta), excepto aquellas situaciones donde el sistema ha dejado de operar debido a que el paquete de procesos ha sido cancelado, suspendido, o retardado, como parte de una labor de mantenimiento previamente negociada.

Arranque en Producción

La fecha de arranque deberá ser establecida en base a los requerimientos definidos en esta propuesta, y los tiempos de configuración, desarrollo, pruebas, y fechas negociables con el area usuaria del sistema.

Costos y Beneficios

En base a la solución propuesta, y tomando como base el costo por hora del personal ejecutivo, deberá establecerse el costo de no contar con el sistema en un momento crítico de utilización del sistema.

Costos

Deberá enfocarse el costo de adquisición del hardware y licencias adicionales contra el costo de no contar con el servicio del sistema. Es necesario enfocarse al bajo costo de la solución contra el nivel de rentabilidad recibido.

Beneficios

- Se logrará mejorar el nivel de disponibilidad del sistema de facturación garantizando hasta un 98% de dias de operacion del año
- Podrán programarse mantenimiento de hardware o software en los equipos al sacar de linea los servicios de un equipo mientras el otro continua ofreciendolos.
- Se obtiene una configuración base para implementar soluciones de alta disponibilidad en otros sistemas dentro de la compañia.

Resumen

La necesidad de implementar una solución de Alta Disponibilidad es urgente, el hecho de no planear y ofrecer esta alternativa significa que la compañía se encontrará en desventaja frente a competidores que podran tomar acciones orientadas a mejorar la competitividad que podrian dejar de lado nuestra empresa en la lucha por el mercado

Se contaria con una plataforma que ofreceria posibilidades de crecer la capacidad sin detener la operacion (escalabilidad), al poder detener los servicios en un nodo mientras se "crece" o remplaza el otro

Se establecerá un procedimiento estándar para la implementación simples de soluciones de Alta Disponibilidad, que podremos utilizar para proyectos posteriores

Riesgos

En caso de no aprobarse este proyecto, los riesgos directos son:

- Las probabilidades de una falla en un momento crítico de toma de decisiones (en una junta de consejo),
- El tiempo de recuperación que consumiría,
- Las decisiones no tomadas que podrían correr el riesgo afectar a la compañía.
- Una falla puede extenderse más allá de lo usual, por no tener piezas de recambio disponibles,
- Dependiendo de los tipos de contrato de soporte, existe una dependencia directa del proveedor, si existiese el cluster, la operación podría continuar en el otro nodo y

Aprobación

Este documento, y los resultados de la evaluación, y negociaciones efectuadas, así como la carta compromiso del proveedor y el plan de implementación del proyecto, deberán de anexarse como información de soporte para que una vez presentado ante la alta dirección, se emita la autorización firmada para el desarrollo total del proyecto.

Se deberá firmar la autorización del proyecto y el presupuesto asociado al mismo, definiendo las fechas y los entregables que deberán ofrecerse para medir el avance del mismo.

Un taller de trabajo será llevado a cabo con los usuarios de cada área involucrada para la demostración del cumplimiento de la funcionalidad

Soluciones de Negocio		Firma
Tecnologías de Información, Director		
Tecnologías de Informacion, Gerencia		
Tecnologías de Informacion, Gerencia de		
Director Administrativo		
Director General de Empresa Comercial		

Aprobación de los usuarios

Este tipo de proyectos, requiere una aprobacion por parte de los usuarios en el sentido de que ellos aceptan la implementación de la herramienta, si esta garantiza que la operación podrá continuar sin efectos directos a la metodología de trabajo de los mismos, y sin afectar la especificación funcional del Sistema. Sin embargo, no se requiere aprobación adicional del usuario, por ser un proyecto puramente interno al área de Tecnologías de Información. La aprobacion deberá ser lograda por el Directorio de Tecnologías de Información y apoyada por el Director General de Empresa Comercial.

Usuario	Área	Firma
	Facturación	
	Administración	
	Embarques	