Congr. Int. Ing. Electrón. Mem. Electro 2012, vol.34, pp. 341-346 Chihuahua, Chih. México
http://depi.itchihuahua.edu.mx/display/memorias_electro/MemoriaElectro2012.zip
ISSN 1405-2172

DISEÑO E IMPLANTACION DE UN DRP CON SERVIDORES UNIX Y SAP

José Ignacio Vega Luna, Gerardo Salgado Guzmán, Mario A. Lagos Acosta
Area de Sistemas Digitales, Dpto. de Electrónica, Universidad Autónoma Metropolitana-Azcapotzalco.
Av. San Pablo 180, Col. Reynosa Tamps.
C.P. 02200, México D.F.
vlji@correo.azc.uam.mx

RESUMEN

Se presenta el diseño e implantación de un plan de recuperación de desastres (DRP). El DRP fue implantado y se encuentra operando en una empresa manufacturera, donde el objetivo fue contar con los procesos, el hardware y el software necesarios para recuperar la operación de las aplicaciones criticas del negocio después de un desastre causado por eventos naturales, fallas de hardware o software o errores humanos. Las ventajas principales de este DRP, con respecto a DRPs típicos son las siguientes: se utilizaron los últimos avances en tecnología para la protección de datos dentro de arreglos de discos, para la replicación remota de información, para la red de almacenamiento y para el particionamiento y virtualización de recursos de los servidores usados, además que se implantó con tres centros de datos, dos de ellos activos, en producción, y los servidores se configuraron en cluster, respaldándose entre sí, permitiendo balancear cargas y aplicaciones.

1. INTRODUCCIÓN

Un plan de recuperación de desastres (DRP-Disaster Recovery Plan) no es un producto que sea vendido por un fabricante o proveedor, es una metodología que debe ser diseñada e implantada de acuerdo a las necesidades, tipo de operación, equipos y presupuesto de cada empresa [1]. Lo que funciona para una empresa no siempre funciona para otra. Existen DRPs complejos y muy completos para empresas en las que el perder unos minutos de operación puede significar miles de dólares, como por ejemplo bancos, aerolíneas, empresas de manufactura y aseguradoras. En estas empresas el contar con redundancia completa en los equipos de TI es más importante que el costo físico que se duplica. Algunas empresas en las que sus procesos no sean 100% automatizados pueden detener su equipo de TI unas horas y la recuperación de capacidad de operación puede tomar unas cuantas horas sin que la pérdida sea considerable. Algunas otras pueden prescindir inclusive de operar con computadoras durante un lapso considerable, inclusive días, donde la operación no depende de los sistemas de cómputo por completo. Un DRP debe ser flexible a las necesidades de cada empresa y debe ser modular adaptándose a los requisitos de la organización

Con el crecimiento de la tecnología de información y las aplicaciones más orientadas a la Internet y multimedia, las empresas están demandando mayor capacidad de información, mayor velocidad de procesamiento y mejores tiempos de respuesta. Estas necesidades del negocio se obtienen contando con arreglos de discos, servidores y redes de comunicación de datos cada vez más sofisticados localizados en centros de datos donde la empresa deposita su confianza. Sin embargo, la operación de un centro de datos y de la empresa puede verse afectada por los siguientes factores: fenómenos naturales (inundaciones, huracanes, sismos, entre otros), fuego, falla en el suministro de energía eléctrica, terrorismo, fallas de hardware y software, errores humanos o asuntos legales. Lo importante es contar con una estrategia para la protección de los datos, del hardware y del software crítico para el restablecimiento o continuidad de las operaciones del negocio, respondiendo lo más rápidamente a la interrupción de los servicios usando un DRP para continuar trabajando con las aplicaciones importantes o críticas del negocio.

Un DRP es usado para asegurar la continuidad del negocio y es recomendable partir de la siguiente premisa en su implantación: siempre desear lo mejor y planear para lo peor. Se estima que algunas empresas gastan hasta el 25% de su presupuesto en proyectos de recuperación de desastre, pensando siempre en evitar pérdidas más grandes. Sin embargo, de las empresas que sufren un desastre y no tienen un DRP el 43% no vuelve a abrir, el 51% cierra en menos de dos años, y sólo el 6% sobrevive a largo plazo.

Después de haber invertido cualquier cantidad en desarrollar un DRP, y contar con la seguridad que el DRP que se tiene es el adecuado para las necesidades de la empresa, sigue la fase de la implantación. En esta fase es importante que las personas involucradas en el proceso tengan una cultura DRP usando las mejores prácticas para que el DRP sea efectivo. Como todo proceso de implementación, si no es supervisado correctamente en un inicio se corre el riesgo de que no se continúe la implantación, y se suspenda la aplicación del programa.
El dedicar un poco de tiempo diario al DRP puede ahorrar tiempo futuro, ya que después de haber ocurrido un desastre lo único que puede ayudar es la forma en que la empresa se anticipó al desastre. Un DRP debe contemplar siempre la peor de las situaciones, ya que de este modo, la contingencia podrá ser solventada en el menor tiempo posible.

De acuerdo a la cantidad e importancia de los datos y equipos la mejores prácticas dictan que se debe usar el estado del arte en lo que se refiere a los últimos avances tecnológicos de hardware y software, incluyendo las siguientes acciones para la implantación de un DRP [2]:

a) Contar con al menos una unidad de respaldo de energía eléctrica para cada centro de datos, que puede ser un banco de baterías, una máquina diesel y una o varias acometidas adicionales del proveedor de energía eléctrica.
b) Mantener el equipo de cómputo, de redes de datos, de telecomunicaciones y de almacenamiento de información en centros de datos que cuenten con especificaciones técnicas de ambiente óptimo de operación en lo referente a temperatura y humedad.
c) Contar con redundancia en los componentes de cada centro de datos. En este punto habrá que evaluar la importancia de los datos y la necesidad de la continuidad en el servicio debido al costo que puede implicar la adquisición o almacenamiento de dispositivos redundantes. Se pueden tener discos duros, memoria, procesadores, ventiladores o hasta otro equipo de reserva en caso de que falle el principal. No es necesario tener un servidor idéntico al que está en operación, puede ser uno de menor capacidad que funcione de forma temporal mientras se lleva a cabo la recuperación del original. Se podría considerar utilizar otro servidor con otras funciones que también se encuentre en operación.
d) Contar con protección de la información tanto de sistemas operativos como datos de usuarios y aplicaciones. Es decir, tener copias de respaldo que pueden ser de las siguientes formas [3]:

   Discos duros en espejo, el cual tendrá una copia idéntica del software y datos actual en operación para que en caso que se dañe un disco duro se pueda utilizar el otro de forma inmediata. SE puede usar alternativamente algún método RAID para la protección de información.

   Respaldos de archivos que incluyan todo el sistema de archivos completo o únicamente los datos sensibles. Estos mismos podrán ser completos (full) si almacenan toda la información o incrementales si almacenan sólo los datos modificados en un periodo determinado de tiempo.

   Respaldos de archivos en dispositivos externos, como por ejemplo cintas magnéticas, DVDs, CDs o discos duros externos. Se puede considerar almacenarlos en diferentes ubicaciones.

   Contar con un programa o política de respaldos de manera automática. Cada cierto tiempo hacer respaldos completos y con más frecuencia hacer respaldos incrementales, así como describir el lugar donde se depositan estos respaldos y la forma en que se utilizarán para su recuperación.

e) Contar con al menos un centro de datos alterno [4] desde el cual pueda continuarse la operación de la empresa después de un desastre del centro de datos principal. Aunque gracias a los últimos avances en la tecnología de replicación remota de información se pueden tener DRPs que consideren el uso de dos o más centros de datos, donde todos se respalden entre sí y en los cuales se encuentren ejecutándose aplicaciones productivas de la empresa con lo cual se logra un balanceo de cargas y todos los centros de datos están en operación. Dentro del estado del arte de tecnologías de replicación de

ISSN 1405-2172

información se encuentran el uso de fibre channel [5], replicaciones remotas entre arreglos de discos síncronas y asíncronas y replicaciones locales dentro de un mismo arreglo de discos, las cuales puede usarse también para respaldos en línea.

2. DESARROLLO

El DRP aquí presentado se configuró con de tres centros de datos. En dos de estos centros de datos se encuentra el equipo de cómputo, los arreglos de discos para el almacenamiento de datos y aplicaciones y los sistemas de comunicación usado para soportar las aplicaciones de la empresa (aplicaciones de misión crítica). Los dos centros de datos operan en un esquema activo-activo, están separados geográficamente por una distancia de 10 kilómetros y en cada uno de ellos se encuentran 5 servidores UNIX y un arreglo de discos de 5PB. En el tercer centro de datos se encuentra un servidor Linux en el que no se encuentran corriendo aplicaciones de la empresa. Tanto los 10 servidores UNIX como el servidor Linux se encuentran configurados formando un cluster. El servidor Linux solo se usa como arbitro del cluster Dada la distancia que existe entre los dos centros de datos principales, el cluster se considera como un cluster metropolitano o metrocluster.

Bajo condiciones normales, en uno de los dos centros de datos principales se encontraran ejecutándose algunas aplicaciones de la empresa y en el otro centro de datos principal se encontraran ejecutándose otras aplicaciones, balanceando la carga y conformando un esquema de operación activo-activo. Así, el punto de falla que representa cada centro de datos fue eliminado usando un cluster de servidores y dos centros de datos separados geográficamente.

Cada una de las aplicaciones de misión crítica, está compuesta por una instancia del manejador de base de datos DB2 y una instancia de SAP. Cada aplicación difiere de las otras en el modulo de SAP utilizado. Algunas instancias de SAP fueron configuradas para el modulo de administración de recursos humanos (HR-Human Resources), otras fueron configuradas para el modulo de planificación de recursos empresariales (ERP-Enterprise Resource Planning) y otras fueron configuradas para los módulos de administración financiera (FI), administración de materiales (MM) y administración de proyectos ((PS). Otra aplicación crítica es el software configurado para implantar las políticas de respaldos de datos. Este software se ejecuta en uno de dos servidores UNIX, cada uno de estos servidores se encuentra en uno de los dos centros de datos principales.

La replicación de la información entre los dos arreglos de discos de los dos centros de datos principales se lleva a cabo usando 4 pares de fibras ópticas [6]. En cada par, una fibra se usa para la transmisión de información de un centro de datos al otro y la otra fibra para la recepción, es decir, en cada centro de datos existen cuatro fibras para transmisión y cuatro fibras para recepción, esto es porque en un momento dado algunas aplicaciones estarán ejecutándose en un centro de datos y otras en el otro centro de datos por lo que la replicación de información debe ser bidireccional. Esta replicación se lleva a cabo usando el software correspondiente de los arreglos de datos configurado para trabajar de manera síncrona, lo cual presenta la ventaja de que cuando se ejecute una aplicación de misión crítica en cualquiera de los dos centros de datos, la información usada por la aplicación y que reside en los arreglos de discos siempre será consistente y será la misma en los dos centros de datos. Con esto se logra la protección de la información de manera remota.

Desde el punto de vista local, dentro de un centro de datos, la protección de la información dentro de cada arreglo de discos se implantó configurando los discos de cada arreglo en RAID 5, eliminando con esto el punto de falla que representa cada arreglo de discos y el punto de falla que representa localmente cada mecanismo físico de cada arreglo [7][8].

Para implantar las políticas adecuadas de respaldos en el DRP, en cada uno de los centros de datos se encuentra instalada una biblioteca de cintas para los respaldos de la información. Tanto la biblioteca como el arreglo de discos son compartidos por los servidores UNIX por medio de una red de almacenamiento (SAN-Storage Area Network) [9]. Para eliminar el punto de falla que representa cada componente de la SAN, se configuraron en cada servidor UNIX cuatro puertos de fibro-canal o fibre channel y dos directores de 64 puertos de fibro-canal cada uno. En los servidores UNIX, que son los que pueden alojar una aplicación de misión crítica y por lo

ISSN 1405-2172

tanto usar los discos del arreglo, se utilizan dos puertos de fibro-canal para acceder los discos del sistema operativo y dos puertos parar acceder a la información de las bases de datos e instancia de SAP. Un puerto de fibro-canal de los servidores configurado para acceder el sistema operativo y un puerto de fibro-canal configurado para acceder a la base de datos se conectó a uno de directores de la SAN, mientras que los dos puertos de restantes de fibro-canal de cada servidor se conectaron al otro director, de manera tal que los dos directores balancean el acceso al arreglo de discos y se respaldan entre sí en caso de una falla de alguno de ellos. El servidor Linux al encontrarse en el tercer centro de datos no tiene acceso a la SAN de los dos centros de datos principales.

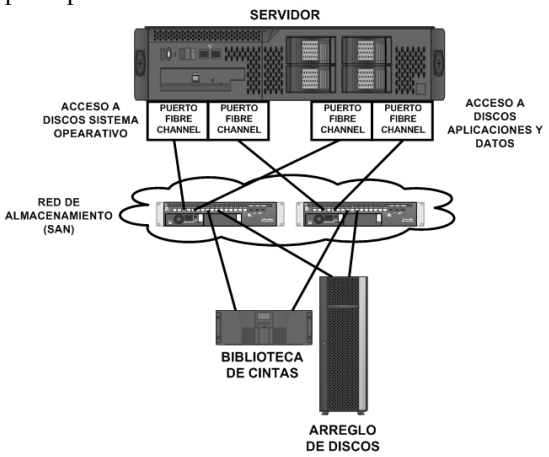

*Figura 1***.** Conexión de cada servidor a la SAN

Para el caso de la comunicación de datos entre los servidores del cluster y con los usuarios de las aplicaciones, se configuraron. en cada servidor UNIX y en el servidor Linux, cuatro puertos de red de 10Gb. Dos puertos están conectados al segmento de red de los usuarios, uno de ellos está activo (puerto primario) y el otro sirve como respaldo del anterior (puerto secundario). Los otros dos puertos de red restantes se encuentran conectados a un segmento privado y exclusivo de del cluster usado para transmitir la señal de latencia o heartbeat entre los servidores o nodos del cluster. En este caso, también se configuró en cada servidor un puerto primario y el otro puerto redundante como puerto de respaldo o secundario. En cada centro de datos se encuentran instalados y configurados dos switches de red, en uno de ellos se encuentran conectados los puertos de red primarios de cada servidor y en el otro se encuentran conectados los puertos secundarios. En los switches se configuraron también dos LAN virtuales (VLANs), una para cada uno de los dos segmentos usados en los servidores del cluster. Ambos switches están interconectados entre sí y conectados a la red corporativa de la empresa. Con esto se está eliminando el punto de falla que representada cada puerto de red de los servidores, cada puerto de los switches y cada switch completo [10].

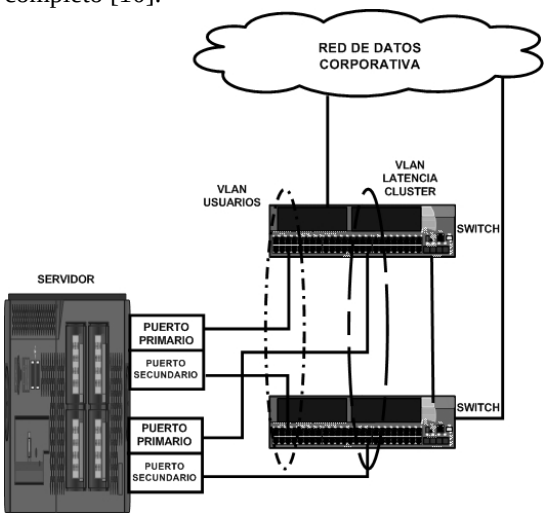

*Figura 2***.** Conexión de cada servidor a los segmentos de la red de datos

3. RESULTADOS

Antes de salir a producción el metrocluster y DRP implantados, se realizó una matriz de pruebas muy extensa que incluyó los siguientes eventos y escenarios: ejecutar las aplicaciones de misión crítica en su servidor UNIX correspondiente de un centro de datos, es decir, todas las aplicaciones ejecutándose en un centro de datos; ejecutar las aplicaciones de misión crítica en su servidor UNIX correspondiente del otro centro de datos, todas las aplicaciones ejecutándose en el otro centro de datos; fallar todo un centro de datos apagando todo el equipo del mismo, lo cual trae como consecuencia que las aplicaciones arranquen automáticamente en el otro centro de datos; fallar puertos de red y puertos de fibro-canal en los servidores UNIX; apagado de switches de red y directores de la SAN; desconexión de fibras de replicación de datos entre los dos centros de datos y realizar respaldo y recuperación de datos en los dos centros de datos.

Una vez en producción el DRP y estando operando, se ha presentado la necesidad de realizar actividades de mantenimiento planeadas al hardware y software como por ejemplo:

ISSN 1405-2172

instalación de parches; actualización de firmware; cambio de tarjetas de red o fibro-canal que han fallado y actualización de versiones de sistemas operativos. En estas situaciones se han movido aplicaciones de misión crítica de un centro de datos para liberar el servidor donde se encontraban corriendo y realizar el mantenimiento correspondiente y seguir proporcionando servicio a los usuarios desde otro servidor sin contratiempos.

4. CONCLUSIONES

El DRP implantado ha respondido satisfactoriamente a eventos planeados y no planeados para lo que fue concebido, cumpliendo el objetivo planteado en su inicio. Se han presentado fallas de componentes hardware y ha entrado en función la redundancia configurada. Así también, el DRP ha servido para continuar proporcionando el servicio y acceso a las aplicaciones de misión crítica cuando se ha presentado la necesidad de realizar tareas de mantenimiento planeado. Solo cabe indicar que cuando se presenta la falla de algún componente, el evento será transparente a los usuarios y solo será vista a ciertos niveles del sistema completo. Por ejemplo la falla de un puerto de red o de un puerto de fibro-canal solo será vista por el sistema operativo del servidor correspondiente y por el software de monitoreo del DRP y no por los usuarios finales ni aplicaciones ya que no se interrumpe el servicio proporcionado a ellos. Sin embargo, la falla de componentes mayores del DRP, como por ejemplo la falla de un servidor UNIX o la falla de todo un centro de datos interrumpen por un breve periodo de tiempo el acceso a las aplicaciones y el servicio a los usuarios, ya que las aplicaciones (instancias del manejador de base de datos e instancia de SAP) deben arrancar en otro servidor para seguir proporcionando servicio a los usuarios.

Finalmente, una de las bases principales en la implantación de este DRP es contar con la suficiente redundancia en los componentes cuya falla pueda interrumpir el servicio a los usuarios, lo cual implica realizar una inversión costosa pero útil como lo es la adquisición de cualquier seguro.

La empresa esta preparada para continuar su operación después de contingencias mayores, y si es necesario implantar un DRP como el aquí presentado en otro lugar, la pregunta inicial que se debe hacer antes de invertir en un sistema como este es la siguiente: ¿cuanto esta dispuesto a perder el negocio después de un desastre?

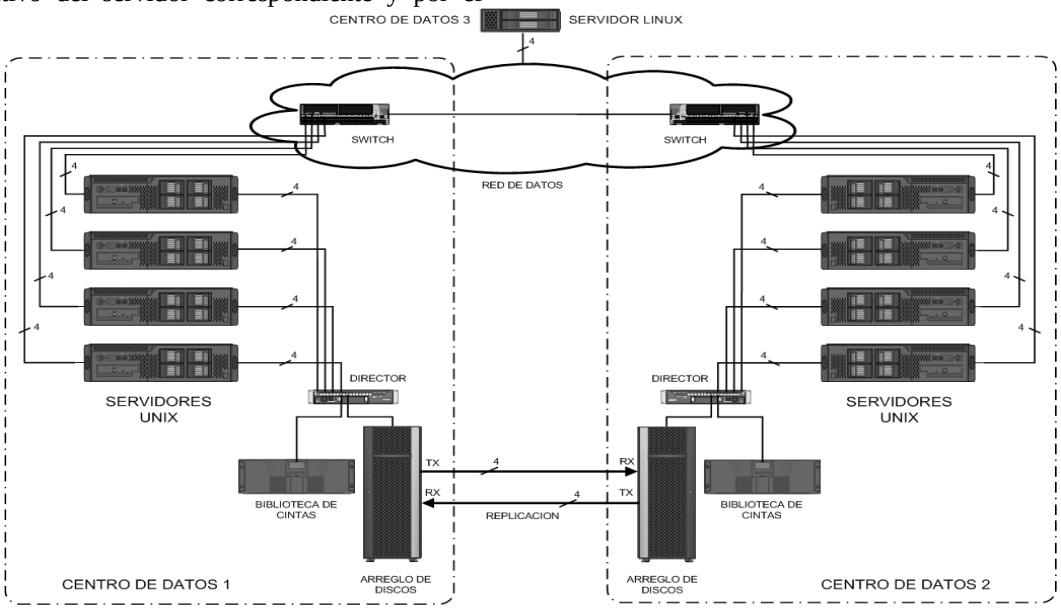

*Figura 3***.** Configuración del DRP

5. REFERENCIAS

[1] Wells, Walker. ***Disaster Recovery: Principles and Practices.*** 1/e. Ed. Prentice Hall. 2007. ISBN-10: 013171127X | ISBN-13: 9780131711273.

[2] Al-Ghamdi, H.S.; Al-Aama, A.Y. ***DRP-DRP: Daata Replication Protocol for Disaster Recovery Planning***. IIT 2008 International Conference on Innovations in Information Technology. pp. 228-232. 2008.

[3] Data Center Services. ***Best-practice strategies for designing and deploying modular data center-Technical White Paper.*** IBM Global Technology Services. 2011.

[4] Nukarapu, D.T.; Bin Tang; Liqiang W.; Shiyong Lu. ***Data Replication in Data Intensive Scientific Applications with Performance Guarantee***. IEEE Transactions on Parallel and Distributed Systems. Vol. 22. Issue 8. pp. 1299-1306. 2011. ISSN: 1045-9219.

[5] Cherkasova, L.; Kotov, V.; Rokicki, T. ***Designing fibre channel fabric***. ICCD '95 Proceedings, 1995 IEEE International Conference on Computer Design. pp. 346-351. 1995.

[6] Yang Ping; Kong Bo. ***Remote disaster recovery system architecture based on database replication technology***. 2010 International Conference On Computer and Communication Technologies in Agriculture Engineering (CCTAE). Vol. 1. pp. 254-257. June 2010. Beijing, China.

[7] Sauers, B. C***hoosing the Right Disk Technology in a High Availability Environment-A Technical White Paper***. Hewlett-Packard Company.

[8] Lingfang, Z.; Dan F. ***ARRAY: A Non-application-Related, Secure, Wide-Area Disaster Recovery Storage System***. 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications. pp. 245-252. Aug. 2009. Wuhan, China.

[9] Sindi, M.; Liu, E.; Al-Shaikh, R. ***SAN performance evaluation testbed***. TridentCom 2009. 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops. pp. 1-5. 2009.

[10] Bianco, A.; Finochietto, J. ***Network planning for disaster recovery.*** 16th IEEE Workshop on Local and Metropolitan Area Networks, 2008. LANMAN 2008. pp. 43-48. Sept. 2008. Torino, Italy.