INTRODUCCION

1 OBJETIVO:

Sin importar cuan duro un administrador trabaje para proteger sus redes de un desastre, hay veces en que lo peor ocurre. Los servidores están sujetos a fallas de hardware debido a su vida útil, uso desmedido o defectos, las pérdidas de datos por ataques de hackers o desastres naturales como un incendio o inundación pueden destruir los datos y los sistemas en si mismos.

Dentro del arsenal de herramientas que un administrador debe contar estarán las políticas de backup, los sistemas de discos tolerantes a fallos y los medios de almacenamiento, de esto hablaremos a lo largo de esta clase.

Al final de esta clase el alumno estará en condiciones de:

- ✓ Comprender la problemática del resguardo de información
- ✓ Entender el concepto de recuperación de desastres y actuar en forma preactiva para minimizar sus efectos.
- ✓ Conocer y enumerar los diferentes medios de resguardo actuales y cuales son las tendencias a futuro.
- ✓ Identificar las diversas estrategias de backup y restauración para así aplicarlas al ambiente que le sea requerido según el caso.

2 DEFINICION Y CLASIFICACION DE DESASTRES:

Un desastre ocurre cuando algún evento impide el normal funcionamiento de las operaciones de negocios de una empresa y puede resultar en alguna forma de perdida de datos.

Es importante identificar tipos de desastres que puedan afectar a una compañía e implementar medidas para tratar con ellos de manera adecuada.

Cuando la gente piensa en desastres, lo hacen generalmente en tormentas, inundaciones, incendios, terremotos u otros eventos naturales. Sin embargo otras amenazas naturales existen, ellas incluyen:

- ✓ Seguridad inadecuada en un área de edificio.
- ✓ Calidad pobre o temperatura elevada de la sala de servidores.
- ✓ Software desactualizado.
- ✓ Equipamiento obsoleto.

Además de estos, los desastres pueden ocurrir como resultado de la acción del hombre, donde tanto accidental como de forma deliberada uno o un grupo de ellos puede causar algún tipo de daño.

Un hacker puede obtener acceso a información sensible, los virus pueden infectar una red y corromper los datos, o empleados pueden sabotear los equipos y comprometer la información.

Cualquiera sea su origen, el desastre resultante tiene el potencial de causar un daño importante para la compañía.

2.1 RECUPERACION DE DESASTRES:

Es el proceso de reconocer o identificar que amenazas tienen el potencial de escalar a un desastre y luego tomar medidas para prevenir o minimizar su impacto. Haciendo esto, los sistemas de misión crítica de una compañía pueden ser restaurados inmediatamente o dentro de un corto periodo de tiempo después que el desastre ocurrió.

La clave de la recuperación de desastres es estar preparado. Algunos desastres son más inesperados que otros. Aunque se sabía que habría repercusiones en la **"falla del año 2000"**, en una determinada fecha y los preparativos deberían estar listos para antes del 1 de enero de 2000, nadie podría por el contrario haber previsto los efectos del 11 de Septiembre de 2001. Bajo el mismo razonamiento uno puede saber que el software Windows dejará de funcionar en una fecha determinada si no se activa el producto, pero es casi imposible determinar cuando un disco duro fallará.

Estableciendo planes y procedimientos y teniendo herramientas y tecnologías antes de que el desastre ocurra, una compañía se recuperara mejor del mismo y retornara pronto a su normal funcionamiento de negocios.

No existe solo un plan o utilidad que pueda enfrentar lo diverso de la naturaleza de los desastres, por lo cual deberían desarrollarse algunos documentos específicos como parte de la política global de recuperación, estos incluyen los siguientes:

- ✓ Planes de continuidad de negocios.
- ✓ Planes de recuperación de desastres.
- ✓ Planes de Backup o Resguardo

2.1.1 PLANES DE CONTINUIDAD DE NEGOCIOS

Tiene que ver con identificar las funciones claves de los departamentos y de las posibles amenazas que puedan ponerlos en peligro.

Por ejemplo si una empresa vende bienes el plan de continuidad de negocios se usa para restaurar la habilidad de la empresa de vender esos bienes y que además puedan llegar al cliente.

2.1.2 PLAN DE RECUPERACIÓN DE DESASTRES:

En cada desastre un minuto ahorrado de antemano es uno que no se desperdiciara luego.

Ciertas contraseñas que son necesarias para acceder a documentos específicos o determinadas cuentas para solucionar un problema por ejemplo, deberían estar disponibles en un lugar seguro pero accesible al personal de IT encargado de la resolución mismo. Una copia de estas debería estar almacenada offiste en caso de que el edificio entero se destruya.

Debería existir una lista de contacto para personas importantes como ser el personal de IT y sus roles, en caso que personas de otras áreas descubran un evento, además de contactos se soporte técnico de hardware o software y del ISP.

Los procedimientos acerca de cómo enfrentar problemas específicos deberían estar disponibles para el personal de IT tanto en formato electrónico e impresos en caso de que los primeros no estuvieran disponibles.

2.1.3 PLAN DE BACKUP O RESGUARDO:

Un backup debería ser creado y también la documentación necesaria para la recuperación de desastres.

La información del plan de resguardo debería incluir que pasos seguir para resguardar y restaurar los datos, donde se encuentra almacenada la información resguardada, y cuan antigua es la información que se tiene.

Asimismo debería estar disponible la documentación y CD de instalación del software crítico debería estar almacenado en un lugar accesible para aquellos que lo necesiten. Los programas instalados en un servidor pueden necesitar ser reparados o reinstalados durante una recuperación

Un punto de partida de una restauración exitosa puede ser el volcado de una imagen tomada en el momento de la instalación fresca del sistema operativo mediante una herramienta como el Symantec Ghost y luego la restauración de los datos de usuarios y bases.

3 ARREGLOS DE DISCOS (RAID)

Una técnica de almacenamiento que nos será útil en la elaboración de nuestro plan de recuperación de desastres es la implementación de RAID (Redundant Array of Inexpensive/Independent Disks)

Consiste en un conjunto de discos trabajando como una única unidad y proporcionando tolerancia a fallos, considerándose esta ultima como ***la habilidad del sistema para continuar funcionando cuando un componente - en este caso un disco duro – ha fallado.***

Hay dos tipos bien diferenciados para lograr este tipo de arreglos, el RAID por software o el RAID por hardware.

El RAID por software es el soportado por el controlador del sistema operativo, como es el caso de Windows Server 2003 O Linux y el RAID por hardware es el que se implementa mediante una controladora dedicada.

La tecnología RAID protege los datos contra el fallo de una unidad de disco duro. Si se produce un fallo, RAID mantiene el servidor activo y en funcionamiento hasta que se sustituya la unidad defectuosa.

La tecnología RAID se utiliza también con mucha frecuencia para mejorar el rendimiento de servidores y estaciones de trabajo. Estos dos objetivos, protección de datos y mejora del rendimiento, no se excluyen entre sí.

Todos los sistemas RAID suponen **la pérdida de parte de la capacidad de almacenamiento** de los discos, para conseguir la redundancia o almacenar los datos de paridad.

Hay una diferencia adicional en cuanto al tratamiento de los discos en los dos esquemas:

3.1 RAID POR SOFTWARE:

Todos los discos físicos son presentados al Sistema Operativo tal como son y este los administra como una configuración RAID. El beneficio de este tipo de RAID es que esta incorporado en el Sistema Operativo.

RAID por software tiene menor rendimiento que su versión de hardware, es barato y fácil de configurar porque no tiene requerimientos especiales más allá de múltiples discos.

La contra es que el Sistema Operativo al ser encargado del mantenimiento del mismo incurre en una sobrecarga de trabajo. Adicionalmente hay limitaciones en cuanto a los niveles de RAID posibles.

3.2 RAID POR HARDWARE:

Las funciones de RAID por hardware son manejadas a través de una combinación de firmware almacenado en la placa controladora y un procesador de entrada/salida incorporado a la misma. La placa actúa como un único disco virtual enmascarando los discos individuales tanto a la motherboard así como al sistema operativo, si un disco falla, la controladora continúa proporcionando datos, la falla del disco y el mecanismo de recuperaron son transparentes al sistema operativo.

Como punto a tener en cuenta se puede usar los niveles RAID 0 y RAID 5 para los volúmenes de Inicio y Sistema.

Soporta todos los niveles de RAID disponibles y sus combinaciones.

Si el costo es mas importante que el rendimiento, software RAID es apropiado, de lo contrario se debe optar por una controladora de hardware.

Un factor a tener en cuenta es que la implementación de esta controladora toma un tiempo mayor en el inicio del Sistema Operativo debido al tiempo de inicialización de la misma.

3.3 ARREGLOS PARALELOS VS ARREGLOS INDEPENDIENTES:

Arreglos paralelos: éstos son aquellos en que cada disco participa en todas las operaciones de entrada/salida. Este tipo de arreglo ofrece **tasas altísimas de transferencia** debido a que las operaciones son **distribuidas** a través de todos los discos del arreglo y ocurren en forma prácticamente simultánea. La tasa de transferencia será muy cercana, 95%, a la **suma de las tasas de los discos miembros**, mientras que los índices de operaciones de entrada/salida serán similares a las alcanzadas por un disco individual. En síntesis, **un arreglo paralelo accederá sólo un archivo a la vez pero lo hará a muy alta velocidad**. Algunas implementaciones requieren de actividades adicionales como la sincronización de discos.

Los RAID de niveles 2 y 3 se implementan con arreglos paralelos.

Arreglos independientes: son denominados así aquellos arreglos en los cuales cada disco integrante opera en forma independiente, aún en el caso de que le sea solicitado atender varios requerimientos en forma concurrente. Este modelo ofrece **operaciones de entrada/salida sumamente rápidas** debido a que cada disco está en posición de atender un requerimiento por separado. De esta forma las operaciones de entrada/salida serán atendidas a una velocidad cercana, 95%, a la **suma de las capacidades de los discos presentes**, mientras que la tasa de transferencia será similar a la de un disco individual debido a que cada archivo está almacenado en sólo un disco.

Los niveles 4 y 5 de RAID se implementan con arreglos independientes, mientras que los niveles 0 y 1 pueden ser implementados tanto en forma de arreglos independientes como en arreglos paralelos.

3.4 NIVELES DE RAID

RAID ofrece varias opciones, llamadas niveles RAID cada una de las cuales proporciona un equilibrio distinto entre tolerancia a fallos, rendimiento y coste.

No hay un nivel de RAID mejor que otro; cada uno es apropiado para determinadas aplicaciones y entornos informáticos. De hecho, resulta frecuente el uso de varios niveles RAID para distintas aplicaciones del mismo servidor. Oficialmente existen siete niveles diferentes de RAID (0-6), definidos y aprobados por el RAID Advisory Board (RAB). Luego existen las posibles combinaciones de estos niveles (10, 50, etc.). **Los niveles RAID 0, 1, 0+1 y 5 son los más populares.**

El nivel de RAID 0 no se tratara debido a que por si solo no ofrece tolerancia a fallos sino aumento de performance, siendo esta ultima una función que no influye en la prevención de perdida de información.

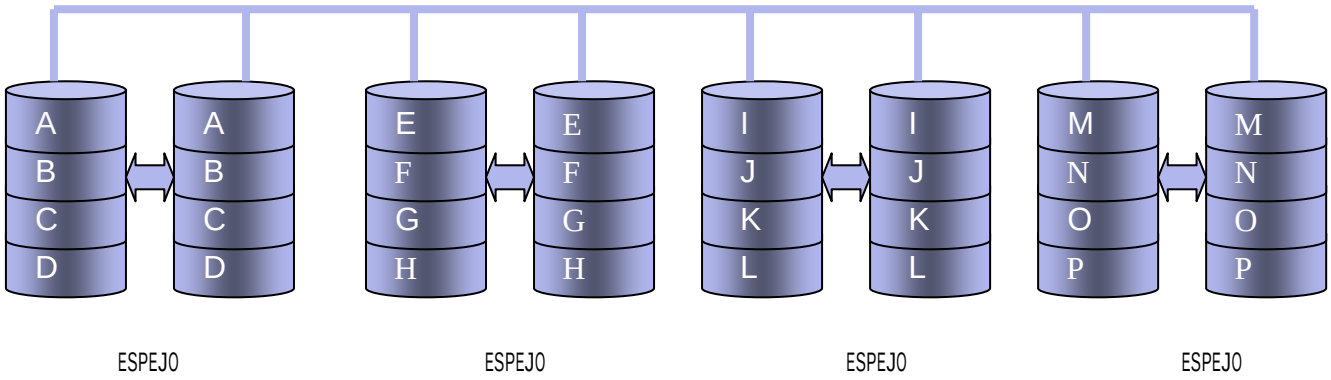
3.4.1 RAID 1 (MIRRORING O ESPEJADO)

También llamado **"Duplicación" (Creación de discos en espejo)**. Se basa en la utilización de discos adicionales sobre los que se realiza una copia en todo momento de los datos que se están modificando. RAID 1 ofrece una excelente disponibilidad de los datos mediante la **redundancia**

total de los mismos. Para ello, se duplican todos los datos de una unidad o matriz en otra. De esta manera se asegura la integridad de los datos y la **tolerancia al fallo**, pues en caso de avería, la controladora sigue trabajando con los discos no dañados sin detener el sistema. Los datos se pueden leer desde la unidad o matriz duplicada sin que se produzcan interrupciones. RAID 1 es una alternativa costosa para los grandes sistemas, ya que las unidades se deben añadir en pares para aumentar la capacidad de almacenamiento. Sin embargo, RAID 1 es una buena solución para las aplicaciones que requieren redundancia cuando hay sólo dos unidades disponibles. Los servidores de archivos pequeños son un buen ejemplo. Si la implementación es por software y ambas unidades están en la misma controladora no habrá tolerancia a fallos si la controladora falla, por eso se recomienda **DISK DUPLEXING**, que significa ubicar a cada disco integrante de la matriz en controladoras separadas. **Se necesita un mínimo de dos unidades para implementar una solución RAID 1.**

RAID1 esta diseñado para sistemas en donde la disponibilidad de información es esencial y su reemplazo resultaría difícil y costoso (mas costoso que reponer el disco en si).

Típico en escrituras aleatorias pequeñas con tolerancia a fallos. El problema de este tipo de arreglos es el costo que implica duplicar el disco.



3.4.2 RAID 2 (ACCESO PARALELO CON DISCOS ESPECIALIZADOS)

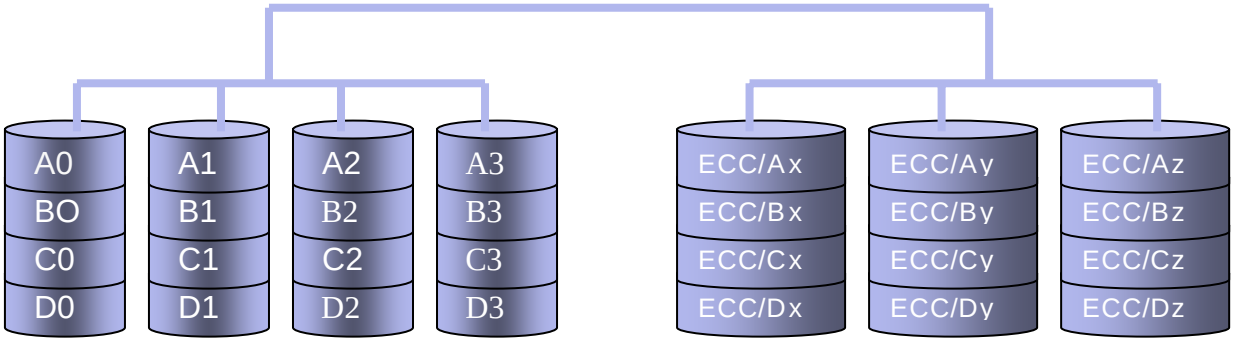
El RAID nivel 2 adapta la técnica comúnmente usada para detectar y corregir errores en memorias de estado sólido. En un RAID de nivel 2, el código ECC (Error Correction Code) se intercala a través de varios discos a nivel de bit. El método empleado es el Hamming. Puesto que el código Hamming se usa tanto para detección como para corrección de errores (Error Detection and Correction),

RAID 2 no hace uso completo de las amplias capacidades de detección de errores contenidas en los discos. Las propiedades del código Hamming también restringen las configuraciones posibles de matrices para RAID 2, particularmente el cálculo de paridad de los discos. Por lo tanto, RAID 2 no ha sido apenas implementado en productos comerciales, lo que también es debido a que requiere características especiales en los discos y no usa discos estándares. Debido a que es esencialmente una tecnología de acceso paralelo, RAID 2 está más indicado para aplicaciones que requieran una

alta tasa de transferencia y menos conveniente para aquellas otras que requieran de una alta tasa de demanda I/O.

Cada BIT de palabra de datos es escrito a un disco de datos (4 en este ejemplo, del 0 al 3). Cada palabra de datos tiene su palabra de código ECC Hamming registrada en los discos de ECC.

Durante la lectura el código ECC verifica los datos correctos o corrige los errores de un disco.



A0 a A3 = Palabra A B0 a B3= Palabra B

C0 a C3= Palabra C D0 a D3= Palabra D

ECC/Ax a Az = ECC Palabra A

ECC/Bx a Bz = ECC Palabra B

ECC/Cx a Cz = ECC Palabra C

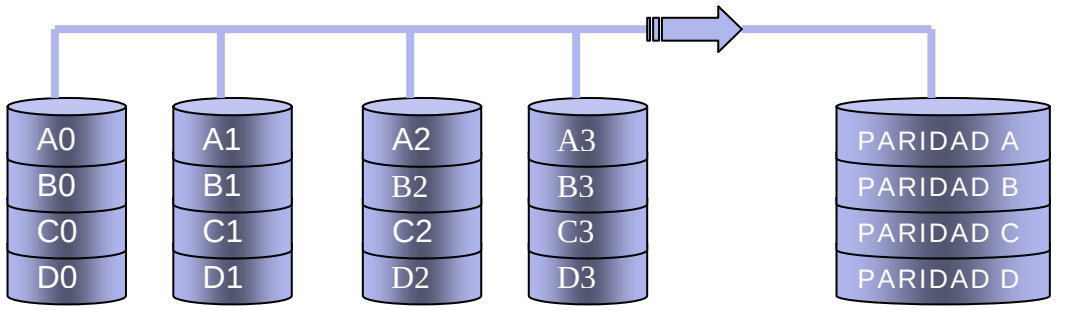
ECC/Dx a Dz = ECC Palabra D

3.4.3 RAID 3 (ACCESO SINCRONO CON UN DISCO DEDICADO A PARIDAD)

Dedica un único disco al almacenamiento de información de paridad. La información de ECC (Error Checking and Correction) se usa para detectar errores. La recuperación de datos se consigue calculando el O exclusivo (XOR) de la información registrada en los otros discos. La operación I/O accede a todos los discos al mismo tiempo, por lo cual el RAID 3 es mejor para sistemas de un sólo usuario con aplicaciones que contengan grandes registros. RAID 3 ofrece altas tasas de transferencia, alta fiabilidad y alta disponibilidad, a un coste intrínsicamente inferior que un Mirroring (RAID 1). Sin embargo, su rendimiento de transacción es pobre porque todos los discos del conjunto operan al unísono. Se necesita un mínimo de tres unidades para implementar una solución RAID 3. Resultan mas adecuados para sistemas en los que transfieren grandes cantidades de datos secuencialmente, ejemplo audio, video. Para estos es el nivel RAID más eficiente ya que nunca es necesario leer modificar, escribir el bloque de paridad. Es menos apropiado para el tipo de acceso de base de datos en los cuales se necesitan transferir pequeñas unidades de datos de manera aleatoria.

GENERACION DE PARIDAD

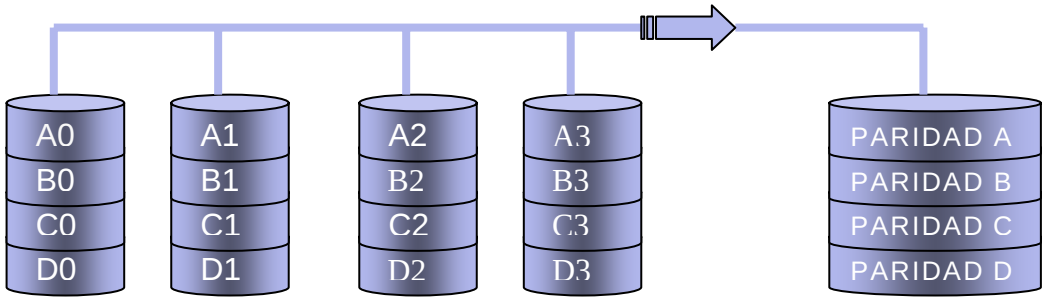
El boque de datos es subdividido (separado n bandas) y escrito en los discos de datos. La paridad de las bandas se genera en las escrituras, registrada en los discos de paridad y chequeada en las lecturas.



Stripe 0 **Stripe 1** **Stripe 2** **Stripe 3** **Paridad Stripes 0.1.2 y3**

3.4.4 RAID 4 (ACCESO INDEPENDIENTE CON UN DISCO DEDICADO A PARIDAD)

Basa su tolerancia al fallo en la utilización de un disco dedicado a guardar la información de paridad calculada a partir de los datos guardados en los otros discos. En caso de avería de cualquiera de las unidades de disco, la información se puede reconstruir en tiempo real mediante la realización de una operación lógica de O exclusivo. Debido a su organización interna, este RAID es especialmente indicado para el almacenamiento de archivos de gran tamaño, lo cual lo hace ideal para aplicaciones gráficas donde se requiera, además, fiabilidad de los datos. **Se necesita un mínimo de tres unidades para implementar una solución RAID 4.** La ventaja con el RAID 3 está en que se puede acceder a los discos de forma individual.



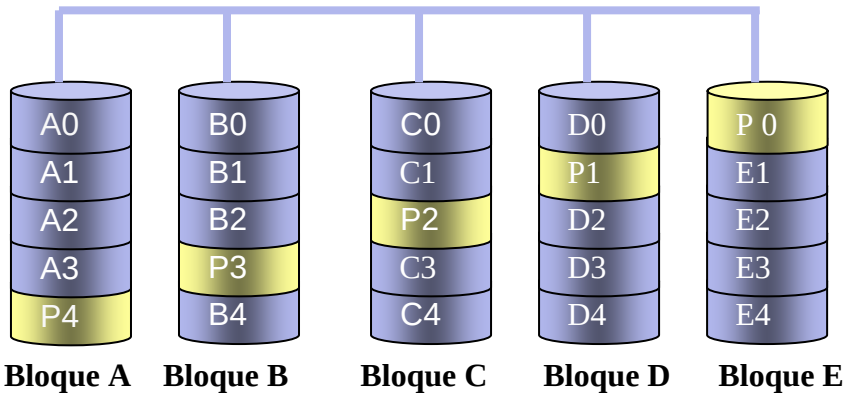
Bloque 0 **Bloque 1** **Bloque 2** **Bloque 3** **Paridad Bloques 0, 1,2 y 3**

Cada bloque es escrito en un disco de datos. La paridad para el mismo bloque es generada durante las escrituras, registrada en el disco de paridad y chequeada en las lecturas.

3.4.5 RAID 5 (ACCESO INDEPENDIENTE CON PARIDAD DISTRIBUIDA)

Este arreglo ofrece tolerancia al fallo, pero además, **optimiza la capacidad del sistema** permitiendo una utilización de hasta el 80% de la capacidad del conjunto de discos. Esto lo consigue mediante el cálculo de información de paridad y su almacenamiento alternativo por bloques en todos los discos del conjunto. La información del usuario se graba por bloques y de forma alternativa en todos ellos. De esta manera, si cualquiera de las unidades de disco falla, se puede recuperar la información en tiempo real, sobre la marcha, mediante una simple operación de lógica de O exclusivo, sin que el servidor deje de funcionar. Así pues, para evitar el problema de cuello de botella que plantea el RAID 4 con el disco de comprobación, el RAID 5 no asigna un disco específico a esta misión sino que asigna un bloque alternativo de cada disco a esta misión de escritura. Al distribuir la función de comprobación entre todos los discos, se disminuye el cuello de botella y con una cantidad suficiente de discos puede llegar a eliminarse completamente, proporcionando una velocidad equivalente a un RAID 0.

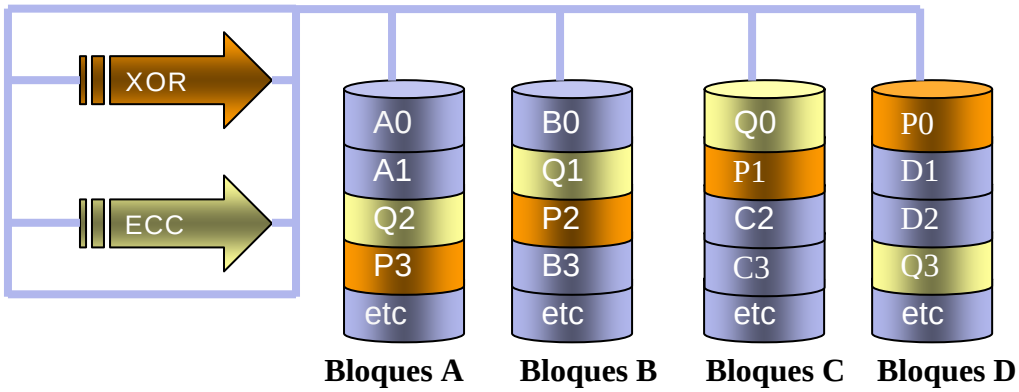
RAID 5 es el nivel de RAID más eficaz y el de uso preferente para las aplicaciones de servidor básicas para la empresa. Comparado con otros niveles RAID con tolerancia a fallos, RAID 5 ofrece la **mejor relación rendimiento-coste en un entorno con varias unidades**. Gracias a la combinación del fraccionamiento de datos y la paridad como método para recuperar los datos en caso de fallo, constituye una solución ideal para los entornos de servidores en los que gran parte del E/S es aleatoria, la protección y disponibilidad de los datos es fundamental y el coste es un factor importante. Este nivel de arreglo es especialmente indicado para trabajar con sistemas operativos multiusuarios. **Se necesita un mínimo de tres unidades para implementar una solución RAID 5.** Los niveles 4 y 5 de RAID pueden utilizarse si se disponen de tres o más unidades de disco en la configuración, aunque su resultado óptimo de capacidad se obtiene con siete o más unidades. RAID 5 es la solución más económica por megabyte, que ofrece la mejor relación de precio, rendimiento y disponibilidad para la mayoría de los servidores.



3.4.6 RAID 6 (ACCESO INDEPENDIENTE CON DOBLE PARIDAD)

Similar al RAID 5, pero incluye un segundo esquema de paridad distribuido por los distintos discos y por tanto ofrece tolerancia extremadamente alta a los fallos y a las caídas de disco, ofreciendo dos

niveles de redundancia. Hay pocos ejemplos comerciales en la actualidad, ya que su coste de implementación es mayor al de otros niveles RAID, ya que las controladoras requeridas que soporten esta doble paridad son más complejas y caras que las de otros niveles RAID. Hay pocas implementaciones comerciales de este tipo. Requiere N+2 discos debido a la doble paridad.

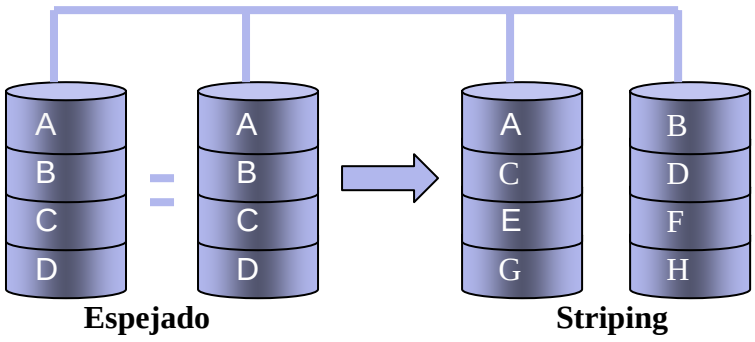


3.4.7 RAID 10 (1+0)

La información se distribuyen en bloques como el RAID 0 y adicionalmente, cada disco se duplica como RAID 1, creando un segundo nivel de arreglo se conoce como "Striping de arreglos duplicados". Se requieren, dos canales, dos discos para cada canal y se utilizan el 50 % de la capacidad para información de control. Requiere un mínimo de 4 unidades para implementarse.

Este nivel ofrece un 100 % de redundancia de la información y un soporte para grandes volúmenes de datos, donde el precio no es un factor importante.

Ideal para sistemas de emisión critica, donde se requiera mayor confiabilidad de la información, ya que pueden fallar dos discos inclusive (uno por cada canal) y los datos todavía se mantienen en línea Es apropiado también en escritura aleatorias pequeñas como una base de datos que requiere disponibilidad.



3.4.8 RAID 30 (3+0)

Es ideal para aplicaciones no interactiva, tal como señales de grafico e imágenes. Se conoce también como Striping de arreglos de paridad dedicada .La información es distribuida a través de los discos, como en RAID 0 y utiliza paridad dedicada, como RAID 3, en un segundo canal, requiere mínimo 6 discos.

Proporciona una alta confiabilidad igual que el RAID 10 ya que también es capaz de tolerar dos fallas físicas en canales diferentes, manteniendo la información disponible

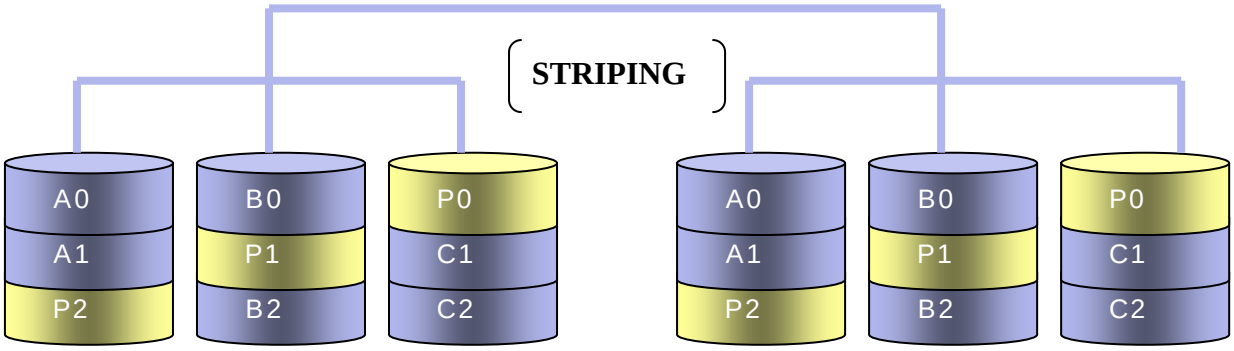
RAID 30 es mejor para aplicaciones no interactivas, tal como señales de video, gráficos, que procesan secuencialmente grandes archivos y requieren alta velocidad y disponibilidad

3.4.9 RAID 50 (5+0)

Esta diseñado para aplicaciones que requieren un almacenamiento altamente confiable una elevada tasa de lectura y un buen rendimiento en la transferencia de datos con un nivel de RAID 50 , la información se reparte en los discos y se usa paridad distribuida , por eso se conoce como Striping de arreglo de paridad distribuidas .Se requiere mínimo 6 discos.

Se logra confiabilidad de la información, un buen rendimiento en general, y además soporta grandes volúmenes de datos. Igualmente si dos discos sufren fallas físicas en diferentes canales, la información no se pierde.

RAID 50 es ideal para aplicaciones que requieran un almacenamiento altamente confiable , una elevada tasa de lectura , y un buen rendimiento en la transferencia de datos .A este nivel se encuentran aplicaciones de oficina con muchos usuarios accediendo a pequeños archivos , al igual que procesamiento de transacciones .

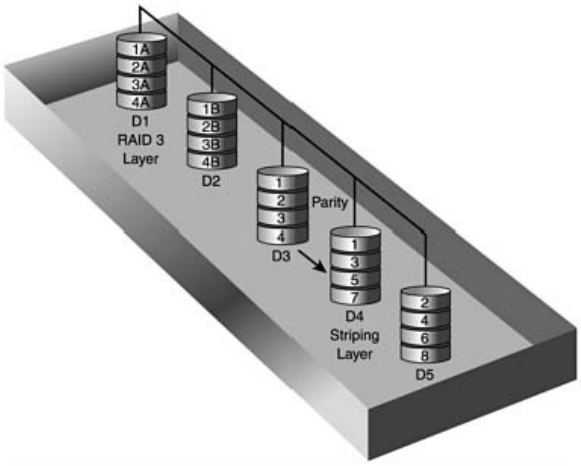


RAID 5 **RAID 5**

3.4.10 RAID 53 (5+3)

Este tipo ofrece un conjunto de bandas en el cual cada banda es un conjunto de discos RAID-3. Esto proporciona mejor rendimiento que el RAID-3, pero a un costo mucho mayor.

Pero de todos estos los que más destacan son los niveles 0, 1, 3,5, y 10 o RAID 0&1. Todos los demás vienen siendo variaciones de estos últimos.



4 CONCEPTOS RELATIVOS A BACKUP

Un backup permite que los datos y los archivos de sistema de una computadora sean archivados en otra ubicación en el disco duro u otro medio de almacenamiento. Cuando un problema ocurre, los archivos resguardados pueden ser restaurados a la ubicación desde donde fueron originalmente copiados o a otra ubicación, como ser un directorio o una maquina distinta.

Realizar backups y restaurar los datos es una parte fundamental de cualquier plan de recuperación de desastres. Un plan de backup da detalles acerca de que se debe backupear, como será backupeado y cuando.

En relación a que backupear, debe incluirse cualquier dato sensible que maneje una compañía como ser bases de datos, archivos de registro, correo electrónico, etc. Las aplicaciones y los archivos temporales no formaran parte del mismo debido a que pueden ser reinstaladas fácilmente.

Es importante realizar un resguardo del servidor por completo en el evento de que este fallara y quedara inutilizable.

Por razones de practicidad se utilizan otros medios que el mismo disco rígido del servidor para hacer las copias de seguridad, ya que si este falla perderemos también los datos resguardados. Esos medios podrán ser cintas y se recomienda hacer tres copias, una de las cuales será almacenada fuera de la oficina, por si un incendio destruye las dos copias. Asimismo por razones de seguridad deberán ser almacenadas en lugares seguros fuera del alcance de personas inescrupulosas.

Es necesario realizar restauraciones de prueba periódicas con el fin de comprobar el correcto funcionamiento de las mismas.

4.1 MEDIOS

Hay muchos tipos diferentes de medios en los cuales los datos resguardados pueden ser almacenados. El tipo que uno elija determinara cuantos datos pueden ser almacenados en un solo medio y la velocidad a la que será resguardado. Al elegir el medio se debería estimar cuantos datos serán copiados durante el backup.

Se puede backupear a disco, cinta, CD-R/W, DVD-R/W o una SAN (Storage Area Network), la cual podrá tener como miembros a Bibliotecas de cintas o cargadores. Los medios ópticos si bien están dentro de las alternativas mencionadas tienen una capacidad que va desde los 650 MB a los 8 GB, siendo esto inaceptable para la cantidad de datos que un servidor actual maneja, estando relegados a las copias de seguridad locales de las estaciones de trabajo.

4.1.1 CINTAS

De los diferentes medios disponibles, las cintas son los más ampliamente difundidos. Las cintas son cintas magnéticas similares a las utilizadas en un grabador de casette.

La mayor ventaja de este medio es el costo, se puede almacenar más datos en cinta por un costo menor que otro medio

Los tipos más comunes de cintas son:

- Digital Audio Tape (DAT)
- Digital Linear Tape (DLT)
- Súper DLT
- LTO Ultrium

4.1.1.1 DAT:

Almacena datos en cintas de 4 mm. Es un medio muy popular debido a su costo menor que DLT.

Usa el formato de almacenamiento Digital Data Storage (DDS), el cual usa un proceso similar al de las VCR para almacenar datos, hace una búsqueda helicoidal, en el cual las cabezas de escritura / lectura giran diagonalmente a lo largo de la cinta DAT. Se usan dos cabezas de escritura y dos cabezas de lectura .Cuando se escriben los datos las cabezas de lectura verifican que los datos hayan sido escritos correctamente a la cinta. Si detectan cualquier error los datos son reescritos, como se ve hay varios formatos de DDS disponibles para cintas:

Tipo de formato	Capacidad de Almacenamiento
DDS	2 GB
DDS-1	2/4 GB
DDS-2	4/8 GB
DDS-3	12/24 GB
DDS-4	20/40 GB

Los datos en el formato original estaban sin comprimir, de manera que se podían almacenar menos datos que los demás medios. DDS-1 fue el primer formato en soportar compresión y permite almacenar hasta 4 GB en un cartucho de120 minutos. DDS-2 lo elevo a 8 GB. DDS-3 usan un cartucho de 125 minutos y permite almacenar hasta 24 GB de datos comprimidos. Este formato también introdujo el uso de Partial Response Maximum Likelihood (PRML), el cual elimina ruidos de manera tal que los datos sean transferidos a la cinta más limpios y con menos errores. Finalmente DDS-4 permite que 40 GB de datos comprimidos se almacenen en un cartucho de 125 minutos

Todos estos formatos con compatibles hacia atrás, o sea que si se tiene un dispositivo DDS-3 se pueden usar cartuchos DDS-1 Y DDS-2.

4.1.1.2 DLT

DLT es más rápido que DAT, y proporciona una capacidad mayor de almacenamiento. Almacena los datos en una cinta de 0.25 pulgadas del tipo reel a reel, donde un reel esta en el cartucho y el otro dentro del dispositivo.

Se ve a continuación las diferentes generaciones de DLT:

Tipo DLT	Capacidad de Almacenamiento
DLT2000	15/30 GB
DLT4000	20/40 GB
DLT7000	35/70 GB
DLT8000	40/80 GB

A diferencia de DDS, cada versión de DLT brinda compresión, como ejemplo DLT2000 sin compresión almacena 15 GB y comprimido 30 GB.

4.1.1.3 SUPER DLT

Las cintas SDLT están optimizadas para almacenar, archivar y backupear grandes volúmenes de datos en ambientes de rango medio

Las capacidades son 2:

- SDLT 1 320 GB
- SDLT 2 600 GB

El **SDLT 1** tiene una capacidad nativa de 160 GB y comprimido (2:1) 320 GB. Tiene una transferencia de datos nativa de 16 MB/seg. (57,6 GB/Hora).

El **SDLT 2** puede almacenar de forma predeterminada 300 GB y comprimido (2:1) 600 GB, transfiriendo 36 MB/seg. (126, 5 GB/Hora)

Ambas versiones suponen una vida útil de alrededor de 1.000.000 de pasadas y/o 30 años de archivo.

Soportan la configuración para trabajar en modo WORM (Write Once Read Many), ideal para archivo.

Los dispositivos de grabación tienen interfaces Ultra 160 SCSI y en algunos casos Fibre Channel

4.1.1.4 LTO ULTRIUM

A medida que las bases de datos requieren mayor almacenamiento y las aplicaciones críticas demandan menores tiempos de downtime, debido a las operaciones de backup, se necesitan soluciones más efectivas. Los cartuchos LTO Ultrium con capacidad nativa de 400 GB y 800 GB comprimidas a 2:1, son una solución para este problema. Su tasa de transferencia es de 80/160 MB/seg. (2:1) Y 40/80 MB/Seg.

Tecnología de disco basada en un standard abierto que brinda compatibilidad de medios entre las diferentes marcas de productos LTO Ultrium.

Las versiones disponibles al momento son:

Tipo	Capacidad
LTO Ultrium1	100/200 GB
LTO Ultrium2	200/400 GB
LTO Ultrium3	400/800 GB

Existen cartuchos de limpieza (Cleaning Cartridge) que deben pasarse cada 15 a 50 ciclos para prevenir obstrucciones en el sistema de grabación

Los dispositivos de grabación disponen de interfaces UW-SCSI, USB 2.0 y Fibre Channel.

4.1.2 BIBLIOTECAS DE CINTAS (TAPE LIBRARIES)

Cuando es necesario alcanzar volúmenes de almacenamiento más allá de los límites de las cintas individuales están disponibles las Bibliotecas de Cintas conectados desde interfaz SCSI hasta SAN por fibra óptica, siendo estos últimos los que permiten una mayor transferencia de datos.

En algunos casos se montan en

Racks, como el caso de la figura ocupando 5 U.

También están disponibles en forma de torre.

Las capacidades van desde los 20 TB hasta cerca de 200 TB, con 264 cintas de LTO3 a 800 GB con compresión.

La transferencia de datos puede alcanzar los 2 TB/Hora.

4.1.3 STORAGE AREA NETWORK (SAN)

Conceptualmente una SAN puede ser pensada como una red independiente de dispositivos de almacenamiento físicamente separados pero conectados a la red.

SAN evoluciono a partir de quitar dispositivos de almacenamiento, y por consiguiente el trafico de almacenamiento fuera de la LAN y crear una red separada dedicada específicamente a los datos.

Los usuarios obtienen acceso a estos dispositivos de almacenamiento a través de sistemas servidor los cuales están conectados tanto a la LAN como a la SAN.

Esto es en oposición al uso tradicional de una LAN para brindar conexión al servidor de almacenamiento, una estrategia que limita el ancho de banda total de la red. Las SAN tratan con los cuellos de botella asociados con el almacenamiento basado en Server LAN y la limitación de escalabilidad encontrada en sistemas de implementación de bus SCSI.

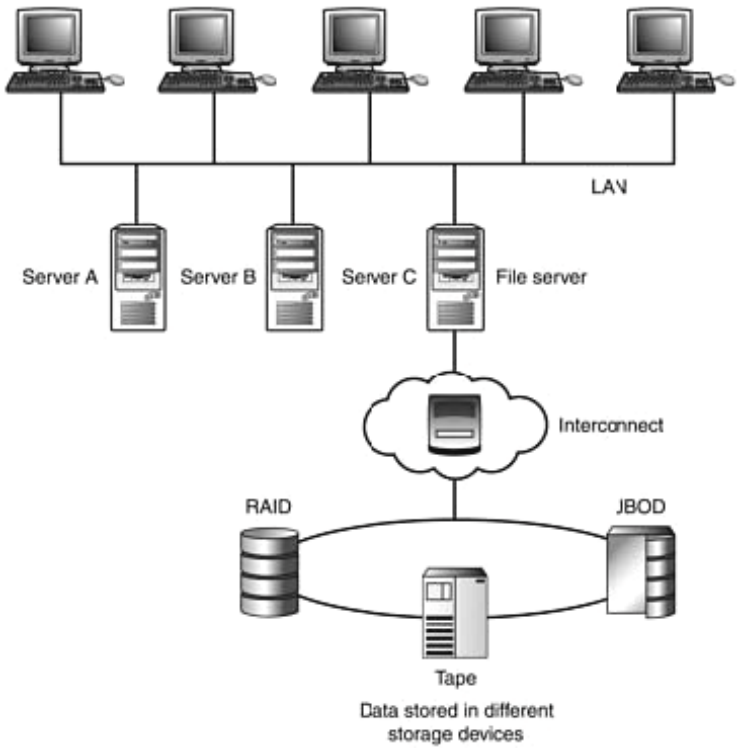
Las ventajas de SAN son numerosas, pero tal vez uno de los mejores ejemplos es aquel del backup sin Server. Este sistema permite a un dispositivo de almacenamiento de disco copiar datos directamente a un dispositivo de backup a través de los vínculos de alta velocidad de la SAN sin ninguna intervención del servidor. Los datos son mantenidos en la SAN, lo que dignifica que los datos no contaminan la LAN y los recursos del servidor están disponibles para los clientes.

Las SAN son comúnmente implementadas usando una tecnología llamada Fibre Channel, que define una tecnología de alta performance de comunicaciones que soporta transferencia de datos muy altas, alrededor de 2 GBPS. Fibre Channel puede ser usado en una configuración punto-a-punto entre dos dispositivos, en una configuración de anillo y un modelo llamado fabrica.

Los dispositivos en la SAN están conectados juntos a través de un switch especial, el cual lleva a cabo las mismas funciones que un switch Ethernet en el hecho de que actúa como un punto de conectividad entre los dispositivos. Como Fibre Channel es una tecnología conmutada puede brindar una ruta dedicada entre dispositivos en la fábrica de manera que usen todo el ancho de banda durante la comunicación.

Los dispositivos de almacenamiento están conectados al switch usando tanto cable de fibra óptica multimodo o monomodo. Multimodo brinda distancias de hasta 2 Km., monomodo 10 km.

En los dispositivos de almacenamiento en si hay interfaces Fibre Channel que brindan la conectividad



4.1.4 iSCSI

Muchos tipos de protocolos SCSI han evolucionado a través de los años: SCSI-1, SCSI-2, SCSI-3, Ultra 2 SCSI, Ultra 3 SCSI y Serial Attached SCSI para nombrar solo unos pocos. Los protocolos SCSI son estándares que existen para definir como los datos son transferidos desde el Server hasta el arreglo de discos. Hasta la llegada de iSCSI, que significa Internet Small Computer Systems Interface, llegara no era posible transferir datos SCSI mas allá de los 25 metros entre el Server y el arreglo de discos.

Con la creación de las SAN fue uno de los propósitos el de tener el almacenamiento lejos de los servidores. Debido a la limitación de distancia de SCSI se debió desarrollar nuevos mecanismos como por ejemplo Fibre Channel, estas conexiones pueden llegar hasta 10 Kilómetros. Esto puede llegar a ser incantable para algunas organizaciones, allí es donde iSCSI tiene lugar.

En esencia donde quiera que una red IP pueda llegar allí puede legar iSCSI.

El potencial de esta tecnología para los escenarios de recuperación de desastres es enorme. Con los sistemas de almacenamiento lejos del sitio original, no hay peligro que se dañen los datos durante un evento catastrófico.

Es una tecnología que promete mucho pero aun debe resolver temas como la latencia debida a los enlaces entre los sitios y la seguridad en la transmisión.

4.2 ORGANIZACIÓN DE LOS MEDIOS

Los backups deben estar organizados de manera tal que se entienda claramente que se ha backupeado, cuando y donde esta actualmente almacenado. Si no es administrado correctamente, las cintas se pueden perder, borradas accidentalmente o sobre-escritas. Debe escribirse en ellas la fecha y la versión del backup .Documentar la fecha también proporciona información de cuantas veces una determinada cinta ha sido utilizada y así controlar de no sobrepasar el limite indicado por el fabricante.

No es muy inteligente tener todos los medios de backup en el mismo sitio y en especial en la sala de servidores donde se ha backupeado la información, pueden ser destruidas simultáneamente por un incendio, por ejemplo.

4.2.1 ALMACENAMIENTO FUERA DEL SITIO

Una de las copias estará mas segura fuera de la oficina, por ejemplo si la empresa tiene varios edificios pueden almacenarse allí o sino en empresas que proporcionan el servicio de almacenamiento.

La clave es mantener las copias lejos de la ubicación original de los datos resguardados.

4.3 BACKUP SET

Un juego de backup es simplemente una colección de archivos y/o carpetas que se quieren backupear conjuntamente.

4.4 MEDIA SET

Un conjunto de medios o Media Set es un grupo ordenado de medios de backup, cintas o archivos en disco, en los cuales una o más operaciones de backup han sido escritas. Un media ser dado usa ya sea unidades de disco o dispositivos de disco pero no ambos.

4.5 ARCHIVOS ABIERTOS (OPEN FILES)

Los archivos abiertos son aquellos que normalmente son saltados durante la operación de backup. Esto ocurre generalmente porque los archivos están bloqueados por un servicio o una aplicación, como ser un sistema operativo, programa de procesador de texto o una aplicación de base de datos.

Es conveniente al adquirir un software de backup hacerlo con aquellos que soporten el tratamiento de esos archivos abiertos aprovechándose de características especiales del sistema operativo, como es el caso de Volume Shadow Copy en Windows Server 2003, tema que trataremos en detalle en clases siguientes.

5 TIPOS DE BACKUP

La programación de la copia de restauración es tal vez la consideración más importante cuando se planea una recuperación de desastre.

El tipo de backup que se hará tiene relación directa con la estrategia de recuperación de los datos. Un plan de backup asume un plan de restauración. Se deberían documentar y probar todos los procesos y tiempos que toman restaurar un servidor de datos.

Los tipos fundamentales de backup son:

- ✓ Total (Full) o Normal
- ✓ Incremental
- ✓ Diferencial
- ✓ Copia
- ✓ Diario

Antes de describir cada tipo de backup, es importante comprender que los tipos elegidos afectaran como ***el atributo de archivo*** es manejado.

El ***atributo de archivo*** es una propiedad de un archivo o carpeta que es usado para indicar si un archivo ha cambiado desde la última vez que fue backupeado Cuando el archivo es modificado el ***atributo de archivo*** es seteado de nuevo, para indicar que ha cambiado y que debe ser backupeado de nuevo.

Sin el ***atributo de archivo,*** la utilidad de backup es incapaz de decir si los archivos necesitan ser backupeados o no.

5.1 BACKUP TOTAL

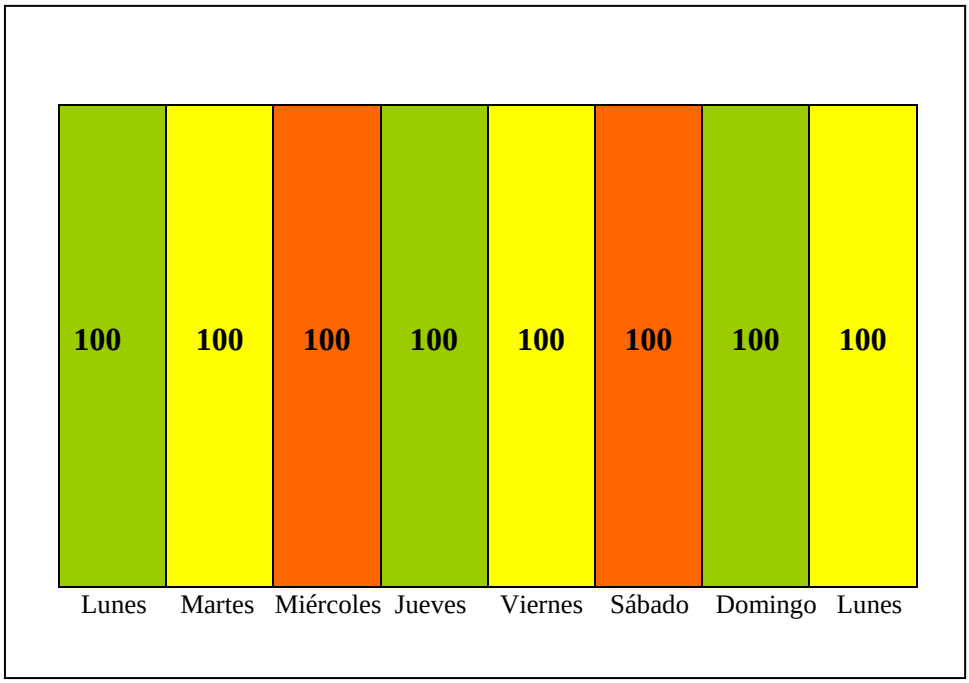
Los backups totales son la base de los demás esquemas y contienen todos los datos en un sistema

A este método también se lo conoce como Normal. Cuando se selecciona este tipo de backup, la utilidad de backup backupea **los archivos seleccionados** a disco o a cinta, ignorando si el ***atributo de archivo*** esta habilitado o deshabilitado .En otras palabras, no importa si un archivo ha sido backupeado antes, será backupeado ahora. Después de backupear el archivo, este cambia el ***atributo de archivo*** para indicar que ha sido backupeado.

Este tipo de backup es el usado inicialmente en un servidor, toma mucho tiempo, porque backupea todos los archivos y carpeta sin importar el estado del ***atributo de archivo.*** En algunos casos, debido a la cantidad de datos que involucra podría ocupar varios medios de almacenamiento.

La principal ventaja de este tipo de backup es la habilidad para rápidamente restaurar los datos, toda la información necesaria esta en un solo juego de backup, su desventaja es el tiempo consumido y la gran cantidad de cintas involucradas.

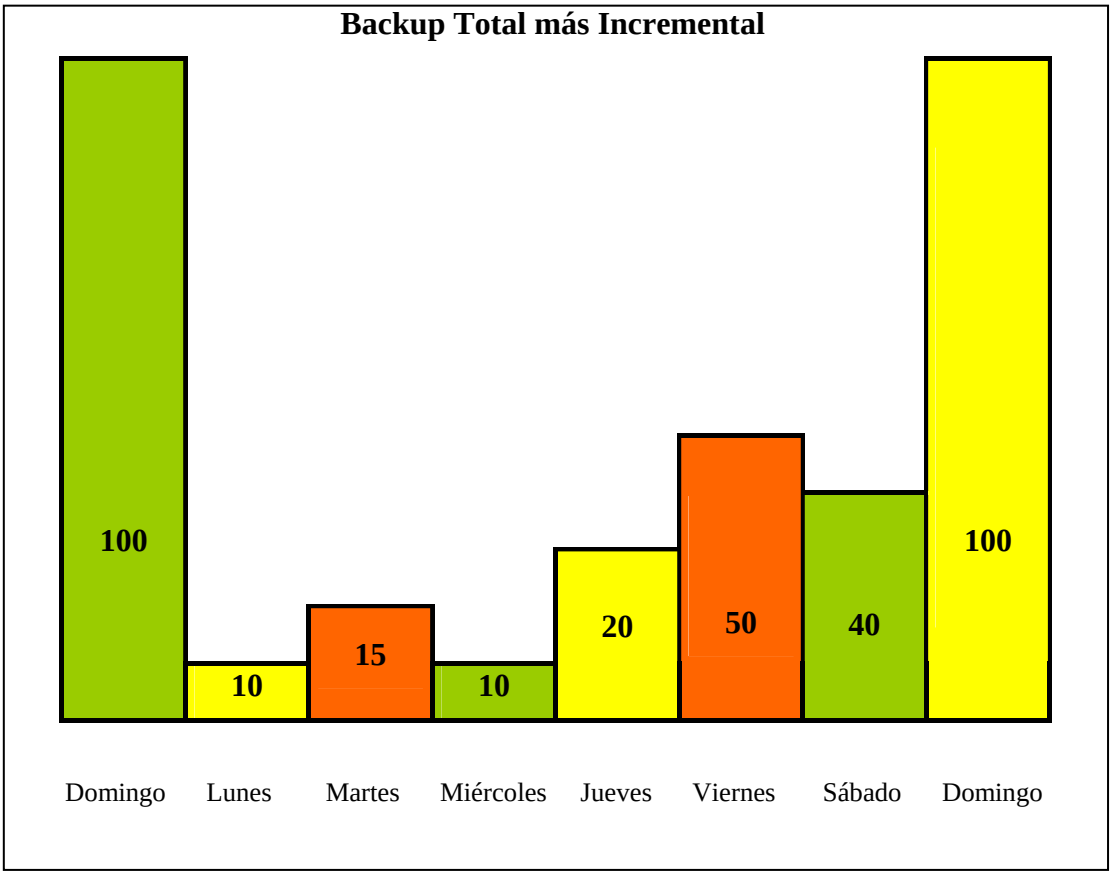
Escenario de un Backup Total



5.2 BACKUP INCREMENTAL

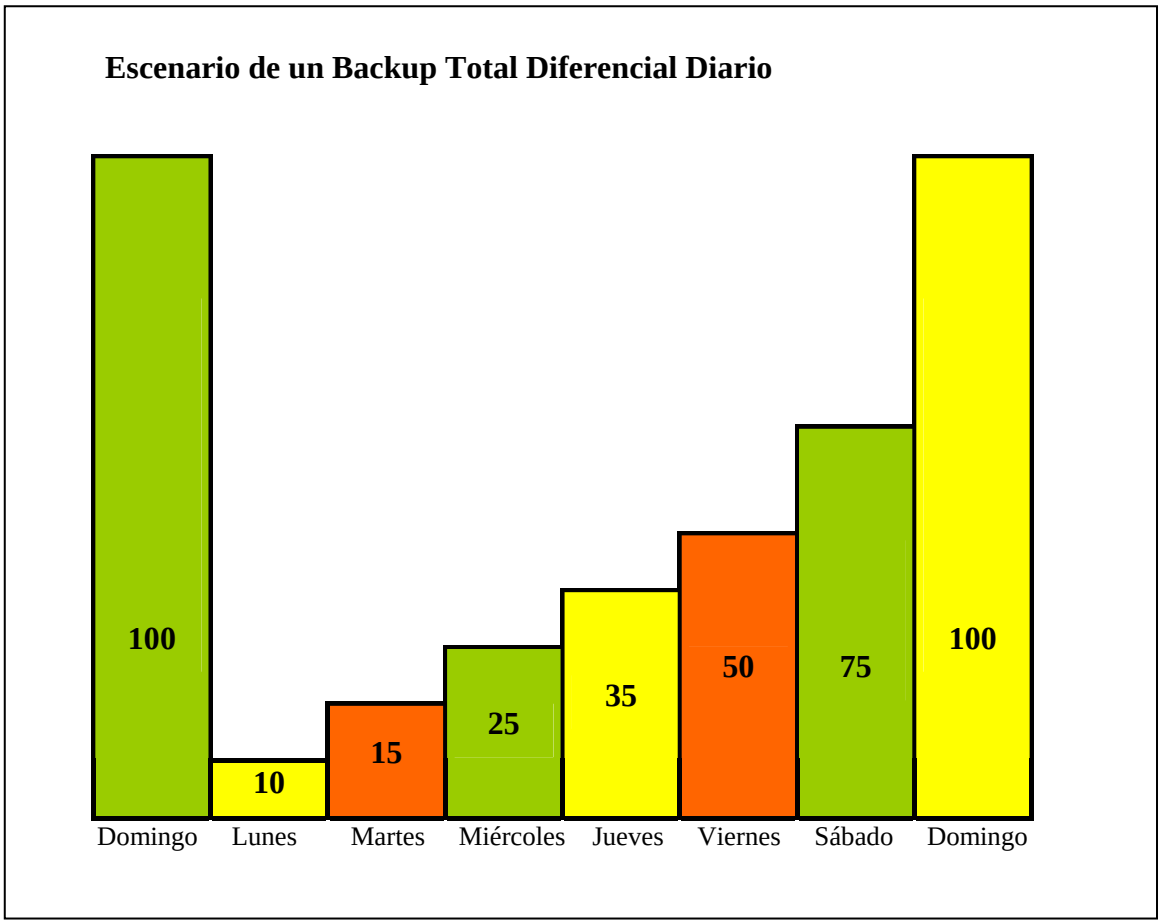
Se utiliza para backupear todos los archivos que han cambiado desde el último backup Normal o Incremental. Cuando cada archivo es backupeado el atributo de archivo se deshabilita. Como solo los archivos que han cambiado se backupean, este tipo de backup toma el menor tiempo de todos para llevarse a cabo. Sin embargo toma la mayor cantidad de tiempo en el momento de restaurar porque el ultimo backup normal y los subsecuentes backups incrementales deben ser restaurados para tener los datos lo mas actualizados posible.

Generalmente se usa entre backups normales. Su principal ventaja es el tiempo reducido que lleva hacerlo así como la reducida cantidad de cintas involucradas. Su desventaja son las operaciones más largas y más complejas de restauración mas aun si hay periodos largos entres backups normales.



5.3 BACKUP DIFERENCIAL

Se utiliza para resguardar los archivos que han cambiado desde el último backup normal o incremental. Sin embargo cuando este tipo de backup es realizado el bit de archivo no se ha deshabilitado. Esto significa que los datos en un backup diferencial contienen la misma información que los diferenciales previos más los archivos adicionales que han cambiado. Como los datos sin cambiar son continuamente backupeados con este método, los backups diferenciales llevan mas tiempo que los incrementales. Sin embargo cuando se restauran datos, solo el último backup normal y el último diferencial serán necesarios para devolver al sistema al punto mas reciente.



5.4 COPIA

Es similar al normal en que pueden ser restaurados a partir de un único trabajo de backup, pero difieren en que una copia no cambia el atributo de archivo.Como el atributo no es modificado, no afecta ningún backup incremental ni diferencial que sean ejecutados luego. Útil si requiere hacer una copia de datos pero no interferir con otras operaciones de backup.

5.5 DIARIO

Su finalidad es la de backupear todos los datos que han sido modificados en un día particular. Los archivos que no han sido modificados ese día no son backupeados. Tampoco afectan los atributos de archivo y no interfieren con los backups incremental o diferencial

6 ESQUEMAS DE ROTACION

Si se utilizan cintas durante un backup la forma en que estas se reutilizan durante el ciclo de backup es una consideración importante. Al rotar las cintas uno se asegura que las versiones de los datos estén siempre disponibles en cinta y esas cintas están protegidas de excesivo uso y daño.

Un error común de los administradores es no retira de uso las cintas luego de un determinado ciclo, es importante seguir las recomendaciones de los fabricantes acerca de su vida útil

Las estrategias de rotación de cintas difieren en cuanto al número de cintas requeridas y el tiempo que el medio es mantenido antes de ser rotado en el esquema. También difieren en como los medios son sacados de la rotación y archivados. Dos esquemas muy comunes de rotación son ***GFS (Grandfather-Father-Son) o Abuelo-Padre-Hijo y Tower of Hanoi o Torre de Hanoi.***

6.1 ABUELO-PADRE-HIJO

Requiere de 20 cintas, asumiendo un esquema de backups de 5 días. Las cintas son usadas y etiquetadas de la siguiente forma:

- **Cuatro cintas (Hijos)** son usadas para realizar Backups incrementales o diferenciales y son etiquetadas con los días de la semana, por ejemplo lunes, martes, miércoles, jueves Cada cinta es reusada cada semana el día que esta etiquetado .Estas cintas son típicamente almacenadas en sitio.
- **Cuatro cintas (Padres)** son usadas para llevar a cabo Backups totales semanales en el día en que una cinta Hijo no es usada, siguiendo el esquema anterior seria el viernes. Son etiquetadas como Semana 1, Semana 2, Semana 3 y Semana 4. Estas cintas son re utilizadas mensualmente y se pueden almacenar en sitio o fuera de el.
- **Doce cintas (Abuelos)** son usadas para llevar a cabo Backups Totales en el último día laboral de cada mes y son etiquetadas con el mes y el año, por ejemplo Mes 1/2006, Mes 2/2006, etc. Las cintas mensuales pueden ser archivadas en forma permanente o reusadas cada cuatro meses o en forma anual, dependiendo de los requerimientos de cada empresa. Estas cintas son almacenadas fuera de sitio.

Si un backup excede la capacidad de una cinta se denomina Backup Set y debe ser etiquetado y tratado como un mismo backup.

En la siguiente tabla vemos un esquema de rotación GFS donde el primer mes termina en un miércoles y el segundo en un viernes:

Lunes	Martes	Miércoles	Jueves	Viernes
				Semana1
Lun	Mar	Mier	Jue	Semana2
Lun	Mar	Mier	Jue	Semana3
Lun	Mar	Mier	Jue	Semana4
Lun	Mar	Mes1/2006	Jue	Semana1
Lun	Mar	Mier	Jue	Semana2
Lun	Mar	Mier	Jue	Semana3
Lun	Mar	Mier	Jue	Semana4
Lun	Mar	Mier	Jue	Mes 2/2006

6.2 TORRE DE HANOI

Este esquema es un poco más complejo

Utiliza cinco backups totales y son etiquetados como A, B, C, D y E.

Iniciando en día 1 se hace un backup total usando en conjunto A, este puede ser usado en base diaria pero nunca dos días seguidos. Debe usarse después de otro conjunto. Luego sigue el B, se usa en el primer día que no se hace un backup con el conjunto A y se repite cada 4 sesiones. El grupo C comienza en el primer día que no se usa ni A ni B y se repite cada 8 sesiones. El conjunto D se usa en el primer día que no se usa ni A ni B ni C y se repite cada 16 sesiones. Se puede aumentar la historia de un backup si se agrega un conjunto de cintas mas, E, en el primer día que no se usan las demás y repitiendo cada 32 sesiones.

Lunes	Martes	Miércoles	Jueves	Viernes
Cinta A	Cinta B	Cinta A	Cinta C	Cinta A
Cinta B	Cinta A	Cinta D	Cinta A	Cinta B
Cinta A	Cinta C	Cinta A	Cinta B	Cinta A
Cinta E	Cinta A	Cinta B	Cinta A	Cinta C
Cinta A	Cinta B	Cinta A		

Aunque mas complejo es un sistema que involucra menos costos desde el lado de las cintas. La desventaja es que es un esquema muy difícil de seguir.

NOTAS

CUESTIONARIO CAPITULO 1

1.- ¿Cómo definiría un desastre informático?

2.- ¿Qué nivel o niveles de RAID implementaría para un servidor de bases de datos?

3.- ¿De que depende la elección del medio de almacenamiento?

4.- ¿Qué diferencia hay entre un Backup Incremental y uno Diferencial?

5.- ¿Con que objeto se debe seguir un esquema de rotación de cintas?