UT4: Hardware y almacenamiento.3ª Parte.

1º Curso CFGM SMR

Índice.

7. Recuperación de datos: copias de seguridad.

- Hoy en día empresas y particulares almacenamos grandes cantidades de información en nuestros equipos.
- Protegemos la información contra ataques lógicos pero ¿hacemos copias de seguridad?
- Ejemplos:
  - Incendio en el DC de SAMSUMG abril 2014
  - http://www.datacenterdynamics.es/focus/archive/2014/04/un-incendio-en-un-dc-de-samsung-provoca-errores-nivel-mundial

7. Recuperación de datos: copias de seguridad.

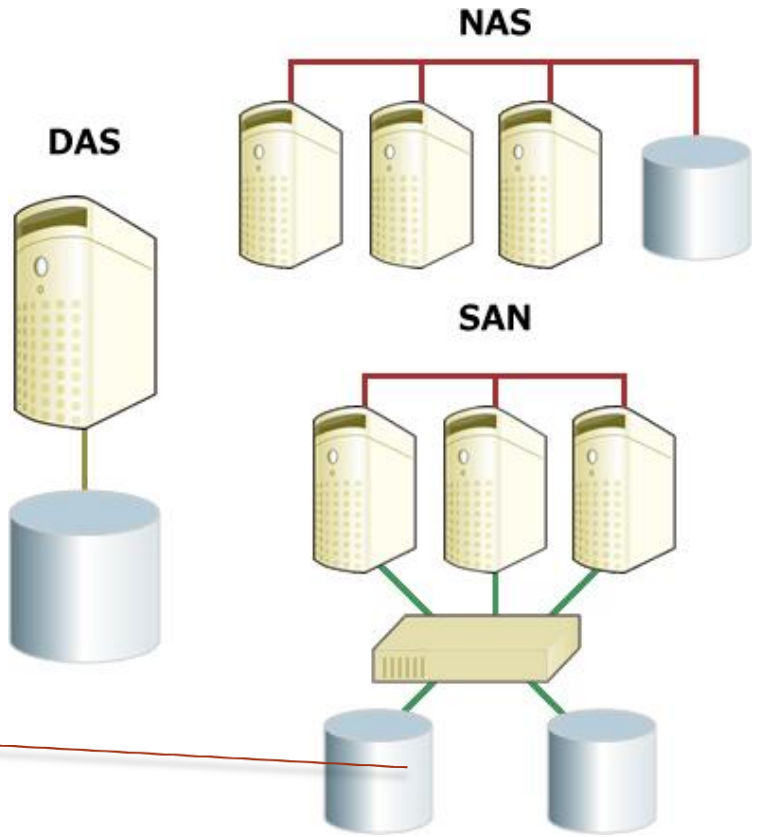
- …Aunque el incendio se prolongó unas siete horas, las incidencias ocasionadas fueron resultas con rapidez por parte de la firma. Al parecer, el centro de datos de Gwacheon funciona como backup de su sitio principal, ubicado en Suwon. Como medida de precaución, se trasladaron los datos almacenados hacia el otro data center, de ahí que los servicios no funcionaran con total normalidad.

7. Recuperación de datos: copias de seguridad.

- **Backup o copia de seguridad:**
  - **Backup, copia de seguridad o respaldo:** *Réplicas de datos que nos permiten recuperar la información original en caso de ser necesario.*
  - **¿Qué se debe copiar?** será preciso clasificar la información a replicar según criticidad. Archivos difíciles o imposibles de reemplazar.
  - **¿Quién y dónde se realizará la copia?** Elegir el **dispositivo sobre el que se hará la copia**: cintas (DAT, DLT, DDS, LTO, …), CD/DVD, dispositivos USB, discos SSD, backup offsite…NUNCA EN EL MISMO DISCO DONDE SE ENCUENTRE LA INFORMACIÓN!!!!!!
  - **¿Con qué frecuencia y de qué tipo?** Elección de una política (frecuencia y tipo del backup).

7. Recuperación de datos: copias de seguridad.

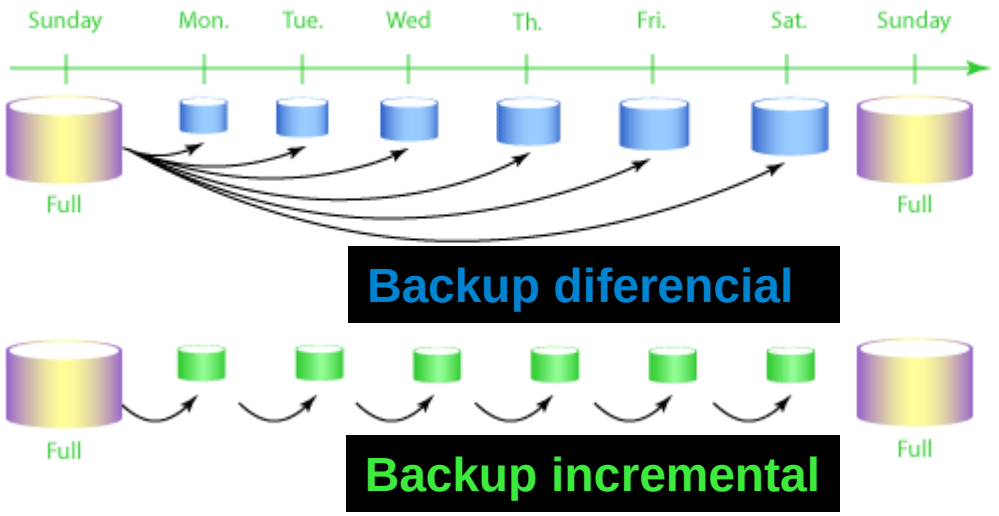
- Modelos de almacenamiento masivo:
  - **DAS** Direct Attached Storage
  - **NAS** Network Attached Storage
  - **SAN** Storage Area Network



De todo esto hay que hacer backup!! Aunque los discos estén en RAID1 o RAID5, si ocurre una catástrofe, los datos se perderán. Por eso, además, es necesario el backup.

8. Políticas de copias de seguridad.

- Dependiendo de qué ficheros copiemos tendremos diferentes tipos de backups:
  - **Backup Full (nivel 0)** completo, íntegro o total. Copiamos todos los datos (todos los directorios y todos los archivos).
  - **Backup Incremental (nivel 1)** copia solo los que han cambiado desde el último backup, sea del tipo que sea, total o sólo de las modificaciones.
  - **Backup diferencial (nivel 2),** copia archivos modificados desde el último total.



8. Políticas de copias de seguridad.

¿Qué necesitamos para restaurar una copia en cada caso?

Método de copia	Espacio de almacenamiento	Velocidad de copia	Restauración	Copia recomendada
Completo	Máximo	Muy lento	Muy simple	Pocos datos a copiar
Completo + incremental	Mínimo	Rápido	Compleja	Muchos datos que cambian frecuentemente
Completo + diferencial	Intermedio	Lento	Sencilla	Datos cuya velocidad de cambio es moderada.

Objetivo: → **Disponer de una copia de seguridad diaria**

Buenas prácticas ...

- ✓No realizar backup sobre el mismo disco del cual tomamos los datos.
- ✓Proteger los soportes contra escritura.
- ✓No reutilizar eternamente los dispositivos.
- ✓Almacenar los soportes en una ubicación diferente.
- ✓Realizar las copias en horas en las que no se está trabajando.
- ✓Etiquetar correctamente los soportes (ver etiqueta para soporte)
- ✓Comprobar que los backups se han realizado correctamente (ver hoja de registro)
- ✓Comprobar periódicamente el estado de las copias (realizar restauraciones aleatorias).
- ✓Mantener hoja de registro de restauraciones.

Ejemplo Diciembre:

Modelo de 16 cintas (diarias)+ 3 cintas (semanales)+ 12 cintas (mensuales)+ 5 cintas (anuales)

22:00	LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	Cintas camión
SEMANA1 mes 12 año 14	Lunes-S1-INC	Martes-S1- INC	Miercoles-S1-INC	Jueves-S1-INC	SEMANA1-TOTAL	Lunes-S1-INC, Martes-S1 INC, Miercoles-S1 INC, Jueves-S1 INC, SEMANA1 TOTAL
SEMANA2	Lunes-S2-INC	Martes-S2- INC	Miercoles-S2-INC	Jueves-S2-INC	SEMANA2-TOTAL	
SEMANA3	Lunes-S3-INC	Martes-S3- INC	Miercoles-S3-INC	Jueves-S3-INC	SEMANA3-TOTAL	
SEMANA4	Lunes-S4-INC	Martes-s4-iNC	Miercoles-S4-INC	Jueves-S4-INC	MES12_14-TOTAL y ANIO14-TOTAL	
Semana 1 mes 1 año 15	Lunes-S1-INC					

-Todos los días laborales se hace un backup incremental a las 22.00h.
-Todos los fines de semana se hace un backup completo.
-Las cintas se guardan:
- -Las diarias durante un mes. Pasado un mes se vuelven a reutilizar.
- -Las del fin de semana se guardan un mes. Pasado el mes se reúsan.
- -El último fin de semana de cada mes, se hace un total que se guarda durante un año.
- -Al final de año se hace un total que se guarda durante 5 años.

-Cada lunes una empresa externa transportará las cintas de la semana en armarios ignífugos a la localización remota. Y devuelve las cintas de la semana anterior.

8. Políticas de copias de seguridad.

- Será más fácil cuanto más cercano en el tiempo sea el archivo a recuperar.
- Será necesario realizar restauraciones aleatorias y con cierta frecuencia para comprobar la fiabilidad de los backups.
- Este tipo de prácticas se incluyen en las auditorías de seguridad informática.
- El procedimiento a seguir en una restauración será:
  1. Localizar la cinta que contiene los datos.
  2. Si está en la oficina, se restaura.
  3. Si no está en la oficina, se solicita a la empresa de custodia la caja que incluya la cinta necesaria.
  4. Se restaura el archivo solicitado y se devuelve.

Almacenamiento remoto

- Actualmente, las empresas que desean garantizar la seguridad de sus datos y no cuentan con servidores externos propios, comienzan a usar la llamada cloud computing, en español
- computación en la nube o nube de cómputo,
- o una red de servicios accesible a través de internet.
- Uno de esos servicios es el almacenamiento de la información.

Almacenamiento remoto

- Mediante la nube de cómputo, todos los programas y datos que manejamos están almacenados permanentemente en servidores de internet, normalmente situados en grandes centros de datos.
- Para contar con este tipo de almacenamiento es necesaria una conexión de banda ancha.
- Se deberá buscar un adecuado proveedor del servicio, que ofrezca las garantías necesarias y las condiciones de uso nos sean favorables, teniendo en cuenta que dejamos nuestros datos en servidores de terceros.

Almacenamiento remoto

- Ejemplos de almacenamiento remoto o la nube:

Herramientas de copias de seguridad.

- *Herramientas para:*
  - *Copiar datos.*
  - *Imágenes del SO.*
  - *Copia del SO.*
- *Opciones a tener en cuenta en una herramienta de copia de seguridad:*
  - Compresión.
  - Duplicado.
  - Tipo de copia.
  - Cifrado.
  - Nombre de archivo.
  - Planificación o automatización de la tarea.

Herramientas de copias de seguridad.

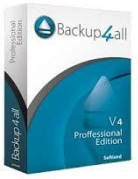
- **Copias de seguridad con herramientas del sistema:**

  - **GNU/Linux:**
    - Modo comando tar: empaquetar.
    - Comando cron: automatizar tarea.

  - **Windows:**
    - ✓ Herramienta preinstalada en el SO de Copias de seguridad.
    - ✓ Partición específica de datos. Mejora la recuperación.
    - ✓ Puntos de restauración.

Herramientas de copias de seguridad.

Copias de seguridad con herramientas específicas:



- Windows:
  - Backup4all: Todas las opciones a tener en cuenta están incluidas.
  - Backupmaker: Todas las funcionalidades, fácil de usar.
  - Fbackup: Con asistente y permite añadir plugings para copias de navegadores, clientes de correo, etc..
  - Toucan: Programa ligero y portable con la misma potencia que uno de escritorio.

- GNU/Linux:
  - BackupPC
  - BackInTime: Interfaz gráfica de rsync
  - Déjà Dup: Interfaz gráfica de duplicity, programa intuitivo.
  - FlyBack: Con asistente para configurar backups.
  - Pybackpack: Asistente para realizar copias con rsync.

Herramientas de copias de seguridad.

- Tar
  - Disponible en todas las versiones de UNIX/Linux.
  - Permite copiar archivos individuales o directorios completos en un único archivo.
  - Oficialmente fué diseñada para copiar ficheros en cinta, aunque ahora se puede volcar a casi cualquier soporte.
  - Desventaja: si falla el medio se pierde todo el archivo.

Tar (opciones) destino origen

Opción	Acción realizada
c	Crea un archivo .tar.
x	Extrae los archivos contenidos en el archivo .tar
t	Muestra el contenido del archivo .tar
f	Indica el nombre del archivo .tar
z	Comprime
v	Muestra los ficheros comprimidos.

Ejemplos:

tar -cvf /dev/rmt/0 /home
Vuelca /home a una unidad de cinta.

tar -cvf /tmp/backup.tar /etc
Vuelca /etc aun archivo en tmp.

tar -tvf /tmp/backup.tar
Muestra el contenido de /tmp/backup.tar

tar -xvf /tmp/backup.tar
Restaura el contenido de backup.tar.

Herramientas de copias de seguridad.

- **Recuperación de datos**:
- Cuando se borra un fichero de un medio de almacenamiento el sistema operativo marca aquellas posiciones que ocupaba dicho fichero en el dispositivo como libres, para almacenar nueva información, pero no las borra.
- Los datos permanecerán hasta que se sobrescriban con nueva información → Es posible recuperar mediante software.
  - Windows:
    - **Recuva, EASEUS Data Recovery Wizard Free Edition, PC-Inspector File Recovery, NTFS Reader.**
  - GNU/Linux:
    - **Testdisk, PhotoRec, Foremost, Scalpel.**