Seguridad física

Copia de seguridad y recuperación

ASO 2004/05

David Borrego Viñas

Índice

- Introducción
- Escenarios de pérdida de información
  - Costes
- Prevención: Plan de contingencia
- Realización de copias de seguridad
- Selección de soportes físicos y almacenamiento

Introducción

- La tarea principal de un administrador
  - Mantenimiento del sistema
  - ***Copias de seguridad***
- En cualquier momento algún archivo/s serán totalmente ilegibles por algún motivo:
  - Se exige capacidad de recuperación
- Las copias de seguridad dependen de la situación y es necesario determinar:
  - De qué archivos hacer la copia, dónde, cómo y cuándo

Escenarios de pérdida de información

Escenarios de pérdida de información

- Causas
  - Fuerzas mayores
    - Desastres naturales, electricidad estática, …
  - Errores de usuario
  - Virus y software destructivo
  - Personas malintencionadas
  - Fallo mecánico
- Costes

Escenarios de pérdida de información: Errores de usuario

- Comandos mal escritos

```
$rm foo *
```

- Errores en el redireccionamiento y uso de tuberías

```
$cat fstab|sed s'/ext2 /ext3' > fstab
```

- Usuarios con acceso de root
  - Los errores anteriores serían catastróficos si ocurrieran sobre directorios o archivos de sistema

Escenarios de pérdida de información: Errores de usuario

- Medidas de prevención sencillas
  - Utilizar alias

    ```
    Alias rm='rm -i'
    ```

  - Utilizar RCS o CVS: Sistema de control de versiones
    - Conservan el archivo original y lleva un histórico de los cambios realizados sobre este
  - Crear copias de seguridad personales
  - Utilizar sudo para limitar el acceso de los usuarios con privilegios de root
    - Se limitará el acceso únicamente a los comandos necesarios para que el usuario pueda llevar a cabo su tarea

Escenarios de pérdida de información: Virus y software destructivo

- Virus
  - Programa que se adhiere a otro ejecutable y trata de propagarse a otros y suele realizar otra acción (desde un mensaje hasta mezclar las tablas de particiones)
  - Linux dispone de funciones de seguridad que dificulta su propagación. Los usuarios no tienen control total del sistema como en windows

Escenarios de pérdida de información: Virus y software destructivo

- Caballos de Troya
  - Programa que se hace pasar por otro
  - Puede funcionar como éste, pero además realizar otras operaciones como obtener y enviar contraseñas
  - El grado de destrucción depende de quien lo ejecuta
- Gusanos
  - Programa que se aprovecha de las debilidades de un sistema para propagarse a otros.
- Software destructivo
  - Aplicaciones no mal intencionadas con errores de programación pueden ser muy dañinas

Escenarios de pérdida de información: Virus y software destructivo

- Medidas de prevención sencillas
  - Software de búsqueda de virus
  - Host víctimas
    - Se usan ciertos equipos para probar software nuevo asumiendo que puede resultar dañado
  - Software para verificar la integridad
    - Ej: Tripwire → controlador de integridad
  - Configuración del entorno
    - Asegurarse de que el directorio actual no esté incluido en la ruta de los programas de manera predeterminada

Escenarios de pérdida de información: Personas malintencionadas

- Crackers
  - Personas que entran en los sistemas de forma a veces ilegal con mejores o peores intenciones
- Usuarios descontentos
  - Usuario que tiene acceso al sistema y con recelo hacia la empresa por algún motivo
- Medidas preventivas
  - Cortafuegos y Seguridad Física para los crackers
  - Seguimiento de personas sospechosas de ser "usuarios descontentos" controlando sus accesos y sus privilegios

Escenarios de pérdida de información: Fallo de Hardware

- Fallo en la unidad de disco duro
  - El kernel suele avisar antes de un fallo completo
- Fallo de la memoria
  - Pérdida de información por la caída del sistema o información corrupta en memoria es copiada a disco
- Prevención y recuperación
  - Redundancia de la información→utilizar RAID
  - Supervisores de registros del sistema
  - Recuperación desde copias de seguridad
  - Intentar leer bloques para construir una imagen con 'dd'
  - Recuperación en entorno estéril → empresa dedicada

Escenarios de pérdida de información: Coste de la recuperación

- Costes directos
  - Sustitución de hardware
  - Coste de las copias de seguridad
    - Hardware, software y dispositivos de almacenamiento
- Costes indirectos
  - Tiempo del administrador de sistemas
  - Retrasos en los proyectos del administrador
  - Inactividad del sistema
- Resulta necesario establecer un plan en caso de desastre teniendo en cuenta estos costes

Prevención

Plan de contingencia

Prevención

- Ante cualquiera de los escenarios de pérdida de información debemos tener la capacidad de recuperarnos inmediatamente o en un corto lapso de tiempo.
- Para cultivar esta capacidad, debemos tener un plan de recuperación de desastres de antemano, incluso antes de instalar Linux
- Resulta muy útil la normalización para aumentar la habilidad para recuperarse y obtener una mayor flexibilidad a la hora de elegir las herramientas de copia de seguridad

Prevención
Normalización

- Normalización de hardware
  - Todos los hosts de la red con hardware idéntico (o muy compatible) expresamente soportado por Linux
  - No comprar paquetes poco convencionales ni con múltiples componentes
  - Construir paquetes para especificaciones concretas
  - Encontrar configuración que funcione bien y partir de ella
  - Ventajas:
    - Pocos proveedores
    - Número limitado de procedimientos de configuración, mantenimiento y actualización.

Prevención
Normalización

- Normalización de software
  - Definir claramente el propósito del host.
  - Establecer un conjunto de aplicaciones consistente
  - Instalarlas junto a programas o scripts relacionados
  - Realizar copia de seguridad del sistema de archivos
  - En Red Hat y otras distribuciones existen aplicaciones para realizar instalaciones a medida

Realización de copias de seguridad

Realización de copias de seguridad

- ¿De qúe archivos realizar la copia de seguridad?
- ¿Dónde? → Selección de dispositivos
- ¿Cómo implementarlo? → Estrategias
- ¿Con qué frecuencia realizarlas?

Realización de copias de seguridad: Contenido del sistema de archivos

- Qué archivos queremos copiar → contenido del sistema de archivos:
  - Archivos de configuración del sistema
    - /etc
  - Archivos de usuario
    - Archivos personales
  - Archivos orientados a tareas
    - Archivos de configuración y datos de programas específicos

Realización de copias de seguridad: Determinación de los dispositivos

- Linux soporta una gran variedad de dispositivos:
  - Unidades de cinta
  - Disquetera
  - Grabadoras CD o DVD
- Una vez elegido el dispositivo los comandos de copia de seguridad saben donde enviarlas.
- En el capítulo siguiente se tratará este tema con detenemiento

Realización de copias de seguridad: Frecuencia de las copias

- Es un factor que se debe decidir teniendo en cuenta:
  - Importancia y cantidad de datos
  - Variabilidad de los datos
  - Y aspectos específicos del host y del plan de recuperación de desastre que se haya diseñado

Realización de copias de seguridad: Estrategias

- Tipos de copias de seguridad:
  - Completas
  - Parciales
  - Incrementales

Realización de copias de seguridad: Copias de seguridad completas

- Se guardan todos los archivos asociados a una computadora
- La restauración necesita solo la última copia
- Comandos que realizan esta copia:
  - Comando dd:
    - La información se guarda como un solo fragmento que se restaura como una única entidad, no se pueden seleccionar archivos

```
dd if=/dev/hda2 of=/dev/nst0   → Copia
dd if=/dev/nst0 of=/dev/hda2   → Restauración
```

Realización de copias de seguridad: Copias de seguridad completas

- Comando dump:
  - Mismo efecto que dd pero ofrece la ventaja que el comando restore correspondiente permite elegir ficheros.
  - Además permite copias de subdirectorios individuales
  - Guarda sus acciones en /etc/dumpdates
  - Tiene varios niveles de copia (ver copias incrementales)

```
/sbin/dump 0uf /dev/nst0 /dev/hda2 → Copia
Restore i → Modo interactivo para la restauración
```

Realización de copias de seguridad: Copias de seguridad completas

- Comando tar:
  - Usado para empaquetar estructuras completas de directorios.
  - Usado para distribuir Linux
  - Puede usarse gzip para comprimir el empaquetado

```
tar –cvf ejemplo.tar * → Empaqueta el directorio actual

gzip ejemplo.tar  → Se genera ejemplo.tar.gz comprimido
```

Realización de copias de seguridad: Copias de seguridad completas

- Comando cpio:
  - Crea archivos de nuestros archivos y directorios para el transporte.

```
ls / | cpio –o > [dispositivo]

-- Obtiene el listado de directorios
-- Se introduce en cpio
-- cpio copia esta información en la salida estandar
-- La salida estandar se redirecciona hacia [dispositivo]
```

Realización de copias de seguridad: Copias de seguridad completas

- Las copias se pueden realizar también en máquinas remotas
- Desventajas de las copias de seguridad completas:
  - Tiempo requerido
  - Cantidad de espacio de almacenamiento
  - Repercusiones en el ancho de banda en copias remotas
  - Disminución del rendimiento de las máquinas implicadas en la copia

Realización de copias de seguridad: Copias de seguridad parciales

- Se copia sólo archivos específicos.
- Proceso de restauración sencillo
  - Sólo necesario restaurar los archivos del medio de almacenamiento
- Problemas
  - Nos dejamos archivos sin copiar.
  - La restauración completa lleva mucho tiempo y es muy susceptible de fallar

Realización de copias de seguridad: Copias de seguridad incrementales

- Se copian sólo los archivos que han cambiado desde la última copia, completa o incremental de mayor o igual nivel.
- Para recuperar el estado del sistema cuando se realizó la última copia incremental:
  - Se restaura la última copia completa
  - Se aplican las copias incrementales en el mismo orden en que fueron hechas
- Suponen menos espacio y menos tiempo

Realización de copias de seguridad: Copias de seguridad incrementales

- Nivel de una copia de seguridad incremental
  - Varían entre 0 (mayor prioridad) y 9 (menor prioridad)
  - Cada incremental de nivel n, realiza una copia de los archivos modificados desde la anterior copia en el mismo nivel o en un nivel mayor.
  - Para sacar rendimiento de este tipo de copia se define un calendario de rotación. Ejemplo:
    - Lunes: Copia de seguridad completa(nivel 0)
    - Martes-Viernes: Incremental de nivel 3
    - Sábado: Incremental de nivel 2
    - Domingo: Incremental de nivel 2

Realización de copias de seguridad: Scripts de copias de seguridad

- Podemos usar scripts para programar nuestras copias de seguridad.
- Estos scripts usarán de la manera que decidamos los comandos vistos anteriormente.
- Ejemplo:
  - Copia de seguridad de archivos modificados en los dos últimos días, exceptuando los que estén en /dev, /var/lock, /var/spool, /tmp y /proc en el archivo changed.tar

```
find / -path '/dev' -prune -o -path '/var/lock'  -prune -o -path '/var/spool'  -prune -o
  -path '/tmp' -prune -o -path '/proc'  -prune -o -type f -mtime 2 -print0 | tar -null -cvf
  changed.tar -files-from=.
```

Realización de copias de seguridad: Scripts de copias de seguridad

- Ejemplo:
  - Podemos usar para nuestros scripts los comandos dump/restore

/sbin/dump -0u -f /dev/nst0 /usr/src → Copia de nivel 0 de /usr/src

/sbin/dump -3u -f /dev/nst0 /usr/src → Copia de nivel 3 de /usr/src sólo archivos modificados desde la última copia de nivel 3 o superior

- Para la restauración usaremos restore en modo interactivo

  restore -if /dev/nst0

- Podremos restaurar total o parcialmente la copia

Realización de copias de seguridad: Sofware específico

- Se puede optar también por usar un software específico para la realización de las copias.
- Es necesario evaluar bien el programa antes de adquirirlo. A tener en cuenta:
  - Fiabilidad
  - Código abierto o marca registrada
  - Compatibilidad de sistemas y de medios

Selección de soportes físicos y almacenamiento

Soportes físicos de copias de seguridad

- Soportes físicos :
  - Unidades WORM
  - Unidades optico-magnéticas
  - Dispositivos de cinta SCSI
  - Dispositivos de cinta IDE
  - Unidades DVD
  - Grabadoras de CD
  - Dispositivos de cinta conectados a tarjetas controladoras de unidades de disquete.
- Nos centraremos en las unidades de cinta

Soportes físicos de copias de seguridad: Criterios de selección de dispositivos

- Coste
  - no solo del dispositivo sino también del soporte físico de almacenamiento .
- Soporte del kernel para el dispositivo
- Soporte para el dispositivo del software
- Capacidad de almacenamiento de datos de los soportes físicos
- Tasa de transferencia de datos para realizar copias de seguridad
- Mecanismo de cargador automático

Soportes físicos de copias de seguridad: Criterios de selección de dispositivos

- Mecanismo de cargador automático
  - Cuando se llena una cinta se inserta otra automáticamente
  - Permite las copias no supervisadas de grandes volúmenes
  - Importante el grado de soporte del software elegido para las copias con respecto al cargador automático.
  - El dispositivo debe incluir así mismo un mecanismo para el control del cargador automático

Soportes físicos de copias de seguridad: Criterios de selección de soportes

- Nos hemos decantado por las cintas pero para elegir un tipo debemos tener en cuenta:
  - Coste de los soportes físicos
  - Cantidad de información que se desea guardar
- Ejemplos:
  - Para grandes volúmenes se usa DLT
  - Para sitios pequeños 8 y 4 mm son recomendables

Soportes físicos de copias de seguridad: DDS de 4mm

- Surgen del formato digital de cintas de sonido
- Tienen una alta fidelidad
- Pueden almacenar desde 2(DDS 1) hasta 24(DDS 3) gigabytes
- Son pequeñas y silenciosas
- La cabeza lectora tiene una esperanza de vida corta
- Comparadas con las de 8mm, son menos fiables

Soportes físicos de copias de seguridad: Exabyte de 8 mm

- Utilizan el mismo mecanismo que una grabadora de video
- Son fiables y silenciosas
- Cintas baratas y fáciles de almacenar
- Pueden almacenar desde 2.5 hasta 25 gigabytes
- La velocidad de transferencia es 1-2 megabytes por segundo en unidades nuevas
- La cabeza lectora tiene una esperanza de vida corta, debido a la alta tasa de movimiento relativo
- El coste del gigabyte es 3 veces superior al del gigabyte en 4mm

Soportes físicos de copias de seguridad: DLT (Cinta lineal digital)

- Se escriben dos pistas de información en paralelo.
- Esto reduce el movimiento relativo
  - La cabeza lectora tiene una esperanza de vida larga (más de 100.000 pases de lectura/escritura)
  - Es de los soportes más fiables
- Pueden almacenar desde 10 hasta 70 gigabytes
- El coste de las cintas es muy elevado
- La velocidad de transferencia es de 1,5-5 megabytes por segundo

Soportes físicos de copias de seguridad: 8mm/AIT

- Siguiente generación de las de 8mm
- Pueden almacenar desde 50 hasta 100 gigabytes
  - Con velocidad de transferencia de 6 o12 megabytes por segundo respectivamente
- El coste de las cintas es muy elevado
- La cabeza lectora tiene una esperanza vida larga (unos 30000 usos)

Soportes físicos de copias de seguridad: Interfaces

- Dispositivos de cinta conectados a tarjetas controladoras de unidades de disquete
- Unidades de cinta ATAPI
- Unidades de cinta SCSI

Soportes físicos de copias de seguridad: Almacenamiento

- Es conveniente no almacenar las copias de seguridad en el mismo lugar que los hosts
  - Ante un desastre como un incendio, se perdería la información de ambas fuentes
  - Si aún así se decide este almacenamiento se debe buscar un armario a prueba de fuego e impermeable
  - Presenta la ventaja de la disponibilidad de las copias
- Almacenar en otro lugar como la caja de un banco es buena opción
  - Aunque se requiere transporte
- Existen servicios de depósito de cintas