Seguridad pasiva

PID_00200514

Jordi Serra Ruiz

Universitat Oberta de Catalunya

Índice

Introducción

La seguridad pasiva es uno de los aspectos más importantes que hay que tener en cuenta a la hora de administrar o instalar un servidor, puesto que, en principio, una vez configuradas las políticas de seguridad pasiva, no hay que preocuparse mucho del funcionamiento que tienen y, por lo tanto, esto hace que se olviden con facilidad y, si hay algún error o problema, no nos damos cuenta de él hasta que muchas veces es demasiado tarde. Sin embargo, el hecho de tener que estar constantemente pendientes de la seguridad pasiva significa que las decisiones tomadas a la hora de configurarla han sido erróneas y, por lo tanto, en realidad esa seguridad no funciona correctamente.

Por ejemplo, un caso típico es la caída de fluido eléctrico. Para solucionar ese problema se puede decidir entre instalar un sistema de alimentación ininterrumpida (SAI) o contratar una doble compañía de suministro eléctrico (así, en caso de que falle una compañía se puede utilizar la otra) e incluso instalar dos fuentes de alimentación o más (la mayoría de los fabricantes de servidores ya tienen esta doble fuente de alimentación en sus equipos).

Más adelante describiremos las políticas de copias de seguridad de los datos que hay en los equipos informáticos: cómo se tiene que hacer, cuándo y dónde. Todo esto lo vamos a ver en este módulo.

Por último, veremos los planes de riesgo, planes y documentos en los que describiremos la actuación en el caso hipotético de que en la empresa, y en especial en la sala donde están los servidores, haya problemas. Mediante estos planes conseguiremos mantener los servidores en funcionamiento o, simplemente, apagar de modo seguro y general todos los servicios y servidores que tiene la empresa.

Objetivos

El objetivo fijado para este módulo es que aprendáis a conocer los diferentes métodos de seguridad pasiva que hay. De manera más concreta, los objetivos son los siguientes:

1. Conocer los dispositivos redundantes que podemos encontrar en un ordenador: las fuentes redundantes, los discos y las tarjetas de red.

2. Aprender a diseñar una buena política de copias de seguridad o *backups*, teniendo en cuenta la cantidad de información para almacenar, los dispositivos que tenemos a nuestro alcance, el tipo de información de la que queremos hacer una copia de seguridad y la importancia de esta información.

3. Conocer y entender qué es un plan de riesgo y cómo nos puede ayudar en la seguridad de la empresa en el día a día.

1. Elementos redundantes

Los elementos redundantes de los sistemas son los componentes que están duplicados en nuestra máquina o incluso en la red. Estos elementos duplicados con más frecuencia son la fuente de alimentación, los discos y las tarjetas de red o comunicaciones.

1.1. Fuentes de alimentación

La fuente de alimentación es una parte muy delicada de la máquina. La red eléctrica es susceptible de tener subidas o bajadas de tensión, que afectan a menudo a las fuentes de alimentación de los ordenadores, que se dañan con frecuencia. Si nosotros, como administradores, somos responsables de un servidor de alta disponibilidad, un servidor que tiene que dar servicio las veinticuatro horas del día los siete días de la semana (24 × 7), nos interesa que la máquina esté en servicio todo el tiempo que se pueda. Un fallo en la fuente de alimentación, a pesar de que es una avería muy rápida de reparar, nos puede dejar sin servicio. Cada vez más los servidores ya disponen de dos fuentes de alimentación incorporadas, por lo que la gestión de esta característica se simplifica considerablemente. Las fuentes redundantes se ponen en funcionamiento cuando detectan que la fuente principal no funciona. De este modo, el servidor puede estar activo mientras reparan la fuente dañada.

Hay que tener presente que, para conseguir un rendimiento óptimo de las fuentes redundantes, es aconsejable tener las dos fuentes conectadas a dos redes eléctricas distintas. De este modo, cuando falla una de las redes, la otra todavía está operativa.

No siempre se puede aplicar la solución óptima, ya que en muchas ciudades solo hay una empresa suministradora de electricidad. En esos casos, si tenemos un SAI o un grupo electrógeno, podemos tener una fuente conectada a los enchufes que son compatibles con el SAI y la otra, a la red eléctrica normal. Así, nos aseguramos ante las posibles caídas de la red eléctrica o del SAI, aunque estas caídas se dan en muy pocos casos.

1.2. Discos

Otros componentes que muy a menudo están duplicados son los discos internos de los servidores. Este tipo de redundancia se puede hacer por software o por hardware, aunque se recomienda hacerlo vía hardware, ya que la eficiencia es mayor. Desde el punto de vista de la seguridad pasiva, la redundancia por hardware de los discos es más robusta. Hoy en día, hay algunas marcas de

ordenadores, como por ejemplo HP, que venden para sus máquinas unas baterías auxiliares que se conectan a la controladora para asegurar la integridad de los discos ante un posible fallo eléctrico.

Si finalmente optamos por la redundancia vía hardware, la máquina debe tener una controladora de discos capaz de hacer esta redundancia. Antiguamente, las únicas controladoras capaces de hacer redundancia de discos por hardware necesitaban que estos discos fueran del tipo *SCSI* (interfaz de sistema para ordenadores pequeños o *small computer system interface*), que son discos más rápidos que los *IDE* (*integrated drive electronic*) debido a la capacidad que tienen de trabajar de manera asíncrona. Hoy en día, a pesar de que la mayoría de las controladoras siguen necesitando discos SCSI, hay en el mercado controladoras capaces de hacer redundancia por hardware que son compatibles con IDE, y sobre todo ahora con los discos *SATA* (*serial AT attachment*), mucho más rápidos que los antiguos IDE y mucho más baratos que los SCSI, a pesar de que más lentos.

En cambio, la redundancia por software no necesita de ninguna controladora, ya que la copia de la información entre los diferentes discos la hace un programa residente en memoria. Esto hace que el sistema operativo sea más lento y las copias sean menos robustas a problemas eléctricos, bajadas de tensión mientras se hace la copia, pero son mucho más baratas, en el caso de GNU/Linux son gratuitas, y no tienen el principal y más grave problema que tienen las controladoras hardware, que es la compatibilidad entre controladoras. En el caso de tener una controladora hardware que se estropee, será necesario cambiarla por una del mismo fabricante o incluso en muchos casos del mismo modelo, para poder recuperar la información que ha guardado en los discos, lo que obliga algunas veces a que en el momento de hacer la compra de la controladora hardware se compren dos para tener este componente duplicado por si falla la controladora. Evidentemente, esto no pasa con las controladoras software, ya que siempre se puede volver a reinstalar el mismo sistema y las mismas controladoras de software que se instalaron en su día.

La redundancia de discos se denomina RAID (conjunto redundante de discos independientes o *redundant array of independent –or inexpensive– disks*). Hay muchos administradores actuales que recurren al RAID con la intención de prevenir la pérdida de información, objetivo inalcanzable, por otro lado. El uso del RAID puede ayudar a evitar la pérdida de información, pero no la puede prevenir. Para entender por qué, y ser capaces de planificar una estrategia de protección de información más eficaz, primero debemos entender los diferentes tipos de fallos que hay y cómo pueden causar la pérdida de información. Estos fallos serían los siguientes:

1) Borrado accidental o intencionado de la información: Una de las principales causas de pérdida de información es el borrado accidental o intencionado de los archivos. Esta causa incluye desde los piratas informáticos o *hackers* malos que han entrado en el sistema hasta el error humano de los mismos

usuarios del dominio. En este tipo de pérdida de información, la redundancia de discos no nos puede ayudar, ya que si se elimina la información de manera normal, desaparece también de todos los discos donde se hace redundancia. Para mitigar este tipo de pérdida es indispensable tener una buena política de copias de seguridad.

2) Fallo total o completo del disco: Este tipo de pérdida de información se produce cuando el cabezal del disco se incrusta en la superficie magnética o cuando, debido a un fallo eléctrico, el disco queda dañado. En este tipo de pérdida, la redundancia de discos sí nos es útil, ya que el RAID almacena la información cruzada en diferentes discos y de manera redundante. Utilizando el RAID puede ser que el fallo total de un disco no produzca ninguna pérdida de información.

3) Pérdida de fluido eléctrico con la corrupción de datos consiguiente: Hay quien piensa que puede verificar la tolerancia a fallos provocando un trabajo intensivo del disco para paralizar después de repente el suministro eléctrico. Esta acción normalmente causa algún tipo de corrupción de la información y no consigue el efecto que quería. La redundancia de disco no nos puede ayudar en el caso de la corrupción de la información. Este tipo de pérdida o corrupción de la información se puede evitar utilizando sistemas de archivos que sean compatibles con *journaling*. A modo de recordatorio, diremos que son los sistemas que llevan un diario o *journal* en el que se anotan todos los accesos a los discos (a qué bloques se accede y qué información se modifica).

4) Sectores defectuosos en un disco: El fallo más común de los discos es la pérdida lenta pero estable de bloques en el disco. Cuando un sector está dañado no podemos leer la información que contenía. Los sectores defectuosos son inevitables en un disco; de hecho, un disco acabado de salir de fábrica puede contener centenares (incluso miles) de bloques dañados. Hoy en día, las controladoras de discos pueden detectar un bloque dañado y reasignar en su lugar un nuevo bloque sano. Todos los accesos subsiguientes que hace el sistema operativo a este sector son, de modo transparente, redireccionados. Este comportamiento es perjudicial a la larga, ya que todos los bloques van fallando lentamente, debido a los saltos del cabezal sobre la superficie magnética del disco. Llega un momento en el que la tabla de bloques erróneos se llena; entonces los bloques erróneos se hacen visibles en el sistema operativo. A pesar de que este fallo es el más común de un disco, es, por desgracia, el que tiene menos soluciones. La redundancia de disco tampoco nos puede ayudar en este caso. Llegados a este punto, solo podemos hacer que el sistema operativo marque todos los bloques dañados, pero se trata de una operación muy lenta (en discos de 160 GB puede tardar un día entero) y se tiene que ejecutar sobre los discos desmontados y solo con los discos que no formen parte de ningún dispositivo ni RAID ni LVM (volumen lógico o *logical volume*).

5) Corrupción general del sistema: Este fallo se debe a la complicada regresión de un sistema hacia el caos total, que tarde o temprano hace que se tenga que reinstalar el sistema. Como los errores o *bugs* en el sistema operativo, la base de datos o las aplicaciones y la lenta acumulación de información corrupta hacen que un sistema se vuelva inutilizable, no se puede hacer gran cosa en estos casos excepto evitar por todos los medios poner servicios críticos a máquinas con sistemas o software beta. Por desgracia, aunque se hagan copias de seguridad de modo regular, es muy posible que estos servicios hayan hecho copias de datos corruptos. En las versiones más modernas de Windows y de la mayoría de las versiones GNU/Linux, este fenómeno se ha erradicado casi del todo. Fijémonos en que este tipo de corrupción del sistema también se puede deber a un hardware en mal estado o mal conectado, o a un entorno con mucho ruido eléctrico. Con la corrupción total de un sistema no hay ninguna estrategia que nos pueda ayudar a minimizar las pérdidas.

Hay muchas maneras de implementar el RAID; la mayoría de estas maneras son una combinación de las tecnologías de duplicado, fraccionado y paridad (*mirroring*, *striping* y *parity*). En 1988, se estandarizaron algunos métodos. Los investigadores encargados de esta estandarización denominaron niveles (*levels*) a cada uno de estos métodos de estandarización. Esta elección fue un tanto desafortunada, ya que la palabra *nivel* tiene connotaciones de jerarquía, es decir, parece que indica que, para lograr un determinado nivel de RAID, tenemos que recorrer todos los niveles inferiores, lo que en realidad en RAID no pasa. La utilización de la palabra *nivel* también lleva implícito, para mucha gente, que el nivel de RAID N+1 es mejor que el nivel RAID N, lo que es absolutamente falso. Los niveles en RAID son completamente independientes los unos de los otros, y cada uno está pensado para dar soluciones en ámbitos diferentes. Por lo tanto, según cuál sea nuestra necesidad utilizaremos un nivel de RAID u otro.

Al principio, el RAID definía cinco niveles y después se añadieron otros. Más adelante, a partir de estos niveles simples también se definieron varios niveles múltiples, en los que se usaba una combinación de dos niveles simples o más para crear nuevos niveles con nuevas capacidades y limitaciones. Muchos de estos niveles de RAID todavía están en uso hoy en día. Algunos niveles de RAID, tanto si son simples como múltiples, han caído en el olvido porque a lo largo del tiempo se han mostrado inferiores al resto de niveles con pocas ventajas en la compensación que tienen. En esta sección, vamos a ver los principales rasgos de los diferentes niveles de RAID. Tenemos que destacar que los niveles simples son mucho más frecuentes y populares que los niveles múltiples, ya que tienen un coste más barato y una implementación más simple, y porque, en general, ya satisfacen a la mayoría de los usuarios. Solo hay algunas aplicaciones muy particulares que requieren el uso de los niveles múltiples de RAID. Hay ocho niveles simples de RAID, los más populares de los cuales son el RAID 0, el RAID 1 y el RAID 5.

- **RAID 0.** Para hacer este nivel hay que tener como mínimo dos discos. Este nivel utiliza la tecnología conocida como fraccionado, que divide los datos en varias partes (tantas como discos tenga) y almacena la información en todos los discos a la vez, es decir, permite un acceso simultáneo a todos los discos. Este nivel tiene unos tiempos de acceso de lectura y escritura muy rápidos. La velocidad de transferencia aumenta según el número de discos que tenemos. Este nivel no hace ninguna redundancia de información; por lo tanto, no tiene ninguna tolerancia a fallos.

- **RAID 1.** Para hacer este nivel hay que tener como mínimo dos discos. Este tipo de RAID se conoce como *mirror* (espejo), ya que escribe de manera simultánea en los dos discos, de modo que cuando falla uno de los dos discos el otro continúa funcionando hasta que podamos reparar el que está dañado. Este nivel, debido al uso del duplicado (*mirroring*), tiene una tolerancia a los fallos muy buena. El inconveniente de este nivel es el bajo porcentaje de almacenamiento que tiene (50%); es decir, de la capacidad de almacenamiento total (dos discos), de modo efectivo solo tenemos uno.

- **RAID 2.** Este nivel es uno de los que no se usan hoy en día, por varias razones: la gran complejidad que tiene, el coste elevado y la necesidad de tener muchos discos para trabajar. Además, este nivel utilizaba una técnica no estándar de RAID (duplicado, fraccionado y paridad), ya que se basaba en un fraccionamiento de bit con codificación de Hamming, que es una técnica utilizada comúnmente para detectar y corregir errores en memorias de estado sólido. En un RAID de nivel 2, el *ECC* (código corrector de errores o *error correction code*) se intercala mediante varios discos a escala de bit.

- **RAID 3.** Este nivel requiere como mínimo tres discos, que deben tener las mismas características y capacidad. El RAID de nivel 3 dedica un único disco a almacenar la información de paridad. Usa una técnica de fraccionamiento a escala de byte con paridad dedicada y accede a todos los discos de manera simultánea. Como tiene un acceso síncrono a los discos, no es recomendable usar este nivel en máquinas multiusuario. La tolerancia a fallos del RAID de nivel 3 es buena, ya que soporta la caída de uno de los discos. En cuanto a la tasa de almacenamiento, depende del número de discos utilizados. Si N es el número de discos, la tasa es de N-1/N.

- **RAID 4.** Este nivel de RAID requiere, igual que el nivel 3, tres discos iguales. Usa una técnica de fraccionamiento a escala de bloque con paridad dedicada. Este nivel es muy parecido al nivel 3. La gran diferencia es que accede a los discos de modo independiente. Este nivel es especialmente apropiado para almacenar archivos de un tamaño muy grande, lo que hace que sea muy adecuado para aplicaciones gráficas. La tolerancia a fallos es buena, ya que puede soportar la caída de uno de los discos que tiene. La tasa de almacenamiento, igual que en el RAID de nivel 3, es de N-1/N.

- **RAID 5.** Este nivel funciona igual que el nivel 4 pero con la paridad distribuida, es decir, cada uno de los discos que forman este RAID contiene a la vez información y paridad. Esta característica lo hace mucho más eficiente que el RAID 4, ya que elimina el cuello de botella que se crea en este RAID 4 (todos los accesos a disco requieren leer del disco de paridad). Este nivel de RAID es el más eficaz y el que tiene una mejor relación rendimiento-coste. Este nivel de RAID es el más indicado para trabajar en entornos multiusuario. Igual que en los dos casos anteriores, requiere como mínimo tres discos, tolera la caída de un disco y la tasa de almacenamiento es de N-1/N.

- **RAID 6.** Este nivel pide como mínimo cuatro discos. Utiliza la misma técnica que el nivel 5 pero con redundancia distribuida de paridad (a diferencia de los niveles anteriores, que solo tenían redundancia de información). La tolerancia a fallos es excelente, soporta hasta la caída simultánea de dos discos. La tasa de almacenamiento, como tiene redundancia de paridad, disminuye en comparación con niveles anteriores y la sitúa en N-2/N. Actualmente este nivel de RAID se utiliza poco, ya que el coste de implantación que tiene es más alto que lo otros niveles de RAID, puesto que las controladoras necesarias son más complejas y, por lo demás, más caras que las de otros niveles.

- **RAID 7.** A diferencia de los demás, este nivel no es un estándar abierto a la industria. El nivel 7 no es más que una marca registrada de Storage Computer Corporation para describir su diseño propietario.

Los niveles de RAID múltiple se usan para mejorar las características de los niveles de RAID simples que lo forman. El nivel simple más combinado es el RAID 0, que se une a menudo con los niveles redundantes, como el nivel 1, 3 y 5. No se dan todas las combinaciones posibles entre niveles, cosa que es lógico que sea así, puesto que la combinación pretende suplir las desventajas de un nivel con las ventajas de otro. Además, no tendría sentido unir, por ejemplo, los niveles 4 y 5, puesto que se parecen mucho.

Antes de tratar con detenimiento cada uno de los niveles, tenemos que saber unas cuantas cosas sobre los niveles múltiples de RAID. Un nivel múltiple se crea dividiendo los discos en volúmenes. A cada uno de los volúmenes se le aplica un nivel simple de RAID. Después se aplica un segundo nivel de RAID entre los diferentes volúmenes para crear un RAID de nivel superior. Por este motivo, a veces, cuando se habla de este tipo de configuraciones, se dice que son RAID anidados.

Como hay dos niveles, hay dos maneras de combinarlos. Podemos hacer RAID X+Y o RAID Y+X. La elección del nivel que se aplica primero y el que se aplica después solo afecta directamente a la tolerancia a fallos del RAID resultante,

ya que las características de los requisitos de los controladores, la capacidad de almacenamiento, la eficiencia de almacenamiento y el funcionamiento son iguales en los dos casos.

Esta diferencia en la tolerancia a fallos se ve mucho más clara con un ejemplo. Imaginemos que queremos aplicar el RAID 0 y el RAID 1 sobre una máquina con diez discos:

- Si usamos RAID 0 primero (RAID 0+1), creamos dos volúmenes de cinco discos cada uno. Los discos 1, 2, 3, 4 y 5 forman el primer volumen, que denominamos A, y los discos 6, 7, 8, 9 y 10 forman el segundo, que denominamos B. A cada uno de los volúmenes (A y B) aplicamos RAID 0. Después, entre A y B aplicamos RAID 1. Ahora imaginemos que falla el disco #2: todo el volumen A queda dañado. Mientras se repara el disco #2 solo nos queda B con RAID 0; por lo tanto, sin redundancia. Si falla cualquier disco del volumen B, por ejemplo, #9, perdemos toda la información.

- Si usamos el RAID 1 primero (RAID 1+0), creamos cinco volúmenes de dos discos. Los discos 1 y 2 forman el volumen A; los discos 3 y 4, el B; los discos 5 y 6, el C; los discos 7 y 8, el D; y los discos 9 y 10, el E. Aplicamos RAID 1 a cada volumen. Después aplicamos RAID 0 entre A, B, C, D y E. Ahora imaginemos que falla el disco #2: el volumen A continúa funcionando con el disco #1 y el RAID 0 entre volúmenes también sigue funcionando. Ahora imaginemos también que falla el disco #9: el volumen E continúa funcionando con el disco #10; por lo tanto, el RAID 0 sigue funcionando.

El RAID 1+0 es mucho más robusto que el RAID 0+1, ya que el primero podría soportar una caída de hasta cinco discos, siempre que se encuentren en volúmenes diferentes, mientras que en el segundo, si caen dos discos (uno de cada volumen), perdemos toda la información. El mismo efecto de la tolerancia también se aplica a la reconstrucción (*rebuild*) del RAID. No es lo mismo reconstruir un volumen de cinco discos (RAID 0+1) que reconstruir un único disco (es el caso de RAID 1+0, en el que solo reparamos el disco #2). Esto se debe tener muy en cuenta, ya que la regeneración de un RAID, cuando uno de los discos que ha dejado de funcionar se ha tenido que sustituir por uno nuevo, es muy costosa en tiempo y pueden pasar muchas horas para poder regenerar un RAID de algunos gigas.

Veamos a continuación qué tipo de niveles múltiples de RAID nos podemos encontrar:

- **RAID 0+1 o 1+0.** Es el RAID múltiple más popular, ya que combina la rapidez del RAID 0 con la redundancia del RAID 1. La desventaja principal que tiene es que requiere como mínimo cuatro discos, de los que solo hay dos que son para almacenar información. Otra desventaja es que, si queremos aumentar de capacidad, se tienen que añadir discos por parejas (de dos en dos), lo que duplica el coste. Este nivel RAID es muy adecuado en entornos

de gran rendimiento, con tolerancia a fallos pero sin mucha necesidad de capacidad de almacenamiento. El RAID 1+0 es el más rápido y seguro de todos los niveles RAID, pero también el más costoso de implementar.

- **RAID 0+3 o 3+0.** Utiliza la fracción a escala de byte con la paridad dedicada y con el fraccionado de bloque. El RAID 3+0 es más común que el RAID 0+3. Este nivel de RAID da un rendimiento mejor que el RAID 3, gracias a las propiedades de rapidez del RAID 0, pero está más cerca del rendimiento del RAID 3 que del rendimiento que ofrece el RAID 0. El RAID 3+0 proporciona mejor rendimiento de reconstrucción de los discos y mejor tolerancia a fallos que el RAID 0+3, pero en ambos casos estos factores dependen del tamaño del RAID 3 en proporción al RAID 0. Este nivel es uno de los menos utilizados.

- **RAID 0+5 o 5+0.** Combina el fraccionado a escala de bloque con paridad distribuida del RAID 5 con el fraccionado del RAID 0. El RAID 5+0 es más común que el RAID 0+5. Ambos casos mejoran el rendimiento y la tolerancia a fallos que ofrece el RAID 5, en especial el RAID 5+0. Muchas de las características del RAID 5+0 son parecidas al RAID 3+0. Este nivel es preferible al RAID 3+0 en entornos de transacciones, donde los archivos son más pequeños. El número mínimo de discos necesarios para este nivel es de seis. Por eso, este nivel es muy complejo y difícil de implantar.

- **RAID 1+5 o 5+1.** Este nivel ofrece, sin duda, la mejor tolerancia a fallos de todos los niveles RAID, fruto de la unión de los dos métodos de RAID que ofrecen redundancia (duplicado y paridad). Estos dos niveles RAID (1+5 y 5+1) son muy parecidos a los niveles RAID 1+0 y RAID 0+1, pero con paridad distribuida. Este nivel requiere como mínimo seis discos, y todos iguales. El coste de esta implantación es muy alto, ya que requiere muchos discos para usar una capacidad de almacenamiento relativamente baja. Las grandes desventajas que tiene son el coste elevado y la complejidad. Estos últimos niveles de RAID múltiple son muy tolerantes a fallos, pero antes de implantarlos podemos buscar otro tipo de soluciones basadas en clústeres o servidores redundantes e implantar un nivel RAID 1+0, que ofrece muchos de los beneficios de estos niveles con un rendimiento más bueno y un precio más bajo.

En cuanto a la seguridad, todos los niveles RAID que ofrecen tolerancia a fallos son buenos niveles, pero entre estos niveles los mejores, por el precio y el rendimiento que tienen, son los RAID 1, RAID 5 y RAID 10. En general, vamos a elegir uno de estos tres según las características del entorno y las necesidades del servidor. El coste también es un factor determinante en los niveles de seguridad que queremos obtener.

Para instalar el RAID en modo hardware, en los entornos Windows generalmente es bastante transparente y se encarga la propia controladora de gestionarlo todo. Pero en sistemas GNU/Linux hay que compilar el núcleo o *kernel*

si no viene por defecto este soporte, a pesar de que en las últimas versiones ya lo tienen en cuenta. Por un lado, debemos seleccionar el tipo de hardware del que disponemos para hacer un RAID. Para hacerlo, debemos seleccionar las opciones siguientes en el núcleo:

```
SCSI Support
[*] SCSI Support
SCSI low-level Drivers
Seleccionar nuestro hardware
```

Por otro lado, tenemos que seleccionar qué tipo de RAID queremos mediante la configuración siguiente en el núcleo:

```
Multi-device Support (RAID LVM)
[*] Multi-device Support
[*] RAID Support
[*] RAID Level 5
```

Una vez hemos seleccionado estas opciones en el núcleo, ya lo podemos compilar e instalar. Normalmente, la configuración del RAID se hace desde un programa que gestiona la controladora de disco. Esta aplicación está integrada en la misma tarjeta de la controladora. Para acceder a este programa en el momento de arranque (tras la configuración del BIOS), nos sale un mensaje que nos indica que, si queremos entrar en la configuración de la tarjeta RAID, tenemos que pulsar (normalmente) Alt + F3. Esta consola interactiva nos permite crear volúmenes, reconstruirlos o borrarlos. Además, podemos seleccionar el nivel RAID que queremos que tenga cada volumen.

1.3. Dispositivos de red

Tener unas cuantas tarjetas de red no quiere decir tener tarjetas de red redundantes, ya que por necesidades del servidor es posible tener una máquina conectada a varias redes. Así, por ejemplo, un servidor que haga de *proxy* del acceso a Internet necesitará dos tarjetas de red, una para escuchar de la red interna de la empresa y otra para la conexión a Internet, lo mismo pasa en aquellos servidores que se dedican a hacer de *firewall* de software de toda la empresa, filtrarán el contenido que pasa desde Internet hacia la red local y a la inversa. Por lo tanto, la redundancia de tarjetas de red se consigue mediante un software específico que gestiona una única conexión a la red local. La finalidad de esta redundancia en las tarjetas de red se debe, principalmente, a dos motivos:

- Tener una tarjeta de copia de seguridad por si la tarjeta principal falla. No obstante, esta solución, a pesar de que tiene un coste muy bajo, solo nos previene si falla la tarjeta de red. Pero ¿qué pasa si falla el equipo de comunicaciones instalado en la red local? Como tenemos dos tarjetas, la tarjeta secundaria la podemos conectar a un segundo equipo de comunicaciones,

otra red diferente de la principal; de este modo nos protegemos no solo ante el fallo de la tarjeta de red, sino también ante el fallo del equipo de comunicaciones de la red local. Ahora bien, ¿qué pasaría si lo que falla es el proveedor de Internet (ISP)? Entonces, aprovechando que tenemos un segundo equipo de comunicaciones, podemos contratar un segundo ISP. Como vemos, hay muchas opciones de redundancia de red. Sin embargo, cuanto más nos protegemos, más aumenta el coste de la implantación. Se tiene que llegar a un compromiso de coste-seguridad que sea suficiente para satisfacer las necesidades reales. Se tendría que hacer un estudio en detalle de cómo es la empresa y a qué se dedica para saber si es o no importante tener este segundo ISP redundante. Si solo tenemos una página web para hacer publicidad de la empresa, no hay que tener un ISP redundante. Si la empresa se dedica al comercio electrónico, entonces sí es conveniente tener un proveedor de Internet redundante, ya que por cada hora que estemos sin conexión perdemos dinero.

- Otra razón para tener redundancia de tarjeta de red es por motivos de balanceo de carga. Si tenemos dos tarjetas en la misma red que ofrecen los mismos servicios con balanceo de carga, podemos atender el doble de peticiones de la red local de manera simultánea, es decir, que todas las peticiones que van de la red local, de los ordenadores cliente de la empresa hacia el servidor, para recuperar ficheros, autenticarse, resolución de nombres y actualizaciones, entre otros, serán mucho más rápidas por tener doblado el acceso al servidor. Pero si solo se dispone de una única salida hacia Internet, un solo IPS, el aumento de velocidad no se verá incrementado en el acceso a Internet, ya que si la línea de salida del ISP es una ADSL, o cable, a 20 Mb/s y tenemos dos tarjetas de red 1000 MB/s, está claro que el cuello de botella será esta salida a Internet. Por lo tanto, con esta configuración no tiene sentido tener una tarjeta redundada con balanceo de carga (salvo que tengamos mucho tráfico interno en la empresa con muchos accesos a la intranet, que hagan mejorar mucho el rendimiento de las comunicaciones internas).

2. Políticas de copias de seguridad

Hay un principio básico que, como administradores o jefes de seguridad, debemos tener siempre muy presente, y es que los discos fallan. Hoy en día, es difícil encontrar un administrador de sistemas que no se haya visto involucrado en la pérdida de un disco. Para ello, solo hay una solución posible: hacer una copia de seguridad.

La mayoría de veces en las que hay una pérdida de información guardada en un disco se debe al hecho de que no se ha planificado nunca que estos datos se tenían que tener guardados, copiados en otro sistema para recuperarlos luego. La decisión de si se tiene que hacer una copia de seguridad o no es bastante importante para no tomársela a la ligera. Por lo tanto, en cierto modo, cuando planificamos estamos decidiendo de qué datos se hará la copia de seguridad y de cuáles no: estamos asumiendo qué datos estamos dispuestos a perder, ya que no los tendremos en caso de pérdida de información.

Esto no solo pasa a escala empresarial; en un estudio llevado a cabo en los Estados Unidos en mayo del 2012 y encargado por la empresa de discos duros Seagate, el 54% de los encuestados reconocieron haber perdido datos, ya sean documentos o fotografías digitales, que ya no pueden recuperar. Pero solo el 11% de las personas a las que se les planteó la encuesta reconocen tener un plan de copias de seguridad de los datos en general en su casa.

En la planificación de los datos de los que se hará una copia de seguridad tenemos que prever no solo los datos de los usuarios, sino también los archivos de configuración, las bases de datos, las bibliotecas importantes y toda la información que sea útil para la empresa.

Cuando sepamos cuáles son los datos que queremos guardar en una copia de seguridad, tenemos que decidir cuándo se tiene que hacer esta copia. Hay datos (los de usuarios, por ejemplo) que cada día tienen cambios; hay otros que cambian mucho más despacio y, finalmente, hay bibliotecas y archivos de configuración que puede ser que no cambien durante toda la vida útil de la máquina, de forma que tenemos que determinar la frecuencia de copia de seguridad de cada uno de estos datos. Cuando tengamos toda esa información, podemos empezar a planificar las copias de seguridad. Para hacerlo, primero debemos saber los diferentes niveles de copias de seguridad que hay.

Nivel 0. Este nivel se conoce como copia de seguridad total. Hace copia de todos los datos marcados para guardar, lo que hay dentro de las particiones, o de los discos, donde se hace la copia de seguridad. Este tipo de copia suele tener, dependiendo de la cantidad de datos que haya, un coste temporal muy alto. Es decir, puede tardar bastantes días en hacerse.

Nivel 1-9. La mayoría de las herramientas comerciales designan estos niveles con un único nombre: incremental. Estos niveles consisten en guardar solo los datos que se han modificado desde la última copia de seguridad total o de nivel inferior (por ejemplo, un incremental de nivel 2 hace una copia de los datos que se han modificado respecto a la última copia de nivel 0 y a la última de nivel 1). Esta manera de anidar la información la veremos mucho más clara con un ejemplo:

> Imaginemos que el sábado por la noche se hace una copia de seguridad total de todas las carpetas y archivos del servidor y el lunes, siguiente día laborable, se hace por la noche una copia incremental de nivel 1, es decir, se copia todo lo que se ha modificado durante el día. ¿Qué se puede hacer el martes por la noche? Si hacemos un incremental de nivel 1, copiamos todos los datos que se han modificado el martes y el lunes, con independencia de que estos últimos datos se hayan modificado el martes o no, es decir, se vuelven a copiar todos los datos que se han modificado desde el sábado. Si por el contrario se hace un incremental de nivel 2, solo se hace una copia de los datos modificados el martes y ocupan menos espacio en el disco duro, ya que los datos modificados el lunes ya están guardados el día anterior, pero en el caso de tener que recuperar todo el sistema de archivos, se tendrá que pasar por todas las copias diarias, ya que no existirá una donde esté todo lo modificado desde el sábado. El proceso de recuperación de los datos es más lento, sobre todo si no se sabe de qué día puede ser la última modificación del archivo que se quiere recuperar.

En la mayoría de las herramientas comerciales de copia de seguridad encontramos el término *diferencial*, con el que se designa un tipo de copia de seguridad incremental, de manera genérica, que hace copias solo de los datos que han cambiado desde el último diferencial. Se trata de un incremental sin tener en cuenta los niveles.

En este tipo de herramientas comerciales, solo se designan tres tipos de copias: total, incremental y diferencial. La recomendación es una total a la semana, una diferencial todas las noches –en la que se reflejarán los cambios que se han producido a lo largo de aquel día– y una incremental solo en los casos en los que nos interesen los cambios que ha habido desde la última total.

Otro factor que debemos tener en cuenta para planificar la copia de seguridad es el tiempo que se tarda en realizar estas copias. En las totales se hace una copia de todos los datos, tanto si se han modificado la última semana como si no. Por lo tanto, si el disco es muy grande podemos tardar muchas horas antes de que se acabe. Por ejemplo, una copia del disco de usuarios de 500 GB puede tardar horas. Hagamos unos pequeños cálculos.

Si tenemos un disco de datos con todo aquello de lo que se tiene que hacer copias de seguridad, por ejemplo los discos de usuarios, la contabilidad, la página web, los *logs* y configuraciones del sistema con unos 500 GB de información, y disponemos de un disco duro SATA2, que tienen una transferencia de datos

de 300 MB/s, se tardará 27 minutos en leer estos datos y otros 27 minutos en guardarlos en otro disco duro de las mismas características. En el supuesto de que se guardaran en una cinta magnética *DLT* (*Digital Line Tape*) a 60 MB/s tardaría 2,3 horas en grabarse e idéntico tamaño para los dispositivos USB 2.0. En cambio, si la copia se ejecuta sobre otro dispositivo que está en la red y, por lo tanto, los datos se tienen que transmitir por una red Ethernet a 100 Mb/s tardaríamos once horas en transmitirlos, lo que colapsaría la red si no se hace en horas no laborales. En el caso de tener una red de comunicaciones que funcione a gigabit, estas once horas se convierten en una hora, lo que hace que la inversión valga la pena para aligerar la red.

Por lo tanto, es aconsejable hacer estos cálculos antes de configurar cuándo se hacen las copias y cómo se hacen, ya que podemos saturar el servidor o la red en el momento de hacer las copias. Si se ve que se tienen que hacer las copias sobre otro servidor, se debe tener en cuenta que por la red los datos tienen que ir cifrados si salen de nuestra empresa, y esto comporta un tiempo añadido de cómputo y más tiempo en la transmisión por Internet, ya que no es lo misma que hemos visto hasta ahora.

Una vez tenemos todos estos datos es cuando hemos de planificar las copias de seguridad. A continuación, mostramos algunas de las planificaciones más usuales que se hacen.

- Total cada día. Es una planificación que solo hacemos si el volumen de información del que queremos hacer la copia es bastante pequeño para que se haga por la noche.

- Total semanal e incremental (nivel 1) diario. La principal ventaja de este método es que solo se necesitan dos volúmenes para recuperar toda la información. Esto se debe al hecho de que todos los días se hace una copia de seguridad de las modificaciones que se han producido a lo largo de la semana. Este tipo de política es la más recomendable si usamos las utilidades simples de copia de seguridad (como `cpio`, `tar`, `dump`, `amanda` o `rdiff-backup` en GNU/Linux, y Windows Server Backup en Windows, que veremos más adelante). Sin embargo, el inconveniente es que hacemos una copia de seguridad de datos innecesarios. Imaginemos que un archivo se modifica solo el lunes: a lo largo de toda la semana haremos copias de seguridad de manera innecesaria de este archivo.

- Total semanal, diferencial diario. La principal ventaja de este método es que las copias de seguridad diarias son muy pequeñas y, por lo tanto, más rápidas. El inconveniente principal es que si queremos recuperar algo el viernes necesitamos seis volúmenes. Si usamos herramientas comerciales, esta desventaja se minimiza, ya que la mayoría de estas herramientas incorporan un sistema de gestión de los volúmenes.

- Hay también otras filosofías de copias de seguridad incrementales que trabajan con las progresiones matemáticas (sobre todo la llamada torre de Hanoi). Mediante estas progresiones se hacen todos los días copias de seguridad incrementales de diferentes niveles (por ejemplo 0, 3, 2, 5, 4, 7, 8, 9 y 1); con esto, conseguimos optimizar el número de cintas en uso, optimizar el tiempo de la copia de seguridad e incluso llegar a hacer una única copia total al mes.

Las políticas de copias de seguridad no son solo las que hemos comentado. Se puede diseñar una que se acople más a las necesidades específicas de cada caso, según el volumen de información y de la frecuencia de cambios que tengamos en la empresa. Ahora bien, hay que tener presente que no habrá nunca suficientes copias de seguridad para satisfacer a los usuarios. Por ejemplo, si falla el sistema un miércoles por la tarde, todos los datos modificados a lo largo de la mañana no están reflejados en ninguna copia de seguridad. Una posible solución a este problema es el uso de discos redundantes (RAID). Si el fallo se ha producido en el ordenador del usuario, allí seguramente no tendremos los discos redundados; por lo tanto, es importante ofrecer a los usuarios unidades de trabajo remotas (unidades de red), situadas en el servidor, donde puedan guardar los documentos.

Dentro de las políticas de copias de seguridad hay otro factor que se debe tener en cuenta: ¿durante cuánto tiempo estamos dispuestos a guardar la copia de seguridad? Si solo utilizamos una única cinta (CD o dispositivo físico donde se hacen las copias) para cada día, quiere decir que si un usuario no se da cuenta de que ha perdido algo antes de una semana ya no la podremos recuperar. Si guardamos las cintas (o CD o DVD) durante más tiempo, necesitaremos muchas más. Necesitaremos un juego de siete cintas para cada semana de más que decidamos guardar.

Otro factor que se debe tener en cuenta es el etiquetado de los dispositivos de copia. Imaginemos que queremos guardar las copias de seguridad durante un mes. Esto hace que tengamos cuatro juegos completos de cintas, uno para cada semana. Debemos tener muy claro qué cinta se tiene que poner cada día de la semana y no confundir cintas del mismo día de la semana pero de semanas diferentes. Por lo tanto, el etiquetado de los soportes físicos es muy importante para no perder información (en caso de poner una cinta que no toca) o para recuperar rápidamente la información que necesitemos.

Una vez tengamos definida la política de copias de seguridad y hayamos hecho la primera, es hora de verificar que la copia de seguridad funciona correctamente. No sirve de nada hacer copias de seguridad si no hemos comprobado que podemos recuperar la información. Para hacerlo, una vez hecha la primera copia de seguridad intentaremos recuperar información. Para no interferir en el funcionamiento del servidor utilizamos la funcionalidad que nos ofrecen las herramientas de copia de seguridad que nos permiten recuperar datos en un directorio diferente del que se hizo la copia. Por ejemplo, los datos de

/home/user se pueden recuperar en /tmp/home/user en el caso de GNU/Linux. De este modo, se comprueba que la copia de seguridad funciona sin modificar los datos que hay en el directorio raíz.

Tras comprobar que las copias de seguridad funcionan correctamente, es decir, que se pueden recuperar tanto archivos individuales como los discos enteros, ya podemos empezar a hacer las copias según la política que hemos definido.

2.1. Herramientas de copias de seguridad en GNU/Linux

En las distribuciones estándar de GNU/Linux encontramos unas cuantas herramientas muy básicas que nos pueden ayudar a llevar a cabo una copia de seguridad. Estas herramientas tienen bastantes limitaciones, pero la ventaja que tienen es que no necesitan ningún coste económico adicional y su instalación y configuración es bastante fácil. A pesar de las limitaciones de estas herramientas, es muy recomendable que un administrador las sepa usar, ya que en muchos casos habrá que hacerlo. Estas herramientas son dump, cpio, amanda y tar. No obstante, por defecto, únicamente está instalada la herramienta tar, ya que es el compresor de archivos que se usa más a menudo en GNU/Linux. En el último apartado de esta sección, vamos a ver una herramienta con licencia GNU llamada Amanda que nos ofrece algunas de las ventajas de las herramientas comerciales de copias de seguridad.

2.1.1. Dump

La orden dump tiene asociada la orden restore para recuperarlos. El funcionamiento de esta herramienta es hacer una copia de seguridad de todo el sistema de archivos en un único fichero, es decir, normalmente de todo el disco, o discos si los tenemos montados dentro del sistema de archivos. Aunque se cree un archivo como un archivo regular, este fichero se suele guardar en un dispositivo externo de copia de seguridad (normalmente una cinta, robots de copias de seguridad o DVD).

Consultar el manual

Para ver las opciones de ejecución de las órdenes dump y restore, consultad el man.

El comando dump puede hacer diferentes tipos de copias de seguridad. Estos tipos son: la total y diferentes niveles de la incremental. Para hacerlo, tiene un parámetro en el que se indica el nivel de copia de seguridad que se quiere hacer (tal como hemos descrito antes, los niveles de copias de seguridad van del 0 al 9). Para indicar qué nivel de copia de seguridad queremos hacer, pasamos el número a la orden de ejecución:

```
root# dump 0 (hace una copia de seguridad total)
root# dump 3 (hace una copia de seguridad de nivel 3)
```

Hay opciones que tienen asociado un parámetro, pero a diferencia de otras órdenes en las que cada opción va seguida del parámetro que tiene, la sintaxis de la orden de ejecución de `dump` es algo compleja, ya que tiene el formato siguiente:

```
root# dump 'options' 'parameters' filesystem
```

donde primero se ponen todas las opciones de manera consecutiva y después todos los parámetros. El orden de las opciones marca el orden de los parámetros. Finalmente, se escribe el dispositivo donde queremos ejecutar la orden `dump`.

Esta también tiene una opción, mediante una orden que está asociada a ella llamada `rdump`, que permite hacer copias de seguridad de máquinas remotas. Esta opción es muy interesante para los administradores, ya que si configuran los permisos de acceso remotos de manera correcta, pueden disponer de un servidor de copias de seguridad para hacer copias de todas las máquinas de la red. De este modo, se dispondrá de una copia de seguridad de todos los equipos informáticos que hay en la organización y, por lo tanto, se reducirá al máximo el tiempo de espera al restablecer el servicio de la organización en caso de un fallo general producido por alguna catástrofe.

Para utilizar el comando `rdump`, tenemos que permitir al servidor de copias de seguridad entrar en los clientes mediante la orden `rsh` y sin contraseña. Por la poca seguridad que tienen este tipo de accesos, es del todo desaconsejable usar el usuario raíz o *root* para hacer copias de seguridad, por lo tanto, se creará un usuario de copias remoto con los suficientes privilegios como para entrar en las máquinas desde la red interna.

Las órdenes `dump` y `restore` tienen muchas funcionalidades. Mediante un *shell script* podemos automatizar la copia de seguridad y obtendremos resultados muy satisfactorios. Sin embargo, estas herramientas también tienen limitaciones:

- No hay ninguna manera de obtener una imagen completa de todo el sistema.

- Para automatizar las tareas de copia de seguridad se necesitan *shell scripts*, que, a pesar de que tienen muy buenos resultados, los debe crear el administrador, y puede ser que contengan algún fallo.

- Cuando hagamos `restore` nos salen todos los archivos que debe haber en la copia de seguridad, aunque estos archivos se hayan copiado mal o no se haya hecho la copia de seguridad porque dice que hay algún tipo de error.

- Hay unas cuantas versiones de estas aplicaciones; cada distribución de Unix o GNU/Linux puede usar versiones diferentes. Algunas de estas versiones de `dump` o `restore` pueden ser incompatibles entre sí.

- No tienen ninguna interfaz que haga más amigable la gestión.

Para instalar `dump` en nuestra máquina debemos ejecutar la orden siguiente:

```
root# apt-get install dump
```

Uno de los archivos de configuración de esta herramienta es `/etc/fstab`. Este fichero es el que gestiona los dispositivos que se montan en la máquina en tiempo de arranque.

La orden `man dump`

Además de estas opciones, la orden `dump` tiene muchas otras. Si queremos conocer estas opciones, debemos consultar el `man` mediante la orden `man dump`.

El quinto campo de cada línea de este fichero es un campo numérico. Si es 1, nos indica que se tienen que hacer copias de este dispositivo. Si es 0, nos indica que no se harán copias de este dispositivo (estas copias suelen ser de uso temporal, o memorias caché de aplicaciones).

Ejemplo de copia de seguridad

Un ejemplo de ejecución de una copia de seguridad mediante la orden `dump` es este:

```
root# dump 0unbf 128 /dev/rmt/0cbn /home
```

Con esta sentencia indicamos a la orden `dump` que haga una copia de seguridad de nivel 0 (primera opción, 0), que el tamaño de los bloques es de 128 (opción b) y que el dispositivo de copia de seguridad está en `/dev/rmt/0cbn` (opción f). Las opciones u y n indican, respectivamente, que se actualicen los archivos de `dump` y que envíe un correo electrónico a los operadores de copia de seguridad cuando se haya acabado esta copia.

Con la instalación del `dump` también hemos instalado `restore`. Para recuperar un directorio de usuario, ejecutamos una orden parecida a esta:

```
root# restore -xvybf 128 /dev/rmt/0cbn ./home/jordi
```

Esta orden nos indica que recupere todos los archivos y los directorios de manera recursiva que hay a partir de `/home/jordi` (opción `x`), que trabaje en modo `verbose` (opción `v`) y que si detecta bloques malos que continúe (opción `y`). Finalmente, las opciones `b` y `f` tienen el mismo significado que en el caso del `dump`: el tamaño de los bloques y el dispositivo.

Las opciones más importantes de la orden `dump` son las siguientes:

1) `0-9`: niveles de copias de seguridad que queremos hacer.

2) `a`: escribir en la cinta hasta que se acabe, sin tener en cuenta los cálculos aproximados del tamaño de la copia de seguridad.

3) `k`: usar Kerberos[1] para la autenticación en el caso de copias de seguridad remotas.

(1)Atención: para usar esta opción hemos tenido que haber compilado antes el `dump` con soporte en Kerberos.

4) `M`: permite hacer muchos volúmenes.

5) `q`: hace que la orden `dump` aborte de manera inmediata.

6) `S`: indica de manera estimada la cantidad de espacio necesario para hacer la copia de seguridad.

7) `W`: indica al administrador qué sistemas son los que necesitan copia de seguridad.

Si queremos ver todas las opciones que permite hacer la orden `dump`, tenemos que ejecutar la orden de ayuda siguiente:

```
root# man dump
```

2.1.2. Cpio

Nuestra segunda opción para poder hacer copias de seguridad de los datos sería hacerlas con la orden `cpio`. Esta orden, a pesar de que hace mucho tiempo que está en activo, no tiene la popularidad de la orden `dump` ni la de la `tar`, que es otra utilidad para comprimir archivos. La principal ventaja del `cpio` es que acepta la lista de archivos de los que se quiere hacer una copia de seguridad por la entrada estándar; es decir, podemos concatenar órdenes mediante *pipes* –se representan mediante el símbolo (`|`)–, para saber cuáles son los archivos de los que tenemos que hacer copia de seguridad. Un ejemplo de esta utilización de la entrada estándar para hacer copias es este:

```
root# find /home -ctime 1 -print | cpio -o
```

Veamos las opciones que hay en el comando `dump`, pero que no tiene la orden `cpio`:

1) Hacer copias de seguridad incrementales, sin la ayuda de la orden `find`. Es decir, `dump` tiene constancia de qué archivos se han modificado desde la última copia de seguridad total que se ha hecho con el mismo pedido, mientras que con el pedido `cpio` se tiene que hacer una busca para ver qué archivos se han modificado desde la última copia, y pasamos la lista de estos ficheros por la entrada estándar al comando `cpio`.

El ejemplo anterior hace precisamente una copia de los archivos del directorio *home* que se han modificado hoy.

2) Hacer el proceso de restauración, `restore`, de manera interactiva.

Un ejemplo de una copia de seguridad con la orden `cpio` es este:

```
root# ls | cpio -oOacv device
```

Esta orden nos hace la copia de todos los archivos que salgan en la orden `ls` y nos envía la salida del listado del directorio al dispositivo `device` (opción `O`). La opción `a` nos deja la `atime` (la última vez que accedimos) de los archivos del mismo modo como estaban antes de hacer la copia de seguridad.

Es aconsejable usar el `man` para ver todas las opciones disponibles de esta orden.

Para recuperar los ficheros lo hacemos con la orden siguiente:

```
root# cpio -icktv < device
```

Esta orden lee por la entrada estándar el dispositivo donde ha almacenado la copia de seguridad y recupera los archivos.

Las opciones más destacadas de la orden `cpio`:

- `i`: ejecución en modo entrada.
- `m`: no modifica los tiempos de los archivos (ni el `atime` ni el `ctime`).
- `O`: ejecución en modo salida.
- `p`: ejecución en modo *bypass*.
- `r`: de manera interactiva renombra los archivos.
- `t`: muestra en la pantalla la tabla de contenidos de la entrada.
- `no-preserve-owner`: cuando extraemos una copia pone como propietario de los archivos el usuario que extrae los archivos.
- `no-absolute-filenames`: extrae los ficheros con el camino relativo al archivo actual. Es decir, el directorio raíz para los archivos que se extraen es el directorio desde donde se ejecuta la orden.

Si queremos ver todas las opciones del `cpio`, tenemos que consultar el `man` mediante la orden

```
root# man cpio
```

2.1.3. Tar

Si lo que queremos es hacer una copia de seguridad del sistema, probablemente la mejor opción es hacerla con la orden dump. Ahora bien, si lo que solo nos interesa es hacer una copia de seguridad del *home* de un usuario, antes, por ejemplo, de darlo de baja, la aplicación tar es sin duda la mejor opción.

A pesar de que el comando tar tiene un origen simultáneo al cpio, tiene una aceptación mayor entre los usuarios; esto se debe al hecho de que las operaciones básicas del comando tar son más simples (y más estándares entre las diferentes versiones) que las del cpio. Una muestra de la popularidad que tiene este comando es que la mayoría de los archivos que bajamos de Internet están con este tipo de compresión. Gracias a la gran popularidad que tiene, es muy importante que conozcamos bien esta herramienta.

Es aconsejable consultar el manual para saber las opciones que tiene esta orden.

Ejemplo de ejecución

Un ejemplo de ejecución con la orden tar es el siguiente:

```
root# tar cvzf backup.tar.gz /home/jordi
```

Esta orden nos crea un archivo (opción c) denominado backup.tar.gz con el contenido recursivo, que es una opción por defecto, que nos informa de posibles errores o advertencias (opción v) del directorio /home/jordi. Además, este archivo se ha comprimido usando la aplicación gunzip (opción z)

Para extraer el contenido de este archivo tenemos que usar la orden siguiente:

```
root# tar xvzf backup.tar.gz
```

La opción x sirve para extraer el contenido de un archivo tar.

Las opciones más destacadas de la orden tar son las siguientes:

- a: añade archivos a un archivo .tar.
- c: crea un archivo .tar.
- d: encuentra las diferencias entre un archivo .tar y el sistema de archivos.
- M: crea muchos archivos .tar.
- r: añade ficheros (al final) de un archivo .tar.
- t: muestra el contenido de un archivo .tar.
- x: extrae el contenido de un archivo .tar.
- Z: comprime el contenido de un archivo .tar con la orden compress.
- z: comprime el contenido de un archivo .tar con la orden gzip.
- atime-preserve: no modifica los tiempos de acceso en los ficheros.

Para conocer todas las opciones de la tar, tenemos que ejecutar la orden siguiente:

```
root# man tar
```

2.1.4. Amanda

La aplicación Amanda (Advanced Maryland Automated Network Disk Archiver) es una herramienta de copia de seguridad de distribución libre desarrollada por la Universidad de Maryland. Esta aplicación ofrece funcionalidades que son igualables a los sistemas comerciales de copias de seguridad que encontramos en el mercado.

Amanda establece un servidor único de copias de seguridad que permite hacer copias de muchas máquinas en un único dispositivo de copia. El dispositivo de copia que usa Amanda son las cintas, es decir, no se puede utilizar ni CD ni DVD a menos que se virtualice una unidad de DVD como unidad de cinta.

Para hacer copias de diferentes máquinas, debemos instalar clientes de Amanda en cada uno de los servidores de los que queremos hacer copia de seguridad. Más adelante, vamos a ver los pasos que hay que seguir para instalar el cliente de copia de seguridad.

Una de las grandes aportaciones de Amanda es el uso del disco de almacenamiento en el servidor de cintas. La idea es hacer muchas copias de seguridad en paralelo y dejar la información en el disco de almacenamiento y, tras un proceso independiente, se encarga de traspasar la información del disco a las cintas. El hecho de utilizar los discos proporciona más rapidez y la posibilidad de hacer las copias de seguridad de más de una máquina a la vez. Otra de las grandes ventajas que nos ofrece son las llamadas copias programadas. Se define un ciclo de copia para cada área con el fin de controlar el tiempo máximo entre copias completas. Amanda toma esta información estadística sobre rendimientos de copias anteriores y estima el tamaño de las copias para decidir qué nivel de copia tiene que usar. Es decir, Amanda es quien planifica qué nivel de copia de seguridad se aplica a cada máquina para cada día de la semana. Esto se aleja de la política de copia de seguridad tradicional, pero permite balancear las copias de forma que el tiempo de ejecución de cada una sea aproximadamente constante de un día para otro.

Los protocolos de copia de ficheros de red que usa Amanda son propios, es decir, no utiliza órdenes como `rsh`, `rdump` o nada que se le parezca. Cada programa cliente de Amanda escribe en la salida estándar, donde el servidor recoge y transmite los datos copiados en el disco de almacenamiento y después en la cinta. Esto permite insertar compresión y cifrado y, además, mantener un catálogo de la imagen para recuperarlo más adelante. Tanto la compresión como el cifrado son transparentes para el administrador, ya que Amanda utiliza estas dos herramientas integradas en sus propios programas de copia de ficheros.

Esta aplicación está preparada para trabajar en modo *batch*. Las máquinas cliente que no estén activas en el momento en el que se hace la copia se anotan y se saltan; se anota que de esta máquina no se ha podido hacer copia de seguridad y se pasa a hacer la de la siguiente máquina de la lista. Si se producen errores en el dispositivo de cintas, hace que a partir de aquel momento Amanda trabaje en modo degradado, es decir, solo hace la copia en el disco de almacenamiento. Y una vez resuelto el problema con las cintas, se vierte (de manera manual) la información del disco hacia las cintas.

A pesar de las múltiples funcionalidades que ofrece esta aplicación y la gran cantidad de clientes que puede llegar a manejar, Amanda es relativamente sencilla de instalar y mantener.

Para instalar el servidor Amanda, basta con descargar el archivo `amanda-x.tar.gz` de la página web http://www.amanda.org y descomprimirlo en una carpeta. Una vez hecho, ya solo queda hacer la compilación y la instalación del programa haciendo:

```
root# ./configure --with-user=backup --with-group=disk
root# make
root# make install
```

También se puede hacer de manera más sencilla usando la orden `apt-get` del sistema, en la que ya nos buscará las dependencias y nos dirá qué otros paquetes iría bien tener también instalados en el equipo para que la aplicación Amanda funcione correctamente. En este caso, sí nos sugiere que instalemos todos estos paquetes para poder hacer copias también remotas.

```
root# apt-get install amanda-server amanda-client amanda-common gnuplot dump smbclient
openbsd-inetd cifs-utils
```

Esto instalará y configurará toda la aplicación de copias de seguridad.

Se pueden cambiar los directorios en el caso de usar la instalación manual (con el `make`) pero, de no cambiarse los directorios, son los siguientes:

- `/usr/local/sbin`: para los programas que ejecuta el administrador.
- `/usr/local/bin`: para las librerías que necesita Amanda.
- `/usr/local/libexec`: para los programas propios de la aplicación Amanda.
- `/usr/local/man`: para la documentación de la aplicación.

Una vez tenemos la aplicación instalada en el equipo, es el momento de configurarla.

Primero se tiene que editar el fichero `/etc/Amanda/MyConfig/amanda.conf` y modificar los registros `org`, `mailto`, `tapecycle` y `tapedev`. El primer registro es el dominio de la organización donde queremos hacer la copia de seguridad. El segundo es el usuario de correo que recibe las notificaciones de funcionamiento de Amanda, a pesar de que no es necesario tenerlo, y en el caso de no tener el servidor de e-mail activado, no estará. El registro `tapecycle` hace referencia al número de cintas que forman parte de la rotación. En el último registro, hemos de configurar en qué dispositivo tenemos mapeado el dispositivo de cintas.

También hemos de configurar el nombre que pondremos a las cintas. Para hacerlo, modificamos el registro `labelstr` mediante las expresiones regulares. Por defecto, las cintas tienen las etiquetas de `MyData00` a `Mydata99`.

También hay que configurar los ciclos de copia, lo que se hará con el parámetro `dumpcycle`, e incluso se puede añadir un parámetro a la aplicación Amanda, que controla el ancho de banda máximo que se quiere asignar a la aplicación en el caso de usar la red para hacer la copia de seguridad de equipos remotos, de tal manera que si la red está ocupada con más tráfico del que ha configurado, no se ejecutará la copia, a la espera de que el ancho de banda baje hasta ese valor y por lo tanto se pueda iniciar la copia por la red. Esto lo lograremos con el parámetro `netusage`, donde el valor asignado denota los KB por segundo asignados.

En el caso de instalar la aplicación en un servidor en el que estén las unidades de cintas, en este archivo se verá la configuración de este tipo de cinta que tiene instalado. Como ya se ha comentado, Amanda únicamente hace copias de seguridad sobre dispositivos de cinta, por lo que, si se quiere usar un disco duro como salida de las copias, se tiene que cambiar la configuración y definir el disco como una cinta virtual. Se puede hacer de la siguiente manera:

1) Cambiamos el parámetro `tapedevide` a "`no-such-device`".

2) Cambiamos el parámetro `rawtapedev` a "`no-such-device`".

3) Cambiamos el parámetro `changerdev` a "`no-such-device`".

4) Cambiamos el parámetro `typetype` a `disksave`.

5) Creamos un nuevo tipo de cinta que será el disco duro `savedisk` y por lo tanto añadimos la siguiente definición al fichero de configuración:

```
define tapetype disksave
{comment "tape for disk"
```

```
length 1000 gbytes
filemark 0 kbytes
speed 2000 kbytes
}
```

6) Se tiene que eliminar (o comentar con `#`) la sección donde se define `holdingdisk`,

7) Cambiamos el valor de `reserve` a 30,

8) Eliminamos o comentamos el parámetro `runtapes`,

9) Indicamos el punto de montaje del disco donde se quiere hacer la copia con `diskdir`,

10) Indicamos el espacio que se quiere ocupar sobre este disco con `disksize`.

Ved también

Al final de esta sección se muestra un ejemplo de este archivo de configuración (extraído de http://www.sergiogonzalez.com).

Una de las tareas que hace la instalación es crear un usuario, si no existe, denominado `backup` o a veces `amanda`. Este usuario es el que tenemos que utilizar para trabajar con la aplicación de copias de seguridad, de este modo no se configurará desde el usuario *root* y en el caso de tener algún *0day* que afecte directamente a este software, no se dispondrán de privilegios de *root* en el sistema.

El siguiente paso es etiquetar las cintas de manera correcta. Para hacerlo, tenemos que ejecutar la orden siguiente:

```
root# su - backup
backup$ amlabel MyConfigSet1 tape_label
```

Si nuestro dispositivo de cintas tiene más de un *slot* de cintas, tenemos que ejecutar:

```
backup$ amlabel MyConfigSet1 tape_label slot num_slot
```

Cabe notar que se ha cambiado de usuario y ahora se usa el usuario `backup`, o `amanda`, dependiendo de lo que se haya configurado en el archivo `amanda.conf`.

En el caso de que, por error, se introduzca una cinta que no corresponde por la numeración, es decir, que necesita la cinta 2 y se ha introducido la 3, la aplicación Amanda lo detecta y no proseguirá con la ejecución de la copia de seguridad.

Ahora es necesario incluir las máquinas y los directorios de los que queremos hacer la copia de seguridad, ya sea de toda la máquina o de alguna carpeta. Imaginemos que queremos hacer una copia de seguridad de las particiones `/`

`home` y `/usr` de una máquina llamada `P1S1`. Para hacerlo, debemos modificar en el servidor el archivo `/etc/amanda/Myconfig/disklist` añadiendo unas líneas parecidas a estas:

```
P1S1 /home comp-root-tar
P1S1 /usr comp-root-tar
```

Consultar el manual

Consultar el `man` para ver el formato de la instrucción y excluir directorios de copia de seguridad.

Tenemos que añadirle una línea parecida a la anterior para cada partición de la máquina de la que queremos hacer una copia de seguridad. Es decir, si queremos hacer una copia de todo el equipo y este tiene cuatro particiones (`/`, `/home`, `/usr`, `/var`), debemos añadir cuatro líneas a este fichero, una por cada partición. Si solo tiene una partición, basta con añadir una sola línea en el directorio raíz para hacer una copia de seguridad de toda la máquina. Si queremos hacer copias de seguridad de los discos de la máquina de los que es servidor Amanda, también tenemos que añadir las líneas correspondientes en este fichero. Es recomendable usar el nombre completo de la máquina y no `localhost` si hacemos la copia de seguridad del servidor Amanda, así identificaremos mejor qué máquina se está configurando y se podrá exportar la configuración.

En el archivo de configuración de la aplicación Amanda, está la definición de cada uno de los tipos de copias de seguridad que se pueden hacer, y que en este fichero `disklist` asociaremos a cada directorio de donde se quiere hacer la copia.

Finalmente, solo hace falta dar permisos. Hay dos tipos de permisos: el primero se da al cliente para que pueda entrar en el servidor a hacer las copias de seguridad, y el segundo se da al servidor para que el cliente pueda entrar a restaurar las copias de seguridad. Para hacerlo, tenemos que usar el *home* del usuario que utilizaremos para hacer la copia de seguridad (por defecto es el usuario `backup` o `amanda`), editar el fichero `.amandahost` y añadirle una línea con el nombre de la máquina y el usuario al que queremos entrar. Imaginemos que el servidor se llama `backupserver` y el cliente se llama `P1S1`. En el fichero `.amandahost` del servidor tenemos que poner:

```
P1S1 backup
P1S1 root
```

Y en el fichero `.amandahost` del cliente añadimos una línea parecida a la siguiente:

```
backupserver backup
```

Una vez dados los pasos anteriores, ya estamos en disposición de hacer una copia de seguridad. Para hacerla, primero comprobamos que están puestas las cintas correspondientes al día de hoy mediante la orden

```
backup$ amcheck -t MyConfig
```

Una vez hecha la comprobación y solucionados los posibles errores que devuelva esta aplicación, que comprueba el fichero de configuración, ejecutamos la copia de seguridad. Tenemos que usar la orden siguiente para llevar a cabo la copia de seguridad correspondiente a todo hoy:

```
backup$ amdump MyConfig
```

Las opciones más importantes de `amcheck`

- `m`: no sale nada por pantalla pero envía un correo electrónico en el caso de que se detecte algún error.
- `c`: ejecuta una revisión médica en el cliente.
- `l`: ejecuta una revisión médica en el servidor local.
- `t`: ejecuta una revisión médica en el dispositivo de cintas.
- `s`: ejecuta una revisión médica en el servidor local y en el dispositivo de cintas (es lo mismo que ejecutar `amcheck` con las opciones `lt`).
- `w`: activa la destrucción de la protección contra escritura. Atención: este parámetro es destructivo, es decir, borra la información que había en la cinta.

Si solo queremos hacer la copia de seguridad de una única máquina, ejecutamos la orden:

```
backup$ amadump MyConfig Machine_name
```

Antes de empezar a hacer la copia de seguridad de manera periódica, debemos comprobar que la copia funciona. La mejor manera de hacerlo es restaurando un directorio de la copia de seguridad. Para ello, tenemos que ir a una copia de la máquina cliente y ejecutar:

```
root# amrecover MyConfig -s server_name backup
```

Entramos en una consola interactiva y ejecutamos las órdenes siguientes:

```
Amrecover> cd directorio_que_queremos_restaurar
Amrecover> add fichero_que_queremos_restaurar
Amrecover> add directorio_que_queremos_restaurar
Amrecover> extract
```

Si la recuperación se hace de modo satisfactorio, ya podemos empezar a hacer la copia de seguridad de manera periódica. Para hacerlo, tenemos que añadir una línea en la orden `crontab`.

Para acceder a la `crontab` tenemos que ejecutar la orden:

```
root# crontab -e
```

La línea que tenemos que añadir es la siguiente:

```
10 01 * * 1-5 su backup -c "/usr/sbin/amdump MyConfig"
```

Mediante esta línea ejecutamos todos los días (de lunes a viernes), a la una y diez de la madrugada, la copia de seguridad diaria. Esto hará cada día una copia de seguridad, pero si queremos que esta copia se guarde en cintas, tenemos que poner cada día las cintas que toquen en el dispositivo de cintas. Esta tarea se tiene que hacer de manera manual. Como ejecutamos Amanda como un proceso y no como un demonio, si queremos parar el servidor de copias de seguridad tenemos que matar el proceso. Si queremos añadir o retirar una máquina del servidor de copia de seguridad, tenemos que rehacer los pasos anteriores de la configuración.

Ejemplo de fichero `amanda.conf` (http://www.sergio-gonzalez.com)

```
#
# amanda.conf - sample Amanda configuration file.
#
# If your configuration is called, say, "DailySet1", then this file
# normally goes in /etc/amanda/DailySet1/amanda.conf.
#
# for explanation of the parameters refer to amanda(8) and
# /usr/doc/amanda/WHATS.NEW.gz

org "Diaria"          # your organization name for reports
mailto "amanda"       # space separated list of operators at your site
dumpuser "amanda"     # the user to run dumps under
#
inparallel 4          # maximum dumpers that will run in parallel
netusage  600         # maximum net bandwidth for Amanda, in KB per sec

# a filesystem is due for a full backup once every <dumpcycle> days
dumpcycle 4 weeks     # the number of days in the normal dump cycle
tapecycle 8 tapes     # the number of tapes in rotation

bumpsize 1 MB       # minimum savings (threshold) to bump level 1->2
bumpdays     1      # minimum days at each level
bumpmult     4      # threshold = bumpsize * (level-1)**bumpmult

#runtapes     9       # explained in WHATS.NEW
#tpchanger "no-changer" # the tape-changer glue script, see TAPE.CHANGERS
tapedev "no-such-device"      # Linux @ tuck, important: norewinding
rawtapedev "no-such-device"  # the raw device to be used (ftape only)
#changerfile "/mnt/amanda/changer"
```

```
changerdev "no-such-device"

tapetype DISKSAVE    # what kind of tape it is (see tapetypes below)
labelstr "^HISS[0-9][0-9]*$"  # label constraint regex: all tapes must match

diskdir "/mnt/backup"         # where the holding disk is
disksize 10 MB                # how much space can we use on it
reserve 30
#diskdir "/dumps/amanda/work" # additionaly holding disks can be specified
#diskdir "/mnt/disk4"
#disksize 1000 MB             #       they are used round-robin


# Amanda needs a few MB of diskspace for the log and debug files,
# as well as a database.  This stuff can grow large, so the conf directory
# isn't usually appropriate.

infofile "/var/lib/amanda/DailySet1/curinfo"    # database filename
logfile  "/var/log/amanda/DailySet1/log"        # log filename

# where the index files live
indexdir "/var/lib/amanda/DailySet1/index"

# Specify holding disks.  These are used as a temporary staging area for
# dumps before they are written to tape and are recommended for most sites.
# The advantages include: tape drive is more likely to operate in streaming
# mode (which reduces tape and drive wear, reduces total dump time); multiple
# dumps can be done in parallel (which can dramatically reduce total dump time.
# The main disadvantage is that dumps on the holding disk need to be flushed
# (with amflush) to tape after an operating system crash or a tape failure.
# If no holding disks are specified then all dumps will be written directly
# to tape.  If a dump is too big to fit on the holding disk than it will be
# written directly to tape.  If more than one holding disk is specified then
# they will all be used round-robin.

#holdingdisk hd1 {
#    comment "main holding disk"
#    directory "/mnt/amanda1"   # where the holding disk is
#    use 30 Mb           # how much space can we use on it
#                        # a non-positive value means:
#                        #        use all space but that value
#    chunksize 1Mb       # size of chunk if you want big dump to be
#                        # dumped on multiple files on holding disks
#                        #  N Kb/Mb/Gb split images in chunks of size N
#                        #             The maximum value should be
#                        #             (MAX_FILE_SIZE - 1Mb)
#                        #  0          same as INT_MAX bytes
```

```
#}

# tapetypes
#
# Define the type of tape you use here, and use it in "tapetype" above.
# Some typical types of tapes are included here.  The tapetype tells amanda
# how many MB will fit on the tape, how big the filemarks are, and how
# fast the tape device is.
#
# For completeness Amanda should calculate the inter-record gaps too, but it
# doesn't.  For EXABYTE and DAT tapes this is ok.  Anyone using 9 tracks for
# amanda and need IRG calculations?  Drop me a note if so.

define tapetype DISKSAVE  {
   comment "Fake tape description for save to disk"
   length 1000 gbytes
   filemark 0 kbytes
   speed 2000 kbytes
}

define tapetype QIC-60 {
    comment "Archive Viper"
    length 60 mbytes
    filemark 100 kbytes         # don't know a better value
    speed 100 kbytes            # dito
}

define tapetype DEC-DLT2000 {
    comment "DEC Differential Digital Linear Tape 2000"
    length 15000 mbytes
    filemark 8 kbytes
    speed 1250 kbytes
}

# goluboff@butch.Colorado.EDU
# in amanda-users (Thu Dec 26 01:55:38 MEZ 1996)
define tapetype DLT {
    comment "DLT tape drives"
    length 20000 mbytes         # 20 Gig tapes
    filemark 2000 kbytes        # I don't know what this means
    speed 1500 kbytes
}

define tapetype SURESTORE-1200E {
    comment "HP AutoLoader"
    length 3900 mbytes
    filemark 100 kbytes
```

```
    speed 500 kbytes
}

define tapetype EXB-8500 {
    comment "Exabyte EXB-8500 drive on decent machine"
    length 4200 mbytes
    filemark 48 kbytes
    speed 474 kbytes
}

define tapetype EXB-8200 {
    comment "Exabyte EXB-8200 drive on decent machine"
    length 2200 mbytes
    filemark 2130 kbytes
    speed 240 kbytes
}

define tapetype HP-DAT {
    comment "DAT tape drives"
    length 1900 mbytes          # these numbers are not accurate
    filemark 100 kbytes         # but you get the idea
    speed 500 kbytes
}

define tapetype DAT {
    comment "DAT tape drives"
    length 1000 mbytes          # these numbers are not accurate
    filemark 100 kbytes         # but you get the idea
    speed 100 kbytes
}

define tapetype MIMSY-MEGATAPE {
    comment "Megatape (Exabyte based) drive through Emulex on Vax 8600"
    length 2200 mbytes
    filemark 2130 kbytes
    speed 170 kbytes            # limited by the Emulex bus interface, ugh
}

define tapetype QIC-3080 {
    comment "QIC 3080"
    length 2000 mbytes
    filemark 64 kbytes
    speed 250 kbytes
}

# dumptypes
#
```

```
# These are referred to by the disklist file.  The dumptype specifies
# certain "options" for dumping including:
#       index         - keep an index of the files backed up
#       compress-fast - (default) compress on the client using fast algorithm
#       compress-best - compress using the best (and slowww) algorithm
#       no-compress   - don't compress the dump output
#       srvcompress   - Compress dumps on the tape host instead of client
#                           machines.  This may be useful when a fast tape host
#                           is backing up slow clients.
#       record        - (default) record the dump in /etc/dumpdates
#       no-record     - don't record the dump, for testing
#       no-hold       - don't go to the holding disk, good for dumping
#                           the holding disk partition itself.
#       skip-full     - Skip the disk when a level 0 is due, to allow
#                           full backups outside Amanda, eg when the machine
#                           is in single-user mode.
#       skip-incr     - Skip the disk when the level 0 is NOT due.  This
#                           is used in archive configurations, where only full
#                           dumps are done and the tapes saved.
#       no-full       - Do a level 1 every night.  This can be used, for
#                           example, for small root filesystems that only change
#                           slightly relative to a site-wide prototype.  Amanda
#                           then backs up just the changes.
#
# Also, the dumptype specifies the priority level, where "low", "medium" and
# "high" are the allowed levels.  These are only really used when Amanda has
# no tape to write to because of some error.  In that "degraded mode", as
# many incrementals as will fit on the holding disk are done, higher priority
# first, to insure the important disks are dumped first.

define dumptype always-full {
    comment "Full dump of this filesystem always"
    options no-compress
    priority high
    dumpcycle 0
    maxcycle 0
}

define dumptype comp-user-tar {
    program "GNUTAR"
    comment "partitions dumped with tar"
    options compress-fast, index, exclude-list "/etc/amanda/exclude.gtar"
    priority medium
}

define dumptype comp-root-tar {
    program "GNUTAR"
```

```
    comment "Root partitions with compression"
    options compress-fast, index, exclude-list "/etc/amanda/exclude.gtar"
    priority low
}

define dumptype user-tar {
    program "GNUTAR"
    comment "partitions dumped with tar"
    options no-compress, index, exclude-list "/etc/amanda/exclude.gtar"
    priority medium
}

define dumptype high-tar {
    program "GNUTAR"
    comment "partitions dumped with tar"
    options no-compress, index, exclude-list "/etc/amanda/exclude.gtar"
    priority high
}

define dumptype root-tar {
    program "GNUTAR"
    comment "Root partitions dumped with tar"
    options no-compress, index, exclude-list "/etc/amanda/exclude.gtar"
    priority low
}

define dumptype comp-user {
    comment "Non-root partitions on reasonably fast machines"
    options compress-fast
    priority medium
}

define dumptype nocomp-user {
    comment "Non-root partitions on slow machines"
    options no-compress
    priority medium
}

define dumptype holding-disk {
    comment "The master-host holding disk itself"
    options no-hold
    priority medium
}

define dumptype comp-root {
    comment "Root partitions with compression"
    options compress-fast
```

```
    priority low
}

define dumptype nocomp-root {
    comment "Root partitions without compression"
    options no-compress
    priority low
}

define dumptype comp-high {
    comment "very important partitions on fast machines"
    options compress-best
    priority high
}

define dumptype nocomp-high {
    comment "very important partitions on slow machines"
    options no-compress
    priority high
}

define dumptype nocomp-test {
    comment "test dump without compression, no /etc/dumpdates recording"
    options no-compress, no-record
    priority medium
}

define dumptype comp-test {
    comment "test dump with compression, no /etc/dumpdates recording"
    options compress-fast, no-record
    priority medium
}
```

Ejemplo de fichero disklist

```
# sample Amanda2 disklist file, derived from CS.UMD.EDU's disklist
#
# If your configuration is called, say, "DailySet1", then this file
# normally goes in /etc/amanda/DailySet1/disklist.
#
# File format is:
#
#       hostname diskdev dumptype
#
# where the dumptypes are defined by you in amanda.conf.
# Configuración
```

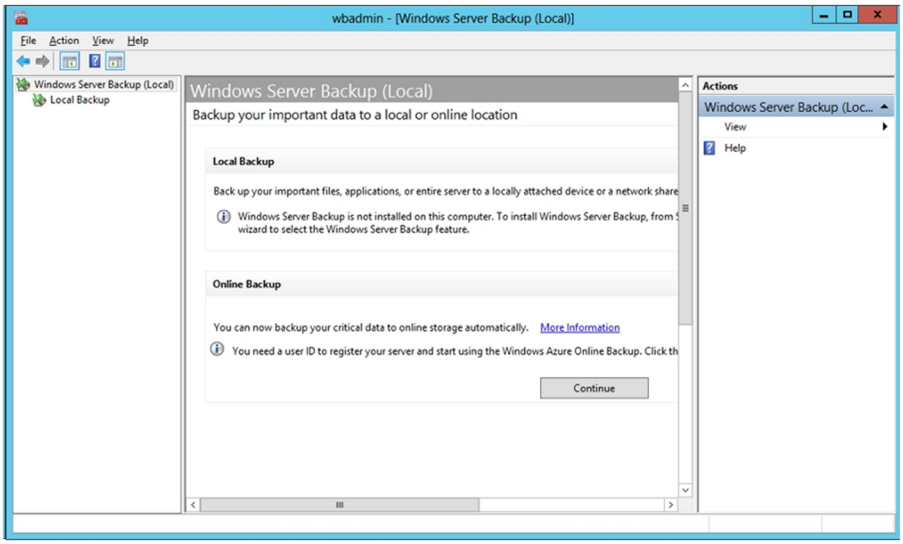
```
localhost /mnt/copia comp-root-tar
```

2.2. Herramientas de copia de seguridad en Windows Server

2.2.1. Ejecución de copias de seguridad en Windows Server 2012

Se puede acceder al programa de copia de seguridad de Windows Server 2012 desde las herramientas administrativas, el Windows Server Backup (podéis ver la figura siguiente):

Windows Server Backup



En esta figura, podemos ver que se pueden llevar a cabo las copias de dos maneras diferentes, una sobre el mismo servidor, en local, y la otra mediante Internet y el programa Azure Online Backup de Microsoft, que es un software que nos ayuda a las gestiones de los servidores haciendo copias y securizando datos en la nube. Tal como se puede ver en la figura anterior, ninguna de las dos opciones está instalada por defecto en el servidor y se tiene que ejecutar el proceso de instalación de una característica o del propio programa Azure.

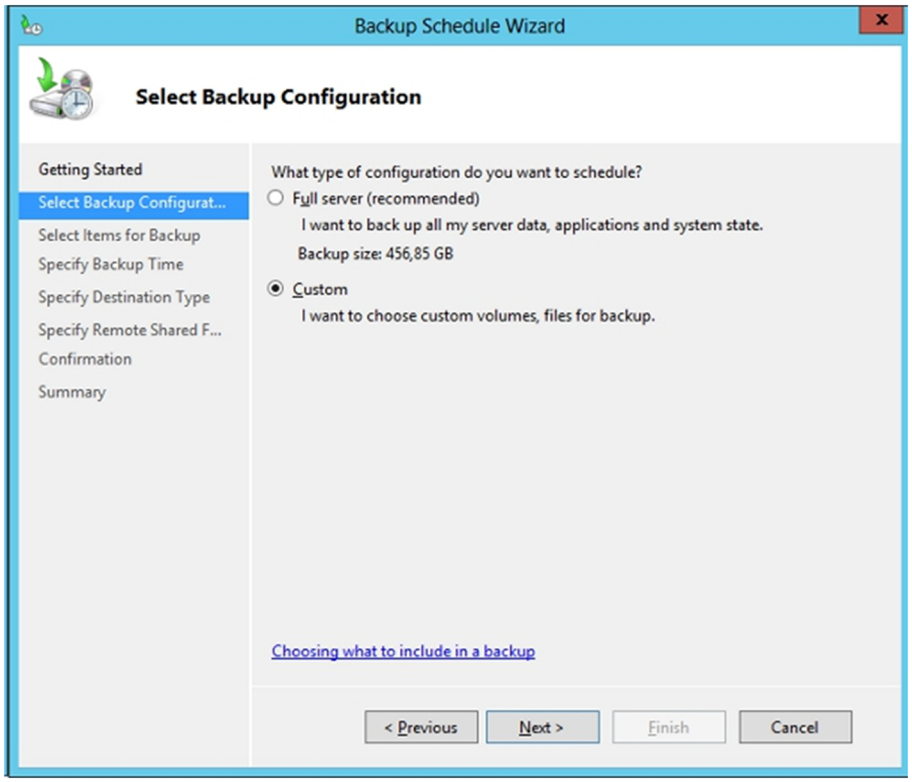
Solo hay que abrir el administrador del servidor donde están los roles y características, buscar esta en la lista y decirle que lo instale en el servidor.

Una vez se ha instalado la característica volvemos a abrir el Windows Server Backup y ahora sí se puede ejecutar ya la configuración de las copias de seguridad en local. Hay dos opciones para configurarlas, hacer una copia planificada o una copia única, que se ejecutará en el momento y ya no se volverá a hacer.

Lo más normal será planificar las copias, a pesar de que puntualmente se podría necesitar hacer una copia entera en un momento dado fuera de la planificación, posiblemente porque se quiere instalar un nuevo hardware dentro del servidor, o un software que puede interactuar con otras partes y tener proble-

mas. Por lo tanto, se ejecutará el asistente de copias planificadas. Únicamente se tiene que ir contestando a las diferentes opciones que tiene dependiendo de lo que interese más. No obstante, en el caso de decidir qué hay que hacer, si una copia de todo el disco o de partes del disco, podemos decidir hacer una copia selectiva, puesto que podemos incluir aquellas partes que nos interesan y excluir también aquellas de las que no hay que hacer copias de seguridad. La figura siguiente nos muestra la pantalla de la configuración de estas copias de seguridad.

Administrador de copias de seguridad locales



En este caso, se podrá incluir una configuración adecuada en las diferentes necesidades y podemos seleccionar entre:

- Todo el equipo.
- El estado del sistema (registro, configuración actual y estado del sistema o Active Directory si se trata de un controlador de dominio).
- La parte de arranque del sistema.
- Los discos duros.

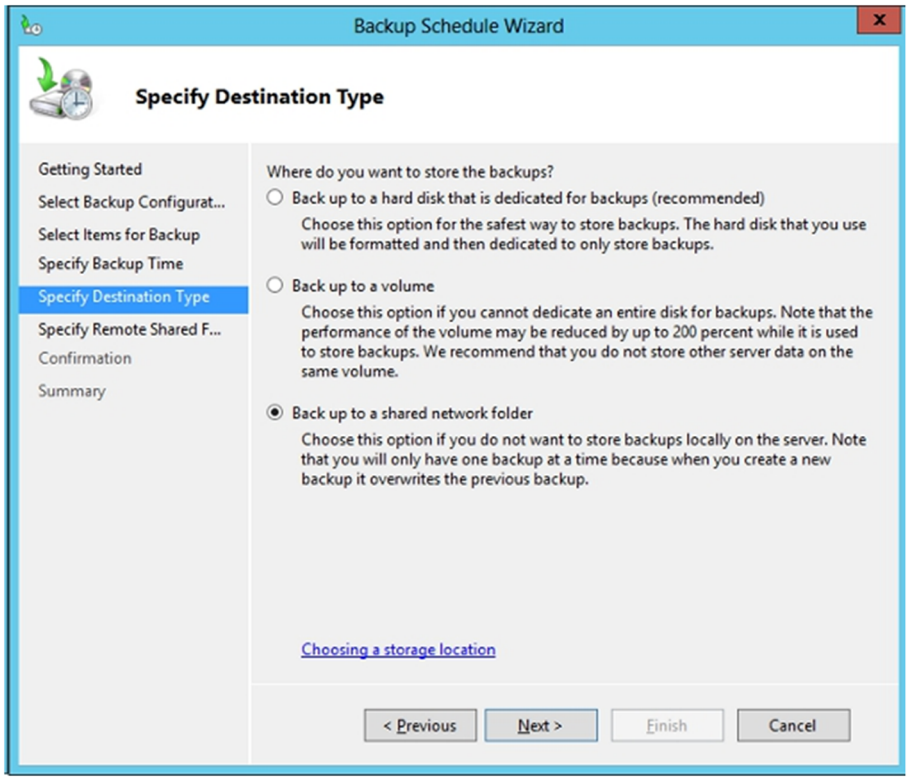
Y además se podrá incluir también en la misma pantalla las exclusiones de la parte que se ha seleccionado y que no hay que hacer copias. Por ejemplo, si por comodidad se ha seleccionado todo el disco duro, se puede excluir de hacer

copias de las papeleras de reciclaje de los usuarios, los directorios temporales o los directorios temporales de las actualizaciones, por ejemplo, así la copia ocupa menos espacio y tiempo.

Lo siguiente que hay que configurar es el momento en el que se hacen las copias de seguridad de lo que se ha seleccionado. Si es de todo el disco, tardará bastante y se tendrá que planificar por la noche, si es del directorio de usuarios y los perfiles, se tendrá que hacer cuando ya se hayan marchado todos y no haya más cambios. Una cuestión importante que se debe tener en cuenta a la hora de pensar en cómo hacer las copias es que este software no permite planificar copias que no sean diarias, por lo tanto, una copia diaria de todo el disco duro del servidor no tiene sentido y especificaremos en el administrador del Windows Server Backup que se hagan las copias de los discos enteros de forma incremental, así se reduce considerablemente el tamaño de estas copias. Pero también lo usaremos para hacer la copia de aquella parte que cambia todos los días, que podría ser las carpetas de usuario y los perfiles de este. Por lo tanto, deberemos añadir estos directorios a la parte donde se incluye aquello de lo que se quiere hacer copia, y no hacerla de todo el sistema.

El siguiente paso es configurar dónde se guardan los ficheros de las copias. La figura siguiente muestra las tres opciones que hay disponibles, usar un disco duro específico para esta finalidad es la manera más segura puesto que no accederemos a este disco por otros propósitos, únicamente para hacer las copias. La segunda opción es usar un disco compartido con otros fines, pero se debe tener en cuenta que se verá muy afectada la capacidad de este disco. Y la tercera opción es usar la red para tener en otro servidor los datos duplicados de los usuarios, por si a este servidor le pasa algo. Es la más segura, pero también la más lenta y costosa, ya que debemos tener otro equipo preparado para guardar los datos. Además, se tendrá que usar un usuario que se valide con los dos equipos, el remoto y el servidor local, y que además en este último caso tenga el grupo de operadores de *backup*.

Configuración del destino de copias



Con esta parte ya queda configurada la copia de seguridad de los datos de los usuarios o de los servidores enteros. Tal como podemos ver, esta herramienta en local no deja configurarse mucho, ya que solo permite una única política de copias de seguridad, no permite hacer dos tipos de copias ni podemos hacer incrementales o diferenciales sobre carpetas de usuario.

2.2.2. Otras herramientas de copias de seguridad

Tal como se ha visto, el software que tiene por defecto el Windows Server es bastante reducido teniendo en cuenta el que se podría necesitar en una empresa mediana. Para una empresa pequeña con una decena de usuarios quizás ya iría bien, pero para empresas medianas y grandes es del todo insuficiente.

Para solucionar esta carencia, Microsoft lanza una plataforma llamada Azure en la que se puede trabajar en la nube y hacer las copias de seguridad directamente desde el mismo gestor de copias, pero en lugar de tener un punto de red local o un disco duro o USB instalado en el mismo servidor, lo gestiona todo con un disco virtual que se tiene que pagar por la cantidad de transferencia que se use. En la web de Azure se puede contratar y vincular el espacio de este disco virtual a la nube con el directorio activo que hay configurado en el servidor.

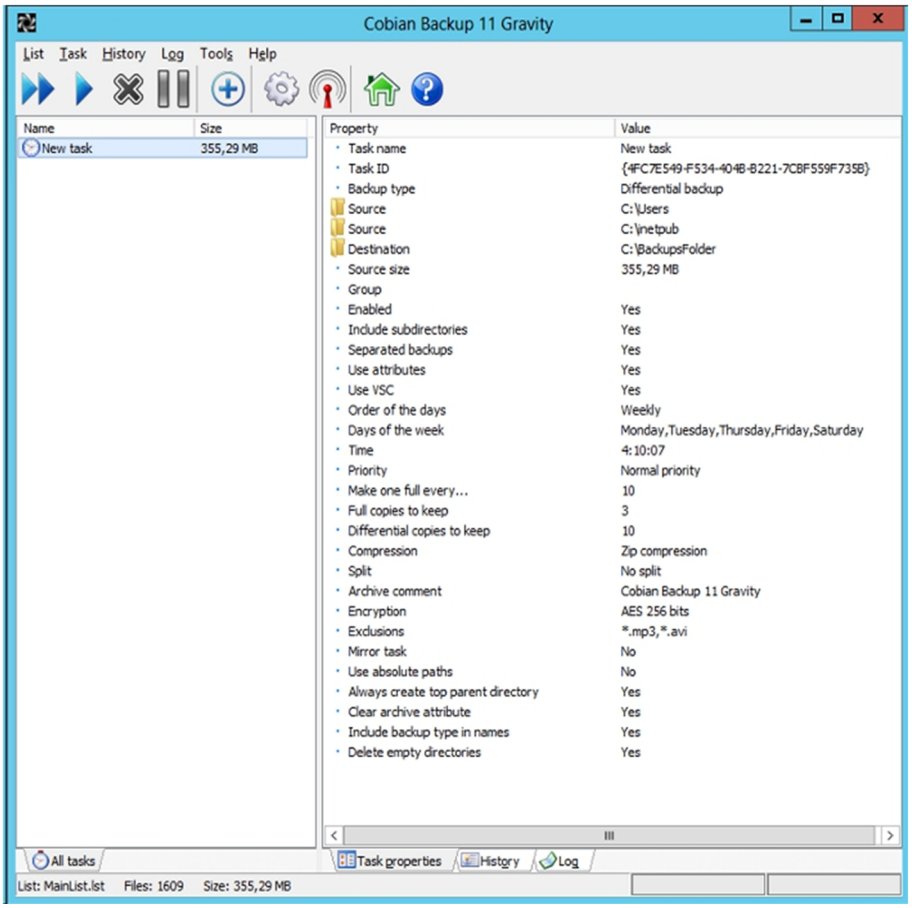
Web recomendada

Se puede encontrar más información en http://www.windowsazure.com.

Otra solución que se puede usar es utilizar alguna de las múltiples herramientas que hay en el mercado que realizan copias de seguridad para sistemas Windows y las hay de pago y gratuitas. Dentro de esta última clasificación podemos encontrar una muy ligera y sencilla de usar como es la Cobian Backup, que en su última versión, la 11, se puede configurar para que realice copias

incrementales, diferenciales, completas, de todo el disco y de directorios. Asimismo, se pueden hacer las copias sobre discos, por FTP o por red local, entre otros, y además se pueden cifrar los documentos de la copia y comprimirlos para que ocupen menos. Se trata de una herramienta muy completa para poder hacer copias de seguridad con mucha facilidad. En la figura siguiente, podemos ver cómo se ha configurado una copia diferencial de las carpetas de los usuarios y de la página web algunos días de la semana con exclusiones de algunos archivos y cifrando y comprimiendo los ficheros que formarán la copia de seguridad.

Configuración de una copia de seguridad



2.2.3. Restauración de copias de seguridad en Windows Server 2012

Para restaurar una copia de seguridad hecha con el programa de copia de seguridad de Windows, seleccionamos la opción Asistente para restauración de la pantalla inicial. A continuación, se inicia el asistente. En la pantalla siguiente se muestran las copias de seguridad que se han hecho. Podemos restaurar una copia o varias copias de seguridad, o incluso solo una parte de estas copias.

En segundo lugar, podemos seleccionar otras opciones de comportamiento de la copia de seguridad, como la acción que hay que llevar a cabo cuando los archivos que se restauren ya estén en el medio de destino. Por último, sale la pantalla de fin del asistente de restauración de copias de seguridad. Una vez finalizamos, empieza el proceso de restauración de los archivos.

2.3. Dispositivos de copia de seguridad

Los dispositivos tradicionales de copia de seguridad han sido desde hace muchos años las cintas. Sin embargo, esto no impide que sean los únicos dispositivos de copia de seguridad; también tenemos CD y DVD, los discos duros, los robots de grandes discos de copia, los servidores FTP o de ficheros, entre otros.

Los DVD son los dispositivos de copia de seguridad más extendidos entre las pequeñas y medianas empresas. Estos dispositivos también son los más utilizados entre los usuarios domésticos que tienen necesidad de hacer copias de seguridad de los documentos. El éxito de este dispositivo lo encontramos en el coste que tiene. Hoy en día, una grabadora de DVD tiene un coste muy bajo. La limitación que tiene este dispositivo es la capacidad de almacenar información, que es de 4,7 GB o de 9,6 GB. A pesar de que hay DVD regrabables, la mayoría de la gente utiliza los discos que solo se pueden grabar una vez (si la copia sale mal, tenemos que tirar el disco) porque al final son mucho más cómodos de usar, puesto que no hay que formatearlos y tienen un coste muy bajo.

Las cintas han sido desde el comienzo los dispositivos de copia de seguridad más utilizados, ya que antes no había medios donde poder guardar grandes cantidades de información. Hoy en día, ya son pocas las empresas que, a pesar de requerir una gran capacidad de copia de seguridad, usan las cintas como dispositivo de copia, ya que se han sustituido por los grandes robots de copias de seguridad con discos extraíbles y los servidores virtuales en la nube, donde se pueden hacer las copias directamente sin tener los problemas que pueden tener las copias en local y el almacenamiento de las cintas.

Aun así, todavía hay pequeñas y medianas empresas que siguen usando las cintas magnéticas, puesto que tienen bastantes ventajas:

1) La capacidad de almacenar información. Pueden llegar a almacenar hasta 600 GB o más.

2) La capacidad de uso. Una cinta se puede utilizar muchas veces.

Pero el inconveniente más grande es el precio y la lentitud que tienen. Esta lentitud se debe al hecho de que las cintas tienen acceso secuencial, es decir, que para llegar al registro 3 tienen que pasar primero por el 1 y por el 2. Por lo tanto, si se quiere recuperar un archivo que está al final de la cinta, se tiene que recorrer toda la cinta antes de recuperarlo.

Hay muchas marcas y dispositivos de cinta. Casi cada marca utiliza una nomenclatura de tipo de cinta diferente. Sin embargo, hay dos tipos de cinta muy implantados en el mercado, como son las cintas DAT y las DLT. Este tipo de nomenclatura nos indica la capacidad de la cinta sin comprimir y la capacidad con los datos comprimidos.

La cinta DLT clásica tiene una capacidad de 40 a 80 GB. Hoy en día, han aparecido en el mercado dispositivos más modernos, que usan formatos parecidos al de esta cinta. Son los llamados Super DLT, que pueden llegar a almacenar de 300 a 600 GB de información. Los dispositivos de cintas más frecuentes en el mercado son los que tienen capacidad para una sola cinta, pero también los hay con capacidades superiores.

El inconveniente es claramente el precio. Estos dispositivos son muy caros y, a pesar de que las cintas son cada vez más rápidas, el acceso secuencial siempre es una desventaja. En resumen, igual que tenemos que definir una política de copia de seguridad que satisfaga nuestros requisitos, debemos elegir un dispositivo de copia de seguridad que se adapte a nuestras necesidades. Los factores que debemos tener en cuenta son la capacidad de información de la que queremos hacer una copia de seguridad y el precio que estamos dispuestos a pagar.

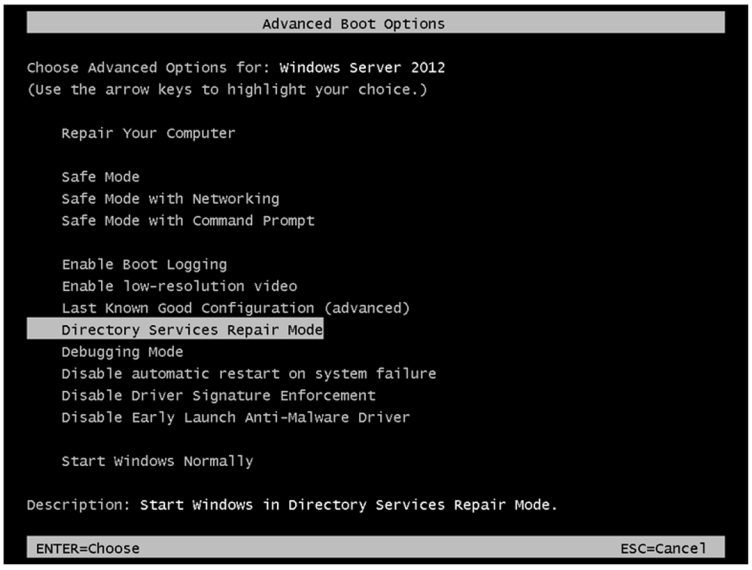
3. Sistemas de recuperación en Windows Server 2012

A veces, cuando se produce un error en el sistema, es posible solucionar el problema con los mecanismos que proporciona Windows. Veamos a continuación algunos de estos mecanismos.

3.1. Arranque en modo seguro

Cuando se produce un error grave del sistema que hace que se quede bloqueado, o que se reinicie automáticamente o se apague el ordenador, el propio sistema hará que en el arranque salga el menú de opciones. Además, podemos hacer que salga un menú de arranque si pulsamos la tecla F8 cuando arranca el sistema y justo sale el logotipo de Windows.

Opción de arranque del sistema



Las diferentes opciones del menú de inicio mostradas en la figura anterior nos permiten iniciar el sistema de diferentes maneras:

1) Modo seguro. Permite iniciar el sistema con el mínimo de controladores y servicios necesarios.

2) Modo seguro con funciones de red. Igual que el modo seguro, pero habilita los controladores y servicios necesarios para utilizar la red.

3) Modo seguro con símbolo del sistema. Igual que el modo seguro, pero se abre una sesión de línea de órdenes, en lugar del escritorio de Windows.

4) Habilitar el registro de inicio. Crea un archivo de registro de todas las incidencias de inicio de los componentes del sistema a medida que se cargan. Este archivo de registros se denomina nrblog.txt y se encuentra en la carpeta de Windows (por ejemplo, c:\windows). El resto de opciones de inicio también crean este archivo de registro (excepto la opción de utilizar la última configuración conocida).

5) Habilitar el modo VGA. Inicia el sistema en modo VGA en lugar de utilizar el controlador de vídeo habitual.

6) La última configuración buena conocida. Inicia el sistema utilizando la misma configuración que la última vez en la que se ha iniciado correctamente el sistema, es decir, la última sesión en la que no ha fallado ningún controlador o servicio al iniciar el sistema.

7) Modo de restauración de los servicios de directorio. Permite recuperar la base de datos del directorio activo. Esta opción solo es válida para controladores de dominio que ya estén configurados como tales.

8) Modo de depuración. Sirve para iniciar el sistema enviando información de depuración mediante un cable de serie a otro equipo conectado, en el que se está ejecutando un depurador.

9) Deshabilita el arranque automático en caso de detectar problemas graves en el servidor. Esto puede ser útil en casos en los que se esté configurando el hardware.

10) Deshabilitar la comprobación de los controladores firmados.

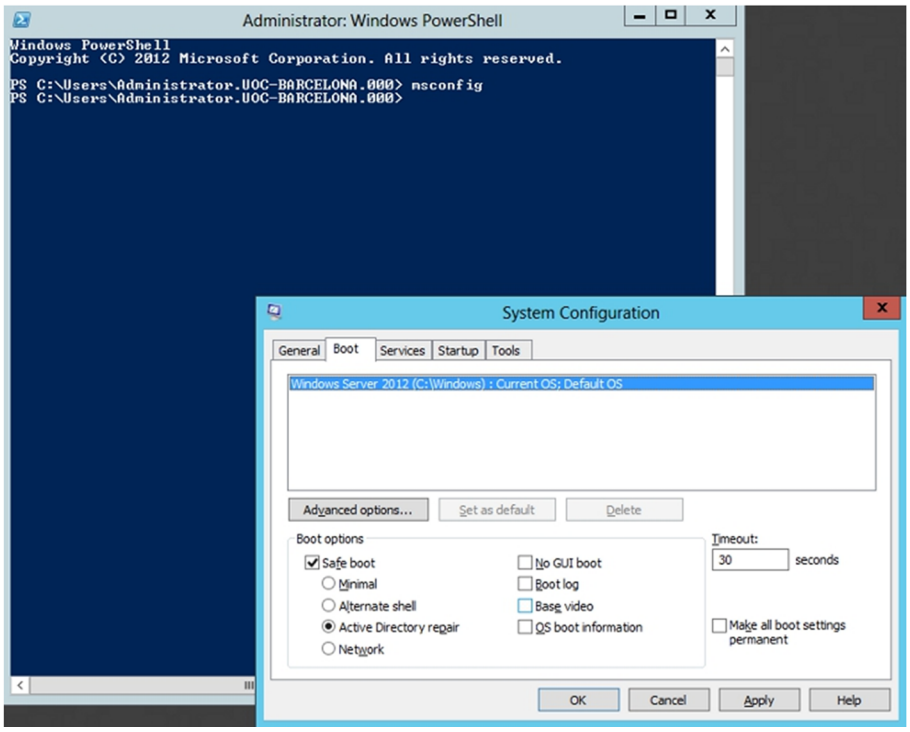
11) Deshabilita el lanzamiento rápido del controlador *antimalware*, por si tenemos problemas con este *driver*.

Una vez se reinicia en modo seguro, se tendrá que iniciar la sesión dentro del servidor con el dominio de la propia máquina y el administrador local, ya que el servidor de dominio, el servidor de nombres (DNS) y otros servidores dejarán de funcionar y no se arrancará el servicio, por lo que se podrán desempeñar tareas de mantenimiento sin que afecten a todo el servicio.

También se puede iniciar esta pantalla de arranque a partir del programa de configuración `msconfig.exe`, donde podemos fijar las diferentes opciones que se quiere en el momento de hacer el arranque del sistema. En la figura siguiente se muestra esta aplicación. Se puede configurar para que arranque unos servicios determinados o en modo seguro, entre otros.

Una vez se hayan solucionado los problemas y se quiera volver al sistema normal de arranque, se tiene que volver a entrar en el configurador de arranque (`msconfig.exe`) y deseleccionar que se inicie en modo seguro, de otro modo volvería a arrancar en esta misma configuración.

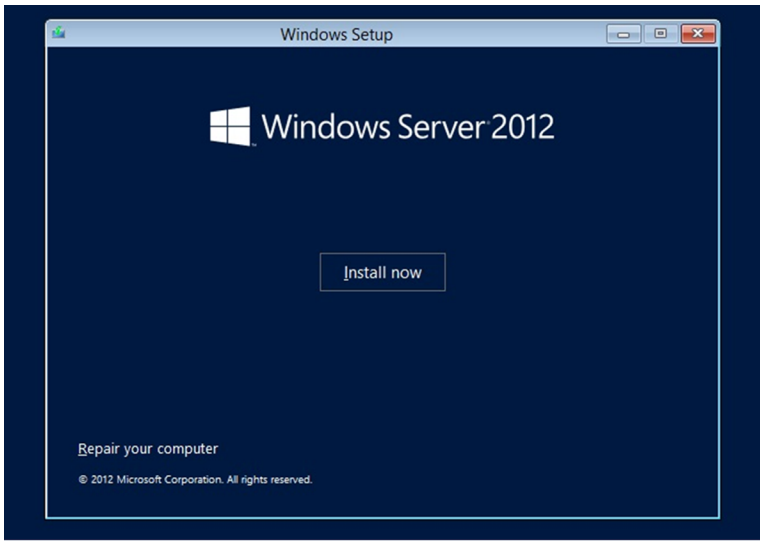
Configuración del arranque del sistema



3.2. Sistemas de recuperación de Windows Server 2012

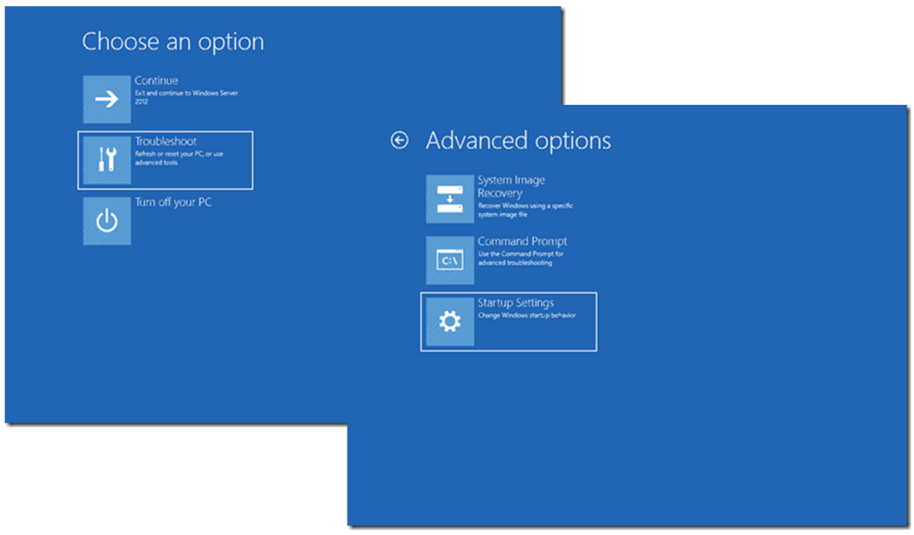
Cuando queremos recuperar un sistema en el que no arranca el modo gráfico, debemos recurrir a herramientas que nos proporciona el mismo sistema operativo, a las que se puede acceder arrancando con el CD de instalación del sistema. Para todas estas herramientas, tenemos que iniciar la instalación del sistema operativo. Para el caso de la consola de recuperación, tenemos que dejar que inicie la instalación y, en el primer cuadro de diálogo, elegir la opción de “Recuperar el servidor”, tal como muestra la figura siguiente.

Pantalla para recuperar el sistema



Una vez se inicia el sistema en modo reparación, aparecen unas pantallas en las que se puede elegir lo que se quiere hacer, que puede ser iniciar una consola donde poder interactuar con el sistema o recuperar el sistema a partir de una copia de seguridad hecha con anterioridad desde el propio sistema operativo con el Windows Server Backup, si se ha hecho de todo el sistema, seleccionando la opción de System Image Recovery. Por lo tanto, una vez tengamos el sistema completamente instalado y configurado, es muy adecuado hacer una copia entera de todo el sistema, e incluso poderla hacer de modo regular, ya que esto nos permitirá poder recuperar todo el sistema de una manera muy rápida y poder tener en producción el servidor lo antes posible. La ventaja de poder hacer esto al reinstalar todo el sistema otra vez desde el inicio es considerable, además de poder recuperar todo el sistema operativo neto en el caso de que se haya tenido una intrusión dentro del sistema. La imagen muestra las opciones que se pueden llevar a cabo con esta herramienta de recuperación del sistema.

Pantallas de herramientas de recuperación del sistema



Queda a nuestra discreción ejecutar las tareas necesarias para recuperar el servidor del fallo. Por ejemplo, si nos parece que el fallo se debe a un servicio instalado últimamente, lo podemos detener desde esta consola.

4. Planes de riesgo

Una de las medidas principales para asegurar la continuidad de los servicios es determinar los riesgos a los que nos enfrentamos ante un fallo en el sistema. Esto implica conocer el alcance de los servicios críticos que hay involucrados, la incidencia interna y externa que tienen y haber medido las consecuencias de un fallo que se podía producir. Por lo tanto, hay que preparar un conjunto de acciones que se deben tomar en caso de fallo, teniendo en cuenta que este puede ser por un problema con el hardware o con el software, ya sean virus, troyanos o ataques maliciosos, por ejemplo. En eso consiste, precisamente, un plan de riesgo.

En el proceso de formulación del plan de riesgo, el objetivo principal es cumplir todas las tareas necesarias de la fase proactiva, que es la fase anterior al riesgo. Una vez se produce el acontecimiento, empieza la fase reactiva y se tiene que ejecutar el plan correspondiente.

Para preparar un plan de riesgo, el primer paso es identificar los riesgos a los que estamos sometidos. Por eso tenemos que determinar qué riesgos nos pueden provocar un fallo en el sistema y determinar cuáles son probables, cuáles son posibles y cuáles son críticos. Después, hemos de determinar las prioridades de estos riesgos basándonos en el entorno de la empresa. Es decir, a pesar de que los riesgos informáticos son parecidos para la mayoría de las empresas, la prioridad que se asigna a estos riesgos depende del uso informático que lleva a cabo la empresa.

Una vez los tenemos identificados y priorizados, debemos decidir cuáles de estos riesgos van a generar un plan de riesgo y cuáles no hay que tener implementados en un plan como este, además de las características que debe tener dicho plan.

Para generar un plan de riesgo, para cada una de las funciones que componen el plan, tenemos que analizar todas las alternativas de solución que permitan que los servicios continúen funcionando aunque haya algún inconveniente. Tras analizar todas las alternativas, confeccionamos el plan. Las soluciones del plan pueden ser técnicas, de atención, de suministro o soluciones momentáneas para problemas puntuales (por ejemplo, en caso de un fallo en el suministro eléctrico, el uso de un generador) o una combinación de todos estos tipos de solución.

Al generar el plan de riesgo se debe tener en cuenta la identificación de las condiciones que implican que se ponga en marcha este plan. En términos generales, el plan de riesgo debe contener los puntos siguientes:

- **Objetivo del plan.** Se tienen que indicar los componentes de los servicios críticos que se pretende cubrir en relación con el riesgo que se tiene en consideración. Estos componentes pueden variar, así como el grado de cobertura que tienen, para los diferentes riesgos analizados.

- **Criterio para ejecutar el plan.** Son las condiciones con las que se considera que se debe empezar a aplicar el plan de riesgo.

- **Tiempo esperado máximo de duración del plan.** Es decir, el tiempo máximo durante el que se puede continuar operando con estas condiciones de riesgo.

- **Roles, responsabilidad y autoridad.** Esto es clave para la buena marcha del plan de riesgo. Se tiene que determinar muy claramente cuál es el papel de cada uno de los sectores de la organización ante el riesgo y cómo se alteran los procedimientos habituales para dar lugar a los procedimientos de riesgo. Aquí hay que implicar con mucha claridad a las personas y los departamentos, marcando qué es lo que tiene que hacer cada persona y en qué momento.

- **Requisito de recursos.** Qué recursos se necesitan para operar en el modo riesgo y cuáles de los recursos utilizados habitualmente no se tienen que utilizar. Esto debe estar documentado y verificado debidamente, del modo más exhaustivo posible, incluso con una relación de precios de todo aquello que se deba adquirir y las prioridades.

Para entender mejor cómo es un plan de riesgo pondremos un ejemplo. Imaginemos que nuestra empresa es una universidad a distancia en la que todos los alumnos reciben las clases mediante el uso del servidor web. El servidor tiene una tarjeta controladora de discos SCSI y los discos son externos (están fuera del servidor) y se conectan al servidor mediante un cable SCSI a la controladora de discos; además, tenemos otra máquina igual (el mismo hardware) para sustituir al servidor en caso de fallo en el hardware. Ahora imaginemos que se ha dañado la fuente de alimentación del servidor principal.

El plan de riesgo debe ser uno parecido al siguiente:

1) Objetivo del plan: el servicio web debe estar parado el mínimo tiempo posible.

2) Criterio de ejecución del plan: cuando se detecta que ha caído el servidor web.

3) Tiempo esperado de ejecución: cinco minutos.

4) Roles: personal de servicios informáticos que está de guardia en aquel momento. Por lo tanto, se deberá tener en cuenta que debe haber personas de la organización pendientes de alguna alarma. Dependerá de cada tipo de organización y de qué tiempo de espera se puede tener. Si ponemos que tienen que ser solo cinco minutos, se tendrá que tener a una persona las veinticuatro horas los siete días de la semana en la empresa por si salta una alarma como esta. En el caso de poder alargar el tiempo de respuesta, bastará con un teléfono de contacto y no habrá que tener a alguien las veinticuatro horas del día en la empresa.

5) Requisitos de recursos: un servidor de repuesto con el mismo hardware. El personal de servicios que está de guardia en el momento en el que detecta que el servidor de páginas web no funciona tiene que hacer lo siguiente:

- Detener el servidor web (si la máquina está puesta en marcha).
- Desconectar el cable SCSI de la tarjeta controladora de discos del servidor web.
- Conectar el cable SCSI a la tarjeta controladora de discos del servidor de repuesto.
- Poner en marcha el servidor de repuesto.