
ResumenIA: LPIC-2 Objetivo 206.2 - Realización de Copias de Seguridad

Peso del Objetivo: 3

Descripción General

El objetivo 206.2 del examen LPIC-2 se centra en la importancia crítica y la práctica de las copias de seguridad (backups) en un entorno Linux. Un administrador de sistemas debe ser capaz de planificar, ejecutar y verificar estrategias de backup, entendiendo los diferentes medios, herramientas y tipos de copias de seguridad, así como los procesos de restauración.

Áreas de Conocimiento Clave Desarrolladas

1. Saber Qué Archivos Hay Que Incluir en las Copias de Seguridad

Decidir qué incluir en una copia de seguridad es tan importante como el proceso en sí. Esto depende de si se busca una restauración completa del sistema o solo de datos específicos.

- Archivos de configuración del sistema:
- `/etc/`: Contiene la mayoría de los archivos de configuración críticos del sistema (red, servicios, usuarios, etc.). Es fundamental para restaurar la funcionalidad del servidor.
- `/boot/`: Contiene el kernel de Linux y los archivos de configuración del gestor de arranque (GRUB). Necesario para que el sistema pueda arrancar.
- Directorios de usuarios:
- `/home/`: Contiene los directorios personales de los usuarios, sus documentos, configuraciones (`.rc`, `.ssh/`, etc.) y datos críticos.
- Datos de aplicaciones y servicios:
- Bases de datos (MySQL, PostgreSQL, etc.): Sus directorios de datos deben ser respaldados, idealmente con volcados lógicos generados por las propias herramientas de la base de datos para asegurar la consistencia.
- Servidores web (Apache, Nginx): Contenido web (`/var/www/`, etc.) y configuraciones.
- Servidores de correo: Buzones y configuraciones.
- Otros servicios: Cualquier directorio que contenga datos generados o modificados por el servicio.
- Registros del sistema:

- `/var/log/`: Contiene los archivos de registro. Aunque no son críticos para la funcionalidad, son vitales para auditorías, resolución de problemas y forensia.
- Archivos de aplicaciones de terceros:
- Si hay software instalado fuera del gestor de paquetes (ej., compilado desde fuente en `/opt/` o `/usr/local/`), esos directorios también deben incluirse.
- Qué NO incluir (o considerar excluir):
- `/proc/`, `/sys/`, `/dev/`: Son sistemas de archivos virtuales o de dispositivos, generados dinámicamente al arrancar. No deben ser respaldados.
- `/tmp/`, `/var/tmp/`: Directorios temporales.
- Archivos de caché o temporales de programas: A menudo se pueden regenerar y solo ocupan espacio.
- Directorios montados con otras fuentes (NFS, Samba): Si son montajes, sus datos residen en otro lugar y deben respaldarse desde la fuente original.

2. Conocer Soluciones de Respaldo en Red

Las soluciones empresariales de backup ofrecen funcionalidades avanzadas como la deduplicación, compresión, cifrado, planificación, monitorización y restauración granular.

- Amanda (Advanced Maryland Automatic Network Disk Archiver): Solución cliente-servidor de código abierto, muy robusta y escalable. Utiliza un modelo de backup de cinta/disco. Es conocida por su eficiencia en el manejo de grandes volúmenes de datos y su integración con sistemas de archivos nativos.
- Bacula: Plataforma de backup, recuperación y verificación de datos de código abierto. Es modular y escalable, diseñada para automatizar tareas de backup a través de una red heterogénea. Soporta una amplia gama de dispositivos de almacenamiento. Tiene una comunidad activa y una versión empresarial.
- Bareos (Backup Archiving REcovery Open Sourced): Un fork de Bacula, manteniendo su arquitectura, pero con un desarrollo más activo y algunas mejoras en funcionalidades y soporte de nuevas tecnologías. También es una solución cliente-servidor.
- BackupPC: Solución de backup de red de alto rendimiento para Linux, Windows y macOS. Utiliza rsync y smbclient para transferir datos. Es conocida por su deduplicación inteligente a nivel de archivo y su interfaz web. Almacena backups en disco, ofreciendo una restauración rápida.

3. Conocer los Beneficios y los Inconvenientes de las Cintas, los CD-R, los Discos y Demás Medios de Respaldo

La elección del medio de almacenamiento es crucial para una estrategia de backup efectiva.

- Cintas (Magnetic Tapes - LTO):
- Beneficios: Muy bajo costo por GB para grandes volúmenes de datos, excelente para almacenamiento a largo plazo (archivo), muy alta densidad de datos, larga vida útil, bajo consumo de energía en reposo.

- Inconvenientes: Acceso secuencial (lento para restaurar archivos individuales), requiere hardware específico (unidad de cinta), susceptibilidad al daño físico, software de backup complejo.
- Discos Duros (HDD/SSD):
- Beneficios: Acceso aleatorio rápido (restauración rápida), fácil de usar (directorio estándar), buena relación costo/GB (HDDs), alta velocidad (SSDs).
- Inconvenientes: Mayor costo por GB que las cintas para grandes volúmenes, menor vida útil que las cintas para archivo, mayor consumo de energía en reposo.
- Medios Ópticos (CD-R/RW, DVD-R/RW, Blu-ray):
- Beneficios: Portátiles, económicos (CD/DVD), buena durabilidad si se almacenan correctamente, adecuados para pequeñas cantidades de datos o backups de arranque.
- Inconvenientes: Baja capacidad, escritura lenta, susceptible a arañazos, la fiabilidad a largo plazo puede ser un problema si la calidad del disco es baja.
- Almacenamiento en Red (NAS/SAN/Cloud):
- Beneficios: Alta disponibilidad, acceso remoto (Cloud), escalabilidad, redundancia incorporada, automatización fácil.
- Inconvenientes: Dependencia de la red, costo de ancho de banda (Cloud), problemas de seguridad/privacidad (Cloud), latencia.

4. Realizar Copias de Seguridad Parciales y Manuales

Para tareas específicas o para sistemas pequeños, las herramientas de línea de comandos son muy efectivas.

- `tar`: La herramienta de archivado más versátil en Linux.
- Backup completo de un directorio:

```
tar -czvf /ruta/a/backup/home_backup_$(date +%Y%m%d).tar.gz /home/usuario
```

- `-c`: Crear archivo.
- `-z`: Comprimir con `gzip`.
- `-v`: Verbose (mostrar archivos).
- `-f`: Especificar archivo de salida.
- `$(date +%Y%m%d)`: Añade la fecha al nombre del archivo para facilitar la gestión.
- Excluir directorios/archivos:

```
tar -czvf backup.tar.gz --exclude=/home/usuario/temp --exclude=*.mp4
/home/usuario
```

- Backup incremental/diferencial (con `--listed-incremental`): `tar` puede guardar el estado

de un backup en un archivo de instantánea, permitiendo backups posteriores que solo incluyan los archivos modificados desde la última instantánea. Es más complejo de gestionar manualmente.

- `dd`: Copia bloques de datos de un dispositivo a otro, útil para backups a nivel de bloque (imágenes de disco/partición).
- Backup de una partición a un archivo:

```
sudo dd if=/dev/sda1 of=/ruta/a/backup/sda1_image.img bs=4M status=progress
```

- `if`: Input File (dispositivo de entrada).
- `of`: Output File (archivo de salida/dispositivo).
- `bs`: Tamaño de bloque (mejora el rendimiento).
- `status=progress`: Muestra el progreso (útil para archivos grandes).
- Advertencia: `dd` no conoce el sistema de archivos. Copia todo, incluyendo espacio vacío, y puede ser peligroso si los parámetros son incorrectos (podrías sobrescribir un disco importante).
- `rsync`: Sincronización de archivos altamente eficiente, ideal para backups incrementales o diferenciales a otro servidor o disco local. Solo copia los cambios.
- Backup de un directorio local a otro local:

```
rsync -avz --delete /home/usuario/ /mnt/backup/home_sync/
```

- `-a`: Modo archivo (mantiene permisos, enlaces simbólicos, tiempos, etc.).
- `-v`: Verbose.
- `-z`: Comprimir datos durante la transferencia (para red).
- `--delete`: Elimina archivos en el destino que ya no existen en el origen.
- Backup a un servidor remoto (vía SSH):

```
rsync -avz /home/usuario/ user@remoteserver:/path/to/backup/
```

- Requiere que `rsync` esté instalado en ambos lados y acceso SSH.
- `/bin/sh` (Scripts de Shell): La base para automatizar cualquier proceso de backup manual. Permite combinar `tar`, `dd`, `rsync` con lógicas de fechas, logging, y notificaciones.

5. Verificar la Integridad de los Archivos de Respaldo

Un backup no es útil si está corrupto. La verificación es una parte crucial del proceso.

- Sumas de verificación (checksums):
- `md5sum`, `sha256sum`, `sha512sum`: Calculan un hash único del archivo. Se puede guardar el

hash después de crear el backup y recalcularlo después para comparar.

```
sha256sum backup.tar.gz > backup.tar.gz.sha256
# Para verificar:
sha256sum -c backup.tar.gz.sha256
```

- Listar el contenido de un tarball:

```
tar -tf backup.tar.gz # -t para listar, -f para archivo.
```

- Si `tar` puede listar el contenido sin errores, es una buena señal de que el archivo no está corrupto a nivel básico.
- Restauración de prueba: La forma más fiable de verificar la integridad es realizar restauraciones de prueba periódicas a un sistema de prueba.

6. Restaurar Copias de Seguridad de Forma Total o Parcial

El objetivo final de un backup es la restauración.

- Restauración con `tar`:
- Restaurar todo el contenido de un tarball:

```
tar -xzvf /ruta/a/backup/home_backup_20250628.tar.gz -C /destino/restauracion
```

- `-x`: Extraer.
- `-C /destino/restauracion`: Cambiar al directorio antes de extraer (asegura que los archivos se extraigan en la ubicación deseada).
- Restaurar archivos específicos de un tarball:

```
tar -xzvf backup.tar.gz path/to/specific_file.txt
```

- Restauración con `dd`:
- Restaurar una imagen de partición a una partición vacía:

```
sudo dd if=/ruta/a/backup/sda1_image.img of=/dev/sda1 bs=4M status=progress
```

- ¡Extremadamente peligroso! Asegúrate de que `of` sea la partición correcta y que esté vacía, ya que sobrescribirá todo.
- Restauración con `rsync`:
- Restaurar de un destino de `rsync` a un origen original (o nuevo):

```
rsync -avz /mnt/backup/home_sync/ /home/usuario/
```

- El origen y el destino de `rsync` simplemente se invierten para la restauración.

7. Dispositivos de Cinta y su Gestión

- `/dev/st*` y `/dev/nst*`: Dispositivos de cinta en Linux.
- `/dev/st0`: Dispositivo de cinta rebobinable. Después de cada operación, la cinta se rebobina automáticamente.
- `/dev/nst0`: Dispositivo de cinta no rebobinable. La cinta permanece en su posición después de una operación, lo que es eficiente para múltiples operaciones secuenciales (ej., escribir varios archivos `tar` seguidos).
- `mt` (Magnetic Tape control): Utilidad para controlar unidades de cinta.
- `mt -f /dev/nst0 status`: Muestra el estado de la unidad de cinta.
- `mt -f /dev/nst0 rewind`: Rebobina la cinta.
- `mt -f /dev/nst0 offline`: Descarga la cinta.
- `mt -f /dev/nst0 fsf 1`: Avanza un archivo (útil si hay múltiples backups en una sola cinta).
