Instalación de Herramientas Necesarias

Antes de sumergirnos en el mundo del cifrado con LUKS, es esencial asegurarse de tener las herramientas adecuadas instaladas en tu sistema. Por lo general, la mayoría de las distribuciones de Linux incluyen estas herramientas de cifrado de manera predeterminada, pero siempre es bueno verificarlo.

Puedes instalar las herramientas necesarias utilizando el gestor de paquetes de tu distribución. En distribuciones basadas en Debian, como Ubuntu, puedes ejecutar el siguiente comando en la terminal:

```
sudo apt install cryptsetup
```

Si estás utilizando una distribución basada en Red Hat, como Fedora o CentOS, puedes instalar las herramientas de cifrado con el siguiente comando:

```
sudo dnf install cryptsetup
```

Una vez que hayas instalado cryptsetup, estarás listo para comenzar a trabajar con LUKS.

Creación de un Volumen LUKS

El primer paso para cifrar una partición o disco en Linux es crear un volumen LUKS. Este volumen actuará como una capa de cifrado que protegerá los datos almacenados en la partición o disco.

Para crear un volumen LUKS, necesitarás especificar la partición o disco que deseas cifrar. Asegúrate de que la partición esté desmontada antes de proceder. Supongamos que queremos cifrar la partición /dev/sdb1. El siguiente comando creará un volumen LUKS en esta partición:

```
sudo cryptsetup luksFormat /dev/sdb1
```

Este comando iniciará el proceso de creación del volumen LUKS en la partición especificada. Serás solicitado a confirmar esta acción, ya que el proceso borrará todos los datos existentes en la partición. Después de confirmar, se te pedirá que ingreses una contraseña para desbloquear el volumen LUKS en el futuro. Asegúrate de elegir una contraseña segura y recuérdala bien, ya que la necesitarás cada vez que quieras acceder a los datos cifrados.

Una vez completado el proceso, tendrás un volumen LUKS creado en la partición especificada, listo para ser utilizado.

Apertura y Cierre del Volumen LUKS

Después de crear un volumen LUKS, el siguiente paso es abrirlo para poder acceder a los datos almacenados en él. Para abrir un volumen LUKS, necesitarás especificar la partición que contiene el volumen y asignarle un nombre.

```
sudo cryptsetup luksOpen /dev/sdb1 mi_particion_cifrada
```

En este comando, /dev/sdb1 es la partición que contiene el volumen LUKS, y mi_particion_cifrada es el nombre que le estamos asignando al volumen abierto. Una vez que ejecutas este comando, se

te pedirá que ingreses la contraseña que especificaste durante la creación del volumen LUKS. Después de ingresar la contraseña correcta, el volumen se abrirá y estará listo para ser utilizado.

Para cerrar el volumen LUKS y bloquear el acceso a los datos cifrados, puedes utilizar el siguiente comando:

```
sudo cryptsetup luksClose mi_particion_cifrada
```

Este comando cerrará el volumen LUKS con el nombre especificado (mi_particion_cifrada en este caso), lo que impedirá el acceso a los datos almacenados en él hasta que vuelva a abrirse.

Creación de un Sistema de Archivos en un Volumen LUKS

Una vez que hayas abierto un volumen LUKS, puedes crear un sistema de archivos en él para comenzar a almacenar datos de forma segura. Puedes utilizar cualquier sistema de archivos compatible con Linux, como xfs, xfs o btrfs.

Supongamos que queremos crear un sistema de archivos xfs en el volumen LUKS abierto (mi_particion_cifrada). El siguiente comando creará un sistema de archivos xfs en el volumen:

```
sudo mkfs.xfs /dev/mapper/mi_particion_cifrada
```

Este comando formateará el volumen LUKS abierto con un sistema de archivos xfs, lo que te permitirá empezar a almacenar datos en él de manera segura.

Montaje y Desmontaje de un Volumen LUKS

Una vez que hayas creado un sistema de archivos en un volumen LUKS, puedes montarlo en el sistema de archivos para acceder a los datos almacenados en él. Para montar un volumen LUKS, puedes utilizar el siguiente comando:

```
sudo mount /dev/mapper/mi_particion_cifrada /mnt
```

En este comando, /dev/mapper/mi_particion_cifrada es la ruta al dispositivo de bloque que representa el volumen LUKS abierto, y /mnt es el punto de montaje donde se montará el sistema de archivos.

Después de montar el volumen LUKS, puedes acceder a los datos almacenados en él como lo harías con cualquier otro sistema de archivos montado en Linux. Cuando hayas terminado de trabajar con los datos, puedes desmontar el volumen LUKS utilizando el siguiente comando:

```
sudo umount /mnt
```

Este comando desmontará el sistema de archivos del volumen LUKS, lo que evitará que accedas a los datos almacenados en él hasta que vuelva a montarse.

Administración de Volumenes LUKS

LUKS proporciona varias herramientas para administrar volumenes, incluida la capacidad de cambiar la contraseña, agregar claves adicionales y realizar copias de seguridad de las cabeceras de los volumenes.

Para cambiar la contraseña de un volumen LUKS, puedes utilizar el siguiente comando:

```
sudo cryptsetup luksChangeKey /dev/sdb1
```

Este comando te pedirá la contraseña actual del volumen LUKS y luego te permitirá ingresar una nueva contraseña.

Si deseas agregar una clave adicional al volumen LUKS, puedes utilizar el siguiente comando:

```
sudo cryptsetup luksAddKey /dev/sdb1
```

Este comando te pedirá la contraseña actual del volumen LUKS y luego te permitirá ingresar una nueva clave adicional.

Para realizar una copia de seguridad de la cabecera de un volumen LUKS, puedes utilizar el siguiente comando:

```
sudo cryptsetup luksHeaderBackup /dev/sdb1 --header-backup-file backup_file
```

Este comando realizará una copia de seguridad de la cabecera del volumen LUKS en el archivo especificado, lo que te permitirá restaurarla en caso de que se dañe la cabecera del volumen.

Resumen de comandos para crear volumen cifrado con luks

```
sudo cryptsetup luksFormat /dev/DISCO
sudo cryptsetup luksOpen /dev/DISCO DISCO_DESCIFRADO
sudo mkfs.xfs /dev/mapper/DISCO_DESCIFRADO
sudo mount /dev/mapper/DISCO_DESCIFRADO /ruta_de_montaje
```

Integración con crypttab y fstab

Una vez que has cifrado una partición o disco utilizando LUKS en Linux, es posible que desees configurar la apertura automática del contenedor LUKS durante el arranque del sistema y montarlo en un punto específico del sistema de archivos. Esto se puede lograr utilizando los archivos de configuración crypttab y fstab.

Configuración de crypttab

El archivo crypttab se utiliza para configurar el mapeo automático de dispositivos cifrados durante el proceso de arranque del sistema. Puedes especificar los dispositivos cifrados y sus correspondientes claves de cifrado en este archivo.

Para configurar un dispositivo cifrado en crypttab, primero necesitas conocer el UUID (Identificador Único Universal) del contenedor LUKS. Puedes encontrar el UUID ejecutando el siguiente comando:

```
sudo cryptsetup luksUUID /dev/sdb1
```

Una vez que tengas el UUID del contenedor LUKS, puedes agregar una entrada en el archivo crypttab para configurar el mapeo automático. Por ejemplo, supongamos que el UUID del contenedor LUKS es 12345678-1234-1234-1234-123456789abc. Puedes agregar la siguiente entrada en el archivo crypttab:

```
mi_particion_cifrada UUID=12345678-1234-1234-1234-123456789abc none luks
```

También puede hacerse así en este caso sin usar el UUID:

```
mi_particion_cifrada /dev/sdb1 none luks
```

En esta entrada, mi_particion_cifrada es el nombre que le hemos dado al contenedor LUKS, y UUID=12345678-1234-1234-1234-123456789abc es el UUID del contenedor. La palabra none indica que no se utiliza una clave precompartida y luks especifica que el dispositivo está cifrado con LUKS.

Configuración de fstab

Una vez que has configurado el mapeo automático del dispositivo cifrado en crypttab, puedes configurar el montaje automático del sistema de archivos en fstab. El archivo fstab se utiliza para configurar el montaje automático de sistemas de archivos durante el arranque del sistema.

Para configurar el montaje automático de un sistema de archivos en fstab, primero necesitas conocer el punto de montaje y el tipo de sistema de archivos del contenedor LUKS. Supongamos que el punto de montaje es /mnt/mi_particion y el sistema de archivos es xfs. Puedes agregar una entrada en el archivo fstab de la siguiente manera:

```
/dev/mapper/mi_particion_cifrada /mnt/mi_particion xfs defaults 0 2
```

En esta entrada, /dev/mapper/mi_particion_cifrada es la ruta al dispositivo de bloque que representa el contenedor LUKS abierto, /mnt/mi_particion es el punto de montaje donde se montará el sistema de archivos, xfs es el tipo de sistema de archivos, defaults especifica las opciones de montaje por defecto, y 0 2 especifica las opciones de comprobación del sistema de archivos.

Recomendaciones con crypptab

En el caso de un servidor yo no tendría activo el crypttab, es decir, dejaria la configuración puesta pero comentada, al igual que con el fstab, Haría los montajes de forma manual tras un reinicio. Así evitamos tener que usar ficheros de clave y tener algunos problemas derivados