Lux Encryption

Transcribed on July 8, 2025 at 10:47 AM by Minutes AI

Speaker 1 (00:18)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a poner en práctica el cifrado Lux, que es una especificación de cifrado de disco completa diseñada especialmente para sistemas Linux.

Lux, o lo que es lo mismo, Linux Unified Key Setup, nos proporciona una capa de seguridad adicional al cifrar particiones enteras de nuestros dispositivos de almacenamiento.

¿Pero, qué hace que Lux sea tan especial?

En primer lugar, Lux ofrece una seguridad robusta mediante el uso de algoritmos de cifrado fuertes como es AES y Chuffis.

Esto asegura que nuestros datos estén protegidos incluso en caso de acceso no autorizado al dispositivo.

Además, Look nos brinda flexibilidad con la capacidad de crear múltiples contenedores cifrados, podemos gestionar diferentes niveles de acceso y proteger distintos conjuntos de datos con contraseñas individuales.

¿Y ahora, cómo funciona Lux en la práctica?

Pues la verdad que es bastante simple.

Básicamente vamos a utilizar el comando crypt setup para inicializar el dispositivo con Lux y poder establecer una contraseña.

Una vez configurado el dispositivo cifrado se comporta como cualquier otro dispositivo de almacenamiento, pero con una capa adicional de protección.

En algunos sistemas operativos, como es el caso de Ubuntu y otras distribuciones similares, por ejemplo Ubuntu Server, a la hora de realizar una nueva instalación del sistema, se puede apreciar en la pantalla donde tenemos que seleccionar la partición para instalar el propio sistema, que podemos seleccionar directamente para cifrar el grupo LVM con Lux.

Esto aplicaría el cifrado de disco directamente durante la instalación.

A continuación, vamos a pasar a ver esta especificación de cifrado en un sistema Linux y cómo utilizar script setup para poder aplicar Lux a una partición.

Me encuentro en un sistema operativo con Ubuntu y aquí lo que vamos a hacer va a ser explorar cómo trabajar o cómo cifrar unidades con Lux.

En primer lugar, debemos montar un nuevo disco que es con el que vamos a trabajar y de hecho esto, si abrimos por aquí una terminal, podremos hacer por ejemplo un Ls sobre dep, que es donde se nos está montando todas las unidades.

De hecho, si hacemos un Ls sobre dep nos saldrán varios, pero tenemos que localizar nuestro disco duro, que de momento se acaba de poner, por así decirlo, nueva al hardware y vamos a tener que montarlo, que darle un formato y sobre todo instalar loops para poder cifrar esa partición.

Así que vemos en primer lugar, por aquí tenemos que tener sda y sdb.

Sda será nuestro normal que le tenemos.

Vamos aquí, aquí tenemos sda, vemos que sda tiene tres particiones y por aquí tenemos sdb que no tiene ninguna.

¿Cómo podemos ver si el disco está montado?

No está montado y qué discos tenemos, pues por ejemplo podemos hacer uso de la utilidad de f para poder ver el espacio que tenemos disponible en el disco, pero es que aquí nos salen las unidades que tenemos montada y vemos como s b no nos aparece montada, así que vamos a hacer uso de otra herramienta que es fdisk, que de hecho vamos a ejecutar en primer lugar la ayuda para que podamos ver qué nos permite hacer esto, que podamos ver qué nos permite hacer esto.

Básicamente se trata de una utilidad para dar formato al disco y nosotros queremos ver en primer lugar, queremos listar cuáles son los discos que tenemos disponibles, cuáles son los discos que tenemos disponibles y aquí vemos como Sdb se trata de un disco duro de 52 megas pero no vemos como digo el resto de particiones que tiene, por ejemplo aquí en SDA vemos que es un disco de 32 gb y que sí que tiene sda, sda y sda.

Entonces en primer lugar lo que vamos a hacer va a ser dar formato una partición a esta unidad, darle un formato y luego ya procedemos a aplicar el cifrado deluxe sobre dicha partición.

Cogemos de nuevo fdisk y decimos que queremos trabajar sobre dev sdb.

Aquí entramos en una herramienta interactiva, es decir, nosotros por ejemplo si le damos a la m pues nos aparece el menú, podemos por ejemplo mostrar información sobre la tabla de particiones, si le damos por ejemplo a la p vemos como digo aquí no tenemos ninguna, luego si lo volvemos a hacer pues veremos que nos aparecen sdb, stb, dependiendo del número de particiones que hagamos también podemos imprimir información sobre una partición, claro ahora no tenemos ninguna partición, entonces me dice que no está definida.

Hay que recordar que lo primero para poder utilizar esta herramienta la hemos ejecutado con permiso utilizando el comando sudo y cuando hagamos cualquier tipo de cambio tendremos que guardarlos antes de salir, esto es importante recordarlo.

Bueno pues lo que vamos a hacer va a ser crear una nueva partición, así que vamos a crear una nueva partición, aquí nos dice que de qué tipo queremos que sea, si es primaria o es extendida, bueno la podríamos hacer extendida o primaria, por defecto es primaria, así que volvamos a hacer la primaria, aunque no vamos a instalar aquí ningún tipo de sistema operativo sino que lo vamos a utilizar para la parte de los datos, pero bueno, vamos a crear una partición primaria, decimos que queremos que sea la partición número un, que el primer sector sea lo más bajito que se pueda, en este caso el 2048 y que nos llegue hasta el último sector, es decir, únicamente quiero hacer una partición en todo el disco, como veis ahora ya sí que me aparece aquí, me dice que tiene un tamaño de 51 megas y ahora bueno, pues sí que podemos, por ejemplo, solicitar información de esta partición, en qué sector empieza, qué sector termina, etc.

La cantidad de sectores que tiene.

Os recuerdo, tenemos que guardar antes de poder utilizar esta partición, así que le damos a la w, esto nos lo guarda y si ahora por ejemplo ya hacemos un lsd, vamos a filtrar por sd, aquí ya vemos que nos aparece sdb y sdb.

Esto también, bueno, ahora mismo si utilizamos de f vamos a ver que todavía no nos aparece, es decir, la unidad no la tenemos montada, eso lo tendremos que hacer ahora, pero sin embargo, si hacemos el fdisk l, aquí ya sí que podemos apreciar que nos aparece correctamente la partición, es decir, hemos hecho la primera parte de manera correcta.

Antes de poder montar esta unidad le deberíamos dar algún tipo de formato, así que lo que voy a hacer va a ser aplicarle el formato más típico aquí en Linux o de los más típicos, con el comando mkfs ext para aplicar este formato ext sobre la partición sdb.

Fijaos que según le he dado formato, la interfaz gráfica del sistema ya me lo ha reconocido y ya me ha puesto aquí directamente el volumen para que yo pueda acceder a él directamente, es decir, me ha hecho el montaje, me lo ha hecho ya aquí directamente.

Ahora ya sí, si aplicamos el DF, pues bueno, todavía no nos aparece aquí, bueno, no le tenemos montado del todo, perdonad.

Vamos entonces a montarlo haciendo el sudo mount y es que utilizando este comando ya sí que vamos a montar esto sobre algún tipo de ruta seguramente, bueno, si le doy aquí nos aparece ya el volumen y podríamos empezar a crear datos, no sé si quizás al clicarle aquí ya nos saca.

Ahora sí, vale, perdonad, ahora sí que al clicarle ahí, como os digo, nos ha hecho el montaje del disco, que nos lo ha hecho en esta ubicación, en media Álvaro y luego con el UID, no os lo había puesto al principio, pero según hemos clicado en la interfaz gráfica ya nos ha hecho el montaje.

Si yo ahora aquí, si es ac, lo quiero desmontar o montar con comandos, vamos a utilizar sudo umoun y el que quiero desmontar es dev sdb, vamos a ver que efectivamente ahora nos la ha desmontado y si lo quisiésemos montar en algún otro, una otra ruta, es común, por ejemplo, ponerlo media o bien en mnt, fijaos que en mnt yo ya tengo una carpeta llamada prueba, que en principio está limpio, no tiene nada y yo lo que quiero hacer es coger y montar la unidad sdb sobre prueba, entonces en este caso haremos sudo mount de sdb sobre mlt prueba.

Aquí vemos, bueno nos ha desaparecido desde aquí, es como que aquí ya no aparece, pero si hacemos un df para ver los discos que tenemos nos aparece de nuevo donde lo tenemos montado.

Esto hasta aquí todavía no hemos aplicado ninguno una parte de cifrado ni nada, eso es lo que vamos a hacer ahora.

Entonces en primer lugar tenemos que asegurarnos de que tenemos la herramienta crypt setup instalada y en el caso de que no la tengamos pues simplemente hacer apt getinstallcrypt setup.

Esto nos hará o nos instalará una serie de herramientas, fijaos que voy a hacer que me saque la ayuda, tenemos bastantes parámetros para poder lanzar y es que de hecho si yo aquí me pongo a tabular vemos que todo esto son las opciones que me van a permitir utilizar el comando decree setup.

Ya os puedo ir adelantando que como esto al final nos va a cifrar la unidad, cuando nosotros queramos ahora montar la unidad previamente la vamos a tener que descifrar.

Entonces aquí es donde entran en juego las opciones como cerrar o abrir la unidad y luego tenemos un montón más para hacer toda la parte o para trabajar con lux como puede ser lux format, que es por donde vamos a empezar para dar ese formato lux.

Luego vamos a ver que podemos añadir varias claves o cambiar una clave que ya tengamos, hacer un dump para poder ver cuáles son todas las claves que se tiene o el espacio de claves que tenemos disponible, podemos eliminar una clave o podemos consultar el identificador único.

Por supuesto que antes de empezar tenemos que otra vez de nuevo volver a desmontar la unidad porque si no no la vamos a poder formatear, así que la desmontamos que en este caso está en dev sdb, de nuevo la GuI nos lo pinta aquí, pero si revisamos con df por ejemplo, vemos que no la tenemos montada.

Ahora lo que vamos a hacer va a ser darle ese formato de loops, así que vamos a hacer sudocript setup, vamos a hacer un loop forma y ahora le decimos sobre qué disco le vamos a aplicar que es dev sdb.

Aquí vamos a tener que definir una nueva contraseña, nos dice oye este disco, bueno ya lo hemos formateado antes con un x t que lo vamos a tener que volver a hacer ahora vamos a formatear la unidad con formato deluxe y luego cuando abramos la unidad le vamos a dar otra vez de nuevo este formato, digamos que este formato de x t que hemos hecho hasta ahora para poder montarlo la primera vez lo vamos a perder.

Le decimos que sí, vamos a sobreescribir los datos.

Aquí tendremos que poner una clave segura.

Recordad que cuando estamos escribiendo no vamos a ver qué es lo que estamos escribiendo, vamos a verificar la contraseña que acabamos de poner y esto ya, bueno, en función del disco, de la capacidad que tenga, podrá tardar más o menos.

Fijaos que esto ahora que ha terminado estamos exactamente igual que antes, es decir, si yo hago un df, ahora mismo no lo tengo montado, pero es que aquí me aparece ya el agui, el disco, y se me está indicando que este disco está cifrado, es decir, antes de poder trabajar con él vamos a tener que descifrarle.

Bueno, de hecho si le doy aquí vais a ver que lo que es la parte de la interfaz directamente me está pintando para introducir la contraseña.

En este caso yo lo que quiero hacer es utilizar de nuevo clip setup y en este caso pues simplemente el comando open sobre dev sdb.

Fijaos que aquí lo que me está pidiendo, y bueno, si revisamos ahora la ayuda de crypt setup, lo que me está pidiendo es que le dé un nombre de mapeo de esta unidad para que lo podamos ver vamos a poner unidad c de cifrada o algo así, le voy a poner así.

Ahora me está pidiendo esta clave que hemos definido antes.

Un, dos, tres, 4 y vemos cómo nos ha hecho el montaje correctamente de la unidad.

Vale, si ahora hago un un df, bueno, no ha hecho el montaje, perdonad, sino se ha descifrado y ahora lo que tenemos que hacer es montarlo, pero ahora se encuentra en la siguiente ruta.

Si hacemos un dep de mapper, fijaos que aquí me aparece unidad 101.º, que esto lo acabo de crear yo en este mismo momento.

Si hiciese por ejemplo un close, aquí vamos a cerrar la unidad, unidad seis, aquí vemos cómo hemos cerrado, hemos conseguido cerrar la unidad y por tanto si hago un Ls sobre devmapper no me aparece.

Que quede esto claro de cómo se utiliza.

Entonces vamos de nuevo, lo voy a volver a abrir, aquí de nuevo lo volvemos a abrir, ponemos la contraseña y ahora vamos a hacer el montaje con sudo mount dev mapper unidad cifrada y lo quiero montar sobre mnt prueba.

Aquí tenemos otro problema que estamos viendo y es que esta unidad como hemos visto no tiene formato, es decir, tenemos que volver a darle el formato ext que hemos hecho antes.

Hacemos sudo mkfs ext sobre def maper unidad cifrada en este caso vemos como ahora esto ya sí me lo ha reconocido bien, vemos como aquí también nos aparece ya el volumen abierto, pero lo quiero montar sobre mi propia ruta, así que le vamos a dar aquí y ahora ya si vemos los discos que tenemos montado le podemos apreciar aquí que sobre mnt prueba encontramos el mapper de unidad 101.º que es el que hemos cerrado.

De hecho si ahora intentamos por ejemplo cerrar el lux, seguramente nos va a dar error de que está en este caso montado.

¿Qué otras cosas podemos hacer?

¿Pues fijaos que si hacemos por ejemplo un sudocript setup y fijaos que aquí podríamos hacer oye, vamos a añadir con Lux, no?

Todas estas opciones son las que podemos hacer con Lux.

Vamos a añadir por ejemplo una nueva clave sobre el dispositivo.

Tengo que introducir una clave que ya tenga previamente y ahora sí puedo coger y añadir una nueva clave distinta.

Así que tecleamos una nueva clave distinta, la verificamos y también lo que os quiero enseñar ahora es que veamos precisamente cómo podemos ver los huecos que hay.

Entonces con Creep Setup también podríamos hacer un dump sobre devora.

Aquí si nos fijamos tenemos el keyslot número cero, que este es el primero que hemos utilizado y también tenemos el keyslot número un.

Podríamos también por terminar con la parte deluxe, si nos fijamos hemos probado el dump, hemos hecho el primer formato que le hemos dado deluxe, hemos añadido una clave, por supuesto que podríamos eliminar una clave, podemos cambiarla que ya conozcamos, por ejemplo vamos a cambiar dev stb, aquí tenemos que poner la que queremos cambiar, aquí podemos definir la nueva.

Si lo he introducido todo bien, vamos a ver que se produce el cambio, aquí lo tendríamos.

Y por supuesto, pues que podríamos ya por último por terminar de probar todo el remove en dev sdb, aquí tenemos que indicar cuál es la contraseña o passphrase que queremos eliminar.

Y ahora de nuevo si hacemos el dump, pues vamos a ver cómo nos aparece cambiando.

¿Veis?

Solamente tenemos un slot.

Si quisiéramos ver cuál es el identificador único de esta unidad, tan sencillo como utilizar lux uid con el valor de la unidad, aquí lo podemos ver.

Esto es interesante de poder hacer luego por ejemplo, que en el arranque se descifre y se monte esta unidad tocando otros ficheros como es el crypt setup o el f setup y por ello es bastante útil saber identificar dónde encontramos este identificador único, que también por supuesto encontramos cuando estamos haciendo el Dam, pero si no queremos hacer el dan concreto directamente lo podemos hacer a través de este comando.

Para finalizar vamos a ver las conclusiones de esta sesión sobre el cifrado Lux.

Durante la presentación hemos explorado como Lux proporciona una capa esencial de seguridad al cifrar particiones completas de dispositivos de almacenamiento en sistemas Linux.

En primer lugar destacamos la robustez y la flexibilidad de Luxembourg, podemos utilizar algoritmos de cifrado sólidos como es el caso de AES o Qfish.

Y es que Lux asegura la protección de nuestros datos, además de la capacidad para poder crear múltiples contenedores cifrados con contraseñas individuales, que nos va a brindar una gran gestión flexible de acceso.

Hemos visto también la implementación práctica de lux gracias al comando cring setup.

Esta demostración nos ha permitido comprender cómo podemos inicializar y gestionar dispositivos cifrados con lux de manera práctica.

Por supuesto que no podemos pasar por alto las consideraciones de seguridad.

Es crucial utilizar contraseñas robustas y realizar copias de seguridad de las claves de acceso para garantizar la seguridad de nuestros datos cifrados.

Además, hay que recordar los beneficios y las aplicaciones deluxe en entornos empresariales y personales.

Esta herramienta nos brinda tranquilidad al proteger nuestros datos sensibles.

En resumen, Lux es una solución poderosa y versátil para la protección de datos en sistemas Linux.

Su implementación adecuada puede marcar la diferencia en la seguridad de la información sensible.

Y con esto llegamos al final de la sesión.

Os esperamos en el próximo vídeo.