Cifrado de Dispositivos

Transcribed on July 8, 2025 at 11:38 AM by Minutes AI

Speaker 1 (00:02)

A continuación vamos a proponer un ejercicio para trabajar con la configuración de dispositivos cifrados utilizando Cryptab y el montaje automático de unidades con Fz.

Este ejercicio nos permitirá comprender cómo configurar y gestionar el cifrado de datos de manera eficiente y segura en nuestros sistemas.

Vamos a conocer cómo debemos abordar este ejercicio.

En primer lugar se trabajará la configuración del dispositivo cifrado utilizando el archivo crypta.

Este archivo se encuentra ubicado en etc crypta y aquí vamos a especificar los detalles del dispositivo como la ruta al dispositivo real, el nombre del dispositivo cifrado y las opciones de cifrado necesarias.

Además, se debe explorar cómo proporcionar la contraseña de cifrado de forma segura, ya sea de manera interactiva al arrancar el sistema o mediante archivos de Cle.

Recordad que este fichero se va a poder montar cuando se tenga instalada las dependencias o las librerías de cripseta, que tiene sentido que se utilice con cripseta.

Por otro lado, 1 vez configurado el dispositivo cifrado, vamos a adentrarnos en la configuración del montaje automático de unidades, en este caso utilizando el archivo fsetup que encontramos en la ruta ETG Fz.

Aquí agregaremos una entrada para el dispositivo cifrado especificando su uid para no evitar que si nos cambian el disco se pueda confundir con el disco.

Especificamos el uid, también indicamos el punto de montaje y por último las opciones de montaje.

Esto nos asegura que el dispositivo cefrado se monte automáticamente al arrancar el sistema, garantizando de esta manera la disponibilidad de los datos cifrados de manera transparente.

Para comprender mejor cómo podemos utilizar estos archivos, vamos a revisar sus manuales para ver qué es lo que esperamos encontrar.

Vamos a empezar hablando del fichero cryptab, que como veis estoy directamente en la web oficial de su manual, aunque también es cierto que en páginas como puede ser por ejemplo man, org, también encontramos los manuales de distintos comandos.

De hecho, incluso también desde el propio sistema operativo, desde la terminal, también podemos acceder a distintos manuales de distintos comandos.

En este caso estamos con cryptab, que vemos que es un fichero de configuración para los dispositivos cifrados.

Aquí, bueno, lo vemos, me voy a dirigir mejor aquí, que yo creo que se ve un poquito más claro.

Y básicamente lo que nos viene a decir es que tendremos que crear nuestro propio fichero cryptab, que esto se va a encargar de hacer el cifrado o en este caso el descifrado de las unidades a la hora de hacer el boot, a la hora de arrancarlo.

Fijaos que básicamente lo que tenemos que hacer es poner una línea con una serie de parámetros, que en este caso son cuatro parámetros de los cuales dos son obligatorios y los otros dos opcionales.

Básicamente tenemos que decir el nombre del volumen, el dispositivo que tenemos cifrado, las claves y también algunas otras opciones que se pueden poner.

En primer lugar, con respecto al nombre, vamos a tener que decir con qué nombre queremos que se mapee el dispositivo o se desbloquee.

Esto nos va a aparecer el nombre que definamos, aquí lo vamos a poder visualizar dentro de Devmapper.

Si habéis trabajado con creep setup, a la hora de utilizar el comando open para poder abrir la unidad, veréis que se le estaba asignando un nombre y que es aquí donde se montan esas unidades cambios, pues en este caso sería ese el nombre que vamos a utilizar.

En el segundo caso lo que se nos pide es el dispositivo, que en este caso el dispositivo se podrá hacer como por ejemplo d sdb, por ejemplo, pero si lo queremos especificar todavía más podemos utilizar el valor o la clave UUID seguido del UID de dicha partición.

En el tercer campo lo que vamos a definir, que este ya es un campo opcional, lo que tenemos que definir es la clave de cifrado si queremos que se descifre en el momento.

Por otro lado, si no estamos indicando esta clave directamente se nos va a pedir para que el propio usuario la tecle por consola a la hora de iniciar el sistema.

Y por último tenemos una serie de campos, vamos a bajar un poco para hablar del manual, y es que aquí si nos vamos al primer título que pone sobre cómo adquirir la clave, podemos ver hasta seis mecanismos diferentes para poder indicarle esta clave, que por la podemos tener por ejemplo en un fichero, en un disco o cosas que recomiendan por ejemplo tenerlo dentro de una unidad extraíble.

Vemos aquí que tenemos seis distintas.

Y luego por otro lado, yo lo que quiero destacar para forzar con lo que se está pidiendo trabajar, en este caso con la especificación lux, pues fijaos que en la parte de las opciones os recomiendo también revisarlas para poder coger un poco más de conocimiento o información con esto, pero una de las cosas que podemos indicar aquí es por ejemplo la opción lux para forzar que se trabaje con esta especificación de cifrado.

Por último, abajo del todo vamos a encontrar unos ejemplos.

Todo esto siguen siendo opciones que se pueden indicar y aquí abajo del todo, un poquito más abajo, encontramos una serie de ejemplos.

Este es el ejemplo más básico, vemos como aquí se le está dando un nombre a una unidad, este sería el caso base o el más básico, le damos un nombre, este nombre le podremos encontrar sobre Dmapperlux, en este caso con esta unidad concreta que la tenemos aquí identificada y aquí tenemos otros ejemplos, por ejemplo, le vamos a llamar swap y en este caso con Dpsda y esto será de donde esté cogiendo esa clave de cifrado.

Aquí hay distintas opciones que tendremos que ir y revisar qué es lo que está haciendo cada una de esas opciones.

Aquí también tenemos otras distintas, con TCR, por ejemplo.

Y bueno, aquí tenemos algunas opciones más.

Todo esto que vemos aquí, si bajamos un poquito más, pues también podemos encontrar ejemplos más concretos como la Yubikey y por aquí abajo tenemos confido, los distintos volúmenes.

Por supuesto que esto, como indicaba anteriormente, lo podemos encontrar aquí en la parte del manual.

Por último, también tenemos que trabajar con Fstab.

En este caso Fstab es el fichero que se va a encargar de montar una unidad que previamente, en el caso de esta cifrada, pues la tendremos que montar una vez que esté descifrada.

De nuevo.

Aquí tenemos una serie de valores para cumplir, en este caso son seis columnas y básicamente lo que se nos pide es, en el caso de la primera columna, vais a ver ahí qué es el propio dispositivo que queremos montar, pues por ejemplo dev sdb podría ser el nuestro.

En el caso que nosotros ya lo tenemos en el devmapper, pues sería por ejemplo devmapper lux, por ejemplo, con el que hemos trabajado.

El segundo caso que estamos poniendo, fijaos que aquí también tenemos una cosa importante y es que se recomienda para evitar si se ha cambiado algún tipo de disco duro y demás, se recomienda trabajar con el valor UUID.

En el segundo caso lo que le estamos indicando es el punto de montaje, por ejemplo, quiero que lo monte sobre mltrueba o cualquier cosa.

En el tercer campo lo que estamos definiendo es el sistema de archivos que tenemos, los más comunes, x, t, ltfs, vfab, lo que sea.

En este caso, si estamos trabajando, si lo tenemos montado con ext, pues se lo indicamos.

En el cuarto campo lo que encontramos son distintas opciones de montaje y aquí tenemos que ver cuál es o si necesitamos alguno.

Lo más común es por ejemplo, utilizar el default, pero en otras ocasiones aquí, pues por ejemplo se puede indicar si se quiere pues solo lectura, solo lectura y escritura, distintos grupos o usuarios, etc.

En el quinto campo lo que se va a poner aquí, si bajamos un poco, esto básicamente nos sirve para poner el orden de comprobación.

Básicamente nos indica en qué orden se debe comprobar esta comprobación, que de hecho por defecto es al cero, que quiere decir que no se va a realizar la comprobación.

Por último tenemos el orden de la copia de seguridad y es que en qué orden se debería realizar esta copia de seguridad.

Por ejemplo, un valor de cero, pues quiere indicar que no se va a utilizar y también en otras ocasiones podemos utilizar por ejemplo un valor dos que también puede ser útil.

Como veis esto es bastante sencillo al final entendiendo un poco la parte más básica.

De hecho si abriéramos aquí una terminal podríamos hacer directamente un cad de etc.

Y aquí sí que podemos ver qué es lo que se está montando.

Vamos a hacerlo así un poquito más grande y veis que le estamos indicando, veis aquí es un uid, esto me lo está montando en la raíz, el tipo, aquí las distintas opciones, en este caso errores y luego tenemos cero 1 para el orden de comprobación y para el orden de copia de seguridad.

Aquí tenemos por ejemplo otro que se monta sobre el boot Efi y veis también el sistema de archivos, las opciones y luego cero.

Durante el ejercicio tenemos que ir asegurándonos de que estamos escribiendo bien los datos en cada apartado.

Después de completar la configuración podríamos realizar las pruebas para garantizar que todo está funcionando correctamente, como sería un reinicio del sistema y ver que efectivamente se está haciendo el descifrado de la unidad y se nos está montando para tenerla disponible desde que arrancamos el equipo.

Así que nada, hasta aquí con esta sesión sobre el mandamiento del ejercicio y os esperamos en el siguiente vídeo.