APUNTES PRÁCTICAS ISE

# Lección 1.

Ubuntu 16.04 introduce system-dev respecto a Ubuntu 14.04.

The **systems development life cycle** (**SDLC**), also referred to as the **application development life-cycle**, is a term used in [systems engineering](https://en.wikipedia.org/wiki/Systems_engineering" \o "Systems engineering), [information systems](https://en.wikipedia.org/wiki/Information_system" \o "Information system) and [software engineering](https://en.wikipedia.org/wiki/Software_engineering) to describe a process for planning, creating, testing, and deploying an [information system](https://en.wikipedia.org/wiki/Information_system" \o "Information system).[[1]](https://en.wikipedia.org/wiki/Systems_development_life_cycle#cite_note-1) The systems development lifecycle concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.

Fedora cuenta con el respaldo de Red-Hat, el cual adquirió CentOS.

Para mirar manuales de CentOS 7, hay que mirar los manuales de Red-Hat 7, ya que CentOS sólo tiene manuales hasta la versión 5.

# RAID. ¿Qué es?

Un **grupo/matriz redundante de discos independientes**[1](https://es.wikipedia.org/wiki/RAID#cite_note-1)​ o **RAID** (del [inglés](https://es.wikipedia.org/wiki/Idioma_ingl%C3%A9s) *redundant array of independent disks*), hace referencia a un [sistema de almacenamiento de datos](https://es.wikipedia.org/wiki/Almacenamiento_de_datos) que utiliza múltiples unidades de almacenamiento de datos ([discos duros](https://es.wikipedia.org/wiki/Disco_duro) o [SSD](https://es.wikipedia.org/wiki/SSD)) entre los que se distribuyen o replican los [datos](https://es.wikipedia.org/wiki/Dato).

Dependiendo de su configuración (a la que suele llamarse *nivel*), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor [integridad](https://es.wikipedia.org/wiki/Integridad_de_datos), [tolerancia frente a fallos](https://es.wikipedia.org/wiki/Tolerancia_frente_a_fallos), [tasa de transferencia](https://es.wikipedia.org/wiki/Throughput) y [capacidad](https://es.wikipedia.org/w/index.php?title=Capacidad_de_almacenamiento&action=edit&redlink=1).

En el nivel más simple, un RAID combina varios discos duros en una sola [unidad lógica](https://es.wikipedia.org/w/index.php?title=Unidad_l%C3%B3gica&action=edit&redlink=1). Así, en lugar de ver varios discos duros diferentes, el [sistema operativo](https://es.wikipedia.org/wiki/Sistema_operativo) ve uno solo. Los RAID suelen usarse en [servidores](https://es.wikipedia.org/wiki/Servidor) y normalmente (aunque no es necesario) se implementan con unidades de disco de la misma capacidad.

Todas las implementaciones pueden soportar el uso de uno o más [discos de reserva](https://es.wikipedia.org/wiki/Disco_de_reserva_(RAID)) (*hot spare*), unidades preinstaladas que pueden usarse inmediatamente (y casi siempre automáticamente) tras el fallo de un disco del RAID. Esto reduce el tiempo del período de reparación al acortar el tiempo de reconstrucción del RAID.

El RAID puede ser de distintos niveles:

## RAID 0 (Data Striping, Striped Volume)

Un RAID 0 (también llamado conjunto dividido, volumen dividido, volumen seccionado) distribuye los datos equitativamente entre dos o más discos (usualmente se ocupa el mismo espacio en dos o más discos) sin información de paridad que proporcione [redundancia](https://es.wikipedia.org/wiki/Redundancia). Es importante señalar que el RAID 0 no era uno de los niveles RAID originales y que no es redundante. El RAID 0 se usa normalmente para proporcionar un alto rendimiento de escritura ya que los datos se escribe en dos o más discos de forma paralela, aunque un mismo fichero solo está presente una vez en el conjunto. RAID 0 también puede utilizarse como forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos. Un RAID 0 puede ser creado con discos de diferentes tamaños, pero el espacio de almacenamiento añadido al conjunto estará limitado por el tamaño del disco más pequeño (por ejemplo, si un disco de 450 [GB](https://es.wikipedia.org/wiki/Gigabyte) se divide con uno de 100 GB, el tamaño del conjunto resultante será sólo de 200 GB, ya que cada disco aporta 100 GB). Una buena implementación de un RAID 0 dividirá las operaciones de lectura y escritura en bloques de igual tamaño, por lo que distribuirá la información equitativamente entre los dos discos. También es posible crear un RAID 0 con más de dos discos.

No debe confundirse RAID 0 con un Volumen Distribuido (Spanned Volume) en el cual se agregan múltiples espacios no usados de varios discos para formar un único disco virtual. Puede que en un Volumen Distribuido el fichero a recuperar esté presente en un solo disco del conjunto debido a que aquí no hay una distribución equitativa de los datos (como dijimos para RAID 0), por lo tanto en ese caso no sería posible la recuperación paralela de datos y no tendríamos mejora del rendimiento de lectura.

## RAID 1 (espejo)

Un RAID 1 crea una copia exacta (o espejo) de un conjunto de datos en dos o más discos. Esto resulta útil cuando queremos tener más seguridad desaprovechando capacidad, ya que si perdemos un disco, tenemos el otro con la misma información. Un conjunto RAID 1 sólo puede ser tan grande como el más pequeño de sus discos. Un RAID 1 clásico consiste en dos discos en espejo, lo que incrementa exponencialmente la fiabilidad respecto a un solo disco; es decir, la probabilidad de fallo del conjunto es igual al producto de las probabilidades de fallo de cada uno de los discos (pues para que el conjunto falle es necesario que lo hagan *todos* sus discos).

Al escribir, el conjunto se comporta como un único disco, dado que los datos deben ser escritos en todos los discos del RAID 1. Por tanto, el rendimiento de escritura no mejora.

El RAID 1 tiene muchas ventajas de administración. Por ejemplo, en algunos entornos [24/7](https://es.wikipedia.org/wiki/24/7_(servicio)), es posible «dividir el espejo»: marcar un disco como inactivo, hacer una [copia de seguridad](https://es.wikipedia.org/wiki/Copia_de_seguridad) de dicho disco y luego «reconstruir» el espejo. Esto requiere que la aplicación de gestión del conjunto soporte la recuperación de los datos del disco en el momento de la división. Este procedimiento es menos crítico que la presencia de una característica de *[snapshot](https://es.wikipedia.org/wiki/Snapshot" \o "Snapshot)* en algunos sistemas de archivos, en la que se reserva algún espacio para los cambios, presentando una vista estática en un punto temporal dado del sistema de archivos. Alternativamente, un conjunto de discos puede ser almacenado de forma parecida a como se hace con las tradicionales cintas.

# LVM

**LVM** es una implementación de un [administrador de volúmenes lógicos](https://es.wikipedia.org/w/index.php?title=Administrador_de_vol%C3%BAmenes_l%C3%B3gicos&action=edit&redlink=1) para el kernel [Linux](https://es.wikipedia.org/wiki/Linux).

LVM incluye muchas de las características que se esperan de un administrador de volúmenes, incluyendo:

* Redimensionado de grupos lógicos
* Redimensionado de volúmenes lógicos
* Instantáneas de sólo lectura (LVM2 ofrece lectura y escritura)
* [RAID0](https://es.wikipedia.org/wiki/RAID#RAID_0:_Conjunto_de_discos_divididos_sin_tolerancia_a_fallos_.28No_Redundante.29) de volúmenes lógicos.

LVM no implementa [RAID1](https://es.wikipedia.org/wiki/RAID#RAID_1:_Espejo_y_Duplexing_.28Espejo.29) o [RAID5](https://es.wikipedia.org/wiki/RAID#RAID_5:_Discos_de_datos_independientes_con_bloques_de_paridad_distribuidos_.28Bloques_de_Intervalo_de_Paridad_Distribuida.29), por lo que se recomienda usar software específico de RAID para estas operaciones, teniendo las LV por encima del [RAID](https://es.wikipedia.org/wiki/RAID)

Un LVM se descompone en tres partes:

* **Volúmenes físicos (*PV*)**: Son las particiones del disco duro con sistema de archivos LVM. ([raid's](https://es.wikipedia.org/wiki/RAID" \o "RAID))
* **Volúmenes lógicos (*LV*)**: es el equivalente a una partición en un sistema tradicional. El LV es visible como un dispositivo estándar de bloques, por lo que puede contener un sistema de archivos (por ejemplo /home)
* **Grupos de volúmenes (*VG*)**: es la parte superior de la LVM. Es la "caja" en la que tenemos nuestros volúmenes lógicos (LV) y nuestros volúmenes físicos (PV). Se puede ver como una unidad administrativa en la que se engloban nuestros recursos. Hay que hacer notar que mientras un PV no se añada al VG, no podemos comenzar a usarlo.

# Crear un Ubuntu Server

Para crear un Ubuntu Server, tenemos que crear /, /home, /boot y /swap.

En VirtualBox, dejamos las opciones por defecto. Creamos un nuevo disco duro (para tener dos). Se recomienda que ambos sean del mismo tamaño.

No ciframos la carpeta personal, ya que ralentizaría muchísimo el sistema. En su defecto podríamos usar lucks, que cifra todo excepto la partición de arranque, y la ralentización es despreciable.

Hablemos de FDE. Full Disk Encryption

FDE consiste en cifrar el disco usando Cryptsetup y LUKS.

El instalador de Ubuntu se llama Ubiquity y para el 14.04 recibió una sola opción de casilla de verificación para el cifrado de disco completo totalmente automatizado. Puede comparar esto con el parámetro 'usar todo el disco y hacer lvm cifrado' en algunos otros instaladores, y realmente no puede ser más fácil que esto. Una ventaja adicional es que no hay un dolor de cabeza posterior a la instalación que intenta intercambiar y hibernar trabajando juntos.

Esta configuración utiliza los valores predeterminados de Cryptsetup con LUKS para AES en el modo XTS\_plain64, una clave de 256 bits con hash de contraseña SHA1 ejecutada durante 1 segundo de PBKDF2, por lo que la cantidad de iteraciones depende de la intensidad de su CPU. El sistema (/ o 'root'), las áreas de inicio y de intercambio están todas insertadas en un volumen lógico encriptado. La partición de arranque debe estar separada en Linux FDE, sin importar qué configuración o distribución, y para la mayoría, también debe estar sin cifrar (excepciones: Arch y Gentoo) para que / boot esté abierto a [atacantes con acceso físico](https://translate.googleusercontent.com/translate_c?depth=1&hl=es&prev=search&rurl=translate.google.es&sl=en&sp=nmt4&u=https://twopointfouristan.wordpress.com/2011/04/17/pwning-past-whole-disk-encryption/&usg=ALkJrhhFfKMcgkFHv0sBXu4VwLv1yYsEgg) a la computadora. Ubiquity crea una partición de arranque de ext2 de alrededor de 250 MB de tamaño.

Si está buscando mantener sus datos a salvo de robos ocasionales, esto está perfectamente bien, algunos incluso podrían argumentar una exageración. Por el contrario, sugiero que este sea el punto en el que cualquier dispositivo portátil deba *comenzar* porque es tan fácil de hacer, sería irresponsable no hacerlo.

El mayor problema con la automatización de Ubiquity es la ausencia de todo control que, en última instancia, significa que no se puede iniciar de forma dual con él, ni siquiera con otras distribuciones de Linux. Puede reformatear todo el disco e instalar solo el Linux cifrado, o puede instalarlo junto con Windows o cualquier otra cosa, sin cifrar.

## **Cifrado de disco completo de especificación personalizada**

Si el objetivo es configurar Cryptsetup con la configuración que elija, esta es actualmente la única forma de hacerlo. Incluso los instaladores alternativos solo le permiten seleccionar entre tres cifrados de cifrado y su tamaño de clave mientras hay más opciones de cifrado de cifrado disponibles al llamar desde la línea de comando.

Volviendo a lo del server:

Tenemos sda y sdb, es decir, dos discos. Vamos a crear una tabla de particiones para cada uno. La tabla de particiones define el tamaño y características de cada partición del disco.

Mientras estamos creando la tabla, vemos varias opciones para configurar.

Primero tenemos que configurar el raid por software. Creamos un dispositivo md, raid1.

Ahora tenemos los discos en un raid1.

Hay dos tipos de raids: Raid Hardware y Raid Software. Las diferencias posiblemente caigan en el examen.

|  |  |
| --- | --- |
|  | en raidhw la orden de escribir en disco a y b lo manda la controladora. en raidsw la orden la manda la cpu. en raidhw es más rápido en escritura y eso, mayor coste. El humanware de raidsw es más alto que de raidhw. en raidhw hay menos posibilidades de que algo vaya mal (cortes de luz y otros fallos). |

Ahora vamos a usar el LVM.

Debemos crear un grupo de volúmenes, seleccionamos md0 y continuamos. Ahora tenemos un volumen físico en uso, y un grupo de volúmenes. Debemos crear 4 volúmenes lógicos en ese grupo. Primero boot, con 200mb aprox. Aquí irá la imagen del kernel (25mb aprox, pero como podemos tener varias, pues le ponemos 200mb). Repetimos con home, raíz y swap, con 800mb, 6gb y el doble de la ram, respectivamente.

Ya tenemos los 4 volúmenes lógicos. Podemos terminar.

Volviendo al menú de configuraciones, vemos que tenemos 4 volúmenes lógicos, un raid1 y dos scsi

Serial Attached **SCSI** (SAS) es una interfaz de transferencia de datos en serie, sucesor del Small Computer System Interface (**SCSI**) paralelo, aunque sigue utilizando comandos **SCSI** para interaccionar con los dispositivos SAS. Aumenta la velocidad y permite la conexión y desconexión de forma rápida.

Vamos a configurar volúmenes cifrados. Le damos a créate encrypted volumes. No podemos activar nada todavía por que todavía no hay. Vamos a cifrar home, swap y raíz. Boot no, ya que grub no permite activar un volumen cifrado. Grub2 sí que lo permite. Un truco de seguridad podría ser llevarte el boot en un pen usb.

Swap hay que cifrarlo ya que si se apaga el pc, podrían acceder al swap para ver qué hay.

Hay varias opciones, pero están bien las opciones por defecto. Para mejorar el rendimiento en swap, por ejemplo, podemos poner una longitud de clave pequeña.

Nos pedirá dos veces para cada volumen lógico la contraseña.

Ahora vamos a configurar uno a uno los volúmenes lógicos. Usamos ext4, el resto de opciones, por defecto.

Por último, dejamos seleccionado standard system utility (utilidades básicas del sistema).

Instalamos el grub en el registro principal de arranque. Podemos hacerlo en sda o sdb, que al haber raid1, da igual.