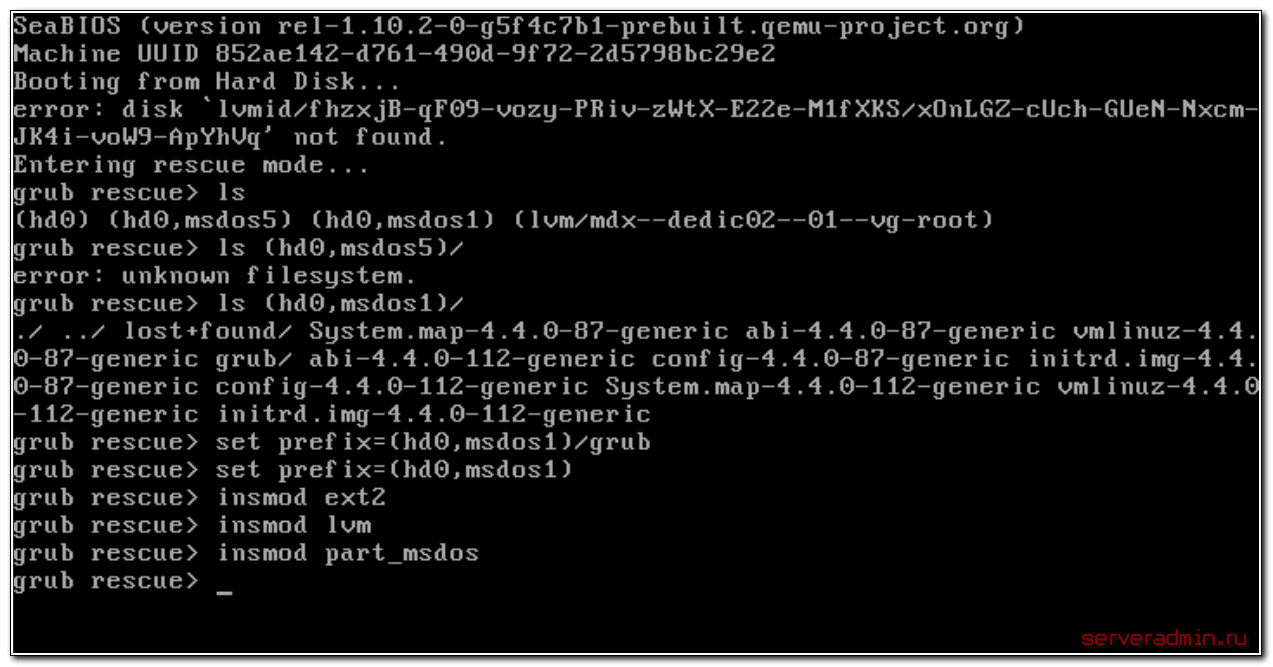
Для зашифровки системы ОС Linux был выбран метод, описанный в статьях <https://habr.com/ru/post/91948/> и <https://xakep.ru/2013/09/06/61210/>. А именно, выбрать основной носитель, на который будет ставиться ОС, и который будет зашифрован, и дополнительный, на «скрытый» (под «скрытым» понимается небольшой, относительно всего размера, раздел, который не будет виден в проводнике при подключении к ОС Windows, так же не будет заметно, что весь носитель сильно уменьшился в размере) раздел которого будет ставиться загрузчик, монтироваться /boot и в нём будет содержаться ключ для дешифрования основного носителя.

(дальше просто о проблемах, без всего алгоритма)

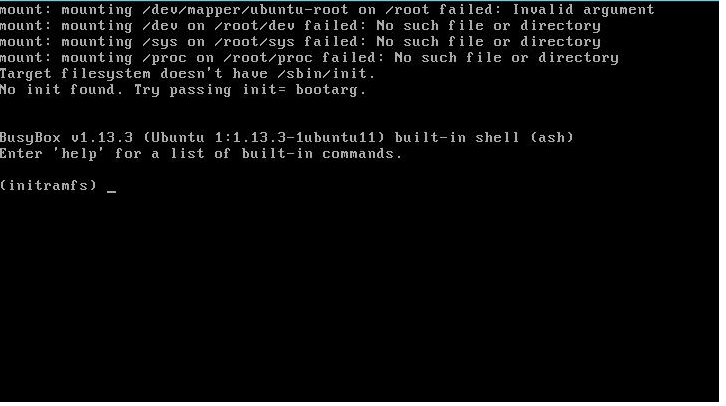
Сначала в качестве основного и дополнительного носителей были выбраны флэшки 8 и 128 ГБ соответственно.

Первая проблема возникла с LiveUSB системой, которая не справлялась с «замусориванием» основного носителя. Запись рандомных данных в блоки по 2 МБ на флэшку с интерфейсом USB 2.0 происходила слишком долго и иногда просто вылетала. Было решено записывать блоки по 8МБ с основной системы (либо в некоторых случаях с виртуальной машины).

Вторая проблема связана с правильной установкой ОС Linux (была выбрана Ubuntu 20.04). Никак не удавалось установить /boot раздел и загрузчик на другой носитель так, чтобы система запускалась без проблем, постоянно приходилось при каждом запуске заново инициализировать /root и показывать загрузчику, где находится файл initrd.img.



Так же была непонятная ошибка с инициализацией файловой системы оперативной памяти, так же непонятно почему она пропала при следующей переустановки системы.



Были неудачные попытки провести стандартную установку, и затем переносить /boot раздел на флэшку. Но это было не так удобно.

Третья проблема связана с правкой конфига grub.cfg, к слову, в некоторых источниках писалось о том, что менять его вручную не следует. Однако сама загвоздка была в разных menuentry – в конфиге их было очень много, как текущая версия системы, так и несколько предыдущих сборок ядра, при чём у каждой из сборок был recovery mod. При замене всех UUID рута на логический том блочного устройства на флэшке (которую мы разбили по алгоритму) система не могла загрузиться. Только при подмене текущей версии сборки ядра на наш логический том, система смогла стартовать. Возможно, связано это с командой

# update-initramfs -u -k all

Которая не могла создать нужные файлы для всех сборок.

Так же оказалось невозможным использовать для /home иной от / файловой системы (если / имеет фс ext4, то и /home должен быть ext4).

Иногда не получалось заархивировать всю систему, т.к. некоторые процессы использовали определенные важные файлы, какие процессы и почему непонятно. Были попытки заархивировать систему из-под другой системы, но в последующих попытках проблем не возникало.

При переносе самой системы оказалось, что не хватает места на флэш-накопителе, хотя её размер 16 ГБ, а система около 5.6 ГБ. Вся проблема была в неверном разбиении на логические тома:

# lvcreate -L3G -nroot vg

В параметре -L3G нужно было указать больше места (например, вместо 3 ГБ выделить 8 ГБ).

Ну и основная проблема заключалась в медленной работе флэш-накопителей. Первые 10 раз, когда я пытался установить систему на флэш-накопитель (для последующего архивирования и переноса), установка проходила от 4 часов, в зависимости от выделенного пространства и кол-ва предустановленных утилит и программ. Даже минимальная установка требовала много времени. Открытие веб-браузера, проводника, терминала, скачивание и установка cryptsetup, lvm2 пакетов было целым испытанием для ОС, не говоря уже о «update-initramfs -u -k all».

Было принято решение взять SSD накопитель, выделить на нём 15 ГБ и устанавливать систему туда. Но после переноса на зашифрованный флэш-накопитель возникала та же проблема, сама расшифровка длилась много времени, и сама загрузка могла быть более 10 часов (во время которых могло просто зависнуть и не было понятно грузится система или зависла). В виду отсутствия более быстрых флэш-накопителей, было решено воспользоваться тем же решением (шифровать раздел SSD диска и переносить систему туда).

Многие из этих проблем были незначительными и решались за 1-2 запроса в гугл, однако некоторые ставили в тупик.