1. Установить три ВМ (ОС AstraLinux 1.6):
2. ALD (2 GB ОЗУ, 20 GB HDD)
3. DLP (8 GB ОЗУ 150 GB HDD)
4. CL ((2 GB ОЗУ, 20 GB HDD)

На всех ВМ пользователь useradmin пароль xxXX1234, название ВМ прописными буквами (маленькими)

После установки настроить сетевой адаптер через графический иинтерфейс

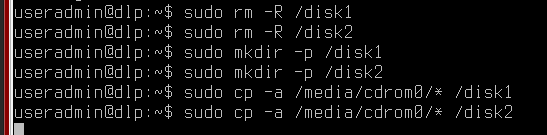
ald X.X.X.130 (шлюз и ДНС не указываем)

dlp X.X.X.131 (шлюз и ДНС – IP ald)

cl X.X.X.132 (шлюз и ДНС – IP ald)

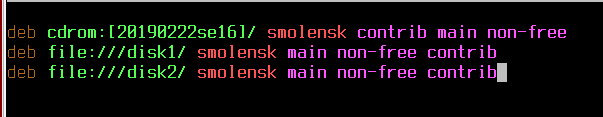
Отредактировать файл hosts (sudo nano /etc/hosts)

1. Создать Astra Linux Domen на ВМ ALD и включить в его состав оставшиеся ВМ (dlp, cl)
2. Для обновления до версии 2 (обновление необходимо произвести на ВМ dlp и cl): скопировать содержимое дисков
3. smolensk-1.6 в disk1
4. devel-smolensk-1.6 в disk2



Добавить две строчки deb <file:///disk1/> Smolensk ……….





Все остальные строки удалить

Смонтировать поочередно диски с обновлением:

1. 20190222se116

Установка обновления, поочередно с каждым диском:

sudo mount /mnt/20190222se16.iso /media/cdrom  
sudo apt-cdrom -m add  
sudo umount /media/cdrom

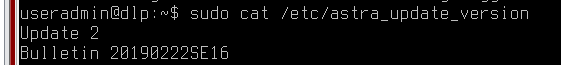
на вопрос об имени диска ввести "20190222se16".

sudo apt update  
sudo apt dist-upgrade  
sudo apt -f install

1. repository-update-dev

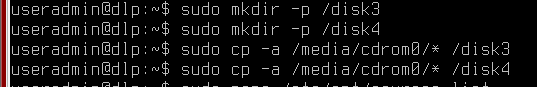
Подключить repository-update-dev и повторить

проверить версию обновления



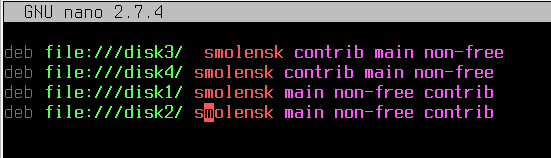
Скопировать содержимое дисков

1. 20190222se16 в disk3
2. repository-update-dev в disk4



перед установкой DLP отредактировать /etc/apt/sources.list

все лишнее удалить



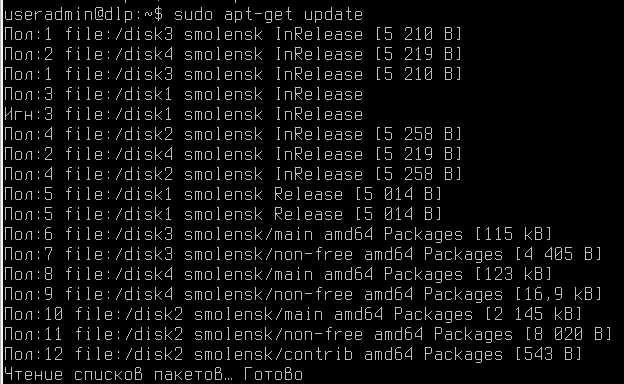
Перезагрузить sudo reboot

1. Создаем директорию distr и копируем в неё установщики IWTM (образ Astra.iso)

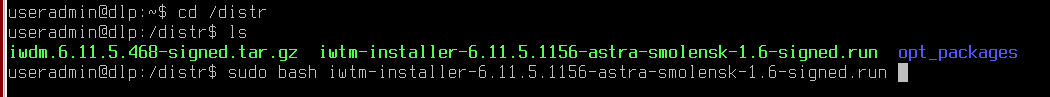




Обновить списки источников

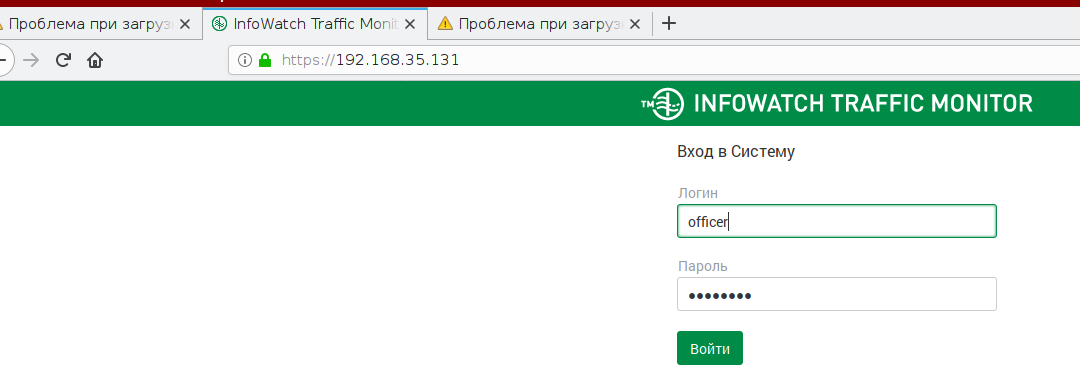


Переходим в директорию с установщиком IWTM и вводим команду установки:



По окончании установки перезагрузить ВМ и с любой другой машины проверить работоспособность подключением через Web-интерфейс

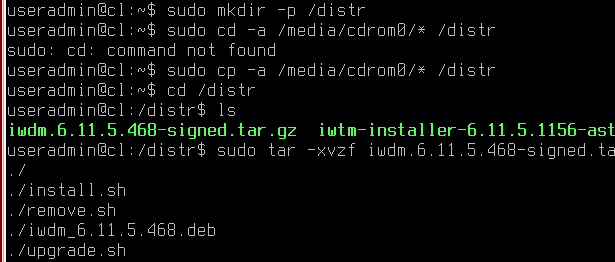
Вводом в адресную строку браузера IP адреса ВМ dlp



Для авторизации использовать логин “officer” пароль “xxXX1234”

1. После успешной инсталляции TM переходим на машину cl и повторяем пункт 3 (обновление системы до версии 2) и пункт 4 (создание репозитория /distr). Создание репозитория /disk3 и /disk4 не выполняем.

5.1 Переходим в директорию с установщиком IWTM и вводим команду распаковки архива:



и установки:

sudo ./install.sh dmserver:15101

где dmserver – имя ВМ с ОС WinServ2019, 15101 – порт

Продукт будет установлен в директорию /opt/iw/dmagent.

Проверить статус сервисов можно командой:

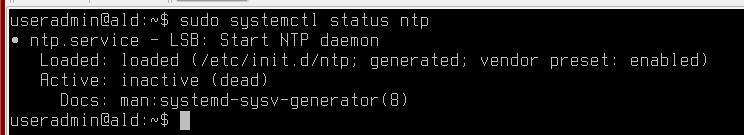
sudo systemctl status iwdm\*

5.2 Редактируем файл hosts

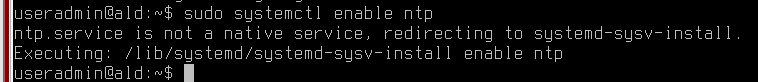
* Добавляем запись Х.Х.Х.135 dmserver

(dmserver - ВМ с ОС WinServer 2019 – 4-я ВМ)

1. После установки IWTM переходим на ВМ ALD и поднимаем службу NTP



Запускаем службу ntp



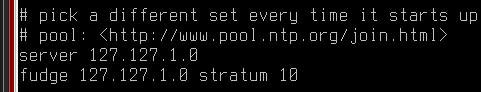
Проверяем статус, если не изменилось, то устанавливаем службу:



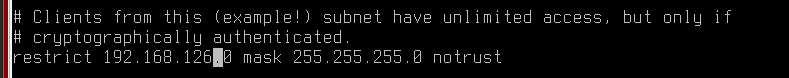
Редактируем конфигурационный файл



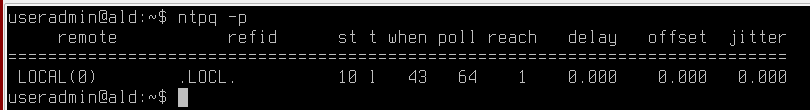
Добавляем строки, предварительно удалив 4-е имеющиеся



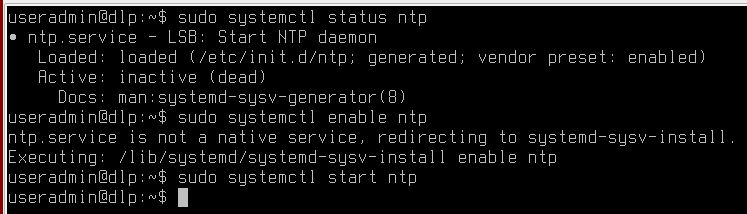
Прописываем третий октет



Проверяем источник времени



на клиентах вкл ntp

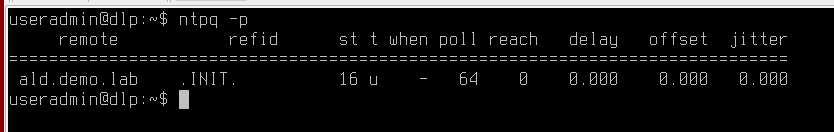


Изменяем файл

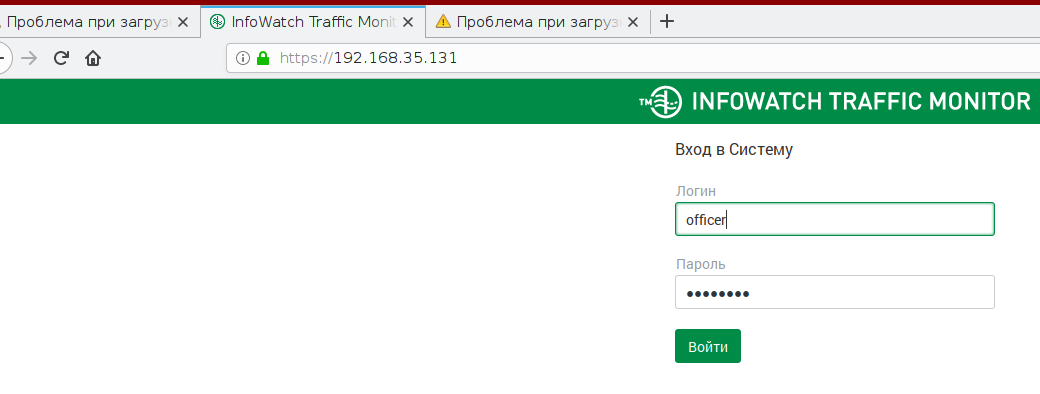




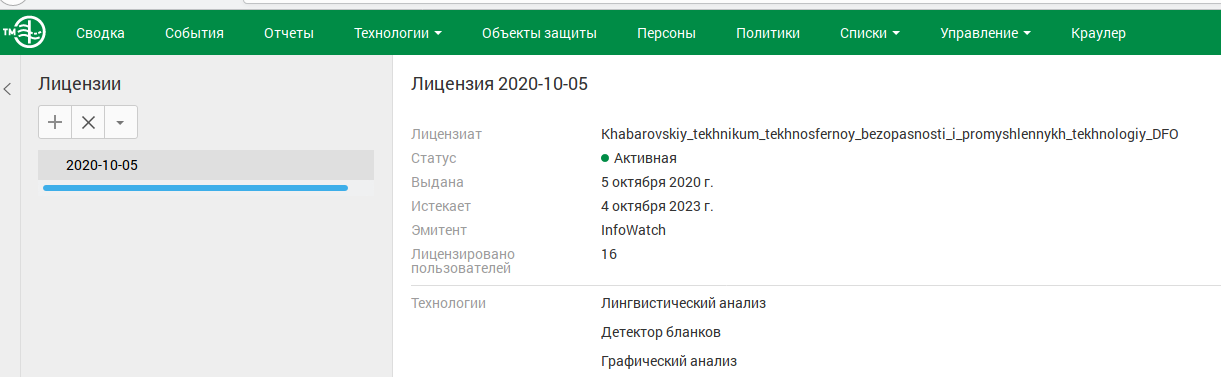




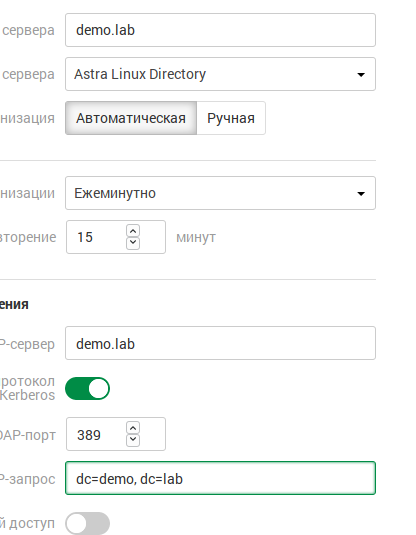
1. После установки службы ntp через браузер набираем в адресной строке IP-адрес dlp, для входа в веб-консоль используем пользователя officer и пароль xxXX1234



Переходим по пути управление/лицензии и подгружаем лицензию Lic\_IWTM\_6\_10.iso



После устанавливаем LDAP-синхронизацию



1. Установка ssh соединения

systemctl enable ssh  
systemctl start ssh

Настройка пакета

Проверить состояние сервиса:

systemctl status ssh

Конфигурация сервера хранится в файле /etc/ssh/sshd\_config.

Чтобы изменения вступили в силу необходимо перезапустить сервис:

systemctl restart sshd

для входа на удаленную ВМ использовать команду:

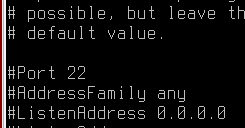


Где user1 – это пользователь под, которым заходим

ald – имя удаленной машины

8.2 Для изменения порта для ssh отредактировать файл

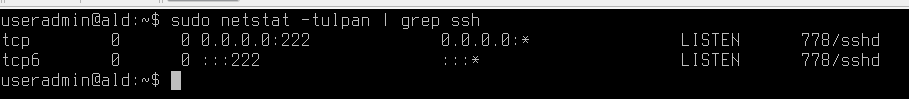




Раскоментировать строку #Port 22 убрать # и изменить 22 на нужный портщ

Перезапустить systemctl restart sshd

Что бы проверить вступили ли в силу изменения выполнить команду



8.3 Для запрета доступа всем ip адресам кроме своих машин необходимо отредактировать файл



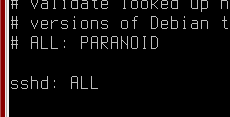
Добавить ip-адреса доверенных машин



Также внести изменения в



Добавить sshd: ALL

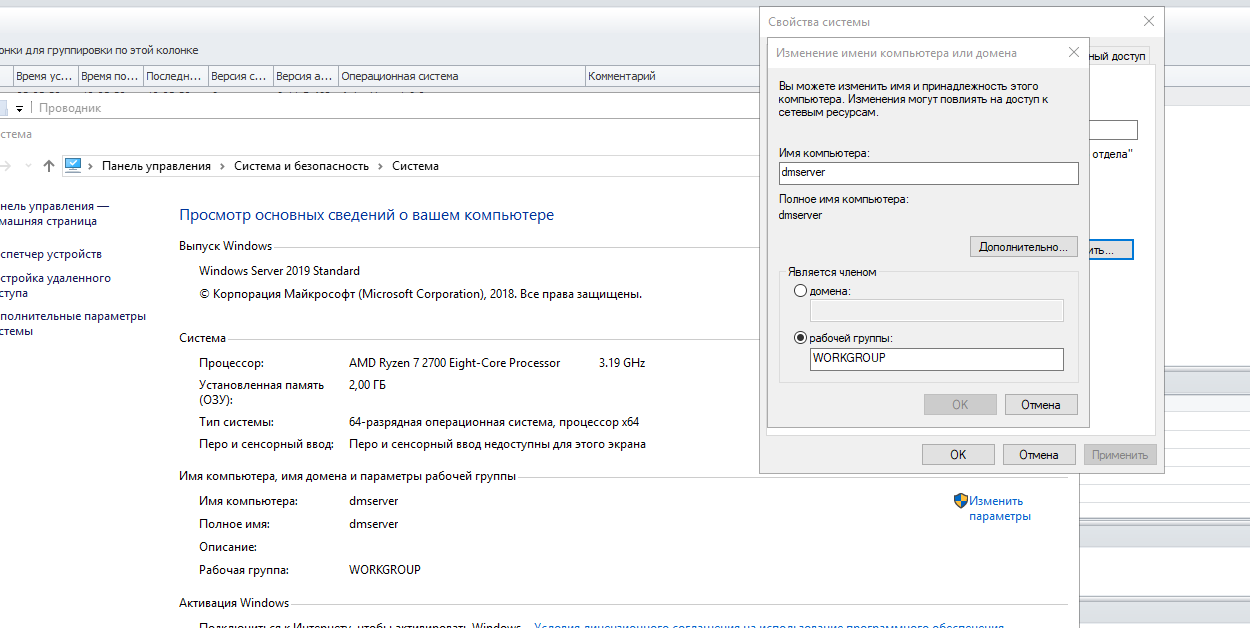


Повторить на всех ВМ с учетом адреса, выше приведен пример для ald, т.е. для dlp в hosts.allow указываем 192.168.Х.130 и 192.168.х.132

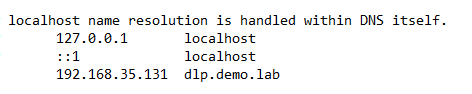
Для client 192.168.х.130 и 192.168.х.131

1. ВМ WinServer 2019

Изменить имя ВМ на dmserver

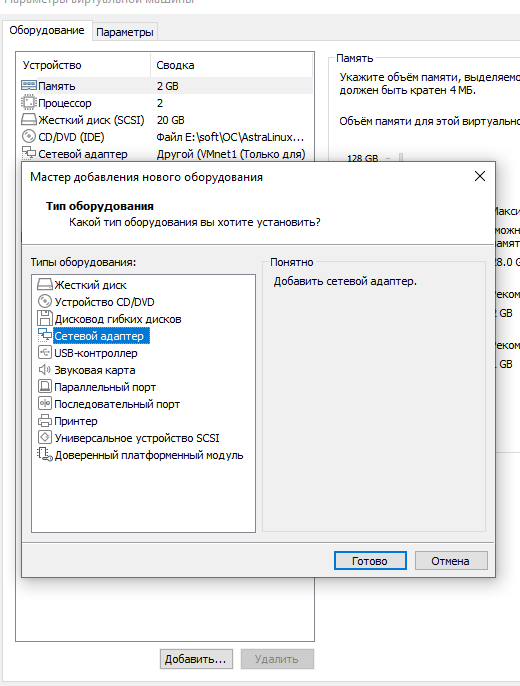


Добавить запись в файл hosts путь 

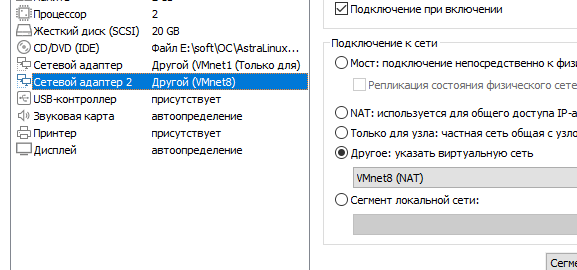


10 подключение доступа к сети интернет

Для ВМ ALD добавляем второй сетевой адаптер



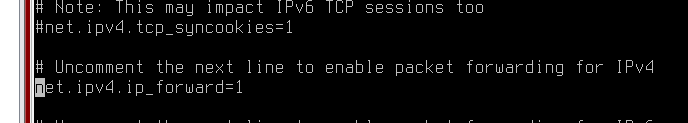
И настраиваем *другое – NAT*



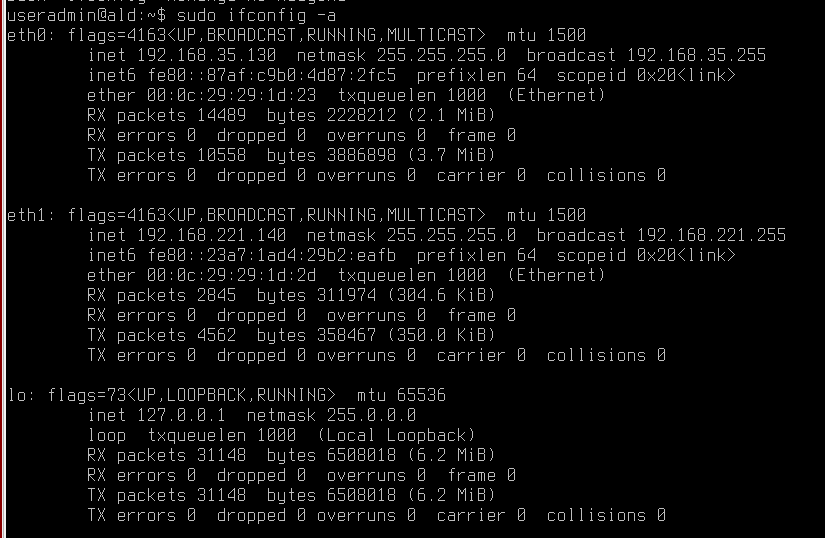
В самой ОС AstraLinux ни каких изменений для адаптера не вносим

Переходим для редактирования



Ищем там строку #net.ipv4.ip\_forward=1, и убираем знак комментария.

Также необходимо узнать названия наших сетевых интерфейсов и их IP адреса. Для этого введем следующую команду: sudo ifconfig -a



Как мы видим адаптер eth1 имеет отличный от нашей сети IP-адрес – это и есть адаптер, смотрящий в интернет.

Для перенаправление tcp порта 2222 на tcp порт 2223 другой машины, необходимо добавить следующие правила iptables:

sudo iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

Это правило разрешает прохождение входящих пакетов внутрь сети.

Теперь опишем форвардинг (forwarding) пакетов:

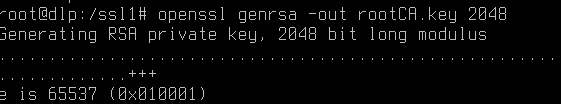


11 Создание сертификата для https

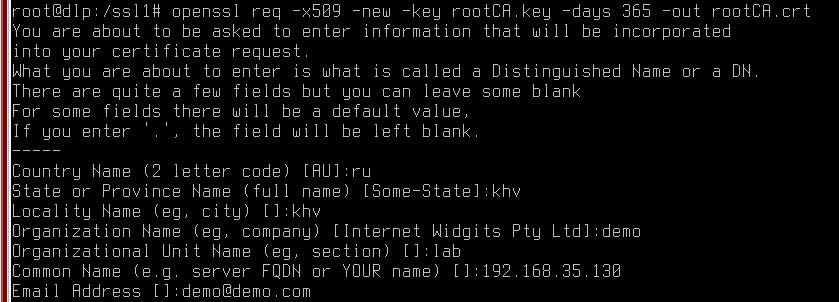
Создаем директорию для хранения



создаём корневой ключ



создаём корневой сертификат

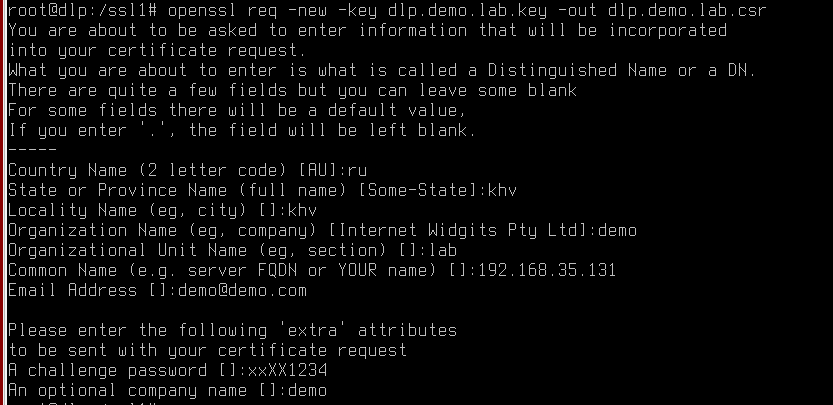


Создаем сертификат подписаный нашим СА

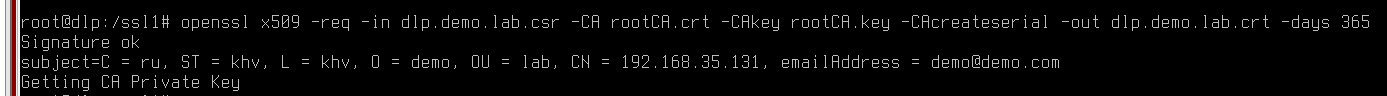
Генерируем ключ.



Создаем запрос на сертификат. Тут важно указать имя сервера: домен или IP



и подписать запрос на сертификат нашим корневым сертификатом



Теперь на клиенты нужно установить корневой сертификат rootCA.crt  
  
**rootCA.crt** — можно давать друзьям, устанавливать, копировать на сервера, выкладывать в публичный доступ  
**rootCA.key** — следует держать в тайне

По заданию все сертификаты должны быть представлены единым пакетом PKCS (.p12), для этого:

Если сертификат и секретный ключ хранятся в разных файлах (например, вы сгенерировали ключи сами, а потом создали запрос на получение сертификата), команда создания пакета PKCS#12 будет выглядеть так:

openssl pkcs12 -export -in rootCA.crt -inkey rootCA.key -out cert.p12

11.2 для распространения **rootCA.crt** необходимо поднять Samba сервер для создания общей папки (ссылка <https://wiki.astralinux.ru/display/doc/Samba>)

sudo apt install fly-admin-samba

Для указания разделяемого ресурса в конфигурационный файл /etc/samba/smb.conf

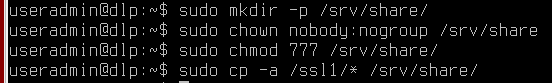
добавить секцию вида:

|  |
| --- |
| [share]      comment = For all doc's  # Доступно всем      guest ok = yes      force user = nobody      force group = nogroup      path = /srv/share      read only = no |

и перезапустить samba, чтобы изменения вступили в силу:

sudo systemctl restart smbd

далее создаем директорию и наделяем права доступа и копируем содержимое папки ssl1, хотя необходимо скопировать только **rootCA.crt**



Для того, чтобы проверить разделяемые ресурсы samba, доступные в сети, можно использовать команду

smbtree

Эта команда выводит дерево рабочих групп, и принадлежащих им ресурсов (файлов, принтеров и пр.) всех серверов samba, доступных в сети.

11.3 Установка сертификатов

12 создание нового диска в режиме LVM на домене (ALD)

<https://guruadmin.ru/page/dobavlajaem-dopolnitelnyj-disk-v-gostevuju-sistemu-linux-pod-vmware-bez-perezagruzki>

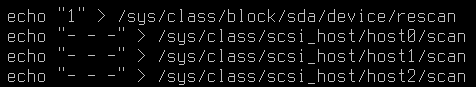
Добавляем новый жесткий к ВМ ALD

Устанавливаем службу LVM



Далее переходим под root (sudo su)

Сканируем диски













Создаем логический раздел, размер - 5 гигабайт



Проверить создание раздела можно командой

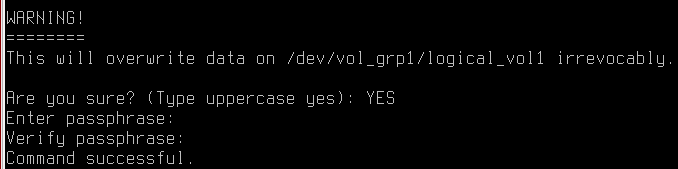


Для создания шифрованного раздела используем Утилиту Cryptsetup,

Для этого выполняем команду







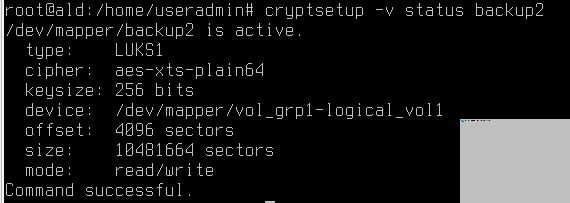
Выполните такую команду чтобы открыть только что созданный раздел с помощью модуля dm-crypt в /dev/mapper, для этого понадобится ввести пароль, с которым выполнялось шифрование luks linux:



Проверить содержимое созданного раздела



Чтобы посмотреть состояние устройства выполните:



### ФОРМАТИРОВАНИЕ РАЗДЕЛА

Давайте для начала отформатируем диск. Для надежности, чтобы стереть все данные, которые были в этом месте раньше, перезапишем наш шифрованный раздел linux нулями. Это уменьшит вероятность взлома шифрования, через увеличение количества случайной информации. Для этого выполните:

 dd if=/dev/zero of=/dev/mapper/backup2

Работа утилиты может занять несколько часов, чтобы иметь возможность наблюдать за процессом, используйте pv:

 pv -tpreb /dev/zero | dd of=/dev/mapper/backup2 bs=128M

Когда процесс завершится мы можем отформатировать устройство в любую файловую систему. Например, отформатируем в ext4:

sudo mkfs.ext4 /dev/mapper/backup2

**МОНТИРОВАНИЕ РАЗДЕЛА**

Теперь можно примонтировать только, что созданную файловую систему:

 mkdir /backup2

sudo mount /dev/mapper/backup2 /backup2

 ls -l /backup2

<https://losst.ru/sozdanie-i-nastrojka-lvm-linux>

<https://www.dmosk.ru/miniinstruktions.php?mini=vmware-add-disksize>