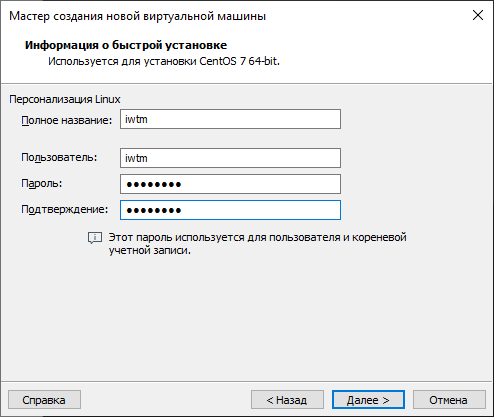
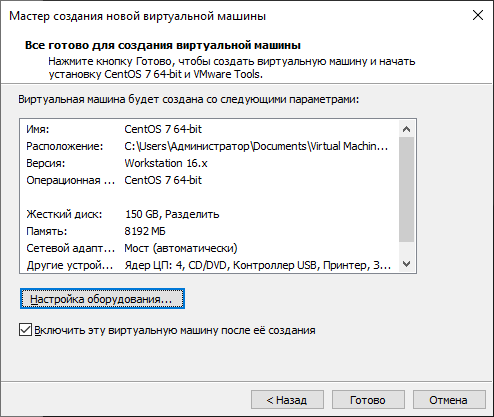
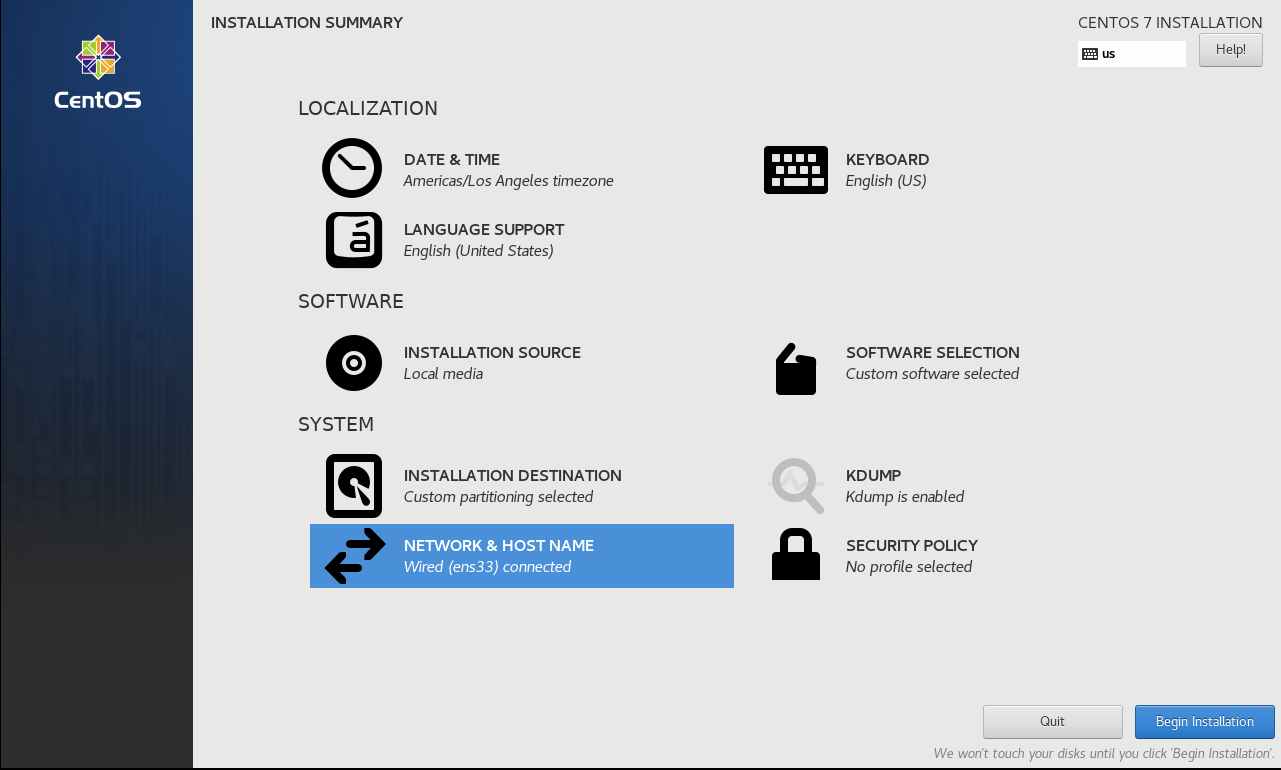
**Установка ТМ**

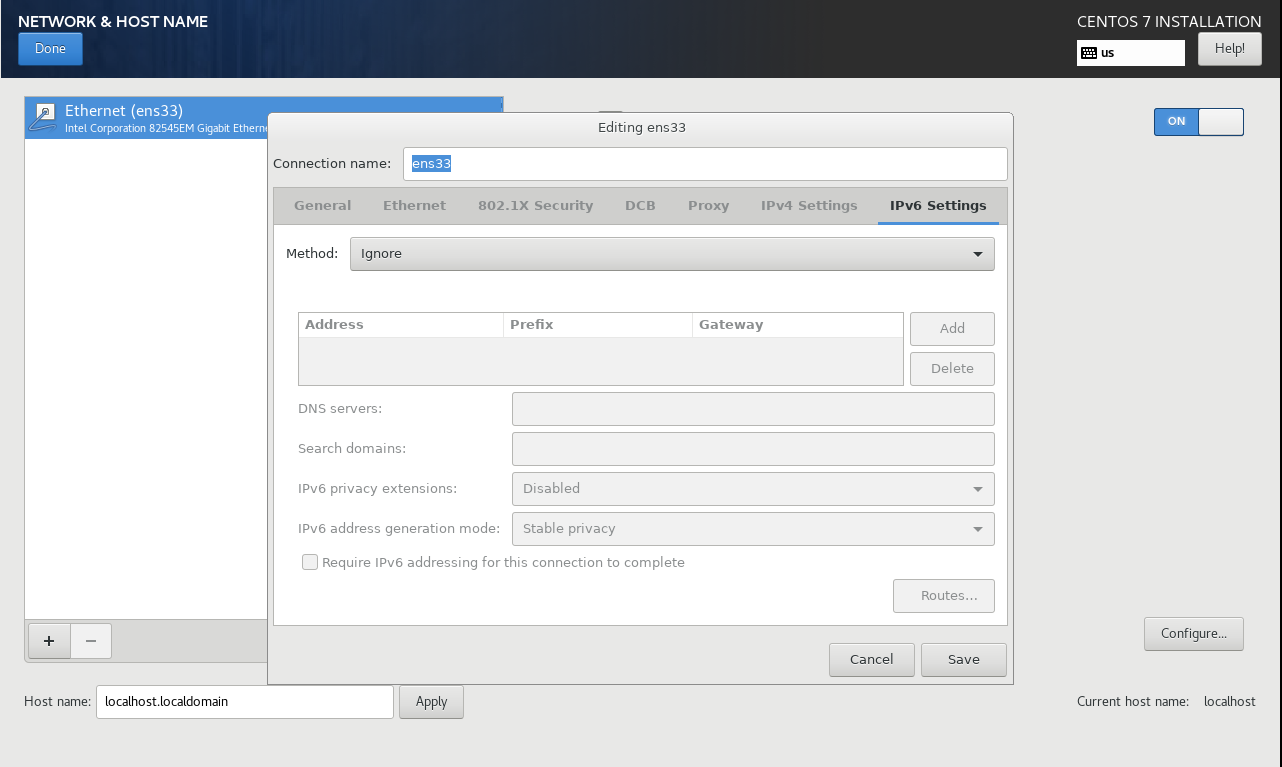
Вводим название и пароль нашей будущей ТМ.

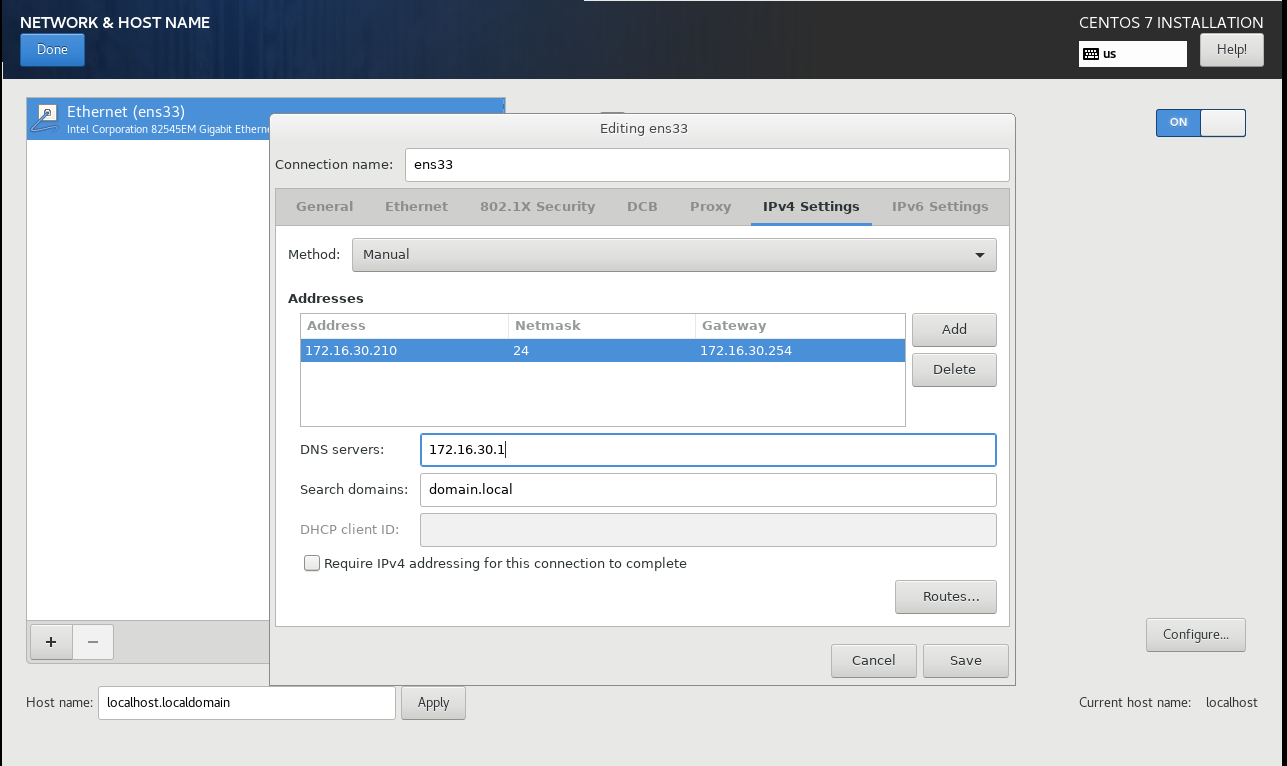


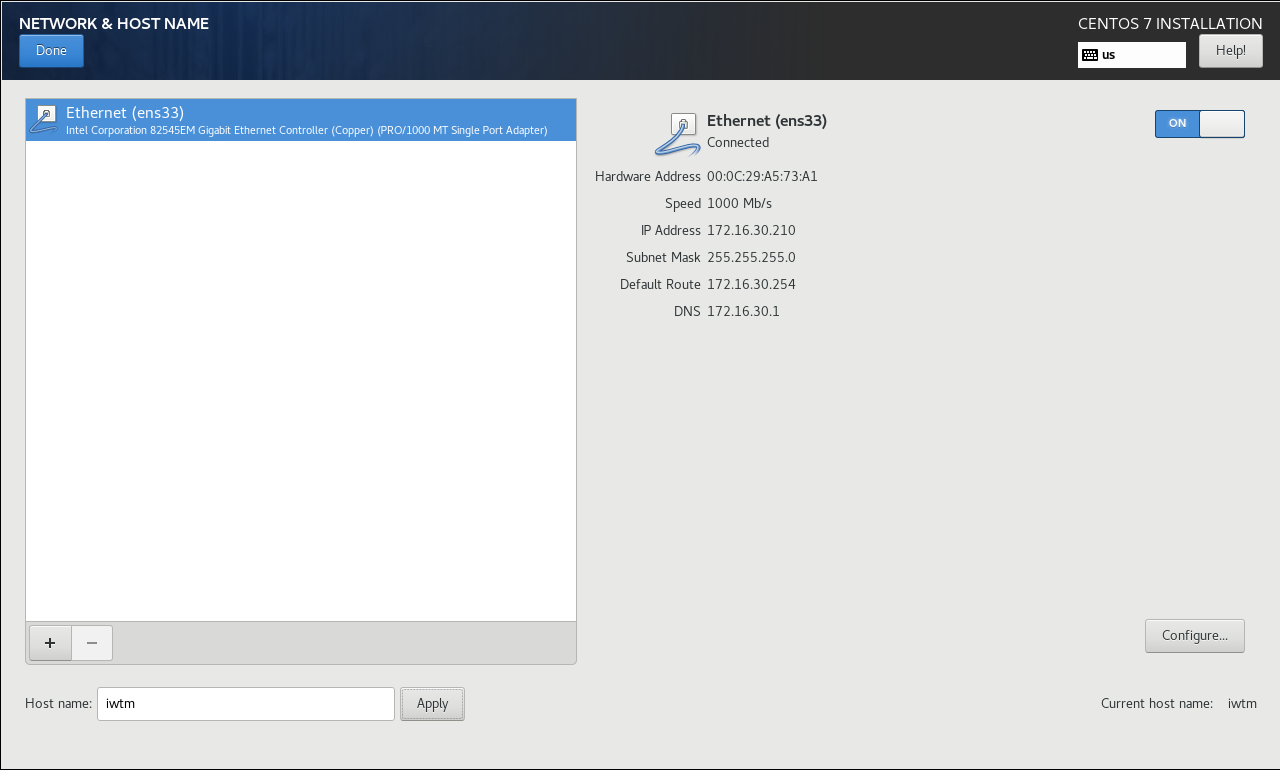




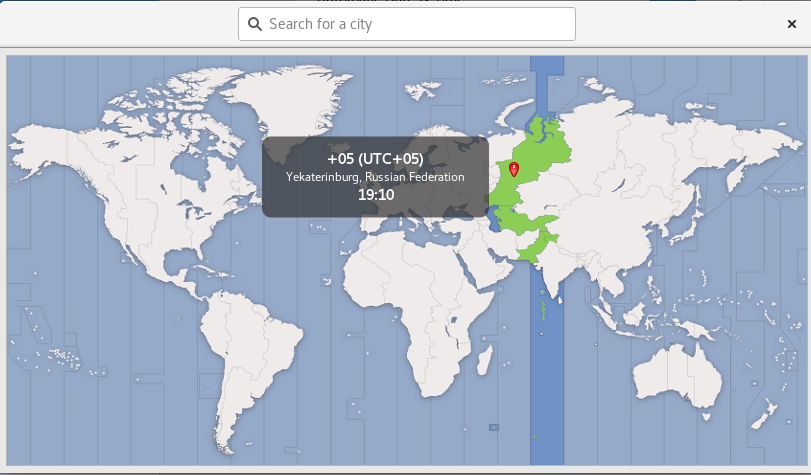
Настройка сети.



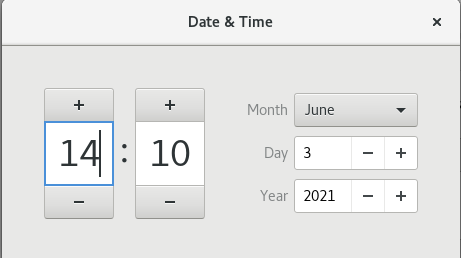


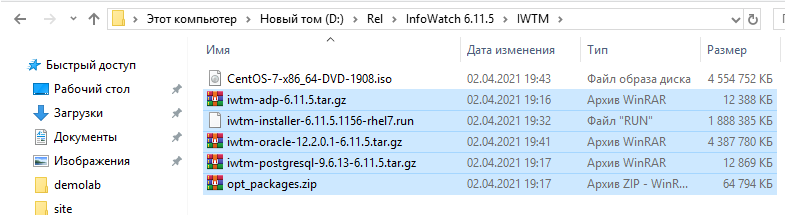


Выбираем часовой пояс Екатеринбург.

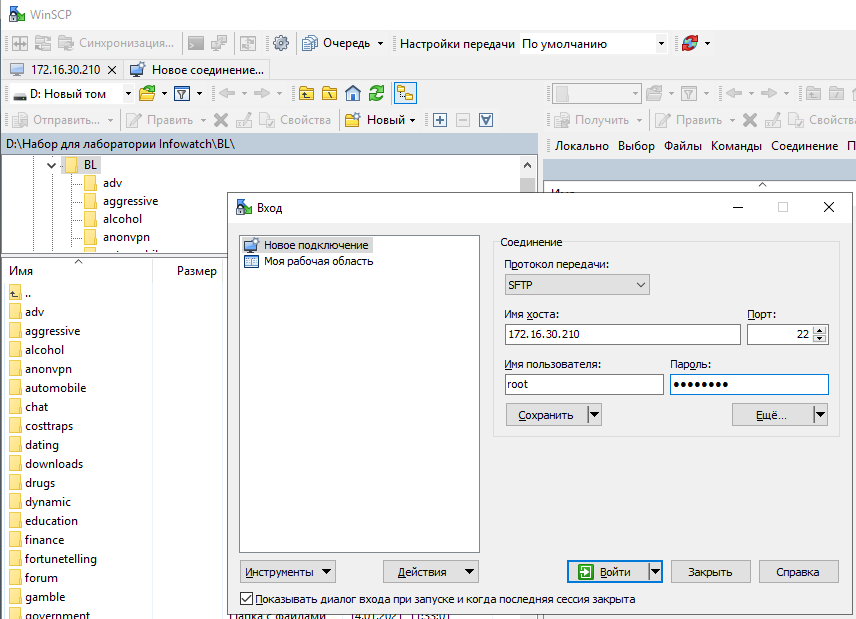


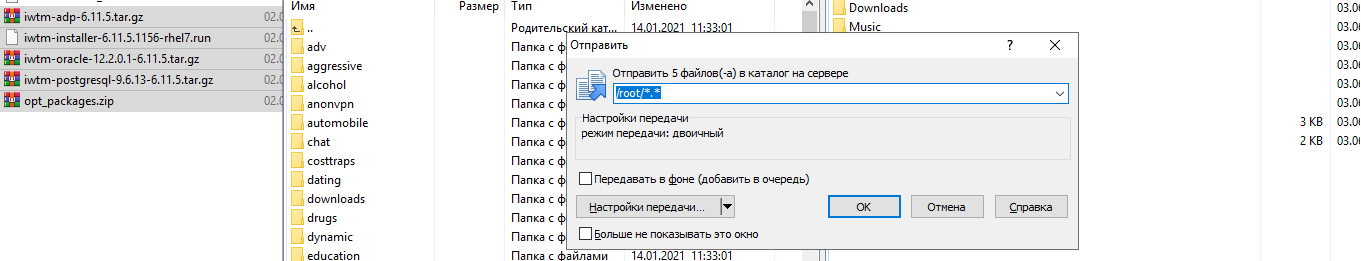
Прописываем дату и время, если нужно.

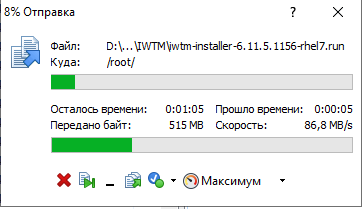


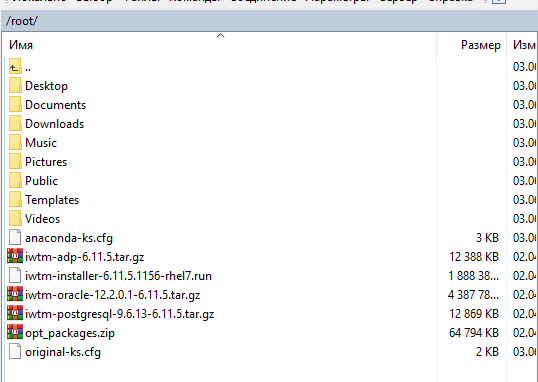


Пересылаем пакеты на нашу ТМ с помощью WinCSP.

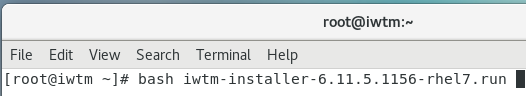


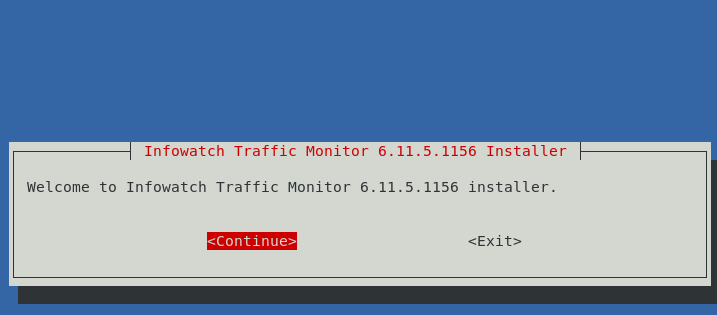




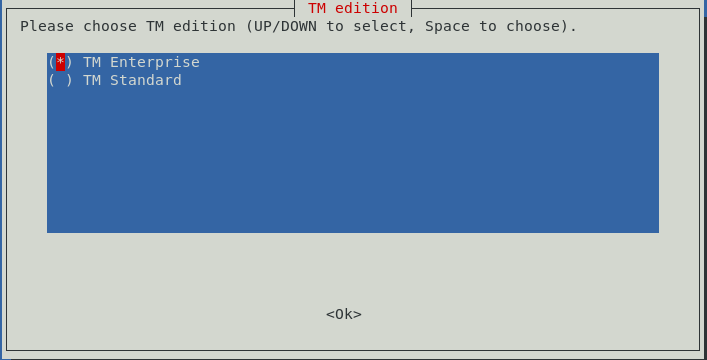


Далее в самой ТМ (консоли) прописываем команду bash для установки пакетов.

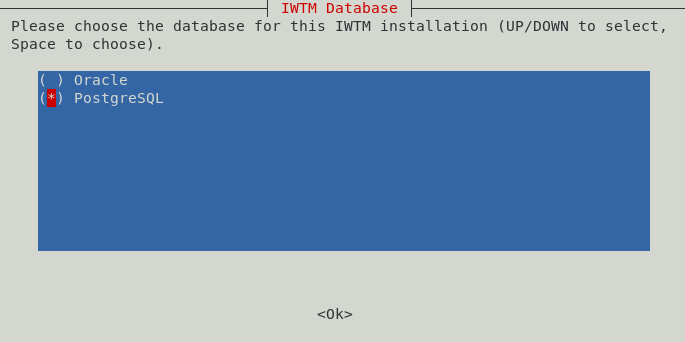




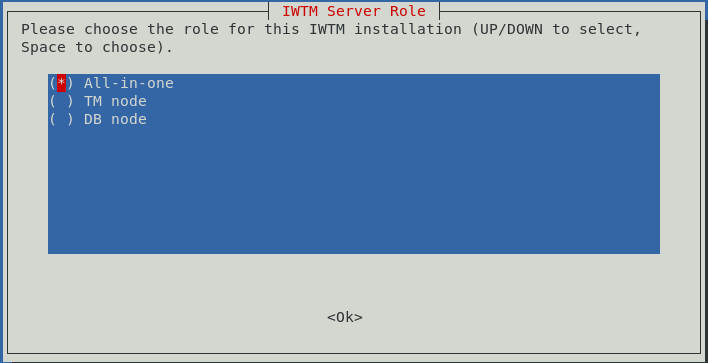
Выбираем TM Enterprise



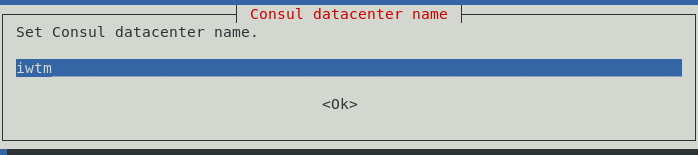
PostgreSQL



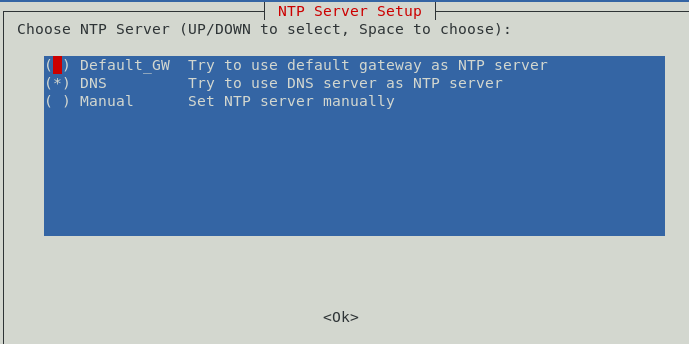
All-in-one



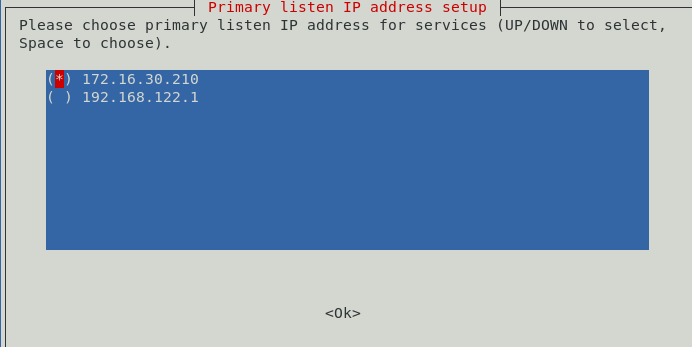
Вводим имя Consul



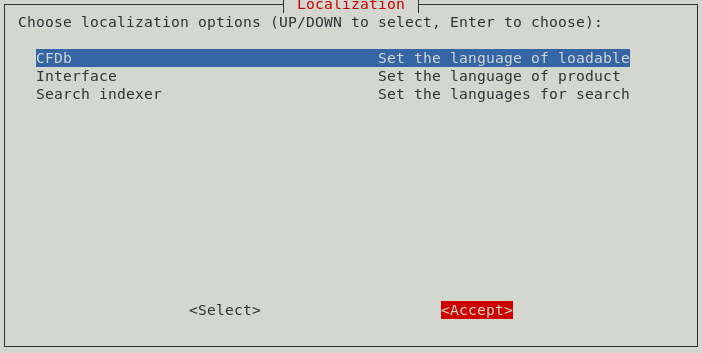
Выбираем DNS

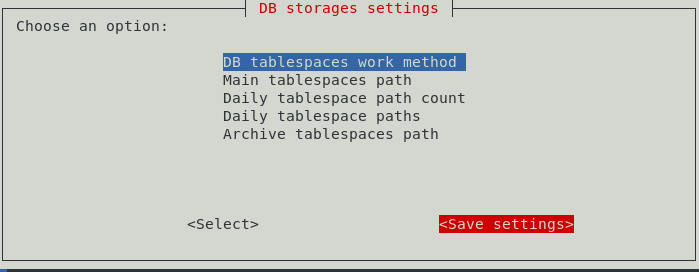


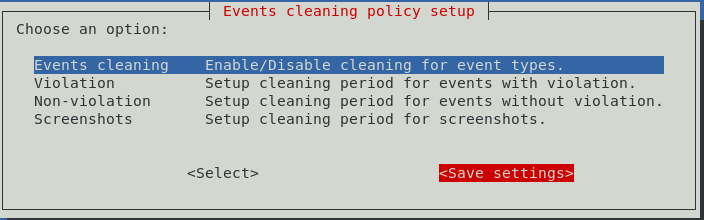
Выбираем ip

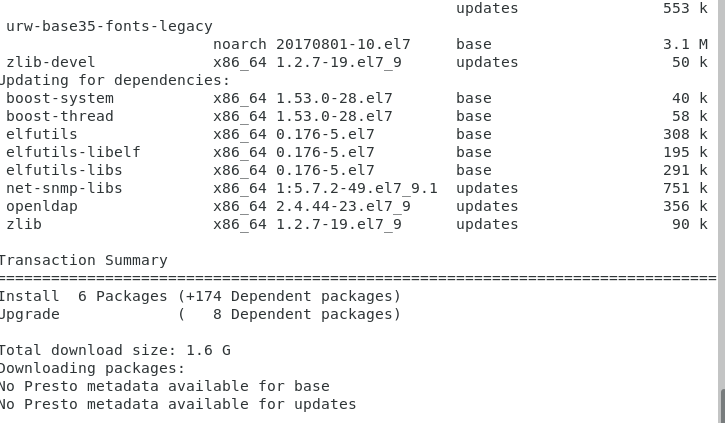


Оставляем все параметры как есть

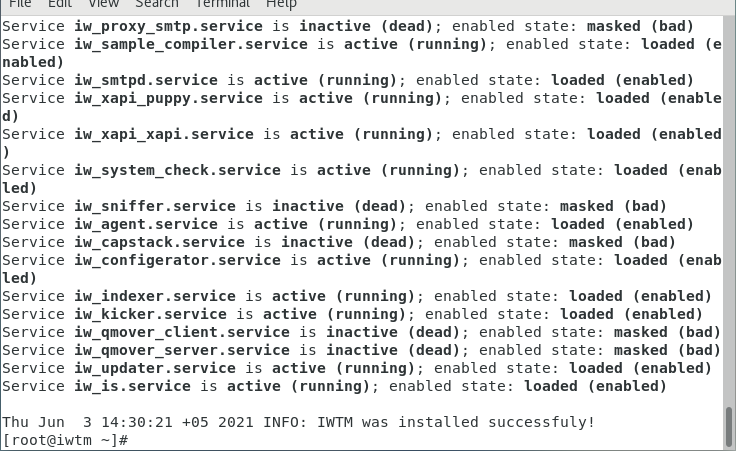




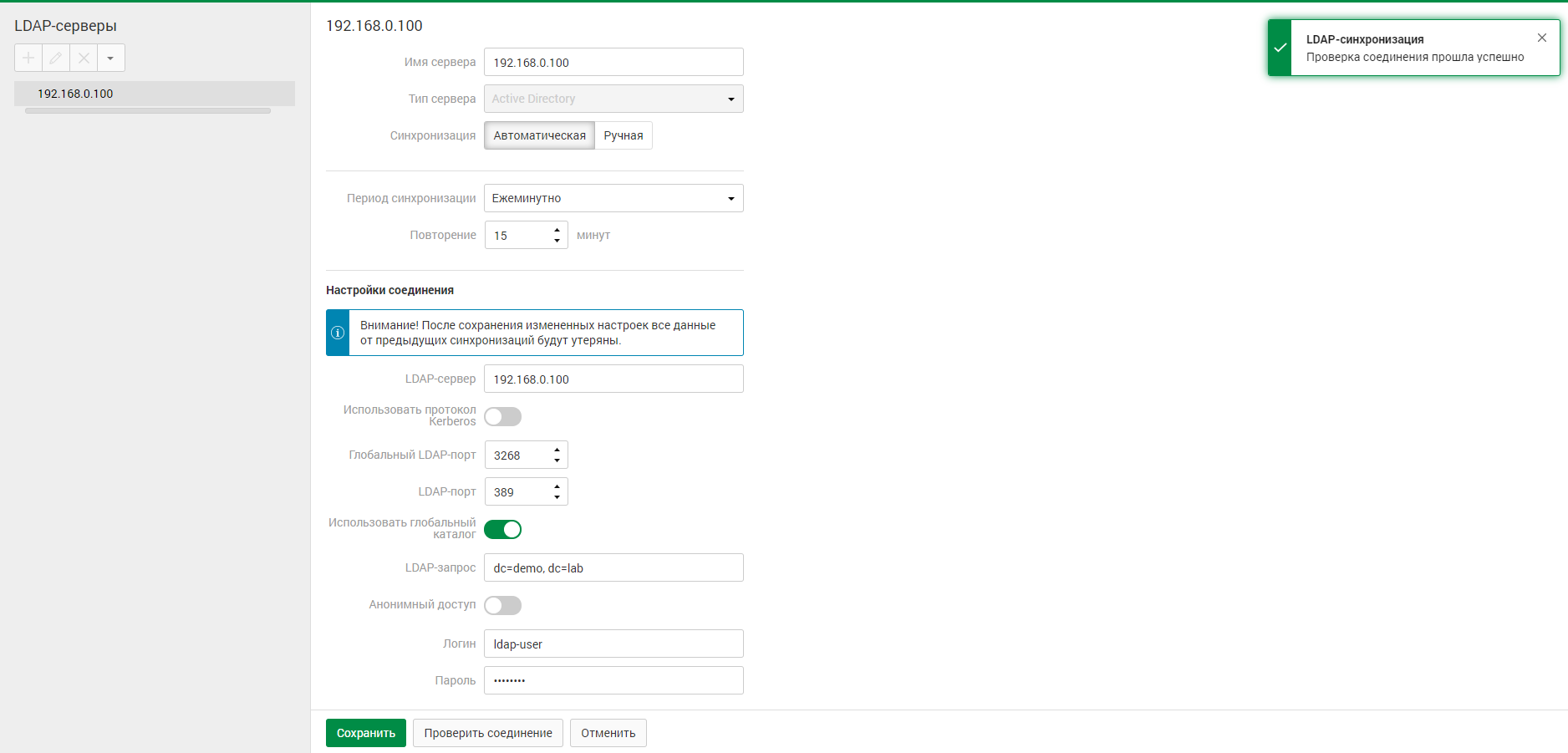




Пакеты установлены



Заходим в браузер вводим ip TM. Пишем логин и пароль: officer – xxXX1234. Потом делаем LDAP синхронизацию



**Задание 7: Защита системы с помощью сертификатов**

Создайте цифровой сертификат (дерево сертификатов) формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности, длине ключа и т.п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата – на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

* корневой root-сертификат (ca)
* серверный (server) сертификат
* по желанию допускается использование пользовательского (user) сертификат

Итоговый результат должен включать:

Дерево из 2 (3)-х сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов.

Содержимое команд по генерации ключей и сертификатов в текстовом файле «отчет.txt»

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе просмотра сертификатов Windows (закладки «Общие», «Путь сертифкации»).

Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации о компании Demo.lab и т.п.

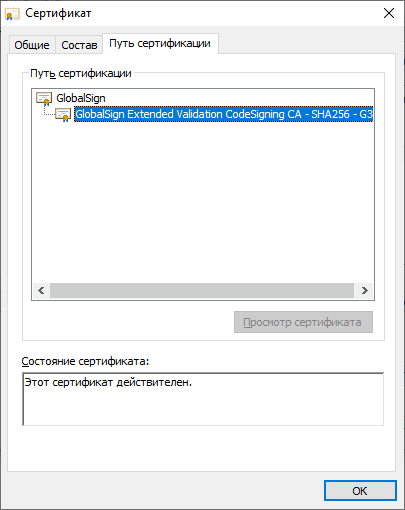
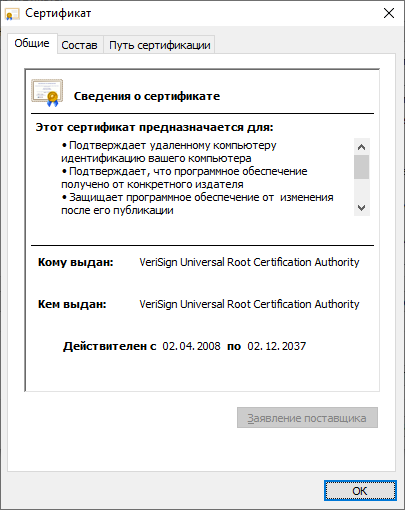


Рис1. Пример скриншотов задания 6

Генерацию сертификатов зафиксируйте скриншотами.

**Сертификаты**

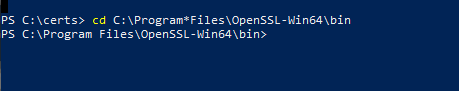
**Установка в AD**

Устанавливаем https://slproweb.com/download/Win64OpenSSL-3\_0\_1.exe

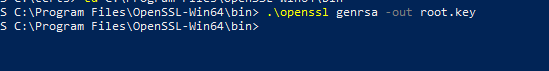
В папке bin копируем файл openssl.conf  

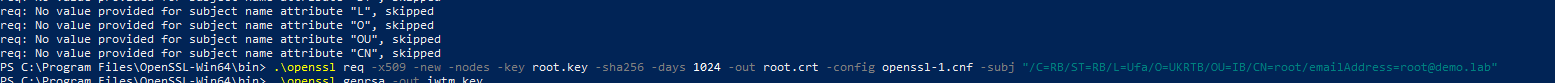

Затем заходим от админа в PowerShell

Вводим



Далее вводим .\openssl.exe genrsa -out root.key

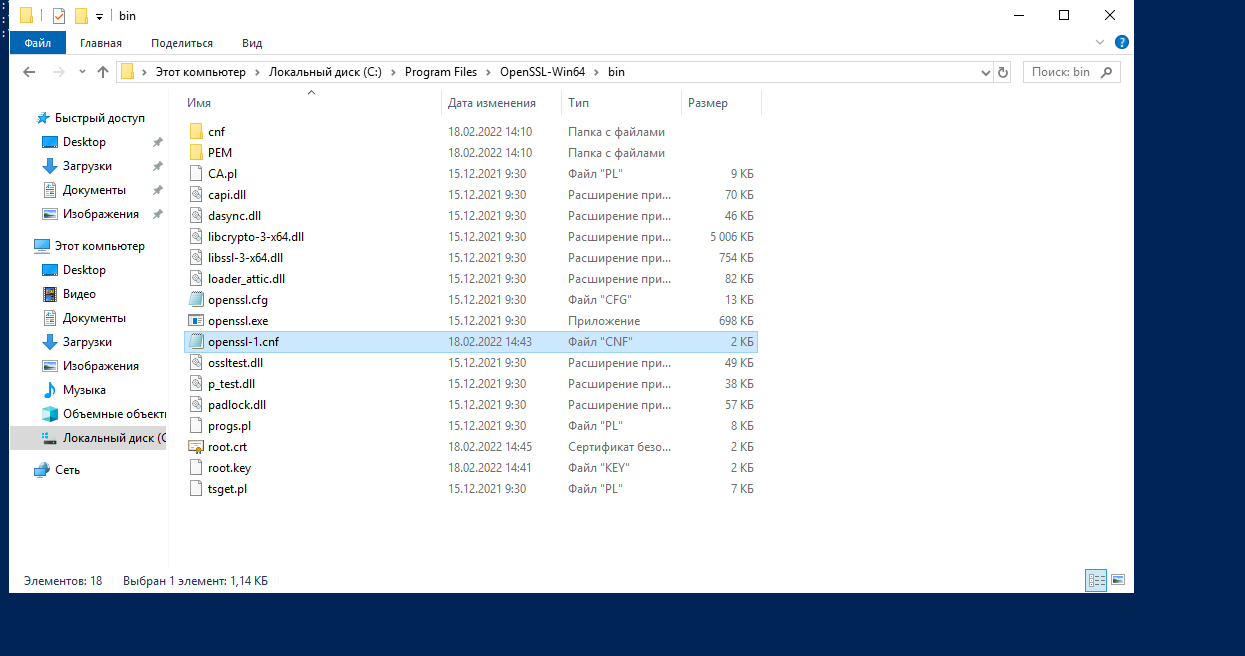




Создаем новый конфиг openssl-1.cnf

.\openssl req -x509 -new -nodes -key root.key -sha256 -days 365 -out root.crt -config openssl-1.cnf -subj "/C=RU/ST=Moskow/L=Moslow/O=demo lab/OU=IT/CN=demo.lab/emailAddress=admin@demo.lab"

Открываем с помощью блокнота

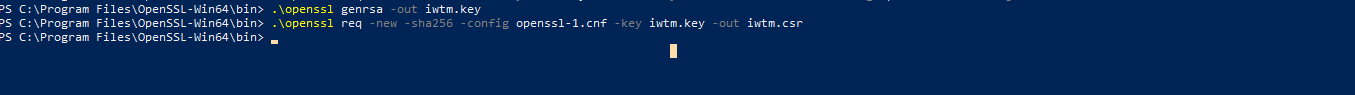


Добавляем промежуточный сервер iwtm

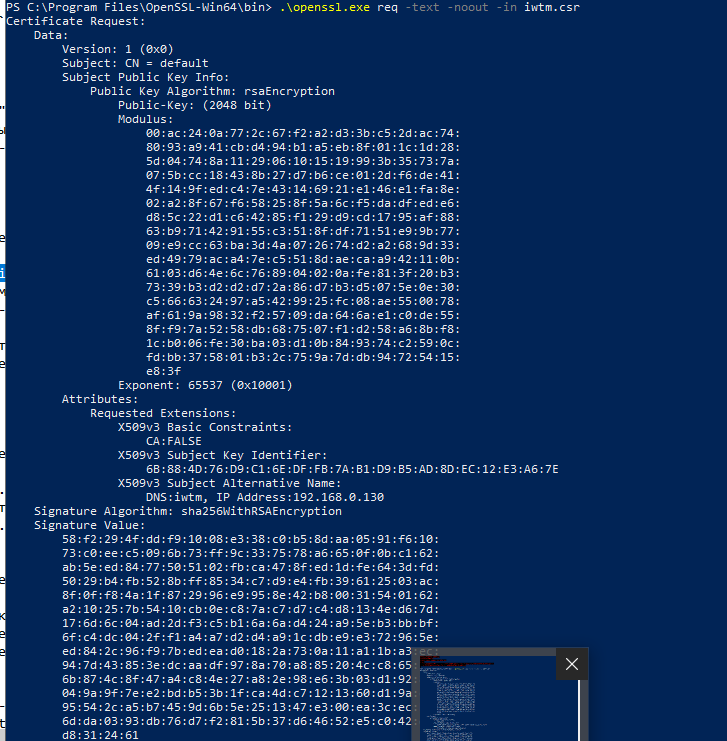
.\openssl.exe genrsa -out iwtm.key

.\openssl.exe req -new -sha256 -config openssl-1.cnf -key iwtm.key -out iwtm.csr

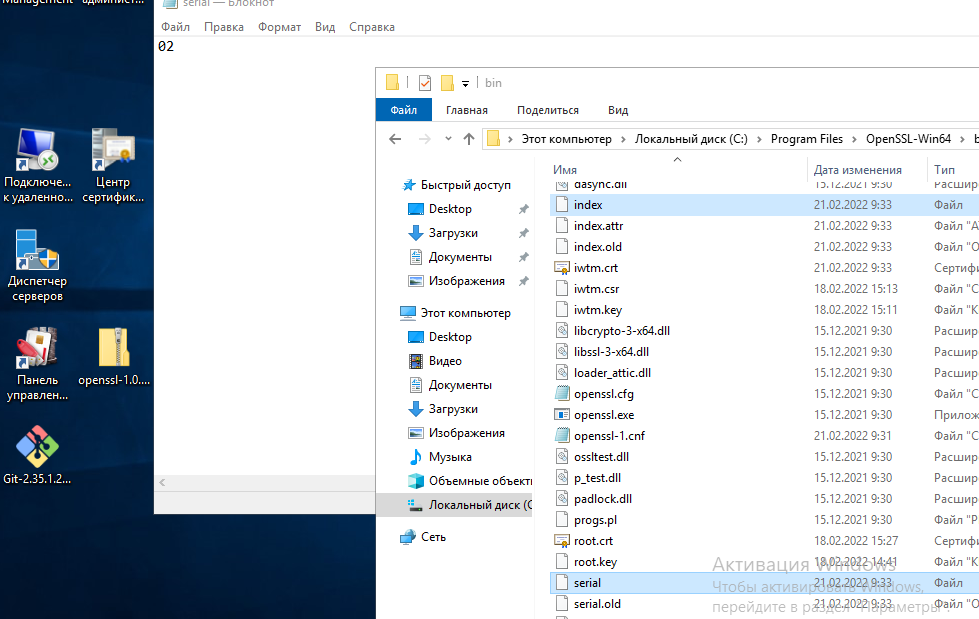
Создание приватного ключа сертификата



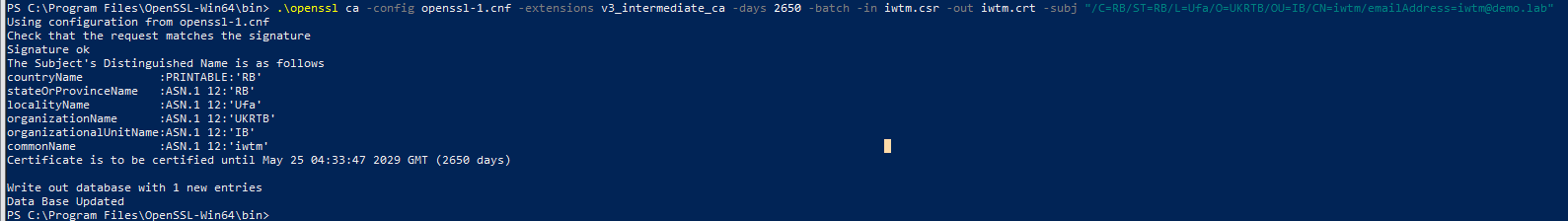
Проверим, что созданный запрос на подпись сертификата (CSR) содержит то, что нам нужно:



Создаем файлы serial с содержимым “02” и пустой файл index без расширений!



Подпись и создание сертификата



**Добавляем пользователя arm**

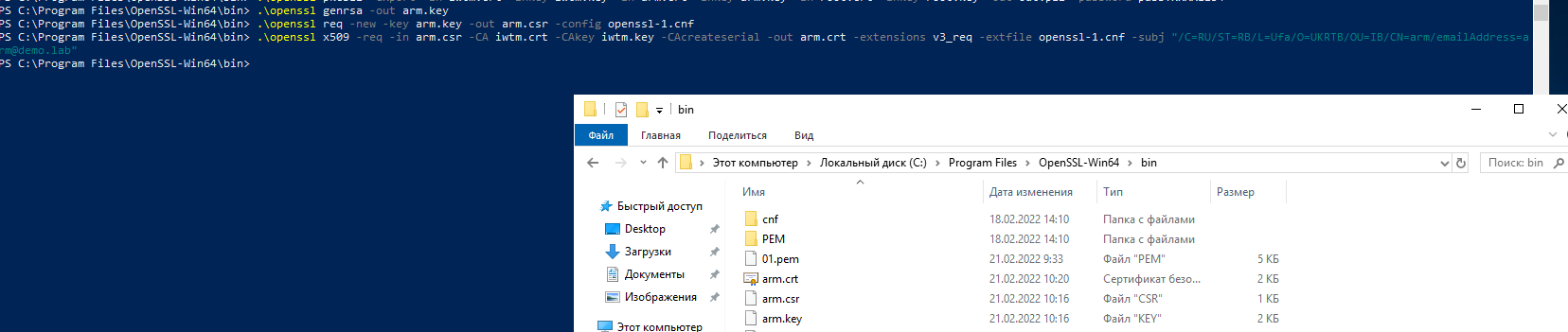
**Создание приватного ключа сертификата**

**Создание запроса на подпись сертификата (CSR)**

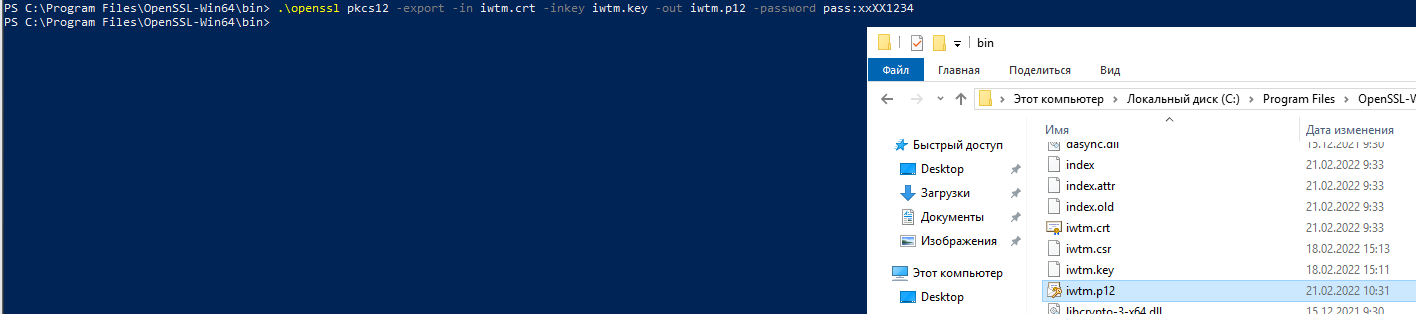
**Подпись и создание сертификата**

**.\openssl x509 -req -in "iwtm.csr" -CA "root.crt" -CAkey "root.key" -CAcreateserial -out "iwtm.crt" -extensions v3\_req -extfile "openssl-1.cnf" -subj "/C=RU/ST=Moskow/L=Moskow/O=demolab/OU=IT/CN=iwtm/emailAddress=iwtm@demo.lab"**

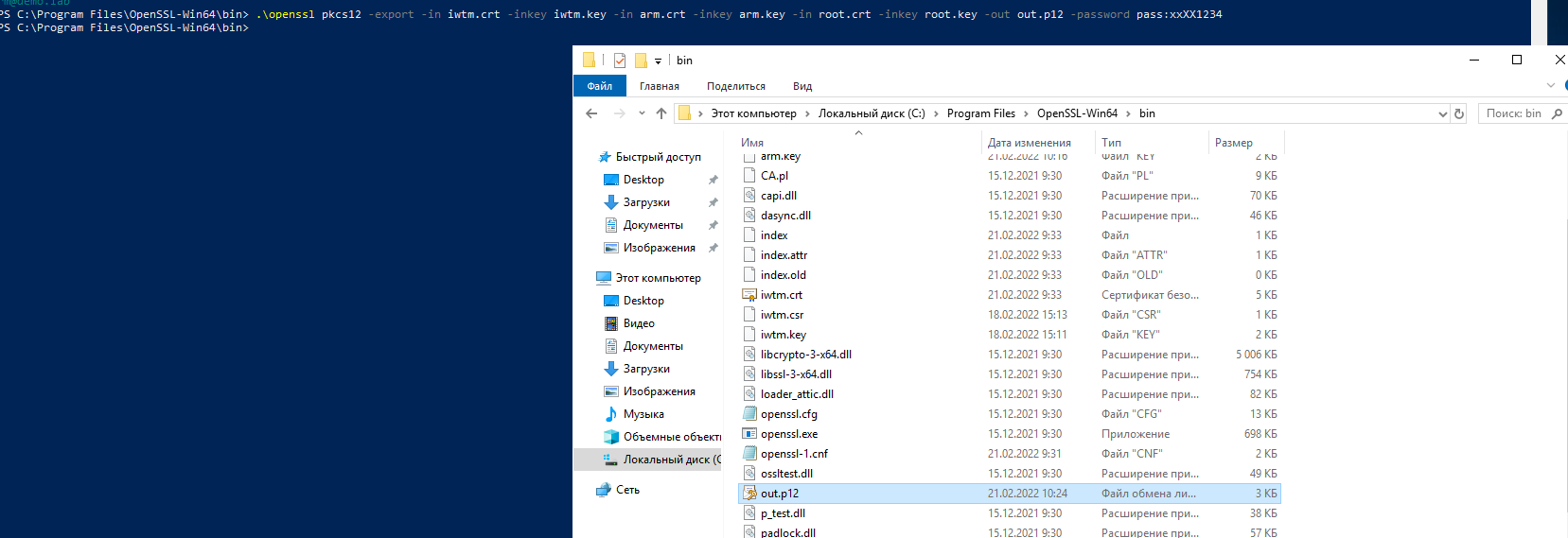
**.\openssl pkcs12 -export -in iwtm.crt -inkey iwtm.key -in root.crt -inkey root.key -out out.p12 -password pass:xxXX1234**



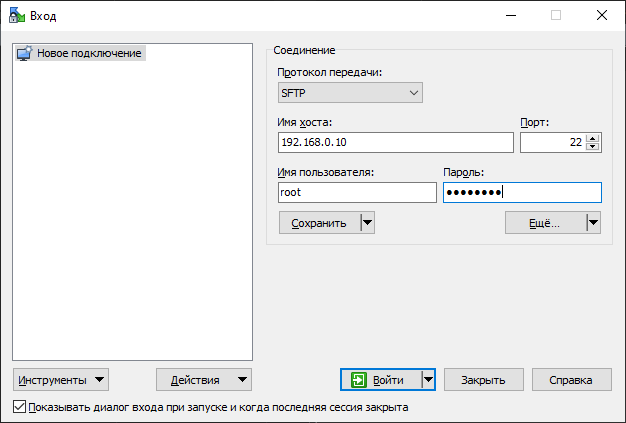
Упаковка ключа и сертификата в файл PKCS12



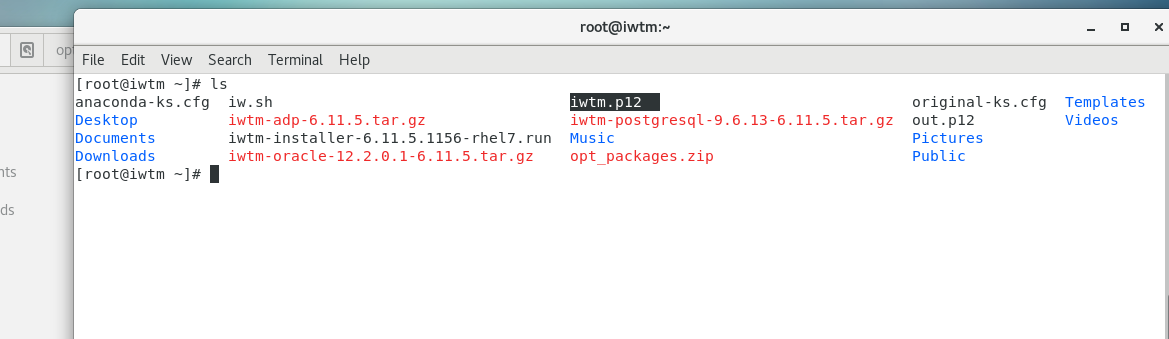
Упаковка всех ключей и сертификатов в out.p12



Подключаемся к ТМ через WinCSP

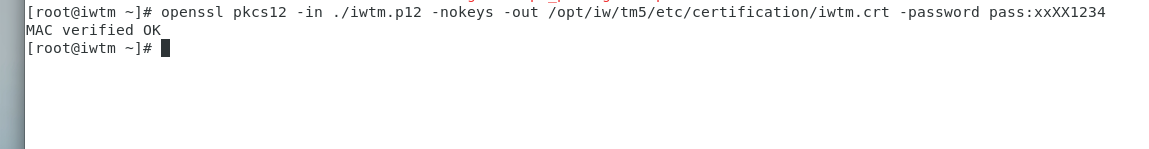


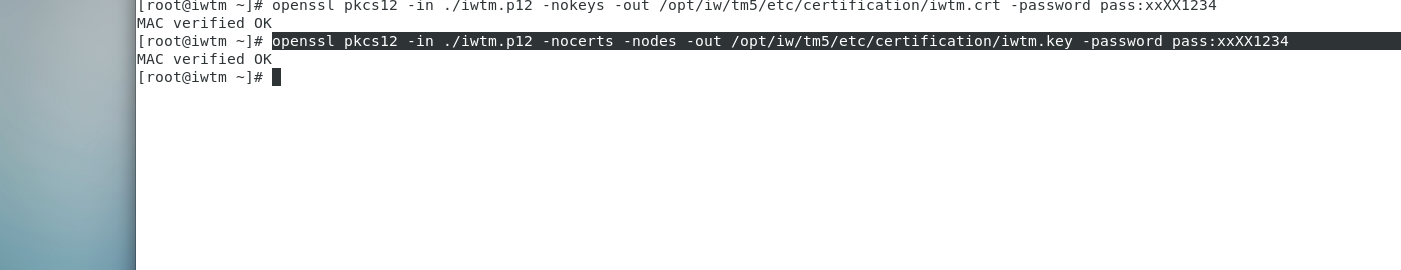
Перекидываем наш сертификат



Извлекаем из сертификата публичный ключ (считаем, что pfx-ключ находится в папке root)

Извлекаем из сертификата закрытый ключ

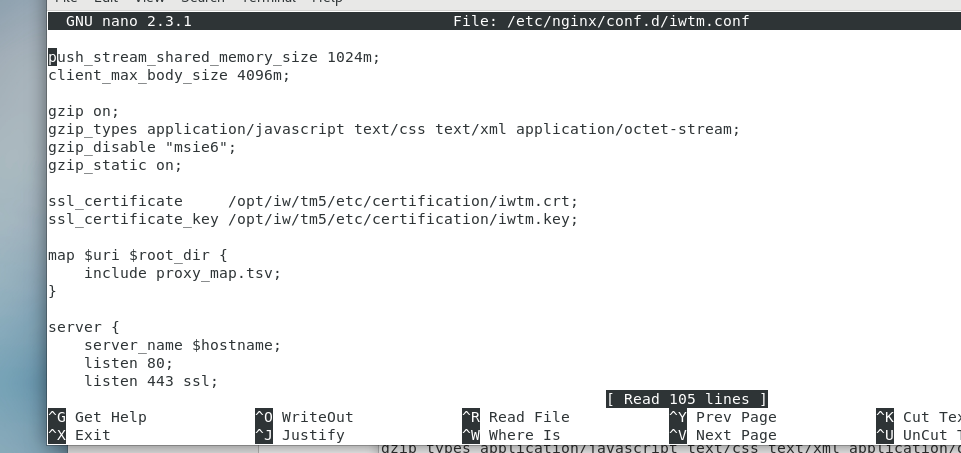




Переносим полученные файлы в папку сертификатов



Изменяем файл конфигурации Nginx /etc/nginx/conf.d/iwtm.conf

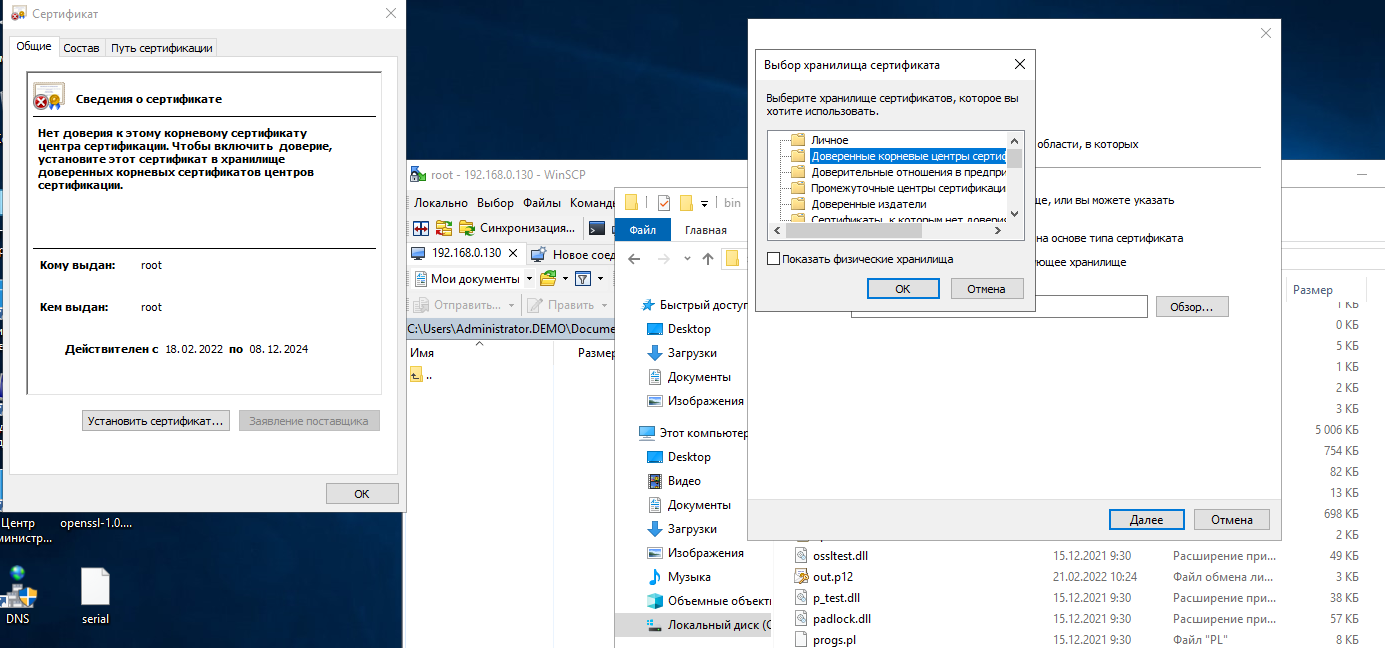


Перезапускаем Nginx

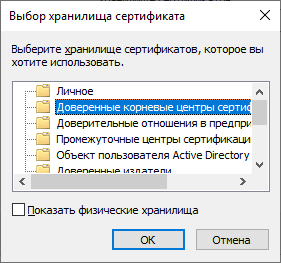


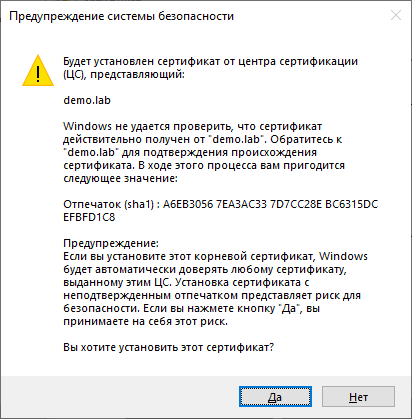
systemctl restart nginx.service

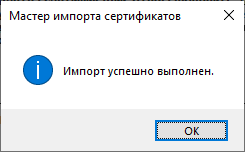
Нажимаем установить сертификат



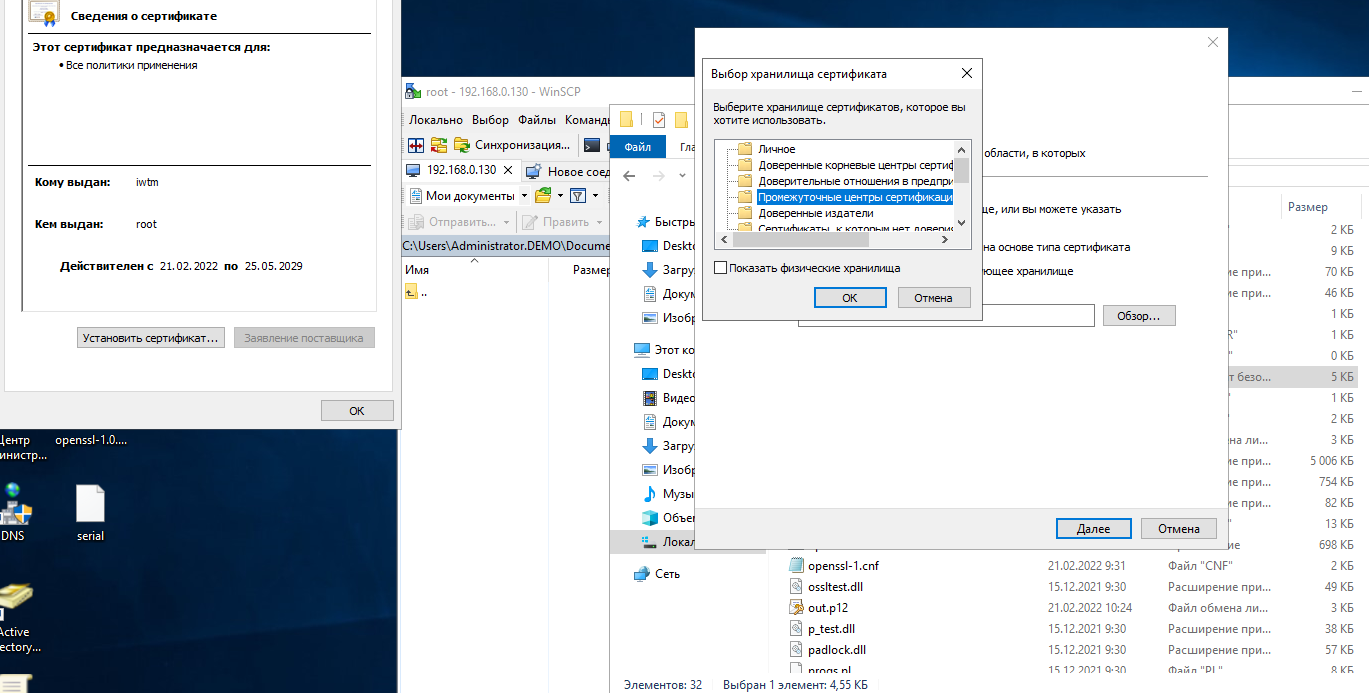
Выбираем Доверенные корневые центры



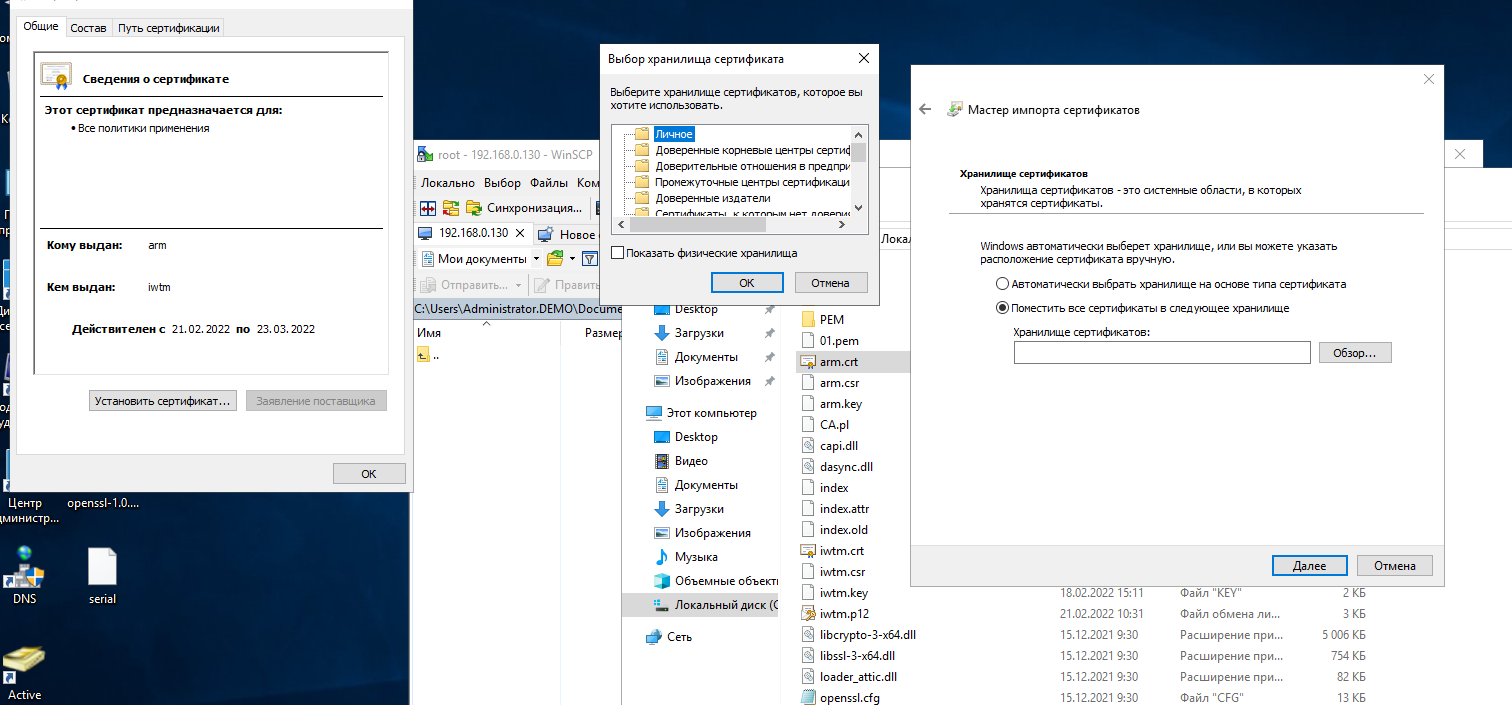


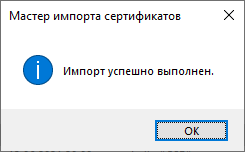


Добавляем сертификат сервера в промежуточные доверенные центры сертификации

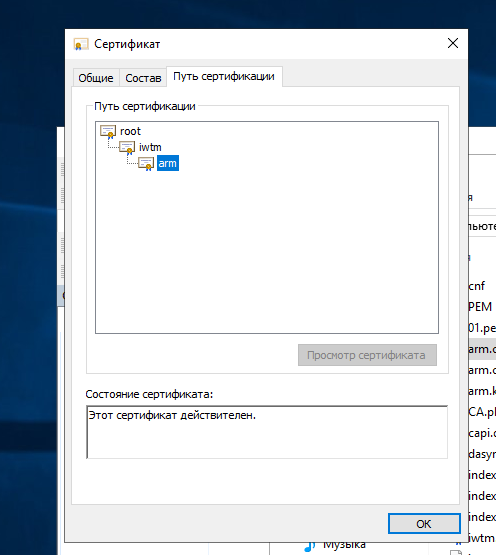


Далее также только в Личное





Видим путь сертификатов



Видим безопасное подключение к ТМ

