Установка OpenSSL сервера на Centos8.

1) Conf both machines with in same network.

2) Make pingable to each other.

------------------------------------------------------------------------------------------

1.Установка первоначальная для Samba на Centos8.

------------------------------------------------------------------------------------------

1.1 sudo yum update -y - Keep the server up to date.

1.2 Sudo yum group install ‘Development Tools’ - We need to install a development tool and few dependencies to install OpenSSL.

1.3 Sudo yum install perl-core zlib-devel -y – Install dependencies.

------------------------------------------------------------------------------------------

2. Download OpenSSL 1.1.1i

------------------------------------------------------------------------------------------

2.1 sudo cd /usr/local/src/ - переходим в директорию.

2.2 sudo wget <https://www.openssl.org/source/openssl-1.1.1i.tar.gz> - и скачиваем файл в нее.

2.3 sudo tar -xzvf openssl-1.1.1i.tar.gz – разархивируем файл.

------------------------------------------------------------------------------------------

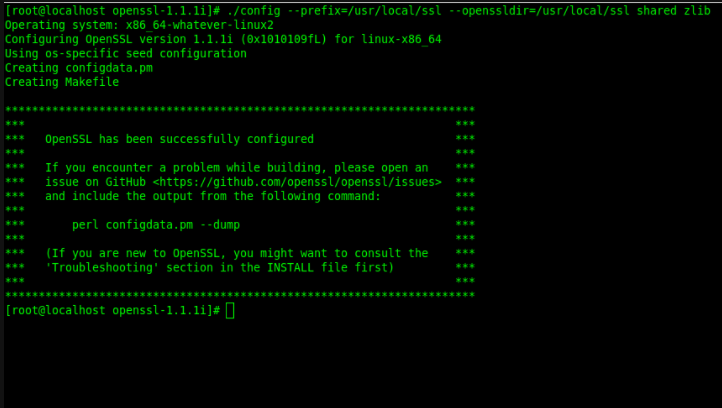
3. Configure and build

------------------------------------------------------------------------------------------

3.1 sudo cd openssl-1.1.1i – переходим в разархивированную папку.

3.2 sudo ./config –prefix=/usr/local/ssl –openssldir=/usr/local/ssl shared zlib – настраиваем путь конфигурационного путя.

Видим это:



3.3 sudo make

sudo make test

sudo make install

прописываем построение.

------------------------------------------------------------------------------------------

4. Configure it shared libraries.

------------------------------------------------------------------------------------------

Once we have successfully installed OpenSSL, configure it shared libraries.

Naviagate to the /etc/ld.so.conf.d directory and create a configuration file.

4.1 sudo cd /etc/ld.so.conf.d/ - переходим в директорию.

4.2 sudo nano openssl-1.1.1i.conf – создаем конфиг файл.

4.3 /usr/local/ssl/lib – добавляем следующий путь в конфиг файле.

Сохраняем.

4.4 sudo ldconfig -v – перезагрузаем линки.

------------------------------------------------------------------------------------------

5. Configure OpenSSL Binary

------------------------------------------------------------------------------------------

Теперь мы собираемся вставить двоичный файл нашей новой версии OpenSSL / usr / local / ssl / bin / openssl и заменить файл openssl по умолчанию.

5.1 sudo mv /bin/openssl /bin/openssl.backup – создадим backup файлов.Щзут

5.2 sudo nano /etc/profile.d/openssl.sh – создаем новый файл для OpenSSL.

5.3 И прописываем внутри «openssl.sh» следующее:

OPENSSL\_PATH=”/usr/local/ssl/bin”  
export OPENSSL\_PATH  
PATH=$PATH:$OPENSSL\_PATH  
export PATH

5.4 sudo chmod +x /etc/profile.d/openssl.sh – делаем его исполняемым.

5.5 sudo systemctl reload OpenSSL – перезагружаем OpenSSL.

5.6 sudo source /etc/profile.d/openssl.sh

5.7 sudo echo $PATH

------------------------------------------------------------------------------------------

6. Give SSL ticket with self-written without Center Certification.

------------------------------------------------------------------------------------------

6.1 sudo openssl genrsa 1024 > example.demo.key – генерируем ключ с ключ 1024 бит и сохраняем его в файл «example.demo.key». Это закрытый ключ.

6.2 sudo openssl req -new -key ./ example.demo.key > example.demo.csr – запрос на подпись сертефиката с ключом созданным до этого и сохранением в файл example.demo.csr.

6.3 После этого будет интерактивная настройка с заданными вопросами:

6.3.1 Country name:

6.3.2 State of Province name:

6.3.3 Locality name (city) :

6.3.4 Organization name:

6.3.5 Organizational Unit:

6.3.6 Hostname: «самый важный тут нужно указать кому будет выдан «example.com»»

6.3.7 E-mail:

6.4 sudo openssl x509 -in example.demo.csr -out example.demo.crt -req -signkey example.demo.key -days 365 – получение сертификата от нашего запроса и с нашим закрытым ключом.

------------------------------------------------------------------------------------------

7. Give SSL ticket with Center Certification on Windows.

------------------------------------------------------------------------------------------

7.1 Должен быть настроен сервер сертификации на Windows.

7.2 Заходя на сайт сертификации через веб-браузер выбираем «request cert»

7.3 Выбираем advanced cert req.

7.4 Открываем «example.demo.csr» и копируем запрос в поле ввода на сайте.

7.5 Выбираем тип шаблона для кого он будет сертификат.

7.6 И после всего мы можем сказать наш сертификат в разных форматах.