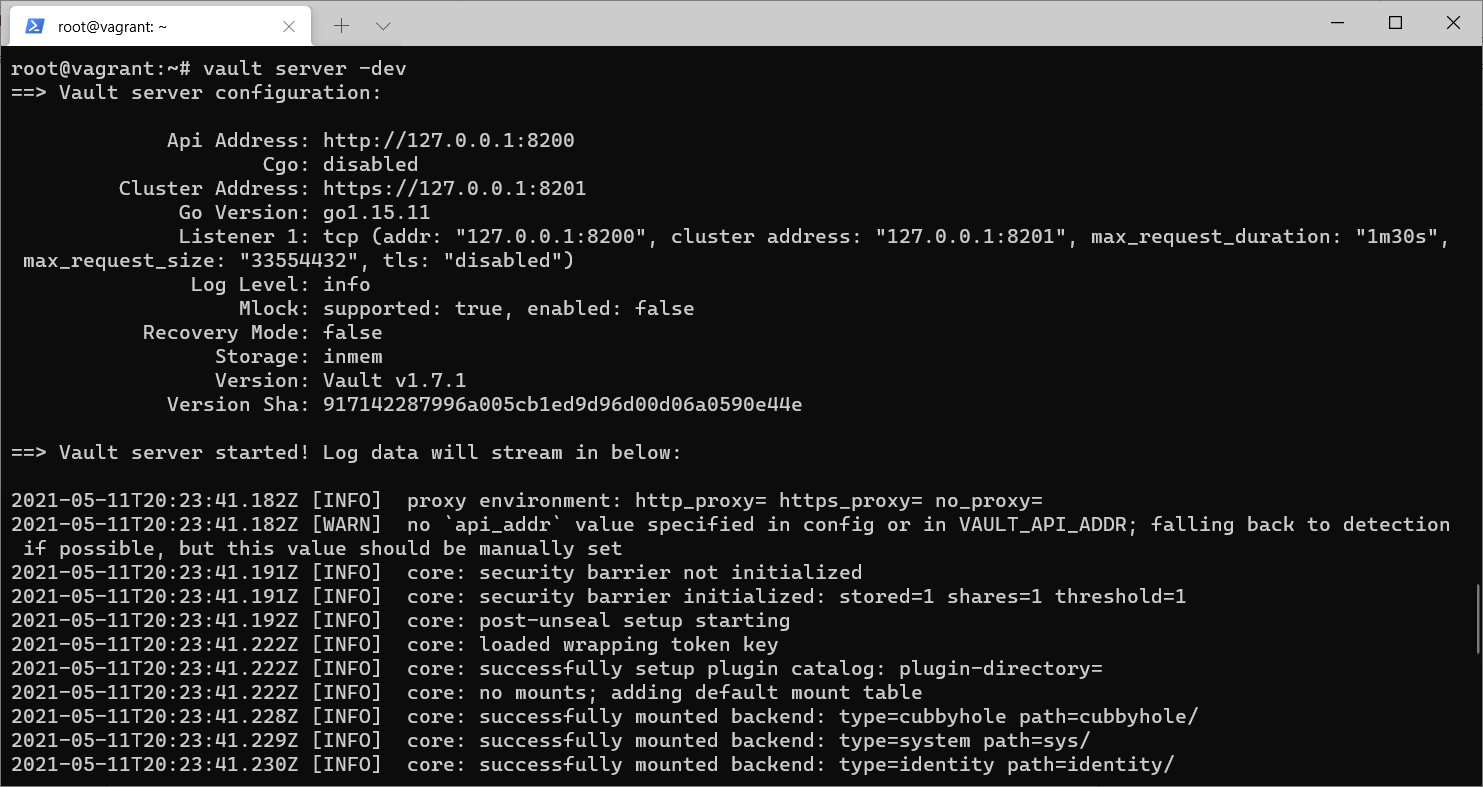
2. Выполнена установка Vault. Запущен vault server

*vault server –dev*

**

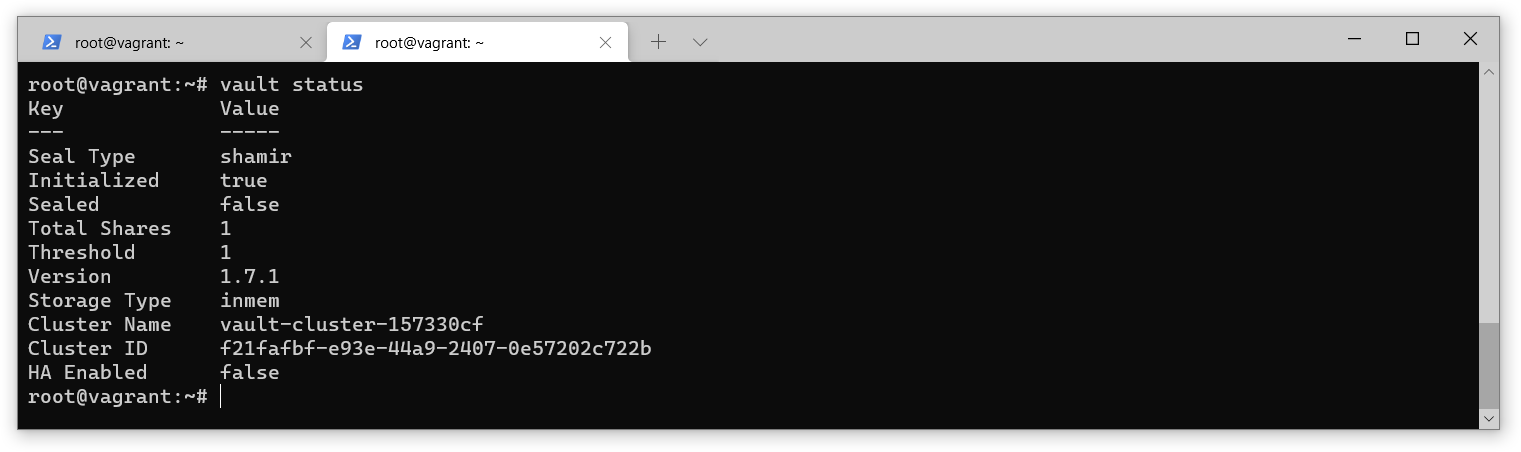
Unseal Key: e4CaQnuyrW3mlYEZrbk3Rx3QuD6v6Z0liFAKBMH3XPo=

Root Token: s.FknQhtRHY3RUBOEf2vEvr7fp

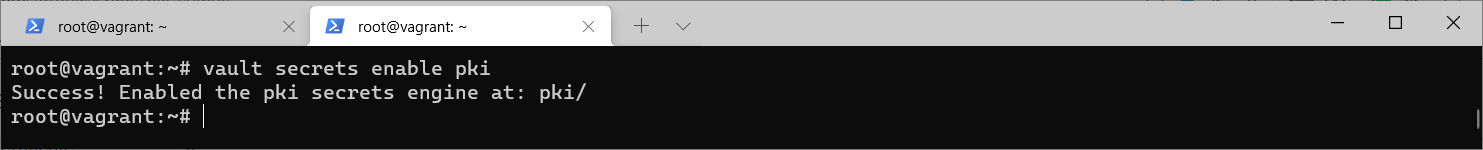
Добавлены 2 переменные окружения.



Выполнена проверка состояния сервера vault status. Сервер работает.

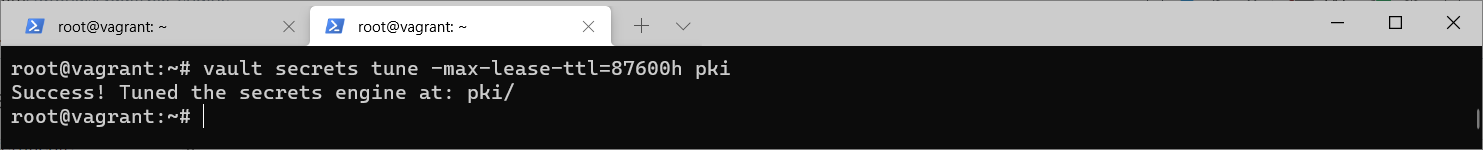


3. Выполнено включение механизма секретов pki на пути pki*vault secrets enable pki*



Выполнена настройка механизма секретов pki для выдачи сертификатов с максимальным временем жизни (TTL) 87600 часов

*vault secrets tune -max-lease-ttl=87600h pki*



Создан корневой сертификат и сохранен в файл.

vault write -field=certificate pki/root/generate/internal \

common\_name="example.com" \

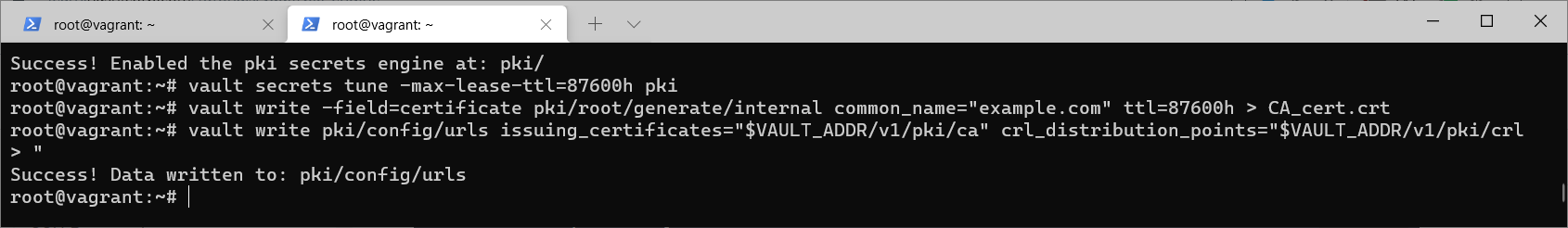
ttl=87600h > CA\_cert.crt

Выполнена настройка URL-адреса CA и CRL

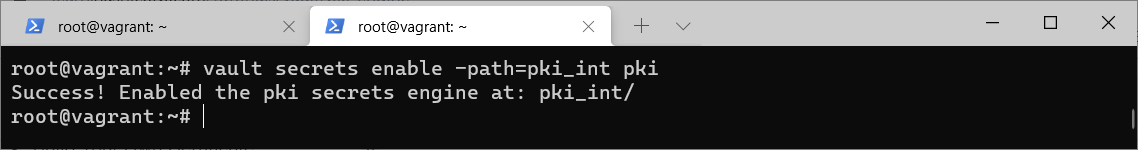
*vault write pki/config/urls \*

*issuing\_certificates="$VAULT\_ADDR/v1/pki/ca" \*

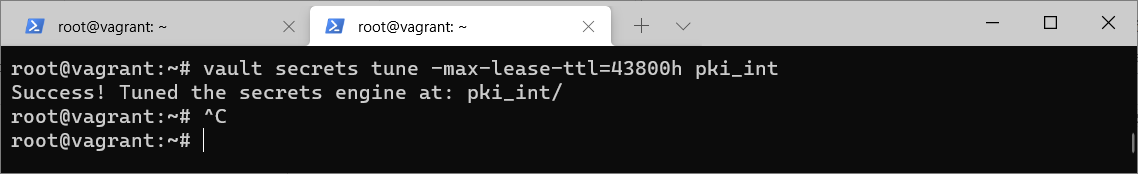
*crl\_distribution\_points="$VAULT\_ADDR/v1/pki/crl"*



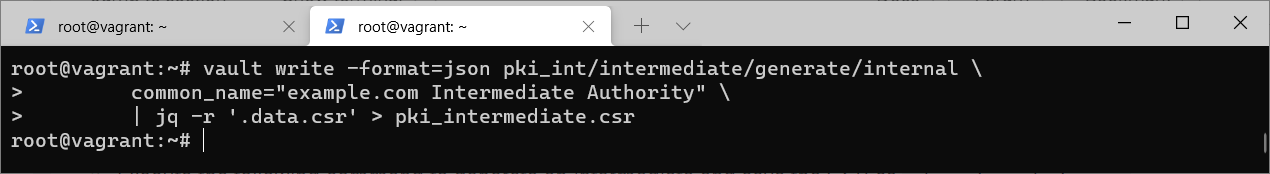
Выполнено включите механизм секретов pki по пути pki\_int



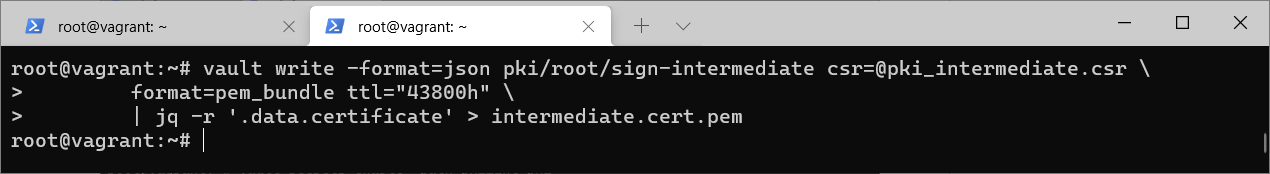
Выполнена настройка механизма секретов pki\_int для выдачи сертификатов с максимальным временем жизни (TTL) 43800 часов.



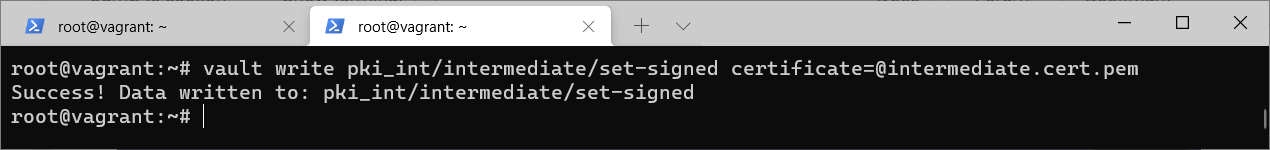
Выполнена следующая команда, чтобы сгенерировать промежуточное звено и сохранить CSR как pki\_intermediate.csr



Промежуточный сертификат подписан закрытым ключом корневого ЦС и сохранен сгенерированный сертификат как intermediate.cert.pem



Подписанный сертификат импортирован обратно в Vault.



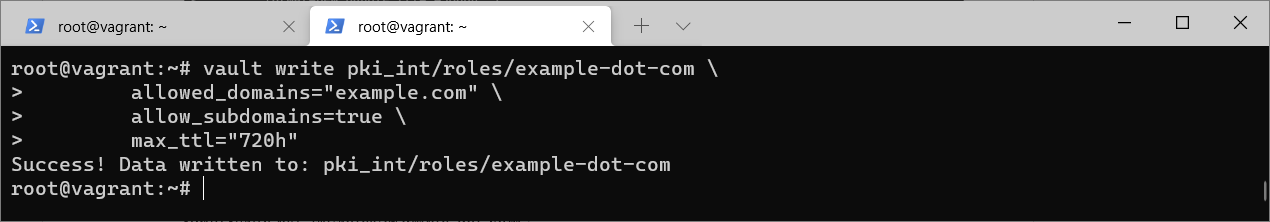
4. Выполнено создание роли с именем example-dot-com, которая разрешает поддомены.

*vault write pki\_int/roles/example-dot-com \*

*allowed\_domains="example.com" \*

*allow\_subdomains=true \*

*max\_ttl="720h"*



Выполнен запрос на новый сертификат для домена netology.example.com на основе роли example-dot-com.

*vault write pki\_int/issue/example-dot-com common\_name="netology.example.com" ttl="240h"*

Из полученного вывода были созданы файлы netology.pem, netology.key.

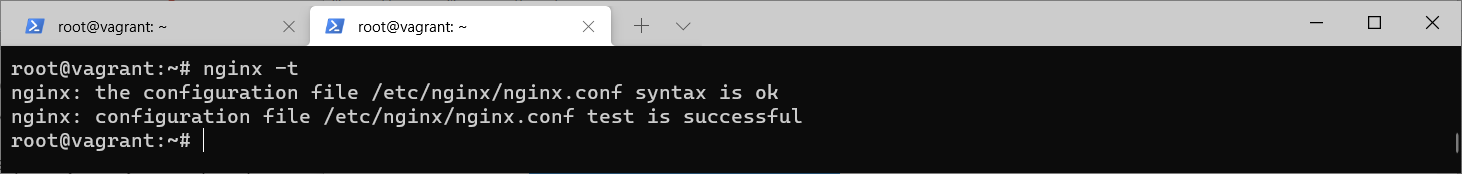
5. Установлен nginx. В /etc/nginx/sites-enabled/default добавлены строки

*listen 443 ssl default\_server;*

*listen [::]:443 ssl default\_server;*

*ssl\_certificate /root/netology.pem;*

*ssl\_certificate\_key /root/netology.key;*



Выполнен перезапуск nginx

*systemctl reload nginx*

6. Созданный ранее свой корневой CA сертификат CA\_cert.crt был добавлен в список доверенных следующими командами:

*sudo cp CA\_cert.crt /usr/local/share/ca-certificate*

*sudo update-ca-certificates*

Модифицировав /etc/hosts командой

*echo 127.0.0.1 example.com >> /etc/hosts*

добились безошибочной с точки зрения HTTPS работы curl на наш тестовый домен

