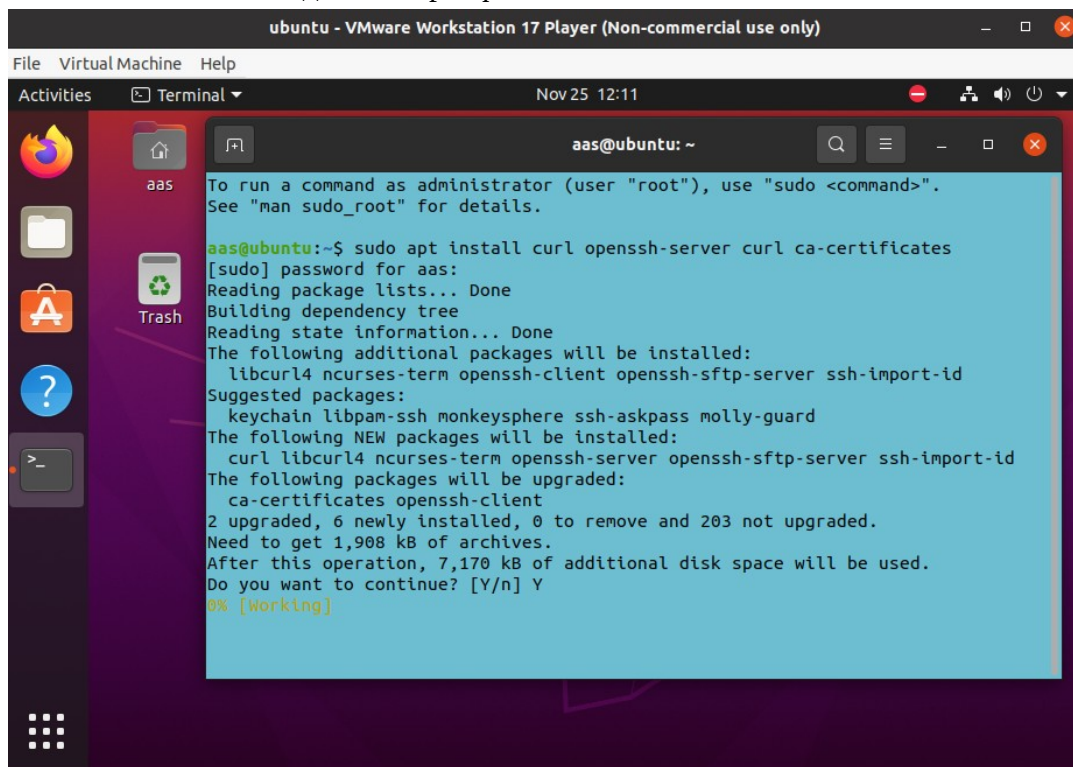


ОСНОВЫ ТЕХНОЛОГИИ VPN

2. Установка и настройка системы контроля версий GitLab

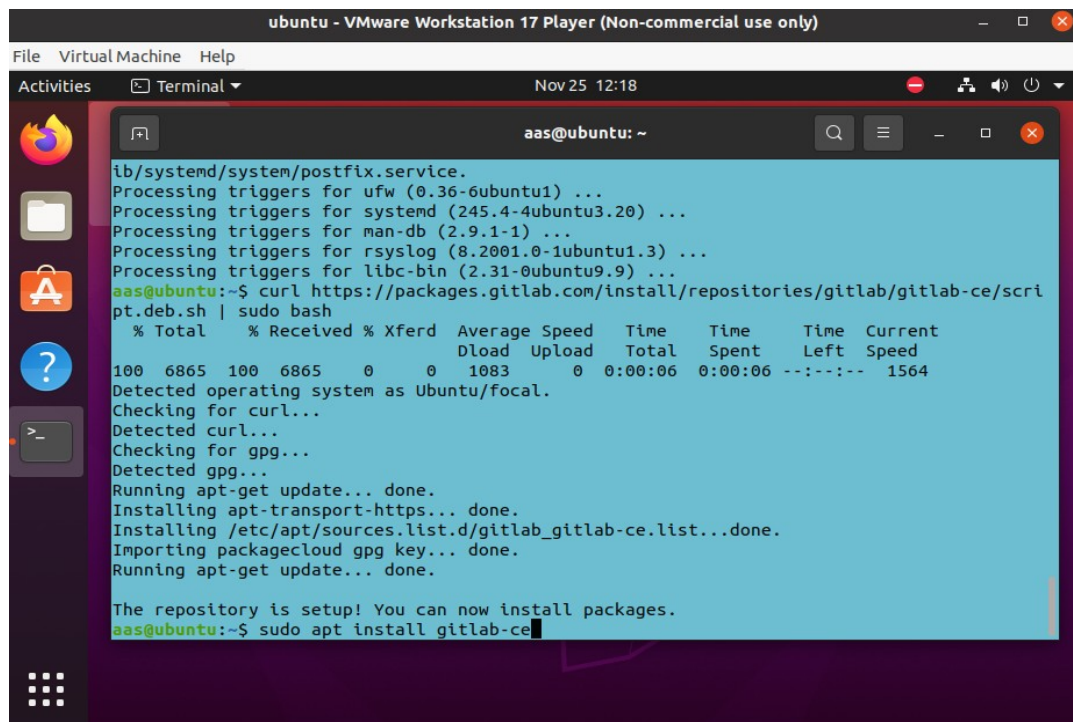
Устанавливаем необходимые сертификаты



```
ubuntu - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Nov 25 12:11
aas@ubuntu: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

aas@ubuntu:~$ sudo apt install curl openssl-server curl ca-certificates
[sudo] password for aas:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcurl4 ncurses-term openssl-client openssl-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  curl libcurl4 ncurses-term openssl-server openssl-sftp-server ssh-import-id
The following packages will be upgraded:
  ca-certificates openssl-client
2 upgraded, 6 newly installed, 0 to remove and 203 not upgraded.
Need to get 1,908 kB of archives.
After this operation, 7,170 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
0% [Working]
```

Выполняем установку репозитория GitLab:

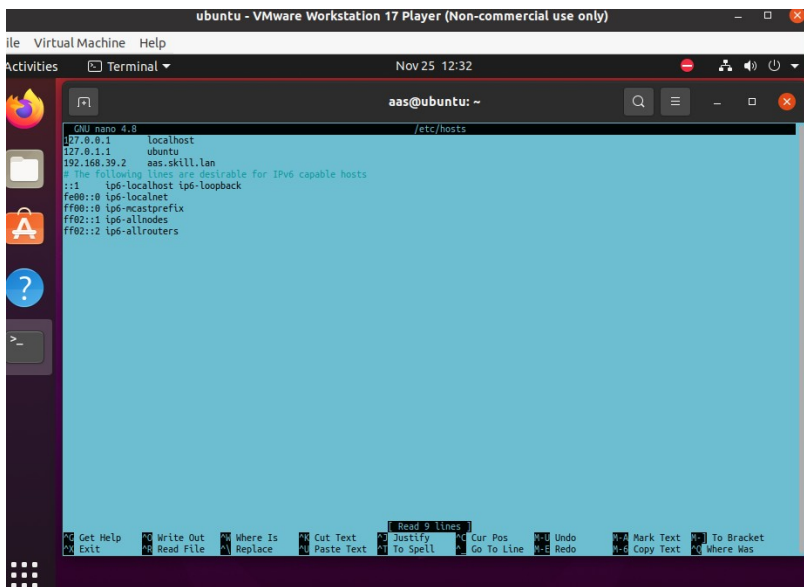


```
ubuntu - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Nov 25 12:18
aas@ubuntu: ~
ib/systemd/system/postfix.service.
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for systemd (245.4-4ubuntu3.20) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for rsyslog (8.2001.0-1ubuntu1.3) ...
Processing triggers for libc-bin (2.31-0ubuntu9.9) ...
aas@ubuntu:~$ curl https://packages.gitlab.com/install/repositories/gitlab/gitlab-ce/scr
pt.deb.sh | sudo bash
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 6865 100 6865 0 0 1083 0 0:00:06 0:00:06 --:--:-- 1564
Detected operating system as Ubuntu/focal.
Checking for curl...
Detected curl...
Checking for gpg...
Detected gpg...
Running apt-get update... done.
Installing apt-transport-https... done.
Installing /etc/apt/sources.list.d/gitlab_gitlab-ce.list...done.
Importing packagecloud gpg key... done.
Running apt-get update... done.

The repository is setup! You can now install packages.
aas@ubuntu:~$ sudo apt install gitlab-ce
```

Настройка GitLab.

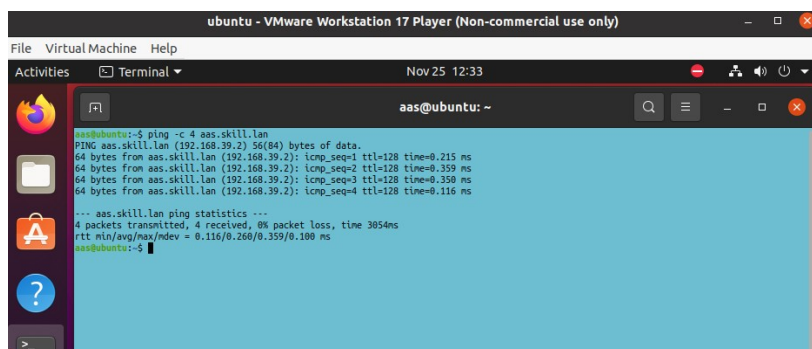
В файле hosts добавляем локальный DNS для переключателя сервисов имён в Linux и проверяем его доступность



```
ubuntu - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Nov 25 12:32
aas@ubuntu: ~
GNU nano 4.8 /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu
192.168.39.2 aas.skill.lan
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

aas@ubuntu:~$ ping -c 4 aas.skill.lan
PING aas.skill.lan (192.168.39.2): 56(84) bytes of data:
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=1 ttl=128 time=0.215 ms
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=2 ttl=128 time=0.359 ms
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=3 ttl=128 time=0.359 ms
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=4 ttl=128 time=0.116 ms

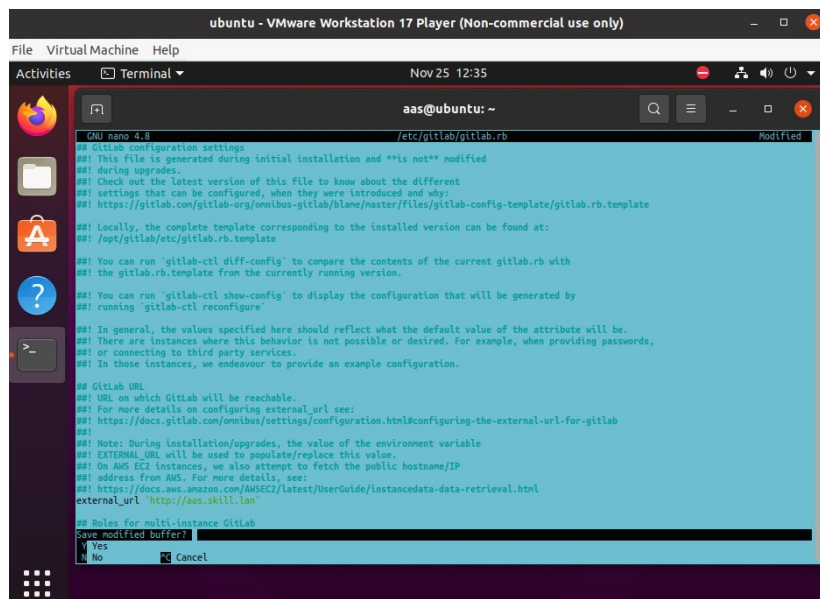
--- aas.skill.lan ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/ndev = 0.116/0.268/0.359/0.108 ms
aas@ubuntu:~$
```



```
ubuntu - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Nov 25 12:33
aas@ubuntu: ~
aas@ubuntu:~$ ping -c 4 aas.skill.lan
PING aas.skill.lan (192.168.39.2): 56(84) bytes of data:
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=1 ttl=128 time=0.215 ms
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=2 ttl=128 time=0.359 ms
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=3 ttl=128 time=0.359 ms
64 bytes from aas.skill.lan (192.168.39.2): icmp_seq=4 ttl=128 time=0.116 ms

--- aas.skill.lan ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/ndev = 0.116/0.268/0.359/0.108 ms
aas@ubuntu:~$
```

Устанавливаем external url:

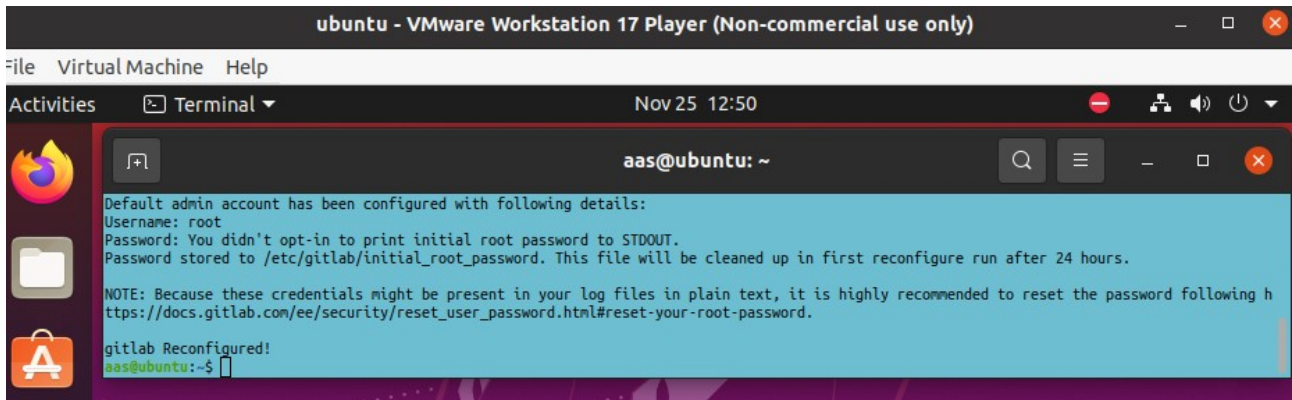


```
ubuntu - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Nov 25 12:35
aas@ubuntu: ~
GNU nano 4.8 /etc/gitlab/gitlab.rb
# GitLab configuration settings
##! This file is generated during initial installation and **is not** modified
##! during upgrades.
##! Check out the latest version of this file to know about the different
##! settings that can be configured, when they were introduced and why:
##! https://gitlab.com/gitlab-org/omnibus-gitlab/blame/master/files/gitlab-config-template/gitlab.rb.template
##! Locally, the complete template corresponding to the installed version can be found at:
##! /opt/gitlab/etc/gitlab.rb.template
##! You can run 'gitlab-ctl diff-config' to compare the contents of the current gitlab.rb with
##! the gitlab.rb.template from the currently running version.
##! You can run 'gitlab-ctl show-config' to display the configuration that will be generated by
##! running 'gitlab-ctl reconfigure'
##! In general, the values specified here should reflect what the default value of the attribute will be.
##! There are instances where this behavior is not possible or desired. For example, when providing passwords,
##! or connecting to third party services.
##! In those instances, we endeavour to provide an example configuration.

## GitLab URL
##! URL on which GitLab will be reachable.
##! For more details on configuring external_url see:
##! https://docs.gitlab.com/omnibus/settings/configuration.html#configuring-the-external-url-for-gitlab
##!
##! Note: During installation/upgrades, the value of the environment variable
##! EXTERNAL_URL will be used to populate/replace this value.
##! On AWS EC2 instances, we also attempt to fetch the public hostname/IP
##! address from AWS. For more details, see:
##! https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html
external_url 'http://aas.skill.lan'

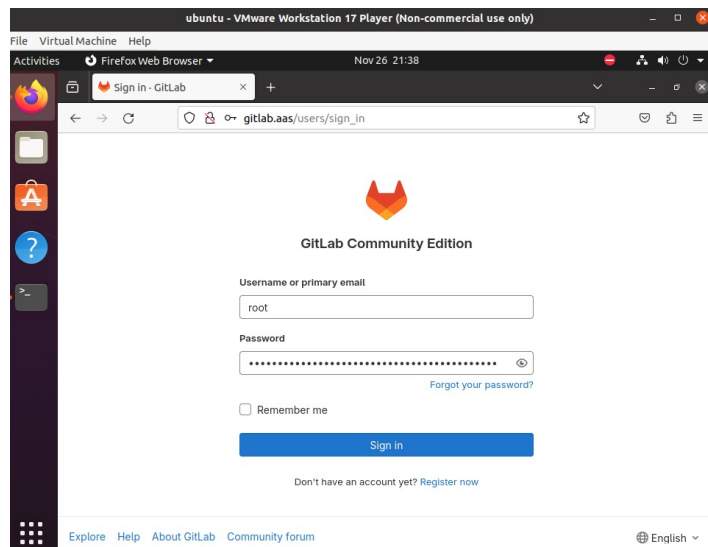
##! Endless for multi-instance GitLab
Save modified buffer
^Y Yes
^N No
^C Cancel
```

Запускаем конфигурирование ***gitlab-ctl reconfigure***

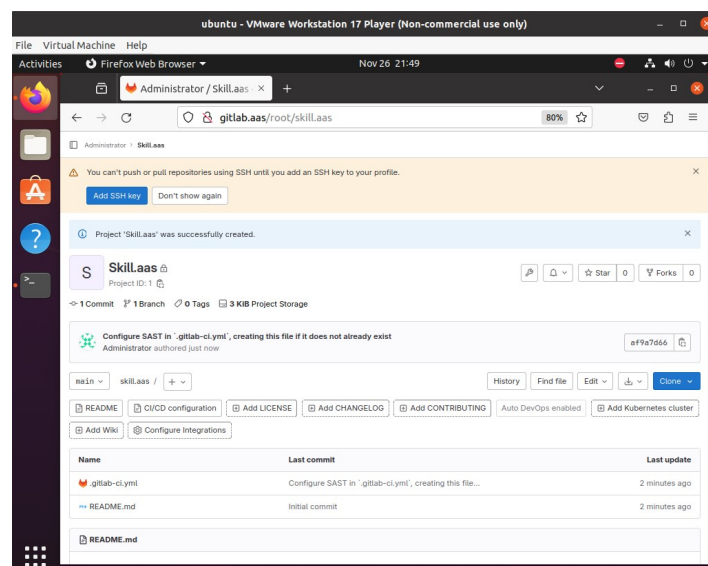


В браузере вводим адрес, который мы указали в настройках в опции `external_url`

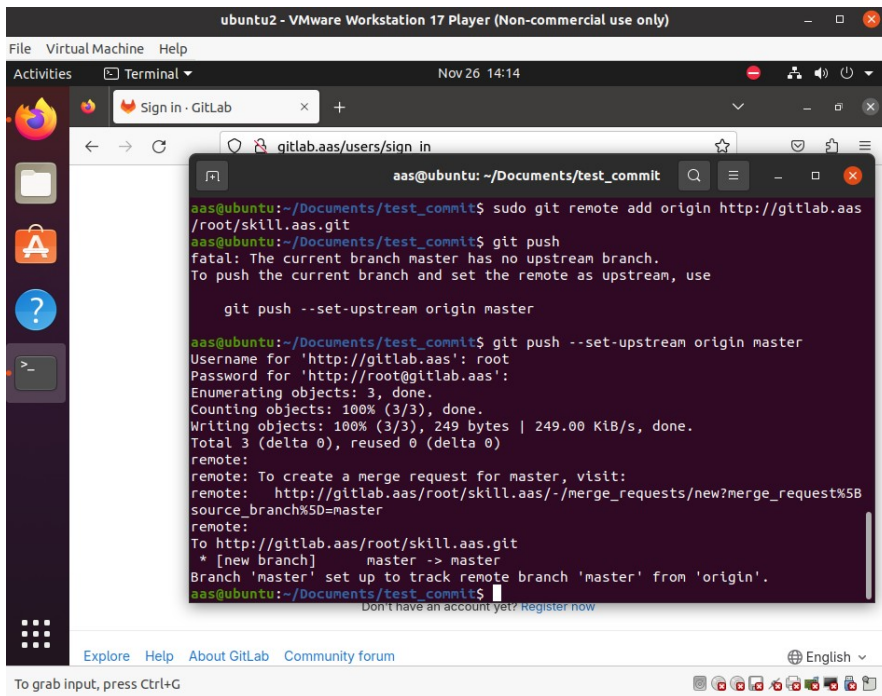
Вводим пароль, который был назначен пользователю после установки можно в файле `/etc/gitlab/initial_root_password`:



Авторизация пройдена, создаем новый проект в интерфейсе GitLab.



Чтобы протестировать на второй машине создаем тестовый коммит с файлом:

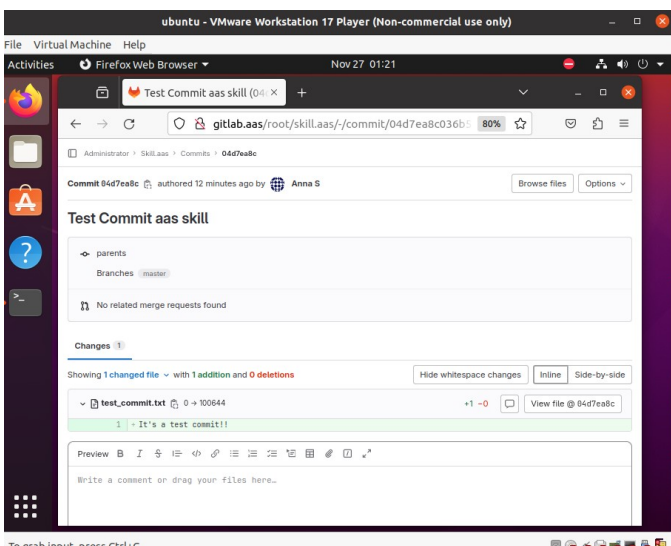
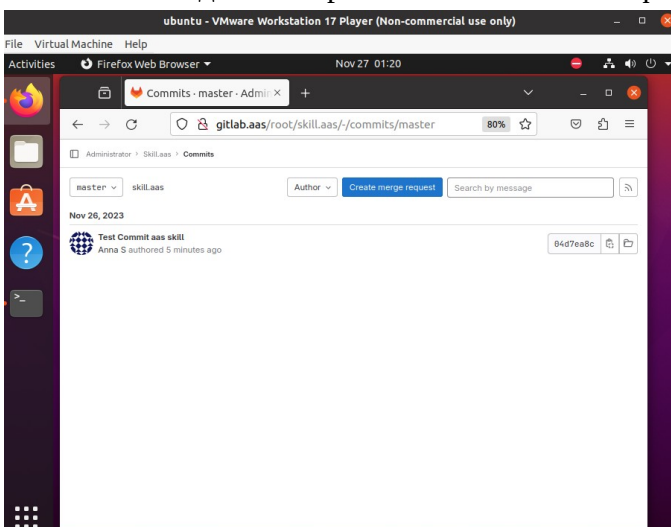


```
ubuntu2 - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Activities Terminal Nov 26 14:14
Sign in - GitLab
gitlab.aas/users/sign in
aas@ubuntu: ~/Documents/test_commit
aas@ubuntu:~/Documents/test_commit$ sudo git remote add origin http://gitlab.aas
/root/skill.aas.git
aas@ubuntu:~/Documents/test_commit$ git push
fatal: The current branch master has no upstream branch.
To push the current branch and set the remote as upstream, use

    git push --set-upstream origin master

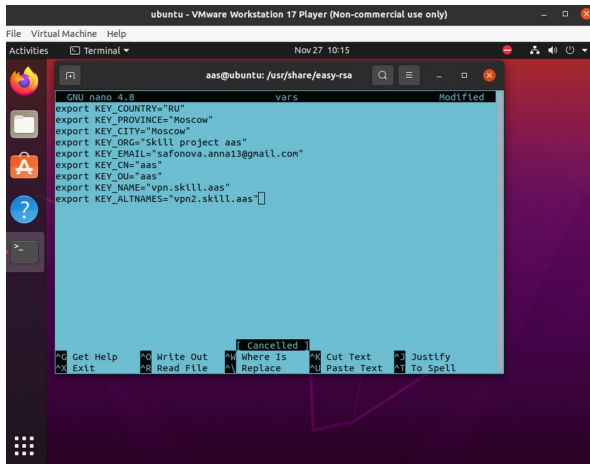
aas@ubuntu:~/Documents/test_commit$ git push --set-upstream origin master
Username for 'http://gitlab.aas': root
Password for 'http://root@gitlab.aas':
Enumerating objects: 3, done.
Counting objects: 100% (3/3), done.
Writing objects: 100% (3/3), 249 bytes | 249.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0)
remote:
remote: To create a merge request for master, visit:
remote:   http://gitlab.aas/root/skill.aas/-/merge_requests/new?merge_request%5B
source_branch%5D=master
remote:
To http://gitlab.aas/root/skill.aas.git
 * [new branch]      master -> master
Branch 'master' set up to track remote branch 'master' from 'origin'.
aas@ubuntu:~/Documents/test_commit$
```

Заливаем в созданный проект закоммиченный файл и проверяем его наличие в репозитории:



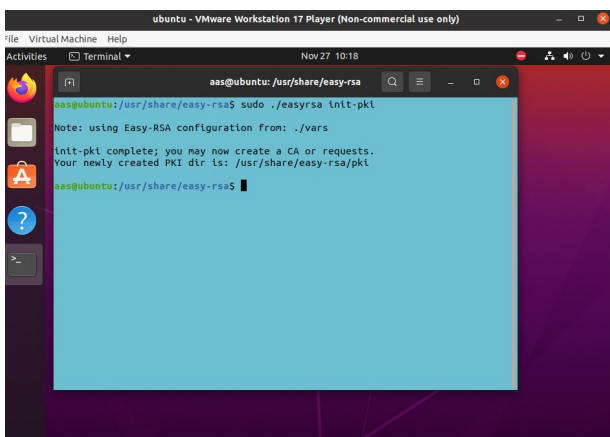
3. Установите и настройте комплексный межсетевой экран с сервером VPN на виртуальной машине посредством VirtualBox, VMware Workstation или других средств виртуализации, обеспечивающих возможность безопасного подключения пользователей из различных филиалов.

1. Устанавливаем OpenVPN-сервер совместно с утилитой по созданию сертификатов Easy-RSA, создаем файл с настройками



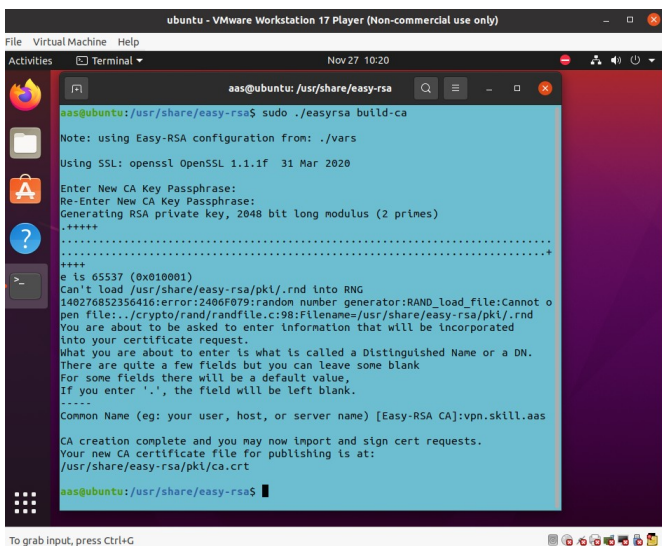
```
GNU nano 4.8 Modified
export KEY_COUNTRY="RU"
export KEY_PROVINCE="Moscow"
export KEY_CITY="Moscow"
export KEY_ORG="skill project aas"
export KEY_EMAIL="safonova.anna13@gmail.com"
export KEY_CN="aas"
export KEY_OU="aas"
export KEY_NAME="vpn.skill.aas"
export KEY_ALIASES="vpn2.skill.aas"
```

Инициализируем PKI:



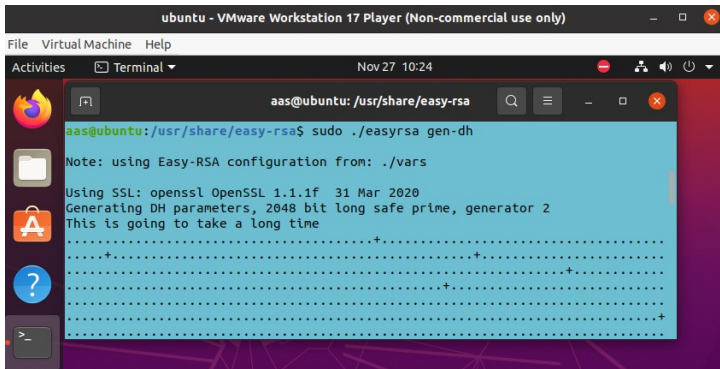
```
aas@ubuntu: /usr/share/easy-rsa$ sudo ./easyrsa init-pki
Note: using Easy-RSA configuration from: ./vars
init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /usr/share/easy-rsa/pki
aas@ubuntu: /usr/share/easy-rsa$
```

Создание корневого сертификата:

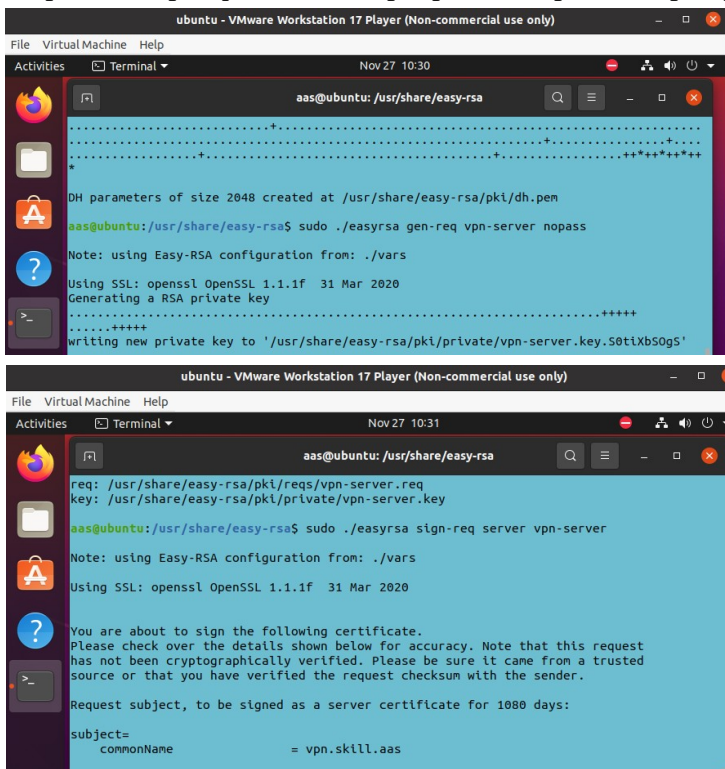


```
aas@ubuntu: /usr/share/easy-rsa$ sudo ./easyrsa build-ca
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+
++++
e is 65537 (0x010001)
Can't load /usr/share/easy-rsa/pki/.rnd into RNG
140276852356416:error:2406F079:random number generator:RAND_load_file:Cannot o
pen file:./crypto/rand/randfile.c:98:Filename=/usr/share/easy-rsa/pki/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
if you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:vpn.skill.aas
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/usr/share/easy-rsa/pki/ca.crt
aas@ubuntu: /usr/share/easy-rsa$
```

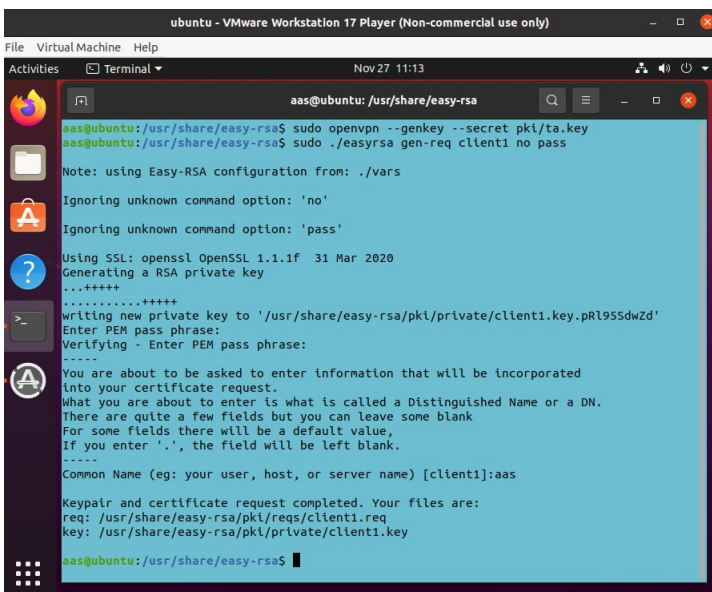
Формируем ключ Диффи-Хеллмана:



Запрос на сертификат для сервера и генерация сертификата:



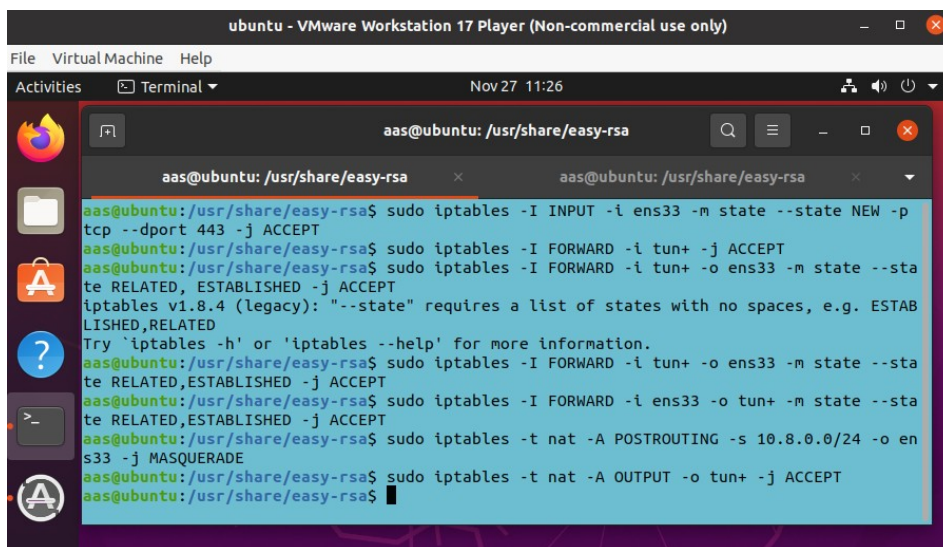
Создаем та ключ и сертификат клиента



Из каталога `pk` на компьютер клиента нужно скопировать файлы:

- `ca.crt`
- `issued/client1.crt`
- `private/client1.key`
- `dh.pem`
- При использовании `tls`, также копируем `ta.key`.

Правила `iptables` на сервере:



```
ubuntu - VMware Workstation 17 Player (Non-commercial use only)
File Virtual Machine Help
Activities Terminal Nov 27 11:26
aas@ubuntu: /usr/share/easy-rsa
aas@ubuntu: /usr/share/easy-rsa
aas@ubuntu: /usr/share/easy-rsa$ sudo iptables -I INPUT -i ens33 -m state --state NEW -p
tcp --dport 443 -j ACCEPT
aas@ubuntu: /usr/share/easy-rsa$ sudo iptables -I FORWARD -i tun+ -j ACCEPT
aas@ubuntu: /usr/share/easy-rsa$ sudo iptables -I FORWARD -i tun+ -o ens33 -m state --sta
te RELATED, ESTABLISHED -j ACCEPT
iptables v1.8.4 (legacy): "--state" requires a list of states with no spaces, e.g. ESTAB
LISHED,RELATED
Try 'iptables -h' or 'iptables --help' for more information.
aas@ubuntu: /usr/share/easy-rsa$ sudo iptables -I FORWARD -i tun+ -o ens33 -m state --sta
te RELATED, ESTABLISHED -j ACCEPT
aas@ubuntu: /usr/share/easy-rsa$ sudo iptables -I FORWARD -i ens33 -o tun+ -m state --sta
te RELATED, ESTABLISHED -j ACCEPT
aas@ubuntu: /usr/share/easy-rsa$ sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o en
s33 -j MASQUERADE
aas@ubuntu: /usr/share/easy-rsa$ sudo iptables -t nat -A OUTPUT -o tun+ -j ACCEPT
aas@ubuntu: /usr/share/easy-rsa$
```