

1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.

Список команд, используемых для установки и конфигурирования сервера:

```
sudo apt install openssh-server -y  
sudo systemctl enable --now ssh
```

проверяем, что openssh сервер запустился

```
sudo systemctl status ssh
```

Выводим список всех правил iptables

```
sudo iptables -L
```

Если нет правила для порта SSH – то вводим команду, чтобы разрешить подключение

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Подготавливаем папку и файл для сертификата openssh для текущего пользователя

```
mkdir ~/.ssh  
chmod 0700 ~/.ssh  
touch ~/.ssh/authorized_keys  
chmod 0644 ~/.ssh/authorized_keys
```

С помощью ssh-keygen или puttygen генерируем сертификаты.

В файл ~/.ssh/authorized_keys копируем публичный сертификат (в формате openssh)

Проверяем в файле /etc/ssh/sshd_config параметр PubkeyAuthentication, нужно чтобы имел значение yes

```
sudo nano /etc/ssh/sshd_config
```

Сервер настроен, проверяем подключение

Успешное подключение к серверу с использованием public_key. Сообщение можно посмотреть в логах /var/log/auth.log

```
login as: skilluser
Authenticating with public key "rsa-key-20230508"
Passphrase for key "rsa-key-20230508":
```

```
Passphrase for key "rsa-key-20230508":
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

13 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

6 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
Last login: Mon May  8 14:58:06 2023 from 192.168.137.223
skilluser@skill-ubuntu:~$
```

```
мая 08 14:58:06 skill-ubuntu sshd[177245]: Accepted publickey for skilluser from 192.168.137.223 port 62885 ssh2: RSA SHA256:Jah0EkGX/RJkFrXihMH6ipQmg96pPhU1YBoG+
мая 08 14:58:06 skill-ubuntu sshd[177245]: pam_unix(sshd:session): session opened for user skilluser(uid=1001) by (uid=0)
```

2. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля:
 - /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3
 - usr/bin/systemctl
 - sbin/ifup, /sbin/ifdown

Создаем пользователя skilluser командой:

```
sudo adduser skilluser
```

Добавляем в файл /etc/sudoers строки, позволяющие запускать утилиты без требования пароля:

```
skilluser    ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3
```

```
skilluser    ALL=(ALL) NOPASSWD: /usr/bin/systemctl
```

```
skilluser    ALL=(ALL) NOPASSWD: /sbin/ifup, /sbin/ifdown
```

```
sudo nano /etc/sudoers
```

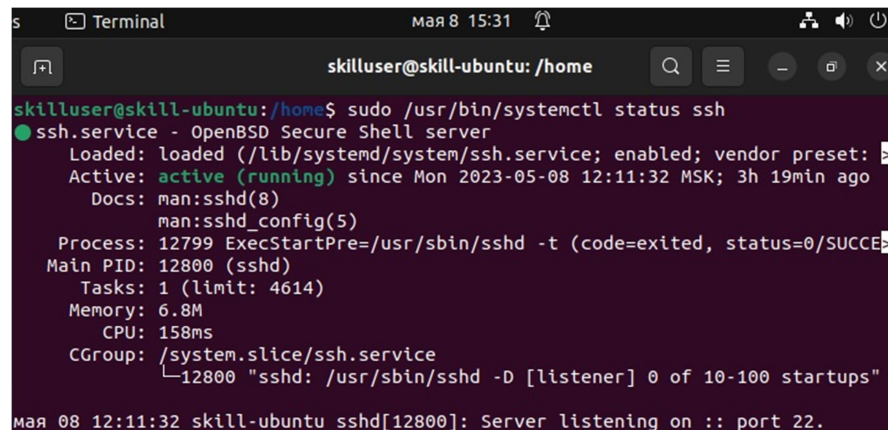
Для проверки заходим под пользователем skilluser

```
su skilluser
```

Запускаем утилиту /usr/bin/systemctl для проверки статуса SSH сервера.

```
sudo /usr/bin/systemctl status ssh
```

Как видно из скриншота, утилита запустилась без ввода пароля суперпользователя



```
skilluser@skill-ubuntu: /home$ sudo /usr/bin/systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:
   Active: active (running) since Mon 2023-05-08 12:11:32 MSK; 3h 19min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 12799 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 12800 (sshd)
     Tasks: 1 (limit: 4614)
    Memory: 6.8M
       CPU: 158ms
   CGroup: /system.slice/ssh.service
           └─12800 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

мая 08 12:11:32 skill-ubuntu sshd[12800]: Server listening on :: port 22.
```

Результат выполнения команды добавления пользователя и содержимое файла /etc/sudoers на скриншоте ниже:

```
Terminal
мая 8 13:05

skill@skill-ubuntu: /home

skill@skill-ubuntu:/home$ ls
skill  skilluser
skill@skill-ubuntu:/home$ cat /etc/passwd |grep skilluser
skilluser:x:1001:1001:,,,:/home/skilluser:/bin/bash
skill@skill-ubuntu:/home$ sudo cat /etc/sudoers |grep skilluser
skilluser    ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap,
/usr/sbin/hping3
skilluser    ALL=(ALL) NOPASSWD: /usr/bin/systemctl
skilluser    ALL=(ALL) NOPASSWD: /sbin/ifup, /sbin/ifdown
skill@skill-ubuntu:/home$
```

3. Установить минимальную длину пароля для пользователя в 8 символов.

Использовалась статья: https://sysadmin78.ru/doku.php/how_to:how_to_set_password_policies_in_linux

Для добавления опции минимальной длины пароля для пользователей, нужно отредактировать файл /etc/pam.d/common-password

`sudo nano /etc/pam.d/common-password`

```
Terminal
мая 8 13:08

skill@skill-ubuntu: /home

skill@skill-ubuntu:/home$ sudo cat /etc/pam.d/common-password |grep minlen
password      [success=2 default=ignore]      pam_unix.so obscure use_authtok
try_first_pass yescrypt minlen=8
skill@skill-ubuntu:/home$
```

4. Установить на сервер пакеты Java.

```
sudo apt update
```

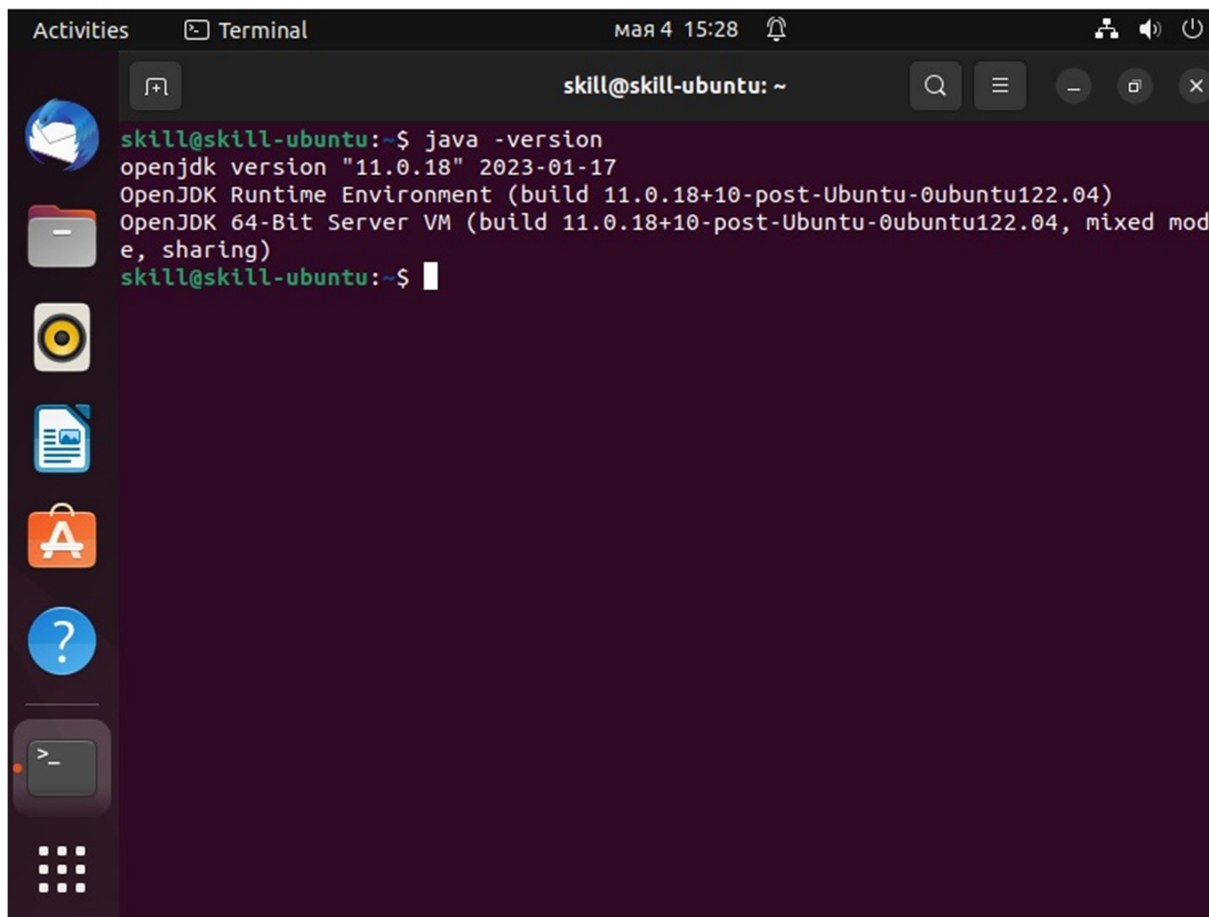
Устанавливаем пакеты JRE

```
sudo apt install default-jre -y
```

проверяем успешность установки пакетов java

```
java -version
```

использовался следующий источник: <https://ubuntu.com/tutorials/install-jre#2-installing-openjdk-jre>



The screenshot shows a terminal window titled "Terminal" with the date and time "мая 4 15:28". The terminal prompt is "skill@skill-ubuntu: ~". The command "java -version" has been executed, resulting in the following output:

```
skill@skill-ubuntu:~$ java -version
openjdk version "11.0.18" 2023-01-17
OpenJDK Runtime Environment (build 11.0.18+10-post-Ubuntu-0ubuntu122.04)
OpenJDK 64-Bit Server VM (build 11.0.18+10-post-Ubuntu-0ubuntu122.04, mixed mode, sharing)
skill@skill-ubuntu:~$
```

5. Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.

Для автоматического сканирования антивирусом clamav всей ОС каждый понедельник в 4 утра создаем задачу в CRON:

```
0 4 * * 1 clamscan --recursive --infected / --move=/tmp/clamscan --log=/var/log/clamscan.log
```

Антивирус clamav уже имеет задачу в CRON на ежедневное обновление. Чтобы увеличить интервал до 1 месяца нужно отключить автоматическое ежедневное обновление и добавить новую задачу в CRON:

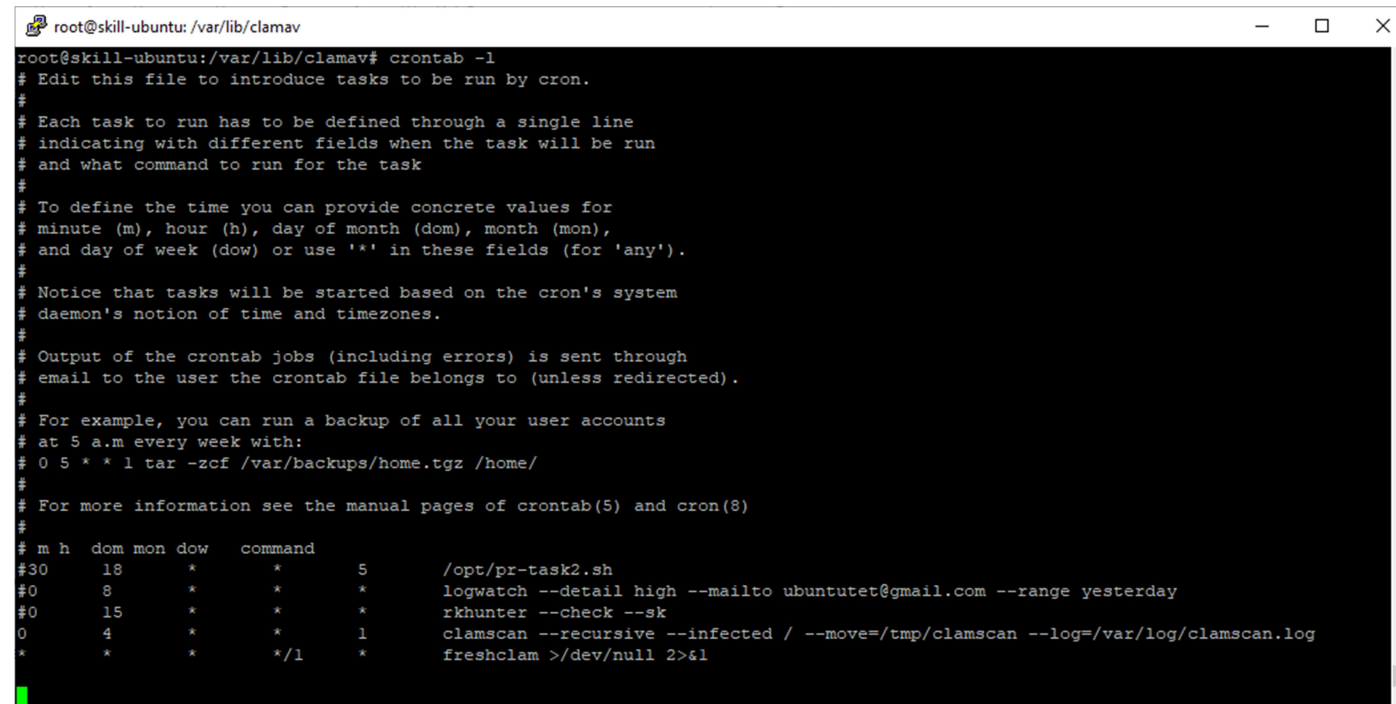
```
sudo stop clamav-freshclam
```

```
sudo update-rc.d clamav-freshclam disable
```

```
crontab -e
```

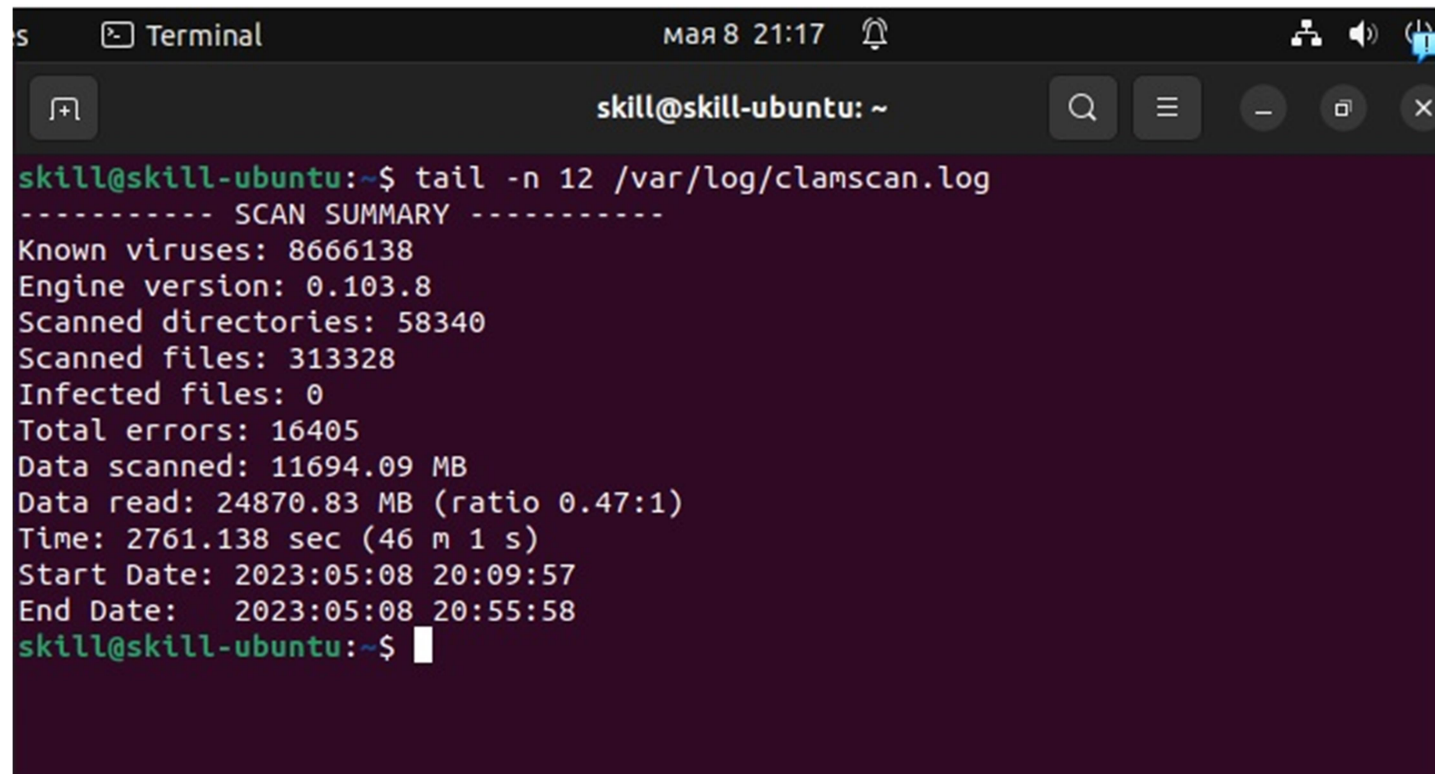
```
* * * */1 * freshclam >/dev/null 2>&1
```

Получаем следующий график в планировщике CRON



```
root@skill-ubuntu: /var/lib/clamav
root@skill-ubuntu:/var/lib/clamav# crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
#30 18 * * * 5 /opt/pr-task2.sh
#0 8 * * * logwatch --detail high --mailto ubuntu@ubuntu.com --range yesterday
#0 15 * * * rkhunter --check --sk
0 4 * * * clamscan --recursive --infected / --move=/tmp/clamscan --log=/var/log/clamscan.log
* * * */1 * freshclam >/dev/null 2>&1
```

Результат сканирования командой `clamscan --recursive --infected / --move=/tmp/clamscan --log=/var/log/clamscan.log`

A terminal window titled "Terminal" with a dark background. The prompt is "skill@skill-ubuntu: ~". The command "tail -n 12 /var/log/clamscan.log" has been executed, displaying the following scan summary:

```
skill@skill-ubuntu:~$ tail -n 12 /var/log/clamscan.log
----- SCAN SUMMARY -----
Known viruses: 8666138
Engine version: 0.103.8
Scanned directories: 58340
Scanned files: 313328
Infected files: 0
Total errors: 16405
Data scanned: 11694.09 MB
Data read: 24870.83 MB (ratio 0.47:1)
Time: 2761.138 sec (46 m 1 s)
Start Date: 2023:05:08 20:09:57
End Date: 2023:05:08 20:55:58
skill@skill-ubuntu:~$
```

6. «Настроить firewall на блокирование всего входящего и исходящего трафика.»

Для блокировки всего входящего и исходящего трафика вводим команды:

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

Получаем следующую таблицу iptables. Исходящий трафик проверяем пингом.


```
Terminal
мая 8 20:24
skill@skill-ubuntu: ~
skill@skill-ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy DROP)
target      prot opt source                destination
skill@skill-ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9202ms

skill@skill-ubuntu:~$
```