Start two parallel SSH servers

1. Створюємо користувача john із домашньою папкою за типовим шляхом.

```
dmytro@ubuntu22:~$ sudo useradd -m -d /home/john -s /bin/bash john
dmytro@ubuntu22:~$
```

2. Встановіть і налаштуйте SSH-сервер, який прослуховує порт 2222, обмежуючи кореневий доступ і забороняючи авторизаці

- Встановлюємо та налаштовуємо SSH сервер

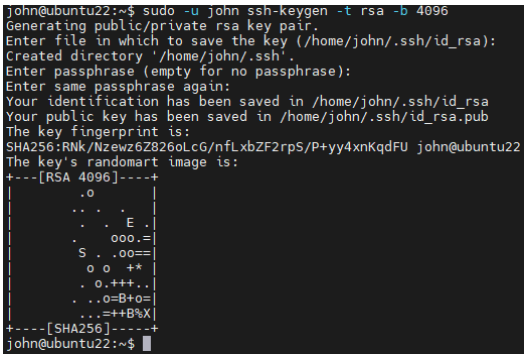
```
dmytro@ubuntu22:~$ sudo apt-get update
```

```
dmytro@ubuntu22:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.10).
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
dmytro@ubuntu22:~$
```

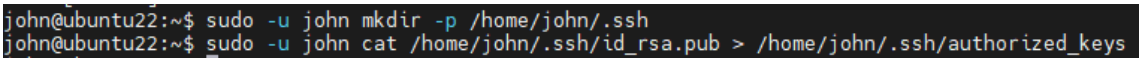
- Відредагуємо конфігураційний файл **etc/ssh/sshd_config**
  Змінимо у файлі наступні параметри
  - Port 2222
  - AllowUsers john
  - PermitRootLogin no
  - PasswordAuthentication no

```
Include /etc/ssh/sshd_config.d/*.conf

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
AllowUsers john

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

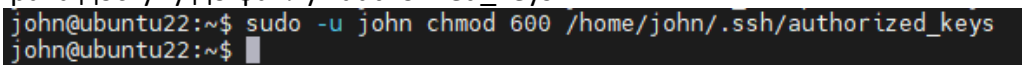
Генеруємо SSH ключі для користувача “john”



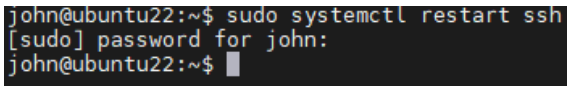
Створюємо директорію «.ssh» для користувача john. Після чого додаємо публічний ключ до файлу “authorized_keys”



Налаштовуємо права доступу до файлу “authorized_keys”

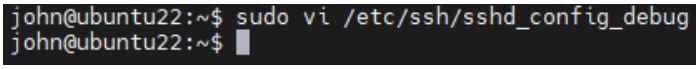


Перезапускаємо SSH сервер



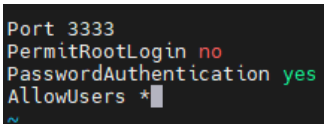
Налаштування SSH у режимі налагодження для порту 3333

Створимо додатковий конфігураційний файл для налагодження

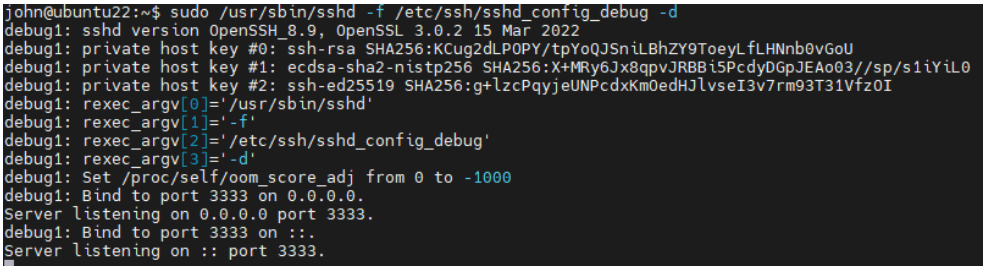


Внесемо у файл деякі дані:

Port 3333 – ssh сервер буде слухати з’єднання на порту 3333
PermitRootLogin no – Забороняє вхід користувачу root
PasswordAuthentication yes – Дозволяє аутентифікацію за паролем
AllowUsers * - дозволяє всім користувачам підключатися через SSH

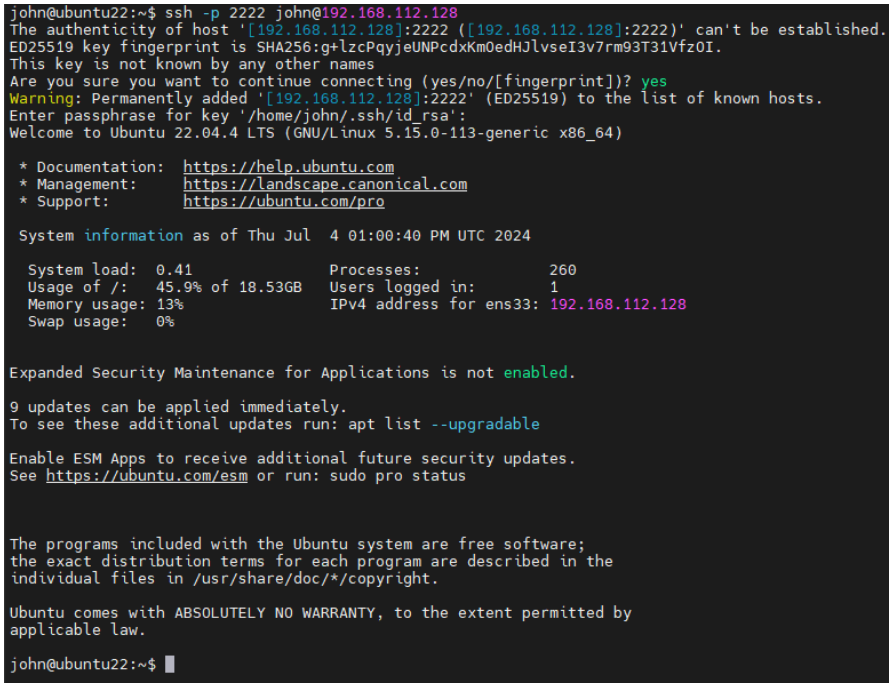


Запустимо SSH у режимі налагодження (sudo /usr/sbin/sshd -f /etc/ssh/sshd_config_debug -d)

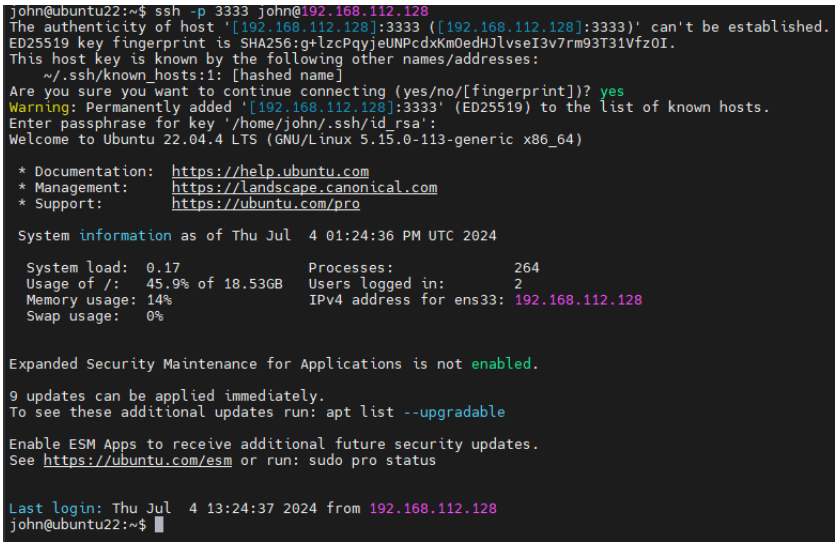


Підключення до серверів та перевірка статусу

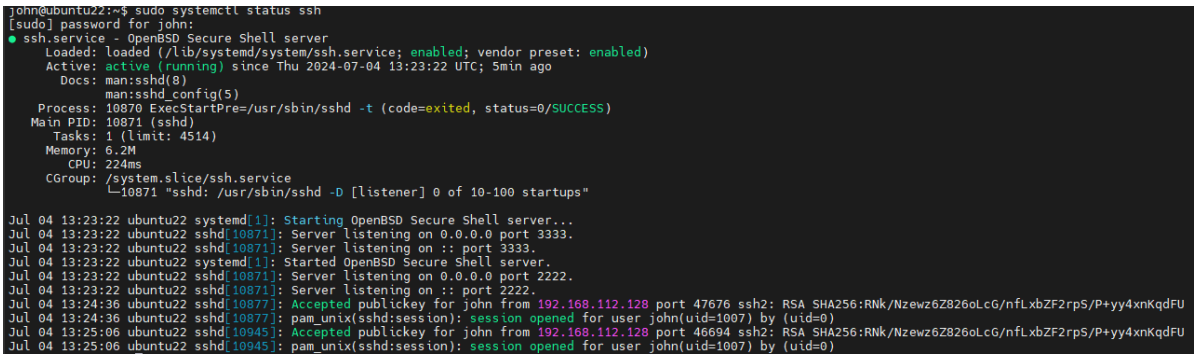
Підключення до серверу на порту 2222



Підключення до серверу на порту 3333



Перевірка статусу SSH-сервера



Перевіримо процес у режимі налагодження