Projet : Sécurisation d'un serveur Ubuntu sur OVH

Description du projet :

Dans ce projet, j'ai mis en place plusieurs mesures de sécurité sur un serveur Ubuntu Server hébergé chez OVH afin de protéger les accès distants et de réduire les risques d'attaques. L'objectif était d'appliquer les bonnes pratiques utilisées en entreprise pour sécuriser un serveur Linux accessible depuis Internet.

Étapes :

1-Connexion SSH par clé **SSH_KEYGEN** avec terminal (cmd)

2-Connexion **SSH** par clé **PuTTYgen** avec **PuTTY**

3- Désactiver root

4- Désactiver les mots de passe SSH

5-Changer port SSH

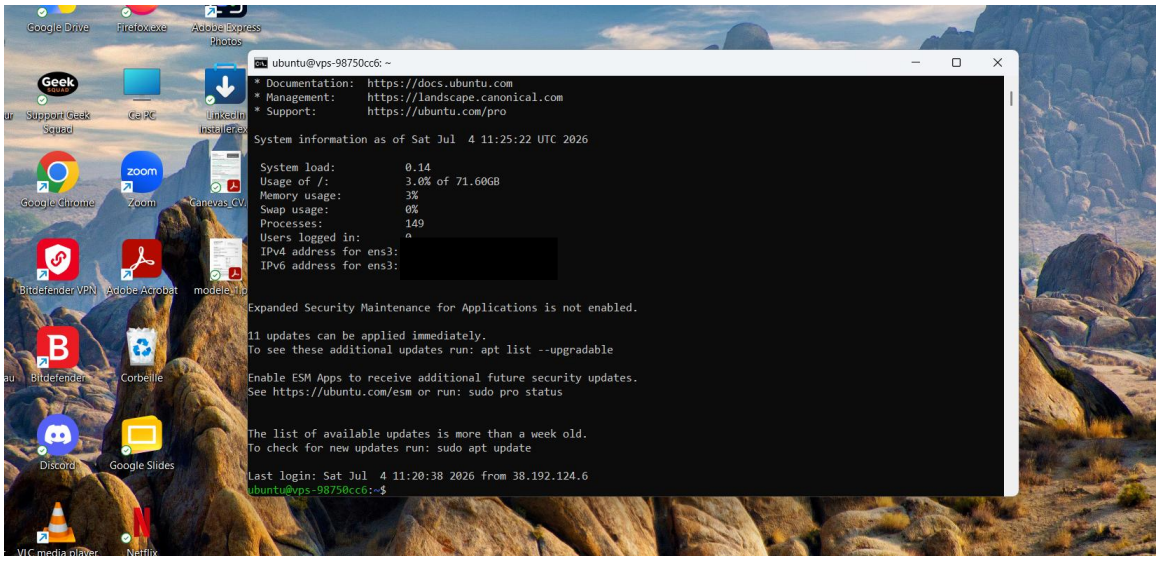
6-Installer **UFW** avec quelques configurations

7-Installer **Fail2Ban** avec quelques configurations

8-Installer Apache2

1-sécurisation ssh : SSH_KEYGEN :

J’ai mis un clé ssh pour me connecter a mon compte administrateur sur ovh directement sans mot de passe a travers mon terminal



root@vps-98750cc6: /home/ubuntu

```
oot@vps-98750cc6:/home/ubuntu# adduser riadh
ew password:
etype new password:
asswd: password updated successfully
hanging the user information for riadh
nter the new value, or press ENTER for the default
        Full Name []: riadh
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
s the information correct? [Y/n] y
oot@vps-98750cc6:/home/ubuntu# usermod -aG sudo riadh
oot@vps-98750cc6:/home/ubuntu# groups riadh
iadh : riadh sudo users
oot@vps-98750cc6:/home/ubuntu#
```

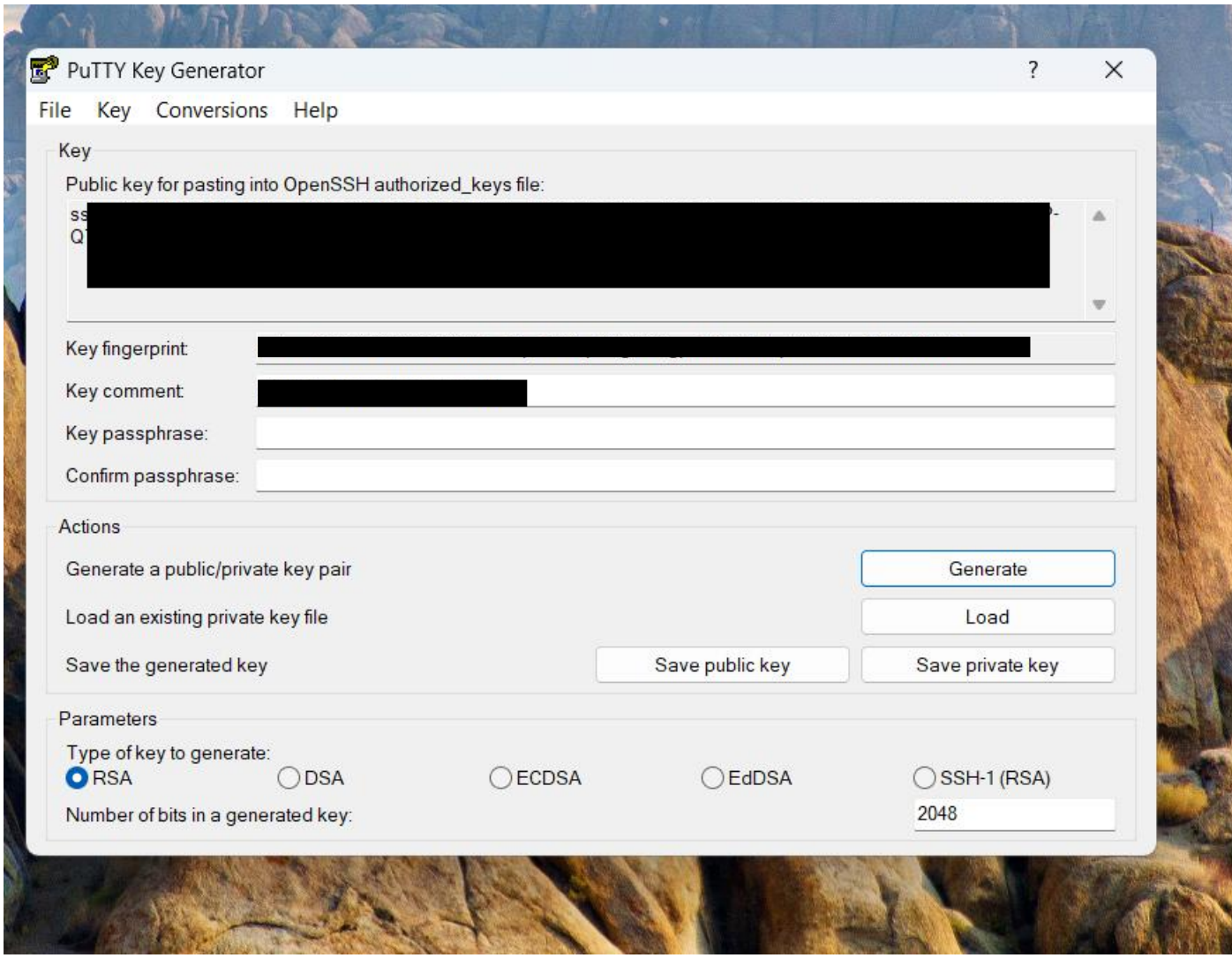
```
:\Windows\System32>ssh-keygen
enerating public/private ed25519 key pair.
nter file in which to save the key (C:\Users\Riadh/.ssh/id_ed25519):
nter passphrase (empty for no passphrase):
nter same passphrase again:
our identification has been saved in C:\Users\Riadh/.ssh/id_ed25519
our public key has been saved in C:\Users\Riadh/.ssh/id_ed25519.pub
he key fingerprint is:
[redacted]

:\Windows\System32>ssh-copy-id riadh@[redacted]
ssh-copy-id' n'est pas reconnu en tant que commande interne
u externe, un programme exécutable ou un fichier de commandes.

:\Windows\System32>type $env:USERPROFILE\.ssh\id_ed25519.pub
a syntaxe du nom de fichier, de répertoire ou de volume est incorrecte.

:\Windows\System32>type %USERPROFILE%\.ssh\id_ed25519.pub
[redacted]

:\Windows\System32>
```

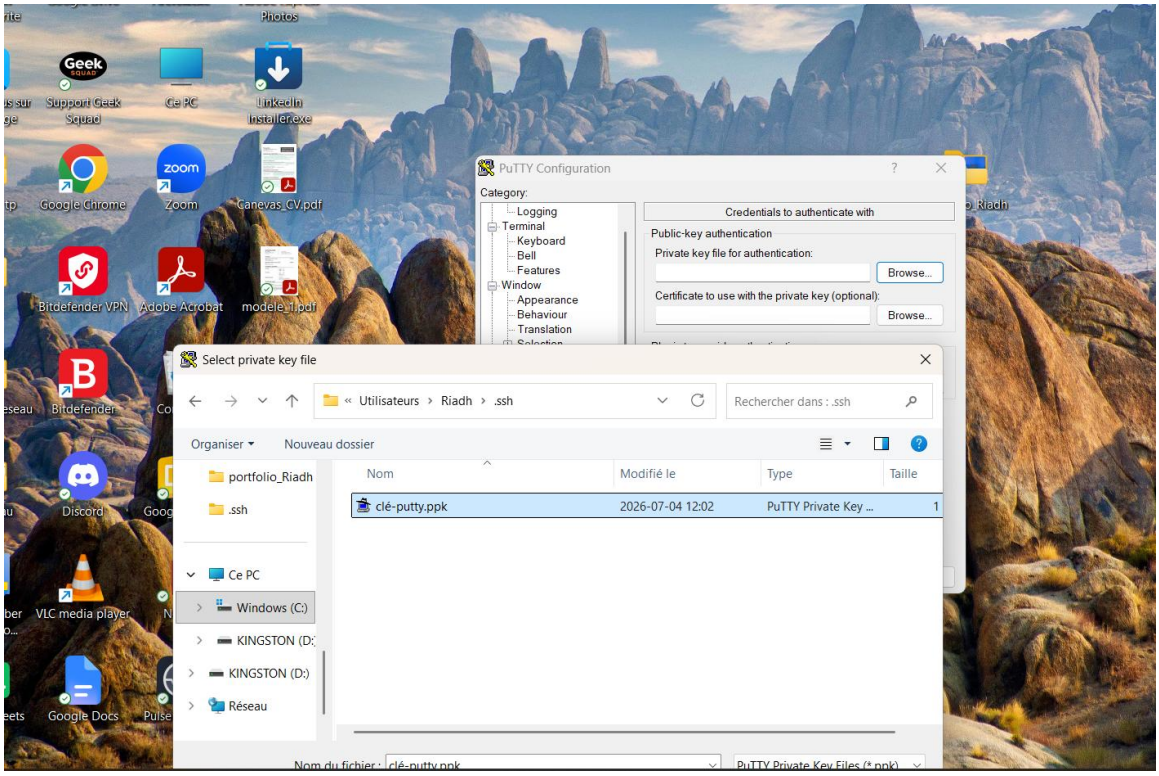
```
root@vps-98750cc6:/home/ubuntu# ls -la ~/.ssh
total 8
drwx------ 2 root root 4096 Jul  4 11:00 .
drwx------ 3 root root 4096 Apr 21 16:31 ..
-rw------- 1 root root    0 Jul  4 11:00 authorized_keys
root@vps-98750cc6:/home/ubuntu# cat ~/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# vim ~/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# nano  ~/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# nano  ~/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# nano  ~/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# chmod 700 ~/.ssh
root@vps-98750cc6:/home/ubuntu#
root@vps-98750cc6:/home/ubuntu# chmod 600 ~/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu#
```

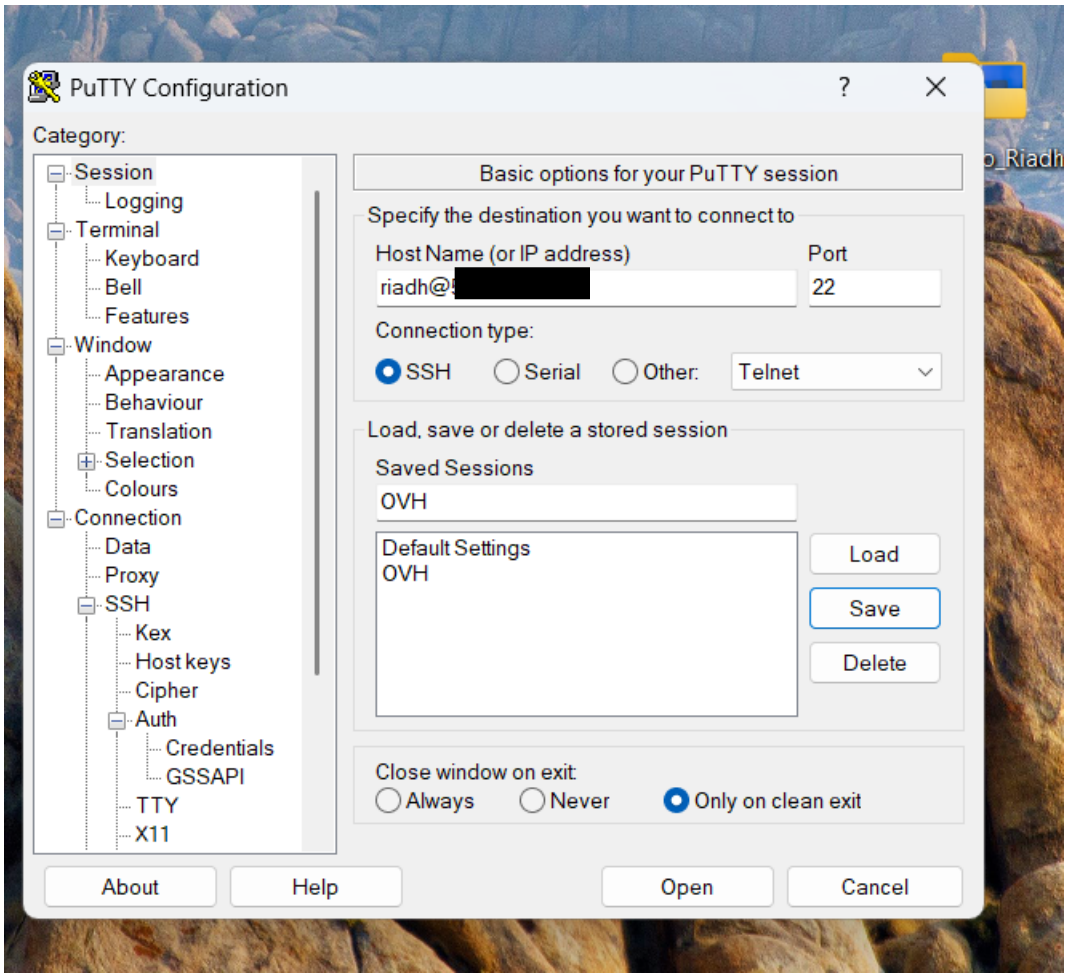
```
root@vps-98750cc6:/home/ubuntu# mkdir -p /home/riadh/.ssh
root@vps-98750cc6:/home/ubuntu# nano /home/riadh/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# chown -R riadh:riadh /home/riadh/.ssh
root@vps-98750cc6:/home/ubuntu# chmod 700 /home/riadh/.ssh
root@vps-98750cc6:/home/ubuntu# chmod 600 /home/riadh/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu#
```

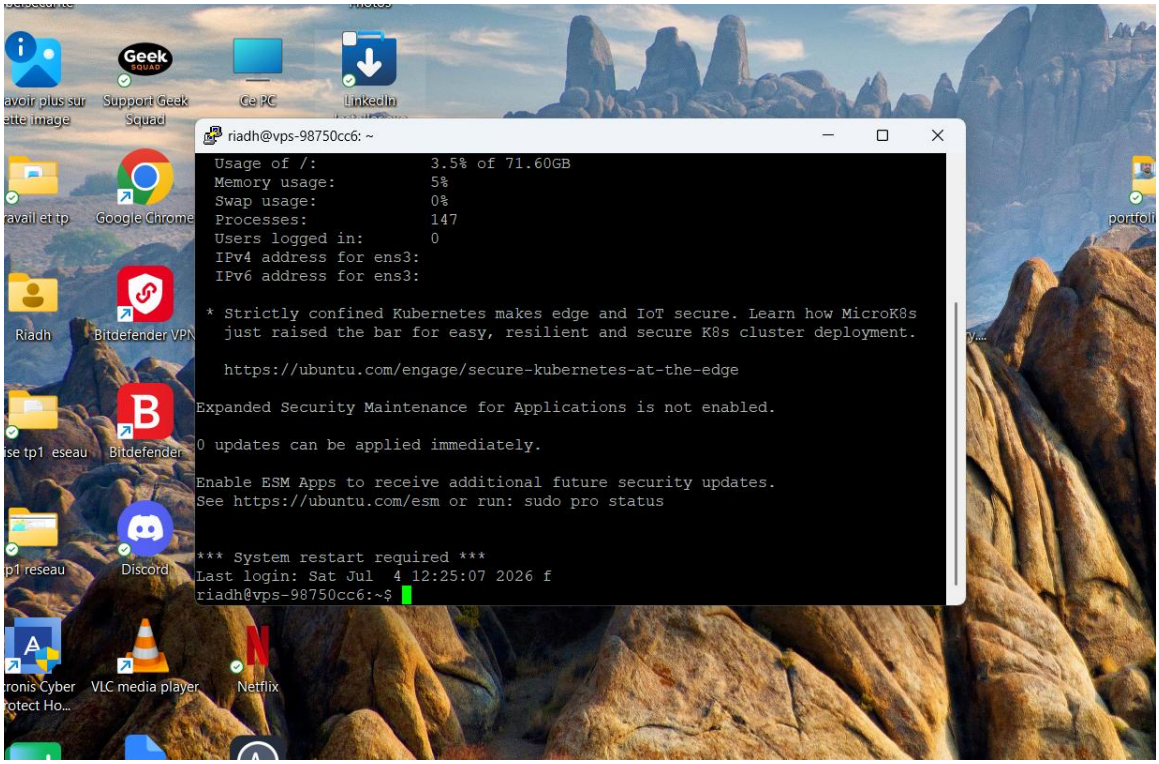
```
root@vps-98750cc6:/home/ubuntu# mkdir -p /home/riadh/.ssh
root@vps-98750cc6:/home/ubuntu# nano /home/riadh/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# chown -R riadh:riadh /home/riadh/.ssh
root@vps-98750cc6:/home/ubuntu# chmod 700 /home/riadh/.ssh
root@vps-98750cc6:/home/ubuntu# chmod 600 /home/riadh/.ssh/authorized_keys
root@vps-98750cc6:/home/ubuntu# ls -la /home/riadh/.ssh
total 12
drwx------ 2 riadh riadh 4096 Jul  4 12:21 .
drwxr-x--- 4 riadh riadh 4096 Jul  4 12:20 ..
-rw------- 1 riadh riadh  103 Jul  4 12:21 authorized_keys
root@vps-98750cc6:/home/ubuntu#
```

2-Connexion SSH par clé PuTTYgen avec PuTTY :




Photos
Support Geek Squad
Ce PC
LinkedIn Installer.exe
Google Chrome
zoom
Zoom
Canevas_CV.pdf
Bitdefender VPN
Adobe Acrobat
modele_1.pdf
Bitdefender
Discord
VLC media player
Google Docs
PuTTY Configuration
Category:
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Credentials to authenticate with
Public-key authentication
Private key file for authentication:
Browse...
Certificate to use with the private key (optional):
Browse...
Select private key file
« Utilisateurs › Riadh › .ssh
Rechercher dans : .ssh
Organiser
Nouveau dossier
portfolio_Riadh
.ssh
Ce PC
Windows (C:)
KINGSTON (D:)
KINGSTON (D:)
Réseau
Nom
Modifié le
Type
Taille
clé-putty.ppk
2026-07-04 12:02
PuTTY Private Key ...
1
Nom du fichier :
clé-putty.ppk
PuTTY Private Key Files (*.ppk)


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
Credentials
GSSAPI
TTY
X11
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
riadh@[redacted]
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
OVH
Default Settings
OVH
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel



3- Désactiver root :

```
# Authentication:

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

```
C:\Windows\System32>ssh root@
root@51.222.31.78's password:
Permission denied, please try again.
root@51.222.31.78's password:
Permission denied, please try again.
root@51.222.31.78's password:
```

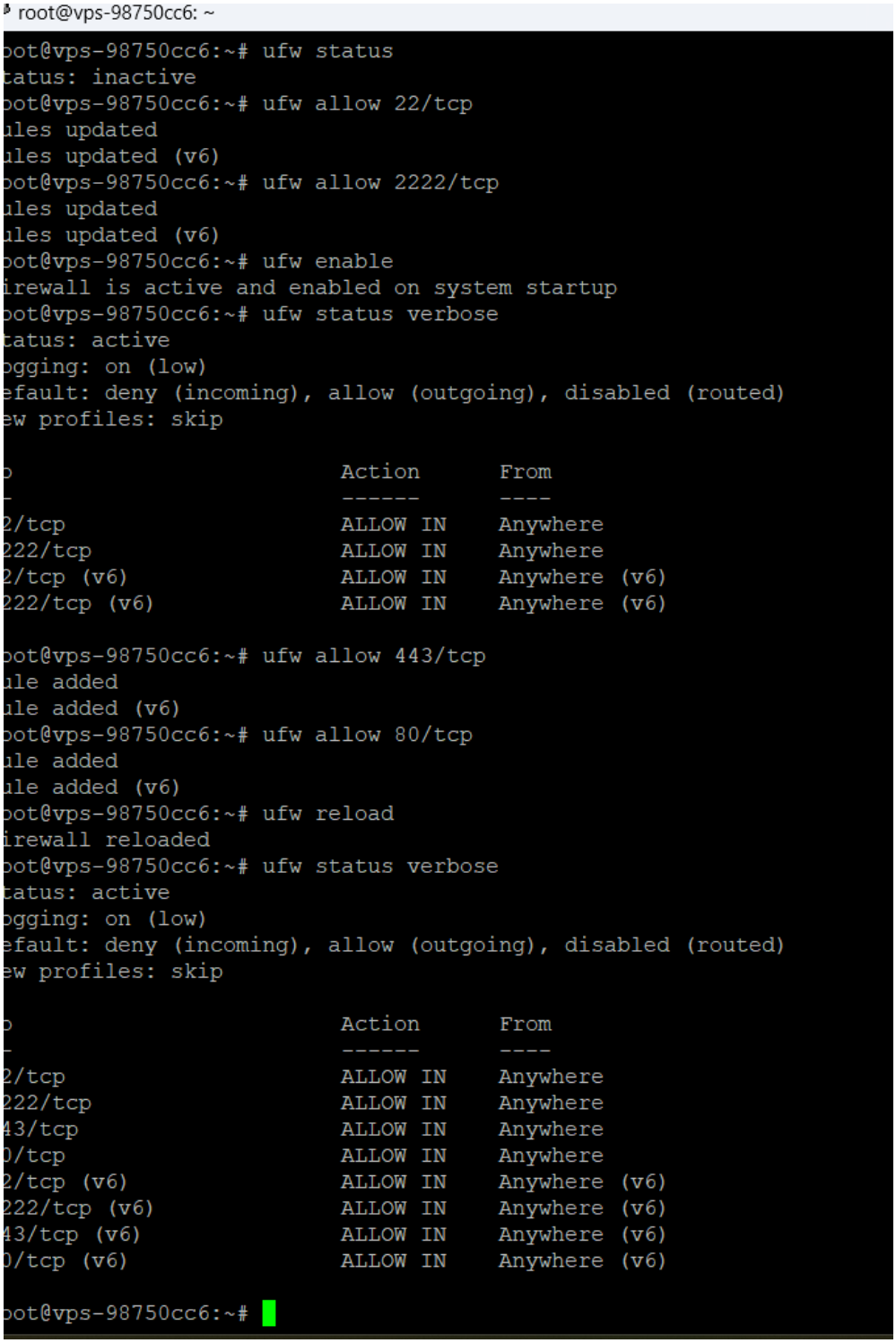
4- Désactiver les mots de passe SSH :

```
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2
#AuthorizedKeysFile     .ssh/au

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobo

# For this to work you will als
#HostbasedAuthentication no
# Change to yes if you don't tr
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhos
#IgnoreRhosts yes

# To disable tunneled clear tex
PasswordAuthentication no
#PermitEmptyPasswords no
```

5- changer port SSH :

```
#
Port 2222
#AddressFamil
#ListenAddres
```

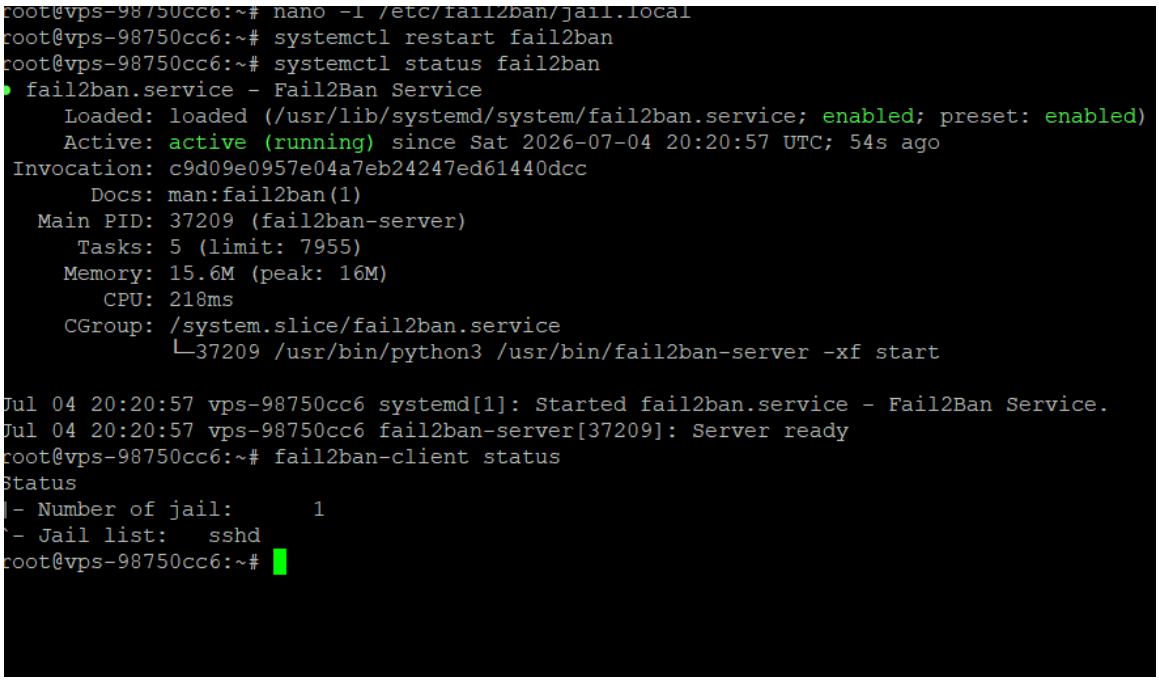
6-Installer UFW avec quelques configurations :



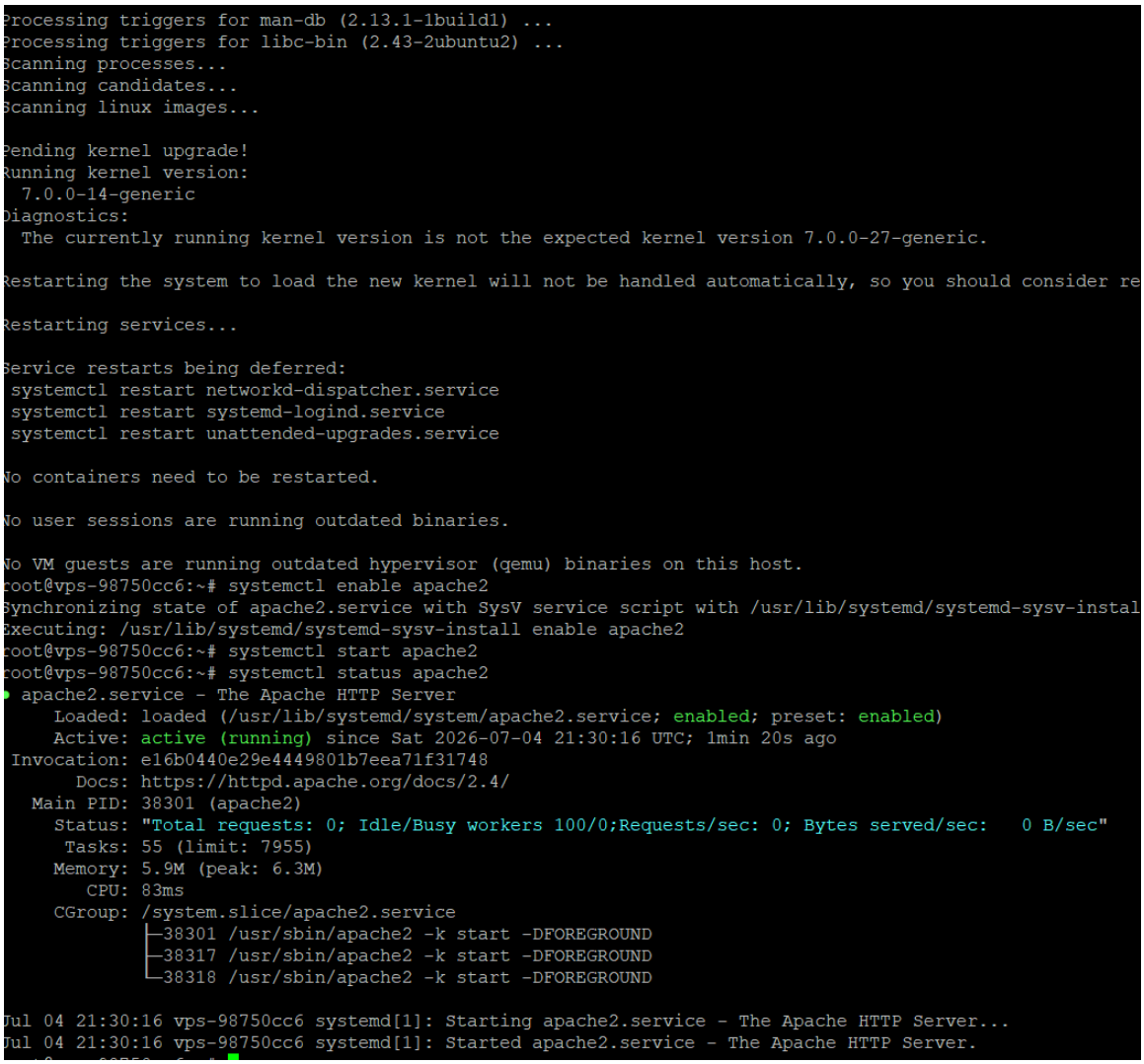
7-Installer Fail2Ban avec quelques configurations :

```
root@vps-98750cc6:~# systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
root@vps-98750cc6:~# systemctl start fail2ban
root@vps-98750cc6:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Sat 2026-07-04 19:11:20 UTC; 2min 4s ago
 Invocation: 708fc5902acb4bd8a5134bfda24dce95
       Docs: man:fail2ban(1)
   Main PID: 35938 (fail2ban-server)
      Tasks: 5 (limit: 7955)
     Memory: 24.5M (peak: 24.8M)
        CPU: 272ms
     CGroup: /system.slice/fail2ban.service
             └─35938 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jul 04 19:11:20 vps-98750cc6 systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jul 04 19:11:20 vps-98750cc6 fail2ban-server[35938]: Server ready
root@vps-98750cc6:~#
```

```
WARNING: heavily refactored in 0.9.0 release.  Please review and
         customize settings for your setup.

Changes:  in most of the cases you should not modify this
          file, but provide customizations in jail.local file,
          or separate .conf files under jail.d/ directory, e.g.:

HOW TO ACTIVATE JAILS:

YOU SHOULD NOT MODIFY THIS FILE.

It will probably be overwritten or improved in a distribution update.

Provide customizations in a jail.local file or a jail.d/customisation.local.
For example to change the default bantime for all jails and to enable the
ssh-iptables jail the following (uncommented) would appear in the .local file.
See man 5 jail.conf for details.

[DEFAULT]
ignoreip = 127.0.0.1/8 ::1
bantime = 1h
findtime = 10m
maxretry = 5

[sshd]
enabled = true
port = 22
maxretry = 3

See jail.conf(5) man page for more information



Comments: use '#' for comment lines and ';' (following a space) for inline comments


[INCLUDES]
```


root@vps-98750cc6:~# nano -l /etc/fail2ban/jail.local
root@vps-98750cc6:~# systemctl restart fail2ban
root@vps-98750cc6:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
Active: active (running) since Sat 2026-07-04 20:20:57 UTC; 54s ago
Invocation: c9d09e0957e04a7eb24247ed61440dcc
Docs: man:fail2ban(1)
Main PID: 37209 (fail2ban-server)
Tasks: 5 (limit: 7955)
Memory: 15.6M (peak: 16M)
CPU: 218ms
CGroup: /system.slice/fail2ban.service
└─37209 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
Jul 04 20:20:57 vps-98750cc6 systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jul 04 20:20:57 vps-98750cc6 fail2ban-server[37209]: Server ready
root@vps-98750cc6:~# fail2ban-client status
Status
|- Number of jail: 1
`- Jail list: sshd
root@vps-98750cc6:~#

8-Installer Apache2 avec quelques configurations de appache2 sur fail2ban :



```
[apache-auth]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s


[apache-badbots]
# Ban hosts which agent identifies spammer robots crawl
# for email addresses. The mail outputs are buffered.
enabled = true
port     = http,https
logpath  = %(apache_access_log)s
bantime  = 48h
maxretry = 1


[apache-noscript]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s


[apache-overflows]
enabled = true
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2
```