

Job 1

```
sophie@sophie-virtual-machine: ~  
Try 'chmod --help' for more information.  
root@sophie-virtual-machine:~# usermod -aG sudo sophie  
root@sophie-virtual-machine:~# su sophie  
sophie@sophie-virtual-machine:/root$ cd  
sophie@sophie-virtual-machine:~$ sudo apt update && sudo apt upgrade  
[sudo] password for sophie:  
Sorry, try again.  
[sudo] password for sophie:  
Sorry, try again.  
[sudo] password for sophie:  
Hit:1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease  
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]  
Hit:3 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:4 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Fetched 110 kB in 1s (82,5 kB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
5 packages can be upgraded. Run 'apt list --upgradable' to see them.  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Calculating upgrade... Done  
The following packages were automatically installed and are no longer required:
```

```
sophie@sophie-virtual-machine: ~  
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...  
sophie@sophie-virtual-machine:~$ sudo apt install ssh  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver  
intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58  
libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchromaprint1  
libcodec2-1.0 libdavid5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1  
libgstreamer-plugins-bad1.0-0 libigdgmm12 libllv-0-0 libmfx1 libmysofa1  
libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2  
libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0  
libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0  
libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1  
libx265-199 libxvidcore4 libzing2 libzmq5 libzvbi-common libzvbi0  
mesa-va-drivers mesa-va-drivers pocketsphinx-en-us va-driver-all  
vdpau-driver-all  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
ncurses-term openssh-server openssh-sftp-server ssh-import-id  
Suggested packages:  
molly-guard monkeysphere ssh-askpass  
The following NEW packages will be installed:
```

Job 2

```
sophie@sophie-virtual-machine:~$ sudo apt upgrade  
sophie@sophie-virtual-machine:~$ sudo apt install apache2  
sophie@sophie-virtual-machine:~$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese  
Active: active (running) since Tue 2022-11-08 10:20:14 CET; 1min 58s ago
```

```
sophie@sophie-virtual-machine:~$ sudo ufw allow 'Apache Full'
```

```
Les règles ont été mises à jour
```

```
Les règles ont été mises à jour (IPv6)
```

```
sophie@sophie-virtual-machine:~$ sudo ufw app list
```

```
Applications disponibles :
```

```
Apache
```

```
Apache Full
```

```
Apache Secure
```

```
CUPS
```

```
OpenSSH
```

```
sophie@sophie-virtual-machine:~$ sudo ufw allow 'Apache'
```

```
La règle a été ajoutée
```

```
La règle a été ajoutée (v6)
```



sophie@sophie-virtual-machine: ~



```
sophie@sophie-virtual-machine:~$ sudo ufw status
```

```
État : actif
```

```
Vers
```

```
Action
```

```
De
```

```
----
```

```
-----
```

```
--
```

```
Apache Full
```

```
ALLOW
```

```
Anywhere
```

```
Apache
```

```
ALLOW
```

```
Anywhere
```

```
Apache Full (v6)
```

```
ALLOW
```

```
Anywhere (v6)
```

```
Apache (v6)
```

```
ALLOW
```

```
Anywhere (v6)
```

```
sophie@sophie-virtual-machine:~$ systemctl status apache2
```

```
● apache2.service - The Apache HTTP Server
```

```
Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
```

```
Active: active (running) since Tue 2022-11-08 10:52:19 CET; 6min ago
```

```
Docs: https://httpd.apache.org/docs/2.4/
```

```
Process: 14016 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/S>
```

```
Main PID: 14021 (apache2)
```

```
Tasks: 55 (limit: 2247)
```

```
Memory: 4.4M
```

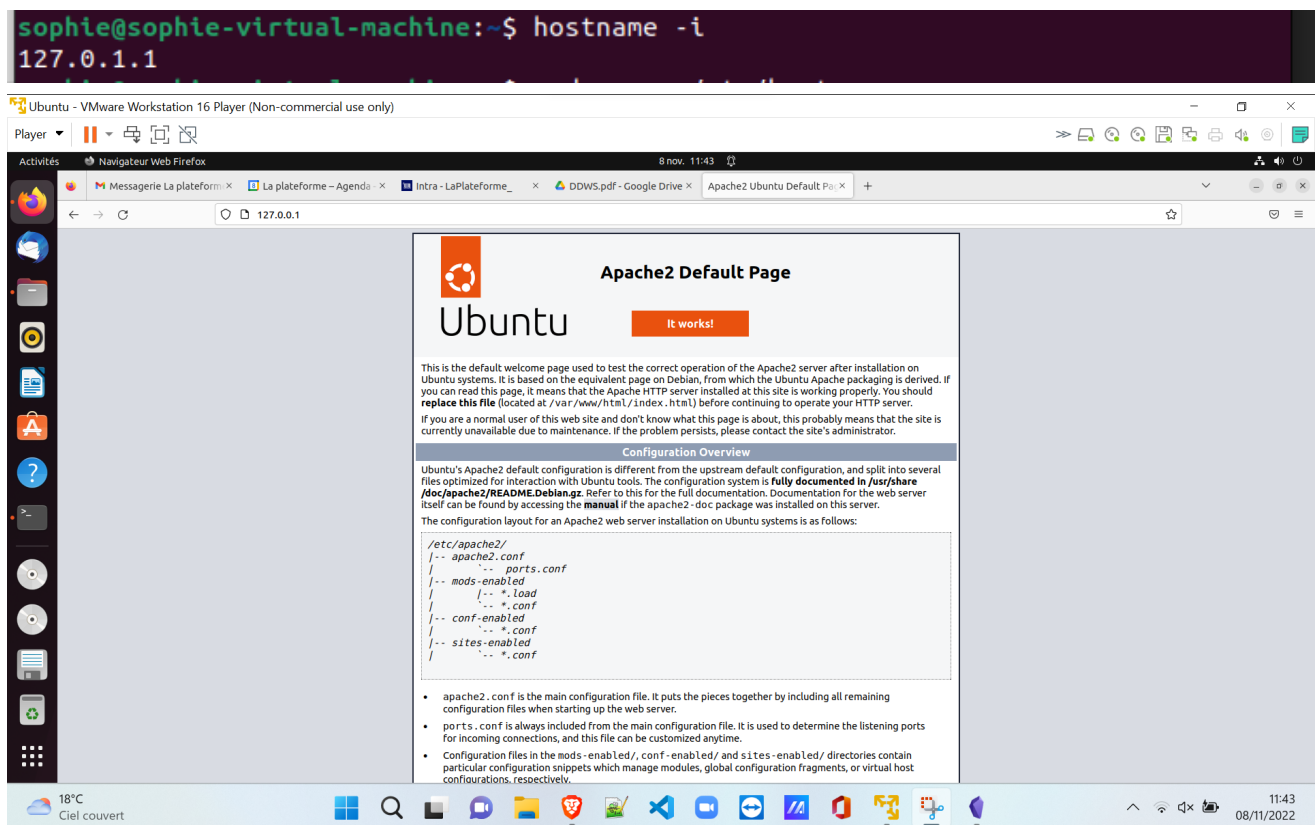
```
CPU: 58ms
```

```
CGroup: /system.slice/apache2.service
```

```
├─14021 /usr/sbin/apache2 -k start
```

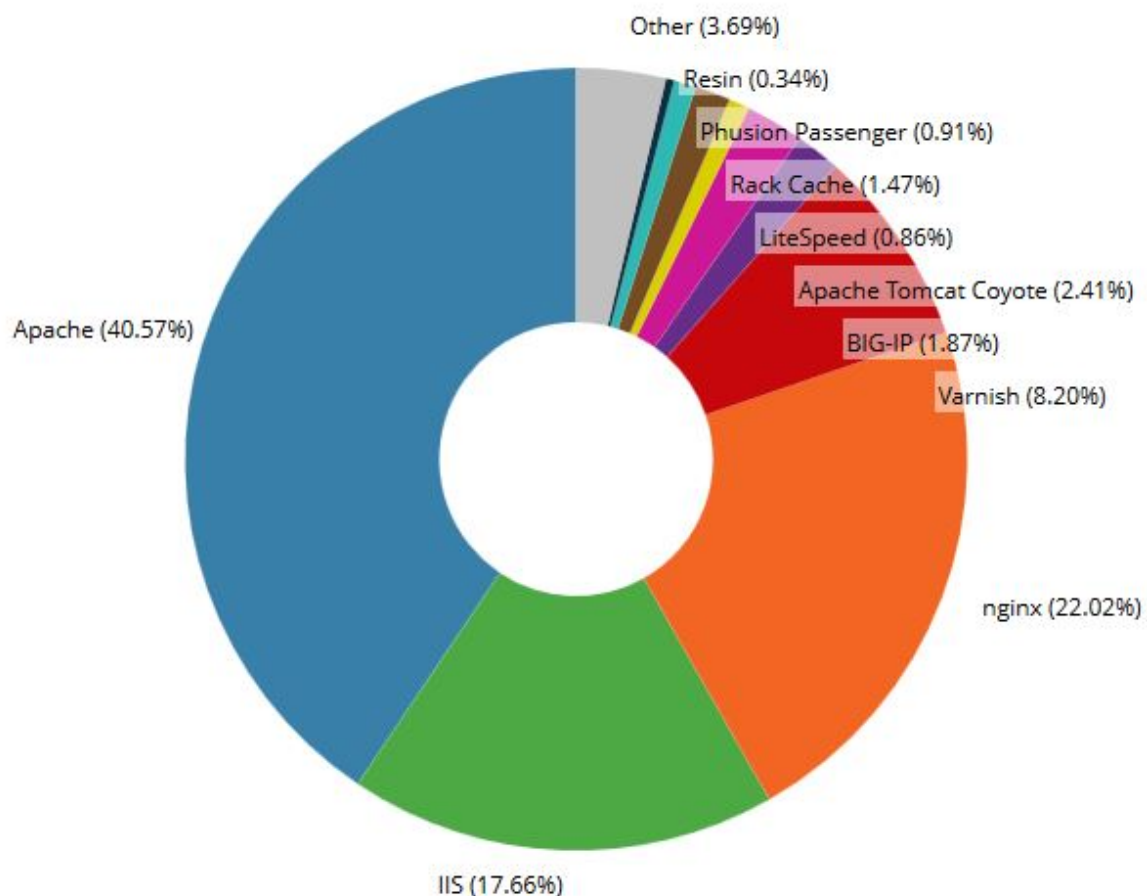
```
├─14022 /usr/sbin/apache2 -k start
```

```
└─14023 /usr/sbin/apache2 -k start
```



Job 3

Comme le montre cette image (source builtwith.com de 2022) les principaux serveurs Web aujourd'hui, sont Apache et Nginx et Microsoft Internet Information Service.



Pour information, les données fournies par Siftety Discover montrent que parmi les

entreprises qui bénéficient des avantages de Nginx, sont cités : Google, Facebook, LinkedIn, Cisco, Autodesk, T-Mobile, GitLab, Microsoft, IBM, Adobe, Salesforce, VMware, Xerox, Citrix Systems, Twitter, Apple, Intel.

Nginx est un serveur proxy inverse qui prend en charge les protocoles HTTP, HTTPS et IMAP. Il permet à un utilisateur d'Internet d'accéder à des serveurs internes.

Bien qu'Apache ne soit pas encore détrôné, Nginx sert du contenu statique environ 2,5 fois plus rapidement qu'Apache. Il s'agit là d'une grande différence de vitesse.

Nginx évoluera probablement plus efficacement qu'Apache et s'adapte mieux.

Il gère mieux le trafic élevé qu'Apache, une autre raison pour laquelle il est plus rapide.

En raison de son fonctionnement, Nginx nécessite de moins de mémoire, ce qui peut aider à économiser sur les coûts d'hébergement. Il est conçu sur mesure pour accélérer le fonctionnement des serveurs privés virtuels (VPS).

Mais Nginx a aussi des inconvénients. Ses options sont limitées. Peu d'hébergeurs offrent la prise en charge de Nginx, donc moins de plans disponibles.

Il a une communauté bien moins développée qu'Apache. Nginx a une moins bonne option pour servir du contenu dynamique, car il utilise un logiciel tiers pour gérer les demandes de contenu dynamique. Dans certains cas, il peut fonctionner moins bien qu'Apache. Et Nginx ne prend pas en charge .htaccess.

Apache est Open-source et gratuit même pour un usage commercial. C'est un logiciel fiable et stable. Il a une mise à jour régulière, ainsi que des correctifs de sécurité. Apache est flexible grâce à sa structure basée sur des modules. Il a une énorme communauté et des tonnes de modules qui facilitent l'obtention d'une assistance pour faire à peu près n'importe quoi. Apache dispose d'un grand nombre de modules disponibles pour l'étendre, il est donc compatible avec beaucoup plus de technologies tierces.

La prise en charge de Python et Perl est intégrée à Apache, il est donc beaucoup plus facile de commencer à coder. Ruby s'exécute plus rapidement dans Apache.

Il est facile à configurer et adapté aux débutants.

La pile LAMP (ensemble de logiciels libres tels que Linux OS, Apache serveur Web, MySQL serveur de base de données, PHP Perl Python langages de script) est presque la norme de l'industrie parmi les hébergeurs Web à faible coût.

La Plateforme-Cross fonctionne sur les serveurs Unix et Windows et Apache fonctionne avec les sites WordPress.

Comme Nginx, Apache a lui aussi quelques inconvénients. Comme des problèmes de performances sur les sites web avec un énorme trafic. Il a trop d'options de configuration qui peuvent mener à la vulnérabilité de la sécurité.

Lorsqu'Apache est surchargé, il manque de RAM et commence à utiliser des fichiers d'échange, ce qui ralentit tout sur le serveur. Et Apache refuse les requêtes lorsqu'il commence à se saturer.

Microsoft IIS est gratuit, facile à configurer et à utiliser. Il s'intègre parfaitement aux autres produits Microsoft. Il reste un choix populaire pour de nombreuses

entreprises et organisations.

Mais bien qu'il soit un serveur Web très riche en fonctionnalités, IIS n'est pas aussi largement pris en charge qu'Apache. Il est plus difficile de trouver de l'aide et de la documentation. IIS n'est pas aussi flexible que certains autres serveurs Web et il peut être difficile à configurer pour certains types de déploiements. On ne peut l'utiliser qu'avec le système d'exploitation Windows.

Job 4

```
sophie@sophie-virtual-machine: ~  
GNU nano 6.2 /etc/hosts  
127.0.0.1    localhost  
127.0.1.1    sophie-virtual-machine  
127.0.0.1    dnsproject.prepa.com  
# 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  
  
[ Lecture de 9 lignes ]  
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement  
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne  
  
sophie@sophie-virtual-machine:~$ ping -c 4 dnsproject.prepa.com  
PING dnsproject.prepa.com (127.0.0.1) 56(84) bytes of data:  
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.139 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.175 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.083 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.103 ms  
  
--- dnsproject.prepa.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3063ms  
rtt min/avg/max/mdev = 0.083/0.125/0.175/0.035 ms
```

Job 5

- Il faut prendre le temps et bien choisir le nom du domaine et son extension.
Il y a trois grands groupes de noms de domaine :
 - ° les génériques (gTLD : generic Top-Level Domains). Ce groupe comporte 12 domaines de premier niveau : .arpa, .biz, .com, .edu, .gov, .info, .int, .mil, .name, .net, .org et .pro. Seuls 7 sont des extensions commerciales ouvertes à tous : .biz, .com, .info, .name, .net, .org et .pro.
 - ° les géographiques (ccTLD : country-code Top-Level Domains). Ce groupe comporte

un domaine pour chaque pays ou territoire de la planète. Par exemple .fr (France), .be (Belgique), .ch (Suisse), .eu (Union Européenne), .re (Réunion), .us (Etats-Unis).

° les commandités (sTLD : sponsored Top-Level Domains). Ce groupe comporte 9 domaines de premier niveau : .aero, .asia, .cat, .coop, .jobs, .museum, .mobi, .tel, .travel. Seules les extensions .mobi et .asia sont ouvertes au grand public.

Le choix de l'extension du nom de domaine doit dépendre des exigences de l'entreprise, de la stratégie de communication du site Internet et du public-cible. Aujourd'hui .com est rentrée dans les habitudes de langage et est devenue une extension quasi obligatoire pour un positionnement au niveau international. En revanche, une extension géographique locale aura l'avantage d'illustrer l'ancrage des activités présentées dans l'aire géographique choisie et de rassurer les visiteurs du pays concerné. Réserver les variantes du nom de domaine protégera des risques d'enregistrement abusif.

(L'abréviation io est l'abréviation en informatique de Input/Output. Elle présente un intérêt particulier pour les entreprises technologiques ou pour le domain hack. Laplateforme.io).

- Vérifier la disponibilité du nom du domaine. Il doit être unique car deux noms strictement identiques ne peuvent coexister. Il ne doit pas porter atteinte à un droit antérieur détenu par un tiers, ni porter atteinte à un droit d'auteur.
- Choisir l'agent d'enregistrement (registrar) qui correspondra le mieux aux besoins du site. Chaque extension est gérée par un registre unique. Cela peut aller d'un simple dépôt rapide et peu cher, jusqu'à l'élaboration de campagnes de dépôts internationales faisant intervenir des dizaines d'acteurs dans différents pays.
- Fournir les informations utiles à l'agent d'enregistrement au moyen d'un simple formulaire électronique avec noms de l'entreprise et de la personne de contact, coordonnées téléphonique, numérique et postale. C'est l'unique moyen de communication directe avec le registre.
- Enregistrer le nom du domaine. L'enregistrement est automatique et le nom de domaine immédiatement activé, valable pour une période d'un à dix ans, renouvelable.
- Enregistrement automatique du nom du domaine dans le répertoire Whois. Le Whois est un moteur de recherches permettant de voir la disponibilité des noms de domaine et de fournir des informations techniques et administratives sur le titulaire d'un nom de domaine.

Job 6/7

Pour ces jobs j'ai d'abord utilisé l'adresse 10.10.29.0. J'ai dû recommencer avec 10.10.30.0 car dès qu'on passe de NAT à bridge, cela fait sauter l'adresse IP.


```
sophie@ubuntu: ~  
GNU nano 6.2 /etc/hosts  
127.0.0.1 localhost  
127.0.1.1 ubuntu  
  
# 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  
  
[ Lecture de 9 lignes ]  
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement  
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

```
sophie@ubuntu: ~  
GNU nano 6.2 /etc/bind/db.direct *  
;  
; BIND data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA      dnsproject.prepa.com. ubuntu.dnsproject.prepa.com. (  
                2          ; Serial  
                604800     ; Refresh  
                86400      ; Retry  
                2419200    ; Expire  
                604800 )   ; Negative Cache TTL  
;  
tr@       IN      NS       ubuntu.dnsproject.prepa.com.  
ubuntu    IN      A        10.10.30.13  
www        IN      CNAME    ubuntu.dnsproject.prepa.com.  
  
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement  
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne  
Location maximum rest de 7200 secondes.
```

```
sophie@ubuntu: ~
GNU nano 6.2 /etc/bind/db.inverse *
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      dnsproject.prepa.com. ubuntu.dnsproject.prepa.com. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
ubuntu    IN      NS       ubuntu.dnsproject.prepa.com.
ubuntu    IN      A        10.10.30.13
www       IN      CNAME    ubuntu.dnsproject.prepa.com.

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
Oclation maximum rest de 7200 secondes.
```

```
sophie@ubuntu:~$ sudo apt install isc-dhcp-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libirs-export161 libiscfg-export163
Paquets suggérés :
  isc-dhcp-server-ldap policycoreutils
Les NOUVEAUX paquets suivants seront installés :
  isc-dhcp-server libirs-export161 libiscfg-export163
0 mis à jour, 3 nouvellement installés, 0 à enlever et 4 non mis à jour.
Il est nécessaire de prendre 528 ko dans les archives.
Après cette opération, 1 546 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 libiscfg-e
xport163 amd64 1:9.11.19+dfsg-2.1ubuntu3 [53,0 kB]
Réception de :2 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 libirs-expo
```



```
sophie@ubuntu: ~  
GNU nano 6.2 /etc/dhcp/dhcpd.conf *  
# option broadcast-address 10.254.239.31;  
# option routers rtr-239-32-1.example.org;  
#}  
  
# A slightly different configuration for an internal subnet.  
subnet 10.10.29.0 netmask 255.255.0.0 {  
    range 10.10.29.10 10.10.29.100;  
    option domain-name-servers 10.10.29.129, www.dnsproject.prepa.com;  
    option domain-name "dnsproject.prepa.com";  
    option subnet-mask 255.255.255.224;  
    option routers 10.10.29.129;  
    option broadcast-address 10.10.29.255;  
    default-lease-time 86600;  
    max-lease-time 72600;  
}  
  
# Hosts which require special configuration options can be listed in  
# host statements.  If no address is specified, the address will be  
# allocated dynamically (if possible), but the host-specific information  
# will still come from the host declaration.  
  
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement  
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

```
sophie@ubuntu: ~  
GNU nano 6.2 /etc/dhcp/dhcpd.conf *  
#subnet 10.254.239.32 netmask 255.255.255.224 {  
#    range dynamic-bootp 10.254.239.40 10.254.239.60;  
#    option broadcast-address 10.254.239.31;  
#    option routers rtr-239-32-1.example.org;  
#}  
  
# A slightly different configuration for an internal subnet.  
subnet 10.10.30.0 netmask 255.255.0.0 {  
    range 10.10.30.20 10.10.30.100;  
    option domain-name-servers 10.10.30.13, www.dnsproject.prepa.com;  
    option domain-name "dnsproject.prepa.com";  
    option subnet-mask 255.255.255.224;  
    option routers 10.10.30.13;  
    option broadcast-address 10.10.255.255;  
    default-lease-time 86600;  
    max-lease-time 72600;  
}  
  
# Hosts which require special configuration options can be listed in  
# host statements.  If no address is specified, the address will be  
  
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement  
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne  
Oclation maximum est de 7200 secondes.
```

```
sophie@ubuntu: ~
GNU nano 6.2 /etc/resolv.conf *
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.
nameserver 10.10.30.13
options edns0 trust-ad
search dnsproject.prepa.com

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^_/ Aller ligne
```

```
sophie@ubuntu: ~
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
sophie@ubuntu:~$ sudo nano /etc/dhcp.conf
sophie@ubuntu:~$ sudo nano /etc/dhcpd.conf
sophie@ubuntu:~$ sudo nano dhcpd.conf
sophie@ubuntu:~$ sudo nano /etc/dhcp/dhcpd.conf
sophie@ubuntu:~$ sudo nano /etc/dhcp/dhcpd.conf
sophie@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:3c:b9:69 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.10.30.13/16 brd 10.10.255.255 scope global dynamic noprefixroute ens33
        valid_lft 452sec preferred_lft 452sec
    inet6 fe80::54fc:9535:1160:3a39/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
sophie@ubuntu:~$
```

```
sophie@ubuntu: /etc/bind
GNU nano 6.2 named.conf.local *
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "dnsproject.prepa.com" IN {
    type master;
    file "/etc/bind/db.direct";
};
zone "10.10.in-addr.arpa" IN {
    type master;
    file "/etc/bind/db.inverse";
};
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^_ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

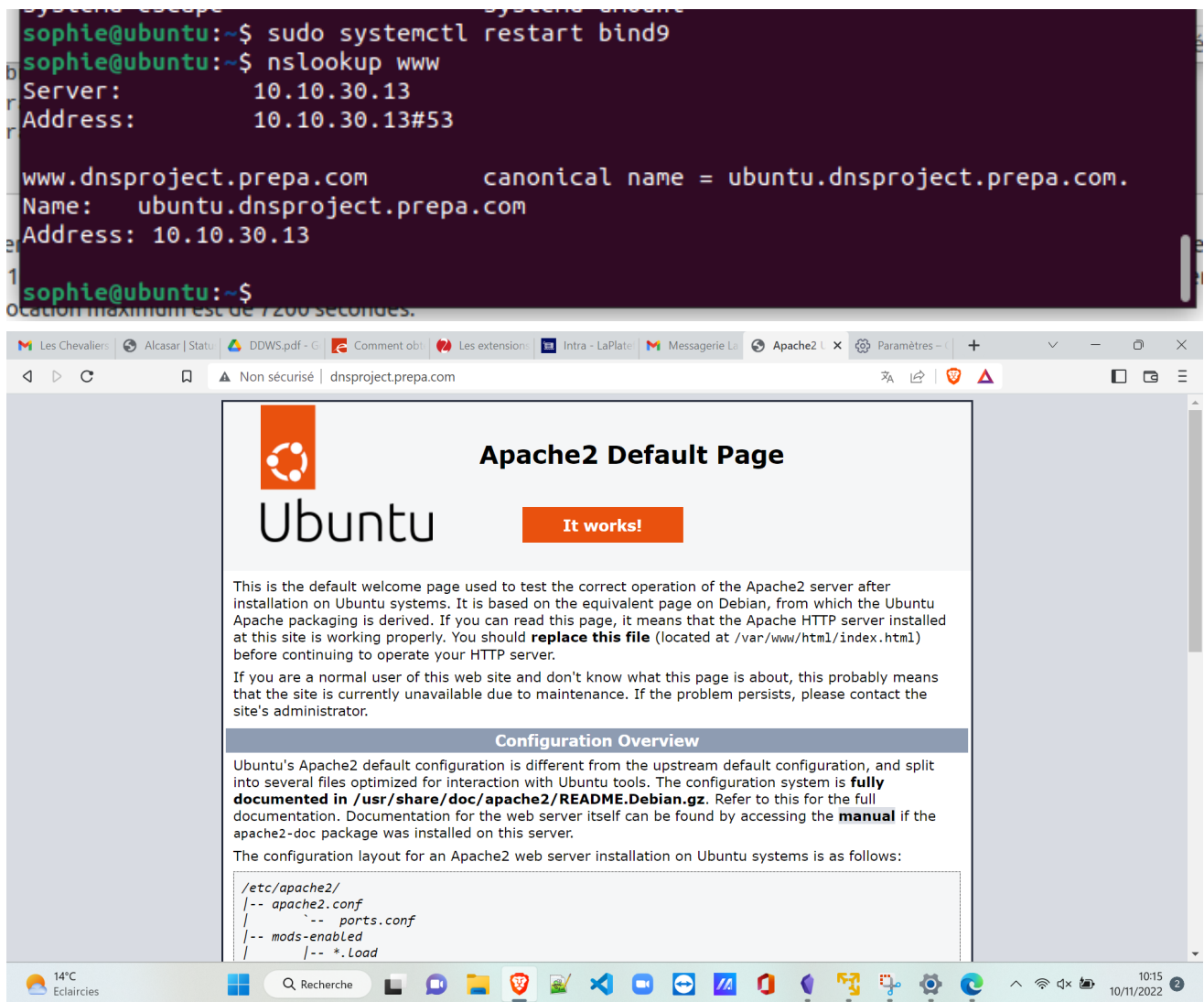
```
sophie@ubuntu: ~
GNU nano 6.2 /etc/dhcp/dhcpd.conf *
#subnet 10.254.239.32 netmask 255.255.255.224 {
#   range dynamic-bootp 10.254.239.40 10.254.239.60;
#   option broadcast-address 10.254.239.31;
#   option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
subnet 10.10.30.0 netmask 255.255.0.0 {
    range 10.10.30.20 10.10.30.100;
    option domain-name-servers 10.10.30.13, www.dnsproject.prepa.com;
    option domain-name "dnsproject.prepa.com";
    option subnet-mask 255.255.255.224;
    option routers 10.10.30.13;
    option broadcast-address 10.10.255.255;
    default-lease-time 86600;
    max-lease-time 72600;
}

# Hosts which require special configuration options can be listed in
# host statements.  If no address is specified, the address will be
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^_ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

Location maximum rest de 7200 secondes.



Job 9

J'ai installé ufw en suivant le tuto suivant :

<https://www.leshirondellesdunet.com/pare-feu-ufw#:~:text=Autoriser%20les%20ping,ping%20ne%20soient%20plus%20autoris%C3%A9s.&text=Pour%20d%C3%A9sactiver%20un%20certain%20type,ligne%20du%20type%20%C3%A0%20d%C3%A9sactiver>

Mais je ne pense pas avoir répondu au Job 9. J'ai compris que même avec un pare-feu (en l'occurrence ufw), il fallait autoriser les ports qui nous intéressent : Apache2, FTP, SSH, DNS, DHCP, HTTP, HTTPS.



```
sophie@ubuntu:~$ sudo ufw enable
[sudo] Mot de passe de sophie :
Le pare-feu est actif et lancé au démarrage du système
sophie@ubuntu:~$ sudo ufw default deny incoming && sudo ufw default deny outgoing
La stratégie par défaut pour le sens « incoming » a été remplacée par « deny »
(veillez à mettre à jour vos règles en conséquence)
La stratégie par défaut pour le sens « outgoing » a été remplacée par « deny »
(veillez à mettre à jour vos règles en conséquence)
sophie@ubuntu:~$ sudo ufw logging on
Journalisation activée
sophie@ubuntu:~$ sudo ufw allow out 53
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out ftp
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out 80/tcp && sudo ufw allow out 443/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out smtp
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out 465/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out pop3
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out pop3s/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out imap
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out imaps/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out 2628/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out 43/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
```

```
sophie@ubuntu:~$ sudo ufw allow out 11371/tcp
```

```
La règle a été ajoutée
```

```
La règle a été ajoutée (v6)
```

```
sophie@ubuntu:~$ sudo ufw status
```

```
État : actif
```

Vers	Action	De
----	-----	--
Apache Full	ALLOW	Anywhere
Apache	ALLOW	Anywhere
Apache Full (v6)	ALLOW	Anywhere (v6)
Apache (v6)	ALLOW	Anywhere (v6)
53	ALLOW OUT	Anywhere
21/tcp	ALLOW OUT	Anywhere
80/tcp	ALLOW OUT	Anywhere
443/tcp	ALLOW OUT	Anywhere
25/tcp	ALLOW OUT	Anywhere
465/tcp	ALLOW OUT	Anywhere
110/tcp	ALLOW OUT	Anywhere
995/tcp	ALLOW OUT	Anywhere
143/tcp	ALLOW OUT	Anywhere
993/tcp	ALLOW OUT	Anywhere
2628/tcp	ALLOW OUT	Anywhere
43/tcp	ALLOW OUT	Anywhere
11371/tcp	ALLOW OUT	Anywhere
53 (v6)	ALLOW OUT	Anywhere (v6)
21/tcp (v6)	ALLOW OUT	Anywhere (v6)
80/tcp (v6)	ALLOW OUT	Anywhere (v6)
443/tcp (v6)	ALLOW OUT	Anywhere (v6)
25/tcp (v6)	ALLOW OUT	Anywhere (v6)
465/tcp (v6)	ALLOW OUT	Anywhere (v6)
110/tcp (v6)	ALLOW OUT	Anywhere (v6)
995/tcp (v6)	ALLOW OUT	Anywhere (v6)
143/tcp (v6)	ALLOW OUT	Anywhere (v6)
993/tcp (v6)	ALLOW OUT	Anywhere (v6)
2628/tcp (v6)	ALLOW OUT	Anywhere (v6)
43/tcp (v6)	ALLOW OUT	Anywhere (v6)
11371/tcp (v6)	ALLOW OUT	Anywhere (v6)


```
sophie@ubuntu: ~
GNU nano 6.2 /etc/ufw/before.rules *
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines

# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp codes for OUTPUT
-A ufw-before-output -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-output -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-output -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-output -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-output -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT

#
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier  ^_ Aller ligne

sophie@ubuntu: ~
sophie@ubuntu:~$ sudo ufw allow out 67/tcp
[sudo] Mot de passe de sophie :
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$ sudo ufw allow out 68/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
sophie@ubuntu:~$
```

```
sophie@ubuntu: ~  
sophie@ubuntu:~$ sudo ufw allow out 67/tcp  
[sudo] Mot de passe de sophie :  
La règle a été ajoutée  
La règle a été ajoutée (v6)  
sophie@ubuntu:~$ sudo ufw allow out 68/tcp  
La règle a été ajoutée  
La règle a été ajoutée (v6)  
sophie@ubuntu:~$ sudo nano /etc/ufw/before.rules  
sophie@ubuntu:~$ sudo ufw allow from 192.168.202.2  
La règle a été ajoutée  
sophie@ubuntu:~$ sudo ufw allow to 192.168.202.2  
La règle a été ajoutée  
sophie@ubuntu:~$ sudo apt -y install gufw  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les NOUVEAUX paquets suivants seront installés :  
  gufw  
0 mis à jour, 1 nouvellement installés, 0 à enlever et 7 non mis à jour.  
Il est nécessaire de prendre 954 ko dans les archives.  
Après cette opération, 3 673 ko d'espace disque supplémentaires seront utilisés.  
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy/universe amd64 gufw all 22.04.0-0ubuntu1 [954 kB]  
954 ko réceptionnés en 0s (3 362 ko/s)  
Sélection du paquet gufw précédemment désélectionné.  
(Lecture de la base de données... 202873 fichiers et répertoires déjà installés.)  
Préparation du dépaquetage de .../gufw_22.04.0-0ubuntu1_all.deb ...  
Dépaquetage de gufw (22.04.0-0ubuntu1) ...  
Paramétrage de gufw (22.04.0-0ubuntu1) ...  
Traitement des actions différées (« triggers ») pour mailcap (3.70+nmu1ubuntu1) ...  
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.26-1ubuntu3) ...  
Traitement des actions différées (« triggers ») pour hicolor-icon-theme (0.17-2) ...  
Traitement des actions différées (« triggers ») pour gnome-menus (3.36.0-1ubuntu3) ...  
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
```

Annuler

Filaire

Appliquer

Détails

Identité

IPv4

IPv6

Sécurité

Vitesse de la connexion

1000 Mb/s

Adresse IPv4

192.168.202.128

Adresse IPv6

fe80::54fc:9535:1160:3a39

Adresse matérielle

00:0C:29:3C:B9:69

Route par défaut

192.168.202.2

DNS

192.168.202.2

☒ Connexion automatique

☒ Rendre accessible aux autres utilisateurs

☐ Connexion avec quota : limite les données ou peut engendrer des frais

Les mises à jour logicielles et autres téléchargements importants ne seront pas démarrés automatiquement.