

SISR - Administration du parc informatique avec SAMBA sous Ubuntu Server 18.04

- [Mission](#)
- [Mise en place](#)

Mission

Le serveur répondra aux services suivants :

- serveur contrôleur d'un domaine (étape 5)
- serveur DNS (étape 1)
- serveur DHCP (étape 1)
- gestion des utilisateurs (étape 5)
- script d'ouverture de session (étape 5)
- partages de dossiers avec Samba (étape 4)
- administration du serveur à distance avec Webmin (étape 3)
- administration du serveur à distance avec putty (étape 1)
- serveur Web (étape 2)
- mise en production de Moodle (étape 2)
- partage d'accès internet (étape 1)
- et protection du serveur en utilisant un parefeu (étape 3)

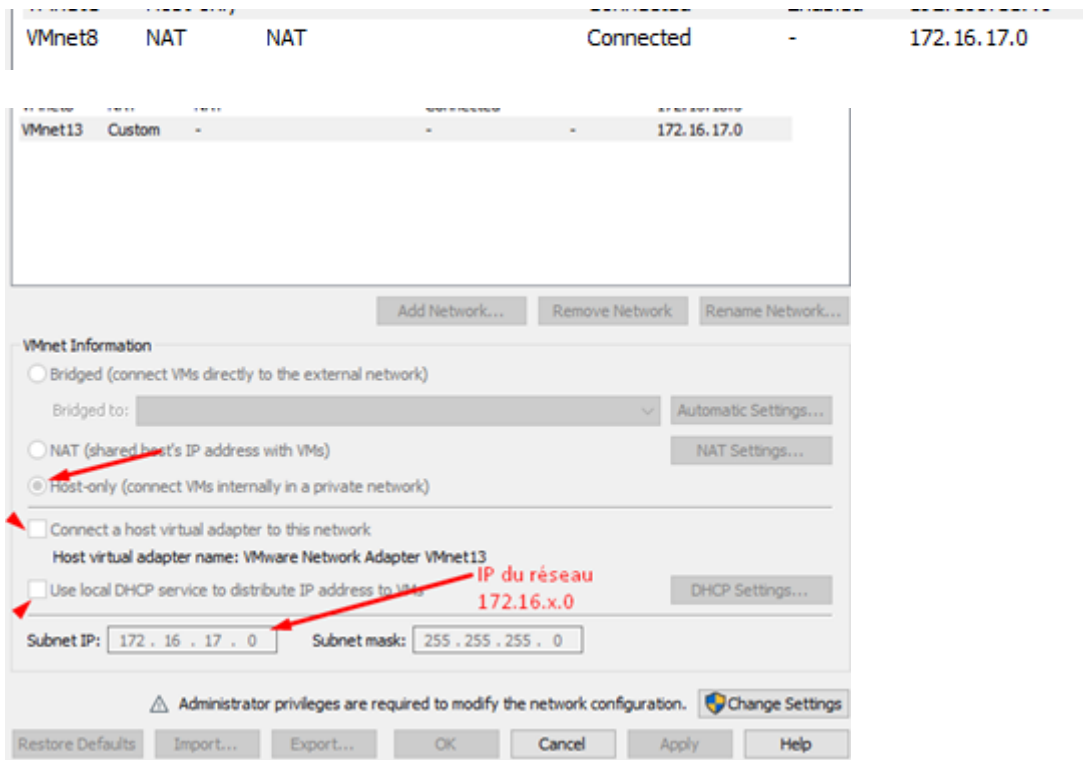
Le serveur sera un Ubuntu Server 18.04.

Mise en place

Préparation de VMware

Edit > Virtual Network Editor

On créer un VMnet, par exemple le 13.



On décoche les deux cases, on prend host-only et on met le masque + IP.

Préparation du serveur

Pour la machine virtuelle, on ajoute deux cartes réseaux : une en bridge pour l'accès internet et l'autre, celle que l'on a créé.

Modification des cartes réseaux : nano /etc/netplan/*.yaml

```

network:
  ethernet:
    ens33:
      addresses:
        - 192.168.0.200/24
      gateway4: 192.168.0.254
      nameservers:
        addresses:
          - 192.168.0.254
          - 192.168.0.1
    ens34:
      addresses:
        - 172.16.17.1/24
      nameservers:
        addresses:
          - 127.0.0.1
  version: 2

```

```

hostname
nano /etc/hostname
/etc/init.d/hostname.sh start

```

On complète le fichier hosts. Le serveur sera client et serveur DNS.

```

nano /etc/host.conf

order hosts, bind
multi on

```

On complète le fichier hosts.

```

nano /etc/hosts

```

```

127.0.0.1      localhost.ab.org      localhost
172.16.17.1    abubuntusrv.ab.org abubuntusrv
172.16.17.2    client1
172.16.17.3    client2

# 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

```

On déclare le nom de domaine dans /etc/resolv.conf

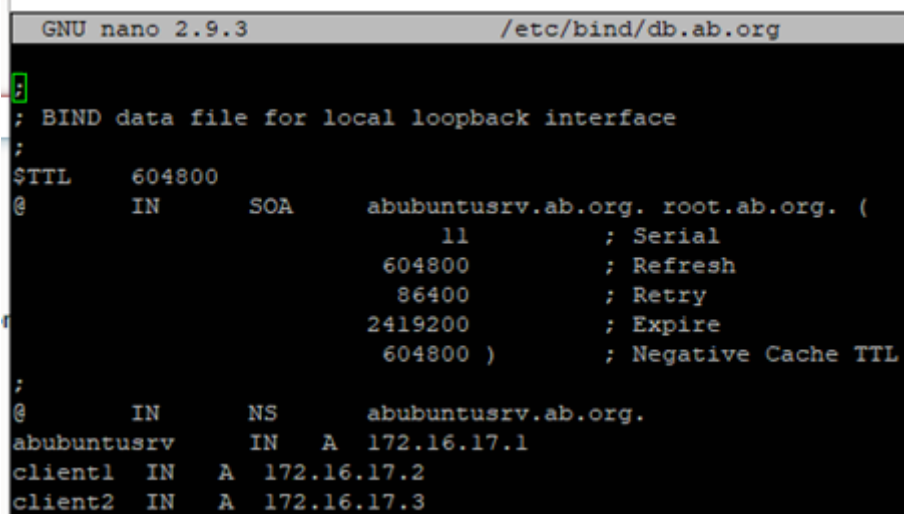
```

nano /etc/resolv.conf

```

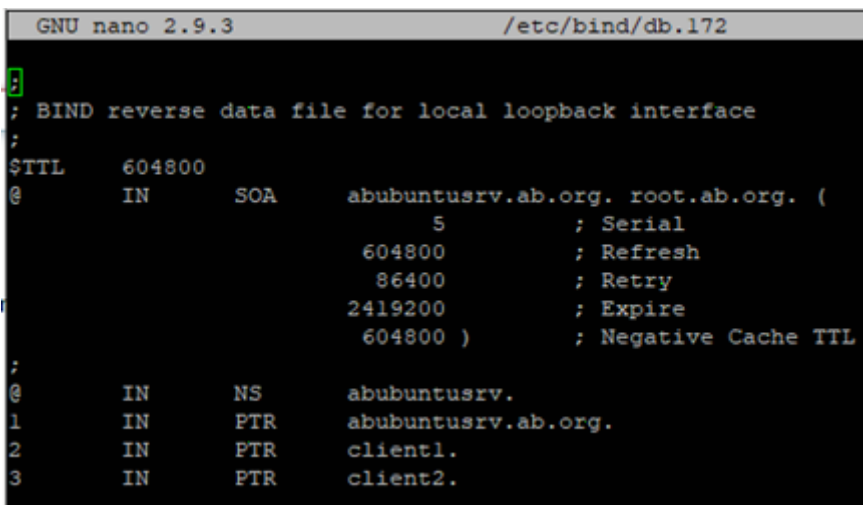
Installation et paramétrage du serveur DNS

```
apt-get install bind9
cp /etc/bind/db.local /etc/bind/db.ab.org
nano /etc/bind/db.ab.org
```



```
GNU nano 2.9.3 /etc/bind/db.ab.org
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      abubuntusrv.ab.org. root.ab.org. (
                        11      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       abubuntusrv.ab.org.
abubuntusrv IN     A       172.16.17.1
client1   IN     A       172.16.17.2
client2   IN     A       172.16.17.3
```

```
cp /etc/bind/db.127 /etc/bind/db.172
nano /etc/bind/db.172
```



```
GNU nano 2.9.3 /etc/bind/db.172
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      abubuntusrv.ab.org. root.ab.org. (
                        5      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       abubuntusrv.
1         IN      PTR      abubuntusrv.ab.org.
2         IN      PTR      client1.
3         IN      PTR      client2.
```

```
nano /etc/bind/named.conf.local
```

```
GNU nano 2.9.3 /etc/bind/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 "ab.org" {
    type master;
    file "/etc/bind/db.ab.org";
    allow-query { any; };
};
zone "17.16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172";
};
```

nano /etc/bind/named.conf.options

```
/options {
    //directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    // 0.0.0.0;
    // };

    //=====
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        192.168.0.1;
        192.168.0.254;
        8.8.8.8;
        8.8.4.4;
        // 212.27.40.240;
        // 212.27.40.241;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    auth-nxdomain no;    # conform to RFC1035
    version none;
    forward only;
    // listen-on-v6 { any; };
};
```

service bind9 restart

nano /etc/bind/db.ab.org

```

GNU nano 2.9.3 /etc/bind/db.ab.o
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      abubuntusrv.ab.org. root.ab.org. (
                        11      ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       abubuntusrv.ab.org.
abubuntusrv      IN      A   172.16.17.1
client1  IN      A   172.16.17.2
client2  IN      A   172.16.17.3

```

```
nano /etc/bind/db.192
```

```

GNU nano 2.9.3 /etc/bind/db.192
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      abubuntusrv.ab.org. root.ab.org. (
                        3       ; Serial
                        604800   ; Refresh
                        86400    ; Retry
                        2419200  ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       abubuntusrv.
1         IN      PTR      abubuntusrv.ab.org.

```

```
/etc/init.d/bind9 restart
```

Vérifications si le DNS se connaît lui-même

```

hostname
nslookup
>abubuntusrv

```



```
> abubuntusrv
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   abubuntusrv
Address: 172.16.17.1
> █
```

On teste en inversée

```
nslookup
> 172.16.17.1
```

```
> 172.16.17.1
1.17.16.172.in-addr.arpa      name = abubuntusrv.ab.org.
1.17.16.172.in-addr.arpa      name = abubuntusrv.
```

Avec dig :

```
root@abubuntusrv:/home/abonnet# dig abubuntusrv

; <<>> DiG 9.11.3-lubuntu1.11-Ubuntu <<>> abubuntusrv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12646
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;abubuntusrv.                IN      A

;; ANSWER SECTION:
abubuntusrv.                0      IN      A      172.16.17.1

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Feb 08 23:20:31 UTC 2020
;; MSG SIZE  rcvd: 56
```

```
root@abubuntusrv:/home/abonnet# dig ab.org

; <<>> DiG 9.11.3-lubuntul.11-Ubuntu <<>> ab.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35697
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ab.org.                IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Feb 08 23:20:50 UTC 2020
;; MSG SIZE rcvd: 35
```

```
root@abubuntusrv:/home/abonnet# dig -x @172.16.17.1

; <<>> DiG 9.11.3-lubuntul.11-Ubuntu <<>> -x @172.16.17.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4972
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;1.17.16.\@172.in-addr.arpa.  IN      PTR

;; Query time: 287 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Feb 08 23:21:04 UTC 2020
;; MSG SIZE rcvd: 54
```

Vérification si le dns connait le/les client(s)

nslookup

Client1

```
> client1
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   client1
Address: 172.16.17.2
> 172.16.17.2
2.17.16.172.in-addr.arpa      name = client1.

Authoritative answers can be found from:
```

Installation du poste Ubuntu

On clique sur installer ubuntu puis on suit la procédure.

Configuration du client

On change le nom du périphérique dans les options pour client1 (=nom dans dns)

On édite le fichier host.

```
nano /etc/host.conf
```

Dans le fichier on aura :

```
order hosts,bind
```

```
multi on
```

On renseigne l'ip du dns dans les paramètres réseaux, on dite le fichier /etc/resolv.conf

```
nano /etc/resolv.conf
```

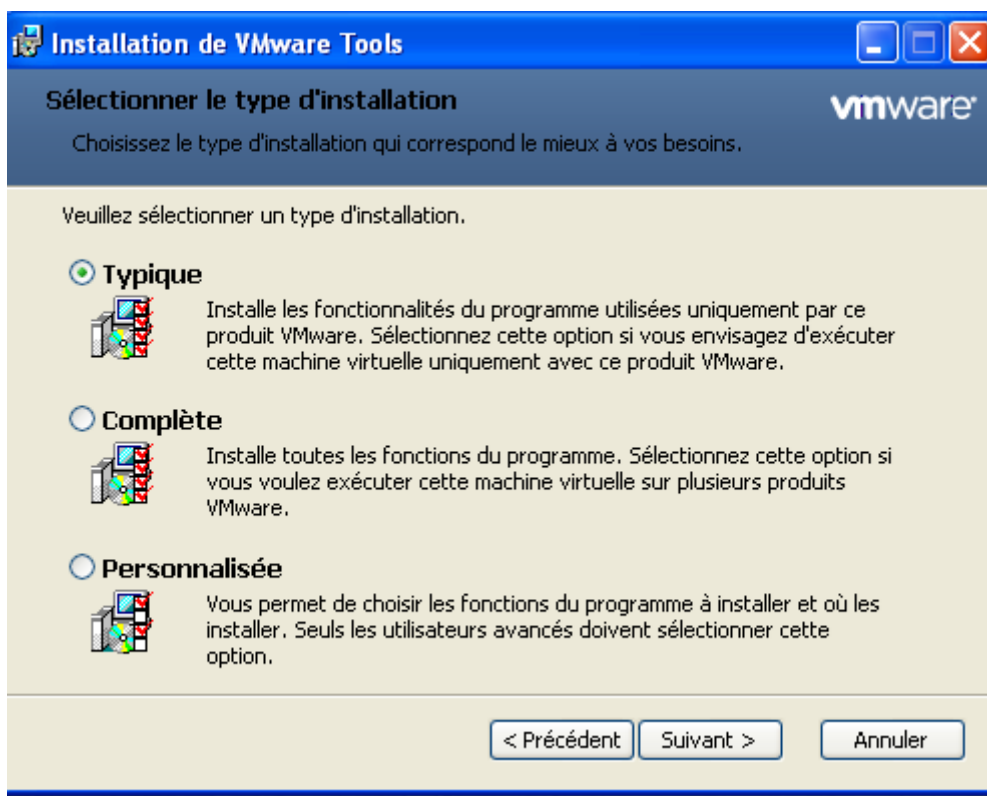
```
domain ab.org
```

search ab.org

nameserver 172.16.17.1

Installation du poste Windows XP

On met l'iso de Windows XP. On presse entrée, on accepte avec F8 puis on rentre toutes les informations demandées. Une fois Windows installé, on installe les VMware Tools pour le confort.



On fait suivant puis installer.

Installation du serveur DHCP

```
sudo apt install isc-dhcp-server
```

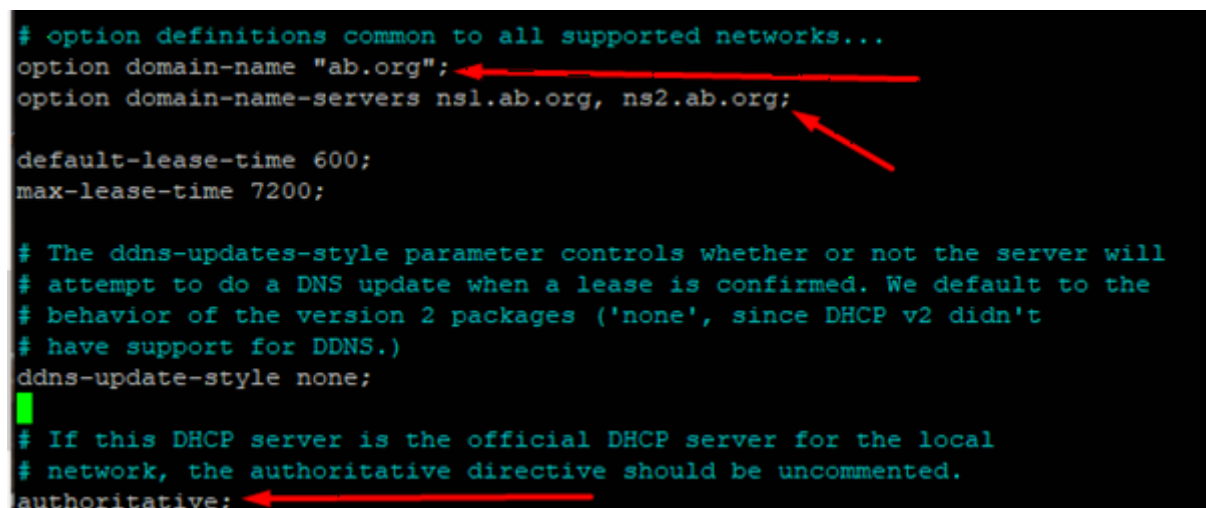
```
sudo vim /etc/default/isc-dhcp-serverINTERFACESv4="ens34"sudo vim /etc/dhcp/dhcpd.conf
```

Change the domain name and domain name servers (DNS) according to yours in the section mentioned below:

```
# option definitions common to all supported networks... option domain-name "your_domain.com";  
option domain-name-servers ns1.your_domain.com, ns2.your_domain.com;
```

If this DHCP server is the official DHCP server for the local network, the authoritative directive should be uncommented.

```
authoritative;
```



```
# option definitions common to all supported networks...  
option domain-name "ab.org";  
option domain-name-servers ns1.ab.org, ns2.ab.org;  
  
default-lease-time 600;  
max-lease-time 7200;  
  
# The ddns-updates-style parameter controls whether or not the server will  
# attempt to do a DNS update when a lease is confirmed. We default to the  
# behavior of the version 2 packages ('none', since DHCP v2 didn't  
# have support for DDNS.)  
ddns-update-style none;  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
authoritative;
```

Mettre abubuntusrv au lieu de ns1 et enlever ns2.ab.org

```
subnet 172.16.17.0 netmask 255.255.255.0 {  
    range 172.16.17.100 172.16.17.110;  
    option domain-name-servers ns1.ab.org;  
    option domain-name "ab.org";  
    option subnet-mask 255.255.255.0;  
    option routers 172.16.17.1;  
    option broadcast-address 172.16.17.255;  
    default-lease-time 600;  
    max-lease-time 7200;  
}
```

Option domain-name-servers abubuntusrv.ab.org

```
sudo service isc-dhcp-server start
```

```
sudo systemctl status isc-dhcp-server.service
```

```
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-02-07 19:11:54 UTC; 2s ago
     Docs: man:dhcpcd(8)
    Main PID: 1776 (dhcpcd)
      Tasks: 1 (limit: 2312)
   CGroup: /system.slice/isc-dhcp-server.service
           └─1776 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server/dhcpcd.pid -cf /etc/dhcp/dhcpcd.conf
```

```
C:\Documents and Settings\alexis>ipconfig /release
```

Configuration IP de Windows

Carte Ethernet Connexion au réseau local:

```
Suffixe DNS propre à la connexion :
Adresse IP. . . . . : 0.0.0.0
Masque de sous-réseau . . . . . : 0.0.0.0
Passerelle par défaut . . . . . :
```

```
C:\Documents and Settings\alexis>ipconfig /renew
```

Configuration IP de Windows

Carte Ethernet Connexion au réseau local:

```
Suffixe DNS propre à la connexion : ab.org
Adresse IP. . . . . : 172.16.17.100
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 172.16.17.1
```

Installation et configuration du proxy : Squid

Installation

```
sudo apt-get install squid
```

Configuration

```
sudo nano /etc/squid/squid.conf
```

On ajoute après la ligne « acl CONNECT » :

```
acl lan src 172.16.17.0/24
```

Après « http_access allow localhost manager »:

```
http_access allow lan
```

On gère les headers.

Après la ligne : « TAG : request_header_access » :

```
request_header_access Via deny all
```

```
request_header_access X-Forwarded-For deny all
```

```
request_header_access Referer deny all
```

```
request_header_access Cache-Control deny all
```

```
sudo systemctl restart squid
```

```
sudo systemctl enable squid
```

Port par défaut = 3128. On le voit « http_port 3128 ».

On voit si c'est fonctionnel :

```
ss -tunelp | grep 3128
```

Pare-feu

On configure le pare-feu :

```
sudo firewall-cmd --add-service=squid --permanent
```

```
sudo firewall-cmd --reload
```

Ajout du proxy sur les clients

Ajout du Ubuntu Desktop

Installation du serveur web

```
apt install apache2 mysql-client mysql-server php libapache2-mod-php sudo apt-get install php-imap php-ldap php-curl php-xmlrpc php-gd php-mysql php-cas
```

```
sudo mysql_secure_installation
```

Pour la dernière commande, on nous demande le mot de passe de mysql. On rentre Y à chaque fois.

Installation de phpmyadmin

```
apt-get install phpmyadmin
```

On choisit apache2 avec la barre espace. Puis non.

On modifie ensuite le mot de passe de phpmyadmin :

```
sudo mysql -u root -p
```

On modifie new-password par le mot de passe souhaité.

- ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'new-password';

- exit

```
sudo service mysql stop
```

```
sudo service mysql start
```

Installation de moodle

```
apt install graphviz aspell ghostscript clamav php7.2-pspell php7.2-curl php7.2-gd php7.2-intl  
php7.2-mysql php7.2-xml php7.2-xmlrpc php7.2-ldap php7.2-zip php7.2-soap php7.2-mbstring
```

```
service apache2 restart
```

```
apt install git
```

```
cd /opt
```

```
git clone git://git.moodle.org/moodle.git
```

```
cd moodle
```

```
git branch -a
```

```
git branch --track MOODLE_38_STABLE origin/MOODLE_38_STABLE
```

```
git checkout MOODLE_38_STABLE
```

```
cp -R /opt/moodle /var/www/html/
```

```
mkdir /var/moodledata
```

```
chown -R www-data /var/moodledata
```

```
chmod -R 777 /var/moodledata
```

```
chmod -R 0755 /var/www/html/moodle
```

```
nano /etc/mysql/mysql.conf.d/mysqld.cnf
```

Dans la catégorie [mysqld], rajouter ces lignes en plus :

```
default_storage_engine = innodb
```

```
innodb_file_per_table = 1
```

```
innodb_file_format = Barracuda
```

```
service mysql restart
```

Ci-dessous, on remplace moodledude par un nom d'utilisateur et passwordformoodledude par un mot de passe.

```
mysql -u root -p
```

- CREATE DATABASE moodle DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
- create user 'moodledude'@'localhost' IDENTIFIED BY 'passwordformoodledude';
- GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,CREATE TEMPORARY TABLES,DROP,INDEX,ALTER ON moodle.* TO moodledude@localhost IDENTIFIED BY 'passwordformoodledude';
- quit;

```
chmod -R 777 /var/www/html/moodle
```

On se rend sur l'interface web. 172.16.17.1/moodle

Chemin pour moodledata : /var/moodledata

Database type : mysql

Database Settings :

Host server: localhost

Database: moodle

User: moodledude (the user you created when setting up the database)

Password: passwordformoodledude (the password for the user you created)

Tables Prefix: mdl_

On poursuit.

```
chmod -R 0755 /var/www/html/moodle
```

Administration > Server > System Paths

Path to du: /usr/bin/du

Path to aspell: /usr/bin/aspell

Path to dot: /usr/bin/dot

Save Changes

mkdir /var/quarantine

chown -R www-data /var/quarantine

Site Administration > Plugins > Antivirus plugins > Manage antivirus plugins

Activer

On change ensuite l'ip du serveur car il est en 192.168.0.200 de base.

cd /var/www/html/moodle

nano config.php

On change la ligne \$CFG->wwwroot = 'http://172.16.17.1/moodle' ;

Installation de Webmin

Webmin n'a pas besoin d'apache pour fonctionner. Webmin est fourni avec un simple serveur web nommé miniserv.py. Selon la documentation de Webmin, l'installer sous Apache impacterait les performances. Cela n'est pas recommandé.

Pour installer Webmin sur un serveur Ubuntu 16.04, on commence par installer quelques dépendances :

```
sudo apt-get install -y perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions python libwww-perl liblwp-protocol-https-perl
```

On ajoute la clef pour vérifier l'intégrité des paquets du dépôt de Webmin:

```
sudo wget -O- http://www.webmin.com/jcameron-key.asc | sudo apt-key add -
```

On ajoute les dépôts à la fin du fichier sources.list :

```
sudo nano /etc/apt/sources.list
```

```
#Webmin
```

```
deb http://download.webmin.com/download/repository sarge contrib
```

```
deb http://webmin.mirror.somersettechsolutions.co.uk/repository sarge contrib
```

Il ne reste plus qu'à mettre à jour la liste des paquets :

```
sudo apt-get update
```

Et à l'installer :

```
sudo apt-get install webmin
```

Webmin est ensuite disponible à l'adresse suivante :

<https://172.16.17.1:10000/>

On rentre les identifiants du serveur.

Voici l'interface obtenue.

Pare-feu

ufw enable

ufw app list

ufw allow in "nom de l'application"

EXEMPLE : ufw allow in "Apache Full"

On autorise SSH, Apache Full, Squid, Samba, Bind9...

Environnement graphique

```
apt-get install gufw
```

Il faut ensuite avoir Putty et Xmind sur le windows.

<https://sourceforge.net/projects/xming/files/latest/download>

On lance XLaunch et on coche « No Access Control”.

On se connecte avec putty et on rentre les commandes suivantes :

```
export DISPLAY=IPDUWINDOWS:0.0
```

```
/usr/bin/gufw-pkexec -ssh
```

Par défaut UFW autorise les requêtes de ping (ICMP Echo Requests). Il faut éditer /etc/ufw/before.rules et remplacer les « ACCEPT » par « DROP » aux lignes suivantes :

Samba

```
Apt-get install samba
```

```
Apt-get install system-config-samba
```

```
Export DISPLAY=IPDUWINDOWS:0.0
```

```
addgroup prof
```

```
addgroup cadre
```

```
addgroup eleve
```

```
adduser xgramine
```

```
adduser rduverver
```

```
...
```

```
adduser xgramine prof
```

```
...
```

```
smbpasswd -a xgramine
```

On définit un mdp

Dans l'interface graphique, on clique sur ajouter un partage, naviguer et dans File System et home, on crée un dossier pour chaque utilisateur.

<https://debian-facile.org/atelier:chantier:samba-partage-reseau>