



*Mise en place d'une solution de supervision  
réseau  
basée sur Zabbix*

Rédigé par :  
**Zyad MOUTAOUAKIL**  
**BTS SIO**

**Année: 2026**

## SOMMAIRE

<b><i>Introduction.....</i></b>	<b><i>1</i></b>
<b><i>Architecture réseau.....</i></b>	<b><i>1</i></b>
<b><i>Plan d'adressage IP.....</i></b>	<b><i>2</i></b>
<b><i>Configuration réseau de VMWare Workstation.....</i></b>	<b><i>2</i></b>
<b><i>Création des machines virtuelles.....</i></b>	<b><i>3</i></b>
<b><i>Installation du système d'exploitation.....</i></b>	<b><i>6</i></b>
<b><i>Configuration du serveur DHCP.....</i></b>	<b><i>9</i></b>
<b><i>Configuration du serveur DNS.....</i></b>	<b><i>13</i></b>
<b><i>Configuration du serveur Zabbix.....</i></b>	<b><i>17</i></b>
<b><i>Installation et configuration des agents sur DHCP_SERVER et DNS_SERVER.....</i></b>	<b><i>21</i></b>
<b><i>Test de fonctionnement.....</i></b>	<b><i>23</i></b>

## Introduction

Ce laboratoire a pour objectif principal la **mise en place d'une solution de supervision des systèmes Linux à l'aide de Zabbix** dans un environnement virtualisé avec **VMware Workstation**. Il s'appuie sur une infrastructure réseau comprenant des serveurs Linux jouant des rôles essentiels tels que **DHCP** et **DNS**, qui serviront de cibles à superviser.

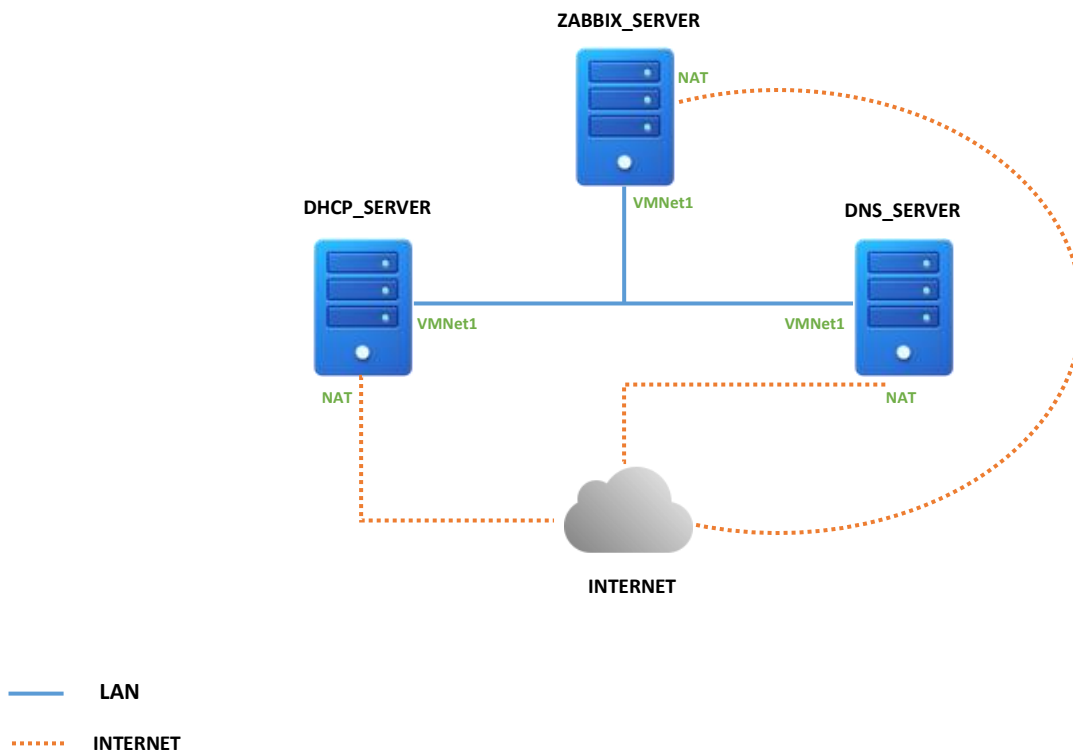
À travers ce lab, l'apprenant découvrira les étapes nécessaires à l'installation et à la configuration du **serveur Zabbix**, ainsi que le déploiement des **agents Zabbix** sur des machines Linux. L'accent est mis sur la collecte, l'analyse et la visualisation des métriques système afin de surveiller l'état global du réseau, détecter les anomalies et assurer la disponibilité des services. Ce travail pratique permet ainsi d'acquérir des compétences concrètes en **supervision, administration réseau et gestion des infrastructures Linux**.

### Outils utilisés :

- VMware Workstation Pro 17
- Ubuntu 22.04

## Architecture réseau

Le schéma suivant montre la structure globale de l'infrastructure réseau du laboratoire.



## Plan d'adressage IP

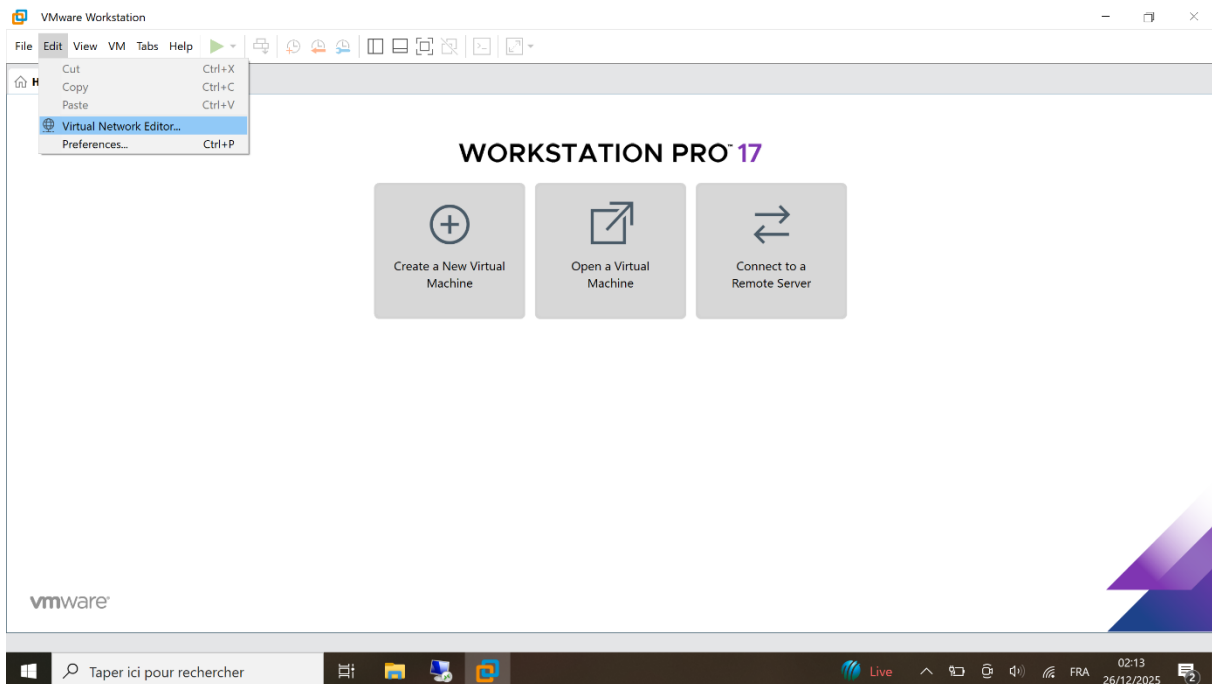
Le plan d'adressage constitue une étape essentielle dans la mise en place de l'infrastructure du laboratoire. Le tableau ci-dessous présente le détail de l'adressage IP utilisé, garantissant une bonne organisation du réseau et facilitant la configuration, la supervision et le dépannage des services.

Adresse IP	Masque de sous-réseau	Adresse DNS	Machine Virtuelle
192.168.20.2	255.255.255.0	192.168.20.3	DHCP_SERVER
192.168.20.3	255.255.255.0	-	DNS_SERVER
192.168.20.4	255.255.255.0	192.168.20.3	ZABBIX_SERVER

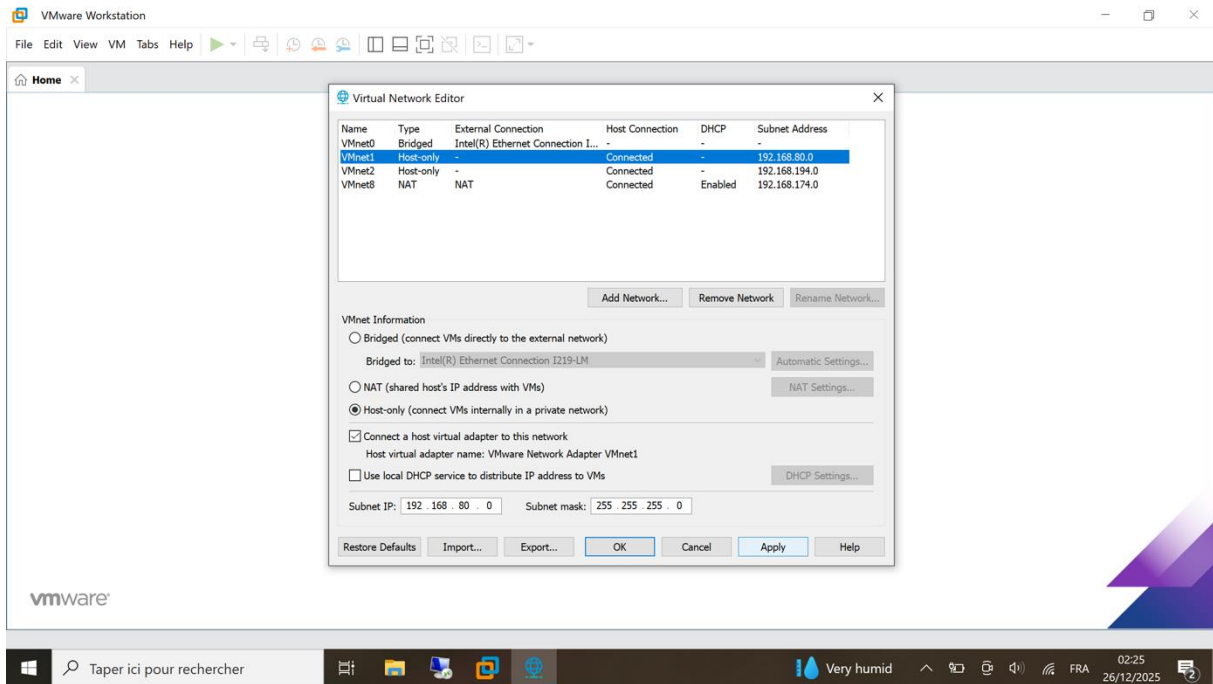
## Configuration réseau de VMWare Workstation

Avant de commencer, il est nécessaire de désactiver le service DHCP intégré à VMware dans les paramètres réseau. Cette étape permet d'éviter tout conflit d'adressage IP avec le serveur DHCP que nous allons installer et configurer au cours de ce lab.

Pour ce faire, ouvrez VMWare > Edit > Virtual Network Editor.

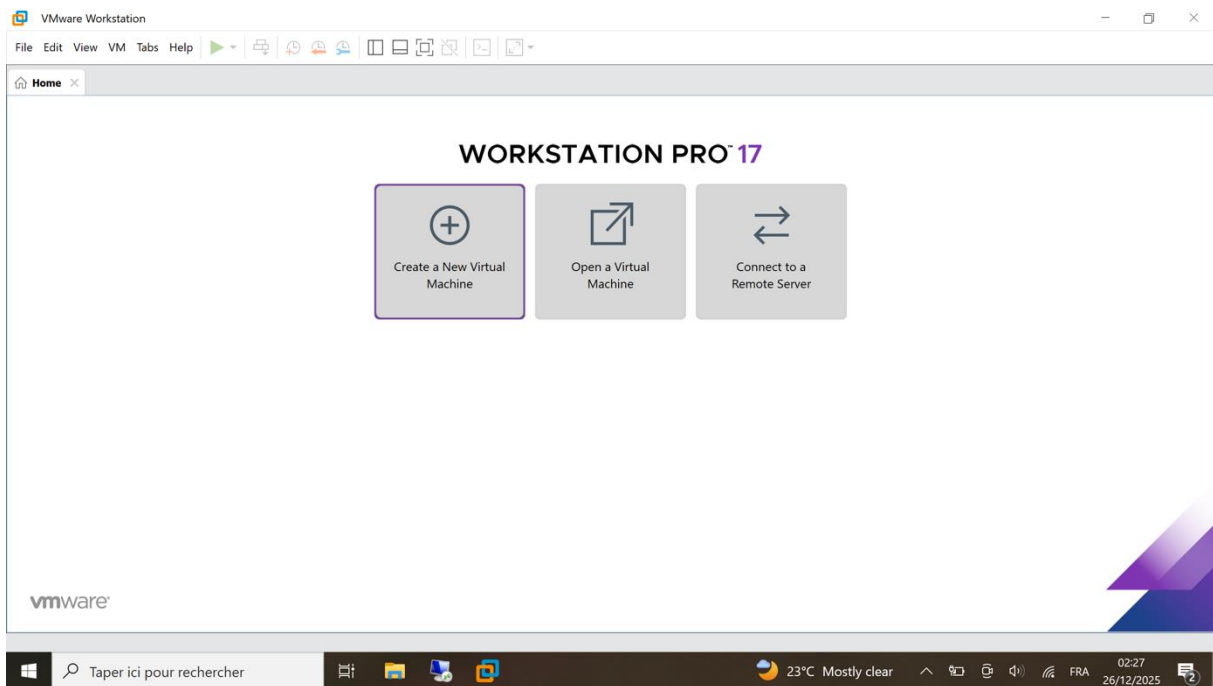


Dans la fenêtre qui s'affiche, cliquez sur Change settings > Sélectionnez la carte VMnet1 > Décochez l'option Use local DHCP service to distribute IP address to VMs.

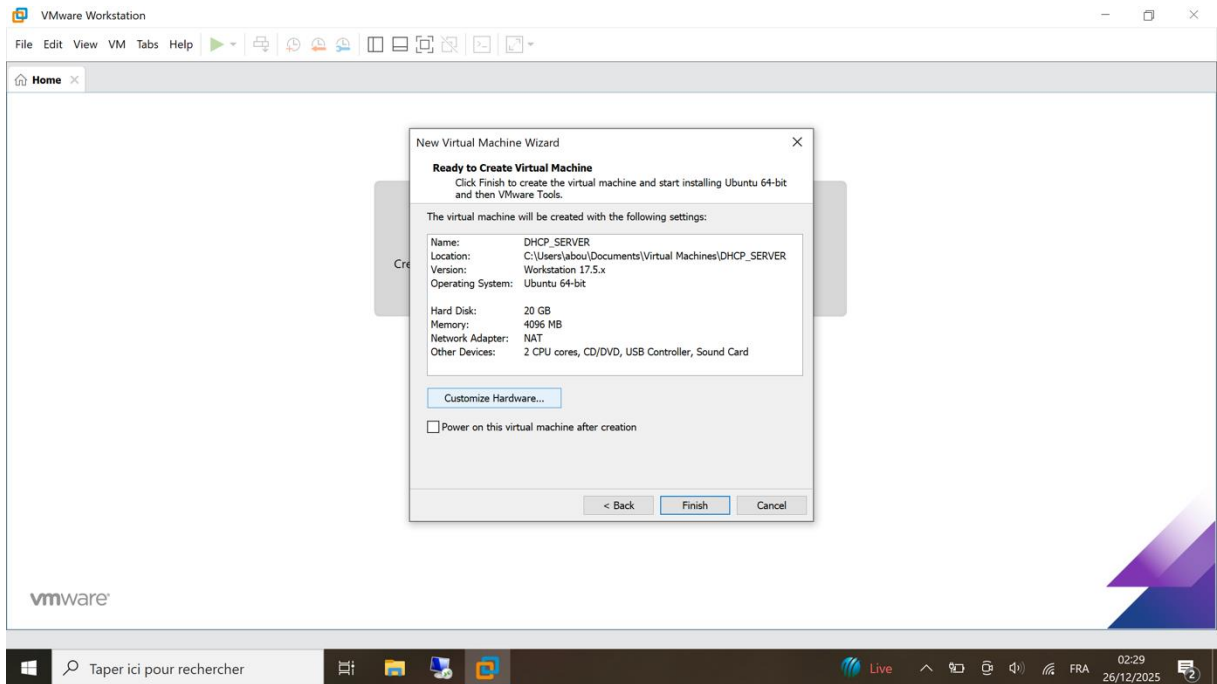


## Création des machines virtuelles

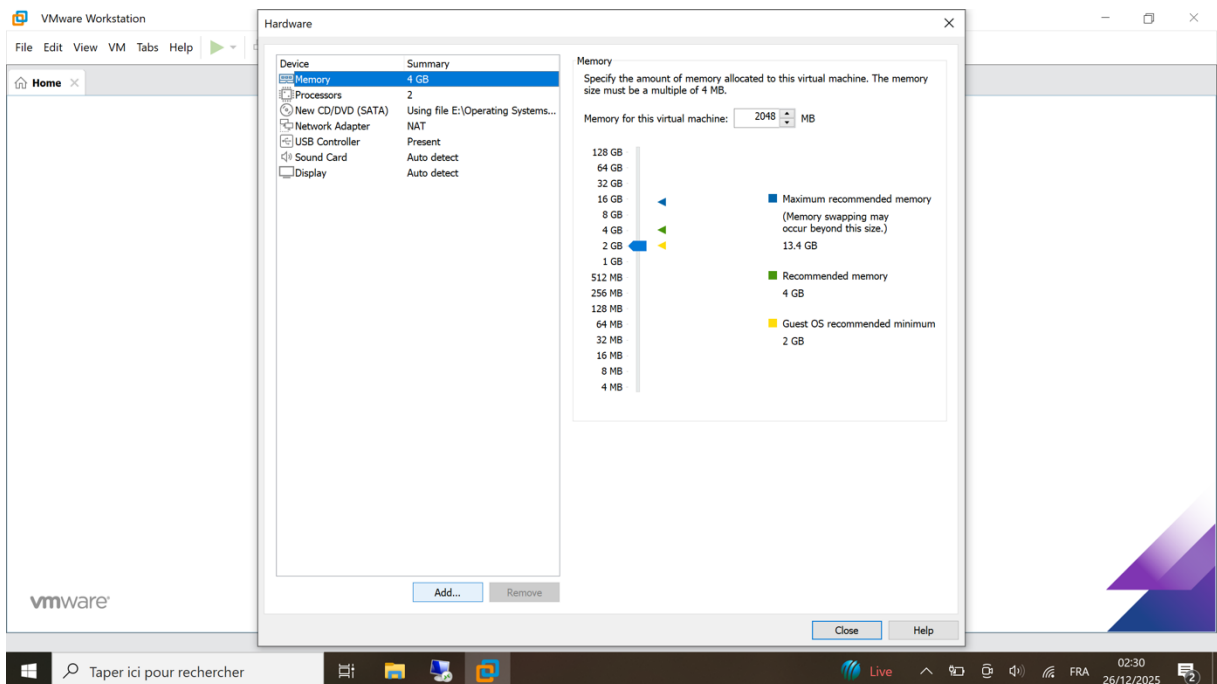
Pour créer une machine virtuelle, cliquez sur Create a New Virtual Machine > Cochez l'option Typical (Recommended) > Installer disc image file (iso) > Cliquez sur Browse puis parcourez vos répertoires afin de sélectionner l'image iso d'Ubuntu > Renseignez le nom d'utilisateur (en minuscule) et mot de passe > Nommer cette machine DHCP\_SERVER > Laissez la taille du disque à 20GB puis cochez l'option Store virtual disk as a single file.



Vous obtenez le récapitulatif des configurations de votre machine comme le montre la figure suivante :

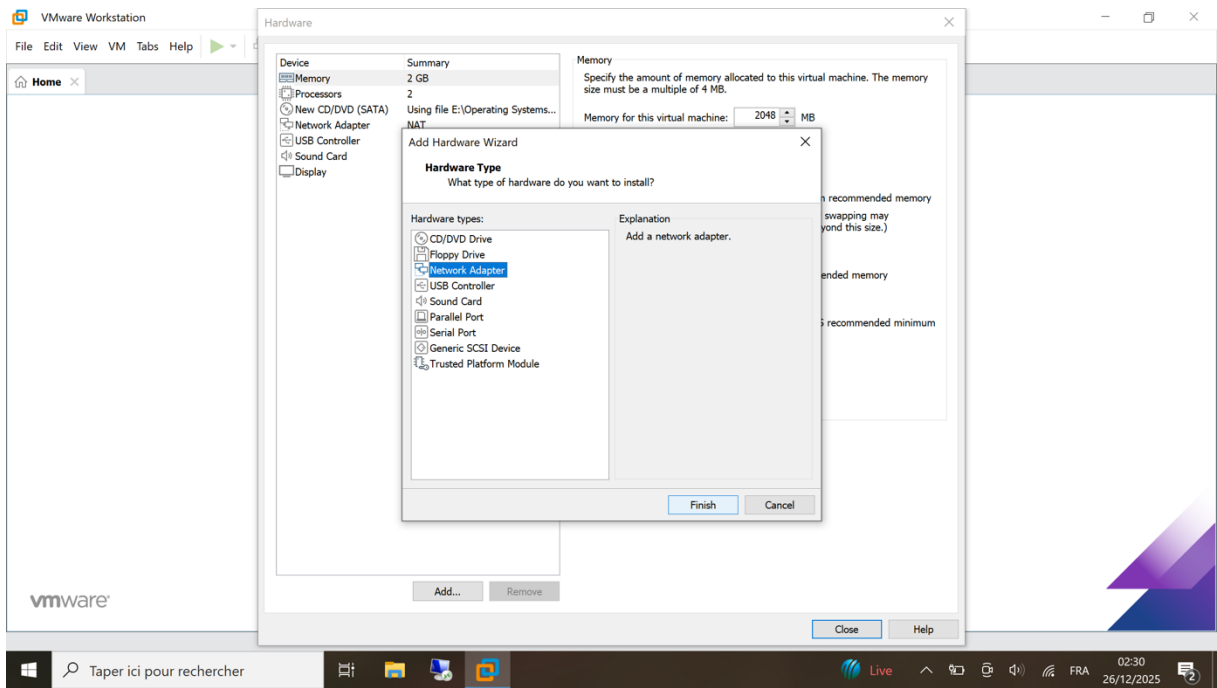


Afin d'optimiser les ressources, nous allons réduire la taille de la mémoire RAM à 2GB. Pour ce faire, cliquez sur **Customize Hardware** puis faire glisser le curseur vers le bas à 2GB.

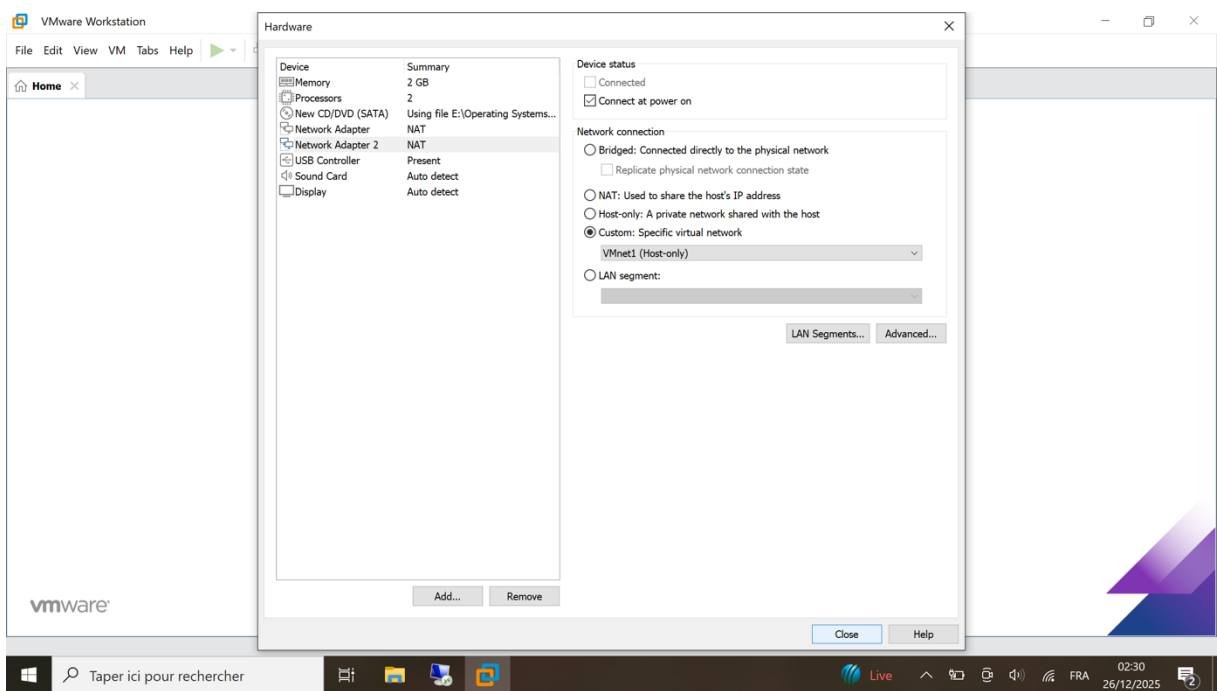


Ensuite, nous allons ajouter une **deuxième carte réseau** au serveur afin qu'elle joue le rôle de **réseau LAN (Host-Only)**, la première carte étant utilisée pour le **WAN (NAT)**.

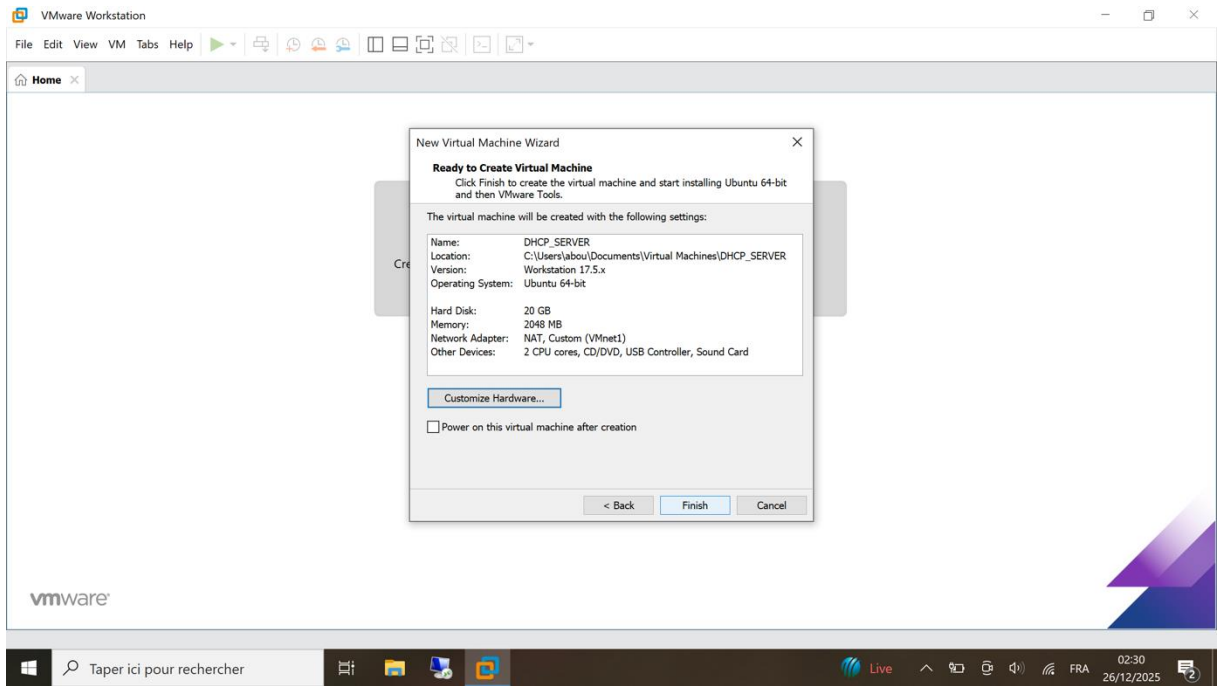
Pour ce faire, cliquez sur Add > Sélectionner Network Adapter > Finish.



Dans l'onglet à droite, sélectionnez l'option Custom: Specific virtual network > VMnet1 (Host-only) > Close.



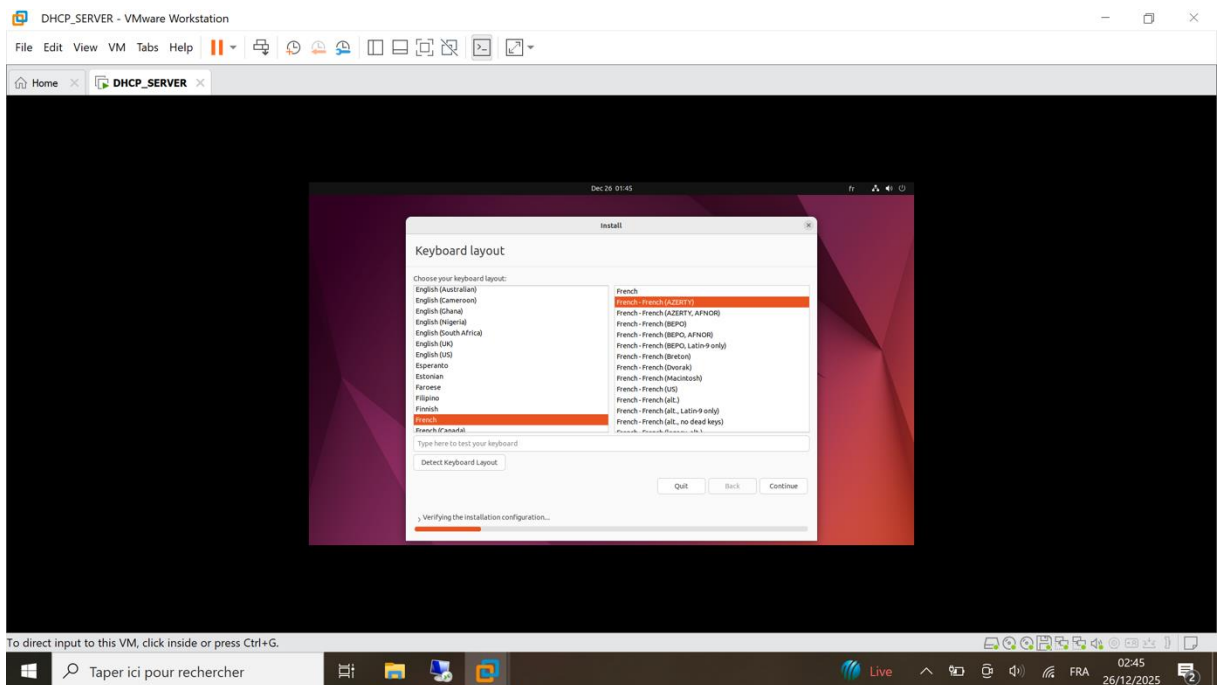
Tout ceci étant fait, cliquez sur finish pour confirmer la création de la machine virtuelle.



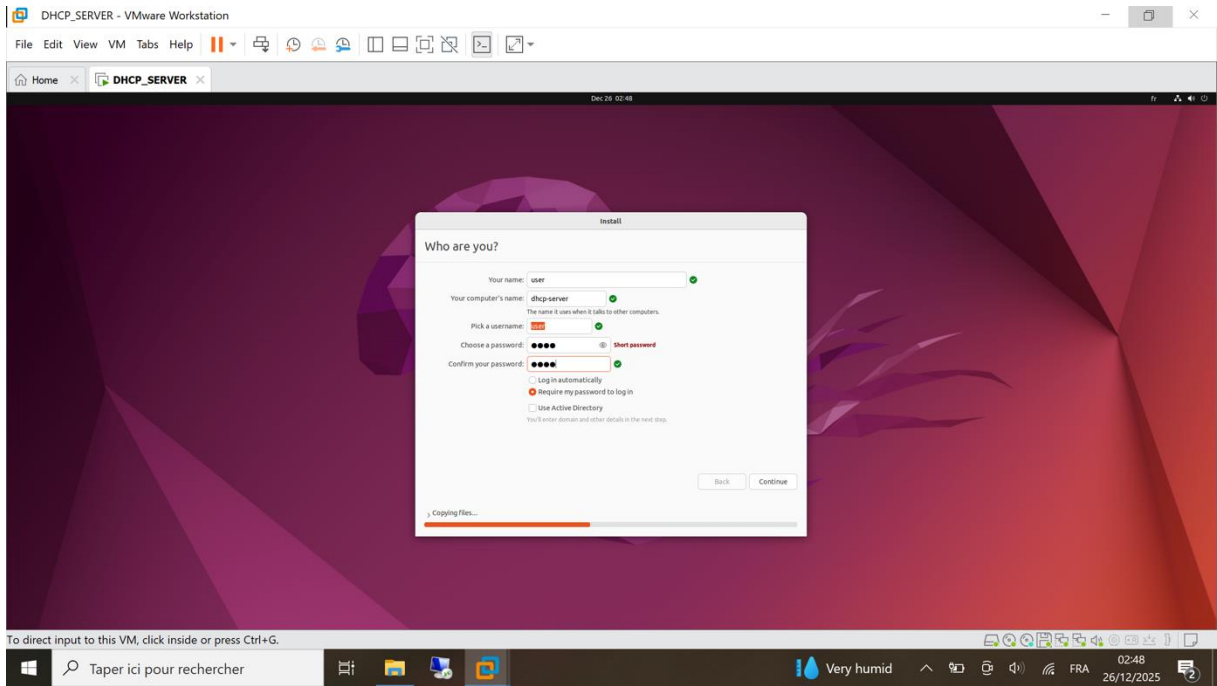
## Installation du système d'exploitation

Après la création de la machine virtuelle, démarrez-la.

Choisissez la langue > Sélectionnez Normal installation > Sélectionnez Erase disk and install Ubuntu > Cliquez sur Continue dans la boîte de dialogue qui s'affiche > Sélectionnez la ville sur la carte.

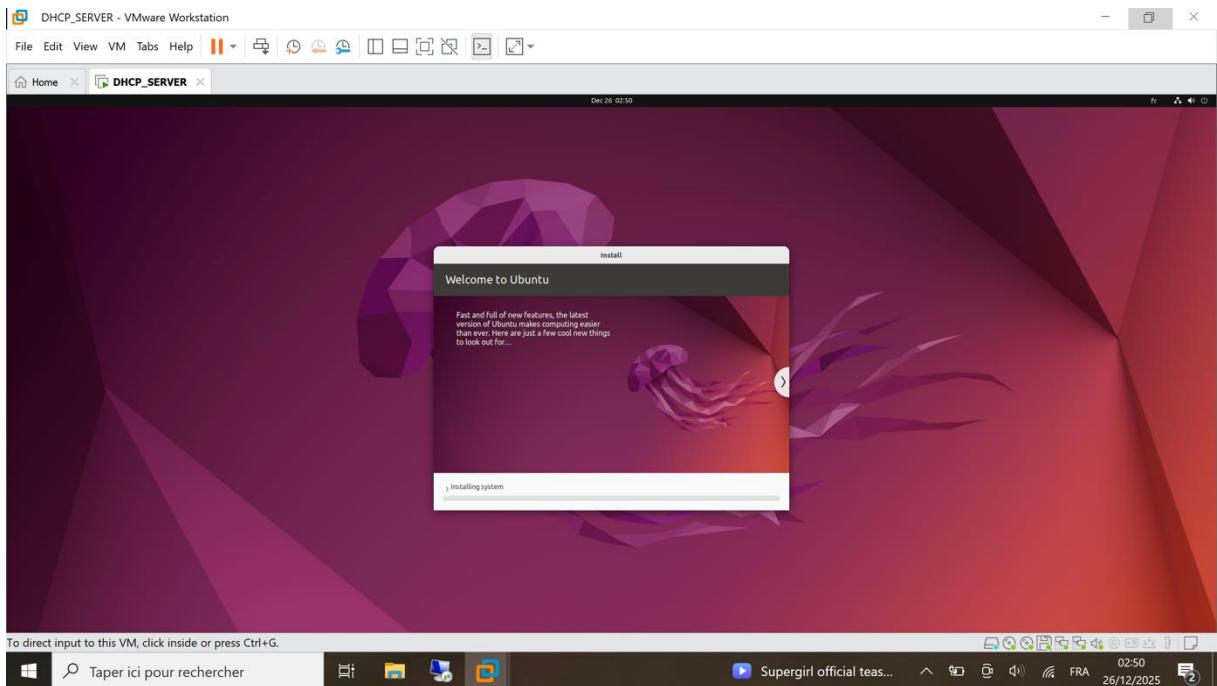


Ensuite saisissez les identifiants (nom d'utilisateur: user et mot de passe: 1234). Modifiez le nom de la machine en **dhcp-server** > Patientez jusqu'à ce que la barre de progression orange en dessous ait terminé de se remplir > Continue.



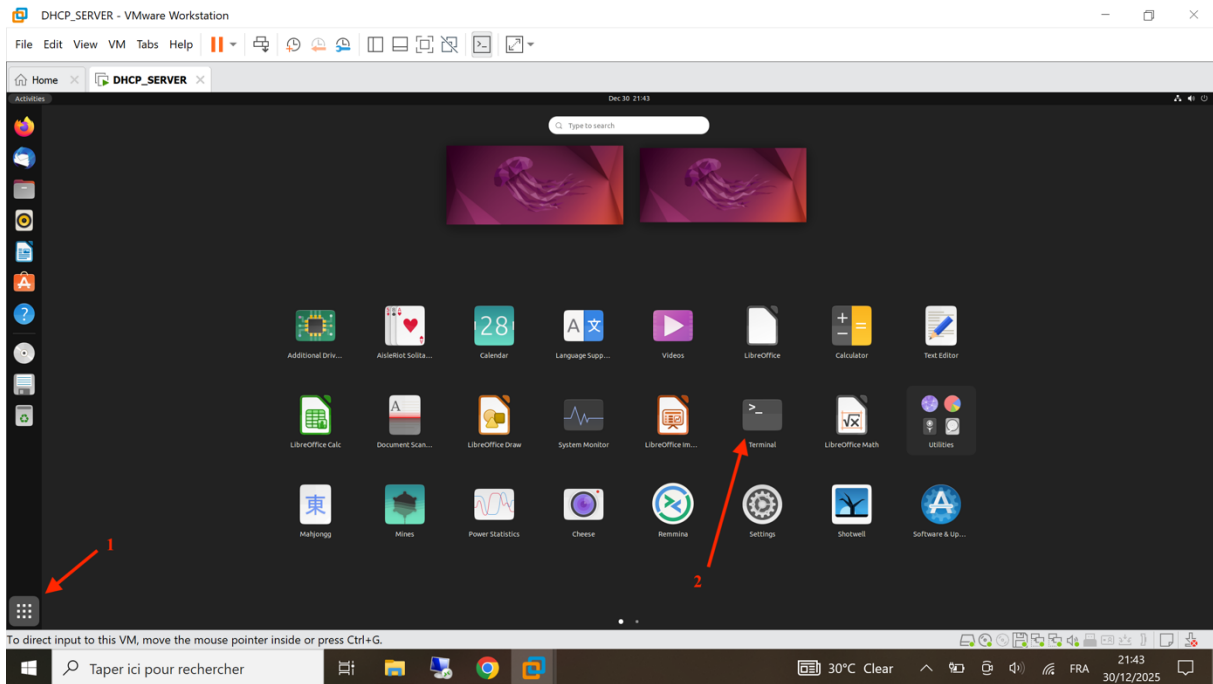
Les configurations terminées, patientez jusqu'à la fin de l'installation.

Une fois celle-ci achevée, vous serez invité à redémarrer la machine.

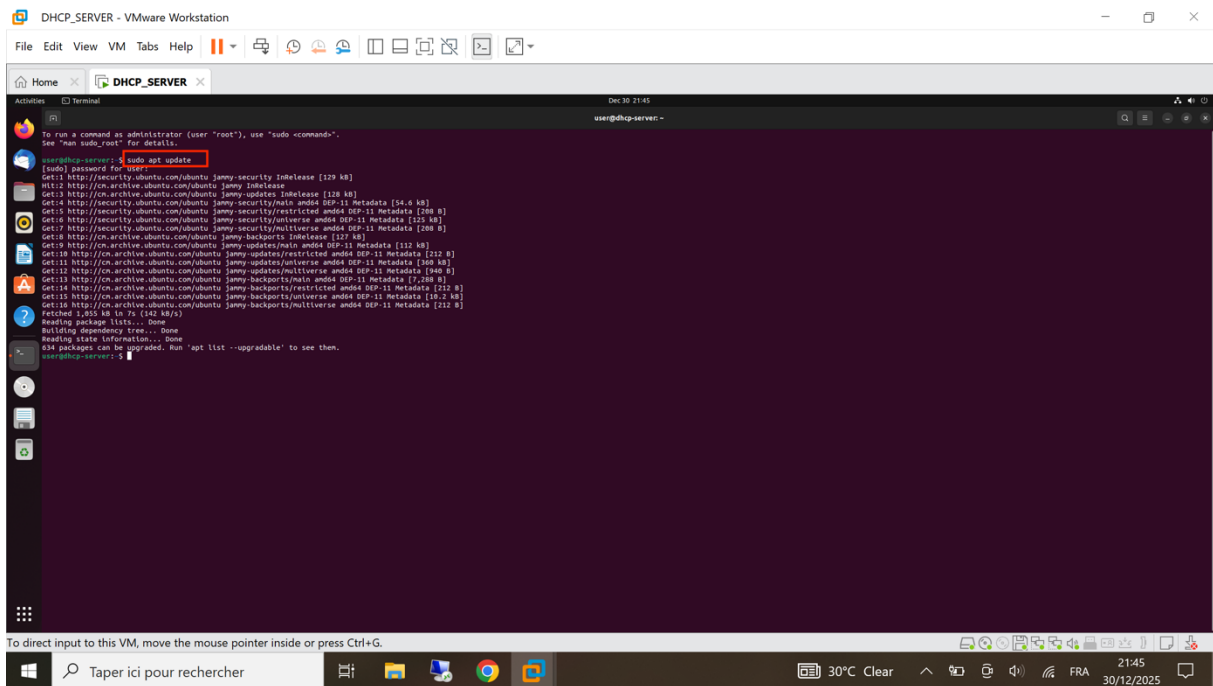


Une fois la machine redémarrée, connectez-vous avec les identifiants précédemment créés.

Ensuite, cliquez sur le bouton **Applications** en bas à gauche, puis ouvrez le **Terminal**.



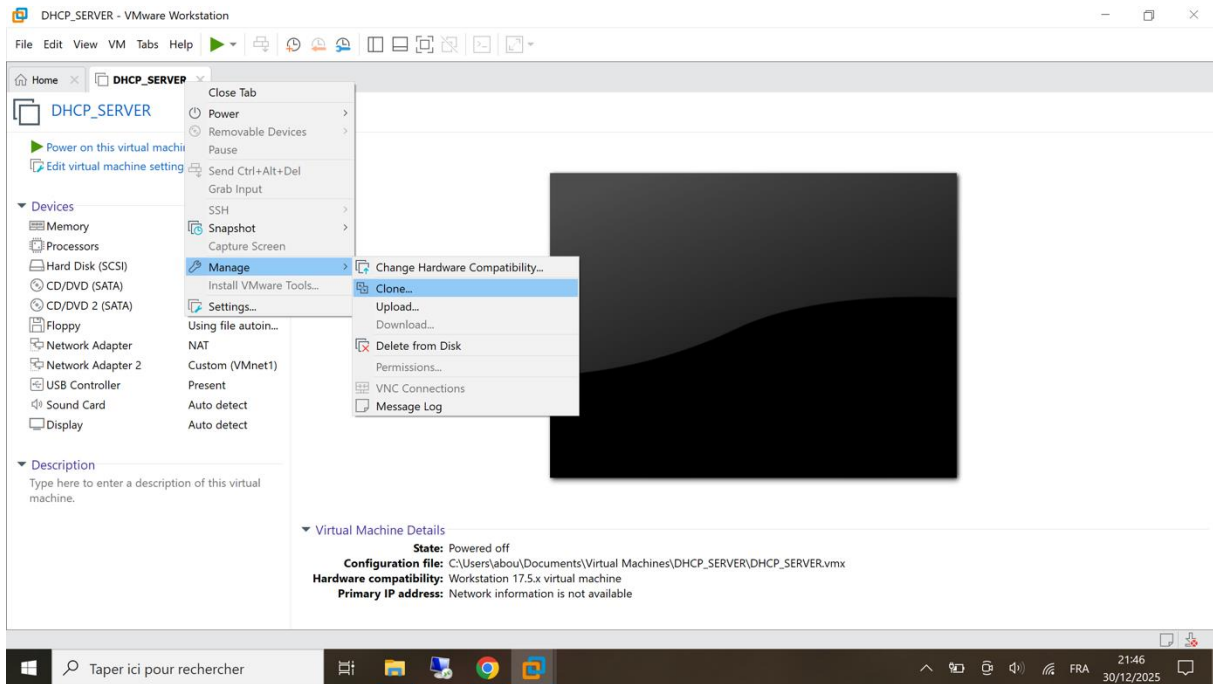
Saisissez la commande **sudo apt update** afin de lancer les mises à jour des listes de paquets.



Passons maintenant au clonage de cette machine afin de créer deux clones à savoir : **DNS\_SERVER** et **ZABBIX\_SERVER**.

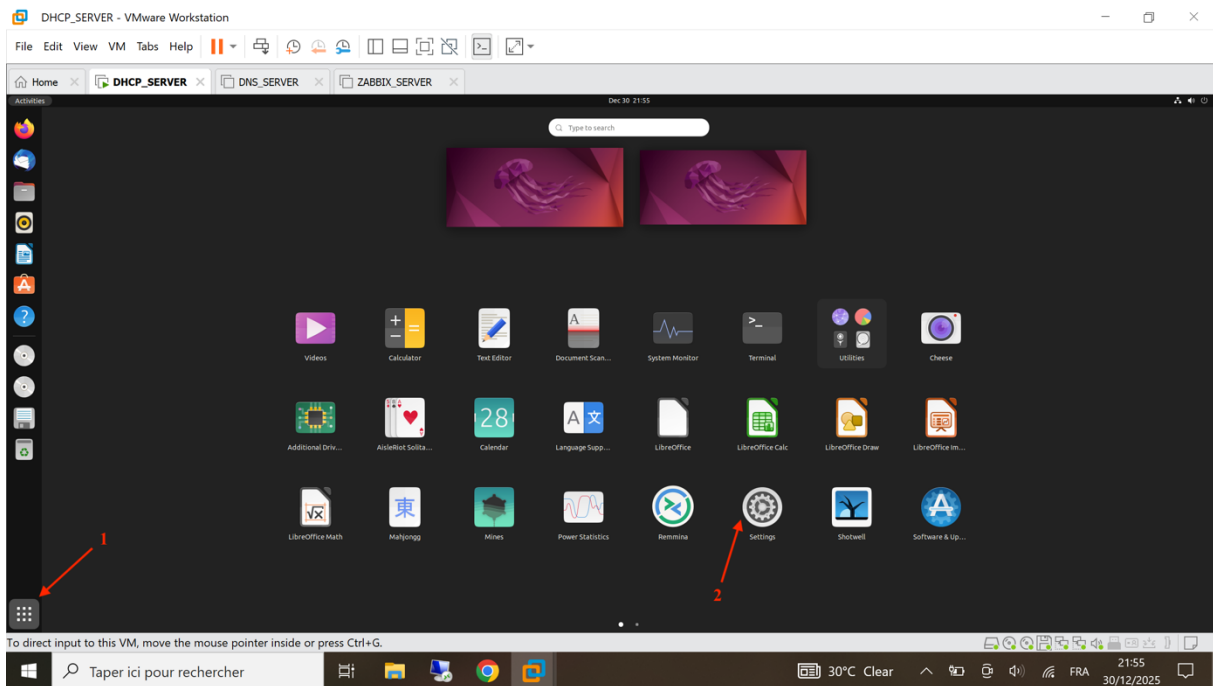
Pour ce faire, éteignez la machine > Effectuez un clic droit sur la machine > Manage > Clone > Cliquez suivant à chaque étape > Choisissez l'option Create a full clone > Donnez à cette machine le nom **DNS\_SERVER** > Terminer > Close.

Répétez la même opération pour créer le clone nommé **ZABBIX\_SERVER**.

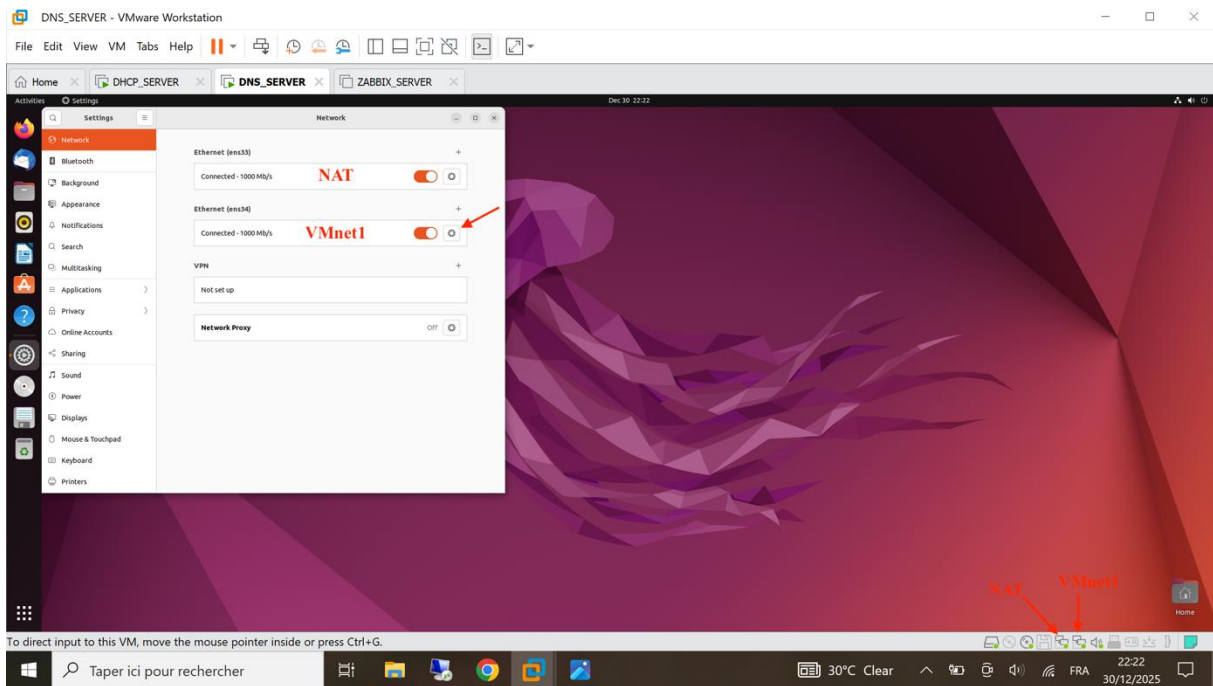


## Configuration du serveur DHCP

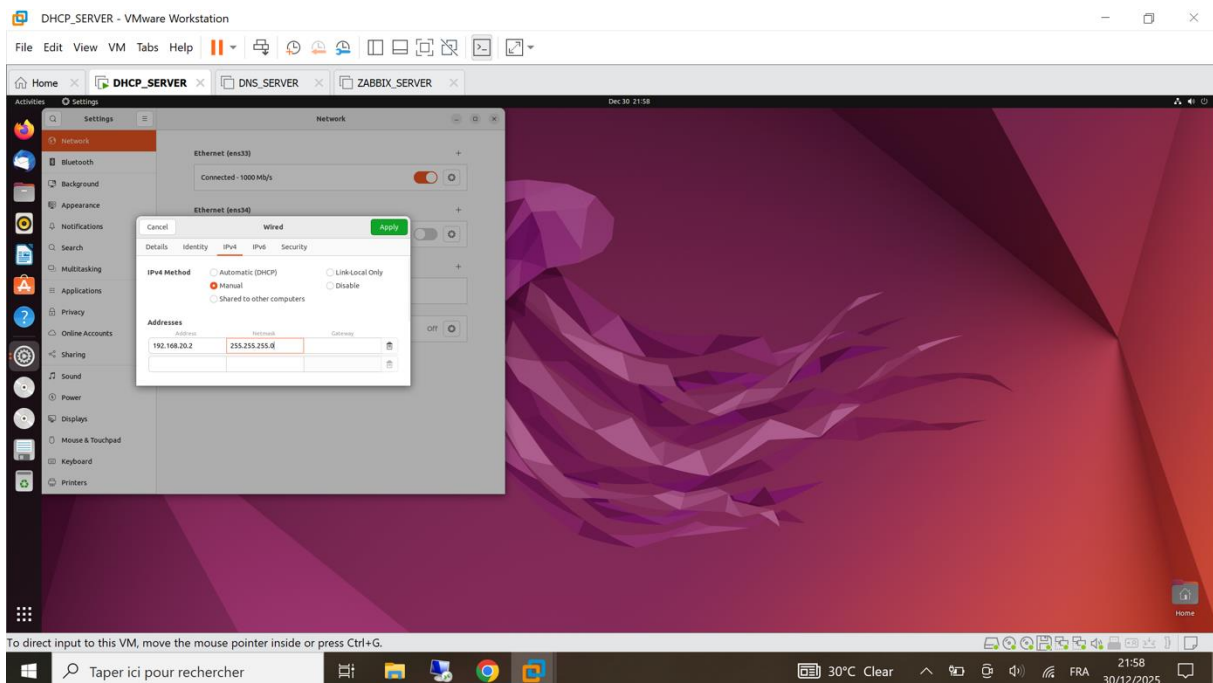
Commençons par lui attribuer une adresse IP. Pour ce faire, cliquez sur le bouton **Applications** > cliquez sur settings.



Ensuite cliquez sur Network dans le volet à gauche > Cliquez sur la roue dentée de la seconde carte réseau.



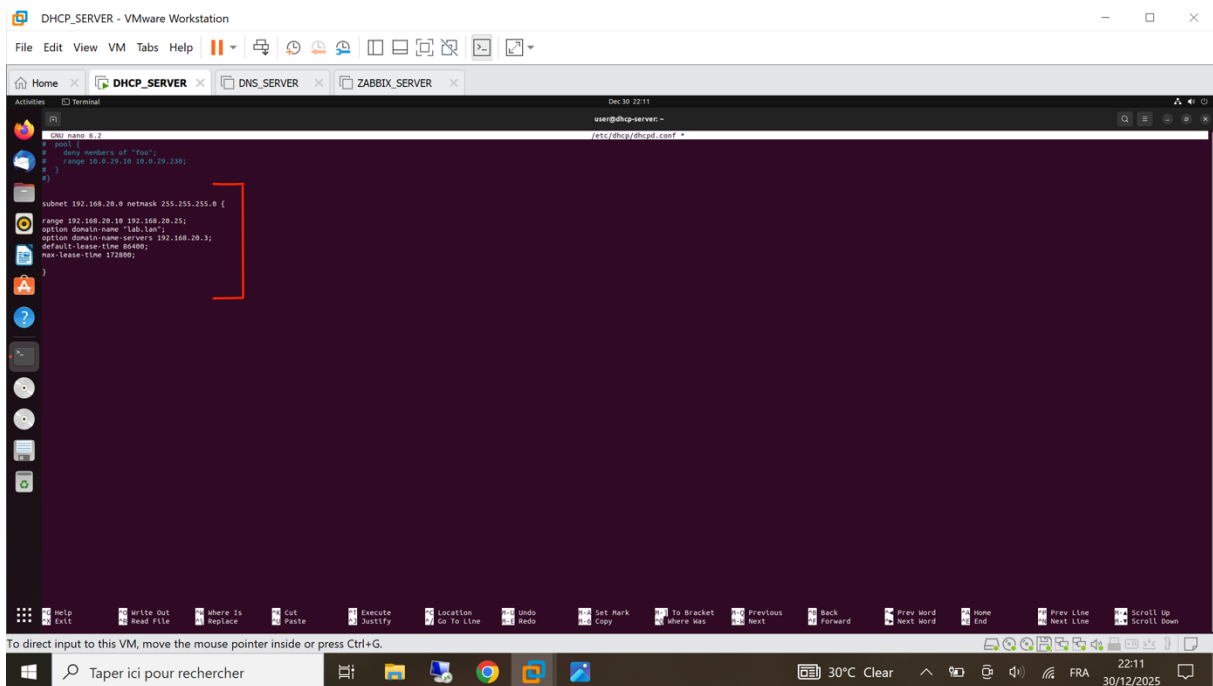
Dans l'onglet IPv4, sélectionnez l'option Manual > Renseignez les informations suivantes : Address: 192.168.20.2 Netmask: 255.255.255.0 > Faites défiler vers le bas, désactivez l'option Automatic pour le DNS puis renseigner l'adresse 192.168.20.3 > Apply > Désactiver puis réactiver la carte pour que les modifications soient prises en compte. (étape très importante)



Saisissez la commande `sudo apt install isc-dhcp-server` afin d'installer le service dhcp sur notre machine virtuelle.



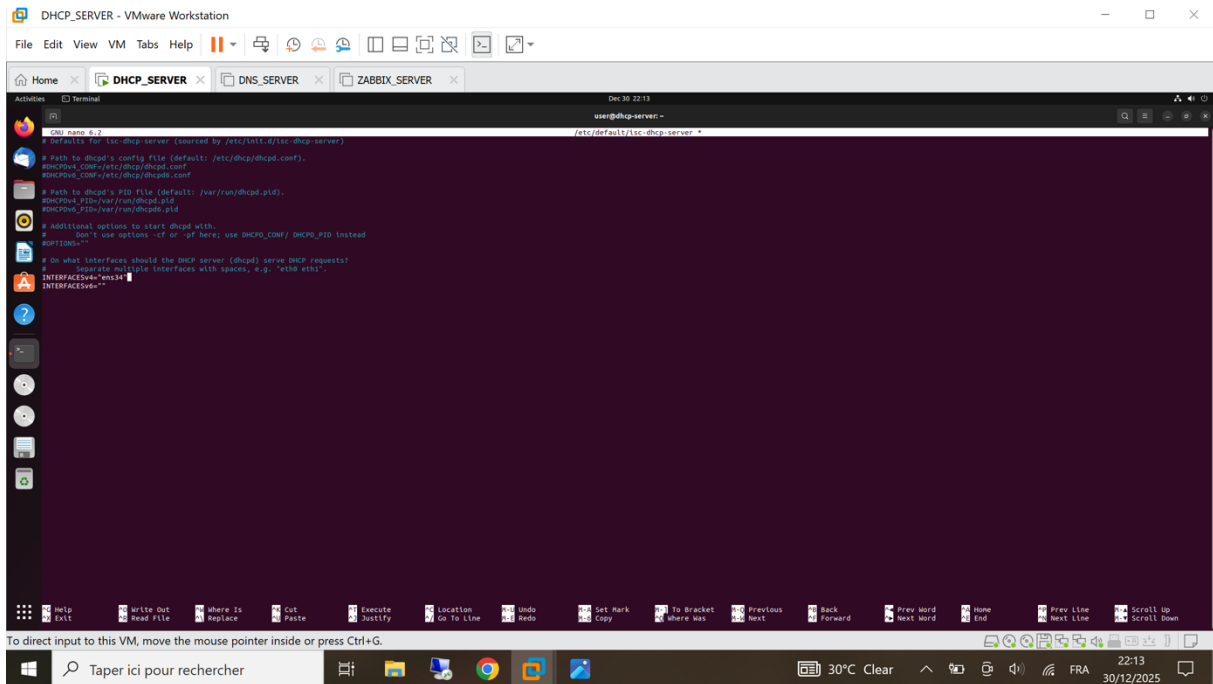
Une fois le service installé, définissons la plage d'adresses dans le fichier de configuration. Pour ce faire, ouvrez le fichier de configuration avec la commande **sudo nano /etc/dhcp/dhcpd.conf** puis renseignez les éléments comme indiqué dans la figure ci-dessous > Enregistrer les modifications en appuyant sur CTRL + O > Fermer le fichier avec CTRL + X.



Il faut maintenant définir l'interface réseau sur laquelle le serveur doit écouter.

Pour cela, saisissez la commande **sudo nano /etc/default/isc-dhcp-server** > Indiquez l'interface réseau LAN (ens34 dans notre cas) au niveau de l'option INTERFACESv4 comme illustré dans la figure suivante > Enregistrer les modifications en appuyant sur CTRL + O > Fermer le fichier avec la combinaison CTRL + X.

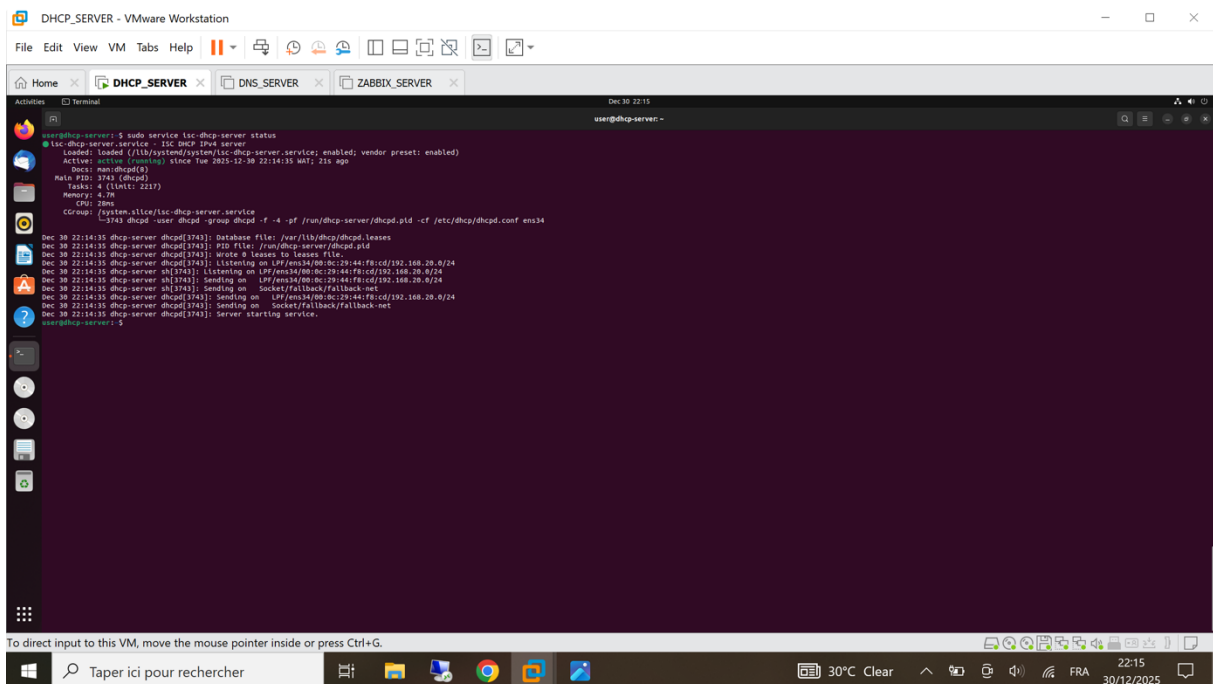
**NB:** Les noms des interfaces réseau peuvent varier d'un système à un autre. Pour connaître le nom de l'interface réseau concernée, accédez aux paramètres réseau. Au niveau de votre carte LAN, vous verrez apparaître **Ethernet (nom de la carte)**.



```
user@dhcp-server: ~$ nano /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPD_CONF=/etc/dhcp/dhcpd.conf
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
DHCPD_PID=/var/run/dhcpd.pid
# Additional options to start dhcpd with.
# Don't use options -f or -p here; use DHCP_CONF/DHCPD_PID instead.
OPTIONS=""
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. 'eth0 eth1'.
INTERFACESv4="ens3"
INTERFACESv6=""
```

Saisissez la commande **sudo service isc-dhcp-server restart** afin de redémarrer le service dhcp.

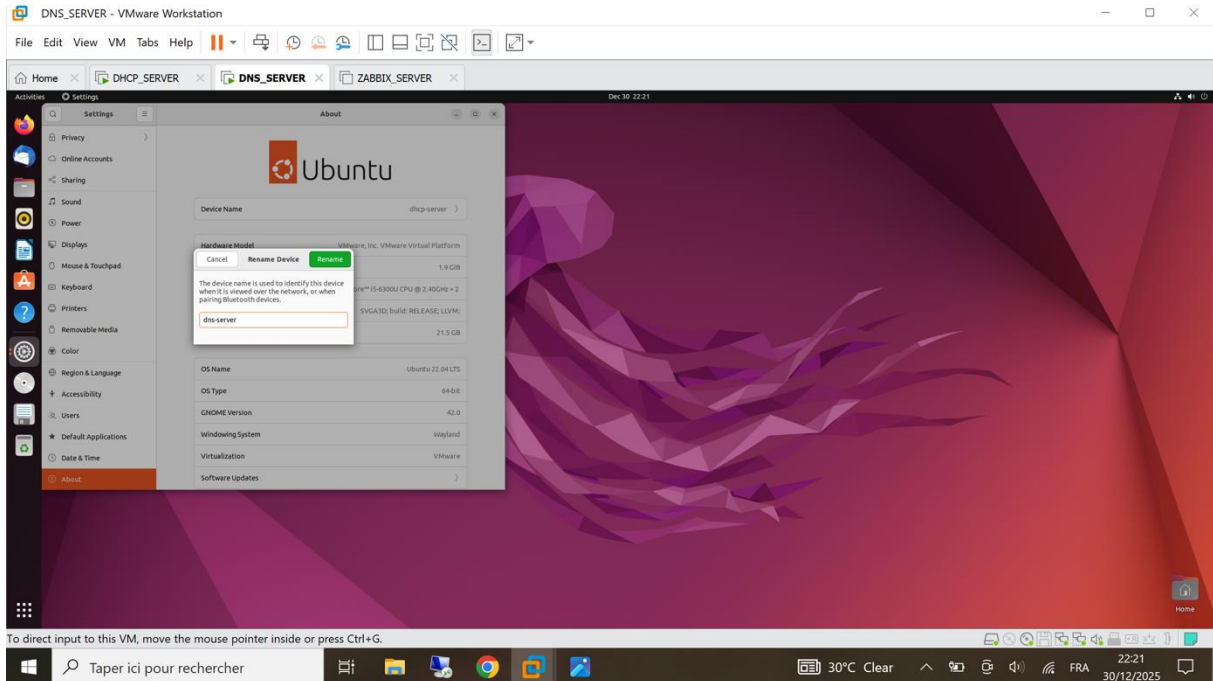
Saisissez la commande **sudo service isc-dhcp-server status** pour s'assurer que le service a bien démarré.



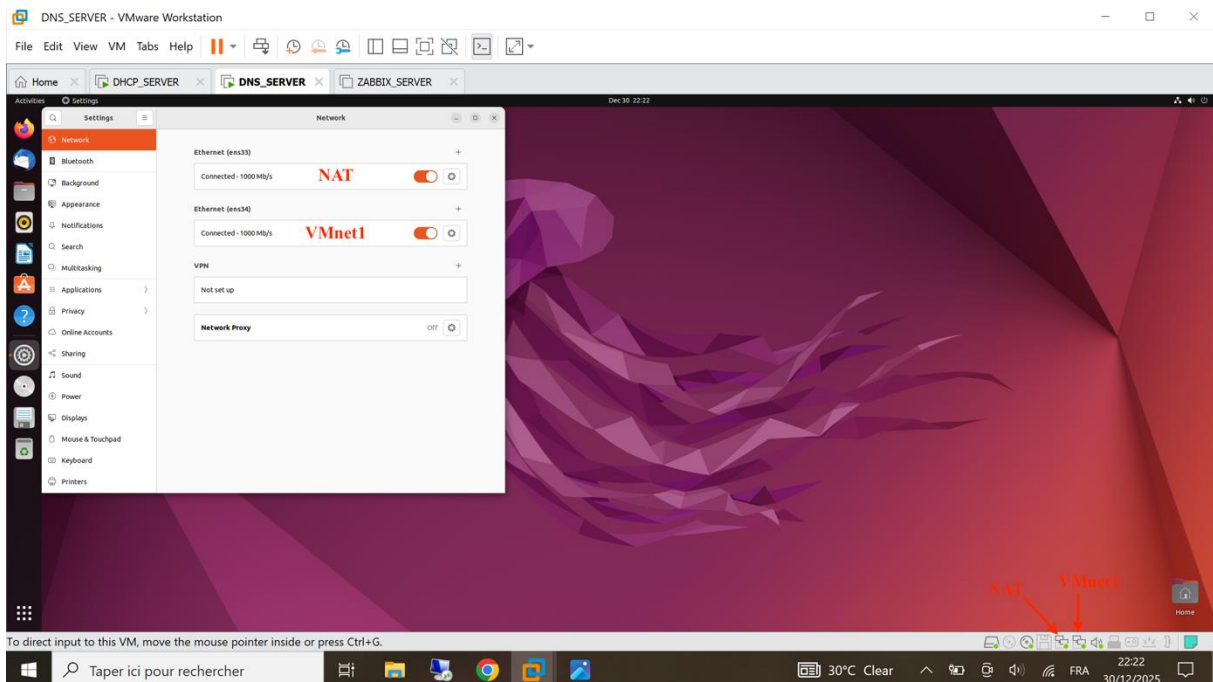
```
user@dhcp-server: ~$ sudo service isc-dhcp-server status
isc-dhcp-server.service - ISC DHCP IPv4 server
Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2025-12-30 22:14:35 MAT; 21s ago
Main PID: 3743 (dhcpd)
Tasks: 4 (Limit: 2227)
CPU: 20ms
Memory: 4.7K
ccrowe@systemd[1]:/etc/systemd/system/isc-dhcp-server.service
└─3743 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf ens34
Dec 30 22:14:35 dhcp-server dhcpd[3743]: Database file: /var/lib/dhcp/dhcpd.leases
Dec 30 22:14:35 dhcp-server dhcpd[3743]: PID file: /run/dhcp-server/dhcpd.pid
Dec 30 22:14:35 dhcp-server dhcpd[3743]: Wrote 0 leases to Leases file.
Dec 30 22:14:35 dhcp-server dhcpd[3743]: Listening on LPF/ens34/08:0c:29:44:f8:cd/192.168.28.0/24
Dec 30 22:14:35 dhcp-server sh[3743]: Listening on LPF/ens34/08:0c:29:44:f8:cd/192.168.28.0/24
Dec 30 22:14:35 dhcp-server sh[3743]: Sending on Socket/fallback/fallback-net
Dec 30 22:14:35 dhcp-server dhcpd[3743]: Sending on LPF/ens34/08:0c:29:44:f8:cd/192.168.28.0/24
Dec 30 22:14:35 dhcp-server dhcpd[3743]: Sending on Socket/fallback/fallback-net
Dec 30 22:14:35 dhcp-server dhcpd[3743]: Server starting service.
user@dhcp-server: ~$
```

## Configuration du serveur DNS

La première étape consiste à renommer le serveur, car étant un clone du serveur DHCP, il a conservé le même nom. Pour effectuer cette modification, ouvrez Terminal > accédez à Settings > About > Device Name: dns-server > Rename.

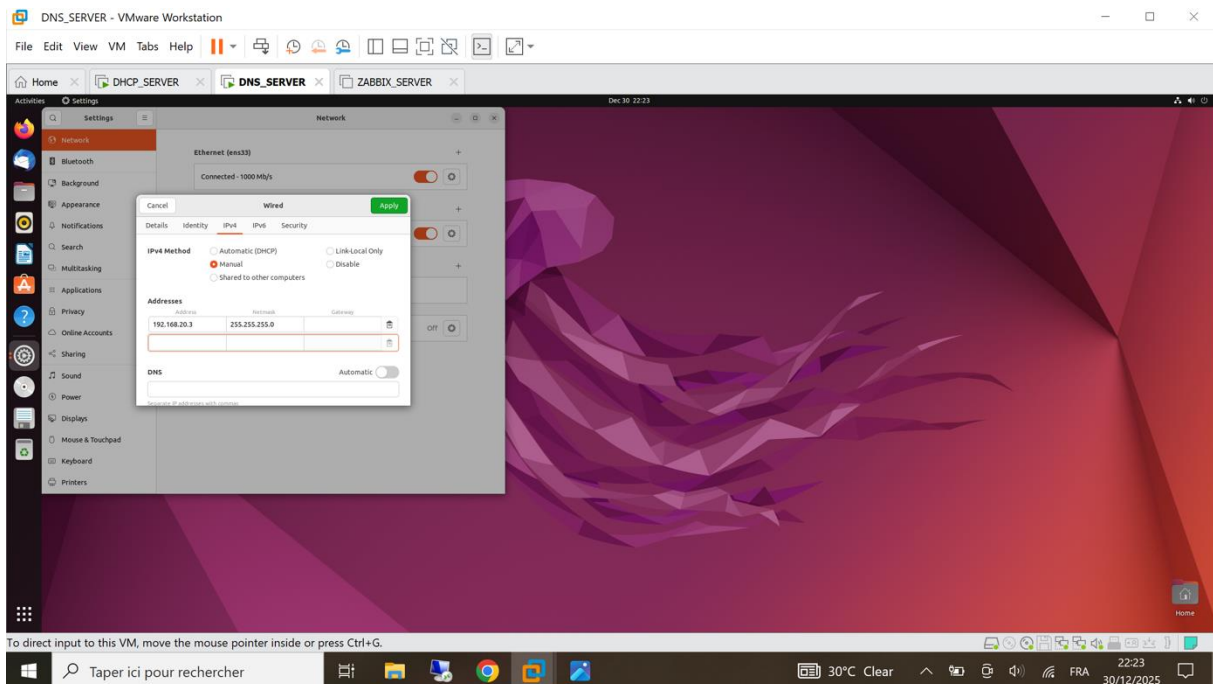


Accédez aux paramètres réseau afin d'attribuer une adresse IP au serveur. Pour ce faire, cliquez sur le bouton applications en bas à gauche de l'écran > Settings > Network > Cliquez sur la roue dentée de la carte réseau LAN (la deuxième carte dans notre cas).

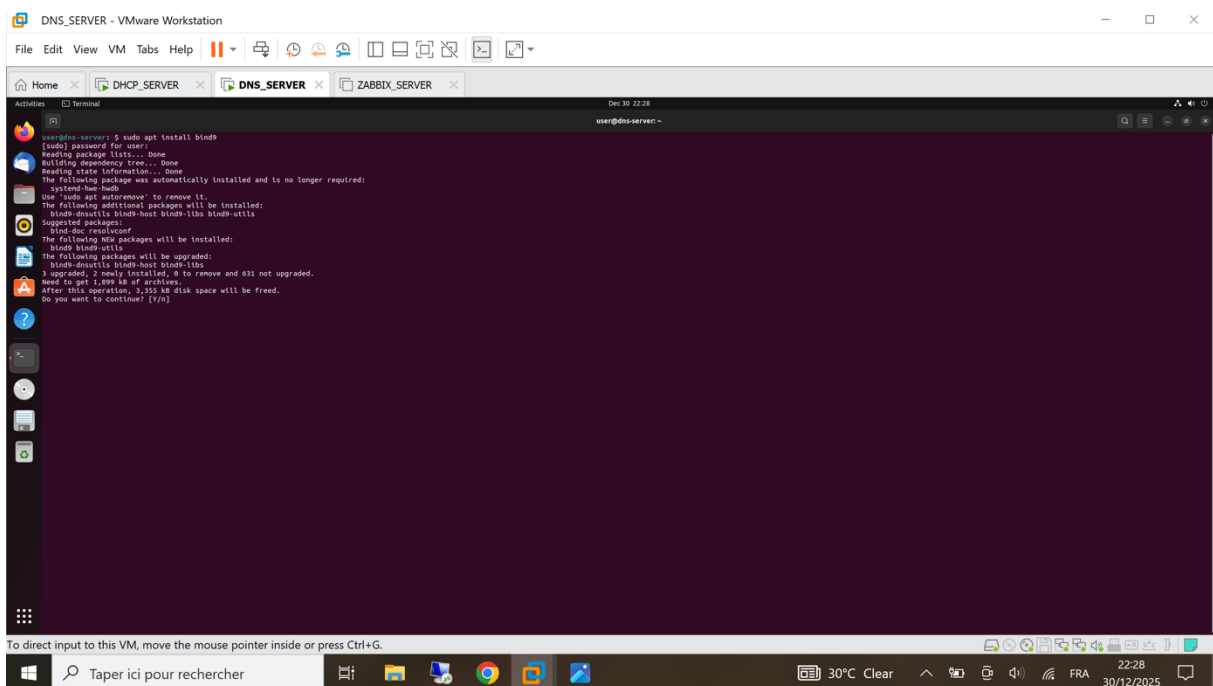


Accédez au volet IPv4 > Manual > Saisissez les informations suivantes: Address: 192.168.20.3  
Netmask: 255.255.255.0 > Apply > Désactiver puis réactiver la carte pour que les modifications soient prises en compte. (étape très importante)

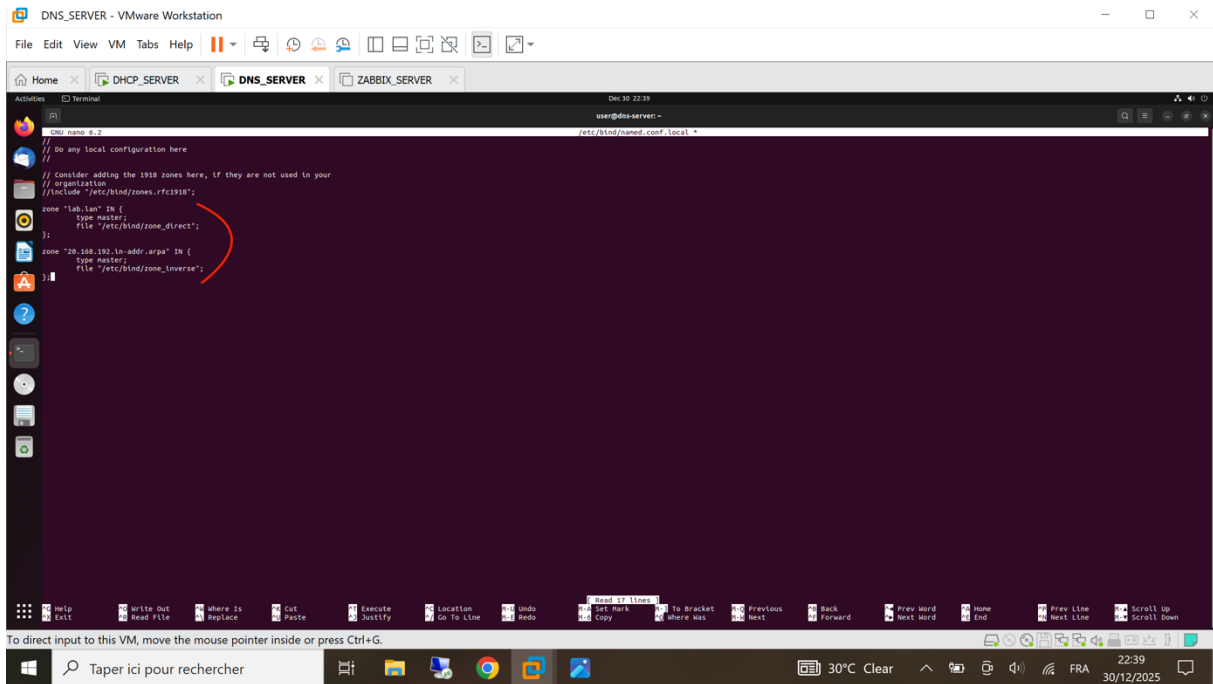
**NB :** Il n'est pas nécessaire de configurer l'adresse DNS, puisque cette machine est destinée à servir de serveur DNS pour les autres machines du réseau.



Utilisez la commande **sudo apt install bind9** afin d'installer le service DNS sur la machine virtuelle. Pour cela, ouvrez le Terminal > Saisissez **sudo apt install bind9**.



Accédez au fichier de configuration dns pour déclarer les zones de recherches dns. Pour ce faire, exécutez la commande **sudo nano /etc/bind/named.conf.local** > Saisissez les informations comme indiqué dans la figure ci-dessous > Enregistrez les modifications en appuyant sur CTRL + O > Fermez le fichier avec CTRL + X.



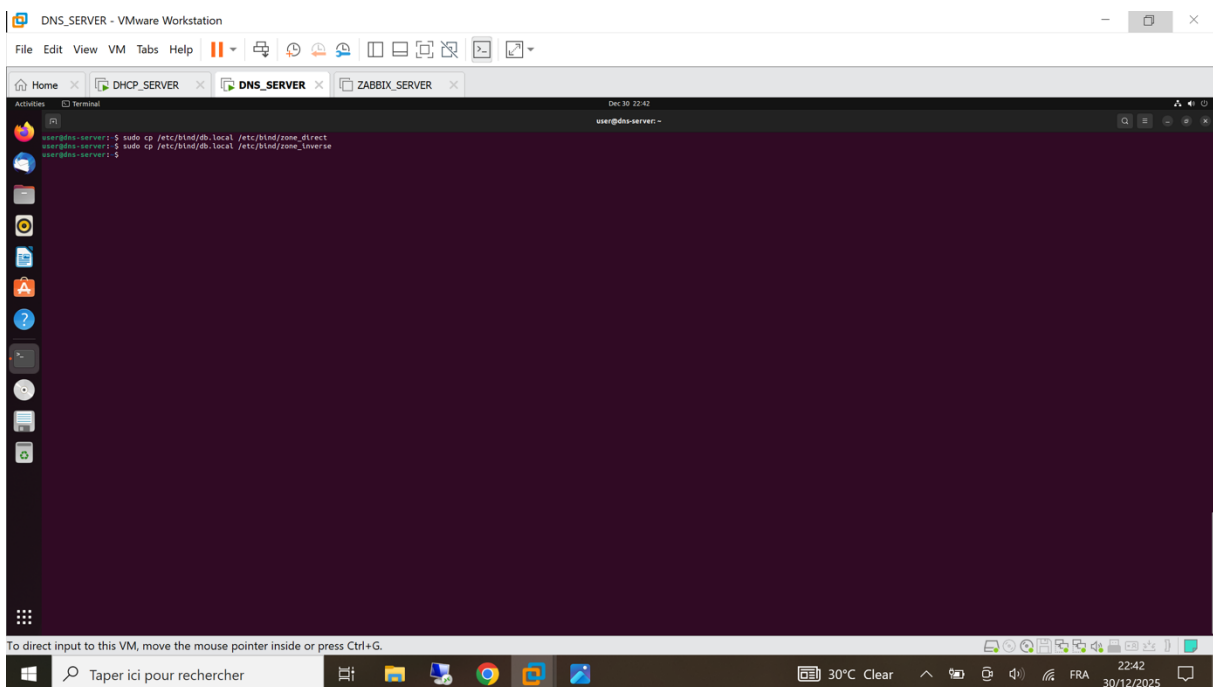
```
user@dns-server:~$ sudo nano /etc/bind/named.conf.local
// Do any local configuration here
// (there are no local zones by default)
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "lab.lan" IN {
    type master;
    file "/etc/bind/zone_direct";
};

zone "20.168.192.la-addr.arpa" IN {
    type master;
    file "/etc/bind/zone_inverse";
};
```

**NB:** lab.lan correspond au nom de domaine, tandis que 20.168.192 représente la partie réseau de l'adressage IP que nous avons choisie.

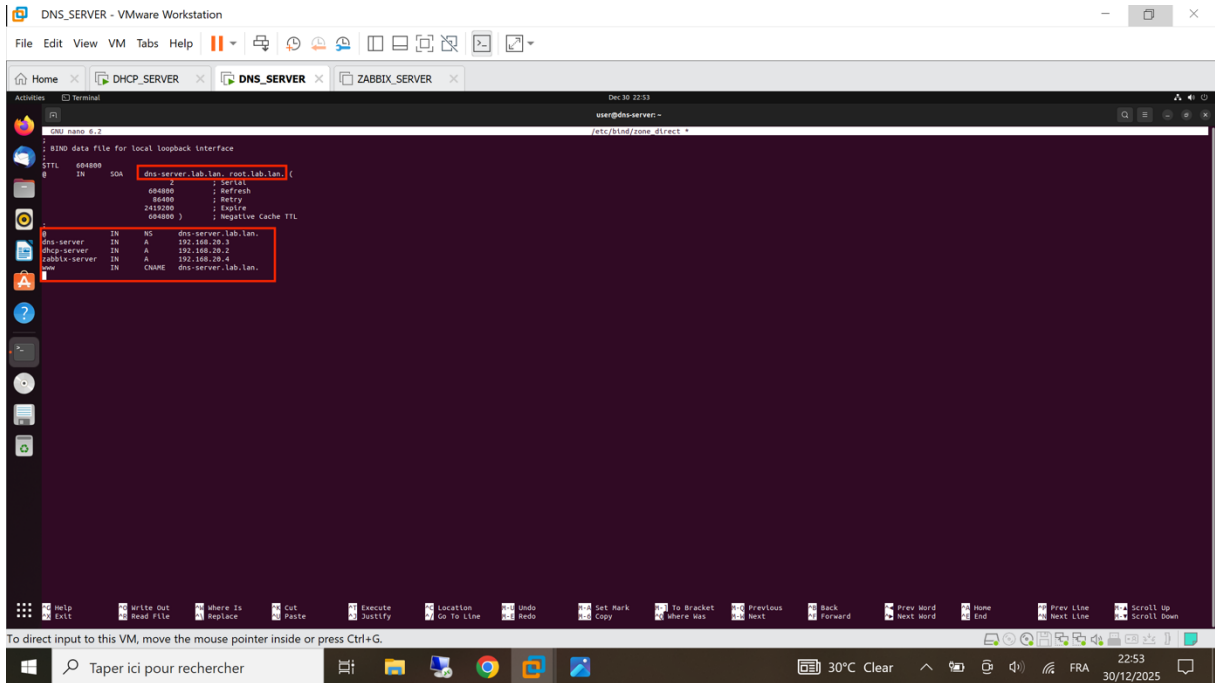
Copiez le contenu du fichier **db.local** dans les nouveaux fichiers zone\_direct et zone\_inverse en exécutant successivement les commandes **sudo cp /etc/bind/db.local /etc/bind/zone\_direct** **sudo cp /etc/bind/db.local /etc/bind/zone\_inverse**



```
user@dns-server:~$ sudo cp /etc/bind/db.local /etc/bind/zone_direct
user@dns-server:~$ sudo cp /etc/bind/db.local /etc/bind/zone_inverse
user@dns-server:~$
```

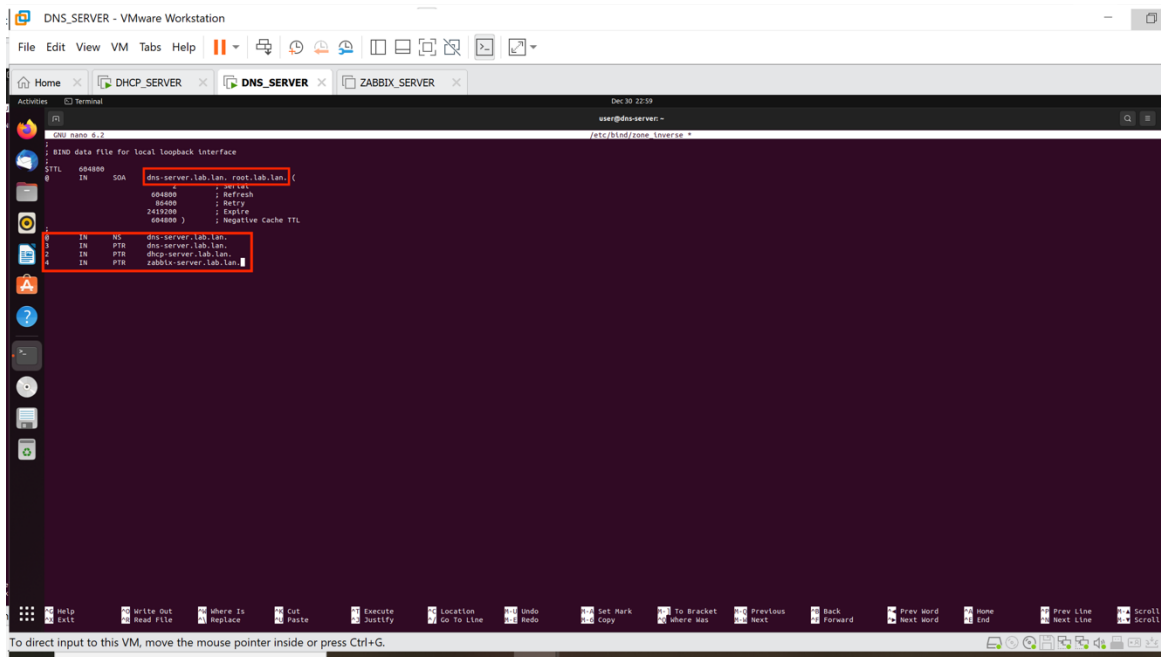
Modifiez le contenu (uniquement les parties indiquées en rouge) du fichier zone\_direct comme illustré dans la figure suivante. Pour cela, exécutez la commande **sudo nano /etc/bind/zone\_direct**

Enregistrez les modifications avec CTRL + O puis fermer avec CTRL + X.

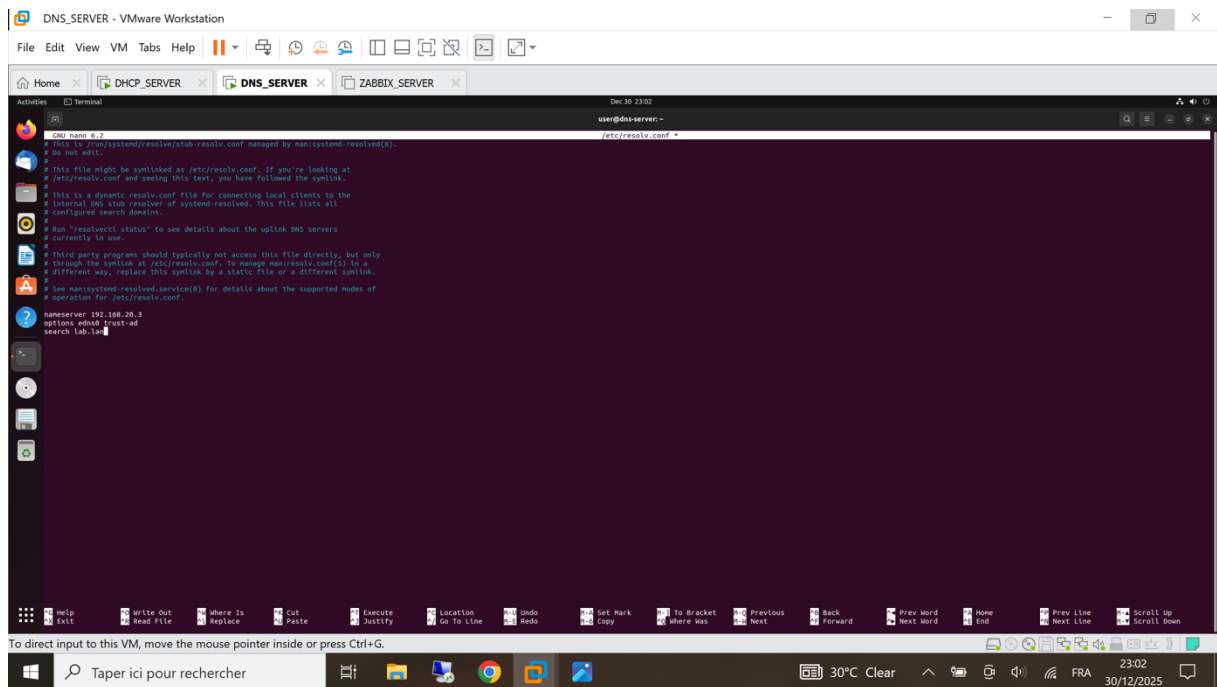


Modifiez le contenu (uniquement les parties indiquées en rouge) du fichier zone\_inverse comme illustré dans la figure suivante. Pour cela, exécutez la commande **sudo nano /etc/bind/zone\_inverse**

Enregistrez les modifications avec CTRL + O puis fermer avec CTRL + X.

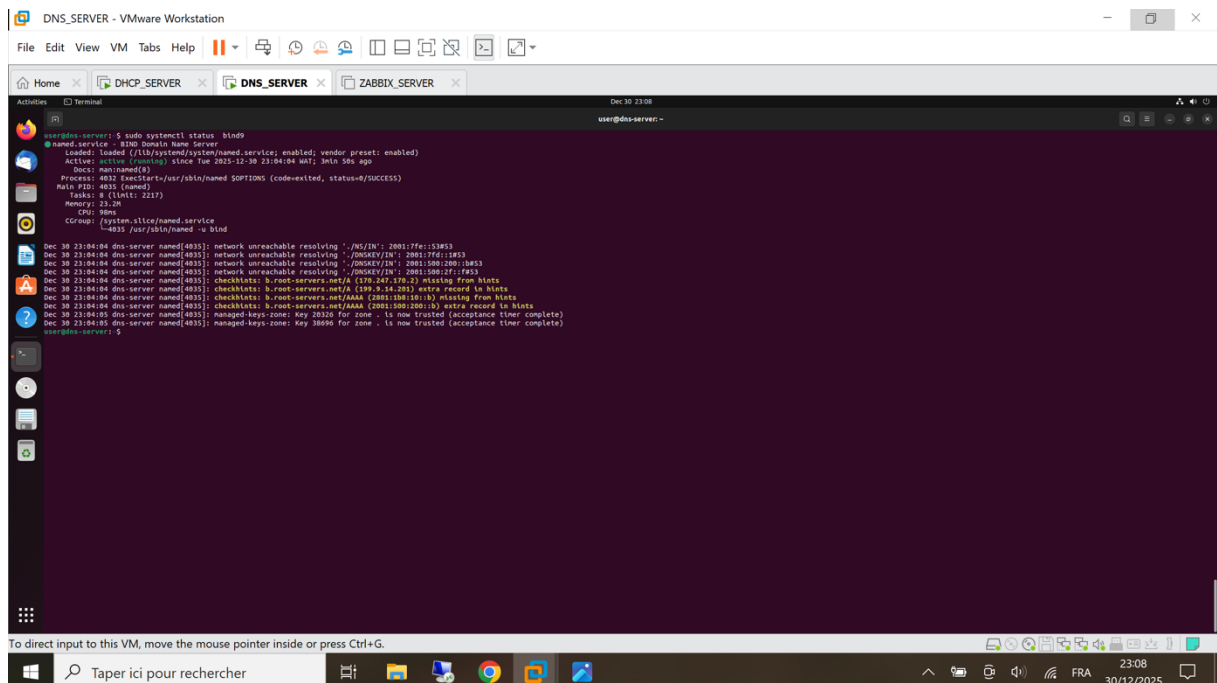


Configurez le fichier de résolution des noms de domaine. Pour cela, exécutez la commande **sudo nano /etc/resolv.conf** > Configurez le fichier comme illustré dans la figure ci-dessous > Enregistrez les modifications en appuyant sur CTRL + O > Fermer le fichier avec CTRL + X.



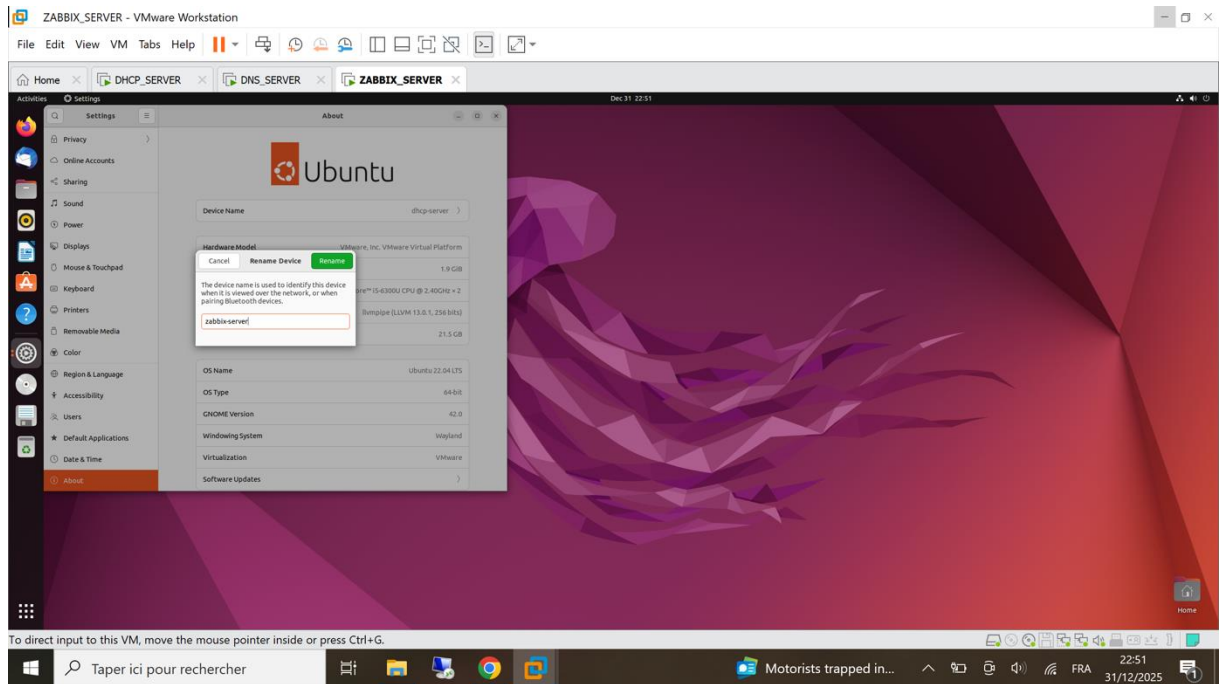
Redémarrez le service DNS en exécutant la commande **sudo systemctl restart bind9**

Vérifiez que le service a bien démarré en exécutant la commande **sudo systemctl status bind9**

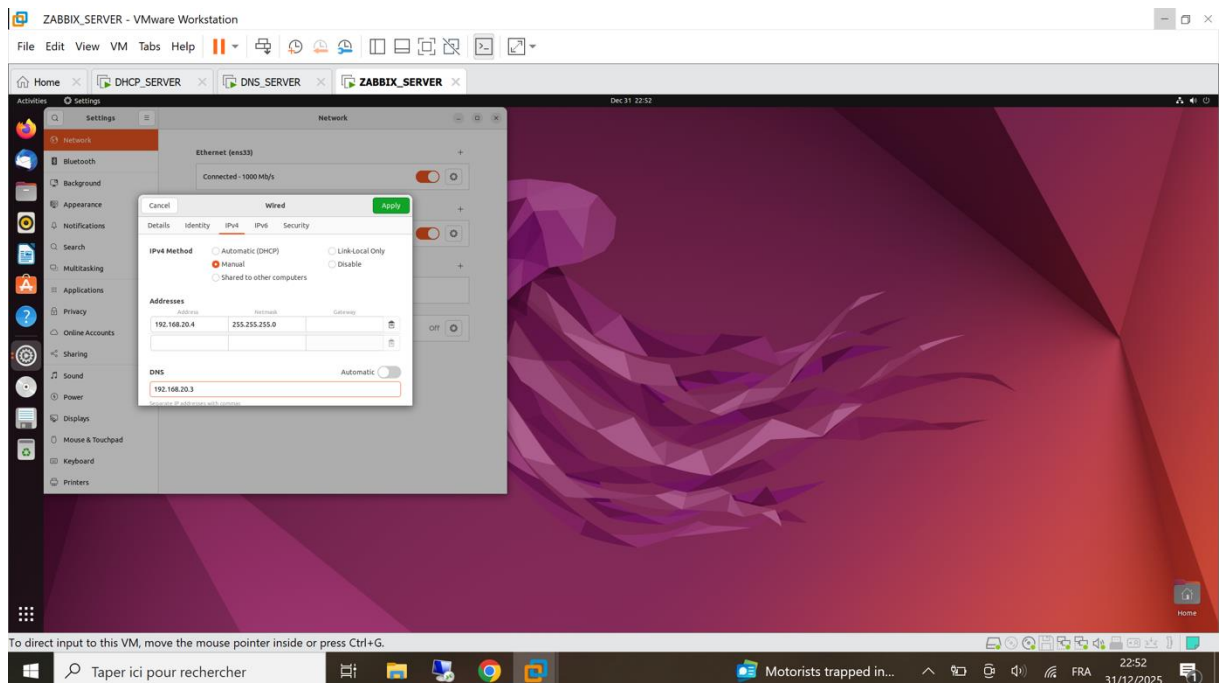


## Configuration du serveur Zabbix

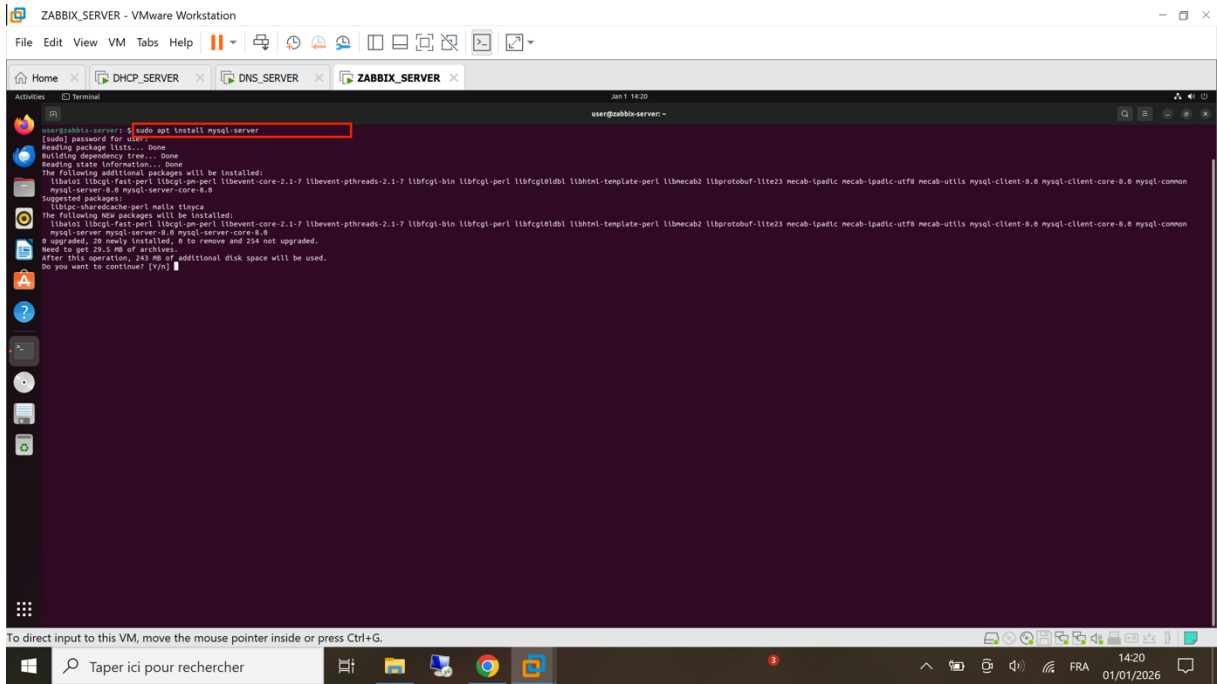
Démarrez la machine virtuelle ZABBIX\_SERVER et commencez par renommer en zabbix-server. Pour cela, accédez au Terminal > Settings > About > Device Name: zabbix-server > Rename.



Ensuite attribuons une adresse IP à la machine. Toujours dans Settings, cliquez sur Network > Cliquez sur la roue dentée de la carte réseau LAN (la deuxième carte dans notre cas) > Accédez à l'onglet IPv4 > Manual > Saisissez les informations suivantes: Address: 192.168.20.4 Netmask: 255.255.255.0 > Faites défiler vers le bas, désactivez l'option Automatic pour le DNS puis renseigner l'adresse 192.168.20.3 > Apply > Désactiver puis réactiver la carte pour que les modifications soient prises en compte. (étape très importante)

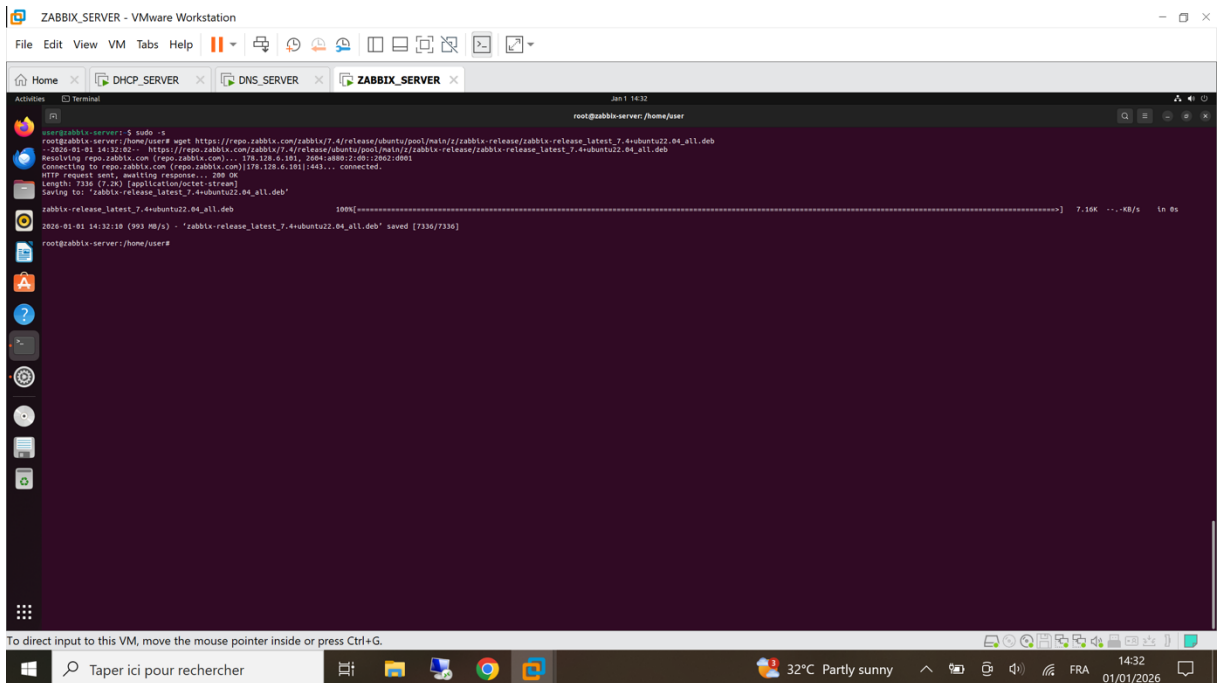


Exécutez la commande **sudo apt install mysql-server** pour installer le Système de Gestion de Base de Données qui sera utilisé par zabbix. C'est une étape cruciale et primordiale pour l'installation de zabbix.



Une fois mysql installé nous pouvons procéder à l'installation de zabbix. Pour cela, accédez au Terminal > Saisissez la commande **sudo -s** pour passer en mode super administrateur > Saisissez la commande

**wget https://repo.zabbix.com/zabbix/7.4/release/ubuntu/pool/main/z/zabbix-release/zabbix-release\_latest\_7.4+ubuntu22.04\_all.deb**



Ensuite saisissez tout à tour les commandes suivantes :

1. **dpkg -i zabbix-release\_latest\_7.4+ubuntu22.04\_all.deb**
2. **apt update**

3. apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
4. mysql -uroot -p (**password** comme mot de passe)
5. create database zabbix character set utf8mb4 collate utf8mb4\_bin;
6. create user zabbix@localhost identified by 'password';
7. grant all privileges on zabbix.\* to zabbix@localhost;
8. set global log\_bin\_trust\_function\_creators = 1;
9. quit;

```

root@zabbix-server:/home/user# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.44-Sublinux.22.04.2 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0.01 sec)

mysql> create user zabbix@localhost identified by 'password';
Query OK, 1 row affected (0.01 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.01 sec)

mysql> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected, 1 warning (0.01 sec)

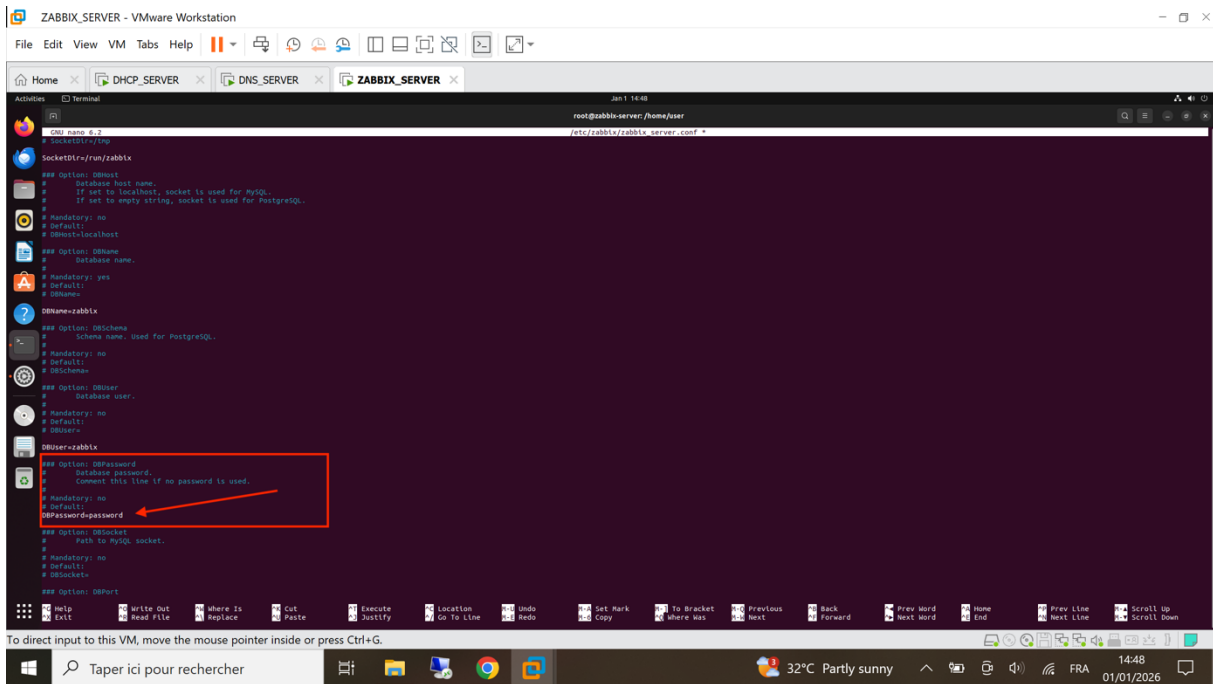
mysql> quit;

```

10. zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix (**password** comme mot de passe)
11. mysql -uroot -p (**password** comme mot de passe)
12. set global log\_bin\_trust\_function\_creators = 0;
13. quit;

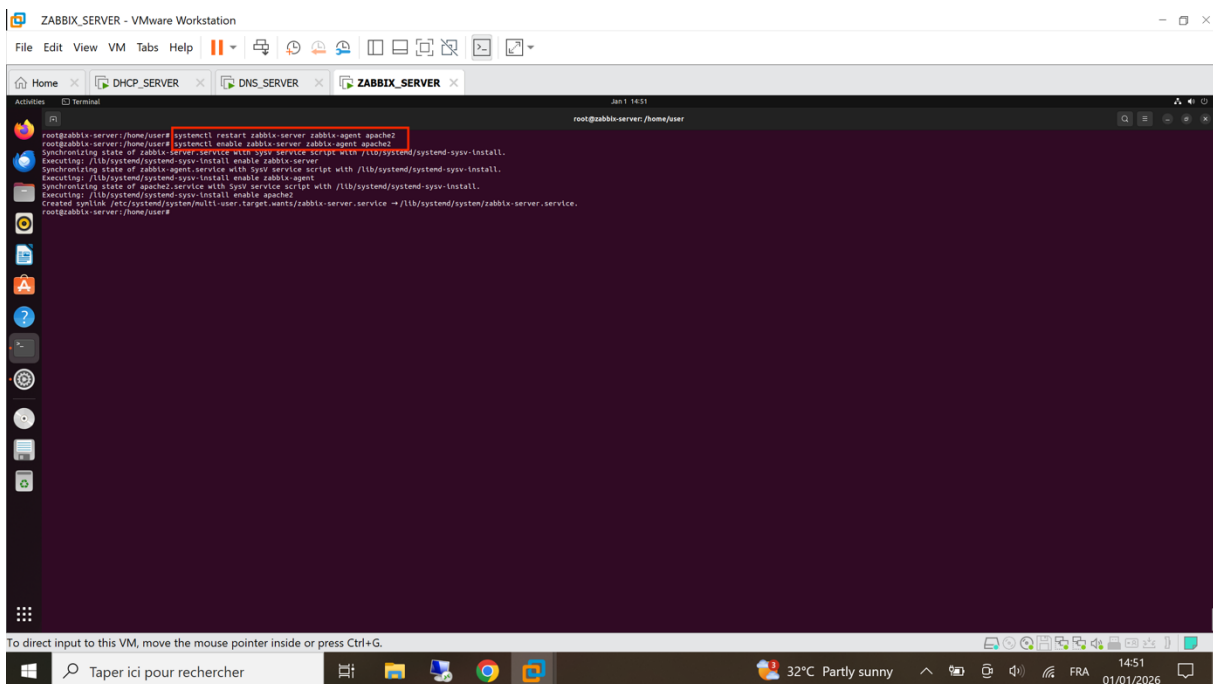
Exécutez la commande `/etc/zabbix/zabbix_server.conf` afin de définir le mot de passe pour la base de données du serveur zabbix. (**password** comme mot de passe).

Enregistrez les modifications avec la combinaison CTRL + O puis fermez le fichier avec la combinaison CTRL + X.



Exécutez successivement les commandes suivantes afin de redémarrer les services zabbix et les activer.

- `systemctl restart zabbix-server zabbix-agent apache2`
- `systemctl enable zabbix-server zabbix-agent apache2`

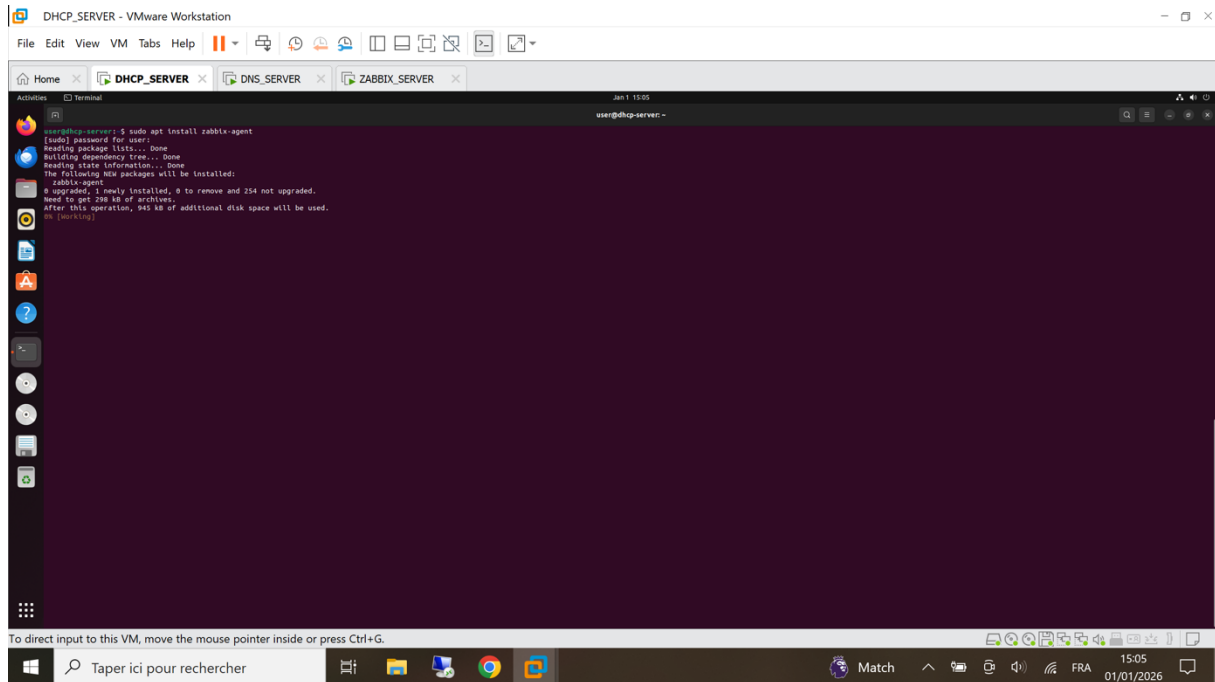


## Installation et configuration des agents sur DHCP\_SERVER et DNS\_SERVER

Pour que Zabbix puisse collecter les données à surveiller, il est nécessaire d'installer des agents Zabbix sur les machines à superviser.

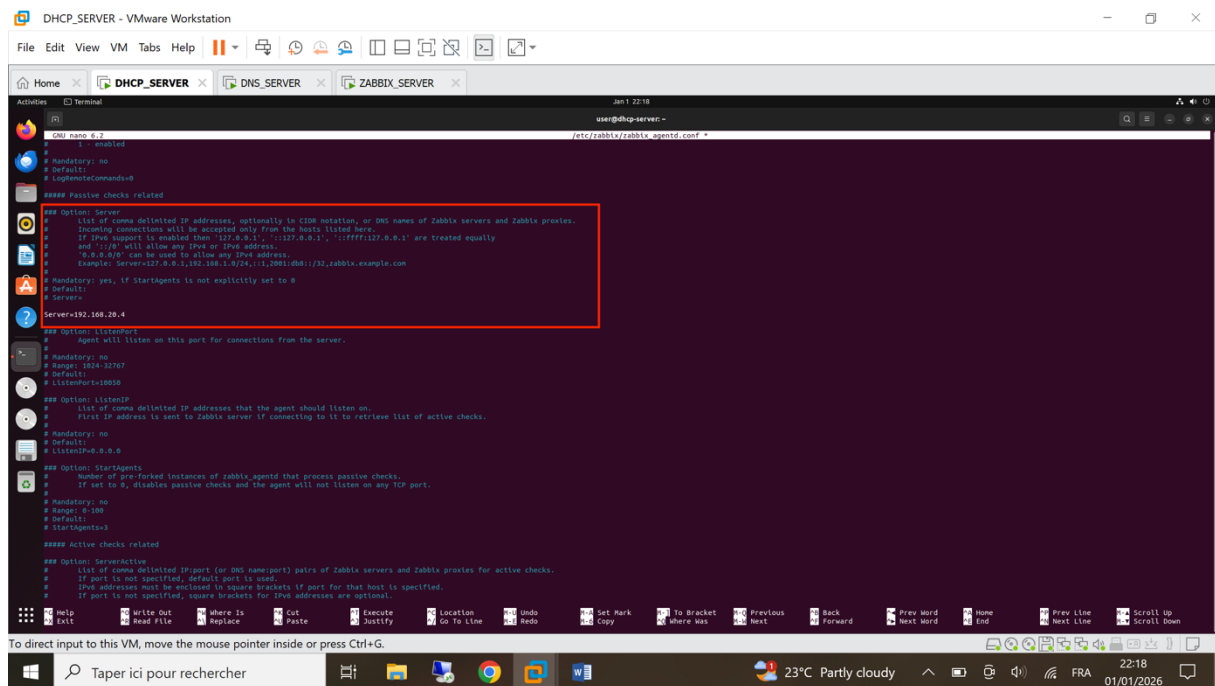
**Remarque :** Les actions qui suivent sont valables sur les deux serveurs.

Pour ce faire, exécutez la commande **sudo apt install zabbix-agent**



```
user@dhcp-server:~$ sudo apt install zabbix-agent
[sudo] password for user:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following new packages will be installed:
zabbix-agent
0 upgraded, 1 newly installed, 0 to remove and 254 not upgraded.
Need to get 298 kB of archives.
After this operation, 945 kB of additional disk space will be used.
deb [working]
```

Ensuite définir l'adresse IP du serveur zabbix au niveau de chaque machine à superviser. Pour cela, exécutez la commande **sudo nano /etc/zabbix/zabbix\_agentd.conf** > Défilez vers le bas, dans la rubrique option: Server > Renseignez l'adresse 192.168.20.4 > Enregistrez les modifications avec la combinaison CTRL + O > Fermez le fichier avec la combinaison CTRL + X.

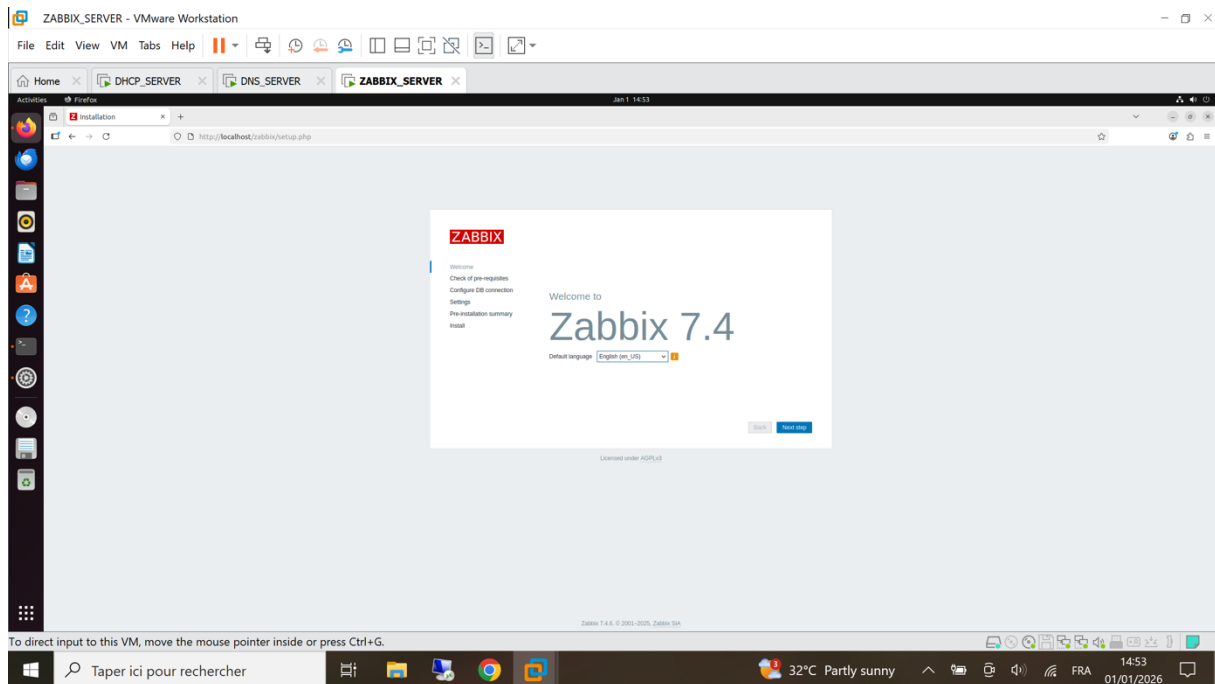


```
user@dhcp-server:~$ sudo nano /etc/zabbix/zabbix_agentd.conf
#
# Mandatory: no
# Default:
# LogRemoteCommands=0
##### Passive checks related
### Option: Server
# List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix servers and Zabbix proxies.
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then ::127.0.0.1, ::127.0.0.1, ::ffff:127.0.0.1 are treated equally
# and ::1/8 will allow any IPv6 or IPv4 address.
# 0.0.0.0/0 can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::1/32,zabbix.example.com
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=
Server=192.168.20.4
### Option: ListenPort
# Agent will listen on this port for connections from the server.
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10101
### Option: ListenIP
# List of comma delimited IP addresses that the agent should listen on.
# First IP address is sent to Zabbix server if connecting to it to retrieve list of active checks.
# Mandatory: no
# Default:
# ListenIP=0.0.0.0
### Option: StartAgents
# Number of pre-forked instances of zabbix_agentd that process passive checks.
# If set to 0, disables passive checks and the agent will not listen on any TCP port.
# Mandatory: no
# Range: 0-256
# Default:
# StartAgents=1
##### Active checks related
### Option: ServerActive
# List of comma delimited IP:port (or DNS name:port) pairs of Zabbix servers and Zabbix proxies for active checks.
# If port is not specified, default port is used.
# IPv6 addresses must be enclosed in square brackets if port for that host is specified.
# If port is not specified, square brackets for IPv6 addresses are optional.
```

Exécutez la commande **sudo systemctl start zabbix-agent** pour que les modifications soient prises en compte.

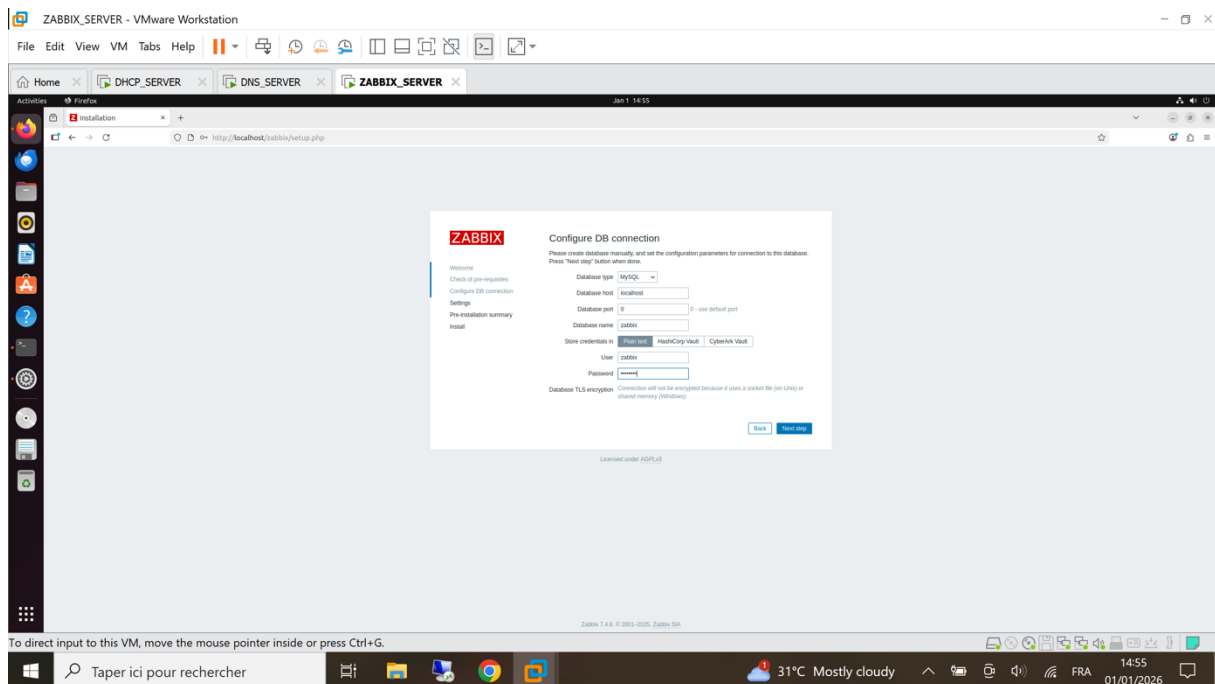
# Test de fonctionnement

À partir du serveur zabbix, ouvrez le navigateur web > Saisissez au niveau de la barre d'URL <http://localhost/zabbix>

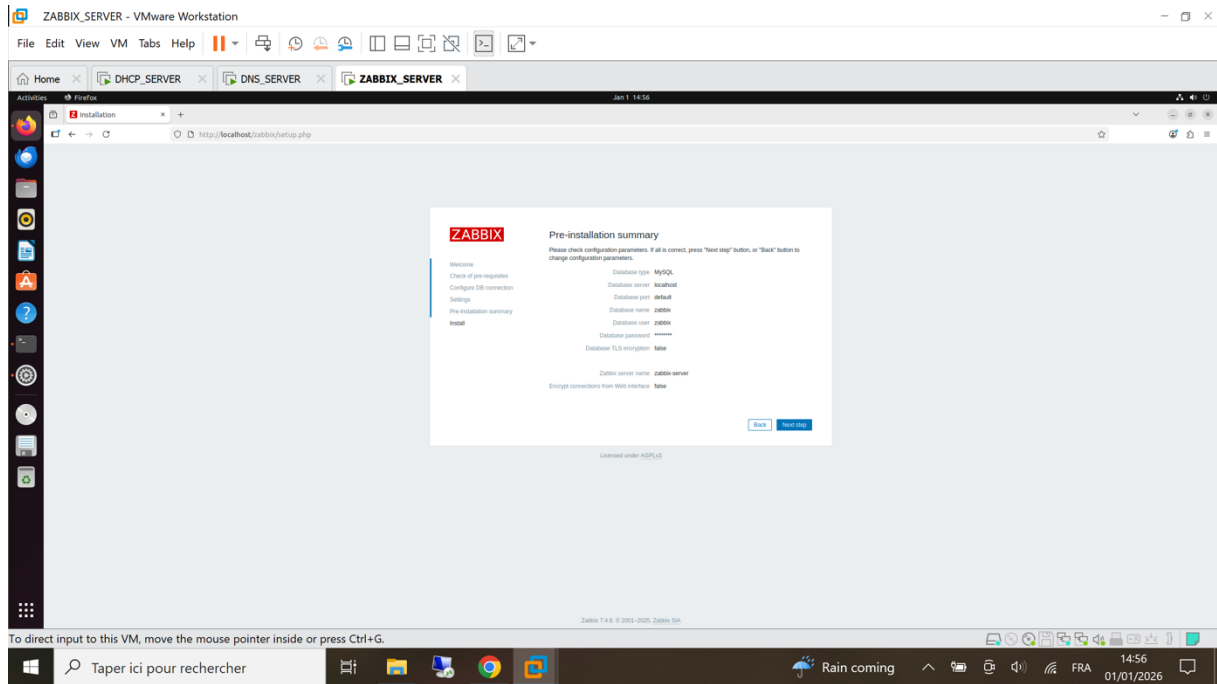


Ensuite renseignez les informations comme suit :

- Database name : **zabbix**
- User : **zabbix**
- Password : **password**
- Zabbix server name : **zabbix-server**



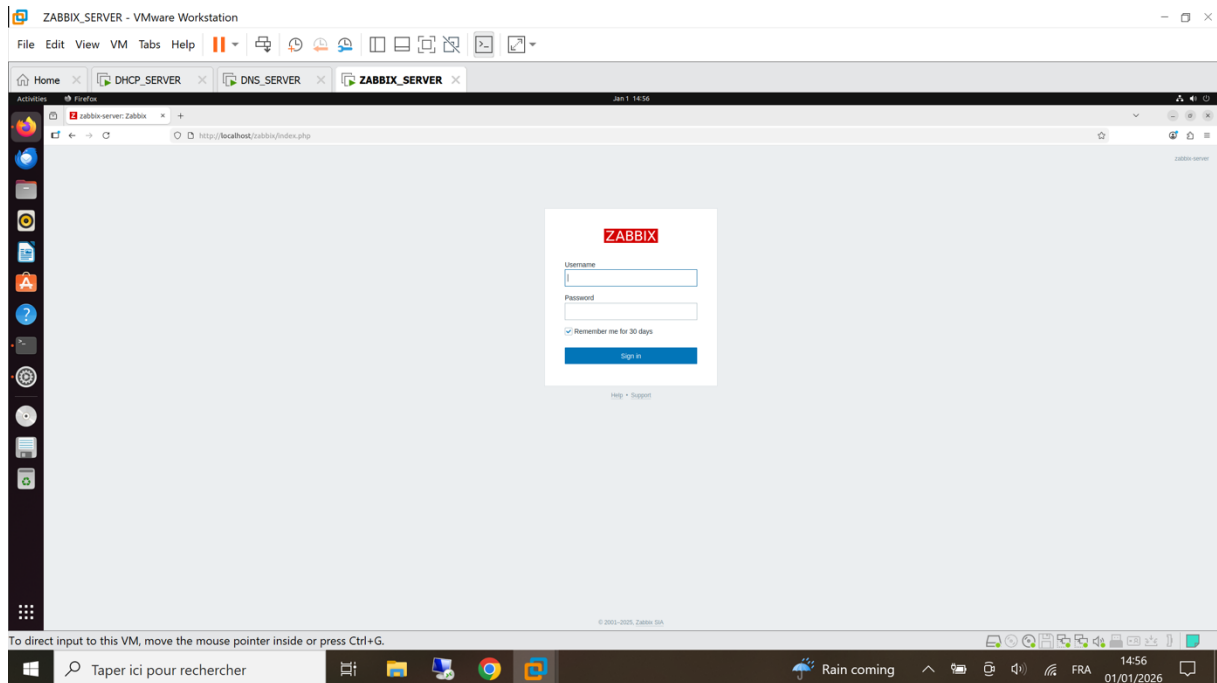
Un récapitulatif de vos paramètres s'affichera avant la confirmation, comme illustré ci-dessous.



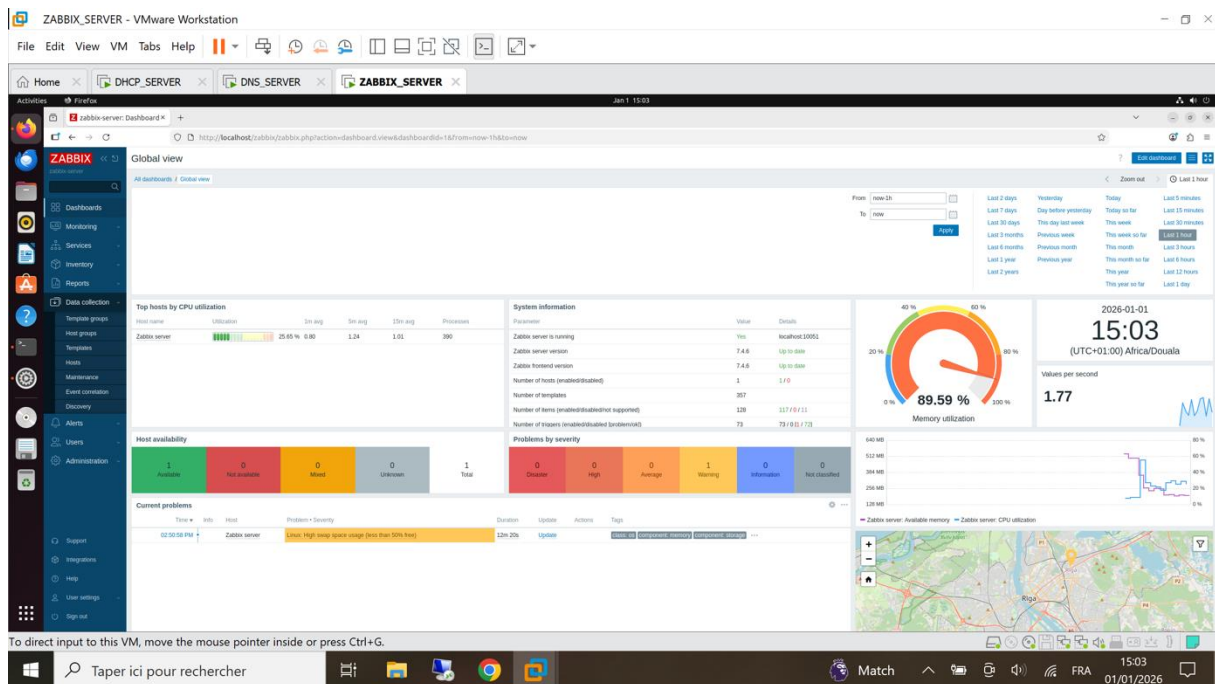
Une fois que la configuration est terminée, l'interface de connexion de Zabbix s'affiche. Les identifiants par défaut sont :

Username : Admin

Password : zabbix



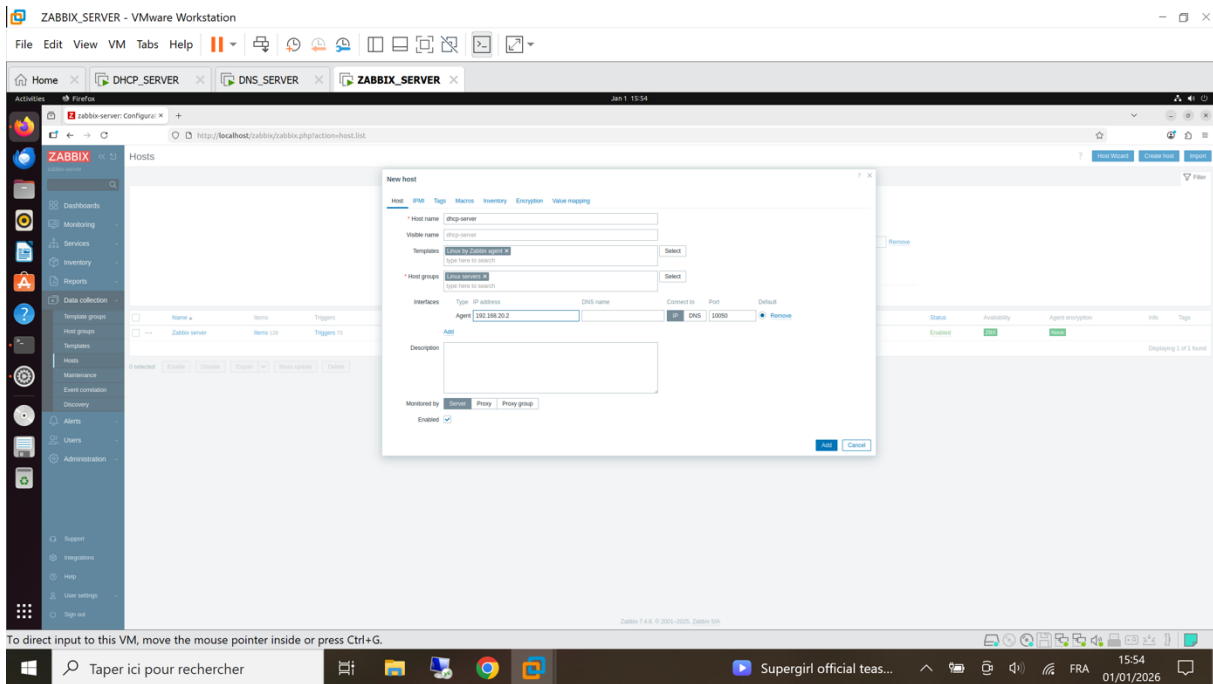
Le **tableau de bord** s'affiche alors, comme illustré ci-dessous.



À partir de ce point nous pouvons ajouter les machines à superviser. Pour ce faire, déroulez section Data collection dans le volet à gauche > Hosts > Create host > Saisissez les informations suivantes :

Host name : **dhcp-server**  
Templates : **Linux by Zabbix agent**  
Host groups: **Linux servers**  
Interfaces: **192.168.20.2**

Puis cliquez sur Add



Pour ajouter le serveur dns, cliquez sur Create host > Saisissez les informations suivantes :

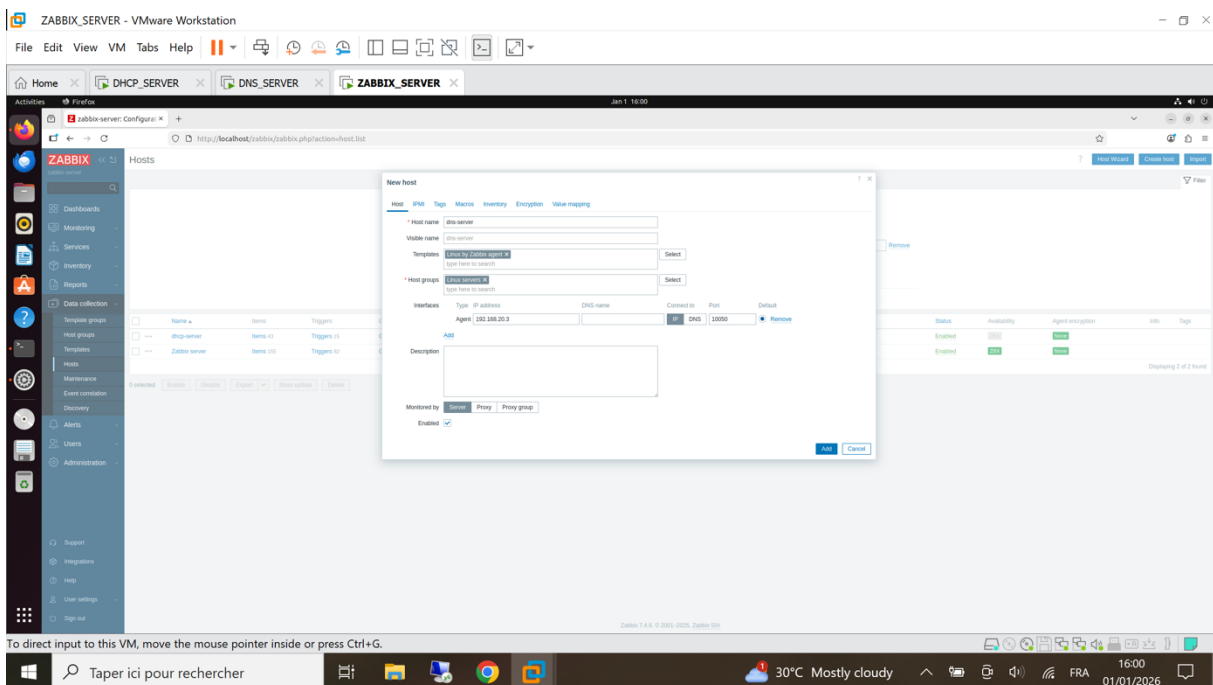
Host name : dns-server

Templates : Linux by Zabbix agent

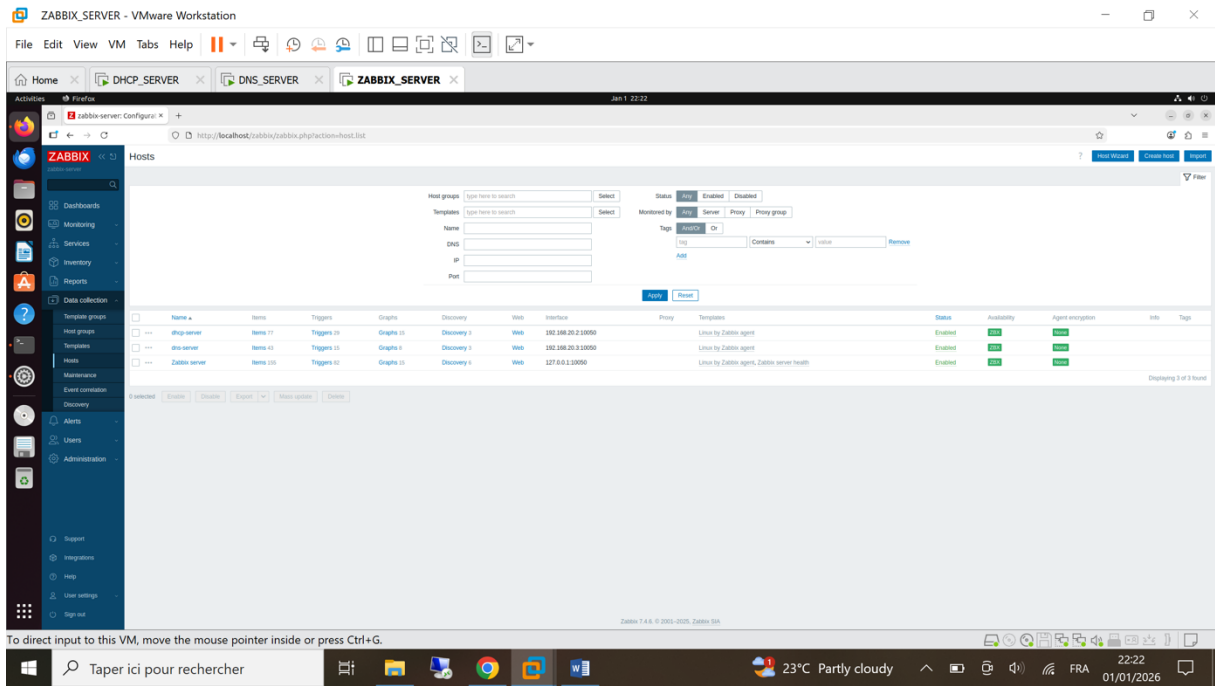
Host groups: Linux servers

Interfaces: 192.168.20.3

Puis cliquez sur Add



Une fois les configurations terminées, les deux serveurs apparaissent désormais dans la liste des hôtes.



Depuis ce tableau de bord, il est possible d'obtenir un aperçu global de l'état de fonctionnement de tous les serveurs.

