

**TP5 : Déploiement des services ISC DHCP – Web Apache 2.0 et DNS Bind9**

**Auteur : BLONDEAU Joan**

**Date : 03 Avril 2024**

**Sommaire**

**Étape 0 : Création des Machines Virtuelles**

1. Création des machines virtuelles

**Étape 1: Réalisation de l'Infrastructure Réseau**

1. Configuration des Interfaces Réseau

2. Apllication des changements

**Étape 2: Mise à Jour des Paquets du SE Linux Debian Bookworm**

1. Configuration des Sources de Paquets (sites miroirs)

2. Rôles des lignes

3. A quoi sert ‘**apt update’** et ‘**apt upgrade’**?

**Étape 3: Déploiement du Service DHCP**

1. Installation du serveur dhcp avec « apt install isc-dhcp-server »

2. Copie du fichier « dhcp.conf »

3. Edition du fichier « isc-dhcp-server »

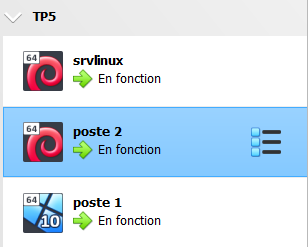
**Étape 4: Déploiement du Service Web Apache 2.0**

1. Installation d'Apache 2.0
2. Création de la page
3. Configuration d'un Hôte Virtuel
4. Tests d'Accès au Site Web

**Étape 5: Déploiement du Service DNS Bind9**

1. Installation et configuration du Service DNS
2. Ajout des zones de cherche directe et inversée
3. Tests de Résolution DNS

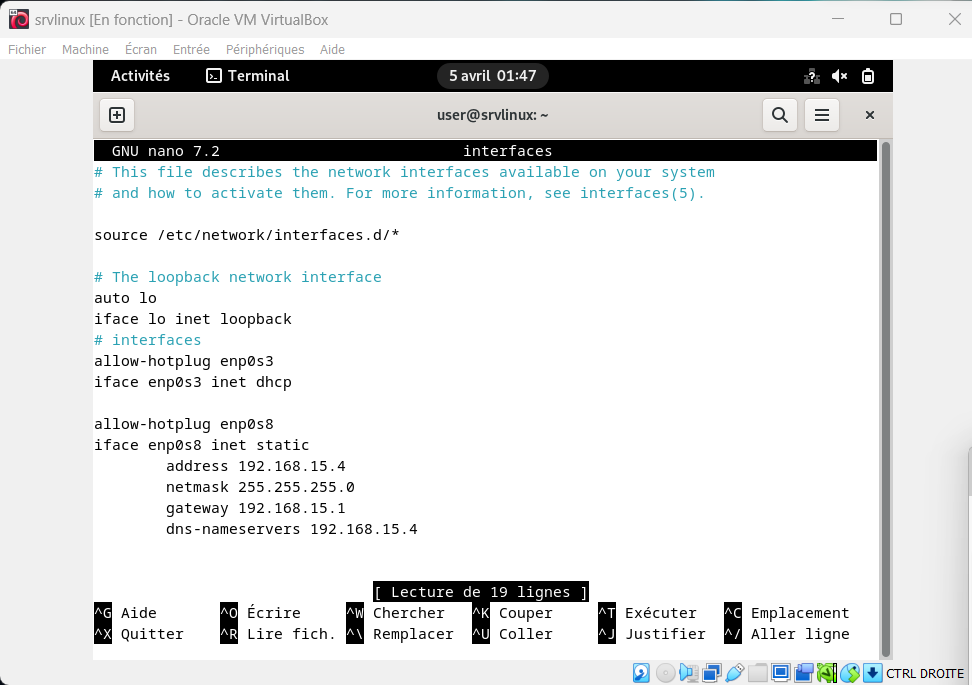
**Étape 0 :** Création des machines virtuelles



**Étape 1 :** Réalisation de l’infrastructure réseau

1. Pour commencer, on va se rendre dans /etc/network/interfaces et on va configurer le fichier comme ceci :

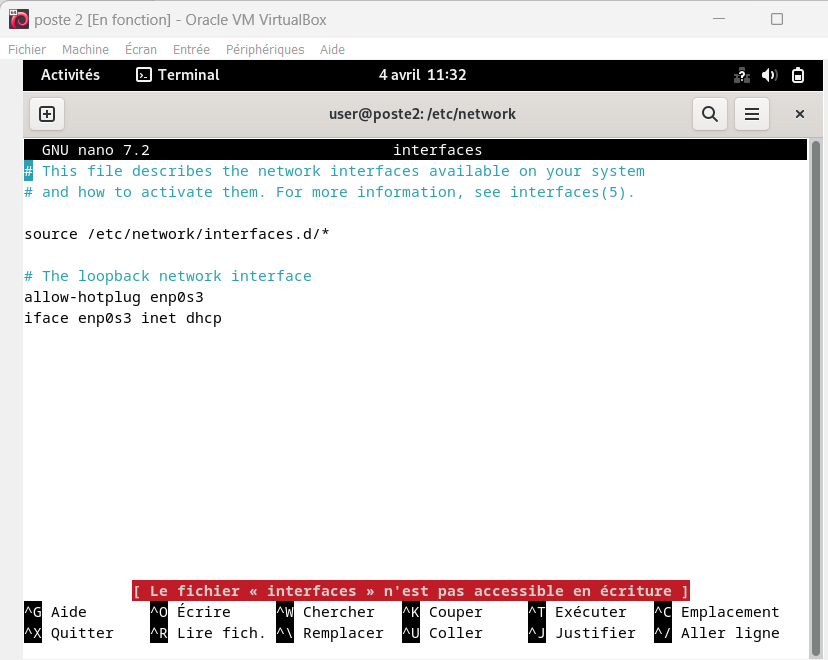
Sur le serveur :



Sur le poste 1 :

Dans la configuration de la carte réseau, il mettre « Obtenir une adresse IP atomiquement » et « Obtenir les adresses des serveurs DNS automatiquement »

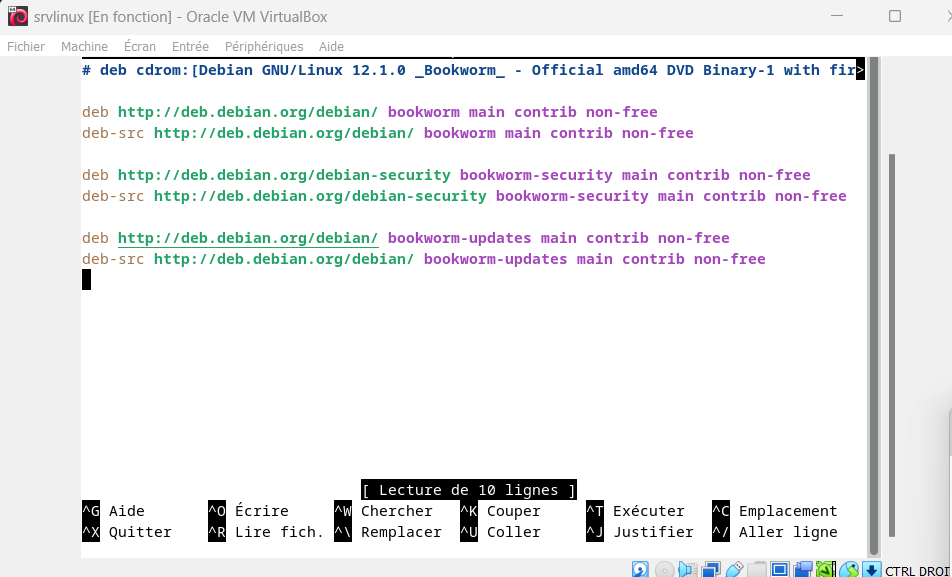
Sur le poste 2 :



2. Pour appliquer les changements, il faut exécuter la commande « **systemctl restart networking** ».

**Étape 2 :** : Mise à jour des paquets du SE Linux Debian Bookworm

1. Indication des sites miroirs



2. Rôle des lignes précédentes

Les lignes indiquées sont des sources de paquets pour APT dans Debian Bookworm, définissant où télécharger les paquets et les mises à jour :

- `deb` et `deb-src` différencient les paquets binaires des sources. `deb` est pour les binaires utilisables directement, `deb-src` pour les codes sources.

- `http://deb.debian.org/debian/ bookworm main contrib non-free` pointe vers le dépôt principal de Debian Bookworm, offrant trois catégories de logiciels :

- « main » pour les logiciels libres,

- « contrib » pour les logiciels libres dépendant de logiciels non libres,

- « non-free » pour les logiciels non libres.

- « `http://deb.debian.org/debian-security bookworm-security main contrib non-free` » est le dépôt de sécurité pour les mises à jour critiques.

- « `http://deb.debian.org/debian/ bookworm-updates main contrib non-free` » contient les mises à jour en temps réel pour les paquets de Bookworm.

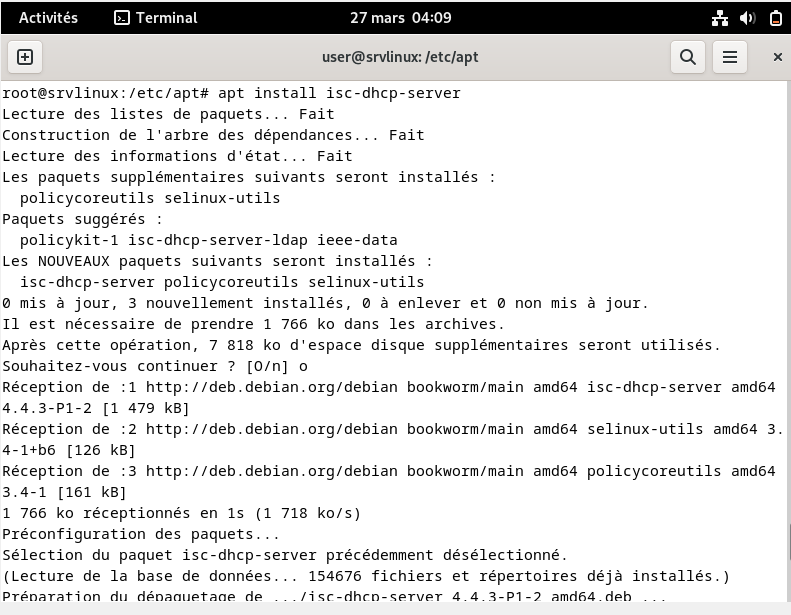
Ces sources permettent à APT de maintenir le système à jour avec les dernières versions de logiciels et corrections de sécurité.

3. A quoi sert ‘**apt update’** et ‘**apt upgrade’**? :

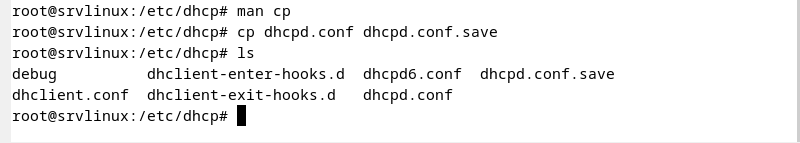
`**apt update**` télécharge la liste des mises à jour disponibles sans les installer, tandis que `**apt upgrade**` installe ces mises à jour pour les paquets déjà présents sur le système, sans supprimer de paquets existants.

**Étape 3 :** Déploiement du service DHCP

1. Installation du serveur dhcp avec « apt install isc-dhcp-server »

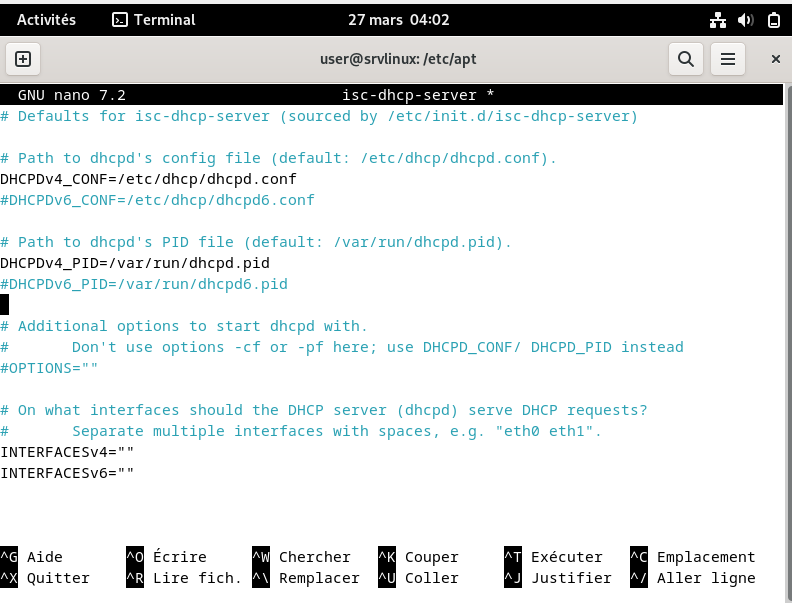


1. Copie du fichier « dhcp.conf » en « dhcp.conf.save » afin d’avoir une sauvegarde du fichier de base au cas où l’on voudrait revenir à la version initial.



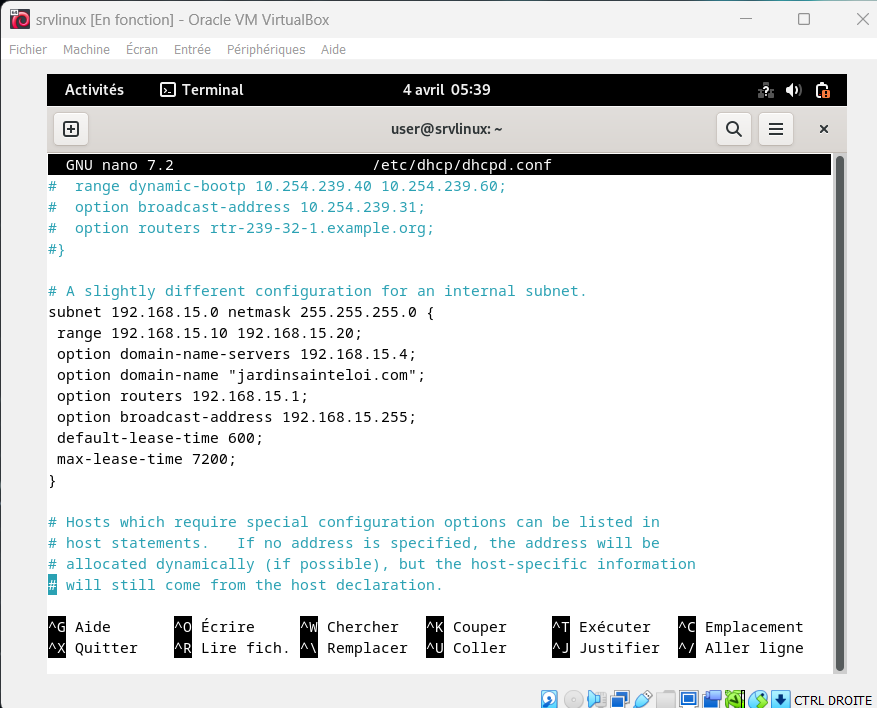
1. A l’aide de la commande « nano », on va editer le fichier « /etc/default/isc-dhcp-server » et décommettez les lignes correspondant aux paramètres suivants :

* Prendre en compte le fichier de configuration « /etc/dhcp/dhcpd.conf »
* Générer le fichier contenant l’identifiant du processus du service dhcp
* Préciser l’interface réseau (ethernet) qui distribue les configurations IP v4 automatiquement.

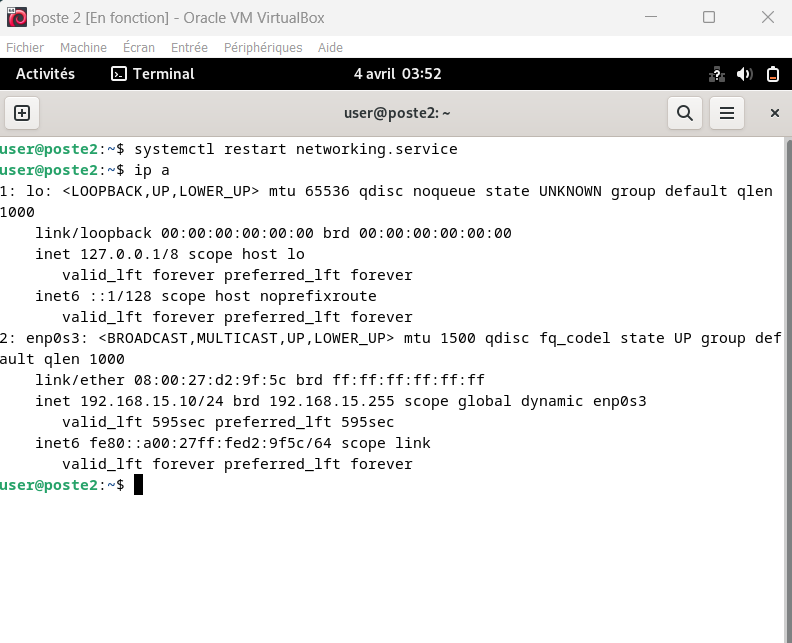


1. A l’aide de la commande « nano », éditez le fichier « dhcp.conf » et configurez le DHCP à l’aide des paramètres suivants :

* Nom de domaine
* Adresse IP du serveur DNS
* Temps attribution d’une adresse
* Temps maximal d’attribution d’une adresse
* Adresse réseau, masque de sous-réseau, plage d’adresses IP, adresse de diffusion,
* Adresse du routeur (passerelle), Adresse IP du DNS, Nom de domaine Indiquez la configuration à réaliser pour exclure les deux premières adresses IP attribuées à la passerelle et au serveur « srvlinux ».

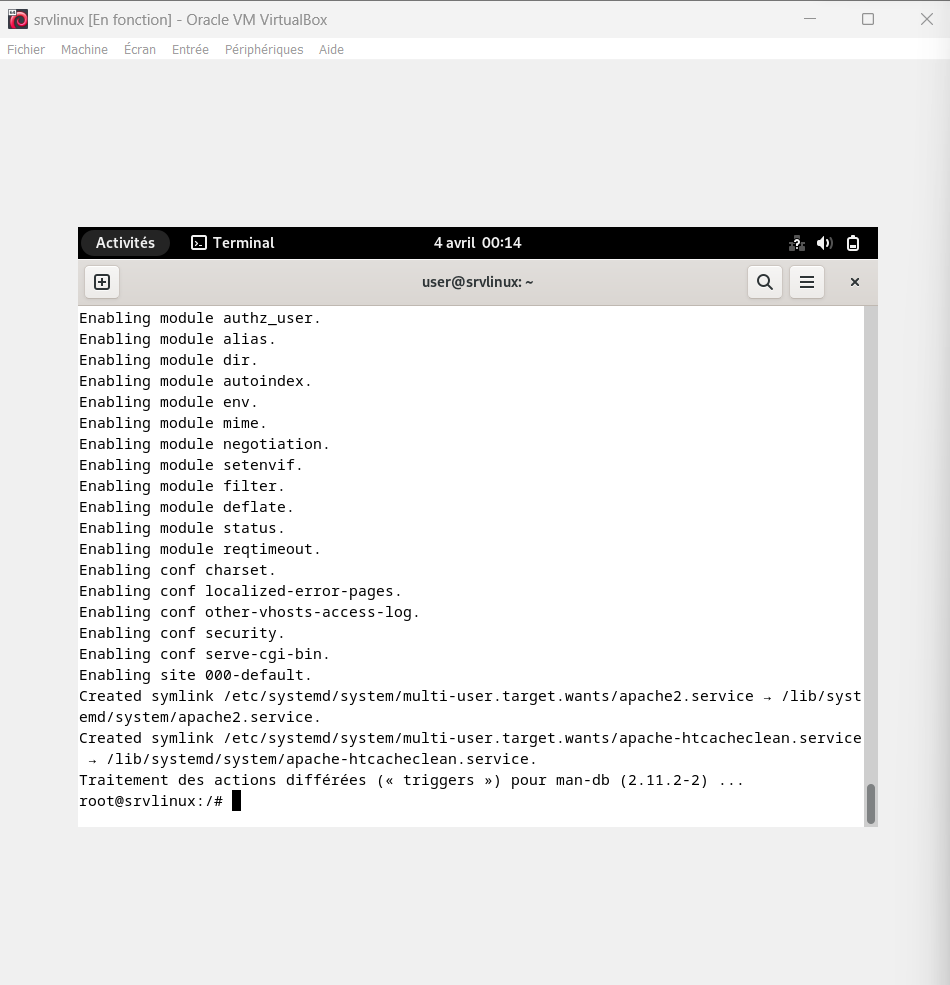


1. On va ensuite relancer le service DHCP avec la commande « systemctl restart networking »
2. Il faut maintenant tester le DHCP sur les postes clients :



**Étape 4 :** Déploiement du service web Apache 2.0

1. Installation du service web Apache 2 avec « apt install apache2 -y »



2. Test du service web Apache

Commencez par vérifier si le service Apache est actif et en cours d'exécution sur votre serveur. Ouvrez un terminal sur votre serveur et exécutez la commande suivante :

*« sudo systemctl status apache2 »*

Si Apache est actif, vous devriez voir une sortie indiquant que le service est actif (running). Si ce n'est pas le cas, vous pouvez démarrer Apache avec la commande :

*« sudo systemctl start apache2 »*

1. Rôle des lignes précédées des instructions « **Include**»

Dans un fichier de configuration **apache2.conf** pour le serveur web Apache, les lignes précédées de l'instruction **Include** servent à intégrer le contenu d'autres fichiers de configuration au fichier principal. Ceci permet d'organiser la configuration en plusieurs fichiers séparés, facilitant ainsi la gestion et la personnalisation des paramètres sans surcharger le fichier **apache2.conf**.

1. Rôle des fichiers dans apache2.conf :

Le fichier `apache2.conf` est le fichier de configuration principal d'Apache sur les systèmes basés sur Debian, comme Ubuntu. Il sert à définir les paramètres globaux du serveur web et intègre différents modules et fichiers de configuration pour permettre une personnalisation et une flexibilité accrues. Voici une liste des fichiers et ensembles de fichiers couramment inclus dans `apache2.conf`, ainsi que leur rôle :

*1. `ports.conf`*

Ce fichier définit sur quels ports Apache doit écouter les requêtes entrantes. Par défaut, Apache est configuré pour écouter sur le port 80 pour les requêtes HTTP non sécurisées et peut également être configuré pour écouter sur le port 443 pour les requêtes HTTPS sécurisées.

*2. Modules (`mods-enabled/\*.load`, `mods-enabled/\*.conf`)*

Ces fichiers sont des liens symboliques vers les fichiers de configuration des modules situés dans `/etc/apache2/mods-available/`. Les fichiers `\*.load` contiennent des instructions pour charger les modules, tandis que les fichiers `\*.conf` contiennent la configuration spécifique à chaque module. Ces modules peuvent ajouter des fonctionnalités supplémentaires à Apache, comme le réécriture d'URLs, le chiffrement SSL/TLS, etc.

*3. Sites (`sites-enabled/\*.conf`)*

Ces fichiers sont des liens symboliques vers les configurations de sites spécifiques situées dans `/etc/apache2/sites-available/`. Chaque fichier `\*.conf` dans `sites-enabled` configure un site virtuel distinct pouvant être servi par Apache. Cela permet à Apache de gérer plusieurs sites web sur un seul serveur physique.

*4. Configuration de la sécurité (`conf-enabled/security.conf`)*

Ce fichier contient des paramètres de configuration destinés à renforcer la sécurité du serveur Apache. Il peut inclure des directives pour masquer la version d'Apache, limiter les méthodes HTTP autorisées, et configurer d'autres paramètres liés à la sécurité.

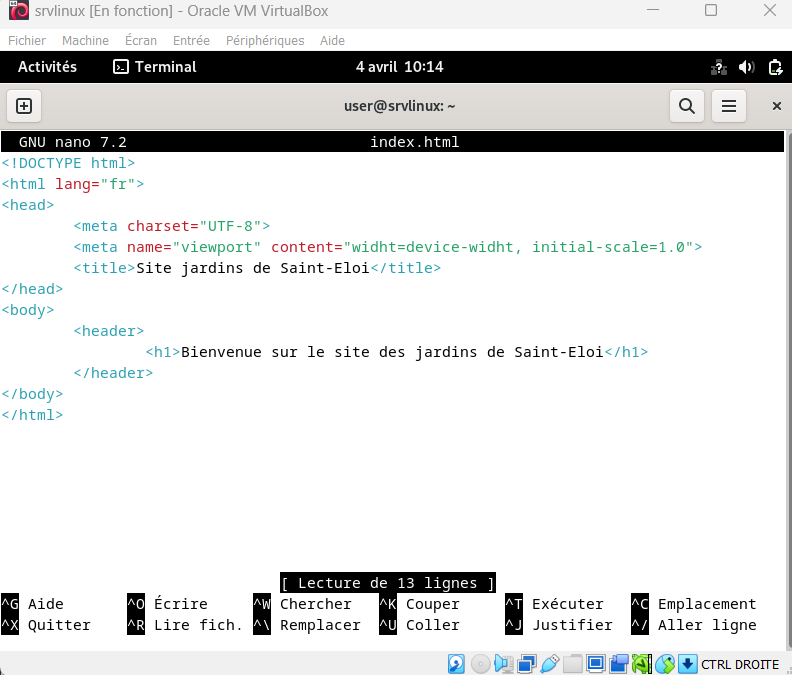
*5. Fichiers de configuration supplémentaires (`conf-enabled/\*.conf`)*

En plus de la configuration de la sécurité, d'autres fichiers dans `conf-enabled` peuvent inclure des configurations globales pour Apache, telles que la personnalisation des fichiers log, les paramètres de langue, etc. Ces fichiers sont aussi des liens symboliques vers les configurations disponibles dans `conf-available`.

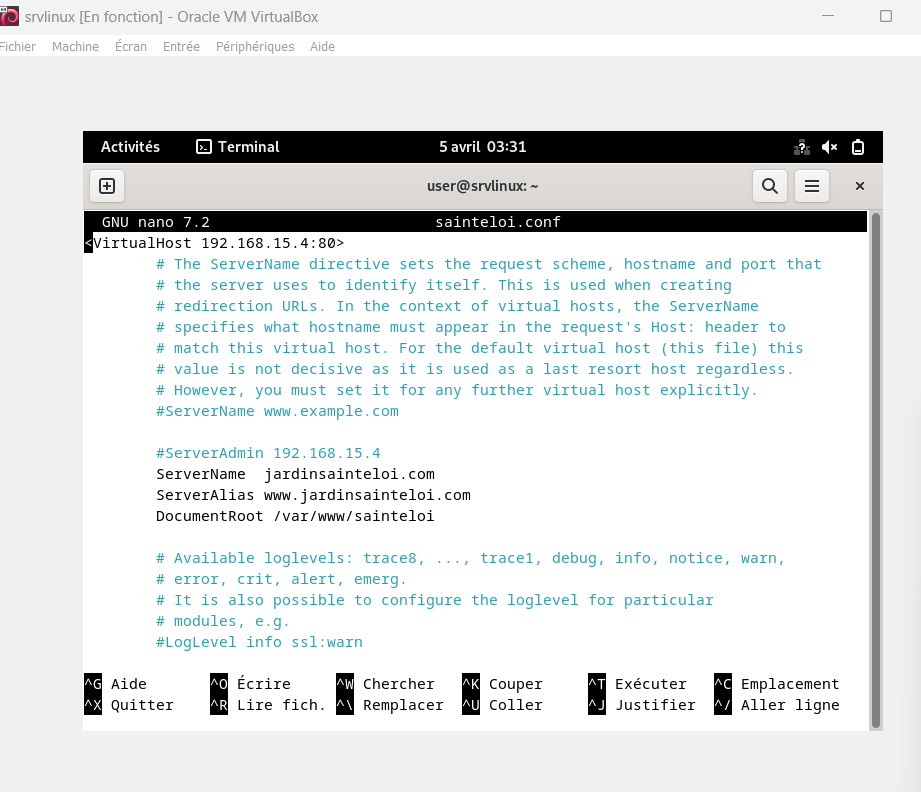
*6. Fichiers de log (`ErrorLog`, `CustomLog`)*

Bien que spécifiquement des directives plutôt que des fichiers inclus, ces directives dans `apache2.conf` spécifient l'emplacement des fichiers de log où Apache enregistre les erreurs (`ErrorLog`) et les requêtes au serveur (`CustomLog`). Ces logs sont cruciaux pour le dépannage et l'analyse de la sécurité.

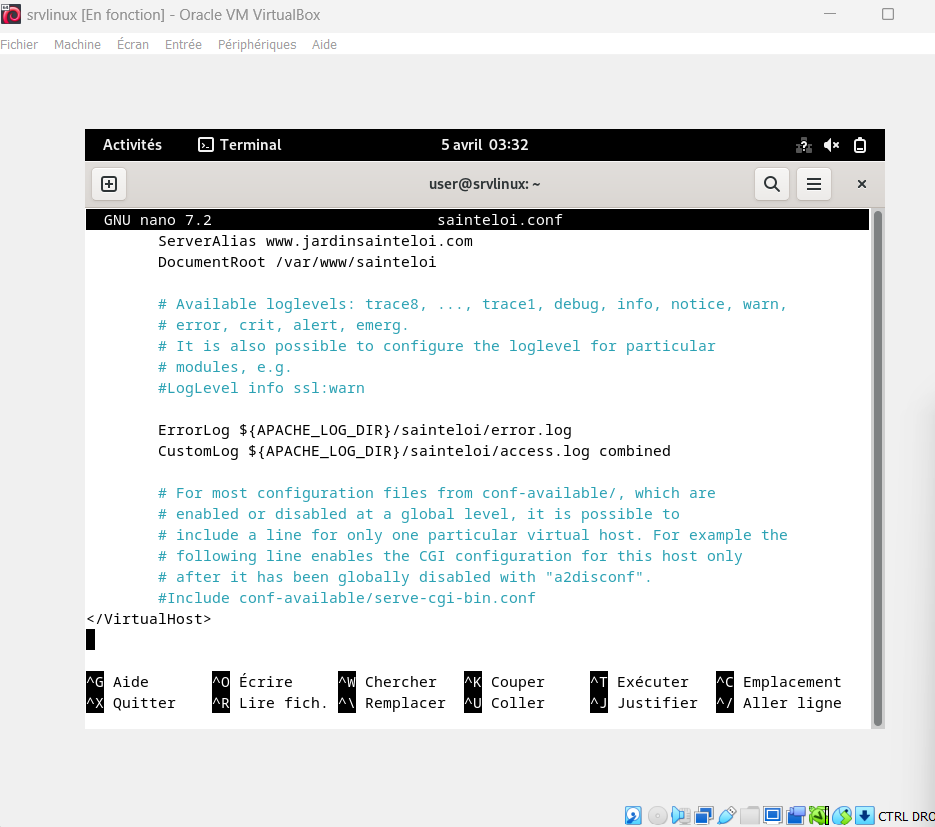
1. Création de la page « index.html » dans « var/www/sainteloi »



1. Création de la copie du fichier « 000-default.conf » en « sainteloi.conf » avec la commande « **cp 000-default.conf sainteloi.conf** »
2. Création de l’hôte virtuelle



1. Suivis des connexions au serveur apache



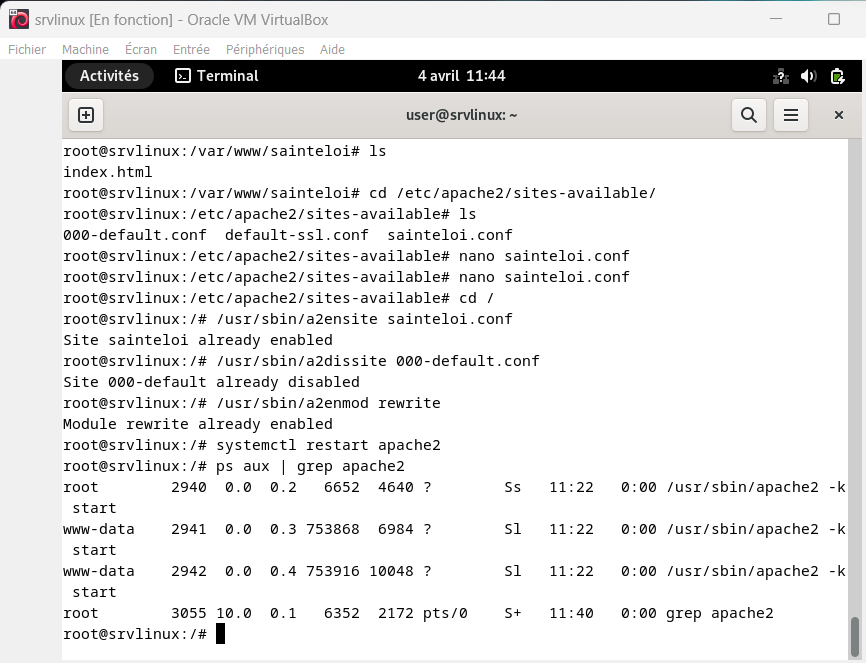
1. Test de l’accès à la page web

Poste 1 :



Poste 2 :



1. Saisie de la commande « ps aux | grep apache2 »

La commande `ps aux | grep apache2` est utilisée pour filtrer et afficher les processus en cours d'exécution qui sont liés au serveur web Apache2. Voici une décomposition de son fonctionnement :

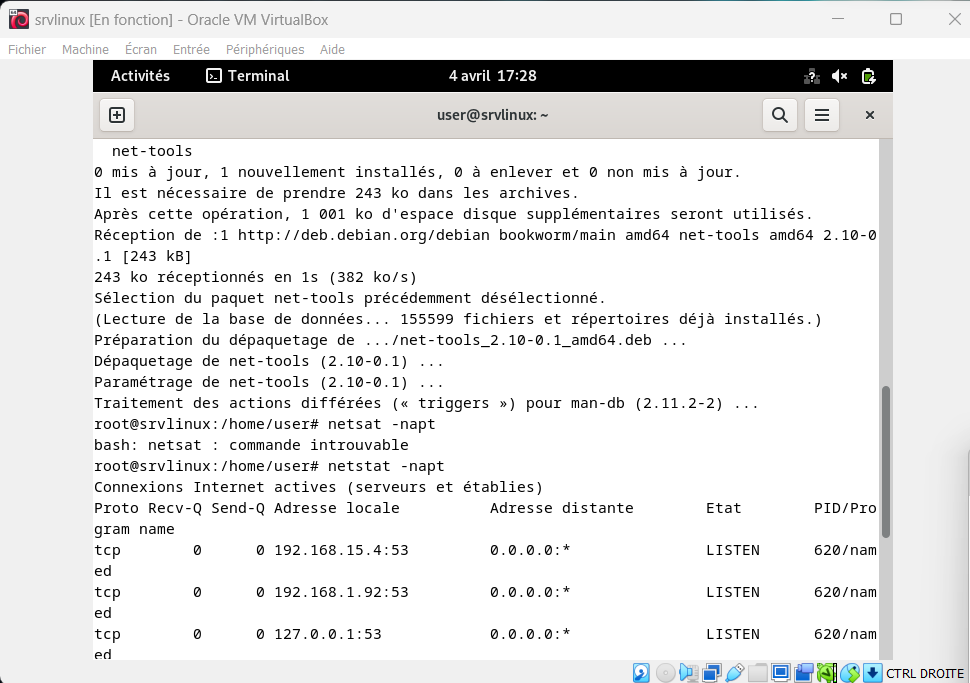
- `ps aux` : Affiche tous les processus en cours sur le système. L'option `a` affiche les processus de tous les utilisateurs, `u` donne une sortie détaillée incluant l'utilisateur qui exécute le processus, et `x` inclut les processus sans terminal de contrôle.

- `|` : Un pipe, qui passe la sortie de la commande à gauche (ici, `ps aux`) à la commande à droite (`grep apache2`).

- `grep apache2` : Filtre la sortie pour ne montrer que les lignes contenant le texte `apache2`, ce qui est utile pour trouver les processus liés à Apache2.

PID = 2940

1. Saisie de la commande « netstat –napt »



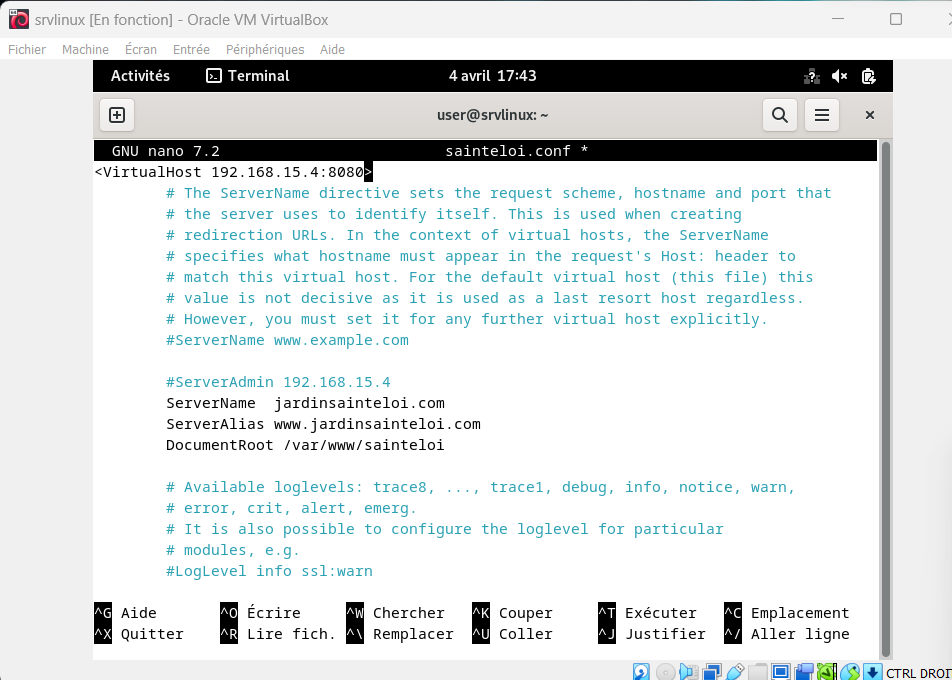
La commande `netstat –napt` est utilisée sur les systèmes Linux pour afficher les connexions réseau, les tables de routage, et les statistiques des ports d'écoute, avec une focalisation spécifique sur les connexions TCP/IP. Voici la signification de chaque option :

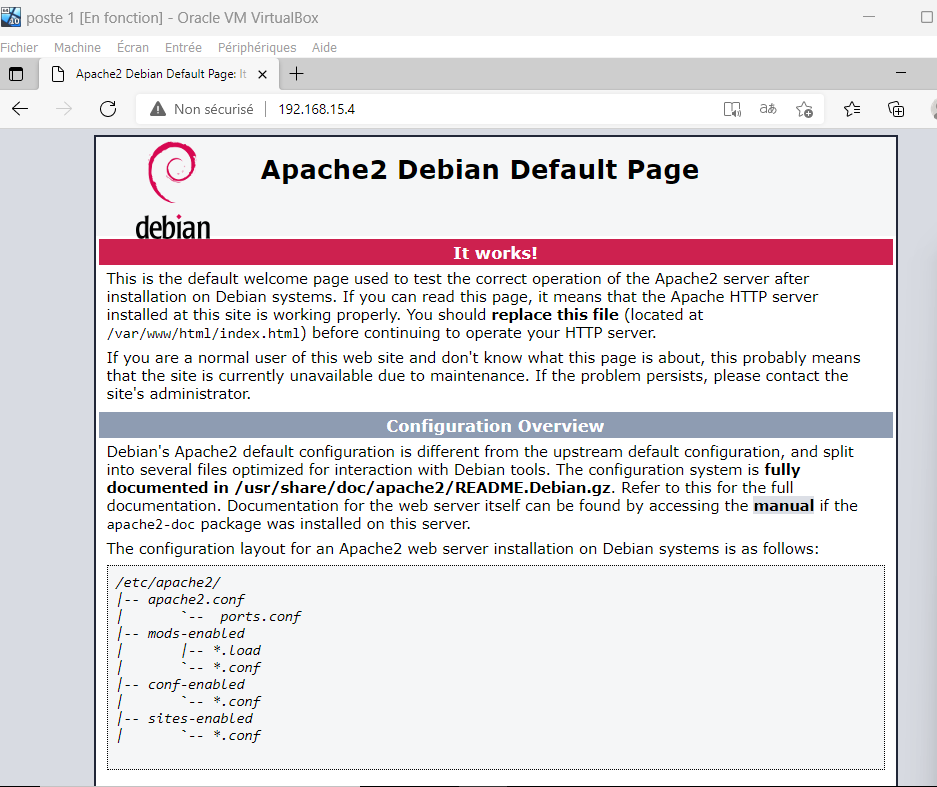
- `-n` : Affiche les adresses IP et les numéros de port en format numérique, sans les résoudre en noms de domaine, accélérant ainsi l'affichage des informations.

- `-a` : Affiche toutes les connexions et les ports d'écoute, y compris ceux en état non établi, permettant de voir aussi bien les connexions actives que les ports en attente d'une connexion.

- `-p` : Montre le nom du programme associé à chaque connexion ou port d'écoute. Cela nécessite des privilèges de superutilisateur (root) pour être affiché pour tous les processus.

- `-t` : Limite l'affichage aux connexions TCP, excluant les connexions UDP et d'autres types de connexions.

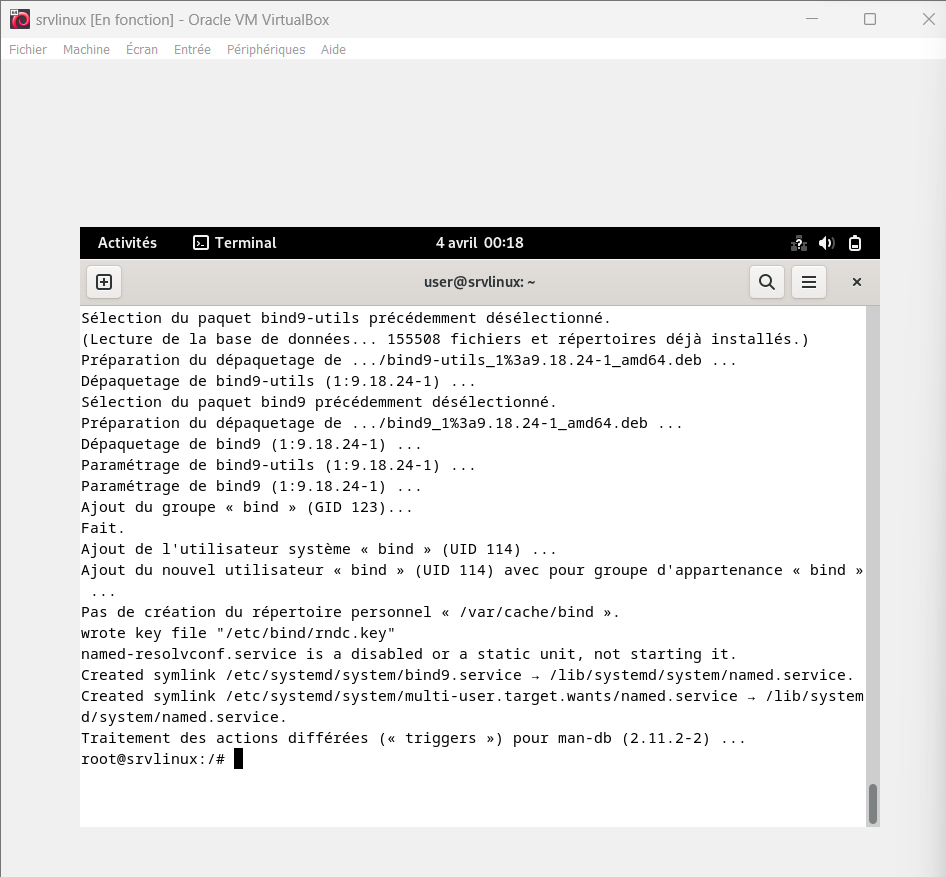
1. Modification du fichier « **sainteloi.conf** » pour changer le port d’exécution d’apache. On passe du port **80** au port **8080**
2. Test pour vérifier la modification



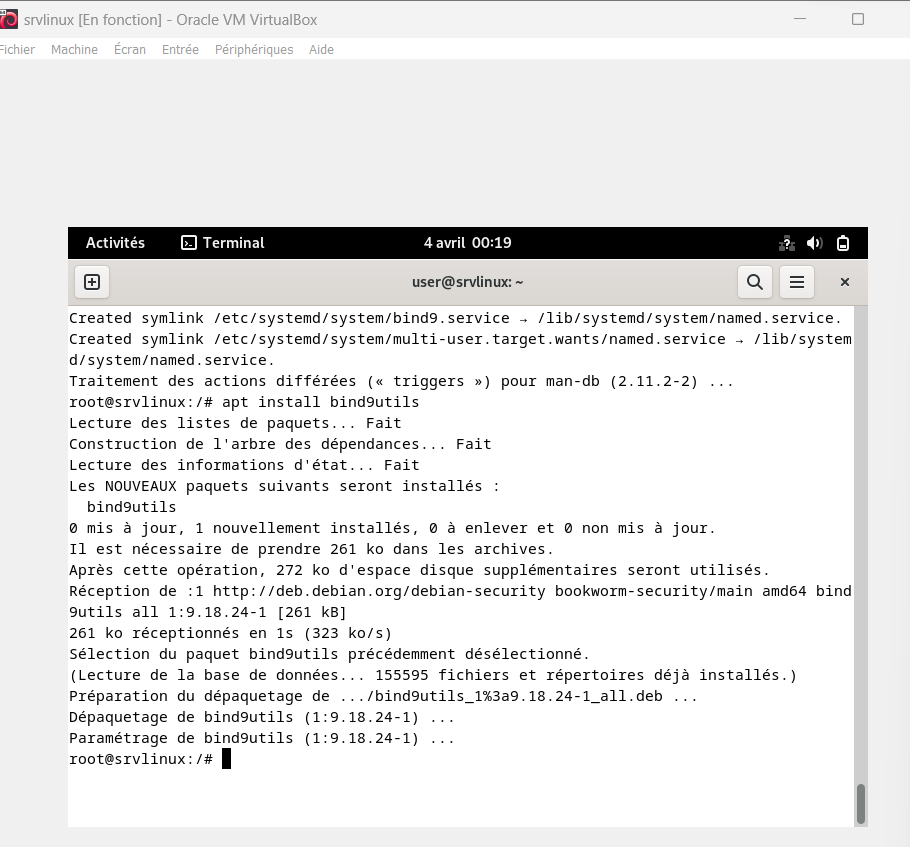
**8. Étape 5 :** Déploiement du service DNS Bind9

1. Installation de **bind9** et **bind9utils**

**Bind9**

****

**Bind9utils :**

****

2. Bind9 s'appuie sur plusieurs fichiers de configuration clés pour son fonctionnement :

- \*\*`named.conf`\*\*: Le fichier principal qui dirige Bind9, intégrant les directives globales et les références à d'autres fichiers.

- \*\*`named.conf.options`\*\*: Contient des options spécifiques au serveur, comme les configurations de sécurité et de cache.

- \*\*`named.conf.default-zones`\*\*: Définit les zones par défaut gérées par Bind9, y compris les zones racines et locales.

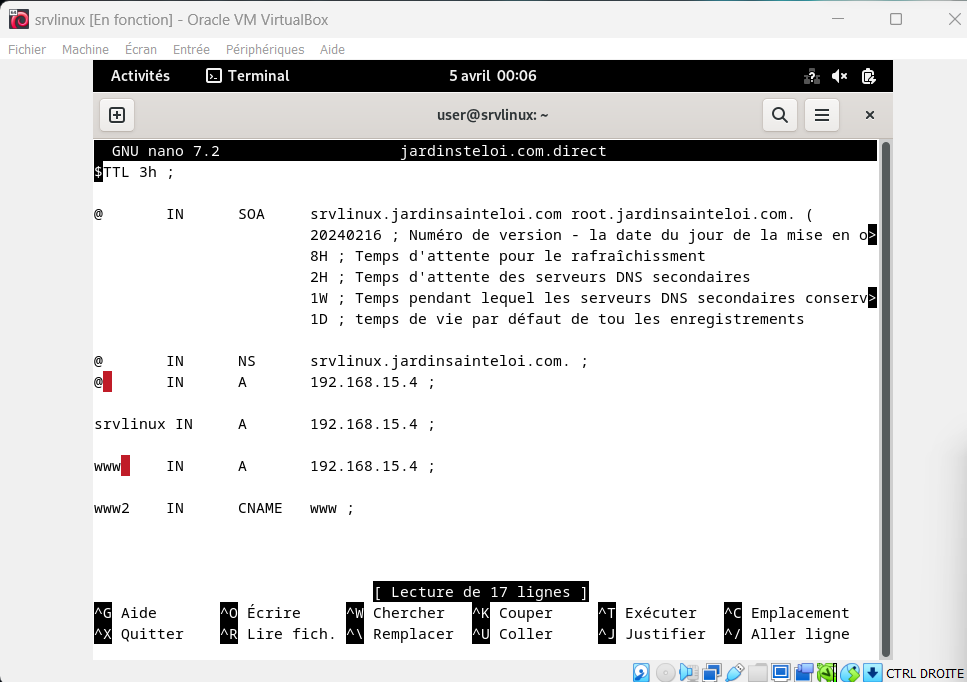
Ces fichiers structurent la configuration du serveur DNS, définissant comment les requêtes sont traitées et quelles réponses sont fournies.

3. Création des fichiers pour la recherche directe et inversée

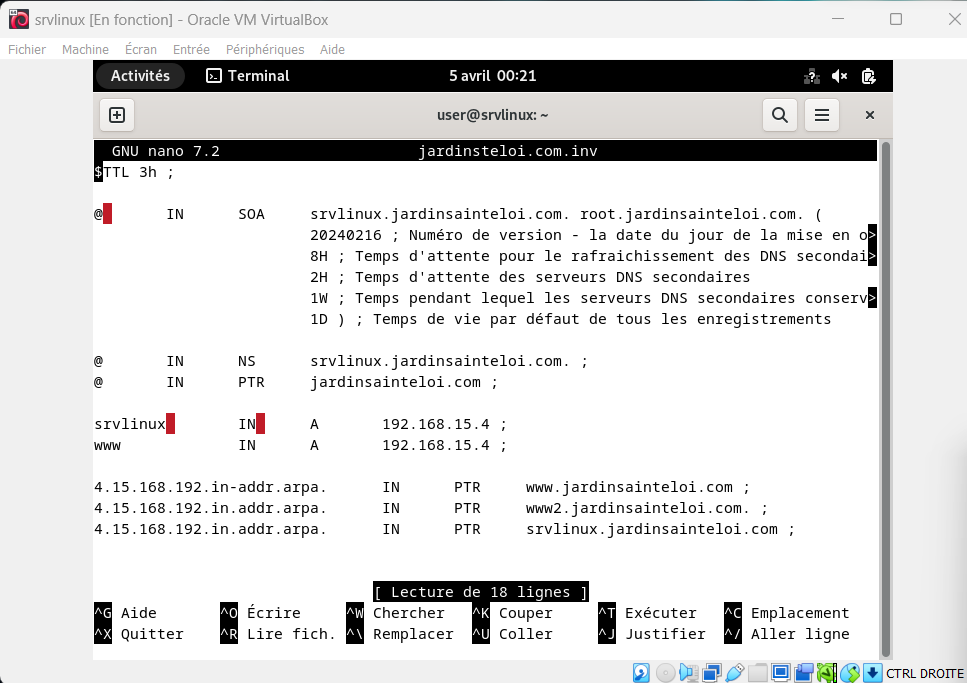
- nano jardinsteloi.com.direct

- nano jardinsteloi.com.inv

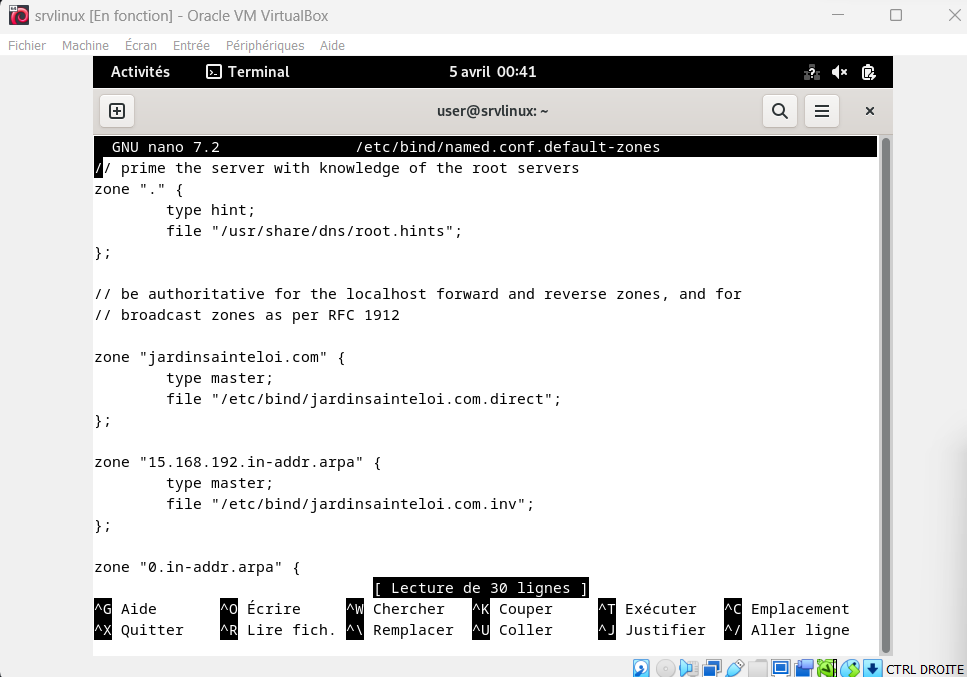
4. Configuration de jardinsainteloi.com.direct. :



1. Configuration de jardinsainteloi.com.inv. :



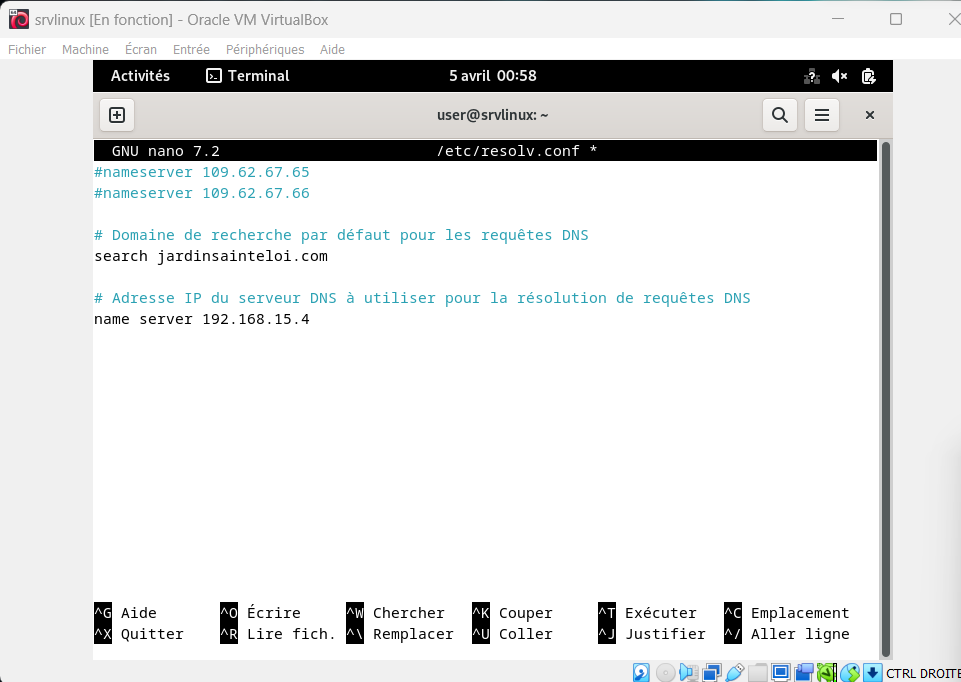
1. Ajout des zones de recherche directe et inversée



1. Saisie de la commande « **named-checkconf** »



1. Modification du fichier « **/etc/resolv.conf** »



1. Pour éviter que le contenu du fichier « **/etc/resolv.conf** », on va changer les droits d’accès avec la commande « chattr +i /etc/resolv.conf »
2. Tests

