COMPTE RENDU RAPPORT PROJET

## Création des utilisateurs et des groupes

**Étape 1 : Mettre à jour le gestionnaire de packages**

Avant d'installer un nouveau logiciel, mettez à jour la liste des référentiels de logiciels avec la commande suivante :



**Étape 2 : Mettre à niveau les paquets de mise à jour installé pour Ubuntu**

Pour installer les mises à niveau disponibles de tous les packages actuellement installés sur le système tapez la commande suivante :



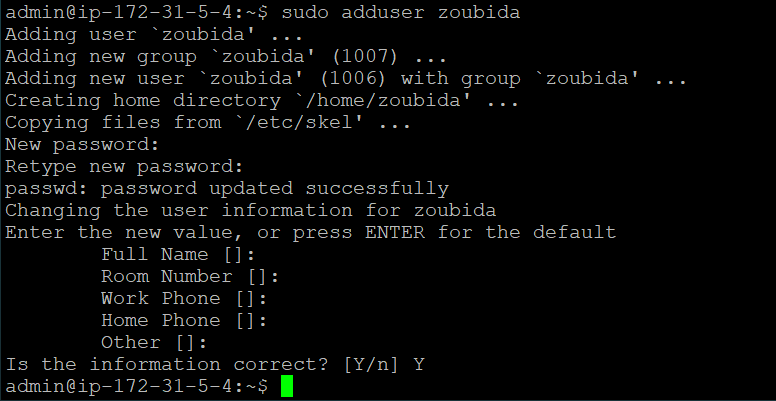
**Étape 3 :** **Création du groupe asktech**

On peut créer des groupes en tapant la commande :

**sudo groupadd asktech**

**Etape 4 : Créer les utilisateurs du groupe asktech**

Pour créer un nouveau utilisateur on tape la commande

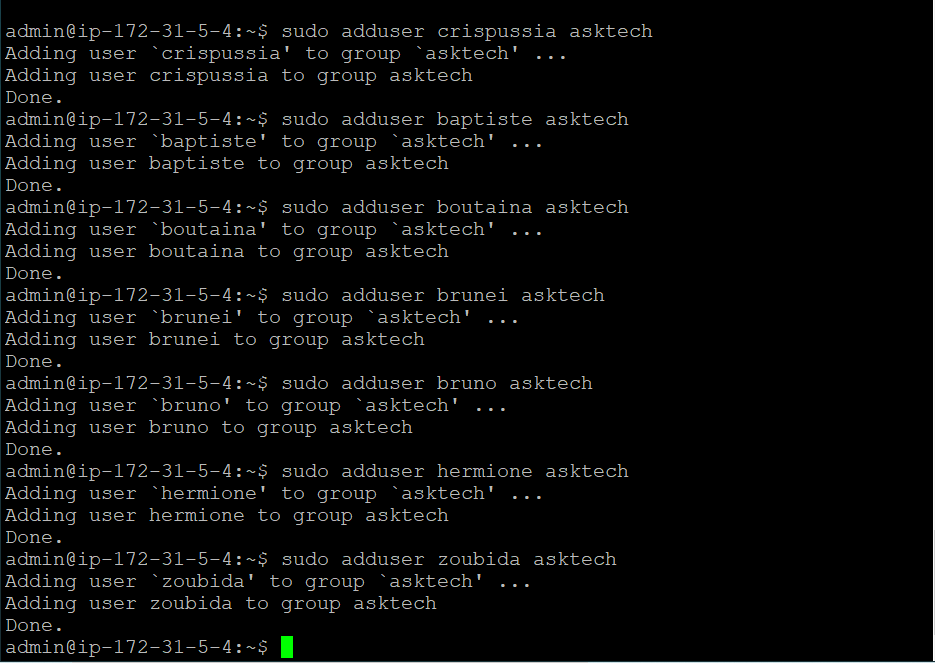
****

On répète la même commande pour tous les utilisateurs du groupe.

**Etape 5 : Ajouter les utilisateurs au groupe asktech**

Pour ajouter les utilisateurs créer au groupe asktech on tape la commande :

**sudo adduser nom\_utilisateur asktech**



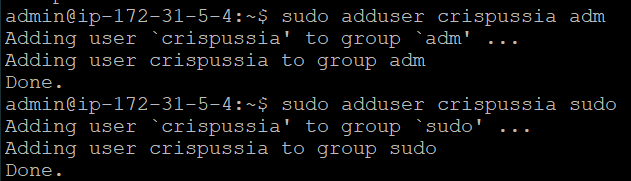
**Etape 6 : Vérifier que les utilisateurs ont été bien ajoutés au groupe**

Pour cela on tape la commande :

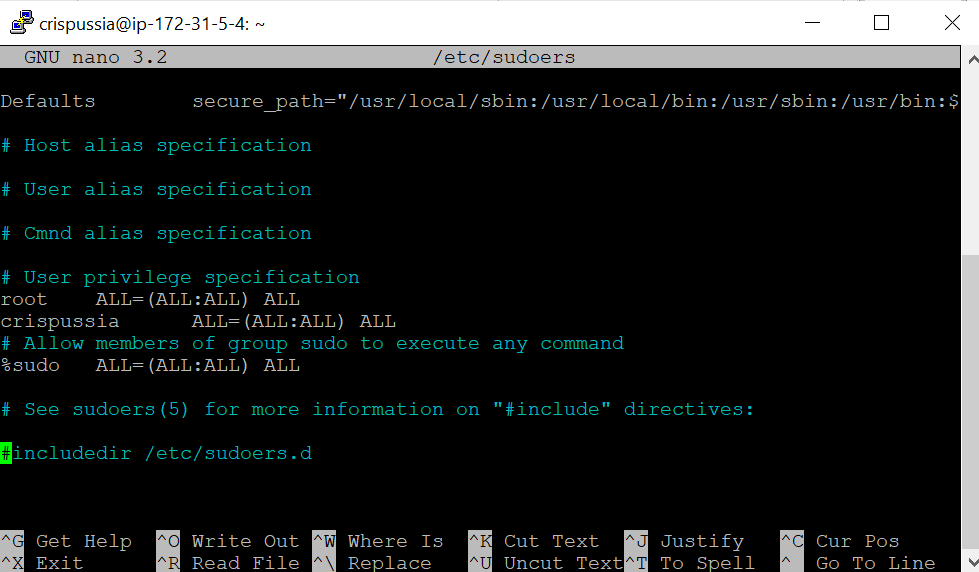
**sudo cat /etc/group**

****

**Etape 7 : Ajouter mon nom d’utilisateur Crispussia comme administrateur**

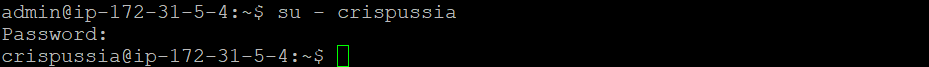


Ensuite on édite le fichier sudoers en tapant la commande : **sudo nano /etc/sudoers**



Ajouter crispussia en tant qu’utilisateur privilégier juste en dessous de celle de route.

**Etape 7 : Se connecter à mon compte utilisateur pour réaliser la connexion ssh**

****

## Connecter les utilisateurs via ssh

A cette étape nous devons permettre à tous les utilisateurs de pouvoir se connecter en renseignant la clé privée et la clé public sans demander le mot de passe.

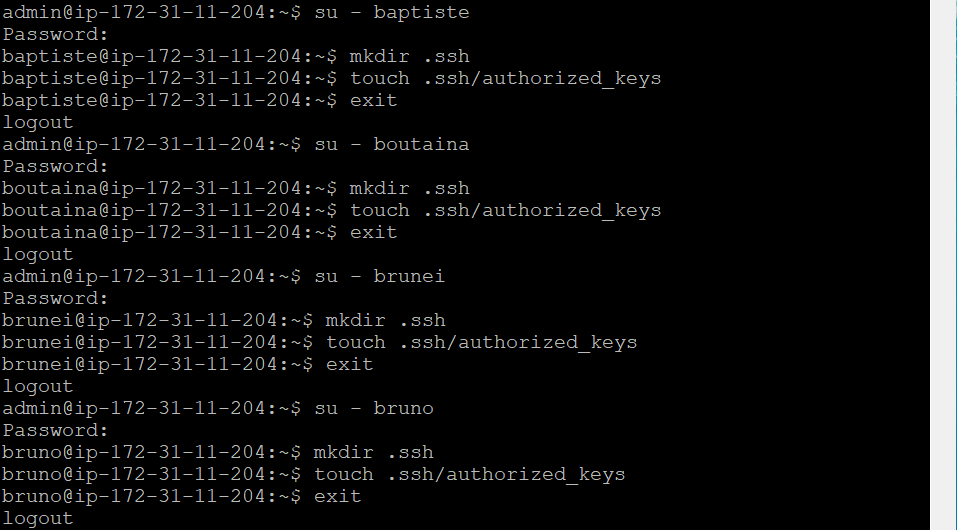
**Etape 1 : Création d’un dossier pour chaque utilisateur :**

On se connecte à chaque compte des utilisateurs puis on tape la commande:

**mkdir .ssh**

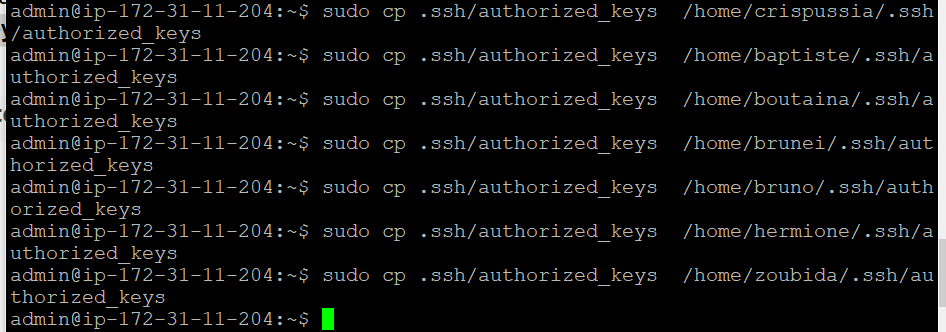
**Etape 2 : Création d’un fichier dans le dossier .ssh pour chaque utilisateur:**

On se connecte à chaque compte des utilisateurs puis on tape la commande:

**touch .ssh/authorized\_keys**

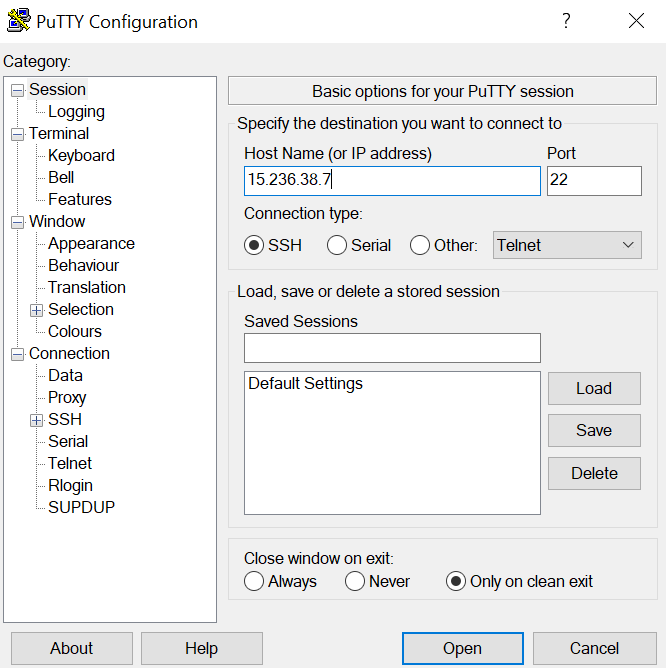
**Etape 3 : Copie du fichier authorized\_keys de l’admin dans le fichier authorized\_keys pour chaque utilisateur:**

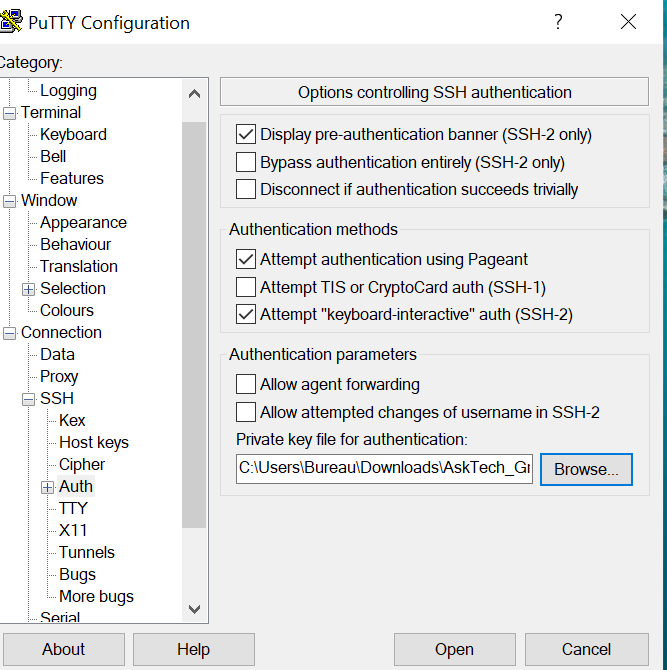
Sur le compte admin on tape la commande suivante pour chaque utilisateur:

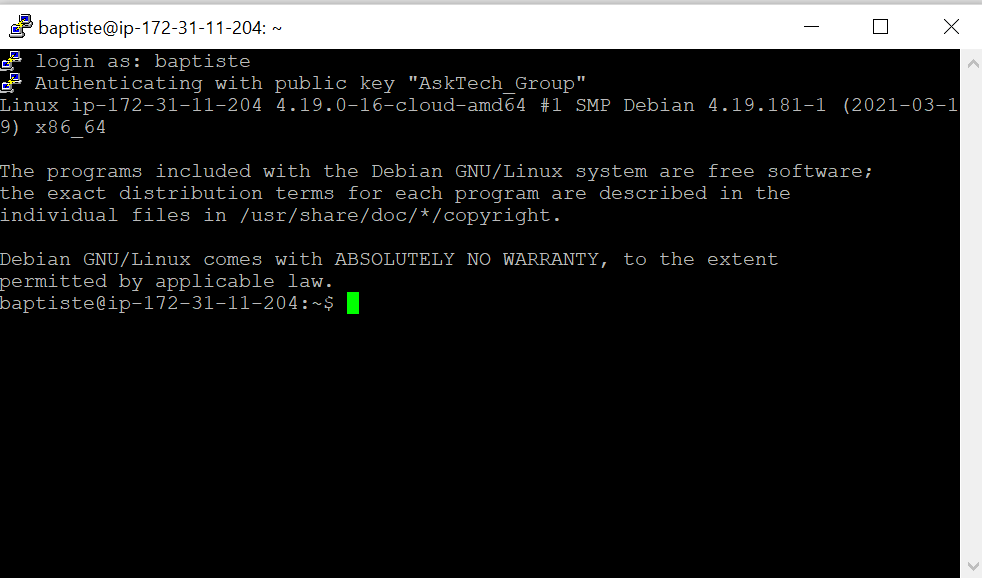
****

**Etape 4: Tester de se connecter à mon utilisateur ou un utilisateur du groupe**

On relance Putty.



****

****

La connexion ssh a bien fonctionné sans mot de passe. Tout utilisateur du groupe ainsi que l’ **admin** peut se connecter en renseignant la clé public du groupe et la clé privée.

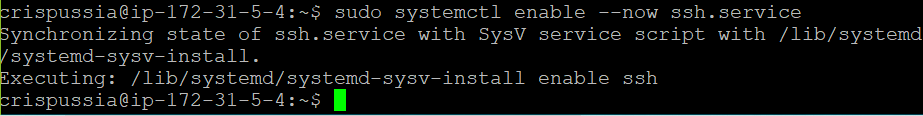
## Connecter les utilisateurs via ssh en demandant un mot de passe

**Source:**[**https://www.linuxtricks.fr/wiki/ssh-installer-et-configurer-un-serveur-ssh**](https://www.linuxtricks.fr/wiki/ssh-installer-et-configurer-un-serveur-ssh)

**Etape 1 : Configuration du serveur ssh :**

1. **Lancer le service ssh au démarrage**

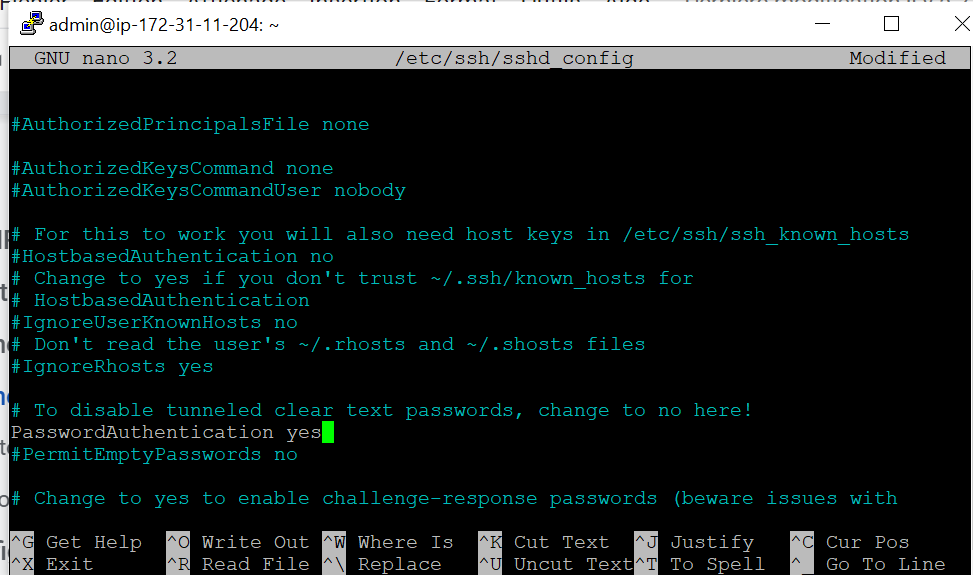
Pour lancer le service ssh au démarrage tapez la commande suivante :

**sudo systemctl enable --now ssh.service**

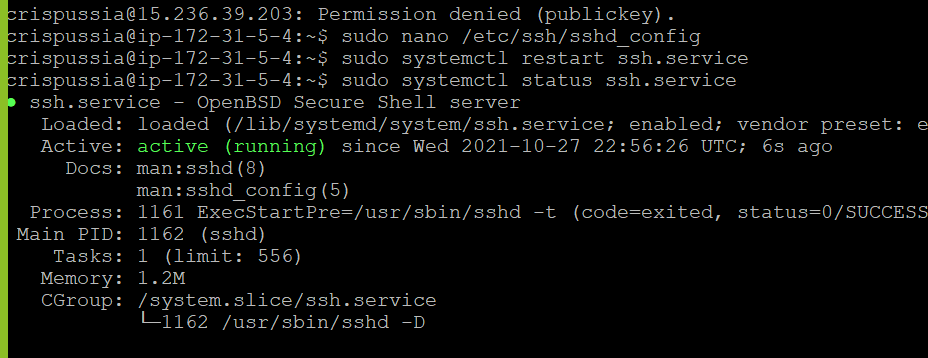
1. **Désactiver les connexions ssh en root**

Pour cela, éditer le fichier /etc/ssh/sshd\_config et modifier cette ligne :

**Password authentification yes**

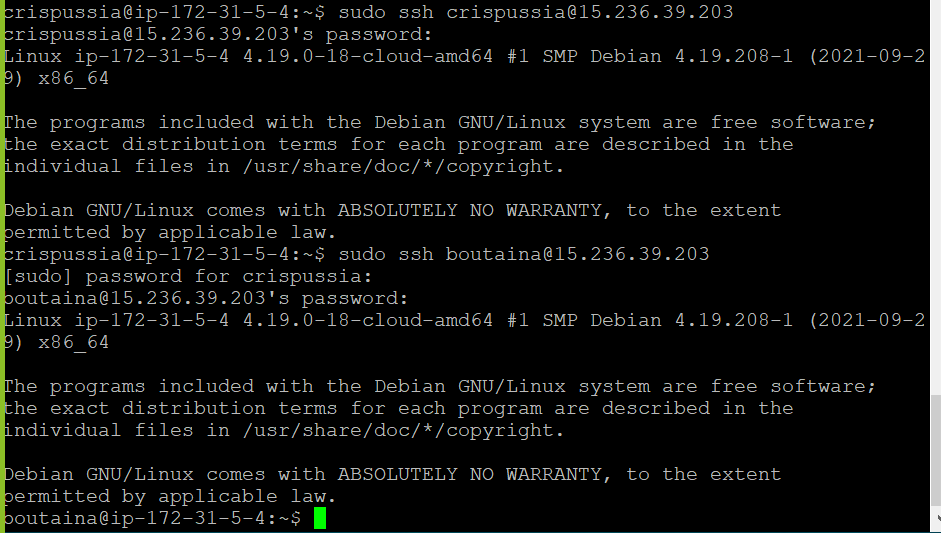
****

1. **Redémarrer notre service ssh**

****

1. **Tester de se connecter à mon utilisateur ou un utilisteur du groupe**

Pour tester cela on tape la commande : sudo ssh nom\_utilisteur@clé\_public ou ouvrir putty et renseigner la clé public pour se connecter



## Configuration de Fail2Ban afin de limiter le nombre d’accès

**Source** [**https://blog.swmansion.com/limiting-failed-ssh-login-attempts-with-fail2ban-7da15a2313b**](https://blog.swmansion.com/limiting-failed-ssh-login-attempts-with-fail2ban-7da15a2313b)

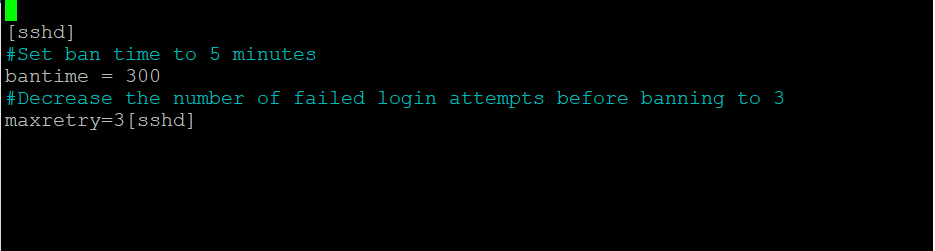
**Etape 1 : Installer Fail2Ban**

Pour l’installer on tape la commande :



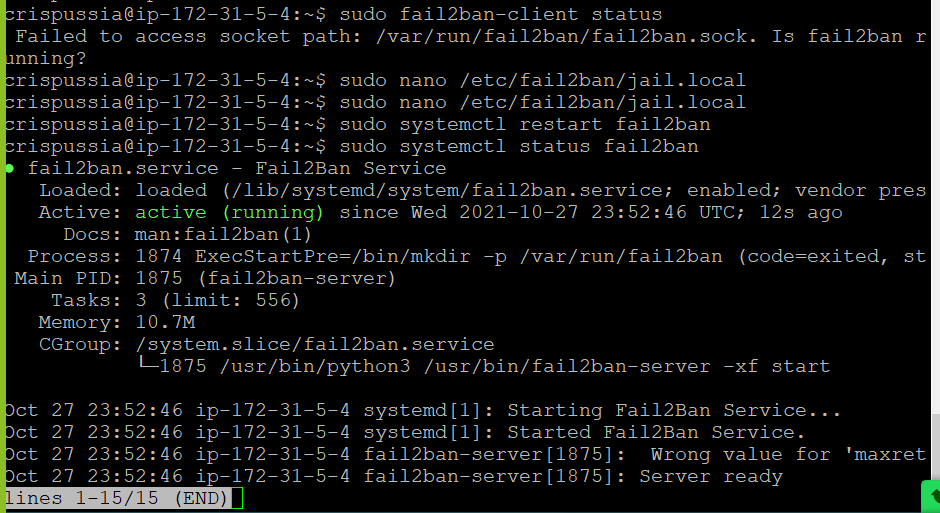
**Etape 2 : Configuration fail2ban**

Avec la configuration standard, fail2ban protégera le serveur SSH et bloquera la partie malveillante pendant 10 minutes après 5 tentatives de connexion infructueuses dans un délai de 10 minutes. Le fichier de configuration par défaut se trouve dans **sudo nano /etc/fail2ban/jail.conf**. On ne doit apporter aucune modification à ce fichier car il pourrait être écrasé lors de la mise à niveau de fail2ban .Pour cela on crée le fichier de configuration **sudo nano */etc/fail2ban/jail.local*** avec les modifications souhaitées.

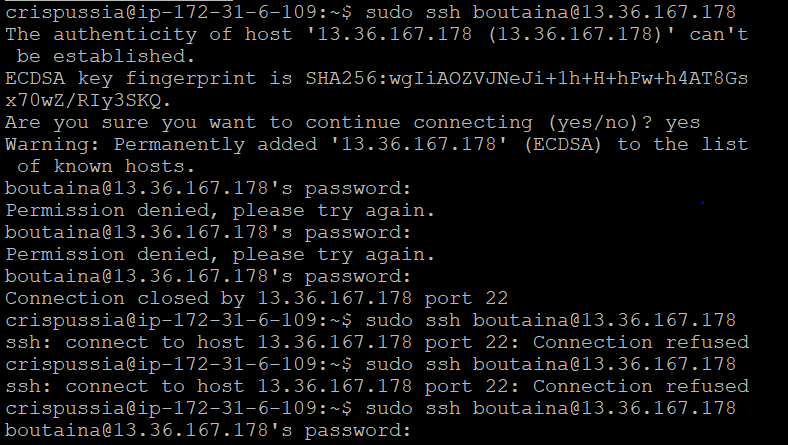


On modifie la durée d'interdiction par défaut ( bantime ) et le nombre de tentatives infructueuses ( maxretry ).

**Etape 2 : Redémarrer et Vérifier si le service est opérationnel**

****

**Etape 3 : Tester la configuration**

****

## Installation et Configuration du serveur DNS

**Source:**

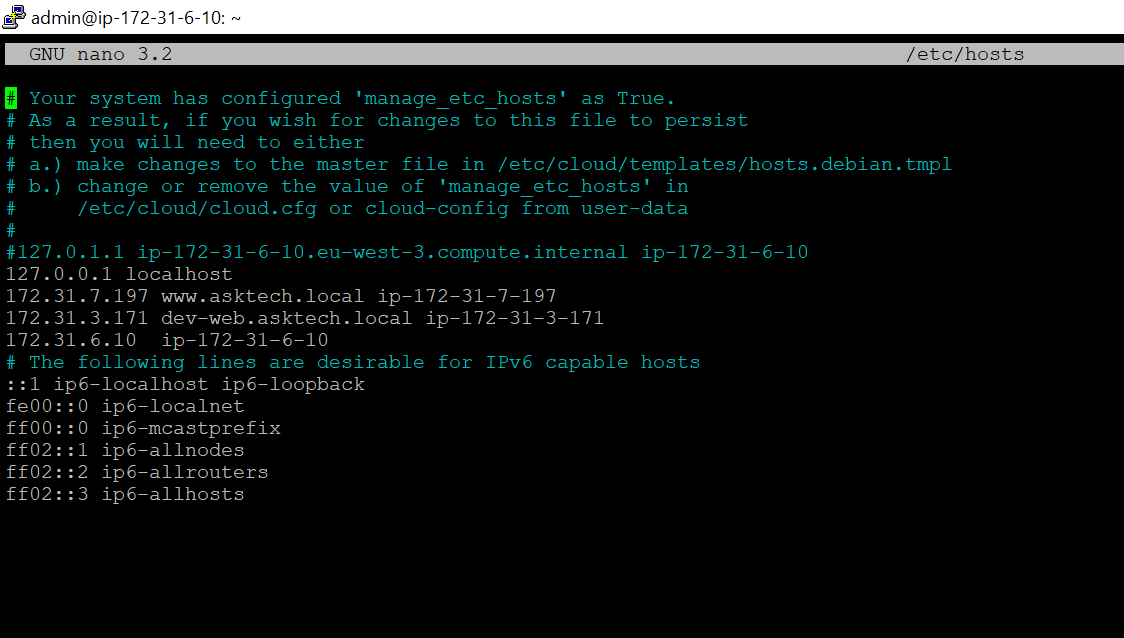
[**https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-debian-9**](https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-debian-9)

**https://www.tecmint.com/set-permanent-dns-nameservers-in-ubuntu-debian/**

Avant toute configuration, on s'assure que les machines ont une adresse IP statique.

| **Hôte** | **Rôle** | **FQDN privé** | **Adresse IP privée** |
| --- | --- | --- | --- |
| **ip-172-31-6-10** | **Serveur DNS primaire** | **ip-172-31-6-10.asktech.local** | **172.31.6.10** |
| **ip-172-31-7-197** | **Hôte générique 1** | **www.asktech.local** | **172.31.7.197** |
| **ip-172-31-3-171** | **Hôte générique 2** | **dev-web.asktech.local** | **172.31.3.171** |

**Modifier le fichier /etc/hosts du server dns(il faut le faire à chaque fois qu’on se connecte car il ne sauvegarde pas)**

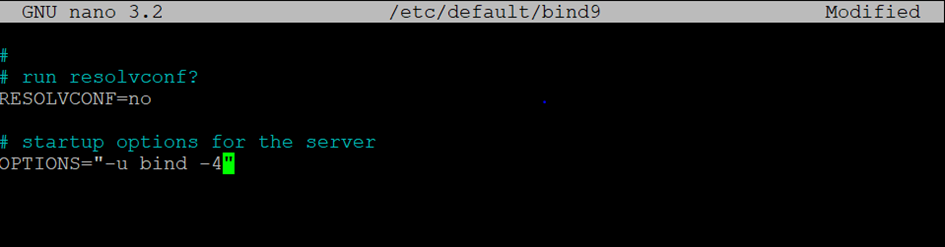
****

**Etape \_1: Installez maintenant BIND**

Pour l’installation on tape la commande:sudo apt install bind9 bind9utils bind9-doc

**Etape 2: Configuration de la liaison au mode IPv4**

Avant de continuer, définissons BIND en mode IPv4 puisque notre réseau privé utilise exclusivement IPv4. On tape la commande **sudo nano /etc/default/bind9.**



**Etape 3: Redémarrez BIND**

Tapez la commande: **sudo systemctl restart bind9**

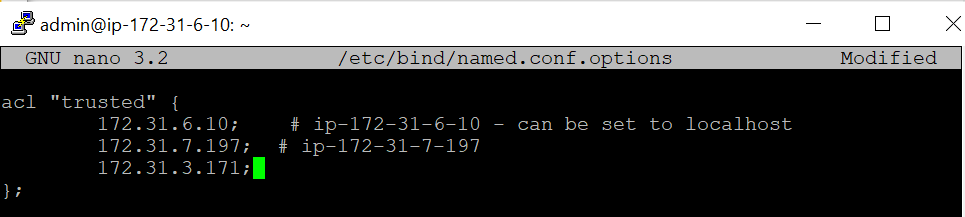


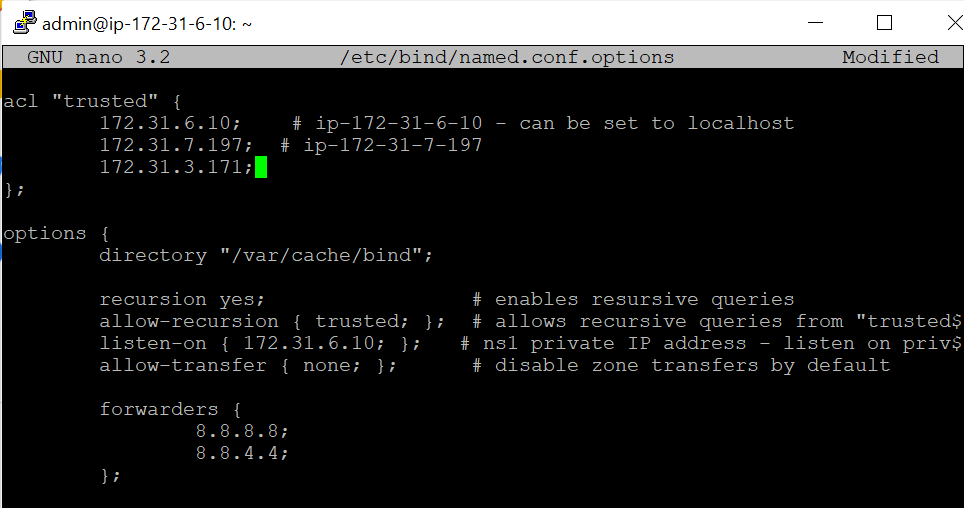
**Etape 4: Configuration du fichier Options**

Editez le fichier **named.conf.optionsfichier**

****

Au-dessus du bloc options existant ,on crée un *nouveau* bloc ACL (liste de contrôle d'accès) appelé « de confiance ». C'est ici que nous définirons une liste de clients à partir desquels nous autoriserons les requêtes DNS récursifs.





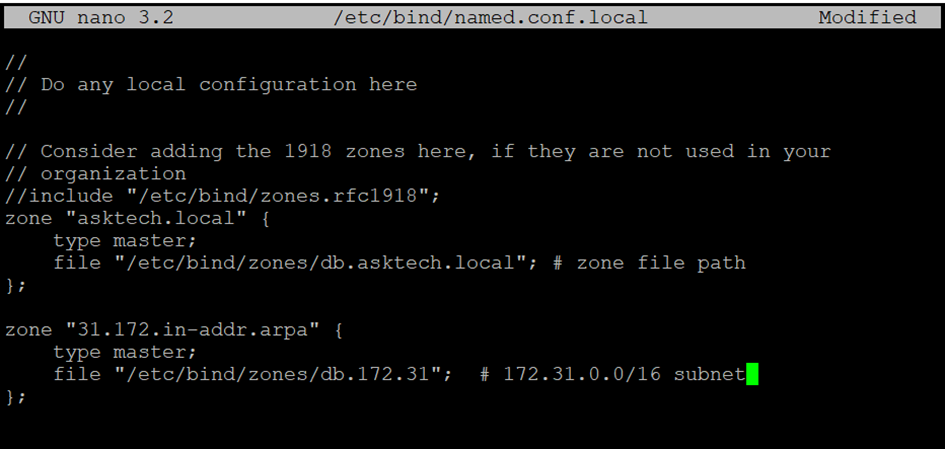
On enregistre et ferme le named.conf.options fichier.

**Etape 5: Configuration du fichier Local**

Editez le named.conf.local fichier



Nous allons spécifier nos zones avant et arrière. Étant donné que nos domaines se trouveront tous dans le sous-domaine « asktech.local », nous l'utiliserons comme zone de transfert. Étant donné que les adresses IP privées de nos serveurs se trouvent chacune dans l' 172.31.0.0/16 espace IP, nous allons configurer une zone inversée afin de pouvoir définir des recherches inversées dans cette plage.

On ajoute la zone de transfert avec les lignes suivantes et la zone inversée:

Nous devons créer les fichiers de zone directe et inverse correspondants.

**Etape 6: Création du fichier de zone de transfert**

Le fichier de zone de transfert est l'endroit où nous définissons les enregistrements DNS pour les recherches DNS de transfert.

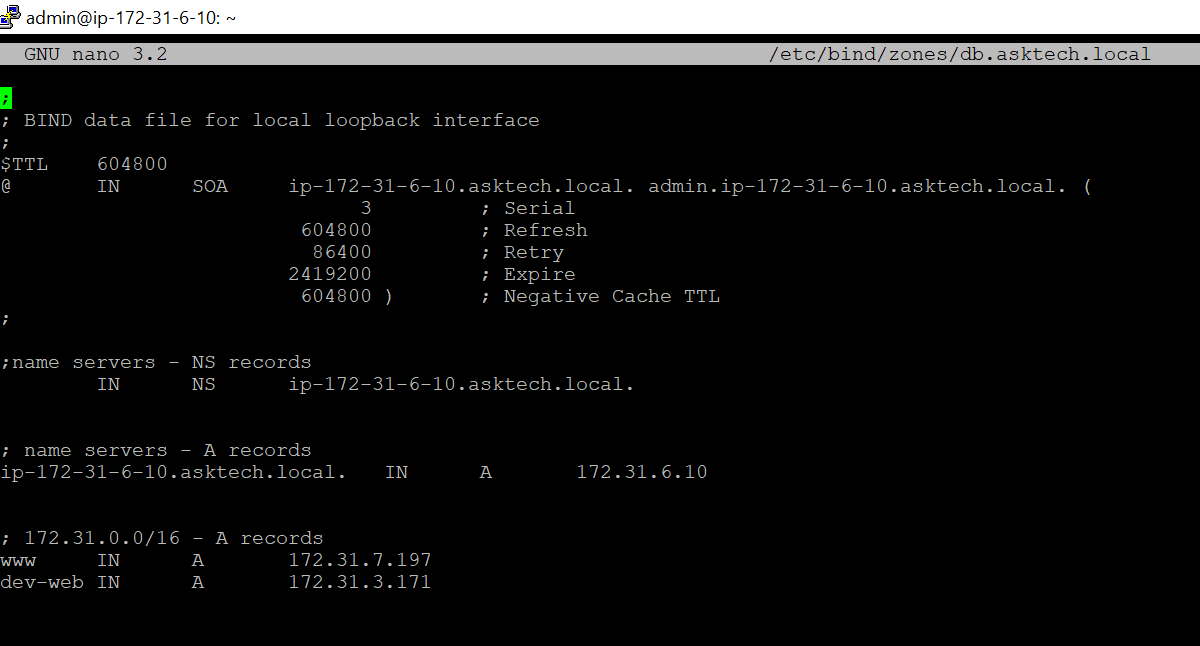
Créons le répertoire où résident nos fichiers de zone. Selon notre configuration **named.conf.local** , cet emplacement devrait être /etc/bind/zones:

Nous allons baser notre fichier de zone de transfert sur l'exemple de db.local fichier de zone.



Editons notre fichier de zone de transfert :

Nous tapons la commande: sudo nano /etc/bind/zones/db.asktech.local



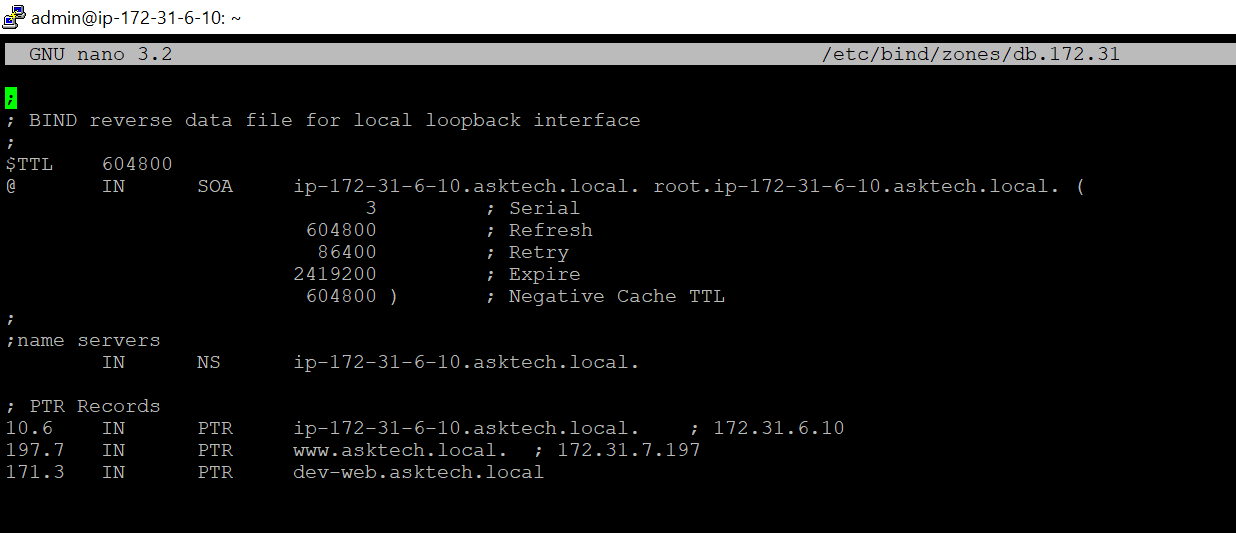
**Etape 7: Création du fichier de zone inversée**

Les fichiers de zone inversée sont l'endroit où nous définissons les enregistrements DNS PTR pour les recherches DNS inversées.

Nous allons baser nos fichiers de zone inversée sur l'exemple de db.127 fichier de zone.



Editez le fichier de **zone inversée** qui correspond à la zone inversée définies dans named.conf.local

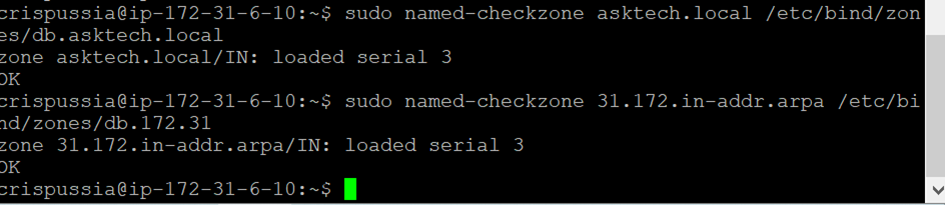


**Etape 8: Vérification de la syntaxe de configuration**

On tape les commandes suivantes:

**sudo named-checkzone asktech.local /etc/bind/zones/db.asktech.local**

**sudo named-checkzone 31.172.in-addr.arpa /etc/bind/zones/db.172.31**



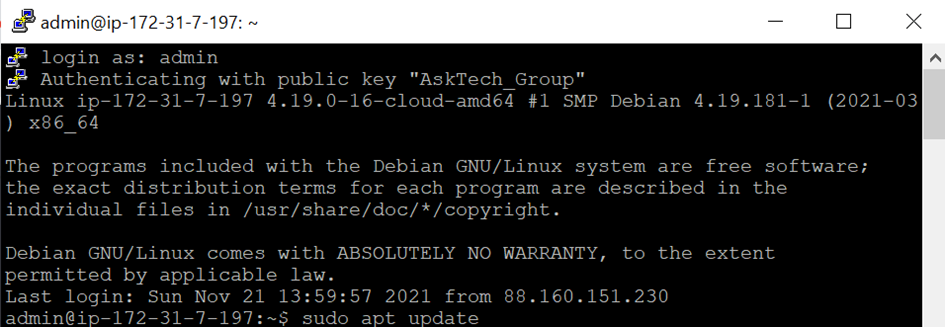
On remarque que les configurations sont correctes.

**Etape 9: Redémarrage de Bind**

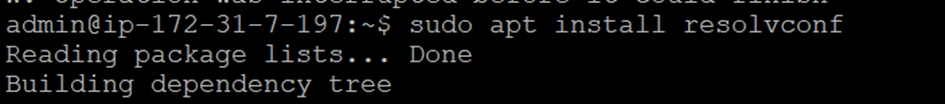
**sudo systemctl restart bind9**

**Etape 10: Connexion aux machines Clients**

On se connecte à la machine client qui servira de Web prod et web dev.

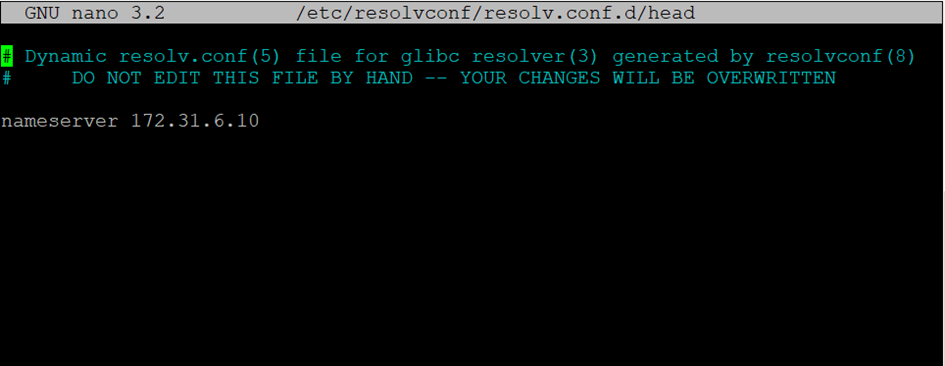
****

**Etape 11: Installation du fichier resolvconf sur les machines clients(Répétez au niveau de la deuxième machine)**

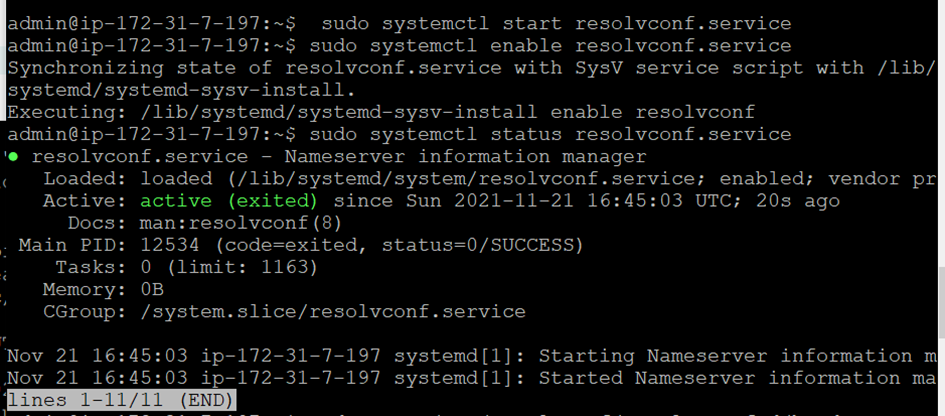
****

**Etape 12: Editer le fichier resolvconf sur la machine client(Répétez au niveau de la deuxième machine )**

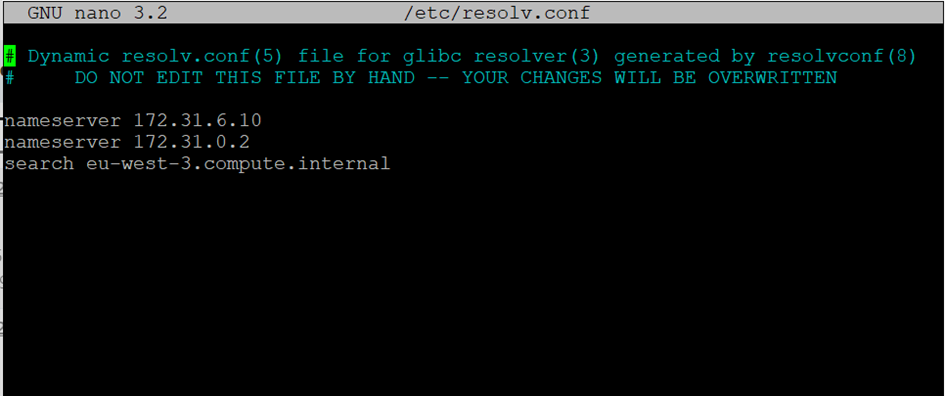
****



Redémarrez le fichier resolvconf

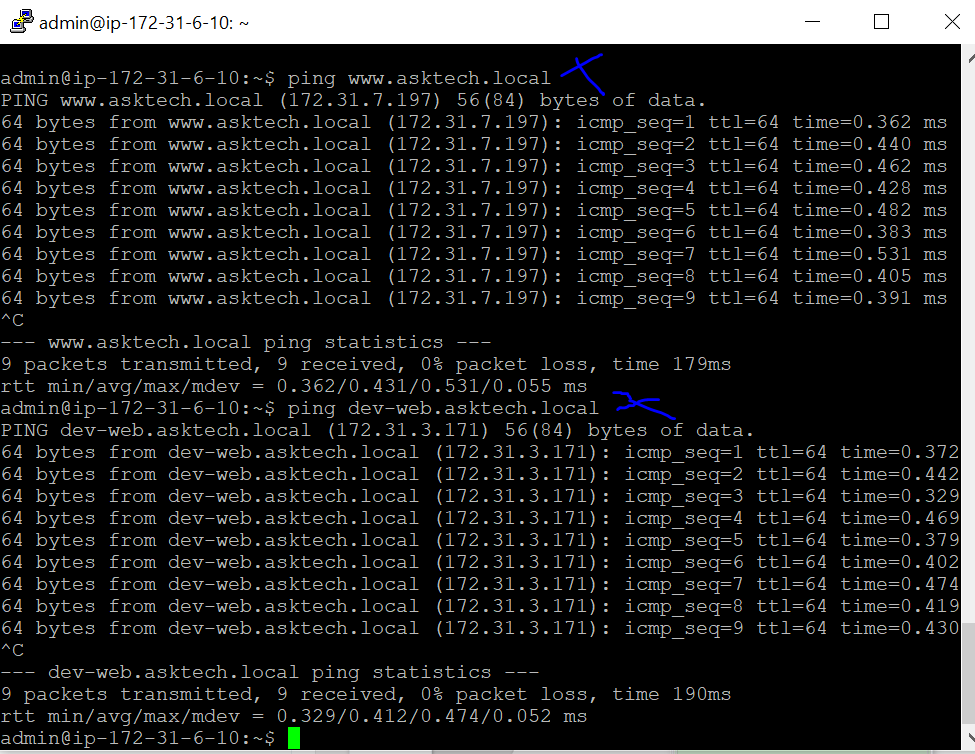


**Etape 13: Afficher le fichier de configuration de Bind resolv.conf sur la machine client(Répétez au niveau de la deuxième machine)**

****

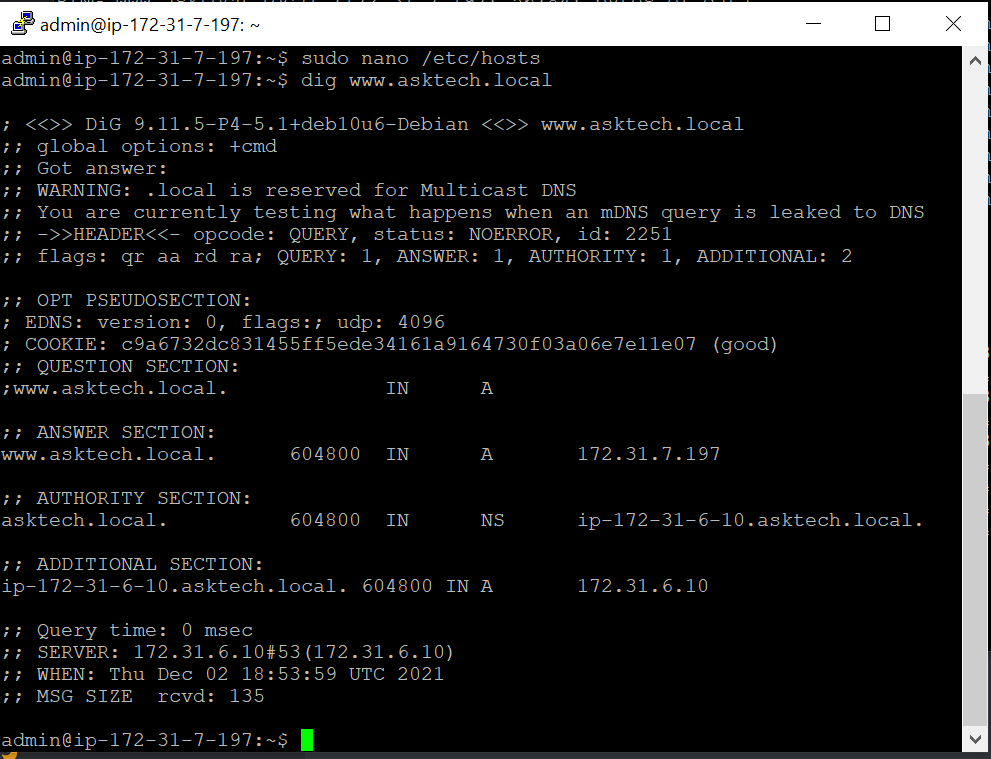
On remarque que le nom de notre serveur a été ajouté.

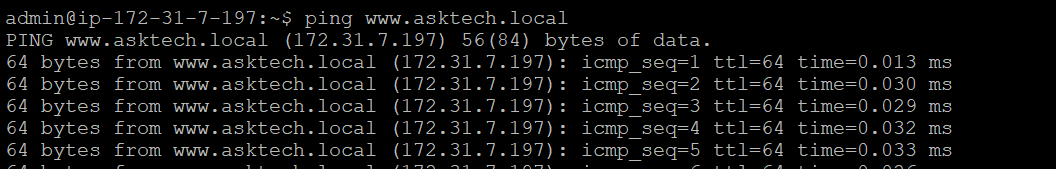
**Etape 14: Tester que la connexion fonctionne:**

****

**Etape 14: Tester que la recherche directe fonctionne pour chaque machine :**

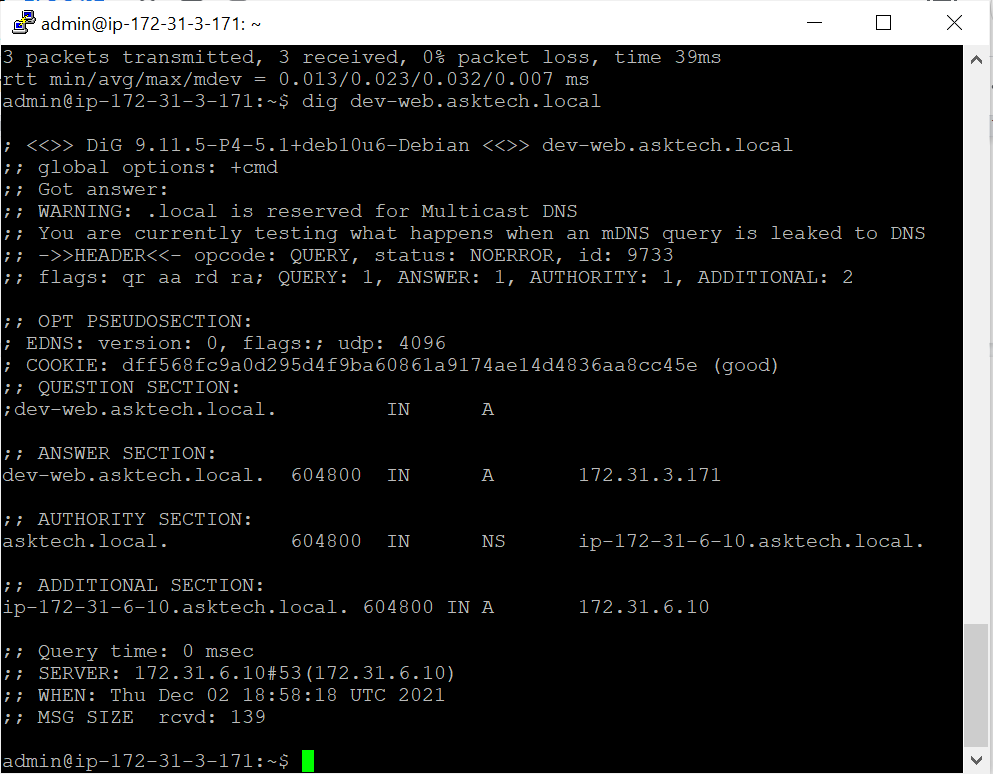
**Machine web prod**

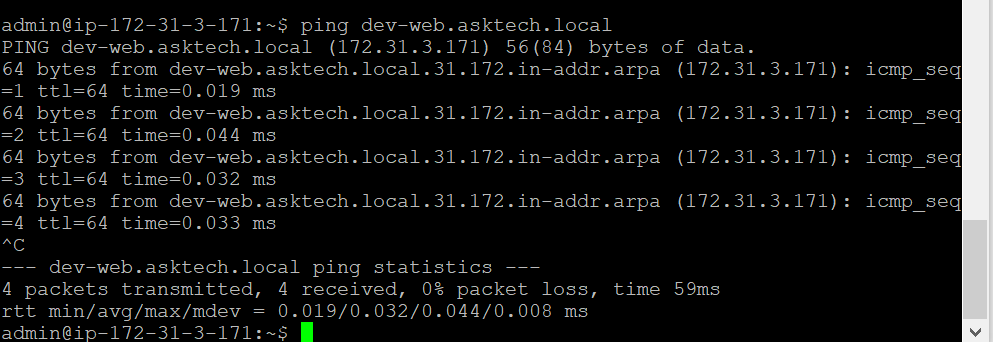


****

La recherche directe **a bel et bien fonctionnée.**

**Machine web dev**

****

****

La recherche directe **a bel et bien fonctionnée.**

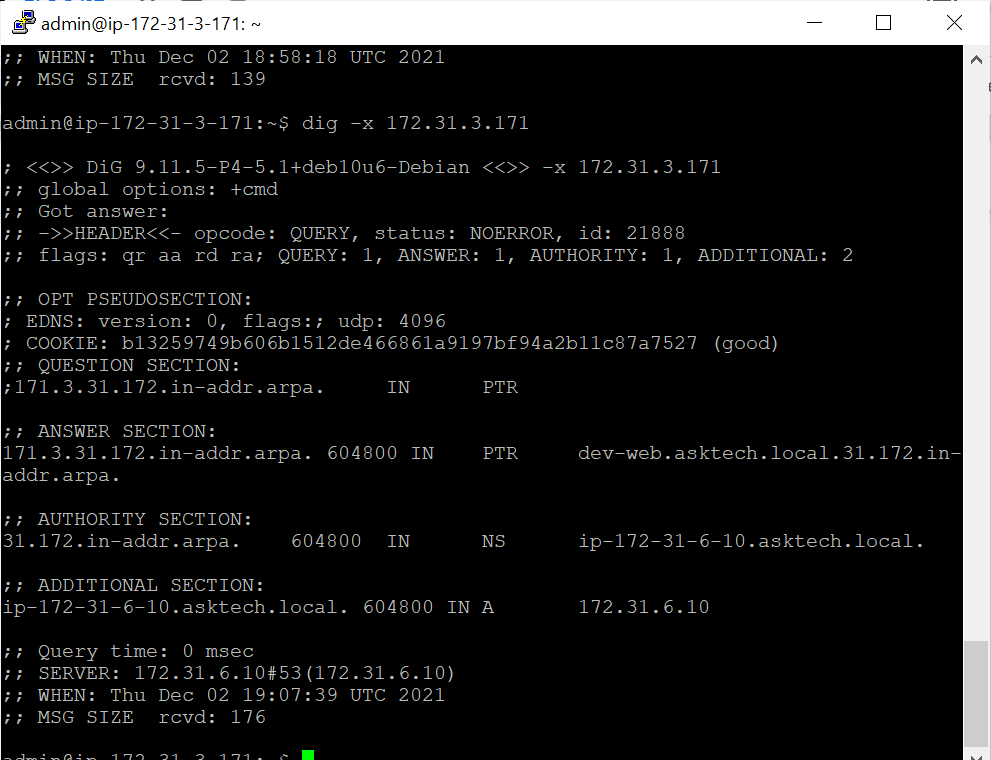
**Etape 15: Tester que la recherche inverse fonctionne:**

**Machine web-Prod**

****

La recherche inverse **a bel et bien fonctionné.**

**Machine Web-Dev**

****

La recherche inverse **a bel et bien fonctionné.**