1. **– Configuration du serveur (DEB01)**

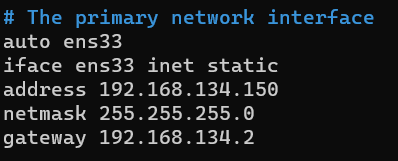
* Renommer le serveur DEBIAN en DEB01 :

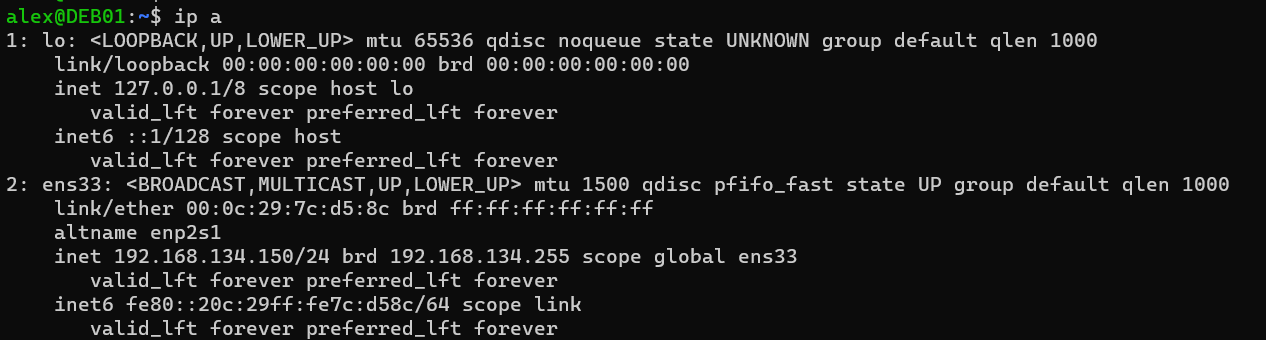
Nano /etc/hostame et indiquer le nom d’hôte du système

* Configuration des cartes réseaux via le fichier (DEB01)

Nano /etc/network/interfaces ET une fois modifié alors il faut redémarrer le service

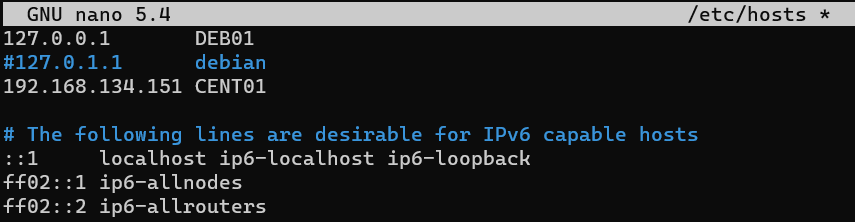
Pour redémarrer le service : *systemctl restart networking.service*





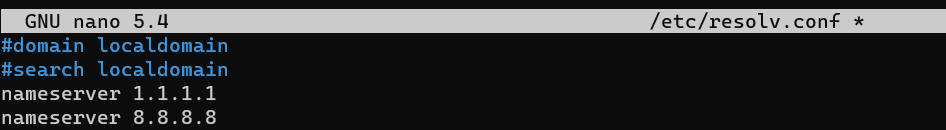
* Ajout de la correspondance des noms d’hôtes avec l’adresse IP dans le fichier HOSTS :

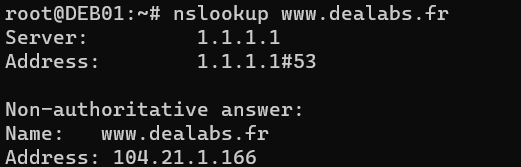
Nano /etc/hosts



* Ajouter les adresse DNS

Nano /etc/resolv.conf puis tester avec la commande nslookup pour la résolution DNS.





1. **– Configuration du serveur (CENT01)**

* **S’il vous manque le paquet NANO ou VIM (éditeur de texte), il faut installer les paquets et il faut une connexion internet.**

**Yum update**

**Ymu install nom\_du\_paquet**

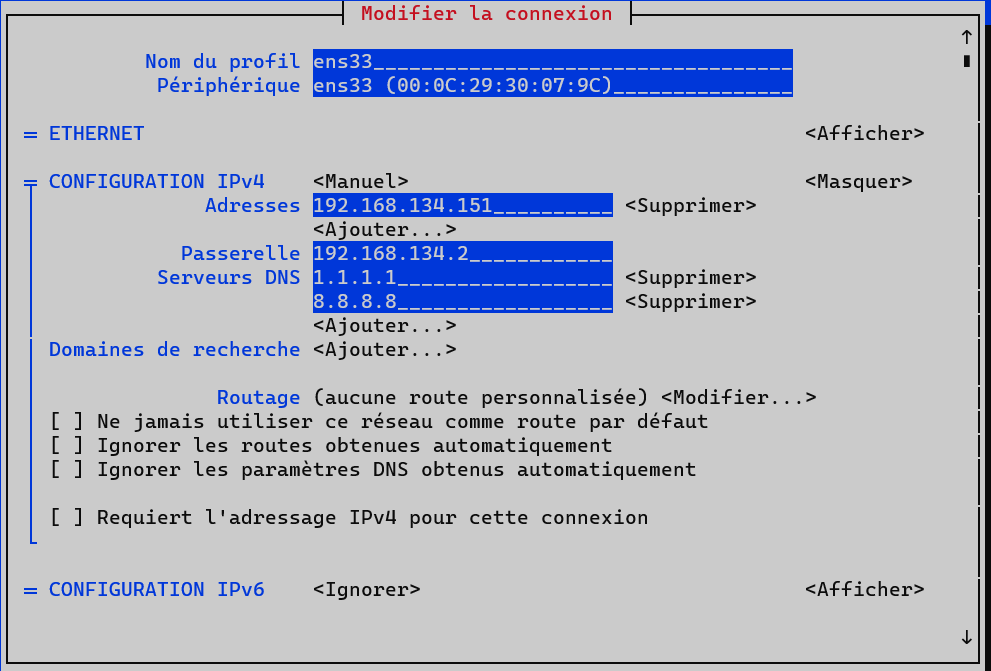
**Exemple : yum install nano**

* Renommer le serveur CENTOS en CENT01 : voir les étapes précédentes ou via NMTUI
* Pour le fichier HOSTS (correspondance des hosts avec IP) même opération que sur DEBIAN.
* Configuration de la carte réseau et des DNS / HOSTNAME via le service NETWORK-MANAGER (CENT01)

Utiliser la commande : nmtui. Cette commande va ouvrir une console.

Une fois les modifications validées n’oubliez pas de redémarrer votre serveur.

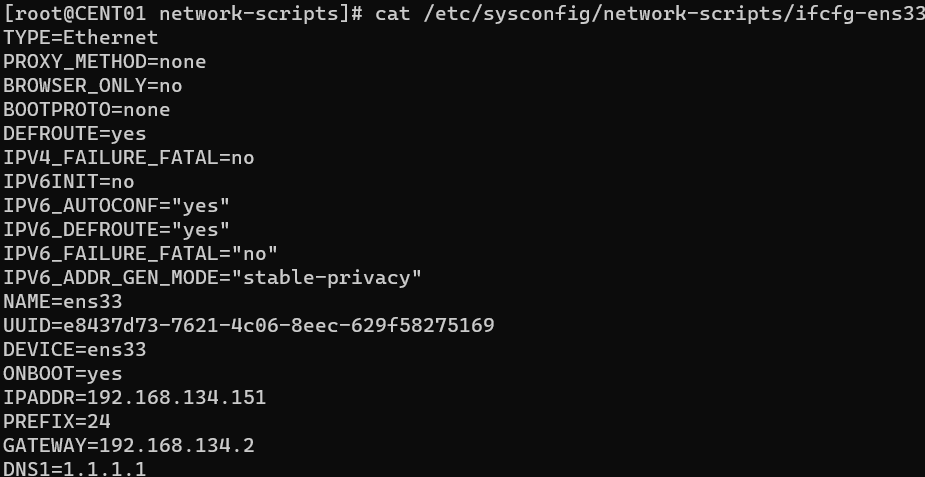
Vous pouvez à partir de la commande nmtui obtenir une console qui va vous permettre de modifier la carte réseau, les adresses DNS et également le hostname.





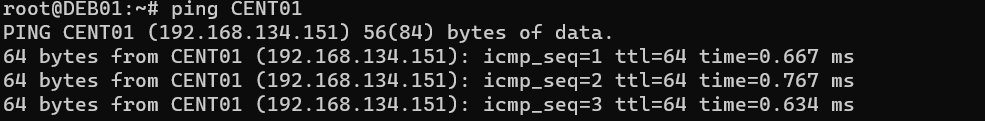
**POUR LE RESEAU DU CENTOS :**

* Le paquet NETWORK MANAGER (nmtui) va modifier le fichier de configuration qui se trouve dans /etc/sysconfig/network-scripts/ifcfg-ens33
* Il est possible de modifier ce fichier à la main (via nano) mais attention il faut désactiver le paquet NETWORK-MANAGER. (Déconseillé car RED-HAT / CENTOS / FEDORA etc… utilise par défaut ce paquet)



* Test des réseaux

Si le fichier HOSTS a bien été rempli, vous devriez être capable de ping les deux machines via leurs noms d’hôtes et non seulement leurs IP.

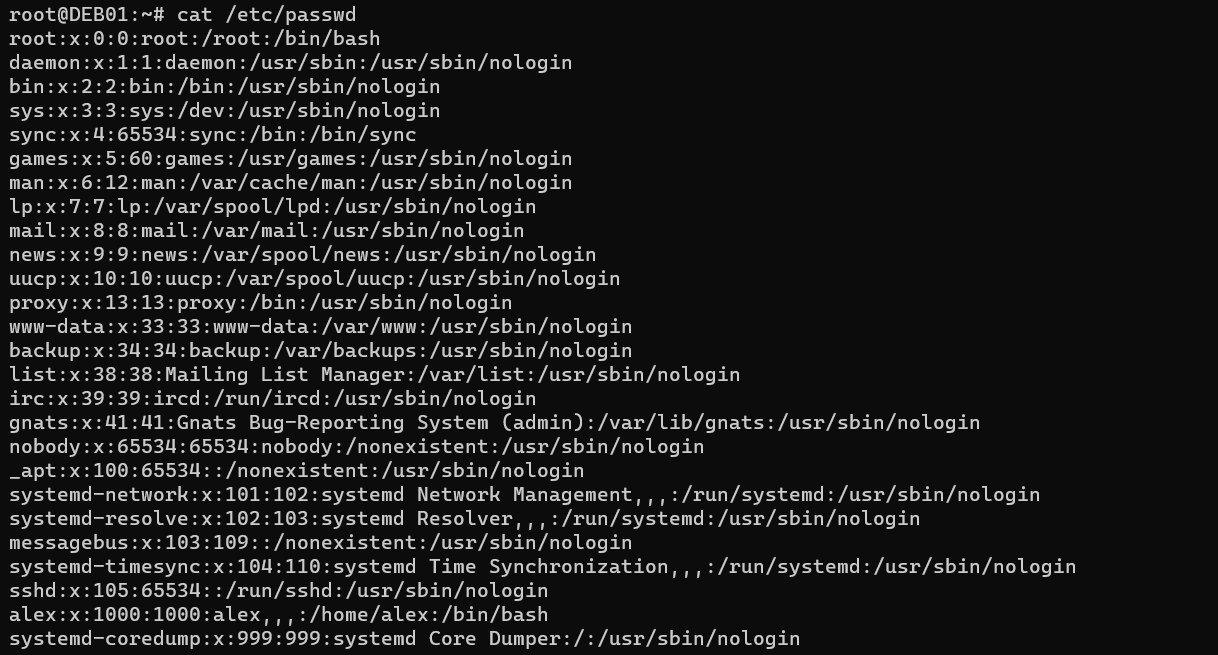


**2 – Utilisateurs et groupes**

* Machine CENT01
* Créer l’utilisateur techcent01 :

Pour trouver la liste des utilisateurs disponibles sur le système LINUX le fichier est dans /etc/passwd.

Aperçu du fichier :



Il est possible de créer des utilisateurs directement en modifiant ce fichier source ou utiliser des commandes comme useradd ou adduser avec des options pour ajouter un utilisateur dans le système.

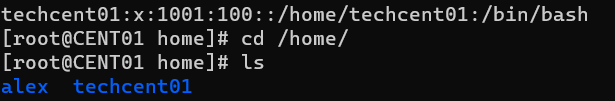
Exemple pour créer l’utilisateur techcent01 :



Les options utilisées :

* -b = indiquer le répertoire de base donc /home
* -m = créer son répertoire donc /home/techcent01
* -N = ne pas créer un groupe qui porte le même nom que l’utilisateur (comportement pas défaut lors de la création d’un user)
* -s = indique le Shell de connexion pour l’utilisateur lorsqu’il va se connecter.

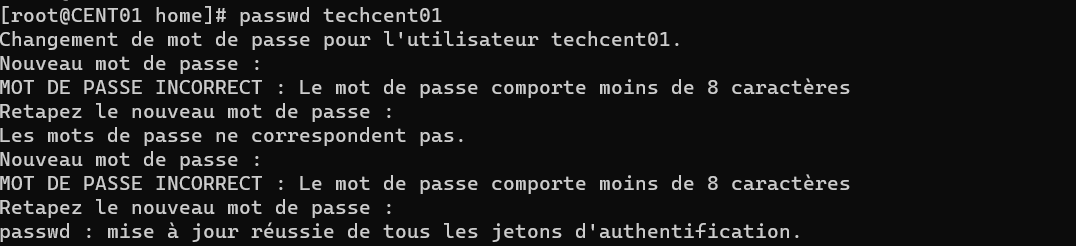
Une fois l’utilisateur créé, consulter le fichier /etc/passwd pour confirmer sa création :



Ici, on peut observer que l’utilisateur techcent01 est présent dans le fichier avec comme UID : 1001 et un groupe primaire GID : 100, en plus on nous indique le répertoire personnel et le shell de connexion.

On peut le rajouter un mot de passe et tester une ouverture de session avec l’utilisateur.

Pour l’ajout du mot de passe (ce qui va permettre d’activer le compte) les mots de passe sont stockés dans /etc/shadow mais crypté donc pas visible :

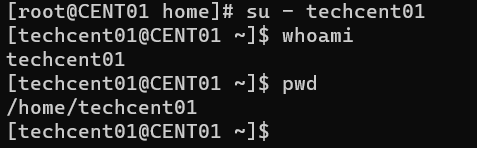
Commande qui permet de mettre un mdp : #passwd techcent01

Aperçu du fichier shadow



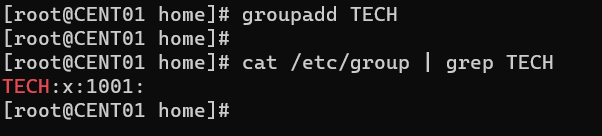
On peut observer que le mot de passe est crypté par sécurité.

Test de la connexion :



* Créer le groupe TECH :

Comme pour les utilisateurs il y’a un fichier pour les groupes qui se trouve dans /etc/group et il est possible de créer un groupe via la commande groupadd ou en éditant directement le fichier source.



Ici, on crée le groupe TECH via la commande et ensuite on observe le résultat dans le fichier source /etc/group en filtrant la recherche. Pour information, ici le groupe TECH à comme GID (group identifiant) 1001.

* Ajout de l’utilisateur TECHCENT01 dans le groupe TECH en tant que secondaire

Concernant linux, il y a la notion de groupe primaire (GID) et groupe secondaire.

Un utilisateur peut avoir un seul groupe primaire et être membre de plusieurs groupes secondaires. Ne pas oublier que lors de la création de l’utilisateur avec la commande useradd par défaut le système va créer un groupe primaire qui porte le même nom que l’utilisateur mais cette option peut être désactivé (manipulation déjà effectué précédemment). Si on modifie le groupe primaire de l’utilisateur cela va impacter les droits et permissions de tous les fichiers et dossiers concernés par l’utilisateur.

Donc ici, on va laisser comme groupe primaire pour l’utilisateur techcent01 le groupe USERS = 100 (correspond au groupe utilisateurs du système linux) et on va lui rajouter un groupes secondaire = TECH.

Exemple : l’utilisateur à comme UID 1001 et GID 100



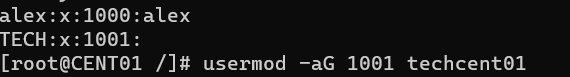
Pour ajouter un groupe secondaire à l’utilisateur sans modifier son groupe primaire GID on peut effectuer cette manipulation via le fichier /etc/group ou avec la commande usermod en indiquant des options.

Méthode 1 : Modifier le fichier /etc/group avec nano et rajouter l’utilisateur dans la ligne du groupe TECH





Méthode 2 : via la commande usermod



Le groupe TECH est identifié avec le numéro 1001 et dans la commande on indique le groupe TECH soit par le nom ou son identifiant.

* **Ajouter le paquet SUDO si besoin et ajouter le techcent01 dans le groupe SUDO comme secondaire.**

Pour information sur CENTOS le paquet sudo s’installe avec la commande yum install sudo mais le groupe se nomme WHEEL et non SUDO.

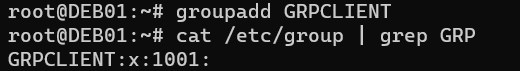
Par contre, les commandes pour utiliser sudo ne change pas exemple : sudo yum update.



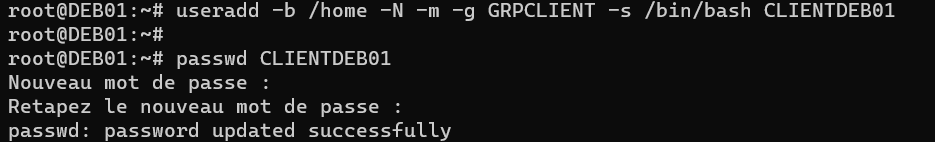
1. **– Utilisateurs et groupes**

**Machine DEB01**

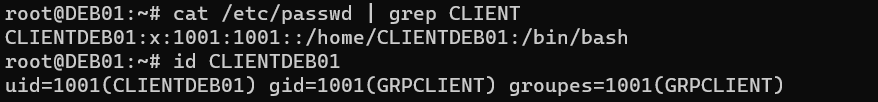
Créer le groupe :



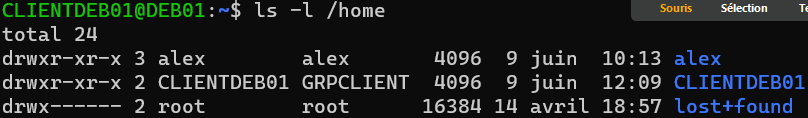
Créer un utilisateur CLIENTDEB01. Le compte doit posséder son propre répertoire personnel et le compte possède comme groupe primaire GRPCLIENT lors de sa création puis ajouter le mot de passe pour l’activer :



Vérification :



On peut observer le répertoire personnel de l’utilisateur à comme groupe GID (primaire) GRPCLIENT.

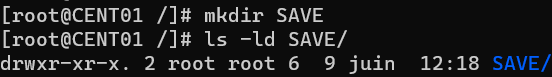


1. **– Arborescence, droit accès et propriétaire.**

**Machine CENT01 :**

Créer un répertoire SAVE dans la racine :

La commande MKDIR permet de créer un répertoire et la commande LS avec l’options -l et -d combiné permet d’afficher sur la console le type de fichier, le propriétaire (UID), le groupe propriétaire (GID) et seulement pour le dossier SAVE (c’est l’option -d qui me permet d’afficher les informations seulement pour le dossier concerné)



Pour comprendre les droits d’un fichier / dossier :

* Le « d » au début indique le type de fichier (ici c’est directory)
* rwx, r-w, r-x ce sont les droits d’accès concernant le dossier SAVE, ils sont découpés en bloc de 3, le premier bloc correspond au droit d’accès du propriétaire donc ici ROOT, le deuxième correspond au droit d’accès du groupe propriétaire donc ici ROOT, et le troisième bloc correspond aux AUTRES qui n’est pas indiqué ici.

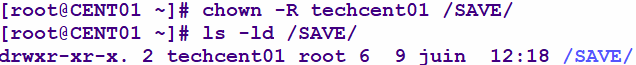
R = read

W = write

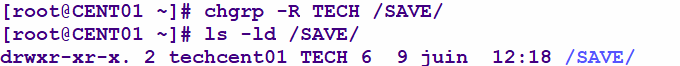
X = exécuter.

* **Changer le propriétaire du répertoire et le groupe propriétaire :**

La commande chown (change owner) permet de changer le propriétaire d’un répertoire ou fichier.



La commande chgrp (change groupe) permet de changer le groupe propriétaire d’un répertoire ou d’un fichier.



Il est possible avec la commande CHOWN de faire la modification du propriétaire et du groupe en même temps (2en1).



* **Les droits d’accès**

Pour modifier les droits d’accès sur un répertoire ou fichier : utiliser la commande chmod.

**1er méthode (binaire) :**

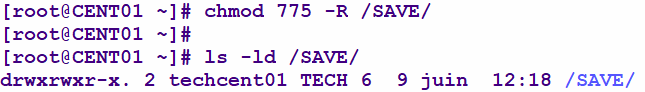
R = 4 | W = 2 | X = 1

*Exemple si je veux un droit en écriture et exécution = 2 + 1 = 3*

*Exemple 2 : Je veux donner comme droit au propriétaire (UID) le droit RWX, le droit R pour le groupe propriétaire (GID) et pour les autres (OTHERS) rien.*

*Résultat : chmod 740 DOSSIER/FICHIER*

Pour le TP :



**2er méthode :**

*Exemple : je veux ajouter le droit W pour le groupe propriétaire de mon dossier RH*

*Chmod -R g+w RH*

*Exemple : je veux retirer le droit X pour les autres de mon dossier COMPTA*

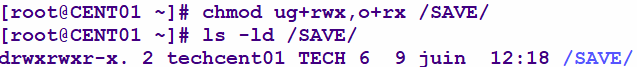
*Chmod -R o-x COMPTA*

*Exemple : je veux affecter (attention l’affectation écrase les droits existant) pour le UID le droit RW*

*Chmod u=rw DOSSIER*

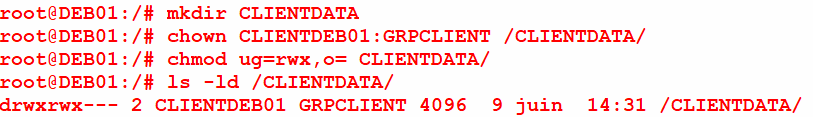
*Si le DOSSIER avait de base comme droit X pour le UID alors il va écraser tout et seulement affecter le droit RW donc attention de ne pas confondre avec l’ajout supplémentaire des droits.*

**Pour le TP :**



**Machine DEB01**

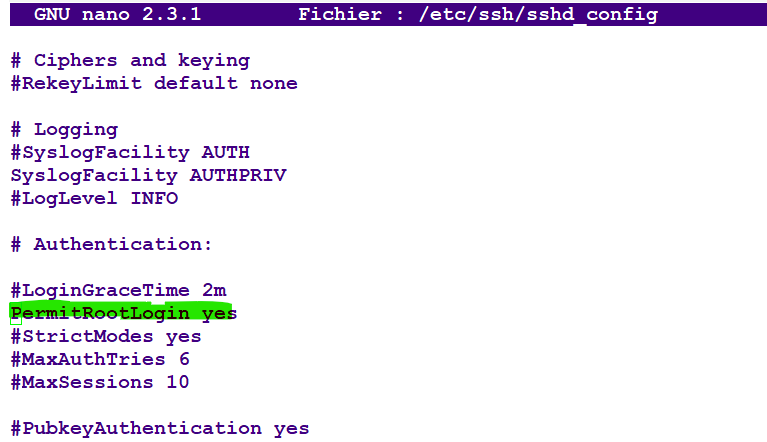
* Créer un répertoire dans la racine qui se nomme CLIENTDATA
* Changer le propriétaire et le groupe propriétaire par CLIENTDEB01 : GRPCLIENT.
* Pour les droits accès RWX pour le UID et GID et aucun pour les autres



**SSH**

Pour activer la connexion en root via le SSH il faut décommenter et ajouter la valeur yes depuis fichier /etc/ssh/sshd\_config.

Une fois la modification validée, pensez à redémarrer le service SSH avec la commande systemctl restart sshd.



Depuis le client DEB01 avec l’utilisateur CLIENTDEB01, nous allons générer une paire de clé public et privée qui sera stockée automatiquement dans son dossier personnel de CLIENTDEB01



Copier la clé publique de l’utilisateur CLIENTDEB01 depuis la machine DEB01 vers l’utilisateur techcent01 de la machine CENT01 (serveur) si l’opération est correcte on devrait pouvoir observer la clé publique du client DEB01 dans le dossier personnel de l’utilisateur techcent01 du serveur CENT01 dans le dossier .SSH et fichier authorized\_keys.



Pour réaliser un test alors connectez vous depuis le client DEB01 vers le serveur CENT01 avec l’utilisateur techcent01 puis on ne vous demande plus de mot de passe l’authentification s’effectue par les clés.



**Pour tester :**

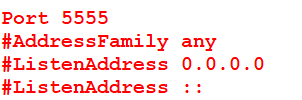
On va créer un dossier DOSSIERTEST dans le serveur CENT01 sur le dossier personnel de techcent01 mais depuis le client DEB01



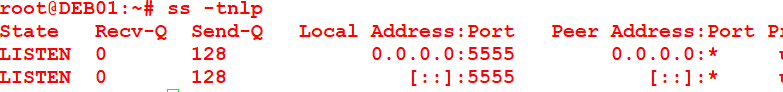
Avec le SSH, il est possible d’exécuter des commandes à distance et sans le mot de passe comme nous avons généré ces paires de clé et qu’on s’authentifie avec celle-ci.

Pour changer le port par défaut du service SSH alors il faut modifier le fichier /etc/ssh/sshd\_config.

Décommenter la ligne et changer le port



Ensuite redémarrer le service et vérifier les ports sur écoute de votre serveur.



Ici on peut observer que le serveur écoute sur toutes ces interfaces sur le port 5555 pour le service SSH.

**ATTENTION POUR LE SERVEUR CENTOS LA MANIPULATION NECESSSITE LE BESOIN DE MODIFIER LE SELINUX AVEC LA COMMADNE SEMANAGE.**

<https://computingforgeeks.com/change-ssh-port-centos-rhel-fedora-with-selinux/>