OFPPT مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Complexe de Formation dans les Métiers des Nouvelles Technologies de l'Information, de l'Offshoring et de l'Electronique -Oujda

Module : Administration d'un Réseau sous Linux

Configuration de base

Formatrice : Ilham ZITI

Sommaire

1. Désactiver SELINUX

SELinux est système disponible sous les distributions récentes de Linux permettant de définir une politique de sécurité d'accès très fine par rapport au système d'exploitation.

Pour désactiver il existe deux techniques **Désactivation permanente et Désactivation temporaire**

1.1 Désactivation permanente :

Pour que ce changement soit permanentent il faut aller éditer le fichier /etc/selinux/config :

```
SELINUX=enforcing
```

enforcing signifie que la politique de sécurité SELinux est appliquer. Pour ne plus l'appliqué il faut remplacer enforcing par **disabled:**

```
SELINUX=disabled
```

Puis de rebooter le système.

```
reboot
```

1.2 Désactivation temporaire :

Pour désactiver SELinux temporairement, dans le cadre d'un test par exemple taper en ligne de commande (root):

```
setenforce 0
```

On peut procéder aussi comme ci-dessous :

```
# echo "0" > /selinux/enforce
```

SELinux sera de nouveau activé au prochain démarrage

2. Désactiver le Pre Feu

Firewalld est la solution de pare-feu par défaut fournie dans le système d'exploitation CentOS. Contrairement à d'autres systèmes d'exploitation, qui utilisent généralement iptables, le service iptables n'est pas installé par défaut dans CentOS 7. Ils utilisent tous deux le cadre netfilter pour accéder et analyser les paquets.
Pour désactiver le service pare-feu, commencer par arrêter firewalld, et s'assurer qu'il est bien coupé :

```
# systemctl stop firewalld.service
```

```
[root@ntic ~]# systemctl stop firewalld
[root@ntic ~]#
```

```
# systemctl status firewalld.service
```

```
root@ntic ~]# systemctl status firewalld
 firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: e
abled)
   Active: inactive (dead) since dim. 2018-12-02 22:47:00 CET; 49s ago
     Docs: man:firewalld(1)
  Process: 770 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exi
ed, status=0/SUCCESS)
 Main PID: 770 (code=exited, status=0/SUCCESS)
```

Ensuite, désactiver son démarrage automatique :

```
#systemctl disable firewalld.service
```

```
[root@ntic ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
[root@ntic ~]#
```

3. Renommer la machine

Pour changer le nom de la machine éditer le fichier /etc/hostname :

```
#vi /etc/hostname
```

Puis modifier la valeur contenue initialement dans ce fichier :

```
nom_machine_
~
~
```

Redémarrer la machine pour appliquer ces changements avec la commande suivante :

```
#reboot
```

On trouvera ensuite le nom de la machine dans le début de la ligne de commande :

```
nom_machine login: root
Password:
Last login: Sat Sep  6 12:49:33 on tty1
[root@nom_machine ~]# _
```

Une autre façon de changer le nom est d'utiliser une commande **hostnamectl** qui va automatiser la procédure :

```
#hostnamectl   set-hostname   nom_machine
```

Le changement va alors s'opérer directement à la prochaine session ouverte ou tout simplement en affichant le contenu du fichier **/etc/hostname**

4. Fixer Adresse IP

Pour identifier les cartes réseaux présentes sur la machine, exécuter la commande suivante:

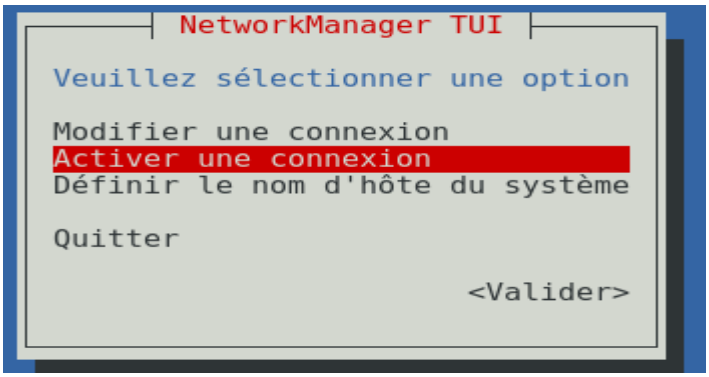
```
#nmcli d
```

```
[root@localhost ~]# nmcli d
DEVICE      TYPE      STATE        CONNECTION
virbr0      bridge    connecté     virbr0
ens33       ethernet  déconnecté   --
lo          loopback  non-géré     --
virbr0-nic  tun       non-géré     --
[root@localhost ~]#
```

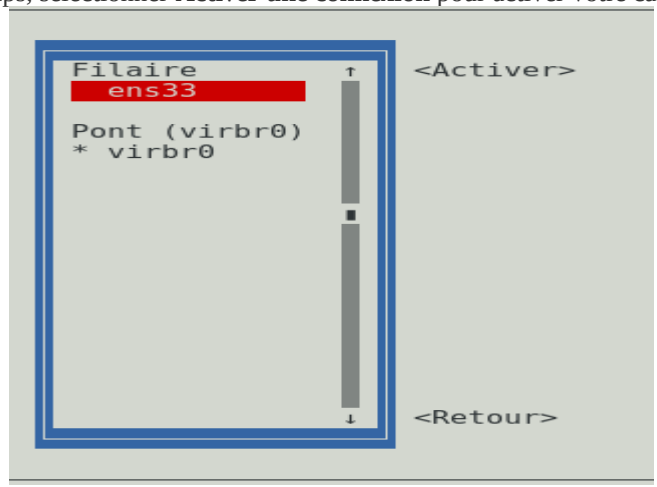
La commande affiche toutes les cartes réseaux disponibles ainsi que leurs statuts. On voit bien ici que la carte est déconnectée.

Pour une configuration avec un assistant, exécuter la commande suivante et suivre les indications à l'écran:

```
#nmtui
```



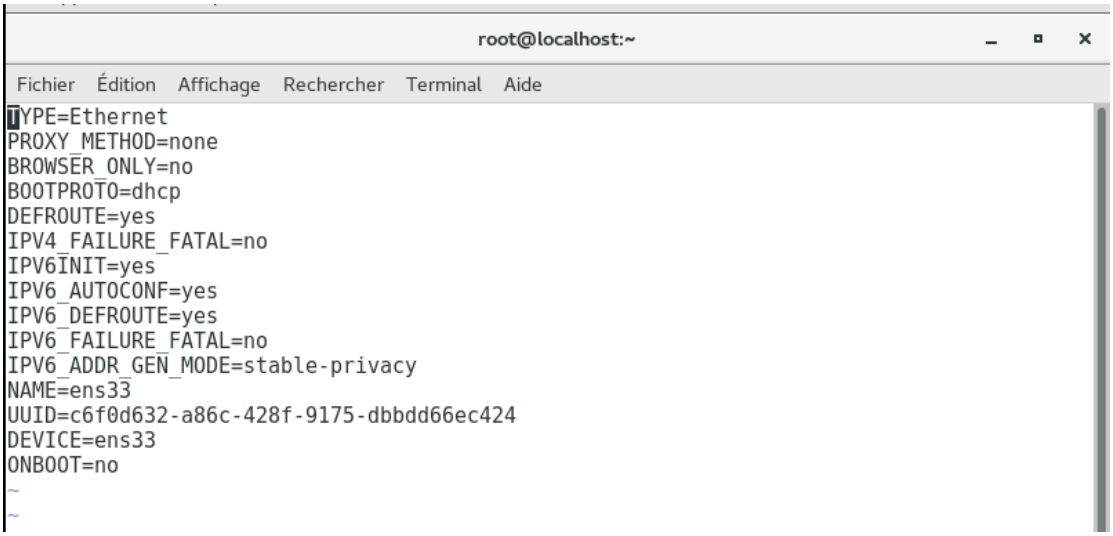
Dans ces menus, vous vous déplacez avec les flèches et la touche tabulation. Dans un premier temps, sélectionner **Activer une connexion** pour activer votre carte réseau.



Puis sélectionner votre carte dans la liste et cliquer sur **Activer**

Pour fixer les paramètres IP éditer directement les paramètres de la carte réseau dans le répertoire /etc/sysconfig/network-scripts et ensuite ouvrez le fichier correspondant au nom de votre carte réseau, nommés sous « ifcfg-X » où X est le nom de la carte réseau

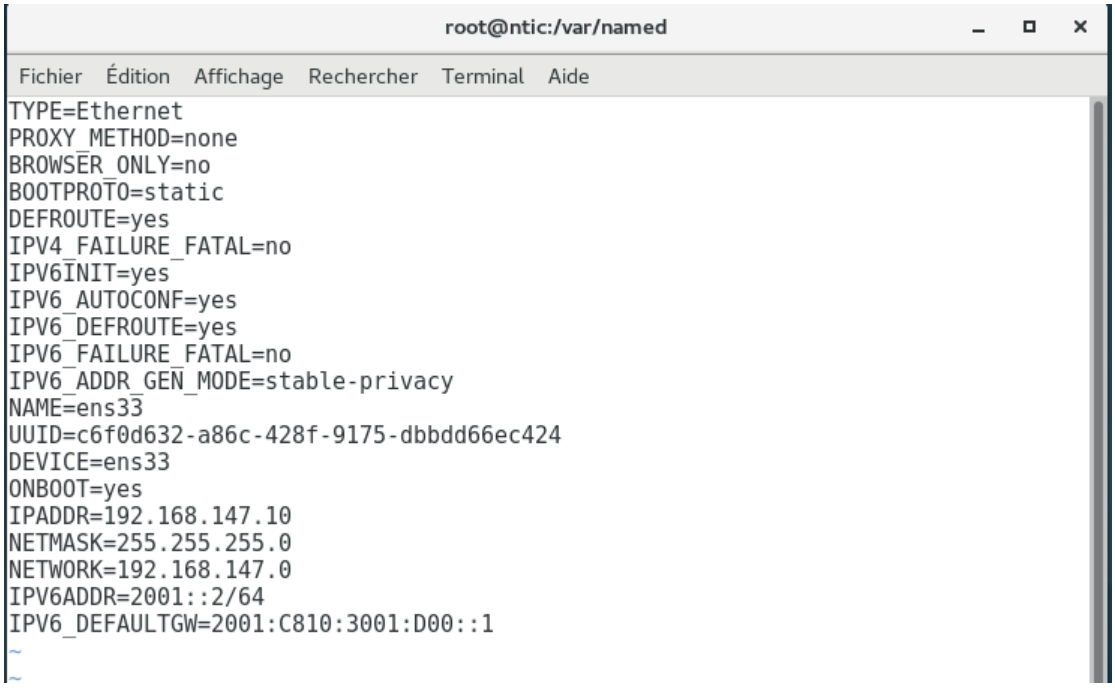
```
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-ens33
[root@localhost ~]#
```



Insérer l'adresse IP et au moins les lignes suivantes :

```
DEVICE=eth0              ## Nom de l'interface

BOOTPROTO=static         ## Passer en mode static et non DHCP

BROADCAST=192.168.0.255  ## Adresse de broadcast

HWADDR=AA:BB:CC:DD:EE:FF  ## MAC ADRESSE de la carte reseau

IPADDR=192.168.0.10      ## Adresse IP de la machine

NETMASK=255.255.255.0    ## Masque sous-reseau

NETWORK=192.168.0.0      ## Adresse reseau

IPV6INIT=yes             ##Activer la configuration d'IPv6 sur l'interface

IPV6ADDR=<ipv6-address>    ##Spécifie une adresse IPv6 statique

IPV6_DEFAULTGW=<ipv6-address> ##Ajoute une route par défaut via l'interface spécifiée

ONBOOT=yes               ## Monter l'interface au boot

NM_CONTROLLED="no"       ## Pas de contrôl via NetworkManager
```

Exemple :



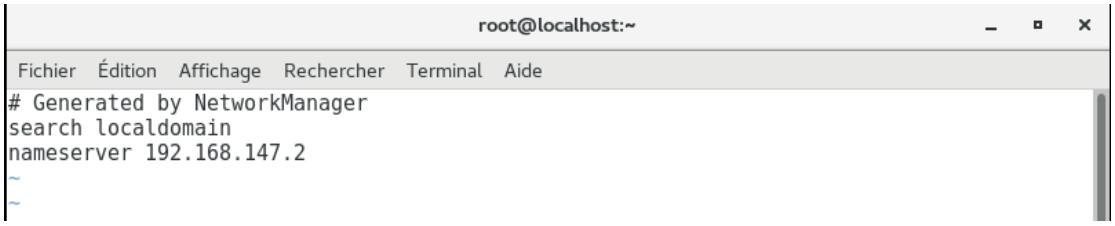
En complément, vous pouvez aussi éditer le fichier **/etc/sysconfig/network**, pour activer le réseau ainsi que la passerelle.

```
#vi /etc/sysconfig/network
```

```
NETWORKING=yes                ## Activer le reseau

GATEWAY=192.168.0.1           ## Adresse ip de votre passerelle
```

Les serveurs DNS sont spécifiés dans le fichier /etc/resolv.conf

```
#vi /etc/resolv.conf
```



Pour prendre toutes ces modifications en compte il faut de redémarrer le réseau.

```
#systemctl restart network
```

Lancer la commande ifconfig pour vérifier les paramètres réseau

```
#ifconfig
```

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.147.10  netmask 255.255.255.0  broadcast 192.168.147.255
        inet6 fe80::c535:8bed:e4f7:8a69  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:ef:d5  txqueuelen 1000  (Ethernet)
        RX packets 927  bytes 67071 (65.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 494  bytes 50248 (49.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5. Gestion des paquets

5.1 Rpm

Centos utilise les fichiers dits « RPM » (RPM Package Manager) qui sont des archives contenant des programmes pré-compilés prêts à l'emploi.

La commande rpm permet de gérer les paquets sous Centos. Voici les commandes de base :

Installer un paquet

```
# rpm -ivh package.rpm
```

Mettre à jour un paquet

```
# rpm -Uhv package.rpm
```

- -i -> install
- -U -> Upgrade (met à jour un paquet ou l'installe s'il n'est pas présent)
- -v -> verbose (détaille l'avancement de l'installation)
- -F -> Freshen (ne met à jour un paquet que s'il est installé)
- -h -> hash (permet d'avoir une « barre de progression »)

Désinstaller un paquet

```
# rpm -e package  (sans '.rpm')
```

Rechercher si un paquet est installé

```
# rpm -q package  (nom complet, sans '.rpm')
```

Recherche dans tous les paquets installés si gcc est présent

```
# rpm -qa | grep gcc
```

Liste de tous les paquets installés

```
rpm -qa
```

5.2 Yum

Lord de l'utilisation de la commande rpm le problème de la gestion des dépendances peut quelquefois devenir un véritable casse-tête (un logiciel qui en nécessite un autre, et un autre...).

Pour gérer les paquets du système, Fedora utilise YUM, un outil permettant de gérer les installations, les désinstallations et les mises à jour de paquets au format **RPM**. Il gére les dépendances en téléchargeant ce qui est nécessaire. Il trouve les paquets sur différentes sources (sites internet) que l'on appelle des **dépôts**.

YUM est fourni en standard dans toutes les versions de **Centos**.

Mettre à jour le système

```
# yum update
```

Mettre à jour un paquet

```
# yum update nom paquet
```

Rechercher un paquet

Pour chercher un paquet faite la commande :

```
# yum list <nom du paquet>
```

Il est aussi possible de faire une recherche plus large, plus uniquement sur le nom du paquet mais aussi sur la description:

```
# yum search <mot clef>
```

Installer un paquet

Pour installer un paquet :

```
# yum install <nom du paquet>
```

Supprimer un paquet

```
# yum remove <nom du paquet>
```

6. NMAP

La commande NMAP permet de scaner les ports

Pour installer Nmap sur Redhat, ouvrez un terminal et lancez la commande suivante :

```
# yum install nmap
```

La syntaxe est la suivante:

```
#nmap   –options   ip_du_serveur
```

Pour Voir tous les ports TCP ouverts sur une machine lancer la commande suivante :

```
#nmap –sS ip_du_serveur
```

Pour voir tous les ports UDP ouverts sur une machine :

```
#nmap –sU ip_du_serveur
```

Voir si une machine est sur le réseau (scan Ping) :

```
#nmap -sP ip_du_serveur
```

Scanner une plage d'adresses. Ici toutes les adresses de 192.168.0 à 192.168.255 :

```
#nmap 192.168.0-255
```

7. Gestionnaire de tache

Pour lister les processus de tous les utilisateurs du système :

```
ps  -aux
```

Pour lister uniquement vos processus :

```
ps  -fux
```

8. Netstat

Netstat (network statistics) est un outil en ligne de commande permettant de surveiller les connexions réseau entrantes et sortantes, ainsi pour afficher des tables de routage, des statistiques d'interface, etc. Netstat est disponible sur tous les systèmes d'exploitation de type Unix et également sur le système d'exploitation Windows. C'est très utile au niveau de dépannage réseau et de mesure des performances. netstat est l'un des outils de débogage les plus élémentaires des services réseau. Il vous indique les ports ouverts et s'il y'a des programmes qui écoutent les ports.

La commande netstat Linux peut prendre de nombreux paramètres :

- a : Tous les ports
- -t : Tous les ports TCP
- -u : Tous les ports UDP
- -l : Tous les ports en écoute
- -n : Affiche directement les IP. Pas de résolution de nom.
- -p : Affiche le nom du programme et le PID associé.

```
root@ntic ~]# netstat -paunt

Connexions Internet actives (serveurs et établies)

Proto Recv-Q Send-Q Adresse locale        Adresse distante       Etat       PID/Program name

tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1200/master

tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      1229/dnsmasq

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      987/sshd

tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      988/cupsd

tcp        0      0 192.168.1.10:37528      104.19.196.151:443      ESTABLISHED 4149/firefox

tcp        0      0 192.168.1.10:58604      172.217.171.226:443     ESTABLISHED 4149/firefox

tcp        0      0 192.168.1.10:60782      216.58.198.66:443       ESTABLISHED 4149/firefox

tcp        0      0 192.168.1.10:55224      172.217.19.46:443       ESTABLISHED 4149/firefox

tcp        0      0 192.168.1.10:37064      23.51.227.119:443       ESTABLISHED 4149/firefox

tcp        0      0 192.168.1.10:45816      172.217.171.195:443     ESTABLISHED 4149/firefox

tcp        0      0 192.168.1.10:37070      23.51.227.119:443       ESTABLISHED 4149/firefox

tcp        0      0 192.168.1.10:58198      172.217.19.33:443       TIME_WAIT   -

tcp        0      0 192.168.1.10:35674      81.192.28.25:80         ESTABLISHED 4149/firefox
```

Comment lire les résultats de la commande netstat, par colonnes :

- Proto : le protocole utilisé. Les classiques TCP et UDP mais également TCP6 et UDP6 pour les variantes IPV6.
- Recv-Q : Le nombre de Bytes dans la file d'attente de réception. Devrait toujours être à zéro
- Send-Q : Le nombre de Bytes dans la file d'attente d'envoi. Devrait toujours être à zéro
- Adresse locale : l'adresse et le port utilisé sur la machine locale
- Adresse distante : l'adresse et le port utilisé par la machine distante
- Etat : LISTEN quand le programme écoute et attend une connexion. ESTABLISHED lorsque la connexion est établie.
- PID/Program name : Le numéro de processus et le nom du programme

9. Traceroute

Une deuxième possibilité est d'utiliser la commande traceroute qui vous donne le chemin parcouru pour arriver jusqu'à une machine ou adresse. Cela correspond à une liste de machine, routeurs par où on passe pour arriver à la machine demandée. Par exemple voici le résultat d'un traceroute sur google.com:

```
[root@ntic ~]# traceroute google.com
traceroute to google.com (172.217.18.46), 30 hops max, 60 byte packets
 1  Tenda.Home (192.168.1.1)  6.489 ms  6.342 ms  6.249 ms
 2  105.154.240.1 (105.154.240.1)  79.965 ms  81.341 ms  83.177 ms
 3  adsl-146-65-192-81.adsl2.iam.net.ma (81.192.65.146)  93.068 ms adsl-154-65-192-81.a
dsl2.iam.net.ma (81.192.65.154)  93.955 ms  96.378 ms
 4  adsl-153-65-192-81.adsl2.iam.net.ma (81.192.65.153)  97.766 ms adsl-145-65-192-81.a
dsl2.iam.net.ma (81.192.65.145)  95.677 ms adsl-153-65-192-81.adsl2.iam.net.ma (81.192.
65.153)  102.074 ms
 5  adsl-22-12-192-81.adsl.iam.net.ma (81.192.12.22)  101.973 ms  101.438 ms adsl-26-12
-192-81.adsl.iam.net.ma (81.192.12.26)  105.802 ms
 6  te0-0-1-6.rcr22.svq01.atlas.cogentco.com (149.11.18.53)  116.717 ms  103.616 ms  10
5.994 ms
 7  be3286.rcr21.opo01.atlas.cogentco.com (130.117.49.81)  115.883 ms  63.466 ms  66.95
2 ms
 8  be3305.ccr52.bio02.atlas.cogentco.com (130.117.1.29)  82.309 ms be3306.ccr51.bio02.
atlas.cogentco.com (130.117.1.37)  79.283 ms be3305.ccr52.bio02.atlas.cogentco.com (130
.117.1.29)  79.565 ms
 9  be3324.ccr42.par01.atlas.cogentco.com (130.117.2.66)  94.927 ms  93.842 ms  98.238
ms
10  be2103.ccr32.par04.atlas.cogentco.com (154.54.61.22)  96.650 ms be2102.ccr32.par04.
atlas.cogentco.com (154.54.61.18)  97.558 ms be2103.ccr32.par04.atlas.cogentco.com (154
```

10.Arp

La commande *arp* est régulièrement utilisée pour 3 usages, afficher le cache arp, ajouter un hôte ou supprimer un hôte du cache.

2.1 Affichage

Afficher le cache arp est utile pour retrouver un hôte posant problème sur le réseau, et pour vérifier la validité des données. Lorsque la commande est invoquée sans options comme dans l'exemple précédent, elle affiche le contenu de la table. Deux options sont intéressantes pour l'affichage. u

3.1 Ajout d'un hôte

L'option permettant d'ajouter un hôte est *-s hôte adresse_materielle hôte* est l'adresse IP d'un hôte ou son nom, et *adresse_materielle* est l'adresse physique correspondante.

```
# arp  -s   192.168.0.2       00:50:12:34:56:78
```

Notez le "*PERM*" pour l'adresse 192.168.0.2 qui indique que l'entrée est statique.

4.1 Suppression d'un hôte

L'option permettant de retirer une entrée du cache arp est -d, on précise ensuite le nom d'hôte ou l'adresse IP à supprimer.

```
# arp   -d   192.168.0.2
```

11.Référence

https://www.quennec.fr/trucs-astuces/syst%C3%A8mes/centos-7/r%C3%A9seau/centos-configuration-ip-statique
https://quick-tutoriel.com/comment-configurer-le-reseau-sur-une-centos-v7
https://waytolearnx.com/2019/05/15-commandes-netstat-pour-la-gestion-de-reseau-sous-linux.html
https://www.leunen.com/linux/2008/03/ping-traceroute-et-nmap/
http://www.linuxcertif.com/doc/keyword//sbin/arp/