

Version : **2022.01**

Dernière mise-à-jour : 2023/02/15 15:54

LCF303 - Gestion du Réseau TCPv4

Contenu du Module

- **LCF303 - Gestion du Réseau TCPv4**
 - Contenu du Module
 - Configuration du Réseau sous RHEL/CentOS 5 et 6
 - Configuration de TCP/IP
 - DHCP
 - /etc/sysconfig/network
 - /etc/sysconfig/network-scripts/ifcfg-ethX (où X=0,1 ...)
 - IP Fixe
 - /etc/sysconfig/network
 - /etc/sysconfig/network-scripts/ifcfg-ethX (où X=0,1 ...)
 - La Commande hostname
 - La Commande ifconfig
 - Activer/Désactiver une Interface Manuellement
 - /etc/networks
 - Résolution d'adresses IP
 - /etc/resolv.conf
 - /etc/nsswitch.conf
 - /etc/hosts
 - Services réseaux
 - xinetd
 - TCP Wrapper
 - Routage Statique
 - La Commande route

- Activer/désactiver le routage sur le serveur
- Configuration du Réseau sous RHEL/CentOS 7
 - La Commande nmcli
 - Connections et Profils
 - Ajouter une Deuxième Adresse IP à un Profil
 - La Commande hostname
 - La Commande ip
 - Activer/Désactiver une Interface Manuellement
 - Routage Statique
 - La commande ip
 - Activer/désactiver le routage sur le serveur
- Diagnostic du Réseau
 - ping
 - netstat -i
 - traceroute
- Connexions à Distance
 - Telnet
 - wget
 - ftp
 - SSH
 - Introduction
 - SSH-1
 - SSH-2
 - L'authentification par mot de passe
 - L'authentification par clef asymétrique
 - Installation
 - Configuration
 - Serveur
 - Utilisation
 - Tunnels SSH
- SCP
 - Introduction
 - Utilisation
 - Mise en place des clefs

Configuration du Réseau sous RHEL/CentOS 5 et 6

Configuration de TCP/IP

La configuration TCP/IP se trouve dans le répertoire **/etc/sysconfig**. Les fichiers importants sont :

DHCP

/etc/sysconfig/network

```
[root@centos6 ~]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=centos6
```

Dans ce fichier vous pouvez constater les directives suivantes :

Directive	Description
NETWORKING	Indique que la prise en charge du réseau est activée
HOSTNAME	Indique le nom d'hôte de la machine

Ce fichier peut également contenir les directives suivantes :

Directive	Description
GATEWAY	Indique l'adresse IPv4 de la passerelle
GATEWAYDEV	Indique l'interface réseau utilisée pour accéder à la passerelle
NISDOMAIN	Indique le domaine NIS s'il en existe un
NETWORKING_IPV6	Active ou désactive le support IPv6

/etc/sysconfig/network-scripts/ifcfg-ethX (où X=0,1 ...)

ifcfg-eth0

```
[root@centos6 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
NM_CONTROLLED="yes"
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth0"
UUID=5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
HWADDR=08:00:27:48:7D:7F
PEERDNS=yes
PEERROUTES=yes
```

Dans ce fichier vous pouvez constater les directives suivantes :

Directive	Description
DEVICE	Indique le nom de l'interface
NM_CONTROLLED	Indique que le service NetworkManager est utilisé pour gérer les interfaces réseau
ONBOOT	Indique que l'interface est activée au démarrage de la machine
TYPE	Indique que le type de réseau est ethernet. Les valeurs permises sont ethernet ou wireless
BOOTPROTO	Indique comment monter l'interface. Les valeurs permises sont dhcp, static ou bootp
DEFROUTE	Définit l'interface en tant que passerelle par défaut
IPV4_FAILURE_FATAL	Stipule que si IPv4 et IPv6 sont activés et la connexion IPv4 est perdue, la connexion IPv6 est considérée d'être perdue
IPV6INIT	Indique que le support IPv6 ne sera pas initialisé
NAME	Indique un nom descriptif de l'interface
UUID	Indique la valeur de l'UUID de l'interface

Directive	Description
HWADDR	Indique l'adresse MAC de l'interface
PEERDNS	Indique que le fichier /etc/resolv.conf doit être modifié automatiquement pour contenir les adresses IP des DNS fournies par le serveur DHCP



Recherchez la définition de la directive **PEERROUTES=yes**.

IP Fixe

/etc/sysconfig/network

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=centos6.fenestros.loc
```

/etc/sysconfig/network-scripts/ifcfg-ethX (où X=0,1 ...)

ifcfg-eth0

```
DEVICE="eth0"
NM_CONTROLLED="no"
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=static
IPV6INIT=no
HWADDR="08:00:27:9B:55:B1"
NETMASK=255.255.255.0
IPADDR=10.0.2.15
```

```
GATEWAY=10.0.2.2
DNS1=8.8.8.8
DNS2=8.8.4.4
DOMAIN=fenestros.loc
USERCTL=yes
```

Dans ce fichier vous pouvez constater les nouvelles directives suivantes :

Directive	Description
NETMASK	Indique le masque de sous-réseau IPv4 associé à l'interface
IPADDR	Indique l'adresse IPv4 de l'interface
GATEWAY	Indique l'adresse IPv4 de la passerelle par défaut
DNS1	Indique le DNS primaire
DNS2	Indique le DNS secondaire
DOMAIN	Indique le nom du domaine local
USERCTL	Indique que les utilisateurs normaux peuvent activer/désactiver l'interface



Notez que VirtualBox fournit une passerelle par défaut (10.0.2.2).

Après avoir modifier les deux fichiers **/etc/sysconfig/network** et **/etc/sysconfig/network-scripts/ifcfg-eth0** vous devez désactiver le service **NetworkManager** utilisé pour la connexion DHCP et activer le service **network** :

```
[root@centos6 ~]# service NetworkManager stop
Arrêt du démon NetworkManager :                [ OK ]
[root@centos6 ~]# chkconfig --del NetworkManager
[root@centos6 ~]# service network start
Activation de l'interface loopback :            [ OK ]
Activation de l'interface eth0 :                 [ OK ]
[root@centos6 ~]#
```

La Commande hostname

Lors du passage à une configuration en IPv4 fixe vous avez modifié la directive **HOSTNAME** du fichier **/etc/sysconfig/network** de **centos** à **centos.fenestros.loc**. Afin d'informer le système immédiatement de la modification du FQDN (*Fully Qualified Domain Name*), utilisez la commande **hostname** :

```
[root@centos6 ~]# hostname
centos6
[root@centos6 ~]# hostname centos6.fenestros.loc
[root@centos6 ~]# hostname
centos6.fenestros.loc
```

Pour afficher le FQDN du système vous pouvez également utiliser la commande suivante :

```
[root@centos6 ~]# uname -n
centos6.fenestros.loc
```

Options de la commande hostname

Les options de cette commande sont :

```
[root@centos6 ~]# hostname --help
Syntaxe : hostname [-v] {hôte|-F fichier}      définit le nom d'hôte (depuis le fichier)
          domainname [-v] {domaine_nis|-F fichier}  définit le domaine NIS (depuis le fichier)
          hostname [-v] [-d|-f|-s|-a|-i|-y]  display formatted name
          hostname [-v]                        affiche le nom d'hôte

          hostname -V|--version|-h|--help      affiche des infos et termine

          dnsdomainname=hostname -d, {yp,nis,}domainname=hostname -y

          -s, --short                          nom d'hôte court
```

```
-a, --alias          noms d'alias
-i, --ip-address     adresses de l'hôte
-f, --fqdn, --long   nom d'hôte long (FQDN)
-d, --domain         nom de domaine DNS
-y, --yp, --nis      nom de domaine NIS/YP
-F, --file           read hostname or NIS domainname from given file
```

This command can read or set the hostname or the NIS domainname. You can also read the DNS domain or the FQDN (fully qualified domain name). Unless you are using bind or NIS for host lookups you can change the FQDN (Fully Qualified Domain Name) and the DNS domain name (which is part of the FQDN) in the /etc/hosts file.

La Commande ifconfig

Pour afficher la configuration IP de la machine il faut saisir la commande suivante :

```
[root@centos6 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:48:7D:7F
          inet adr:10.0.2.15  Bcast:10.0.2.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe48:7d7f/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16765 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15256 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:12435171 (11.8 MiB)  TX bytes:4767389 (4.5 MiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 lg file transmission:0  
RX bytes:480 (480.0 b) TX bytes:480 (480.0 b)
```

La commande ifconfig est également utilisée pour configurer une interface.

Créez maintenant une interface fictive ainsi :

```
[root@centos6 ~]# ifconfig eth0:1 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
```

Constatez maintenant le résultat :

```
[root@centos6 ~]# ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:48:7D:7F  
          inet adr:10.0.2.15  Bcast:10.0.2.255  Masque:255.255.255.0  
          adr inet6: fe80::a00:27ff:fe48:7d7f/64 Scope:Lien  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:16904 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:15337 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 lg file transmission:1000  
          RX bytes:12445250 (11.8 MiB)  TX bytes:4816855 (4.5 MiB)  
  
eth0:1    Link encap:Ethernet  HWaddr 08:00:27:48:7D:7F  
          inet adr:192.168.1.2  Bcast:192.168.1.255  Masque:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
  
lo        Link encap:Boucle locale  
          inet adr:127.0.0.1  Masque:255.0.0.0  
          adr inet6: ::1/128 Scope:Hôte  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 lg file transmission:0  
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)
```

Options de la commande ifconfig

Les options de cette commande sont :

```
[root@centos6 ~]# ifconfig --help
```

Usage:

```
ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
[add <adresse>[/<lg_prefixe>]]
[del <adresse>[/<lg_prefixe>]]
[[-]broadcast [<adresse>]] [[-]pointopoint [<adresse>]]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <adresse>] [metric <NN>] [mtu <NN>]
[[-]trailers] [[-]arp] [[-]allmulti]
[multicast] [[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
[[-]dynamic]
[up|down] ...
```

<HW>=Type de matériel.

Liste des types de matériels possibles:

```
loop (Boucle locale) slip (IP ligne série) cslip (IP ligne série - VJ )
slip6 (IP ligne série - 6 bits) cslip6 (IP ligne série - 6 bits VJ) adaptive (IP ligne série adaptative)
strip (Metricom Starmode IP) ash (Ash) ether (Ethernet)
tr (16/4 Mbps Token Ring) tr (16/4 Mbps Token Ring (New)) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
ppp (Protocole Point-à-Point) hdlc ((Cisco)-HDLC) lapb (LAPB)
arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Périphérie d'accès Frame Relay)
sit (IPv6-dans-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
irda (IrLAP) ec (Econet) x25 (generic X.25)
infiniband (InfiniBand)
```

<AF>=famille d'Adresses. Défaut: inet

Liste des familles d'adresses possibles:

unix (Domaine UNIX) inet (DARPA Internet) inet6 (IPv6)
ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
ash (Ash) x25 (CCITT X.25)

Activer/Désactiver une Interface Manuellement

Deux commandes existent pour activer et désactiver manuellement une interface réseau :

```
[root@centos6 ~]# ifdown eth0
[root@centos6 ~]# ifconfig
lo          Link encap:Boucle locale
            inet adr:127.0.0.1  Masque:255.0.0.0
            adr inet6: ::1/128 Scope:Hôte
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:384 errors:0 dropped:0 overruns:0 frame:0
            TX packets:384 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 lg file transmission:0
            RX bytes:32496 (31.7 KiB)  TX bytes:32496 (31.7 KiB)

[root@centos6 ~]# ifup eth0
État de connexion active&nbsp;; activation
État de chemin actif&nbsp;;: /org/freedesktop/NetworkManager/ActiveConnection/0
état&nbsp;;: activé
Connexion activée
[root@centos6 ~]# ifconfig
eth0        Link encap:Ethernet  HWaddr 08:00:27:9B:55:B1
            inet adr:10.0.2.15  Bcast:10.0.2.255  Masque:255.255.255.0
            adr inet6: fe80::a00:27ff:fe9b:55b1/64 Scope:Lien
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:27 errors:0 dropped:0 overruns:0 frame:0
            TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 lg file transmission:1000
RX bytes:4271 (4.1 KiB) TX bytes:6145 (6.0 KiB)

lo    Link encap:Boucle locale
      inet adr:127.0.0.1  Masque:255.0.0.0
      adr inet6: ::1/128 Scope:Hôte
      UP LOOPBACK RUNNING  MTU:65536  Metric:1
      RX packets:392 errors:0 dropped:0 overruns:0 frame:0
      TX packets:392 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:0
      RX bytes:33600 (32.8 KiB) TX bytes:33600 (32.8 KiB)
```

/etc/networks

Ce fichier contient la correspondance entre des noms de réseaux et l'adresse IP du réseau :

```
[root@centos6 ~]# cat /etc/networks
default 0.0.0.0
loopback 127.0.0.0
link-local 169.254.0.0
```

Résolution d'adresses IP

La configuration DNS est stockée dans le fichier **/etc/resolv.conf**.

/etc/resolv.conf

La configuration DNS est stockée dans le fichier **/etc/resolv.conf** :

```
[root@centos6 ~]# cat /etc/resolv.conf
```

```
# Generated by NetworkManager

# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so:
#
# DNS1=xxx.xxx.xxx.xxx
# DNS2=xxx.xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
nameserver 8.8.8.8
nameserver 8.8.4.4
search fenestros.loc
```



Notez que les DNS utilisés sont les serveurs DNS publics de Google.

/etc/nsswitch.conf

L'ordre de recherche des services de noms est stocké dans le fichier **/etc/nsswitch.conf**. Pour connaître l'ordre, saisissez la commande suivante :

```
[root@centos6 ~]# grep '^hosts:' /etc/nsswitch.conf
hosts:      files dns
```

/etc/hosts

Le mot **files** dans la sortie de la commande précédente fait référence au fichier **/etc/hosts** :

```
[root@centos6 ~]# cat /etc/hosts
10.0.2.15    centos6    # Added by NetworkManager
```

```
127.0.0.1    localhost.localdomain    localhost
::1 centos6  localhost6.localdomain6  localhost6
```

Pour tester le serveur DNS, deux commandes sont possibles :

```
[root@centos6 ~]# nslookup www.i2tch.com
```

```
Server:      8.8.8.8
```

```
Address:     8.8.8.8#53
```

```
Non-authoritative answer:
```

```
www.i2tch.com canonical name = i2tch.com.
```

```
Name:   i2tch.com
```

```
Address: 90.119.37.144
```

```
[root@centos6 ~]# dig www.i2tch.com
```

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.i2tch.com
```

```
;; global options: +cmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25061
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 65494
```

```
;; QUESTION SECTION:
```

```
;www.i2tch.com.          IN      A
```

```
;; ANSWER SECTION:
```

```
www.i2tch.com.          6563    IN      CNAME    i2tch.com.
```

```
i2tch.com.              50      IN      A          90.119.37.144
```

```
;; Query time: 1 msec
```

```
;; SERVER: 8.8.8.8#53(8.8.8.8)
```

```
;; WHEN: Mon Jan 22 18:00:27 CET 2018
```

```
;; MSG SIZE rcvd: 72
```

Services réseaux

Quand un client émet une demande de connexion vers une application réseau sur un serveur, il utilise un socket attaché à un port local **supérieur à 1023**, alloué d'une manière dynamique. La requête contient le port de destination sur le serveur. Certaines applications serveurs se gèrent toutes seules, ce qui est le cas par exemple d'**httpd**. Par contre d'autres sont gérées par le service **xinetd**.

xinetd

Sous RHEL/CentOS 6 xinetd n'est pas installé par défaut. Installez-le grâce à yum :

```
[root@centos6 ~]# yum install xinetd
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: fr2.rpmfind.net
 * extras: fr2.rpmfind.net
 * updates: fr2.rpmfind.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package xinetd.i686 2:2.3.14-33.el6 set to be updated
--> Finished Dependency Resolution
```

Dependencies Resolved

Package	Arch	Version	Repository	Size
Installing:				
xinetd	i686	2:2.3.14-33.el6	base	121 k

Transaction Summary

```
=====
Install      1 Package(s)
Upgrade      0 Package(s)
```

Total download size: 121 k

Installed size: 258 k

Is this ok [y/N]: y

Downloading Packages:

```
xinetd-2.3.14-33.el6.i686.rpm          | 121 kB      00:00
```

Running rpm_check_debug

Running Transaction Test

Transaction Test Succeeded

Running Transaction

```
Installing      : 2:xinetd-2.3.14-33.el6.i686                1/1
```

Installed:

xinetd.i686 2:2.3.14-33.el6

Complete!

Le programme xinetd est configuré via le fichier **/etc/xinetd.conf** :

```
[root@centos6 ~]# cat /etc/xinetd.conf
#
# This is the master xinetd configuration file. Settings in the
# default section will be inherited by all service configurations
# unless explicitly overridden in the service configuration. See
# xinetd.conf in the man pages for a more detailed explanation of
# these attributes.

defaults
{
# The next two items are intended to be a quick access place to
```

```
# temporarily enable or disable services.
#
#   enabled      =
#   disabled     =

# Define general logging characteristics.
    log_type      = SYSLOG daemon info
    log_on_failure = HOST
    log_on_success = PID HOST DURATION EXIT

# Define access restriction defaults
#
#   no_access     =
#   only_from     =
#   max_load      = 0
#   cps           = 50 10
#   instances     = 50
#   per_source    = 10

# Address and networking defaults
#
#   bind          =
#   mdns          = yes
#   v6only        = no

# setup environmental attributes
#
#   passenv       =
#   groups        = yes
#   umask         = 002

# Generally, banners are not used. This sets up their global defaults
#
#   banner        =
```

```
# banner_fail    =  
# banner_success  =  
}  
  
includedir /etc/xinetd.d
```

Les valeurs des directives dans le fichier **/etc/xinetd.conf** sont héritées par toutes les configurations des services sauf dans le cas où une variable est explicitement fixée dans un des fichiers de définitions des services se trouvant dans **/etc/xinetd.d**.

Les variables les plus importantes dans **/etc/xinetd.conf** :

Directive	Description
instances	Le nombre de demandes d'accès simultanés
log_type	Indique à xinetd d'adresser les traces à SYSLOG avec l'étiquette de sous-système applicatif daemon et la priorité de info
log_on_success	Indique que SYSLOG doit journaliser le PID, HOST, DURATION et EXIT en cas de succès
log_on_failure	Indique que SYSLOG doit journaliser le HOST en cas d'échec
cps	Indique 50 connexions par seconde avec un temps d'indisponibilité de 10 secondes si le seuil est atteint

Les options concernant les journaux sont :

HOST	Journalisation de l'adresse IP de l'hôte distant
PID	Journalisation du PID du processus qui reçoit la demande d'accès
DURATION	Journalisation des durées d'utilisation
EXIT	Journalisation de l'état ou du signal de fin de service

Il est aussi possible de trouver les options suivantes pour les journaux :

ATTEMPT	Journalisation des connexions en échec
USERID	Journalisation des données concernant l'utilisateur selon la RFC 1413

Examinons maintenant le répertoire **/etc/xinetd.d** :

```
[root@centos6 ~]# ls -l /etc/xinetd.d  
total 52
```

```
-rw-----. 1 root root 1157 7 déc. 22:07 chargen-dgram
-rw-----. 1 root root 1159 7 déc. 22:07 chargen-stream
-rw-r--r--. 1 root root 523 25 juin 2011 cvs
-rw-----. 1 root root 1157 7 déc. 22:07 daytime-dgram
-rw-----. 1 root root 1159 7 déc. 22:07 daytime-stream
-rw-----. 1 root root 1157 7 déc. 22:07 discard-dgram
-rw-----. 1 root root 1159 7 déc. 22:07 discard-stream
-rw-----. 1 root root 1148 7 déc. 22:07 echo-dgram
-rw-----. 1 root root 1150 7 déc. 22:07 echo-stream
-rw-r--r--. 1 root root 332 20 mai 2009 rsync
-rw-----. 1 root root 1212 7 déc. 22:07 tcpmux-server
-rw-----. 1 root root 1149 7 déc. 22:07 time-dgram
-rw-----. 1 root root 1150 7 déc. 22:07 time-stream
```

A l'examen de ce répertoire vous noterez que celui-ci contient des fichiers nominatifs par application-serveur, par exemple pour le serveur cvs :

```
[root@centos6 ~]# cat /etc/xinetd.d/cvs
# default: off
# description: The CVS service can record the history of your source \
#               files. CVS stores all the versions of a file in a single \
#               file in a clever way that only stores the differences \
#               between versions.
service cvspserver
{
    disable          = yes
    port             = 2401
    socket_type      = stream
    protocol         = tcp
    wait             = no
    user             = root
    passenv          = PATH
    server           = /usr/bin/cvs
    env              = HOME=/var/cvs
    server_args      = -f --allow-root=/var/cvs pserver
```

```
# bind          = 127.0.0.1
}
```

Les directives principales de ce fichier sont :

Paramètre	Description
disable	no : Le service est actif. yes : Le service est désactivé
port	Le numéro de port ou, à défaut, le numéro indiqué pour le service dans le fichier /etc/services
socket_type	Nature du socket, soit stream pour TCP soit dgram pour UDP
protocol	Protocole utilisé soit TCP soit UDP
wait	no : indique si xinetd active un serveur par client. yes : indique que xinetd active un seul serveur pour tous les client
user	Indique le compte sous lequel le serveur est exécuté
server	Indique le chemin d'accès de l'application serveur
env	Définit un environnement système
server_args	Donne les arguments transmis à l'application serveur

Cependant il est aussi possible d'utiliser les directives suivantes :

Paramètre	Description	Exemple
nice	Fixe le niveau de nice entre -19 et +20	10
max_load	Fixe la charge CPU maximum admise. Au delà aucune connexion supplémenaire en sera acceptée	2.5
bind	Limite le service à l'interface dont l'adresse IP est indiquée	192.168.1.1
only_from	Limite le service aux seuls clients indiqués par la plage donnée	192.168.1.0/24 fenestros.loc
no_access	Interdit le service aux clients indiqués par la plage donnée	192.168.2.0/24, i2tch.loc
access_time	Limite l'accès au service à une plage horaire	09:00-19:00
redirect	Redirige les requêtes sur un port donné à une autre adresse IP	192.168.1.10 23

Afin d'activer une application serveur, il suffit de modifier le paramètre **disable** dans le fichier concerné et de relancer le service xinetd.

TCP Wrapper

TCP Wrapper contrôle l'accès à des services réseaux grâce à des **ACL**.

Quand une requête arrive pour un serveur, xinetd active le wrapper **tcpd** au lieu d'activer le serveur directement.

tcpd met à jour un journal et vérifie si le client a le droit d'utiliser le service concerné. Les ACL se trouvent dans deux fichiers:

- **/etc/hosts.allow**
- **/etc/hosts.deny**

Il faut noter que si ces fichiers n'existent pas ou sont vides, il n'y a pas de contrôle d'accès.

Le format d'une ligne dans un de ces deux fichiers est:

```
démon : liste_de_clients
```

Par exemple dans le cas d'un serveur **démon**, on verrait une ligne dans le fichier **/etc/hosts.allow** similaire à:

```
démon : LOCAL, .fenestros.loc
```

ce qui implique que les machines dont le nom ne comporte pas de point ainsi que les machines du domaine **fenestros.loc** sont autorisées à utiliser le service.

Le mot clef **ALL** peut être utilisé pour indiquer tout. Par exemple, **ALL:ALL** dans le fichier **/etc/hosts.deny** bloque effectivement toute tentative de connexion à un service xinetd sauf pour les ACL inclus dans le fichier **/etc/hosts.allow**.

Routage Statique

La Commande route

Pour afficher la table de routage de la machine vous pouvez utiliser la commande **route** :

```
[root@centos6 ~]# route  
Table de routage IP du noyau
```

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
192.168.1.0	*	255.255.255.0	U	0	0	0	eth0
10.0.2.0	*	255.255.255.0	U	0	0	0	eth0
link-local	*	255.255.0.0	U	1002	0	0	eth0
default	10.0.2.2	0.0.0.0	UG	0	0	0	eth0

La table issue de la commande **route** indique les informations suivantes:

- La destination qui peut être un hôte ou un réseau et est identifiée par les champs **Destination** et **Genmask**
- La route à prendre identifiée par les champs **Gateway** et **Iface**. Dans le cas d'une valeur de 0.0.0.0 ceci spécifie une route directe. La valeur d'Iface spécifie la carte à utiliser,
- Le champ **Indic** qui peut prendre un ou plusieurs de valeurs suivantes:
 - U - **Up** - la route est active
 - H - **Host** - la route conduit à un hôte
 - G - **Gateways** - la route passe par une passerelle
- Le champ **Metric** indique le nombre de sauts (passerelles) pour atteindre la destination,
- Le champ **Ref** indique le nombre de références à cette route. Ce champ est utilisé par le Noyau de Linux,
- Le champ **Use** indique le nombre de recherches associés à cette route.

La commande **route** permet aussi de paramétrer le routage indirect. Par exemple pour supprimer la route vers le réseau 192.168.1.0 :

```
[root@centos6 ~]# route del -net 192.168.1.0 netmask 255.255.255.0
[root@centos6 ~]# route
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref       Use Iface
10.0.2.0          *               255.255.255.0    U        0      0         0 eth0
link-local        *               255.255.0.0      U       1002    0         0 eth0
default          10.0.2.2        0.0.0.0          UG        0      0         0 eth0
```

Pour ajouter la route vers le réseau 192.168.1.0 :

```
[root@centos6 ~]# route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.2
[root@centos6 ~]# route
Table de routage IP du noyau
```

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
192.168.1.0	192.168.1.2	255.255.255.0	UG	0	0	0	eth0
10.0.2.0	*	255.255.255.0	U	0	0	0	eth0
link-local	*	255.255.0.0	U	1002	0	0	eth0
default	10.0.2.2	0.0.0.0	UG	0	0	0	eth0



La commande utilisée pour ajouter une passerelle par défaut prend la forme suivante **route add default gw *numéro_ip* interface**.

Les options cette commande sont :

```
[root@centos6 ~]# route --help
Syntaxe: route [-nNvee] [-FC] [<AF>]          Liste les tables de routage noyau
          route [-v] [-FC] {add|del|flush} ...  Modifie la table de routage pour AF.

          route {-h|--help} [<AF>]              Utilisation détaillée pour l'AF spécifié.
          route {-V|--version}                  Affiche la version/auteur et termine.

          -v, --verbose                        mode verbeux
          -n, --numeric                        don't resolve names
          -e, --extend                         display other/more information
          -F, --fib                           display Forwarding Information Base (default)
          -C, --cache                          affiche le cache de routage au lieu de FIB

<AF>=Use '-A <af>' or '--<af>'; default: inet
Liste les familles d'adresses possibles (supportant le routage):
  inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
  x25 (CCITT X.25)
```

Vous pouvez aussi utiliser la commande **netstat** pour afficher la table de routage de la machine :

```
[root@centos6 ~]# netstat -nr
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic   MSS  Fenêtre  irrt  Iface
192.168.1.0      192.168.1.2     255.255.255.0    UG      0 0        0 eth0
192.168.1.0      0.0.0.0         255.255.255.0    U       0 0        0 eth0
10.0.2.0         0.0.0.0         255.255.255.0    U       0 0        0 eth0
0.0.0.0          10.0.2.2        0.0.0.0          UG      0 0        0 eth0
```

La table issue de la commande **netstat -nr** indique les informations suivantes:

- La champ **MSS** indique la taille maximale des segments TCP sur la route,
- Le champ **Window** indique la taille de la fenêtre sur cette route,
- Le champ **irrt** indique le paramètre IRRT pour la route.

Activer/désactiver le routage sur le serveur

Pour activer le routage sur le serveur, il convient d'activer la retransmission des paquets:

```
[root@centos6 ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@centos6 ~]# cat /proc/sys/net/ipv4/ip_forward
1
```

Pour désactiver le routage sur le serveur, il convient de désactiver la retransmission des paquets:

```
[root@centos6 ~]# echo 0 > /proc/sys/net/ipv4/ip_forward
[root@centos6 ~]# cat /proc/sys/net/ipv4/ip_forward
0
```

Configuration du Réseau sous RHEL/CentOS 7

RHEL/CentOS 7 utilise exclusivement **Network Manager** pour gérer le réseau. Network Manager est composé de deux éléments :

- un service qui gère les connexions réseaux et rapporte leurs états,
- des front-ends qui passent par un API de configuration du service.



Important : Notez qu'avec cette version de NetworkManager, IPv6 est activée par défaut.

Le service NetworkManager doit toujours être lancé :

```
[root@centos7 ~]# systemctl status NetworkManager.service
● NetworkManager.service - Network Manager
   Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2016-08-07 09:18:20 CEST; 1 day 1h ago
   Main PID: 673 (NetworkManager)
   CGroup: /system.slice/NetworkManager.service
           └─ 673 /usr/sbin/NetworkManager --no-daemon
              └─ 2673 /sbin/dhclient -d -q -sf /usr/libexec/nm-dhcp-helper -pf /var/run/dhclient-enp0s3.pid -lf
                 /var/lib/NetworkManager/dhclient-45b701c1-0a21-4d76-a795-...

Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    nameserver '8.8.8.8'
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    (enp0s3): DHCPv4 state changed unknown ->
bound
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    (enp0s3): device state change: ip-config ->
ip-check (reason 'none') [70 80 0]
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    (enp0s3): device state change: ip-check ->
secondaries (reason 'none') [80 90 0]
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    (enp0s3): device state change: secondaries ->
activated (reason 'none') [90 100 0]
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    NetworkManager state is now CONNECTED_LOCAL
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    NetworkManager state is now CONNECTED_GLOBAL
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    Policy set 'Wired connection 1' (enp0s3) as
default for IPv4 routing and DNS.
Aug 08 11:03:55 centos7.fenestros.loc NetworkManager[673]: <info>    (enp0s3): Activation: successful, device
```

activated.

Aug 08 11:03:55 centos7.fenestros.loc dhclient[2673]: bound to 10.0.2.15 -- renewal in 39589 seconds.

La Commande nmcli

La commande **nmcli** (Network Manager Command Line Interface) est utilisée pour configurer NetworkManager.

Les options et les sous-commandes peuvent être consultées en utilisant les commandes suivantes :

```
[root@centos7 ~]# nmcli help
Usage: nmcli [OPTIONS] OBJECT { COMMAND | help }

OPTIONS
  -t[erse]                terse output
  -p[retty]               pretty output
  -m[ode] tabular|multiline  output mode
  -f[ields] <field1,field2,...>|all|common  specify fields to output
  -e[scape] yes|no         escape columns separators in values
  -n[ocheck]              don't check nmcli and NetworkManager versions
  -a[sk]                  ask for missing parameters
  -w[ait] <seconds>        set timeout waiting for finishing operations
  -v[ersion]              show program version
  -h[elp]                 print this help

OBJECT
  g[eneral]               NetworkManager's general status and operations
  n[etworking]            overall networking control
  r[adio]                 NetworkManager radio switches
  c[onnection]            NetworkManager's connections
  d[evice]                devices managed by NetworkManager
  a[gent]                 NetworkManager secret agent or polkit agent

[root@centos7 ~]# nmcli g help
```

```
Usage: nmcli general { COMMAND | help }
```

```
COMMAND := { status | hostname | permissions | logging }
```

```
status
```

```
hostname [<hostname>]
```

```
permissions
```

```
logging [level <log level>] [domains <log domains>]
```

```
[root@centos7 ~]# nmcli g status help
```

```
Usage: nmcli general status { help }
```

Show overall status of NetworkManager.

'status' is the default action, which means 'nmcli gen' calls 'nmcli gen status'

Connections et Profils

NetworkManager inclut la notion de **connections** ou **profils** permettant des configurations différentes en fonction de la localisation. Pour voir les connections actuelles, utilisez la commande **nmcli c** avec la sous-commande **show** :

```
[root@centos7 ~]# nmcli c show
```

NAME	UUID	TYPE	DEVICE
Wired connection 1	45b701c1-0a21-4d76-a795-2f2bcba86955	802-3-ethernet	enp0s3

Comme on peut constater ici, il n'existe pour le moment, qu'un seul profil.

Créez donc un profil IP fixe rattaché au périphérique **enp0s3** :

```
[root@centos7 ~]# nmcli connection add con-name ip_fixe ifname enp0s3 type ethernet ip4 10.0.2.16/24 gw4 10.0.2.2
```

Connection 'ip_fixe' (fb3a11d9-4e03-4032-b26e-09d1195d2bcd) successfully added.

Constatez sa présence :

```
[root@centos7 ~]# nmcli c show
```

NAME	UUID	TYPE	DEVICE
ip_fixe	fb3a11d9-4e03-4032-b26e-09d1195d2bcd	802-3-ethernet	--
Wired connection 1	45b701c1-0a21-4d76-a795-2f2bcba86955	802-3-ethernet	enp0s3

Notez que la sortie n'indique pas que le profil **ip_fixe** soit associé au périphérique **enp0s3** car le profil **ip_fixe** n'est pas activé :

```
[root@centos7 ~]# nmcli d show
```

GENERAL.DEVICE:	enp0s3
GENERAL.TYPE:	ethernet
GENERAL.HWADDR:	08:00:27:03:97:DD
GENERAL.MTU:	1500
GENERAL.STATE:	100 (connected)
GENERAL.CONNECTION:	Wired connection 1
GENERAL.CON-PATH:	/org/freedesktop/NetworkManager/ActiveConnection/2
WIRED-PROPERTIES.CARRIER:	on
IP4.ADDRESS[1]:	10.0.2.15/24
IP4.GATEWAY:	10.0.2.2
IP4.DNS[1]:	8.8.8.8
IP6.ADDRESS[1]:	fe80::a00:27ff:fe03:97dd/64
IP6.GATEWAY:	
GENERAL.DEVICE:	lo
GENERAL.TYPE:	loopback
GENERAL.HWADDR:	00:00:00:00:00:00
GENERAL.MTU:	65536
GENERAL.STATE:	10 (unmanaged)
GENERAL.CONNECTION:	--
GENERAL.CON-PATH:	--
IP4.ADDRESS[1]:	127.0.0.1/8

```
IP4.GATEWAY:
IP6.ADDRESS[1]:          ::1/128
IP6.GATEWAY:
```

Pour activer le profil `ip_fixe`, utilisez la commande suivante :

```
[root@centos7 ~]# nmcli connection up ip_fixe
```

Le profil `ip_fixe` est maintenant activé tandis que le profil `enp0s3` a été désactivé :

```
[root@centos7 ~]# nmcli c show
NAME                UUID                                TYPE          DEVICE
ip_fixe             fb3a11d9-4e03-4032-b26e-09d1195d2bcd 802-3-ethernet enp0s3
Wired connection 1  45b701c1-0a21-4d76-a795-2f2bcba86955 802-3-ethernet --
[root@centos7 ~]# nmcli d show
GENERAL.DEVICE:      enp0s3
GENERAL.TYPE:        ethernet
GENERAL.HWADDR:      08:00:27:03:97:DD
GENERAL.MTU:          1500
GENERAL.STATE:        100 (connected)
GENERAL.CONNECTION:   ip_fixe
GENERAL.CON-PATH:     /org/freedesktop/NetworkManager/ActiveConnection/3
WIRED-PROPERTIES.CARRIER: on
IP4.ADDRESS[1]:      10.0.2.16/24
IP4.GATEWAY:          10.0.2.2
IP6.ADDRESS[1]:      fe80::a00:27ff:fe03:97dd/64
IP6.GATEWAY:

GENERAL.DEVICE:      lo
GENERAL.TYPE:        loopback
GENERAL.HWADDR:      00:00:00:00:00:00
GENERAL.MTU:          65536
GENERAL.STATE:        10 (unmanaged)
GENERAL.CONNECTION:   --
```

```
GENERAL.CON-PATH:      --
IP4.ADDRESS[1]:        127.0.0.1/8
IP4.GATEWAY:
IP6.ADDRESS[1]:        ::1/128
IP6.GATEWAY:
```

Pour consulter les paramètres d'un profil, utilisez la commande suivante :

```
[root@centos7 ~]# nmcli -p connection show "Wired connection 1"
=====
                        Connection profile details (Wired connection 1)
=====
connection.id:          Wired connection 1
connection.uuid:        45b701c1-0a21-4d76-a795-2f2bcba86955
connection.interface-name: --
connection.type:        802-3-ethernet
connection.autoconnect: yes
connection.autoconnect-priority: 0
connection.timestamp:   1470647387
connection.read-only:   no
connection.permissions:
connection.zone:        --
connection.master:      --
connection.slave-type:  --
connection.autoconnect-slaves: -1 (default)
connection.secondaries:
connection.gateway-ping-timeout: 0
connection.metered:     unknown
-----
802-3-ethernet.port:    --
802-3-ethernet.speed:   0
802-3-ethernet.duplex:  --
802-3-ethernet.auto-negotiate: yes
802-3-ethernet.mac-address: 08:00:27:03:97:DD
```

```
802-3-ethernet.cloned-mac-address:  --
802-3-ethernet.mac-address-blacklist:
802-3-ethernet.mtu: auto
802-3-ethernet.s390-subchannels:
802-3-ethernet.s390-nettype:  --
802-3-ethernet.s390-options:
802-3-ethernet.wake-on-lan: 1 (default)
802-3-ethernet.wake-on-lan-password:  --
```

```
-----
ipv4.method: auto
ipv4.dns:
ipv4.dns-search:
ipv4.addresses:
ipv4.gateway:  --
ipv4.routes:
ipv4.route-metric: -1
ipv4.ignore-auto-routes: no
ipv4.ignore-auto-dns: no
ipv4.dhcp-client-id:  --
ipv4.dhcp-send-hostname: yes
ipv4.dhcp-hostname:  --
ipv4.never-default: no
ipv4.may-fail: yes
```

```
-----
ipv6.method: auto
ipv6.dns:
ipv6.dns-search:
ipv6.addresses:
ipv6.gateway:  --
ipv6.routes:
ipv6.route-metric: -1
ipv6.ignore-auto-routes: no
ipv6.ignore-auto-dns: no
ipv6.never-default: no
```

```
ipv6.may-fail:          yes
ipv6.ip6-privacy:       -1 (unknown)
ipv6.dhcp-send-hostname: yes
ipv6.dhcp-hostname:     --
```

```
-----
[root@centos7 ~]# nmcli -p connection show ip_fixe
```

```
=====
                        Connection profile details (ip_fixe)
=====
```

```
connection.id:          ip_fixe
connection.uuid:        fb3a11d9-4e03-4032-b26e-09d1195d2bcd
connection.interface-name: enp0s3
connection.type:        802-3-ethernet
connection.autoconnect: yes
connection.autoconnect-priority: 0
connection.timestamp:   1470647577
connection.read-only:   no
connection.permissions:
connection.zone:        --
connection.master:      --
connection.slave-type:   --
connection.autoconnect-slaves: -1 (default)
connection.secondaries:
connection.gateway-ping-timeout: 0
connection.metered:     unknown
```

```
-----
802-3-ethernet.port:    --
802-3-ethernet.speed:   0
802-3-ethernet.duplex:  --
802-3-ethernet.auto-negotiate: yes
802-3-ethernet.mac-address: --
802-3-ethernet.cloned-mac-address: --
802-3-ethernet.mac-address-blacklist:
802-3-ethernet.mtu:     auto
```

```
802-3-ethernet.s390-subchannels:
802-3-ethernet.s390-nettype:      --
802-3-ethernet.s390-options:
802-3-ethernet.wake-on-lan:      1 (default)
802-3-ethernet.wake-on-lan-password:  --
-----
ipv4.method:                      manual
ipv4.dns:
ipv4.dns-search:
ipv4.addresses:                  10.0.2.16/24
ipv4.gateway:                   10.0.2.2
ipv4.routes:
ipv4.route-metric:              -1
ipv4.ignore-auto-routes:        no
ipv4.ignore-auto-dns:           no
ipv4.dhcp-client-id:            --
ipv4.dhcp-send-hostname:         yes
ipv4.dhcp-hostname:             --
ipv4.never-default:             no
ipv4.may-fail:                  yes
-----
ipv6.method:                     auto
ipv6.dns:
ipv6.dns-search:
ipv6.addresses:
ipv6.gateway:                   --
ipv6.routes:
ipv6.route-metric:              -1
ipv6.ignore-auto-routes:        no
ipv6.ignore-auto-dns:           no
ipv6.never-default:             no
ipv6.may-fail:                  yes
ipv6.ip6-privacy:               -1 (unknown)
ipv6.dhcp-send-hostname:         yes
```

```
ipv6.dhcp-hostname: --
-----
=====
    Activate connection details (fb3a11d9-4e03-4032-b26e-09d1195d2bcd)
=====
GENERAL.NAME:          ip_fixe
GENERAL.UUID:          fb3a11d9-4e03-4032-b26e-09d1195d2bcd
GENERAL.DEVICES:       enp0s3
GENERAL.STATE:         activated
GENERAL.DEFAULT:       yes
GENERAL.DEFAULT6:      no
GENERAL.VPN:           no
GENERAL.ZONE:          --
GENERAL.DBUS-PATH:     /org/freedesktop/NetworkManager/ActiveConnection/3
GENERAL.CON-PATH:      /org/freedesktop/NetworkManager/Settings/1
GENERAL.SPEC-OBJECT:   /
GENERAL.MASTER-PATH:   --
-----
IP4.ADDRESS[1]:        10.0.2.16/24
IP4.GATEWAY:           10.0.2.2
-----
IP6.ADDRESS[1]:        fe80::a00:27ff:fe03:97dd/64
IP6.GATEWAY:
-----
```

Pour consulter la liste profils associés à un périphérique, utilisez la commande suivante :

```
[root@centos7 ~]# nmcli -f CONNECTIONS device show enp0s3
CONNECTIONS.AVAILABLE-CONNECTION-PATHS: /org/freedesktop/NetworkManager/Settings/{0,1}
CONNECTIONS.AVAILABLE-CONNECTIONS[1]:   45b701c1-0a21-4d76-a795-2f2bcba86955 | Wired connection 1
CONNECTIONS.AVAILABLE-CONNECTIONS[2]:   fb3a11d9-4e03-4032-b26e-09d1195d2bcd | ip_fixe
```

Les fichiers de configuration pour le périphérique **enp0s3** se trouvent dans le répertoire **/etc/sysconfig/network-scripts/** :

```
[root@centos7 ~]# ls -l /etc/sysconfig/network-scripts/ | grep ifcfg
-rw-r--r--. 1 root root  296 Aug  8 11:08 ifcfg-ip_fixe
-rw-r--r--. 1 root root  254 Sep 16  2015 ifcfg-lo
```

L'étude du fichier **/etc/sysconfig/network-scripts/ifcfg-ip_fixe** démontre l'absence de directives concernant les DNS :

```
[root@centos7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixe
TYPE=Ethernet
BOOTPROTO=none
IPADDR=10.0.2.16
PREFIX=24
GATEWAY=10.0.2.2
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=ip_fixe
UUID=fb3a11d9-4e03-4032-b26e-09d1195d2bcd
DEVICE=enp0s3
ONBOOT=yes
```

La résolution des noms est donc inactive :

```
[root@centos7 ~]# ping www.free.fr
ping: unknown host www.free.fr
```

Modifiez donc la configuration du profil **ip_fixe** :

```
[root@centos7 ~]# nmcli connection mod ip_fixe ipv4.dns 8.8.8.8
```

L'étude du fichier **/etc/sysconfig/network-scripts/ifcfg-ip_fixe** démontre que la directive concernant le serveur DNS a été ajoutée :

```
[root@centos7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixe
TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=ip_fixe
UUID=fb3a11d9-4e03-4032-b26e-09d1195d2bcd
DEVICE=enp0s3
ONBOOT=yes
IPADDR=10.0.2.16
PREFIX=24
GATEWAY=10.0.2.2
DNS1=8.8.8.8
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
```

Afin que la modification du serveur DNS soit prise en compte, re-démarrez le service NetworkManager :

```
[root@centos7 ~]# systemctl restart NetworkManager.service
[root@centos7 ~]# systemctl status NetworkManager.service
● NetworkManager.service - Network Manager
   Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2016-08-08 11:16:53 CEST; 7s ago
     Main PID: 8394 (NetworkManager)
       CGroup: /system.slice/NetworkManager.service
               └─8394 /usr/sbin/NetworkManager --no-daemon

Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> (enp0s3): device state change: prepare ->
```

```
config (reason 'none') [40 50 0]
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> (enp0s3): device state change: config -> ip-
config (reason 'none') [50 70 0]
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> (enp0s3): device state change: ip-config ->
ip-check (reason 'none') [70 80 0]
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> (enp0s3): device state change: ip-check ->
secondaries (reason 'none') [80 90 0]
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> (enp0s3): device state change: secondaries ->
activated (reason 'none') [90 100 0]
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> NetworkManager state is now CONNECTED_LOCAL
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> NetworkManager state is now CONNECTED_GLOBAL
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> Policy set 'ip_fixe' (enp0s3) as default for
IPv4 routing and DNS.
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> (enp0s3): Activation: successful, device
activated.
Aug 08 11:16:53 centos7.fenestros.loc NetworkManager[8394]: <info> wpa_supplicant running
```

Vérifiez que le fichier **/etc/resolv.conf** ait été modifié par NetworkManager :

```
[root@centos7 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search fenestros.loc
nameserver 8.8.8.8
```

Dernièrement vérifiez la resolution des noms :

```
[root@centos7 ~]# ping www.free.fr
PING www.free.fr (212.27.48.10) 56(84) bytes of data.
64 bytes from www.free.fr (212.27.48.10): icmp_seq=1 ttl=63 time=10.4 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=2 ttl=63 time=9.44 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=3 ttl=63 time=12.1 ms
^C
--- www.free.fr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
```

```
rtt min/avg/max/mdev = 9.448/10.680/12.171/1.126 ms
```



Important : Notez qu'il existe un front-end graphique en mode texte, **nmtui**, pour configurer NetworkManager.

Ajouter une Deuxième Adresse IP à un Profil

Pour ajouter une deuxième adresse IP à un profil sous RHEL/CentOS 7, il convient d'utiliser la commande suivante :

```
[root@centos7 ~]# nmcli connection mod ip_fixe +ipv4.addresses 192.168.1.2/24
```

Redémarrez la machine virtuelle puis en tant que root saisissez la commande suivante :

```
[root@centos7 ~]# nmcli connection show ip_fixe
connection.id:                ip_fixe
connection.uuid:              fb3a11d9-4e03-4032-b26e-09d1195d2bcd
connection.interface-name:    enp0s3
connection.type:              802-3-ethernet
connection.autoconnect:       yes
connection.autoconnect-priority: 0
connection.timestamp:         1470555543
connection.read-only:         no
connection.permissions:
connection.zone:              --
connection.master:            --
connection.slave-type:        --
connection.autoconnect-slaves: -1 (default)
connection.secondaries:
connection.gateway-ping-timeout: 0
connection.metered:           unknown
802-3-ethernet.port:          --
```

```
802-3-ethernet.speed: 0
802-3-ethernet.duplex: --
802-3-ethernet.auto-negotiate: yes
802-3-ethernet.mac-address: --
802-3-ethernet.cloned-mac-address: --
802-3-ethernet.mac-address-blacklist:
802-3-ethernet.mtu: auto
802-3-ethernet.s390-subchannels:
802-3-ethernet.s390-nettype: --
802-3-ethernet.s390-options:
802-3-ethernet.wake-on-lan: 1 (default)
802-3-ethernet.wake-on-lan-password: --
ipv4.method: manual
ipv4.dns: 8.8.8.8
ipv4.dns-search:
ipv4.addresses: 10.0.2.16/24, 192.168.1.2/24
ipv4.gateway: 10.0.2.2
ipv4.routes:
ipv4.route-metric: -1
ipv4.ignore-auto-routes: no
ipv4.ignore-auto-dns: no
ipv4.dhcp-client-id: --
ipv4.dhcp-send-hostname: yes
ipv4.dhcp-hostname: --
ipv4.never-default: no
ipv4.may-fail: yes
ipv6.method: auto
ipv6.dns:
ipv6.dns-search:
ipv6.addresses:
ipv6.gateway: --
ipv6.routes:
ipv6.route-metric: -1
ipv6.ignore-auto-routes: no
```

```
ipv6.ignore-auto-dns:      no
ipv6.never-default:        no
ipv6.may-fail:             yes
ipv6.ip6-privacy:          -1 (unknown)
ipv6.dhcp-send-hostname:   yes
ipv6.dhcp-hostname:        --
GENERAL.NAME:              ip_fixe
GENERAL.UUID:              fb3a11d9-4e03-4032-b26e-09d1195d2bcd
GENERAL.DEVICES:           enp0s3
GENERAL.STATE:             activated
GENERAL.DEFAULT:           yes
GENERAL.DEFAULT6:          no
GENERAL.VPN:               no
GENERAL.ZONE:              --
GENERAL.DBUS-PATH:         /org/freedesktop/NetworkManager/ActiveConnection/0
GENERAL.CON-PATH:          /org/freedesktop/NetworkManager/Settings/0
GENERAL.SPEC-OBJECT:       /
GENERAL.MASTER-PATH:       --
IP4.ADDRESS[1]:            10.0.2.16/24
IP4.ADDRESS[2]:            192.168.1.2/24
IP4.GATEWAY:               10.0.2.2
IP4.DNS[1]:                8.8.8.8
IP6.ADDRESS[1]:            fe80::a00:27ff:fe03:97dd/64
IP6.GATEWAY:
```



Important : Notez l'ajout de la ligne **IP4.ADDRESS[2]:**.

Consultez maintenant le contenu du fichier **/etc/sysconfig/network-scripts/ifcfg-ip_fixe** :

```
[root@centos7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixe
TYPE=Ethernet
```

```
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=ip_fixe
UUID=fb3a11d9-4e03-4032-b26e-09d1195d2bcd
DEVICE=enp0s3
ONBOOT=yes
DNS1=8.8.8.8
IPADDR=10.0.2.16
PREFIX=24
IPADDR1=192.168.1.2
PREFIX1=24
GATEWAY=10.0.2.2
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
```



Important : Notez l'ajout de la ligne **IPADDR1=192.168.1.2**.

La Commande hostname

La procédure de la modification du hostname est simplifiée et sa prise en compte est immédiate :

```
[root@centos7 ~]# nmcli general hostname centos.fenestros.loc
[root@centos7 ~]# cat /etc/hostname
centos.fenestros.loc
[root@centos7 ~]# hostname
```

```
centos.fenestros.loc
[root@centos7 ~]# nmcli general hostname centos7.fenestros.loc
[root@centos7 ~]# cat /etc/hostname
centos7.fenestros.loc
[root@centos7 ~]# hostname
centos7.fenestros.loc
```

La Commande ip

Sous RHEL/CentOS 7 la commande **ip** est préférée par rapport à la commande ifconfig :

```
[root@centos7 ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:03:97:dd brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.16/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet 192.168.1.2/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe03:97dd/64 scope link
        valid_lft forever preferred_lft forever
[root@centos7 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
```

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:03:97:dd brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.16/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet 192.168.1.2/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe03:97dd/64 scope link
        valid_lft forever preferred_lft forever
```

Options de la Commande ip

Les options de cette commande sont :

```
[root@centos7 ~]# ip --help
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | addr | addrlabel | route | rule | neigh | ntable |
                  tunnel | tuntap | maddr | mroute | mrule | monitor | xfrm |
                  netns | l2tp | tcp_metrics | token }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                   -f[amily] { inet | inet6 | ipx | dnet | bridge | link } |
                   -4 | -6 | -I | -D | -B | -0 |
                   -l[oops] { maximum-addr-flush-attempts } |
                   -o[neline] | -t[imestamp] | -b[atch] [filename] |
                   -rc[vbuf] [size]}
```

Activer/Désactiver une Interface Manuellement

Deux commandes existent pour désactiver et activer manuellement une interface réseau :

```
[root@centos7 ~]# nmcli device disconnect enp0s3
```

```
[root@centos7 ~]# nmcli device connect enp0s3
```

Routeage Statique

La commande ip

Sous RHEL/CentOS 7, pour supprimer la route vers le réseau 192.168.1.0 il convient d'utiliser la commande `ip` et non pas la commande `route` :

```
[root@centos7 ~]# ip route
default via 10.0.2.2 dev enp0s3 proto static metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.16 metric 100
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.2 metric 100
```

```
[root@centos7 ~]# ip route del 192.168.1.0/24 via 0.0.0.0
```

```
[root@centos7 ~]# ip route
default via 10.0.2.2 dev enp0s3 proto static metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.16 metric 100
```

Pour ajouter la route vers le réseau 192.168.1.0 :

```
[root@centos7 ~]# ip route add 192.168.1.0/24 via 10.0.2.2
```

```
[root@centos7 ~]# ip route
default via 10.0.2.2 dev enp0s3 proto static metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.16 metric 100
192.168.1.0/24 via 10.0.2.2 dev enp0s3
```



La commande utilisée pour ajouter une passerelle par défaut prend la forme suivante **`ip route add default via adresse ip`**.

Activer/désactiver le routage sur le serveur

Pour activer le routage sur le serveur, il convient d'activer la retransmission des paquets:

```
[root@centos7 ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@centos7 ~]# cat /proc/sys/net/ipv4/ip_forward
1
```

Pour désactiver le routage sur le serveur, il convient de désactiver la retransmission des paquets:

```
[root@centos7 ~]# echo 0 > /proc/sys/net/ipv4/ip_forward
[root@centos7 ~]# cat /proc/sys/net/ipv4/ip_forward
0
```

Diagnostic du Réseau

ping

Pour tester l'accessibilité d'une machine, vous devez utiliser la commande **ping** :

```
[root@centos7 ~]# ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=63 time=0.602 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=63 time=0.375 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=63 time=0.512 ms
64 bytes from 10.0.2.2: icmp_seq=4 ttl=63 time=0.547 ms
^C
--- 10.0.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
rtt min/avg/max/mdev = 0.375/0.509/0.602/0.083 ms
```

Options de la commande ping

Les options de cette commande sont :

```
[root@centos7 ~]# ping --help
ping: invalid option -- '-'
Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
          [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
          [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
          [-w deadline] [-W timeout] [hop1 ...] destination
```

netstat -i

Pour visualiser les statistiques réseaux, vous disposez de la commande **netstat** :

```
[root@centos7 ~]# netstat -i
Kernel Interface table
```

Iface	MTU	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
enp0s3	1500	101676	0	0 0		72270	0	0	0	BMRU
lo	65536	1606599	0	0 0		1606599	0	0	0	LRU

Options de la commande netstat

Les options de cette commande sont :

```
[root@centos7 ~]# netstat --help
usage: netstat [-vWeenNcCF] [<Af>] -r          netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -I[<Iface>] | [-veenNac] -i | [-cnNe] -M | -s [-6tuw] } [delay]
```

```
-r, --route          display routing table
-I, --interfaces=<Iface> display interface table for <Iface>
-i, --interfaces     display interface table
-g, --groups         display multicast group memberships
-s, --statistics     display networking statistics (like SNMP)
-M, --masquerade     display masqueraded connections

-v, --verbose        be verbose
-W, --wide           don't truncate IP addresses
-n, --numeric        don't resolve names
--numeric-hosts      don't resolve host names
--numeric-ports      don't resolve port names
--numeric-users      don't resolve user names
-N, --symbolic       resolve hardware names
-e, --extend         display other/more information
-p, --programs       display PID/Program name for sockets
-o, --timers         display timers
-c, --continuous     continuous listing

-l, --listening      display listening server sockets
-a, --all            display all sockets (default: connected)
-F, --fib            display Forwarding Information Base (default)
-C, --cache          display routing cache instead of FIB
-Z, --context        display SELinux security context for sockets
```

```
<Socket>={-t|--tcp} {-u|--udp} {-U|--udplite} {-w|--raw} {-x|--unix}
          --ax25 --ipx --netrom
```

```
<AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
```

```
List of possible address families (which support routing):
```

```
inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
```

La commande traceroute

La commande ping est à la base de la commande **traceroute**. Cette commande sert à découvrir la route empruntée pour accéder à un site donné :

```
[root@centos7 ~]# traceroute www.i2tch.eu
traceroute to www.i2tch.eu (217.160.122.33), 30 hops max, 60 byte packets
 1 gateway (10.0.2.2) 0.245 ms 0.098 ms 0.196 ms
 2 192.168.0.1 (192.168.0.1) 0.334 ms 0.312 ms 0.391 ms
 3 * * *
 4 195-132-10-137.rev.numericable.fr (195.132.10.137) 13.868 ms 13.799 ms 19.753 ms
 5 ip-190.net-80-236-8.asnieres.rev.numericable.fr (80.236.8.190) 20.041 ms 19.949 ms 19.859 ms
 6 ip-185.net-80-236-8.asnieres.rev.numericable.fr (80.236.8.185) 19.811 ms 15.239 ms 22.338 ms
 7 172.19.132.146 (172.19.132.146) 27.180 ms 27.044 ms 26.839 ms
 8 oneandone.franceix.net (37.49.236.42) 65.178 ms 64.946 ms 64.618 ms
 9 ae-8-0.bb-a.bap.rhr.de.oneandone.net (212.227.120.42) 30.706 ms 30.599 ms 30.493 ms
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
...
```

Options de la commande traceroute

Les options de cette commande sont :

```
[root@centos7 ~]# traceroute --help
Usage:
```

```
tracert [ -4dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [ -q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]
```

Options:

-4	Use IPv4
-6	Use IPv6
-d --debug	Enable socket level debugging
-F --dont-fragment	Do not fragment packets
-f first_ttl --first=first_ttl	Start from the first_ttl hop (instead from 1)
-g gate,... --gateway=gate,...	Route packets through the specified gateway (maximum 8 for IPv4 and 127 for IPv6)
-I --icmp	Use ICMP ECHO for tracerouting
-T --tcp	Use TCP SYN for tracerouting (default port is 80)
-i device --interface=device	Specify a network interface to operate with
-m max_ttl --max-hops=max_ttl	Set the max number of hops (max TTL to be reached). Default is 30
-N squeries --sim-queries=squeries	Set the number of probes to be tried simultaneously (default is 16)
-n	Do not resolve IP addresses to their domain names
-p port --port=port	Set the destination port to use. It is either initial udp port value for "default" method (incremented by each probe, default is 33434), or initial seq for "icmp" (incremented as well, default from 1), or some constant destination port for other methods (with default of 80 for "tcp", 53 for "udp", etc.)
-t tos --tos=tos	Set the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets
-l flow_label --flowlabel=flow_label	

```
Use specified flow_label for IPv6 packets
-w waittime --wait=waittime
    Set the number of seconds to wait for response to
    a probe (default is 5.0). Non-integer (float
    point) values allowed too
-q nqueries --queries=nqueries
    Set the number of probes per each hop. Default is
    3
-r
    Bypass the normal routing and send directly to a
    host on an attached network
-s src_addr --source=src_addr
    Use source src_addr for outgoing packets
-z sendwait --sendwait=sendwait
    Minimal time interval between probes (default 0).
    If the value is more than 10, then it specifies a
    number in milliseconds, else it is a number of
    seconds (float point values allowed too)
-e --extensions
    Show ICMP extensions (if present), including MPLS
-A --as-path-lookups
    Perform AS path lookups in routing registries and
    print results directly after the corresponding
    addresses
-M name --module=name
    Use specified module (either builtin or external)
    for traceroute operations. Most methods have
    their shortcuts (`-I' means `-M icmp' etc.)
-O OPTS,... --options=OPTS,...
    Use module-specific option OPTS for the
    traceroute module. Several OPTS allowed,
    separated by comma. If OPTS is "help", print info
    about available options
--sport=num
    Use source port num for outgoing packets. Implies
    `-N 1'
--fwmark=num
    Set firewall mark for outgoing packets
-U --udp
    Use UDP to particular port for tracerouting
    (instead of increasing the port per each probe),
```

```
-UL          default port is 53
             Use UDPLITE for tracerouting (default dest port
             is 53)
-D  --dccp    Use DCCP Request for tracerouting (default port
             is 33434)
-P prot  --protocol=prot  Use raw packet of protocol prot for tracerouting
--mtu      Discover MTU along the path being traced. Implies
             '-F -N 1'
--back      Guess the number of hops in the backward path and
             print if it differs
-V  --version  Print version info and exit
--help      Read this help and exit
```

Arguments:

```
+      host      The host to traceroute to
      packetlen  The full packet length (default is the length of an IP
                  header plus 40). Can be ignored or increased to a minimal
                  allowed value
```

Connexions à Distance

Telnet



La commande **telnet** n'est pas installée par défaut sous CentOS 7. Installez-le à l'aide de la commande **yum install telnet** en tant que root.

La commande **telnet** est utilisée pour établir une connexion à distance avec un serveur telnet :

```
# telnet numero_ip
```



Le service telnet revient à une redirection des canaux standards d'entrée et de sortie. Notez que la connexion n'est **pas** sécurisée. Pour fermer la connexion, il faut saisir la commande **exit**. La commande telnet n'offre pas de services de transfert de fichiers. Pour cela, il convient d'utiliser la commande **ftp**.

Options de la commande telnet

Les options de cette commande sont :

```
[root@centos7 ~]# telnet --help
telnet: invalid option -- '-'
Usage: telnet [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
        [-n tracefile] [-b hostalias ] [-r]
        [host-name [port]]
```

wget

La commande **wget** est utilisée pour récupérer un fichier via http, https ou ftp :

```
[root@centos7 ~]# wget https://www.dropbox.com/s/li5tyou8msfuwb/fichier_test?dl=0
--2017-06-22 16:53:39-- https://www.dropbox.com/s/li5tyou8msfuwb/fichier_test?dl=0
Resolving www.dropbox.com (www.dropbox.com)... 162.125.65.1
Connecting to www.dropbox.com (www.dropbox.com)|162.125.65.1|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location:
https://dl.dropboxusercontent.com/content_link/enf8fglFyPxthmTsBfruPFaa0D7pStW4llpPQbU6SjeYhsRDwtN76xpVXuHrLIz/f
ile [following]
--2017-06-22 16:53:40--
https://dl.dropboxusercontent.com/content_link/enf8fglFyPxthmTsBfruPFaa0D7pStW4llpPQbU6SjeYhsRDwtN76xpVXuHrLIz/f
```

```
ile
Resolving dl.dropboxusercontent.com (dl.dropboxusercontent.com)... 162.125.65.6
Connecting to dl.dropboxusercontent.com (dl.dropboxusercontent.com)|162.125.65.6|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17 [text/plain]
Saving to: 'fichier_test?dl=0'

100%[=====>] 17          --.-K/s
in 0s

2017-06-22 16:53:41 (480 KB/s) - 'fichier_test?dl=0' saved [17/17]
```

Options de la commande wget

Les options de cette commande sont :

```
[root@centos7 ~]# wget --help
GNU Wget 1.14, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V, --version          display the version of Wget and exit.
  -h, --help            print this help.
  -b, --background      go to background after startup.
  -e, --execute=COMMAND execute a `.wgetrc'-style command.

Logging and input file:
  -o, --output-file=FILE log messages to FILE.
  -a, --append-output=FILE append messages to FILE.
  -d, --debug          print lots of debugging information.
  -q, --quiet          quiet (no output).
```

-v, --verbose	be verbose (this is the default).
-nv, --no-verbose	turn off verboseness, without being quiet.
--report-speed=TYPE	Output bandwidth as TYPE. TYPE can be bits.
-i, --input-file=FILE	download URLs found in local or external FILE.
-F, --force-html	treat input file as HTML.
-B, --base=URL	resolves HTML input-file links (-i -F) relative to URL.
--config=FILE	Specify config file to use.

Download:

-t, --tries=NUMBER	set number of retries to NUMBER (0 unlimits).
--retry-connrefused	retry even if connection is refused.
-O, --output-document=FILE	write documents to FILE.
-nc, --no-clobber	skip downloads that would download to existing files (overwriting them).
-c, --continue	resume getting a partially-downloaded file.
--progress=TYPE	select progress gauge type.
-N, --timestamping	don't re-retrieve files unless newer than local.
--no-use-server-timestamps	don't set the local file's timestamp by the one on the server.
-S, --server-response	print server response.
--spider	don't download anything.
-T, --timeout=SECONDS	set all timeout values to SECONDS.
--dns-timeout=SECS	set the DNS lookup timeout to SECS.
--connect-timeout=SECS	set the connect timeout to SECS.
--read-timeout=SECS	set the read timeout to SECS.
-w, --wait=SECONDS	wait SECONDS between retrievals.
--waitretry=SECONDS	wait 1..SECONDS between retries of a retrieval.
--random-wait	wait from 0.5*WAIT...1.5*WAIT secs between retrievals.
--no-proxy	explicitly turn off proxy.
-Q, --quota=NUMBER	set retrieval quota to NUMBER.
--bind-address=ADDRESS	bind to ADDRESS (hostname or IP) on local host.
--limit-rate=RATE	limit download rate to RATE.

--no-dns-cache	disable caching DNS lookups.
--restrict-file-names=OS	restrict chars in file names to ones OS allows.
--ignore-case	ignore case when matching files/directories.
-4, --inet4-only	connect only to IPv4 addresses.
-6, --inet6-only	connect only to IPv6 addresses.
--prefer-family=FAMILY	connect first to addresses of specified family, one of IPv6, IPv4, or none.
--user=USER	set both ftp and http user to USER.
--password=PASS	set both ftp and http password to PASS.
--ask-password	prompt for passwords.
--no-iri	turn off IRI support.
--local-encoding=ENC	use ENC as the local encoding for IRIs.
--remote-encoding=ENC	use ENC as the default remote encoding.
--unlink	remove file before clobber.

Directories:

-nd, --no-directories	don't create directories.
-x, --force-directories	force creation of directories.
-nH, --no-host-directories	don't create host directories.
--protocol-directories	use protocol name in directories.
-P, --directory-prefix=PREFIX	save files to PREFIX/...
--cut-dirs=NUMBER	ignore NUMBER remote directory components.

HTTP options:

--http-user=USER	set http user to USER.
--http-password=PASS	set http password to PASS.
--no-cache	disallow server-cached data.
--default-page=NAME	Change the default page name (normally this is 'index.html').
-E, --adjust-extension	save HTML/CSS documents with proper extensions.
--ignore-length	ignore 'Content-Length' header field.
--header=STRING	insert STRING among the headers.
--max-redirect	maximum redirections allowed per page.
--proxy-user=USER	set USER as proxy username.

--proxy-password=PASS	set PASS as proxy password.
--referer=URL	include 'Referer: URL' header in HTTP request.
--save-headers	save the HTTP headers to file.
-U, --user-agent=AGENT	identify as AGENT instead of Wget/VERSION.
--no-http-keep-alive	disable HTTP keep-alive (persistent connections).
--no-cookies	don't use cookies.
--load-cookies=FILE	load cookies from FILE before session.
--save-cookies=FILE	save cookies to FILE after session.
--keep-session-cookies	load and save session (non-permanent) cookies.
--post-data=STRING	use the POST method; send STRING as the data.
--post-file=FILE	use the POST method; send contents of FILE.
--content-disposition	honor the Content-Disposition header when choosing local file names (EXPERIMENTAL).
--content-on-error	output the received content on server errors.
--auth-no-challenge	send Basic HTTP authentication information without first waiting for the server's challenge.

HTTPS (SSL/TLS) options:

--secure-protocol=PR	choose secure protocol, one of auto, SSLv2, SSLv3, and TLSv1.
--no-check-certificate	don't validate the server's certificate.
--certificate=FILE	client certificate file.
--certificate-type=TYPE	client certificate type, PEM or DER.
--private-key=FILE	private key file.
--private-key-type=TYPE	private key type, PEM or DER.
--ca-certificate=FILE	file with the bundle of CA's.
--ca-directory=DIR	directory where hash list of CA's is stored.
--random-file=FILE	file with random data for seeding the SSL PRNG.
--egd-file=FILE	file naming the EGD socket with random data.

FTP options:

--ftp-user=USER	set ftp user to USER.
--ftp-password=PASS	set ftp password to PASS.

```
--no-remove-listing    don't remove '.listing' files.
--no-glob              turn off FTP file name globbing.
--no-passive-ftp       disable the "passive" transfer mode.
--preserve-permissions preserve remote file permissions.
--retr-symlinks        when recursing, get linked-to files (not dir).
```

WARC options:

```
--warc-file=FILENAME    save request/response data to a .warc.gz file.
--warc-header=STRING    insert STRING into the warcinfo record.
--warc-max-size=NUMBER  set maximum size of WARC files to NUMBER.
--warc-cdx              write CDX index files.
--warc-dedup=FILENAME   do not store records listed in this CDX file.
--no-warc-compression   do not compress WARC files with GZIP.
--no-warc-digests       do not calculate SHA1 digests.
--no-warc-keep-log      do not store the log file in a WARC record.
--warc-tempdir=DIRECTORY location for temporary files created by the
                        WARC writer.
```

Recursive download:

```
-r,  --recursive        specify recursive download.
-l,  --level=NUMBER     maximum recursion depth (inf or 0 for infinite).
      --delete-after    delete files locally after downloading them.
-k,  --convert-links    make links in downloaded HTML or CSS point to
                        local files.
--backups=N             before writing file X, rotate up to N backup files.
-K,  --backup-converted before converting file X, back up as X.orig.
-m,  --mirror           shortcut for -N -r -l inf --no-remove-listing.
-p,  --page-requisites  get all images, etc. needed to display HTML page.
      --strict-comments turn on strict (SGML) handling of HTML comments.
```

Recursive accept/reject:

```
-A,  --accept=LIST      comma-separated list of accepted extensions.
-R,  --reject=LIST      comma-separated list of rejected extensions.
      --accept-regex=REGEX regex matching accepted URLs.
```

--reject-regex=REGEX	regex matching rejected URLs.
--regex-type=TYPE	regex type (posix pcre).
-D, --domains=LIST	comma-separated list of accepted domains.
--exclude-domains=LIST	comma-separated list of rejected domains.
--follow-ftp	follow FTP links from HTML documents.
--follow-tags=LIST	comma-separated list of followed HTML tags.
--ignore-tags=LIST	comma-separated list of ignored HTML tags.
-H, --span-hosts	go to foreign hosts when recursive.
-L, --relative	follow relative links only.
-I, --include-directories=LIST	list of allowed directories.
--trust-server-names	use the name specified by the redirection url last component.
-X, --exclude-directories=LIST	list of excluded directories.
-np, --no-parent	don't ascend to the parent directory.

Mail bug reports and suggestions to <bug-wget@gnu.org>.

ftp



La commande **ftp** n'est pas installée par défaut sous CentOS 7. Installez-le à l'aide de la commande **yum install ftp** en tant que root.

La commande **ftp** est utilisée pour le transfert de fichiers:

```
[root@centos7 ~]# ftp ftp2.fenestros.com
Connected to ftp2.fenestros.com (213.186.33.14).
220 anonymous.ftp.ovh.net NcFTPd Server (licensed copy) ready.
Name (ftp2.fenestros.com:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230 Logged in anonymously.
Remote system type is UNIX.
```

```
Using binary mode to transfer files.  
ftp>
```

Une fois connecté, il convient d'utiliser la commande **help** pour afficher la liste des commandes disponibles :

```
ftp> help  
Commands may be abbreviated.  Commands are:  
  
!      debug      mdir      sendport  site  
$      dir        mget      put       size  
account disconnect  mkdir     pwd       status  
append  exit        mls       quit      struct  
ascii   form        mode      quote     system  
bell    get         modtime   recv      sunique  
binary  glob        mput      reget     tenex  
bye     hash        newer     rstatus   tick  
case    help        nmap      rhelp     trace  
cd      idle        nlist     rename    type  
cdup    image       ntrans    reset     user  
chmod   lcd         open      restart   umask  
close   ls          prompt    rmdir     verbose  
cr      macdef      passive   runique   ?  
delete  mdelete     proxy     send  
ftp>
```

Le caractère **!** permet d'exécuter une commande sur la machine cliente

```
ftp> !pwd  
/root
```

Pour transférer un fichier vers le serveur, il convient d'utiliser la commande **put** :

```
ftp> put nom_fichier_local nom_fichier_distant
```

Vous pouvez également transférer plusieurs fichiers à la fois grâce à la commande **mput**. Dans ce cas précis, il convient de saisir la commande suivante:

```
ftp> mput nom*.*
```

Pour transférer un fichier du serveur, il convient d'utiliser la commande **get** :

```
ftp> get nom_fichier
```

Vous pouvez également transférer plusieurs fichiers à la fois grâce à la commande **mget** (voir la commande **mput** ci-dessus).

Pour supprimer un fichier sur le serveur, il convient d'utiliser la commande **del** :

```
ftp> del nom_fichier
```

Pour fermer la session, il convient d'utiliser la commande **quit** :

```
ftp> quit  
[root@centos7 ~]#
```

SSH

Introduction

La commande  **ssh** est le successeur et la remplaçante de la commande  **rlogin**. Il permet d'établir des connexions sécurisées avec une machine distante. SSH comporte cinq acteurs :

- Le **serveur SSH**
 - le démon sshd, qui s'occupe des authentifications et autorisations des clients,
- Le **client SSH**
 - ssh ou scp, qui assure la connexion et le dialogue avec le serveur,
- La **session** qui représente la connexion courante et qui commence juste après l'authentification réussie,

- Les **clefs**
 - **Couple de clef utilisateur asymétriques** et persistantes qui assurent l'identité d'un utilisateur et qui sont stockés sur disque dur,
 - **Clef hôte asymétrique et persistante** garantissant l'identité du serveur et qui est conservé sur disque dur
 - **Clef serveur asymétrique et temporaire** utilisée par le protocole SSH1 qui sert au chiffrement de la clé de session,
 - **Clef de session symétrique qui est générée aléatoirement** et qui permet le chiffrement de la communication entre le client et le serveur. Elle est détruite en fin de session. SSH-1 utilise une seule clef tandis que SSH-2 utilise une clef par direction de la communication,
- La **base de données des hôtes connus** qui stocke les clés des connexions précédentes.

SSH fonctionne de la manière suivante pour la mise en place d'un canal sécurisé:

- Le client contacte le serveur sur son port 22,
- Les client et le serveur échangent leur version de SSH. En cas de non-compatibilité de versions, l'un des deux met fin au processus,
- Le serveur SSH s'identifie auprès du client en lui fournissant :
 - Sa clé hôte,
 - Sa clé serveur,
 - Une séquence aléatoire de huit octets à inclure dans les futures réponses du client,
 - Une liste de méthodes de chiffrement, compression et authentification,
- Le client et le serveur produisent un identifiant identique, un haché MD5 long de 128 bits contenant la clé hôte, la clé serveur et la séquence aléatoire,
- Le client génère sa clé de session symétrique et la chiffre deux fois de suite, une fois avec la clé hôte du serveur et la deuxième fois avec la clé serveur. Le client envoie cette clé au serveur accompagnée de la séquence aléatoire et un choix d'algorithmes supportés,
- Le serveur déchiffre la clé de session,
- Le client et le serveur mettent en place le canal sécurisé.

SSH-1

SSH-1 utilise une paire de clefs de type RSA1. Il assure l'intégrité des données par une  **Contrôle de Redondance Cyclique (CRC)** et est un bloc dit **monolithique**.

Afin de s'identifier, le client essaie chacune des six méthodes suivantes :

- **Kerberos,**
- **Rhosts,**
- **RhostsRSA,**

- Par **clef asymétrique**,
- **TIS**,
- Par **mot de passe**.

SSH-2

SSH-2 utilise **DSA** ou **RSA**. Il assure l'intégrité des données par l'algorithme **HMAC**. SSH-2 est organisé en trois **couches** :

- **SSH-TRANS** – Transport Layer Protocol,
- **SSH-AUTH** – Authentication Protocol,
- **SSH-CONN** – Connection Protocol.

SSH-2 diffère de SSH-1 essentiellement dans la phase authentification.

Trois méthodes d'authentification :

- Par **clef asymétrique**,
 - Identique à SSH-1 sauf avec l'algorithme DSA,
- **RhostsRSA**,
- Par **mot de passe**.

Options de la commande

Les options de cette commande sont :

```
[root@centos6 ~]# ssh --help
usage: ssh [-1246AaCfGkKMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
          [-D [bind_address:]port] [-e escape_char] [-F configfile]
          [-i identity_file] [-L [bind_address:]port:host:hostport]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-R [bind_address:]port:host:hostport] [-S ctl_path]
          [-w local_tun[:remote_tun]] [user@]hostname [command]
```

L'authentification par mot de passe

L'utilisateur fournit un mot de passe au client ssh. Le client ssh le transmet de façon sécurisée au serveur ssh puis le serveur vérifie le mot de passe et l'accepte ou non.

Avantage:

- Aucune configuration de clef asymétrique n'est nécessaire.

Inconvénients:

- L'utilisateur doit fournir à chaque connexion un identifiant et un mot de passe,
- Moins sécurisé qu'un système par clef asymétrique.

L'authentification par clef asymétrique

- Le **client** envoie au serveur une requête d'authentification par clé asymétrique qui contient le module de la clé à utiliser,
- Le **serveur** recherche une correspondance pour ce module dans le fichier des clés autorisés `~/.ssh/authorized_keys`,
 - Dans le cas où une correspondance n'est pas trouvée, le serveur met fin à la communication,
 - Dans le cas contraire le serveur génère une chaîne aléatoire de 256 bits appelée un **challenge** et la chiffre avec la **clé publique du client**,
- Le **client** reçoit le challenge et le déchiffre avec la partie privée de sa clé. Il combine le challenge avec l'identifiant de session et chiffre le résultat. Ensuite il envoie le résultat chiffré au serveur.
- Le **serveur** génère le même haché et le compare avec celui reçu du client. Si les deux hachés sont identiques, l'authentification est réussie.

Installation

Pour installer/mettre à jour le serveur **sshd**, utilisez **yum** :

```
[root@centos7 ~]# yum install openssh-server
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
```

```
* base: centos.mirror.fr.planethoster.net
* extras: ftp.ciril.fr
* updates: centos.mirrors.ovh.net
Package openssh-server-6.6.1p1-25.el7_2.x86_64 already installed and latest version
Nothing to do
```



Important - Pour les stations de travail, installez le client : **openssh-clients**.

Options de la commande

Les options de la commande sont :

SYNOPSIS

```
sshd [-46DdeiqtT] [-b bits] [-C connection_spec] [-f config_file] [-g login_grace_time] [-h host_key_file]
[-k key_gen_time] [-o option] [-p port] [-u len]
```

Configuration



Important - La configuration doit s'effectuer dans la fenêtre de la VM sous VirtualBox. Les connexions en ssh doivent de faire à partir d'un terminal ou à partir de l'application putty.

Serveur

La configuration du serveur s'effectue dans le fichier **/etc/ssh/sshd_config** :

```
[root@centos7 ~]# cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.93 2014/01/10 05:59:19 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# The default requires explicit activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Lifetime and size of ephemeral version 1 server key
```

```
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
```

```
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnablek5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
```

```
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in Red Hat Enterprise Linux and may cause several
# problems.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
UsePrivilegeSeparation sandbox      # Default for new installations.
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
```

```
# no default banner path
#Banner none

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#   X11Forwarding no
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand cvs server
```

Pour ôter les lignes de commentaires dans ce fichier, utilisez la commande suivante :

```
[root@centos7 ~]# cd /tmp ; grep -E -v '^(#|$)' /etc/ssh/sshd_config > sshd_config
[root@centos7 tmp]# cat sshd_config
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
AuthorizedKeysFile .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
X11Forwarding yes
```

```
UsePrivilegeSeparation sandbox      # Default for new installations.
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem sftp /usr/libexec/openssh/sftp-server
```

Pour sécuriser le serveur ssh, ajoutez ou modifiez les directives suivantes :

```
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
StrictModes yes
X11Forwarding no
```

Votre fichier ressemblera à celui-ci :

```
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
```

```
StrictModes yes
X11Forwarding no
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
AuthorizedKeysFile .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
UsePrivilegeSeparation sandbox      # Default for new installations.
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem sftp /usr/libexec/openssh/sftp-server
```



A Faire - Renommez le fichier **/etc/ssh/sshd_config** en **/etc/ssh/sshd_config.old** puis copiez le fichier **/tmp/sshd_config** vers **/etc/ssh/**. Redémarrez ensuite le service sshd. N'oubliez pas de mettre l'utilisateur **trainee** dans le groupe **adm** !

Pour générer les clefs sur le serveur saisissez la commande suivante en tant que **root**:

Lors de la génération des clefs, la passphrase doit être **vide**.

```
[root@centos7 ~]# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa): /etc/ssh/ssh_host_dsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

```
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.  
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.  
The key fingerprint is:  
d5:54:d3:30:1c:f5:da:f8:21:15:1f:c8:6c:3b:b1:ff root@centos7.fenestros.loc  
The key's randomart image is:  
+--[ DSA 1024]-----+  
|           +oBB.|  
|          o *.o*|  
|         . o +.o|  
|        .  +.+ |  
|       S   .=. .|  
|          .o. |  
|           o |  
|           E |  
|           |  
+-----+-----+
```



Le chemin à indiquer pour le fichier est **/etc/ssh/ssh_host_dsa_key**. De la même façon, il est possible de générer les clefs au format **RSA**, **ECDSA** et **ED25519**.

Les clefs publiques générées possèdent l'extension **.pub**. Les clefs privées n'ont pas d'extension :

```
[root@centos7 ~]# ls /etc/ssh  
moduli      sshd_config      ssh_host_dsa_key.pub  ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub  
ssh_host_rsa_key.pub  
ssh_config  ssh_host_dsa_key  ssh_host_ecdsa_key    ssh_host_ed25519_key    ssh_host_rsa_key
```

Re-démarrez ensuite le service sshd :

```
[root@centos7 ~]# systemctl restart sshd.service
```

Saisissez maintenant les commandes suivantes en tant que **trainee** :



Lors de la génération des clefs, la passphrase doit être **vide**.

```
[trainee@centos7 ~]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_dsa):
Created directory '/home/trainee/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_dsa.
Your public key has been saved in /home/trainee/.ssh/id_dsa.pub.
The key fingerprint is:
97:92:85:d1:ae:97:f7:64:d2:54:45:89:eb:57:b1:66 trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ DSA 1024]-----+
|      ..  ..=|
|      0.  . 0.|
|      ...  ..0|
|      0.. ..E.|
|      S.o..oo .|
|      .oo 0.+ .|
|      .  . =.  |
|      .      |
|      .      |
+-----+
[trainee@centos7 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

```
Your identification has been saved in /home/trainee/.ssh/id_rsa.
Your public key has been saved in /home/trainee/.ssh/id_rsa.pub.
The key fingerprint is:
80:4c:5a:bf:d0:2f:d1:a1:34:7c:09:a1:9c:0d:ed:2d trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ RSA 2048]-----+
|      +0=0..      |
|     * Xo+o.      |
|    . B.Bo.       |
|     .E=.         |
|      o.S         |
|      .           |
|                 |
|                 |
|                 |
+-----+
[trainee@centos7 ~]$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ecdsa.
Your public key has been saved in /home/trainee/.ssh/id_ecdsa.pub.
The key fingerprint is:
41:5d:64:cf:d6:4a:ce:8e:a9:a8:4a:62:04:57:09:fc trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ECDSA 256]---+
| ..... .. 0+    |
| ... . .. 0 .   |
| . .. . = .     |
| o E . = .     |
| . S +         |
| . +          |
| o . o .      |
```

```
| . 0      . . |
|      . . . . . |
+-----+
[trainee@centos7 ~]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ed25519.
Your public key has been saved in /home/trainee/.ssh/id_ed25519.pub.
The key fingerprint is:
66:3a:83:d1:6d:79:46:48:88:7c:d9:65:59:bb:e6:d0 trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ED25519 256--+
|    . . +..00.    |
|    0 +..0.      |
|    . . . .      |
|    . . 0 . .    |
|    . . S + E    |
|    0 = 0 +      |
|    . +          |
|    0            |
+-----+
```



Les clés générées seront placées dans le répertoire **~/.ssh/**.

Utilisation

La commande ssh prend la forme suivante:

```
ssh -l nom_de_compte numero_ip (nom_de_machine)
```

En saisissant cette commande sur votre propre machine, vous obtiendrez un résultat similaire à celle-ci :

```
[trainee@centos7 ~]$ su -  
Mot de passe :  
Dernière connexion : lundi 9 mai 2016 à 22:47:48 CEST sur pts/0  
  
[root@centos7 ~]# ssh -l trainee localhost  
The authenticity of host 'localhost (127.0.0.1)' can't be established.  
ECDSA key fingerprint is 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.  
trainee@localhost's password: trainee  
Last login: Mon May 9 23:25:15 2016 from localhost.localdomain
```

Tunnels SSH

Le protocole SSH peut être utilisé pour sécuriser les protocoles tels telnet, pop3 etc.. En effet, on peut créer un *tunnel* SSH dans lequel passe les communications du protocole non-sécurisé.

La commande pour créer un tunnel ssh prend la forme suivante :

```
ssh -N -f compte@hôte -Lport-local:localhost:port_distant
```

Dans votre cas, vous allez créer un tunnel dans votre propre vm entre le port 15023 et le port 23 :

```
[root@centos7 ~]# ssh -N -f trainee@localhost -L15023:localhost:23  
trainee@localhost's password:
```

Installez maintenant le client et le serveur telnet :

```
[root@centos7 ~]# yum install telnet telnet-server
```

Telnet n'est ni démarré ni activé. Il convient donc de le démarrer et de l'activer :

```
[root@centos7 ~]# systemctl status telnet.socket
```

```
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:telnetd(8)
    Listen: [::]:23 (Stream)
   Accepted: 0; Connected: 0
```

```
[root@centos7 ~]# systemctl start telnet.socket
```

```
[root@centos7 ~]# systemctl status telnet.socket
```

```
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
   Active: active (listening) since Mon 2016-05-09 23:40:13 CEST; 3s ago
     Docs: man:telnetd(8)
    Listen: [::]:23 (Stream)
   Accepted: 0; Connected: 0
```

```
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Listening on Telnet Server Activation Socket.
```

```
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Starting Telnet Server Activation Socket.
```

```
[root@centos7 ~]# systemctl enable telnet.socket
```

```
Created symlink from /etc/systemd/system/sockets.target.wants/telnet.socket to
/usr/lib/systemd/system/telnet.socket.
```

```
[root@centos7 ~]# systemctl status telnet.socket
```

```
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; vendor preset: disabled)
   Active: active (listening) since Mon 2016-05-09 23:40:13 CEST; 36s ago
     Docs: man:telnetd(8)
    Listen: [::]:23 (Stream)
```

```
Accepted: 0; Connected: 0
```

```
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Listening on Telnet Server Activation Socket.  
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Starting Telnet Server Activation Socket.
```

Connectez-vous ensuite via telnet sur le port 15023, vous constaterez que votre connexion n'aboutit pas :

```
[root@centos7 ~]# telnet localhost 15023  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
  
Kernel 3.10.0-327.13.1.el7.x86_64 on an x86_64  
centos7 login: trainee  
Password:  
Last login: Mon May  9 23:26:32 from localhost.localdomain  
[trainee@centos7 ~]$
```



Notez bien que votre communication telnet passe par le tunnel SSH.

SCP

Introduction

La commande **scp** est le successeur et la remplaçante de la commande **rcp** de la famille des commandes **remote**. Il permet de faire des transferts sécurisés à partir d'une machine distante :

```
$ scp compte@numero_ip(nom_de_machine):/chemin_distant/fichier_distant /chemin_local/fichier_local
```

ou vers une machine distante :

```
$ scp /chemin_local/fichier_local compte@numero_ip(nom_de_machine):/chemin_distant/fichier_distant
```

Utilisation

Nous allons maintenant utiliser **scp** pour chercher un fichier sur le «serveur» :

Créez le fichier **/home/trainee/scp_test** :

```
[trainee@centos7 ~]$ pwd
/home/trainee
[trainee@centos7 ~]$ touch scp_test
```

Récupérez le fichier **scp_test** en utilisant scp :

```
[trainee@centos7 ~]$ touch /home/trainee/scp_test
[trainee@centos7 ~]$ scp trainee@127.0.0.1:/home/trainee/scp_test /tmp/scp_test
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
trainee@127.0.0.1's password: trainee
scp_test                                                    100%    0
0.0KB/s    00:00
[trainee@centos7 ~]$ ls /tmp/scp_test
/tmp/scp_test
```

Mise en place des clefs

Il convient maintenant de se connecter sur le «serveur» en utilisant ssh et vérifiez la présence du répertoire ~/.ssh :

En saisissant cette commande, vous obtiendrez une fenêtre similaire à celle-ci :

```
[trainee@centos7 ~]$ ssh -l trainee 127.0.0.1
trainee@127.0.0.1's password:
Last login: Mon May  9 23:42:46 2016 from localhost.localdomain
[trainee@centos7 ~]$ ls -la | grep .ssh
drwx-----.  2 trainee trainee 4096 May  9 23:25 .ssh
[trainee@centos7 ~]$ exit
logout
Connection to 127.0.0.1 closed.
```



Si le dossier distant `.ssh` n'existe pas dans le répertoire personnel de l'utilisateur connecté, il faut le créer avec des permissions de 700. Dans votre cas, puisque votre machine joue le rôle de serveur **et** du client, le dossier `/home/trainee/.ssh` existe **déjà**.

Ensuite, il convient de transférer le fichier local `.ssh/id_ecdsa.pub` du «client» vers le «serveur» en le renommant en **authorized_keys** :

```
[trainee@centos7 ~]$ scp .ssh/id_ecdsa.pub trainee@127.0.0.1:/home/trainee/.ssh/authorized_keys
trainee@127.0.0.1's password: trainee
id_ecdsa.pub                                100%  227
0.2KB/s   00:00
```

Connectez-vous via telnet et insérer les clefs publiques restantes dans le fichier `.ssh/authorized_keys` :

```
root@centos7 ~]# ssh -l trainee localhost
trainee@localhost's password: trainee
Last login: Tue May 10 01:39:33 2016 from localhost.localdomain
[trainee@centos7 ~]$ cat .ssh/id_rsa.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/id_dsa.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/id_ed25519.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/authorized_keys
ecdsa-sha2-nistp256
```

```
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG5Bt0MFLrUbxD//RLELvkkA06CQvXuJqKSjSB2dLUXgaPyEJXuwH00pxcdbr
g4qqb0f9sE75oMVowXxYgqhWDE= trainee@centos7.fenestros.loc
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQAC9K0uEH5+kyihhm99Na8UTA4Gi5Afi0VeJyS3UzH7ta73ewmv7JJzaXzar1NlHcpEMkCUs2yKxHy0/yAfjb
CSdow5vfwJiuJTes+HbpvsJqKp1+OR7tf+0MgjDcajoGi7DYuybIs9QrbWgh57QclbldHQXR0+xbeUTykxcRun7AvR5uWZe4zMooBAMVVEmS+l1rn
8Cui+D811jqQGSpu39PxkojTAwgbxlevT/Twy4sfeRR47UHc3AbrHb8SgyKqbx5/S9UxkbbkhJjckx0s58fnAwf9nX5rKE7RdCQisRvdLeLHozq3EO
omvc7kzejefBtUDWxBEjnSeAgIP3+0EQL trainee@centos7.fenestros.loc
ssh-dss
AAAAB3NzaC1kc3MAAACBAK9/4siucBnf/NAHBMjZWIX1coA/wYVBj fudVyKArip1fVUuYqf0Ri9vTorG8KJ2zzLRbW5z7V5ZDSn4f6P5Kv7K5xVPn
e9dYQHxImkZiLjpFseUW56BwCvcgTNZVLD0tYZzF+B0/Py4waJW+pnTDfZush6DYyAhVnEuxIPI4i+PAAAFQCeCZyDRo1o41lf19qWGJTg7W+ChQ
AAAIAKtQe9Qlkw4CA9kP+q4v3N07WR5TzWsvfZARjGXgrSqTo0BeQgMLwRJHeE0hdsgJ30cNbl6QXlB4G4J6dUoTiN/sY1dFbXzjzsT/MHledsllV
fXXRQxgvN2nsbsKEUnmqEBWzgw5s6K0kGX33+0Six0E3xv0rYxkMNLP/5VT4aQwAAAIEm0S94peBeo78yCKzCvSFnEL72dUCFFA6CGFGqgf fhK1v
P5H5pG5vQxzBn9NnIXURCACF7ZxtZaxohSoB1M0/s0DfrfNIvXRMGvsJpZ9B2psTMDl9qBffI fIARnwkWKG1gC/lWaovUpDByE1wl09ZCDnZp/16
ULJY0zvJ566Seg= trainee@centos7.fenestros.loc
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIENas3A3hmXFj1cb+l rn2NA t6g95Pla6qUFQHd1wg2y1 trainee@centos7.fenestros.loc
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG5Bt0MFLrUbxD//RLELvkkA06CQvXuJqKSjSB2dLUXgaPyEJXuwH00pxcdbr
g4qqb0f9sE75oMVowXxYgqhWDE= trainee@centos7.fenestros.loc
```

Lors de la connexion suivante au serveur, l'authentification utilise le couple de clefs asymétrique et aucun mot de passe n'est requis :

```
[trainee@centos7 ~]$ ssh -l trainee localhost
Last login: Tue May 10 01:50:39 2016 from localhost.localdomain
[trainee@centos7 ~]$ exit
déconnexion
Connection to localhost closed.
```



Le fichier **authorized_keys** doit avoir les permissions de 600.

Copyright © 2023 Hugh Norris.
