Version : **2022.01**

Dernière mise-à-jour : 2022/03/09 18:44

LCF603 - Gestion du Réseau

Contenu du Module

Présentation

RHEL/CentOS 8 utilise **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@centos8 ~]# systemctl status NetworkManager.service
● NetworkManager.service - Network Manager
   Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vendor pr>
   Active: active (running) since Thu 2021-07-22 05:05:29 EDT; 1 months 7 days ago
     Docs: man:NetworkManager(8)
 Main PID: 1002 (NetworkManager)
```

```
    Tasks: 3 (limit: 23535)
   Memory: 6.8M
   CGroup: /system.slice/NetworkManager.service
           └─1002 /usr/sbin/NetworkManager --no-daemon

Warning: Journal has been rotated since unit was started. Log output is incomplete or>
lines 1-11/11 (END)
[^q]
```

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@centos8 ~]# nmcli help
Usage: nmcli [OPTIONS] OBJECT { COMMAND | help }

OPTIONS
  -a, --ask                                ask for missing parameters
  -c, --colors auto|yes|no                 whether to use colors in output
  -e, --escape yes|no                      escape columns separators in values
  -f, --fields <field,...>|all|common      specify fields to output
  -g, --get-values <field,...>|all|common  shortcut for -m tabular -t -f
  -h, --help                               print this help
  -m, --mode tabular|multiline             output mode
  -o, --overview                           overview mode
  -p, --pretty                             pretty output
  -s, --show-secrets                       allow displaying passwords
  -t, --terse                              terse output
  -v, --version                            show program version
  -w, --wait <seconds>                     set timeout waiting for finishing operations
```

```
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
  m[onitor]       monitor NetworkManager changes
```

LAB #1 - Configuration du Réseau

1.1 - Connections et Profils

NetworkManager inclus 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@centos8 ~]# nmcli c show
NAME    UUID                                  TYPE      DEVICE
ens18   fc4a4d23-b15e-47a7-bcfa-b2e08f49553e  ethernet  ens18
virbr0  03f6c432-2a09-47e7-9693-208431a572ee  bridge    virbr0
```

Créez donc un profil IP fixe rattaché au périphérique **ens18** :

```
[root@centos8 ~]# nmcli connection add con-name ip_fixe ifname ens18 type ethernet ip4 10.0.2.46/24 gw4 10.0.2.1
Connection 'ip_fixe' (0f48c74d-5d16-4c37-8220-24644507b589) successfully added.
```

Constatez sa présence :

```
[root@centos8 ~]# nmcli c show
NAME     UUID                                  TYPE      DEVICE
ens18    fc4a4d23-b15e-47a7-bcfa-b2e08f49553e  ethernet  ens18
```

```
virbr0   03f6c432-2a09-47e7-9693-208431a572ee  bridge    virbr0
ip_fixe  0f48c74d-5d16-4c37-8220-24644507b589  ethernet  --
```

Notez que la sortie n'indique pas que le profil **ip_fixe** soit associé au periphérique **ens18** car le profil **ip_fixe** n'est pas activé :

```
[root@centos8 ~]# nmcli d show
GENERAL.DEVICE:                         ens18
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         4E:B1:31:BD:5D:B2
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     ens18
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         10.0.2.45/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
IP4.DNS[1]:                             8.8.8.8
IP6.ADDRESS[1]:                         fe80::86b6:8d39:cab2:d84d/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255

GENERAL.DEVICE:                         virbr0
GENERAL.TYPE:                           bridge
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected (externally))
GENERAL.CONNECTION:                     virbr0
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
IP4.ADDRESS[1]:                         192.168.122.1/24
IP4.GATEWAY:                            --
IP4.ROUTE[1]:                           dst = 192.168.122.0/24, nh = 0.0.0.0, mt = 0
```

```
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:                            --
IP6.ROUTE[1]:                           dst = ::1/128, nh = ::, mt = 256

GENERAL.DEVICE:                         virbr0-nic
GENERAL.TYPE:                           tun
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          10 (unmanaged)
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
lines 28-50/50 (END)
[q]
```

Pour activer le profil ip_fixe, utilisez la commande suivante :

```
[root@centos8 ~]# nmcli connection up ip_fixe
```

Notez que votre terminal est bloqué à cause du changement de l'adresse IP.

A faire - Revenez à l'accueil du cloud IT Training et re-connectez-vous à la VM en tant que

trainee en utilisant la connexion **CentOS8_SSH_10.0.2.46**.

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

```
[root@centos8 ~]# nmcli c show
NAME     UUID                                  TYPE      DEVICE
ip_fixe  0f48c74d-5d16-4c37-8220-24644507b589  ethernet  ens18
virbr0   03f6c432-2a09-47e7-9693-208431a572ee  bridge    virbr0
ens18    fc4a4d23-b15e-47a7-bcfa-b2e08f49553e  ethernet  --
[root@centos8 ~]# nmcli d show
GENERAL.DEVICE:                         ens18
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         4E:B1:31:BD:5D:B2
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     ip_fixe
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         10.0.2.46/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
IP6.ADDRESS[1]:                         fe80::5223:aee1:998e:9f27/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255

GENERAL.DEVICE:                         virbr0
GENERAL.TYPE:                           bridge
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected (externally))
GENERAL.CONNECTION:                     virbr0
```

```
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnect>
IP4.ADDRESS[1]:                         192.168.122.1/24
IP4.GATEWAY:                            --
IP4.ROUTE[1]:                           dst = 192.168.122.0/24, nh = 0.0.0.0, mt = 0
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:                            --
IP6.ROUTE[1]:                           dst = ::1/128, nh = ::, mt = 256

GENERAL.DEVICE:                         virbr0-nic
GENERAL.TYPE:                           tun
GENERAL.HWADDR:                         52:54:00:79:02:66
GENERAL.MTU:                            1500
GENERAL.STATE:                          10 (unmanaged)
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
lines 27-49/49 (END)
[q]
```

Pour consulter les paramètres du profil **ens18**, utilisez la commande suivante :

```
[root@centos8 ~]# nmcli -p connection show ens18
===============================================================================
                      Connection profile details (ens18)
```

```
===============================================================================
connection.id:                          ens18
connection.uuid:                        fc4a4d23-b15e-47a7-bcfa-b2e08f49553e
connection.stable-id:                   --
connection.type:                        802-3-ethernet
connection.interface-name:              ens18
connection.autoconnect:                 yes
connection.autoconnect-priority:        0
connection.autoconnect-retries:         -1 (default)
connection.multi-connect:               0 (default)
connection.auth-retries:                -1
connection.timestamp:                   1630224060
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
connection.lldp:                        default
connection.mdns:                        -1 (default)
connection.llmnr:                       -1 (default)
connection.wait-device-timeout:         -1
-------------------------------------------------------------------------------
802-3-ethernet.port:                    --
802-3-ethernet.speed:                   0
802-3-ethernet.duplex:                  --
802-3-ethernet.auto-negotiate:          no
802-3-ethernet.mac-address:             --
802-3-ethernet.cloned-mac-address:      --
802-3-ethernet.generate-mac-address-mask:--
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:             default
802-3-ethernet.wake-on-lan-password:    --
------------------------------------------------------------------------------
ipv4.method:                            manual
ipv4.dns:                               8.8.8.8
ipv4.dns-search:                        ittraining.loc
ipv4.dns-options:                       --
ipv4.dns-priority:                      0
ipv4.addresses:                         10.0.2.45/24
ipv4.gateway:                           10.0.2.1
ipv4.routes:                            --
ipv4.route-metric:                      -1
ipv4.route-table:                       0 (unspec)
ipv4.routing-rules:                     --
ipv4.ignore-auto-routes:                no
ipv4.ignore-auto-dns:                   no
ipv4.dhcp-client-id:                    --
ipv4.dhcp-iaid:                         --
ipv4.dhcp-timeout:                      0 (default)
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.dhcp-fqdn:                         --
ipv4.dhcp-hostname-flags:               0x0 (none)
ipv4.never-default:                     no
ipv4.may-fail:                          yes
ipv4.dad-timeout:                       -1 (default)
ipv4.dhcp-vendor-class-identifier:      --
ipv4.dhcp-reject-servers:               --
------------------------------------------------------------------------------
ipv6.method:                            auto
```

```
ipv6.dns:                               --
ipv6.dns-search:                        --
ipv6.dns-options:                       --
ipv6.dns-priority:                      0
ipv6.addresses:                         --
ipv6.gateway:                           --
ipv6.routes:                            --
ipv6.route-metric:                      -1
ipv6.route-table:                       0 (unspec)
ipv6.routing-rules:                     --
ipv6.ignore-auto-routes:                no
ipv6.ignore-auto-dns:                   no
ipv6.never-default:                     no
ipv6.may-fail:                          yes
ipv6.ip6-privacy:                       0 (disabled)
ipv6.addr-gen-mode:                     stable-privacy
ipv6.ra-timeout:                        0 (default)
ipv6.dhcp-duid:                         --
ipv6.dhcp-iaid:                         --
ipv6.dhcp-timeout:                      0 (default)
ipv6.dhcp-send-hostname:                yes
ipv6.dhcp-hostname:                     --
ipv6.dhcp-hostname-flags:               0x0 (none)
ipv6.token:                             --
------------------------------------------------------------------------------
proxy.method:                           none
proxy.browser-only:                     no
proxy.pac-url:                          --
proxy.pac-script:                       --
------------------------------------------------------------------------------
lines 56-100/100 (END)
[q]
```

De même, pour consulter les paramètres du profil **ip_fixe**, utilisez la commande suivante :

```
[root@centos8 ~]# nmcli -p connection show ip_fixe
===============================================================================
                    Connection profile details (ip_fixe)
===============================================================================
connection.id:                          ip_fixe
connection.uuid:                        0f48c74d-5d16-4c37-8220-24644507b589
connection.stable-id:                   --
connection.type:                        802-3-ethernet
connection.interface-name:              ens18
connection.autoconnect:                 yes
connection.autoconnect-priority:        0
connection.autoconnect-retries:         -1 (default)
connection.multi-connect:               0 (default)
connection.auth-retries:                -1
connection.timestamp:                   1630224329
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
connection.lldp:                        default
connection.mdns:                        -1 (default)
connection.llmnr:                       -1 (default)
connection.wait-device-timeout:         -1
-------------------------------------------------------------------------------
802-3-ethernet.port:                    --
802-3-ethernet.speed:                   0
802-3-ethernet.duplex:                  --
802-3-ethernet.auto-negotiate:          no
802-3-ethernet.mac-address:             --
```

```
802-3-ethernet.cloned-mac-address:      --
802-3-ethernet.generate-mac-address-mask:--
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:             default
802-3-ethernet.wake-on-lan-password:    --
------------------------------------------------------------------------------
ipv4.method:                            manual
ipv4.dns:                               --
ipv4.dns-search:                        --
ipv4.dns-options:                       --
ipv4.dns-priority:                      0
ipv4.addresses:                         10.0.2.46/24
ipv4.gateway:                           10.0.2.1
ipv4.routes:                            --
ipv4.route-metric:                      -1
ipv4.route-table:                       0 (unspec)
ipv4.routing-rules:                     --
ipv4.ignore-auto-routes:                no
ipv4.ignore-auto-dns:                   no
ipv4.dhcp-client-id:                    --
ipv4.dhcp-iaid:                         --
ipv4.dhcp-timeout:                      0 (default)
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.dhcp-fqdn:                         --
ipv4.dhcp-hostname-flags:               0x0 (none)
ipv4.never-default:                     no
ipv4.may-fail:                          yes
ipv4.dad-timeout:                       -1 (default)
ipv4.dhcp-vendor-class-identifier:      --
```

```
ipv4.dhcp-reject-servers:               --
---------------------------------------------------------------------------
ipv6.method:                            auto
ipv6.dns:                               --
ipv6.dns-search:                        --
ipv6.dns-options:                       --
ipv6.dns-priority:                      0
ipv6.addresses:                         --
ipv6.gateway:                           --
ipv6.routes:                            --
ipv6.route-metric:                      -1
ipv6.route-table:                       0 (unspec)
ipv6.routing-rules:                     --
ipv6.ignore-auto-routes:                no
ipv6.ignore-auto-dns:                   no
ipv6.never-default:                     no
ipv6.may-fail:                          yes
ipv6.ip6-privacy:                       -1 (unknown)
ipv6.addr-gen-mode:                     stable-privacy
ipv6.ra-timeout:                        0 (default)
ipv6.dhcp-duid:                         --
ipv6.dhcp-iaid:                         --
ipv6.dhcp-timeout:                      0 (default)
ipv6.dhcp-send-hostname:                yes
ipv6.dhcp-hostname:                     --
ipv6.dhcp-hostname-flags:               0x0 (none)
ipv6.token:                             --
---------------------------------------------------------------------------
proxy.method:                           none
proxy.browser-only:                     no
proxy.pac-url:                          --
proxy.pac-script:                       --
---------------------------------------------------------------------------
===========================================================================
```

```
      Activate connection details (0f48c74d-5d16-4c37-8220-24644507b589)
===============================================================================
GENERAL.NAME:                           ip_fixe
GENERAL.UUID:                           0f48c74d-5d16-4c37-8220-24644507b589
GENERAL.DEVICES:                        ens18
GENERAL.IP-IFACE:                       ens18
GENERAL.STATE:                          activated
GENERAL.DEFAULT:                        yes
GENERAL.DEFAULT6:                       no
GENERAL.SPEC-OBJECT:                    --
GENERAL.VPN:                            no
GENERAL.DBUS-PATH:                      /org/freedesktop/NetworkManager/ActiveConnection/4
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/Settings/4
GENERAL.ZONE:                           --
GENERAL.MASTER-PATH:                    --
-------------------------------------------------------------------------------
IP4.ADDRESS[1]:                         10.0.2.46/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
-------------------------------------------------------------------------------
IP6.ADDRESS[1]:                         fe80::5223:aee1:998e:9f27/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255
-------------------------------------------------------------------------------
lines 83-127/127 (END)
[q]
```

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

```
[root@centos8 ~]# nmcli -f CONNECTIONS device show ens18
CONNECTIONS.AVAILABLE-CONNECTION-PATHS:
/org/freedesktop/NetworkManager/Settings/1,/org/freedesktop/NetworkManager/Settings/4
```

```
CONNECTIONS.AVAILABLE-CONNECTIONS[1]:   fc4a4d23-b15e-47a7-bcfa-b2e08f49553e | ens18
CONNECTIONS.AVAILABLE-CONNECTIONS[2]:   0f48c74d-5d16-4c37-8220-24644507b589 | ip_fixe
```

Les fichiers de configuration pour le periphérique **ens18** se trouvent dans le répertoire **/etc/sysconfig/network-scripts/** :

```
[root@centos8 ~]# ls -l /etc/sysconfig/network-scripts/ | grep ifcfg
-rw-r--r--. 1 root root 417 Jun 16 06:39 ifcfg-ens18
-rw-r--r--. 1 root root 326 Aug 29 03:58 ifcfg-ip_fixe
```

1.2 - Résolution des Noms

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

```
[root@centos8 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixe
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=10.0.2.46
PREFIX=24
GATEWAY=10.0.2.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ip_fixe
UUID=0f48c74d-5d16-4c37-8220-24644507b589
DEVICE=ens18
ONBOOT=yes
```

La résolution des noms est donc inactive :

```
[root@centos8 ~]# ping www.free.fr
ping: www.free.fr: Name or service not known
```

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

```
[root@centos8 ~]# 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@centos8 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixe
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=10.0.2.46
PREFIX=24
GATEWAY=10.0.2.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ip_fixe
UUID=0f48c74d-5d16-4c37-8220-24644507b589
DEVICE=ens18
ONBOOT=yes
DNS1=8.8.8.8
```

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

```
root@centos8 ~]# systemctl restart NetworkManager.service
[root@centos8 ~]# 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 2021-08-29 04:15:11 EDT; 8s ago
     Docs: man:NetworkManager(8)
 Main PID: 973390 (NetworkManager)
    Tasks: 4 (limit: 23535)
   Memory: 4.6M
   CGroup: /system.slice/NetworkManager.service
           └─973390 /usr/sbin/NetworkManager --no-daemon

Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2235] device (ens18): state
change: ip-check -> secondaries (reas>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2237] device (virbr0): state
change: secondaries -> activated (re>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2241] manager: NetworkManager
state is now CONNECTED_LOCAL
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.2251] policy: set 'ip_fixe'
(ens18) as default for IPv4 routing a>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3090] device (virbr0):
Activation: successful, device activated.
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3098] device (ens18): state
change: secondaries -> activated (rea>
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3102] manager: NetworkManager
state is now CONNECTED_SITE
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3111] device (ens18):
Activation: successful, device activated.
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3116] manager: NetworkManager
state is now CONNECTED_GLOBAL
Aug 29 04:15:12 centos8.ittraining.loc NetworkManager[973390]: <info>  [1630224912.3121] manager: startup
complete
lines 1-20/20 (END)
```

```
[q]
```

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

```
[root@centos8 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ittraining.loc
nameserver 8.8.8.8
```

Dernièrement vérifiez la resolution des noms :

```
[root@centos8 ~]# 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=47 time=29.3 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=2 ttl=47 time=29.4 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=3 ttl=47 time=29.4 ms
64 bytes from www.free.fr (212.27.48.10): icmp_seq=4 ttl=47 time=29.4 ms
^C
--- www.free.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 29.266/29.377/29.428/0.183 ms
```

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

1.3 - Ajouter une Deuxième Adresse IP à un Profil

Pour ajouter une deuxième adresse IP à un profil sous RHEL/CentOS 8, il convient d'utiliser la commande suivante :

```
[root@centos8 ~]# nmcli connection mod ip_fixe +ipv4.addresses 192.168.1.2/24
```

Rechargez la configuration du profil :

```
[root@centos8 ~]# nmcli con up ip_fixe
```

Saisissez ensuite la commande suivante :

```
[root@centos8 ~]# nmcli connection show ip_fixe
connection.id:                          ip_fixe
connection.uuid:                        0f48c74d-5d16-4c37-8220-24644507b589
connection.stable-id:                   --
connection.type:                        802-3-ethernet
connection.interface-name:              ens18
connection.autoconnect:                 yes
connection.autoconnect-priority:        0
connection.autoconnect-retries:         -1 (default)
connection.multi-connect:               0 (default)
connection.auth-retries:                -1
connection.timestamp:                   1630225792
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
connection.lldp:                        default
connection.mdns:                        -1 (default)
connection.llmnr:                       -1 (default)
connection.wait-device-timeout:         -1
802-3-ethernet.port:                    --
```

```
802-3-ethernet.speed:                   0
802-3-ethernet.duplex:                  --
802-3-ethernet.auto-negotiate:          no
802-3-ethernet.mac-address:             --
802-3-ethernet.cloned-mac-address:      --
802-3-ethernet.generate-mac-address-mask:--
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:             default
802-3-ethernet.wake-on-lan-password:    --
ipv4.method:                            manual
ipv4.dns:                               8.8.8.8
ipv4.dns-search:                        --
ipv4.dns-options:                       --
ipv4.dns-priority:                      0
ipv4.addresses:                         10.0.2.46/24, 192.168.1.2/24
ipv4.gateway:                           10.0.2.1
ipv4.routes:                            --
ipv4.route-metric:                      -1
ipv4.route-table:                       0 (unspec)
ipv4.routing-rules:                     --
ipv4.ignore-auto-routes:                no
ipv4.ignore-auto-dns:                   no
ipv4.dhcp-client-id:                    --
ipv4.dhcp-iaid:                         --
ipv4.dhcp-timeout:                      0 (default)
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.dhcp-fqdn:                         --
ipv4.dhcp-hostname-flags:               0x0 (none)
ipv4.never-default:                     no
```

```
ipv4.may-fail:                          yes
ipv4.dad-timeout:                       -1 (default)
ipv4.dhcp-vendor-class-identifier:      --
ipv4.dhcp-reject-servers:               --
ipv6.method:                            auto
ipv6.dns:                               --
ipv6.dns-search:                        --
ipv6.dns-options:                       --
ipv6.dns-priority:                      0
ipv6.addresses:                         --
ipv6.gateway:                           --
ipv6.routes:                            --
ipv6.route-metric:                      -1
ipv6.route-table:                       0 (unspec)
ipv6.routing-rules:                     --
ipv6.ignore-auto-routes:                no
ipv6.ignore-auto-dns:                   no
ipv6.never-default:                     no
ipv6.may-fail:                          yes
ipv6.ip6-privacy:                       -1 (unknown)
ipv6.addr-gen-mode:                     stable-privacy
ipv6.ra-timeout:                        0 (default)
ipv6.dhcp-duid:                         --
ipv6.dhcp-iaid:                         --
ipv6.dhcp-timeout:                      0 (default)
ipv6.dhcp-send-hostname:                yes
ipv6.dhcp-hostname:                     --
ipv6.dhcp-hostname-flags:               0x0 (none)
ipv6.token:                             --
proxy.method:                           none
proxy.browser-only:                     no
proxy.pac-url:                          --
proxy.pac-script:                       --
GENERAL.NAME:                           ip_fixe
```

```
GENERAL.UUID:                           0f48c74d-5d16-4c37-8220-24644507b589
GENERAL.DEVICES:                        ens18
GENERAL.IP-IFACE:                       ens18
GENERAL.STATE:                          activated
GENERAL.DEFAULT:                        yes
GENERAL.DEFAULT6:                       no
GENERAL.SPEC-OBJECT:                    --
GENERAL.VPN:                            no
GENERAL.DBUS-PATH:                      /org/freedesktop/NetworkManager/ActiveConnection/3
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/Settings/2
GENERAL.ZONE:                           --
GENERAL.MASTER-PATH:                    --
IP4.ADDRESS[1]:                         10.0.2.46/24
IP4.ADDRESS[2]:                         192.168.1.2/24
IP4.GATEWAY:                            10.0.2.1
IP4.ROUTE[1]:                           dst = 10.0.2.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[2]:                           dst = 192.168.1.0/24, nh = 0.0.0.0, mt = 100
IP4.ROUTE[3]:                           dst = 0.0.0.0/0, nh = 10.0.2.1, mt = 100
IP4.DNS[1]:                             8.8.8.8
IP6.ADDRESS[1]:                         fe80::5223:aee1:998e:9f27/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255
lines 72-116/116 (END)
[q]
```

Important : Notez l'ajout de l'adresse secondaire à la ligne **ipv4.addresses:** ainsi que l'ajout de la ligne **IP4.ADDRESS[2]:**.

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

```
[root@centos8 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ip_fixe
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=10.0.2.46
PREFIX=24
GATEWAY=10.0.2.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ip_fixe
UUID=0f48c74d-5d16-4c37-8220-24644507b589
DEVICE=ens18
ONBOOT=yes
DNS1=8.8.8.8
IPADDR1=192.168.1.2
PREFIX1=24
```

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

1.4 - La Commande hostname

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

```
[root@centos8 ~]# hostname
centos8.ittraining.loc

[root@centos8 ~]# nmcli general hostname centos.ittraining.loc

[root@centos8 ~]# cat /etc/hostname
centos.ittraining.loc

[root@centos8 ~]# hostname
centos.ittraining.loc

[root@centos8 ~]# nmcli general hostname centos8.ittraining.loc

[root@centos8 ~]# cat /etc/hostname
centos8.ittraining.loc

[root@centos8 ~]# hostname
centos8.ittraining.loc
```

1.5 - La Commande ip

Sous RHEL/CentOS 8 la commande **ip** est préférée par rapport à la commande ifconfig :

```
[root@centos8 ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 4e:b1:31:bd:5d:b2 brd ff:ff:ff:ff:ff:ff
```

```
    inet 10.0.2.46/24 brd 10.0.2.255 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet 192.168.1.2/24 brd 192.168.1.255 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::5223:aee1:998e:9f27/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:79:02:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:79:02:66 brd ff:ff:ff:ff:ff:ff
```

Options de la Commande ip

Les options de cette commande sont :

```
[root@centos8 ~]# ip --help
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
                   netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila |
                   vrf | sr | nexthop | mptcp }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -iec | -j[son] | -p[retty] |
                    -f[amily] { inet | inet6 | mpls | bridge | link } |
                    -4 | -6 | -I | -D | -M | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                    -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                    -c[olor]}
```

1.6 - Activer/Désactiver une Interface Manuellement

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

```
# nmcli device disconnect enp0s3
# nmcli device connect enp0s3
```

Important : Veuillez ne **PAS** exécuter ces deux commandes.

1.7 - Routage Statique

La commande ip

Sous RHEL/CentOS 8, 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@centos8 ~]# ip route
default via 10.0.2.1 dev ens18 proto static metric 100
10.0.2.0/24 dev ens18 proto kernel scope link src 10.0.2.46 metric 100
192.168.1.0/24 dev ens18 proto kernel scope link src 192.168.1.2 metric 100
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown

root@centos8 ~]# ip route del 192.168.1.0/24 via 0.0.0.0
[root@centos8 ~]# ip route
default via 10.0.2.1 dev ens18 proto static metric 100
10.0.2.0/24 dev ens18 proto kernel scope link src 10.0.2.46 metric 100
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
```

Pour ajouter la route vers le réseau 192.168.1.0 :

```
[root@centos8 ~]# ip route add 192.168.1.0/24 via 10.0.2.1
[root@centos8 ~]# ip route
default via 10.0.2.1 dev ens18 proto static metric 100
10.0.2.0/24 dev ens18 proto kernel scope link src 10.0.2.46 metric 100
192.168.1.0/24 via 10.0.2.1 dev ens18
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
```

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

Désactiver/Activer le routage sur le serveur

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

```
[root@centos8 ~]# cat /proc/sys/net/ipv4/ip_forward
1
[root@centos8 ~]# echo 0 > /proc/sys/net/ipv4/ip_forward
[root@centos8 ~]# cat /proc/sys/net/ipv4/ip_forward
0
```

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

```
[root@centos8 ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@centos8 ~]# cat /proc/sys/net/ipv4/ip_forward
1
```

LAB #2 - Diagnostique du Réseau

2.1 - ping

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

```
[root@centos8 ~]# ping -c4 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from 10.0.2.1: icmp_seq=2 ttl=64 time=0.325 ms
64 bytes from 10.0.2.1: icmp_seq=3 ttl=64 time=0.250 ms
64 bytes from 10.0.2.1: icmp_seq=4 ttl=64 time=0.123 ms

--- 10.0.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3083ms
rtt min/avg/max/mdev = 0.104/0.200/0.325/0.092 ms
```

Options de la commande ping

Les options de cette commande sont :

```
[root@centos8 ~]# ping --help
ping: invalid option -- '-'
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-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
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
             [-l preload] [-m mark] [-M pmtudisc_option]
             [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
             [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
```

```
             [-W timeout] destination
```

2.2 - netstat -i

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

```
[root@centos8 ~]# netstat -i
Kernel Interface table
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens18            1500   476056      0      0 0        363562      0      0      0 BMRU
lo              65536    10936      0      0 0         10936      0      0      0 LRU
virbr0           1500        0      0      0 0             0      0      0      0 BMU
```

Options de la commande netstat

Les options de cette commande sont :

```
[root@centos8 ~]# 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} {-S|--sctp} {-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)
```

2.3 - 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@centos8 ~]# traceroute www.ittraining.network
bash: traceroute: command not found...
Install package 'traceroute' to provide command 'traceroute'? [N/y] y
```

```
 * Waiting in queue...
The following packages have to be installed:
 traceroute-3:2.1.0-6.el8.x86_64        Traces the route taken by packets over an IPv4/IPv6 network
Proceed with changes? [N/y] y



 * Waiting in queue...
 * Waiting for authentication...
 * Waiting in queue...
 * Downloading packages...
 * Requesting data...
 * Testing changes...
 * Installing packages...
traceroute to www.ittraining.network (109.228.56.52), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.1)  0.132 ms  0.101 ms  0.078 ms
 2  79.137.68.252 (79.137.68.252)  0.542 ms  0.656 ms  0.809 ms
 3  10.50.24.61 (10.50.24.61)  0.238 ms  0.219 ms 10.50.24.60 (10.50.24.60)  0.239 ms
 4  10.50.0.16 (10.50.0.16)  0.172 ms 10.50.0.22 (10.50.0.22)  0.194 ms  0.173 ms
 5  10.73.248.192 (10.73.248.192)  0.766 ms 10.73.248.194 (10.73.248.194)  0.730 ms 10.73.248.192 (10.73.248.192)
0.757 ms
 6  waw-wa2-sbb1-nc5.pl.eu (91.121.131.150)  1.102 ms  1.396 ms  1.099 ms
 7  fra-fr5-sbb1-nc5.de.eu (213.251.128.113)  18.309 ms fra-fr5-sbb2-nc5.de.eu (54.36.50.116)  21.881 ms fra-fr5-
sbb1-nc5.de.eu (213.251.128.113)  16.764 ms
 8  10.200.0.6 (10.200.0.6)  20.922 ms 10.200.0.0 (10.200.0.0)  16.959 ms 10.200.0.4 (10.200.0.4)  21.143 ms
 9  decix.bb-a.fra3.fra.de.oneandone.net (80.81.192.123)  18.789 ms decix.bb-c.act.fra.de.oneandone.net
(80.81.193.123)  20.310 ms decix.bb-a.fra3.fra.de.oneandone.net (80.81.192.123)  18.693 ms
10  ae-14.bb-b.fr7.fra.de.oneandone.net (212.227.120.149)  22.222 ms  22.206 ms  22.257 ms
11  port-channel-3.gw-ngcs-1.dc1.con.glo.gb.oneandone.net (88.208.255.131)  39.660 ms  39.679 ms ae-19.bb-
b.thn.lon.gb.oneandone.net (212.227.120.33)  33.973 ms
12  109.228.63.209 (109.228.63.209)  37.363 ms port-channel-3.gw-ngcs-1.dc1.con.glo.gb.oneandone.net
(88.208.255.131)  39.534 ms 109.228.63.209 (109.228.63.209)  37.901 ms
13  * 109.228.63.209 (109.228.63.209)  38.014 ms  37.991 ms
14  * * *
15  * * *
```

```
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *^C
```

Options de la commande traceroute

Les options de cette commande sont :

```
[root@centos8 ~]# traceroute --help
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squeries ] [ -
p port ] [ -t tos ] [ -l flow_label ] [ -w MAX,HERE,NEAR ] [ -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 MAX,HERE,NEAR  --wait=MAX,HERE,NEAR
                              Wait for a probe no more than HERE (default 3)
                              times longer than a response from the same hop,
                              or no more than NEAR (default 10) times than some
                              next hop, or MAX (default 5.0) seconds (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),
                            default port is 53
-UL                         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
```

LAB #3 - Connexions à Distance

3.1 - Telnet

WRAP center round important> **Important** - Si la commande **telnet** n'est pas installée sous CentOS 8, installez-le à l'aide de la commande **dnf install telnet** en tant que root. </WRAP>

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

```
  # telnet numero_ip
```

Important - 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 command **ftp**.

Options de la commande telnet

Les options de cette commande sont :

```
[[root@centos8 ~]# telnet --help
telnet: invalid option -- '-'
Usage: telnet [-4] [-6] [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
        [-n tracefile] [-b hostalias ] [-r]
 [host-name [port]]
```

3.2 - wget

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

```
[root@centos8 ~]# wget https://www.dropbox.com/s/lqtl47jpj2qu5od/wget_file.txt
--2021-08-29 06:22:26--  https://www.dropbox.com/s/lqtl47jpj2qu5od/wget_file.txt
Resolving www.dropbox.com (www.dropbox.com)... 162.125.67.18, 2620:100:6023:18::a27d:4312
Connecting to www.dropbox.com (www.dropbox.com)|162.125.67.18|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: /s/raw/lqtl47jpj2qu5od/wget_file.txt [following]
--2021-08-29 06:22:27--  https://www.dropbox.com/s/raw/lqtl47jpj2qu5od/wget_file.txt
Reusing existing connection to www.dropbox.com:443.
HTTP request sent, awaiting response... 302 Found
Location:
https://uc8a5f475f4a5f849fd1055f560f.dl.dropboxusercontent.com/cd/0/inline/BVLLQHvou_Z6M6ahJQIL0h_F294OM7CU4q_am-
_dpLy8Ifk66MQQSSe66akMc1yzJ_gMMBw0rHAsccFgTriPPpRvY9gMEBBB9FP3gyf2eT1b7SeonjZZshyppFw9-
KxrWTJN_3bRB4Rx_t6DXaozZVnV/file# [following]
--2021-08-29 06:22:27--
https://uc8a5f475f4a5f849fd1055f560f.dl.dropboxusercontent.com/cd/0/inline/BVLLQHvou_Z6M6ahJQIL0h_F294OM7CU4q_am-
_dpLy8Ifk66MQQSSe66akMc1yzJ_gMMBw0rHAsccFgTriPPpRvY9gMEBBB9FP3gyf2eT1b7SeonjZZshyppFw9-
KxrWTJN_3bRB4Rx_t6DXaozZVnV/file
Resolving uc8a5f475f4a5f849fd1055f560f.dl.dropboxusercontent.com
(uc8a5f475f4a5f849fd1055f560f.dl.dropboxusercontent.com)... 162.125.67.15, 2620:100:6023:15::a27d:430f
Connecting to uc8a5f475f4a5f849fd1055f560f.dl.dropboxusercontent.com
(uc8a5f475f4a5f849fd1055f560f.dl.dropboxusercontent.com)|162.125.67.15|:443... connected.
```

```
HTTP request sent, awaiting response... 200 OK
Length: 46 [text/plain]
Saving to: ‘wget_file.txt’

wget_file.txt       100%[===================>]      46  --.-KB/s    in 0s

2021-08-29 06:22:27 (26.9 MB/s) - ‘wget_file.txt’ saved [46/46]

[root@centos8 ~]# cat wget_file.txt
This is a file retrieved by the wget command.
```

Options de la commande wget

Les options de cette commande sont :

```
[root@centos8 ~]# wget --help
GNU Wget 1.19.5, 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
       --input-metalink=FILE       download files covered in local Metalink 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
       --no-config                 do not read any config file
       --rejected-log=FILE         log reasons for URL rejection to FILE

Download:
  -t,  --tries=NUMBER              set number of retries to NUMBER (0 unlimits)
       --retry-connrefused         retry even if connection is refused
       --retry-on-http-error=ERRORS    comma-separated list of HTTP errors to retry
  -O,  --output-document=FILE      write documents to FILE
  -nc, --no-clobber                skip downloads that would download to
                                     existing files (overwriting them)
       --no-netrc                  don't try to obtain credentials from .netrc
  -c,  --continue                  resume getting a partially-downloaded file
       --start-pos=OFFSET          start downloading from zero-based position OFFSET
       --progress=TYPE             select progress gauge type
       --show-progress             display the progress bar in any verbosity mode
  -N,  --timestamping              don't re-retrieve files unless newer than
                                     local
       --no-if-modified-since      don't use conditional if-modified-since get
                                     requests in timestamping mode
       --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
       --use-askpass=COMMAND       specify credential handler for requesting
                                     username and password.  If no COMMAND is
                                     specified the WGET_ASKPASS or the SSH_ASKPASS
                                     environment variable is used.
       --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
       --keep-badhash              keep files with checksum mismatch (append .badhash)
       --metalink-index=NUMBER     Metalink application/metalink4+xml metaurl ordinal NUMBER
       --metalink-over-http        use Metalink metadata from HTTP response headers
       --preferred-location        preferred location for Metalink resources
       --xattr                     turn on storage of metadata in extended file attributes

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
       --compression=TYPE           choose compression, one of auto, gzip and none. (default: none)
       --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
       --method=HTTPMethod          use method "HTTPMethod" in the request
       --body-data=STRING           send STRING as data. --method MUST be set
       --body-file=FILE             send contents of FILE. --method MUST be set
       --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, TLSv1, TLSv1_1, TLSv1_2 and PFS
       --https-only                only follow secure HTTPS links
       --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 CAs
       --ca-directory=DIR          directory where hash list of CAs is stored
       --crl-file=FILE             file with bundle of CRLs
       --pinnedpubkey=FILE/HASHES  Public key (PEM/DER) file, or any number
                                   of base64 encoded sha256 hashes preceded by
                                   'sha256//' and separated by ';', to verify
                                   peer against

       --ciphers=STR           Set the priority string (GnuTLS) or cipher list string (OpenSSL) directly.
                                   Use with care. This option overrides --secure-protocol.
                                   The format and syntax of this string depend on the specific SSL/TLS engine.
HSTS options:
       --no-hsts                   disable HSTS
       --hsts-file                 path of HSTS database (will override default)

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)

FTPS options:
       --ftps-implicit                 use implicit FTPS (default port is 990)
       --ftps-resume-ssl               resume the SSL/TLS session started in the control connection when
                                         opening a data connection
       --ftps-clear-data-connection    cipher the control channel only; all the data will be in plaintext
       --ftps-fallback-to-ftp          fall back to FTP if FTPS is not supported in the target server
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
       --convert-file-only         convert the file part of the URLs only (usually known as the basename)
       --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)
  -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's last component
  -X,  --exclude-directories=LIST  list of excluded directories
  -np, --no-parent                 don't ascend to the parent directory

Email bug reports, questions, discussions to <bug-wget@gnu.org>
and/or open issues at https://savannah.gnu.org/bugs/?func=additem&group=wget.
```

3.3 - ftp

Important - Si la commande **ftp** n'est pas installée sous CentOS 8, installez-le à l'aide de la commande **dnf install ftp** en tant que root.

La commande **ftp** est utilisée pour le transfert de fichiers. 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 ~]#
```

3.4 - SSH

Présentation

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 er 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 chiiffrement 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 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 chiffrage, 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** – Authentification 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@centos8 ~]# ssh --help
unknown option -- -
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
```

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.

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 décrypte 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.

Configuration du Serveur

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

```
[root@centos8 ~]# cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj 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:/usr/local/sbin:/usr/sbin
```

```
# 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 ::

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# This system is following system-wide crypto policy. The changes to
# crypto properties (Ciphers, MACs, ...) will not have any effect here.
# They will be overridden by command-line options passed to the server
# on command line.
# Please, check manual pages for update-crypto-policies(8) and sshd_config(5).

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:
```

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

#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
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# 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 Fedora and may cause several
# problems.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
```

```
# It is recommended to use pam_motd in /etc/pam.d/sshd instead of PrintMotd,
# as it is more configurable and versatile than the built-in version.
PrintMotd no

#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#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@centos8 ~]# cd /tmp ; grep -E -v '^(#|$)'  /etc/ssh/sshd_config > sshd_config
[root@centos8 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
PermitRootLogin yes
AuthorizedKeysFile      .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
X11Forwarding yes
PrintMotd no
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 :

```
[root@centos8 tmp]# vi sshd_config
[root@centos8 tmp]# cat sshd_config
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
PermitRootLogin yes
AuthorizedKeysFile      .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
PrintMotd no
```

```
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
```

Renommez le fichier **/etc/ssh/sshd_config** en **/etc/ssh/sshd_config.old** :

```
[root@centos8 tmp]# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.old
```

Copiez le fichier **/tmp/sshd_config** vers **/etc/ssh/** :

```
[root@centos8 tmp]# cp /tmp/sshd_config /etc/ssh
cp: overwrite '/etc/ssh/sshd_config'? y
```

Redémarrez le service sshd :

```
[root@centos8 tmp]# systemctl restart sshd
[root@centos8 tmp]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-08-30 02:17:00 EDT; 11s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1042039 (sshd)
    Tasks: 1 (limit: 23535)
   Memory: 1.1M
   CGroup: /system.slice/sshd.service
           └─1042039 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-
ctr,aes256-cbc,aes128-gcm@openssh.com,a>

Aug 30 02:17:00 centos8.ittraining.loc systemd[1]: Starting OpenSSH server daemon...
Aug 30 02:17:00 centos8.ittraining.loc sshd[1042039]: Server listening on 0.0.0.0 port 22.
Aug 30 02:17:00 centos8.ittraining.loc sshd[1042039]: Server listening on :: port 22.
```

```
Aug 30 02:17:00 centos8.ittraining.loc systemd[1]: Started OpenSSH server daemon.
[q]
```

Mettez l'utilisateur **trainee** dans le groupe **adm** :

```
[root@centos8 tmp]# groups trainee
trainee : trainee
[root@centos8 tmp]# usermod -aG adm trainee
[root@centos8 tmp]# groups trainee
trainee : trainee adm
```

Pour générer les clefs du serveur, saisissez la commande suivante en tant que **root**. Notez que la passphrase doit être **vide**.

```
[root@centos8 tmp]# 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:
SHA256:dywC6jKyIMaTxsaEamz1kmthEmuG18HxmS22qRICOYk root@centos8.ittraining.loc
The key's randomart image is:
+---[DSA 1024]----+
|                 |
|    .            |
|.o . o.+         |
|E.  o.*..  .     |
|+ooo.o +S o o    |
|X==++ o  o o     |
|B/=+oo           |
|Ooo++            |
|. .o             |
```

```
+----[SHA256]-----+
```

De la même façon, il est possible de générer les clefs au format **RSA**, **ECDSA** et **ED25519** :

```
[root@centos8 tmp]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /etc/ssh/ssh_host_rsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
SHA256:8jXFK50NnoJCz9E7aPKpFYSYCstCPfRsdmlLBTNUnKg root@centos8.ittraining.loc
The key's randomart image is:
+---[RSA 3072]----+
|   .  .==o.      |
|  o oo o=+ .     |
|.. oo=+=o . +    |
|oo .+E++.+ = *   |
|o..   +.S B * .  |
|.      B + =     |
|        =        |
|       o         |
|      .          |
+----[SHA256]-----+
[root@centos8 tmp]# ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/root/.ssh/id_ecdsa): /etc/ssh/ssh_host_ecdsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_ecdsa_key.
Your public key has been saved in /etc/ssh/ssh_host_ecdsa_key.pub.
The key fingerprint is:
SHA256:AMqFUJKGqnUEPh/IYda0wnbW1kXK+lnprpHsOo4UMbI root@centos8.ittraining.loc
```

```
The key's randomart image is:
+---[ECDSA 256]---+
|++*=+    .o      |
|oX.=o+ o o       |
|o %.B + +        |
|...O.= o   .     |
|..E.o . S o      |
|.    . o =       |
|    .   * .      |
|   . ... o       |
|    ..ooo..      |
+----[SHA256]-----+
[root@centos8 tmp]# ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519): /etc/ssh/ssh_host_ed25519_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_ed25519_key.
Your public key has been saved in /etc/ssh/ssh_host_ed25519_key.pub.
The key fingerprint is:
SHA256:CtbcN9iXv00PfbHFGf2bEW7iRibOFwRctyqM5hmlhwE root@centos8.ittraining.loc
The key's randomart image is:
+--[ED25519 256]--+
|       E  .... . |
|        .  .. . o|
|         . . . +.|
|     o . oB ..o.=|
|    o o S*+=o* *+|
|   . . .o.*o*.+.B|
|      .  o o +o++|
|            o  =o|
|              . o|
+----[SHA256]-----+
```

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

```
[root@centos8 tmp]# ls /etc/ssh
moduli      ssh_config.d  sshd_config.old     ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub
ssh_host_rsa_key.pub
ssh_config  sshd_config   ssh_host_ecdsa_key  ssh_host_ed25519_key    ssh_host_rsa_key
```

Re-démarrez ensuite le service sshd :

```
[root@centos8 tmp]# systemctl restart sshd.service
[root@centos8 tmp]# systemctl status sshd.service
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-08-30 02:24:57 EDT; 9s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1042204 (sshd)
    Tasks: 1 (limit: 23535)
   Memory: 1.1M
   CGroup: /system.slice/sshd.service
           └─1042204 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-
ctr,aes256-cbc,aes128-gcm@openssh.com,a>

Aug 30 02:24:57 centos8.ittraining.loc systemd[1]: Starting OpenSSH server daemon...
Aug 30 02:24:57 centos8.ittraining.loc sshd[1042204]: Server listening on 0.0.0.0 port 22.
Aug 30 02:24:57 centos8.ittraining.loc sshd[1042204]: Server listening on :: port 22.
Aug 30 02:24:57 centos8.ittraining.loc systemd[1]: Started OpenSSH server daemon.
[q]
```

Configuration du Client

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

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

```
[root@centos8 tmp]# exit
logout
[trainee@centos8 ~]$ 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:
SHA256:Qd17X1iROjk5rLOQBbyVg1hNXkUdTeiFtEpn3rgPKc4 trainee@centos8.ittraining.loc
The key's randomart image is:
+---[DSA 1024]----+
|        =o+o.o+OB|
|       o +o=o oo=|
|        . +.+oB+ |
|         o o.&+o.|
|        S o o.*.o|
|         o o   o.|
|          . + +  |
|           + . o |
|            E   .|
+----[SHA256]-----+
[trainee@centos8 ~]$ 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:
SHA256:BgEjoWQrGCzdJfyZczVZYVoafiHsz9GK5PDWuywG/z0 trainee@centos8.ittraining.loc
The key's randomart image is:
+---[RSA 3072]----+
|o+o++oo  .oo*.   |
|=+o.oo . .=B .   |
|=.   ..o o+...   |
|.     =.o o.. .  |
|       oS= = o   |
|       .. = =    |
|         +   .   |
|          +...E  |
|         . o+... |
+----[SHA256]-----+
[trainee@centos8 ~]$ 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:
SHA256:mpBDgsCxP2DqRPkmGvXHpNnvm5B+Cl7MSiiZKfDjWLk trainee@centos8.ittraining.loc
The key's randomart image is:
+---[ECDSA 256]---+
|o..              |
|.oo              |
|.*o . .          |
|+.++ B           |
|+o =B + S        |
|=*oo.* =         |
|B.* o O .        |
```

```
|.= = = o..       |
|. E o oo+.       |
+----[SHA256]-----+
[trainee@centos8 ~]$ 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:
SHA256:JfFxG2mg9feAvFGxoxZ8uSsON3sXvtYQYYg5iVxzZS4 trainee@centos8.ittraining.loc
The key's randomart image is:
+--[ED25519 256]--+
|       ..o*=++=. |
|        o==O+Boo |
|        o ooE.O. |
|         o   O.= |
|        S   + ...|
|           .  .o |
|          . + o.o|
|           + +.oo|
|            o..o.|
+----[SHA256]-----+
```

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

```
[trainee@centos8 ~]$ ls .ssh
id_dsa  id_dsa.pub  id_ecdsa  id_ecdsa.pub  id_ed25519  id_ed25519.pub  id_rsa  id_rsa.pub
```

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@centos8 ~]# ssh -N -f trainee@localhost -L15023:localhost:23
\S
Kernel \r on an \m
trainee@localhost's password: trainee
```

Installez maintenant le serveur telnet :

```
[root@centos8 ~]# dnf install telnet-server
```

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

```
[root@centos8 ~]# 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@centos8 ~]# systemctl start telnet.socket

[root@centos8 ~]# 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 2021-08-30 02:44:01 EDT; 4s ago
     Docs: man:telnetd(8)
```

```
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0;
   CGroup: /system.slice/telnet.socket

Aug 30 02:44:01 centos8.ittraining.loc systemd[1]: Listening on Telnet Server Activation Socket.

[root@centos8 ~]# systemctl enable telnet.socket
Created symlink /etc/systemd/system/sockets.target.wants/telnet.socket → /usr/lib/systemd/system/telnet.socket.
```

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

```
[root@centos8 ~]# telnet localhost 15023
Trying ::1...
Connected to localhost.
Escape character is '^]'.

Kernel 4.18.0-305.7.1.el8.i2tch.x86_64 on an x86_64
centos8 login: trainee
Password:
Last login: Mon Aug 30 02:37:00 from ::1
[trainee@centos8 ~]$ whoami
trainee
[trainee@centos8 ~]$ pwd
/home/trainee
```

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

3.5 - SCP

Présentation

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@centos8 ~]$ touch scp-test
[trainee@centos8 ~]$ exit
logout
Connection closed by foreign host.
[root@centos8 ~]#
```

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

```
[root@centos8 ~]# scp trainee@127.0.0.1:/home/trainee/scp-test .
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:Q7T/CP0SLiMbMAIgVzTuEHegYS/spPE5zzQchCHD5Vw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
\S
Kernel \r on an \m
```

```
trainee@127.0.0.1's password: trainee
scp-test
100%    0     0.0KB/s   00:00

[root@centos8 ~]# ls -l
total 32
-rw-------. 1 root root 1358 Jun 16 06:40 anaconda-ks.cfg
drwxr-xr-x. 3 root root   21 Jun 16 06:39 home
-rw-r--r--. 1 root root 1749 Aug 24 11:20 I2TCH.asc
-rw-r--r--. 1 root root 1853 Jun 16 06:54 initial-setup-ks.cfg
-rw-r--r--. 1 root root   31 Aug 24 11:22 message.txt
-rw-r--r--. 1 root root  561 Aug 24 11:32 message.txt.asc
-rw-r--r--. 1 root root  367 Aug 24 11:30 message.txt.gpg
-rw-r--r--. 1 root root  329 Aug 24 11:23 message.txt.sig
-rw-r--r--. 1 root root    0 Aug 30 03:55 scp-test
-rw-r--r--. 1 root root   46 Aug 29 06:22 wget_file.txt
```

3.6 - Mise en Place des Clefs Asymétriques

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

```
[root@centos8 ~]# ssh -l trainee 127.0.0.1
\S
Kernel \r on an \m
trainee@127.0.0.1's password: trainee
Activate the web console with: systemctl enable --now cockpit.socket

[trainee@centos8 ~]$ ls -la | grep .ssh
drwx------.  2 trainee trainee      4096 Aug 30 02:26 .ssh
```

Important - 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@centos8 ~]$ exit
logout
Connection to 127.0.0.1 closed.

[root@centos8 ~]# exit
logout

[trainee@centos8 ~]$ scp .ssh/id_ecdsa.pub trainee@127.0.0.1:/home/trainee/.ssh/authorized_keys
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:Q7T/CP0SLiMbMAIgVzTuEHegYS/spPE5zzQchCHD5Vw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
\S
Kernel \r on an \m
trainee@127.0.0.1's password: trainee
id_ecdsa.pub
100%  192   497.6KB/s   00:00
```

Connectez-vous via telnet :

```
[trainee@centos8 ~]$ ssh -l trainee localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:Q7T/CP0SLiMbMAIgVzTuEHegYS/spPE5zzQchCHD5Vw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
\S
Kernel \r on an \m
```

```
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Aug 30 03:57:14 2021 from 127.0.0.1
[trainee@centos8 ~]$
```

Important - Lors de la connexion au serveur, l'authentification utilise le couple de clefs asymétrique au format ecdsa et aucun mot de passe n'est requis.

Insérez maintenant les clefs publiques restantes dans le fichier .ssh/authorized_keys :

```
[trainee@centos8 ~]$ cd .ssh
[trainee@centos8 .ssh]$ ls
authorized_keys  id_dsa  id_dsa.pub  id_ecdsa  id_ecdsa.pub  id_ed25519  id_ed25519.pub  id_rsa  id_rsa.pub
known_hosts
[trainee@centos8 .ssh]$ cat authorized_keys
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHDrzSXP+Ecxf/sQ18VwCRNm7rrSrrsaJmuIw/RgTH5puKF5E+Yy15cvAAKBX
pJPxUmrOaOyhab84PevV7XSHcI= trainee@centos8.ittraining.loc

[trainee@centos8 .ssh]$ cat id_rsa.pub >> authorized_keys
[trainee@centos8 .ssh]$ cat id_dsa.pub >> authorized_keys
[trainee@centos8 .ssh]$ cat id_ed25519.pub >> authorized_keys

[trainee@centos8 .ssh]$ cat authorized_keys
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHDrzSXP+Ecxf/sQ18VwCRNm7rrSrrsaJmuIw/RgTH5puKF5E+Yy15cvAAKBX
pJPxUmrOaOyhab84PevV7XSHcI= trainee@centos8.ittraining.loc
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQD3ZSMn/GIAHtaDFc6ZNnKJam9hzq8TxqMN5IopUr8QhwODyPadbB+FgH4r50qTux4ubwr1BlymgIdqRVWy3
2mE15M8tdtKc3j8DNMpUwPGEh+s/PT7GW+3E3shoyPvpLc1kKaKXKGl/JwfCK/8IYsubk2BmiiJYkzLECotPlaaxm4w1K0AtlnZQuLHt1HK3/rHCh
xo2o2w1t59/QwNcMLiKve1Z+zQ1POKo8VJ/DDrf90y2QWC28ejUs/ZjP6f6C4bn5Jjol4TbHls3ArMsbU6C1Ev5jqbzZ0kmognQ2CnRjeNM51YdFo
```

```
6nRsLoPQKpeLRMBpT/87HK1bPUOBVCyhXxSkqkVhMlgg8tgcD/MRlBaUVFoZ1wQ0L26Fe+q7c2Oykj54pdXCAK2ZTpCXGfhd/FxrfqGw7cSeKlGX4
QUzHMjMk2oHFC9h30BUk1gGN21KJPTh7/S1OZVrnCc3GUi5fXPvEpral0IU0sws+j03dj0sWm5ICQFKRkmZN11HCyT0=
trainee@centos8.ittraining.loc
ssh-dss
AAAAB3NzaC1kc3MAAACBALIdwEEqHrMWSUdzARm9ldsZK9ebbtZShtmwgdjphOk77fxymK0y6wV7QEmLL25LOcLb12uZ1F0LtRt/t2oqgrwqk3vUS
pCPLr09AXpcD/nxL9kc+rUxHyl6u1mHtyfCVLCPSvavCMR8TaA8egVMk3EwGRfHTiuDOKi7Iwus7gXPAAAAFQDHEQPGVRI7gVYKzCT6nrjDsQQ6jw
AAAIEAhhhH7fEjdldASXY0qTWkCvcs3cfK9/Ff315zByn47O02y9Vdo3QG5nOr1Oo8fc2xEkIBNmFr8Rr2g60cpvEev5hy4XZ1ghxnQ53iwKuiS72
ZATwhD6bZBrsiH0k1Et25gRcj5KCvDe/jHhbxCxsCuHUH2qvWsQNVwztE7hD0sxkAAACAQ8Dkpy8zXj7jW8o1txxf2W6J4r2+1lPldymA45ywZokN
4SCwvXlpPAuyBt0/HiU0R2PI9aqOAMosCLcy9WmnSwLQ2Z7QcD2i3XlAih2+1q9NJP22sPT3jSK9UZcdRjoZ/eNiz84sXZucNape32tFxjvcV4txo
bH/vD53q8g63fA= trainee@centos8.ittraining.loc
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOfFQULLU8IZyKiSU63D2Zz6yGLqyHcBHnCRdSR9JSmc trainee@centos8.ittraining.loc
```
