DEMO 5 : Outils de diagnostic et de suivi de l'activité réseau

La commande `netstat`

Affichage des informations sur les différentes interfaces :

```
# netstat -in
Iface           MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-
OVR Flg
enp38s0        1500    12406      0     60 0          2373      0      0
0 BMRU
lo            65536      199      0      0 0           199      0      0
0 LRU
wlo1           1500        0      0      0 0             0      0      0
0 BMU
```

⇨ Le système dispose de deux interfaces réseau, en plus de celle de bouclage interne lo. On peut voir l'activité réseau écoulée, messages transmis (TX) et reçus (RX). Les indicateurs (flags) renseignent sur l'état et la configuration des interfaces : U active (Up), L bouclage (Loopback), B broadcast géré, M multicast géré, R routage géré.

Affichage des informations de routage :

```
# netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt   If
ace
0.0.0.0         192.168.1.254   0.0.0.0         UG        0 0          0
enp38s0
10.1.0.0        0.0.0.0         255.255.0.0     U         0 0          0
enp38s0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0
enp38s0
```

⇨ Le système participe à deux réseaux IP, 192.168.1.0/24 et 10.1.0.0/16. La passerelle par défaut (Destination = 0.0.0.0) est à l'adresse 192.168.1.254. Les indicateurs indiquent l'état de la route : U active (Up), G via une passerelle (Gateway).

Affichage des informations sur les sockets réseau, y compris celles sur lesquelles des processus sont en attente, avec les processus associés :

```
# netstat --inet -nap
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale       Adresse
distante      Etat        PID/Program name
tcp        0      0
0.0.0.0:111           0.0.0.0:*               LISTEN      1/systemd
tcp        0      0
0.0.0.0:22            0.0.0.0:*               LISTEN      1001/sshd
tcp        0      0
127.0.0.1:631         0.0.0.0:*               LISTEN      1002/cupsd
tcp        0      0 192.168.1.108:22      192.168.1.141:63681   ESTABLISHED
1835/sshd: root [pr
tcp        0    272 192.168.1.108:22      192.168.1.141:64368   ESTABLISHED
4462/sshd: root [pr
```

```
tcp        0      0 10.1.0.1:44730       10.1.0.2:22             ESTABLISHED
4391/ssh
udp        0      0
0.0.0.0:5353          0.0.0.0:*                           929/avahi-daemon: r
udp        0      0
0.0.0.0:53008         0.0.0.0:*                           929/avahi-daemon: r
udp        0      0 192.168.1.108:68     192.168.1.254:67 ESTABLISHED
984/NetworkManager
udp        0      0
0.0.0.0:111           0.0.0.0:*                           1/systemd
```

Exemples avec `ss`

(Cet exemple reprend le précédent, en utilisant les nouvelles commandes à la place de `netstat`.)

On utilise la commande `ss`, avec les options -n (pas de résolution de noms) et -f inet (uniquement les sockets réseau IPv4), sur une distribution RHEL 8.5.

On regarde d'abord la configuration des interfaces et la table de routage, via la commande `ip` :

Affichage des informations sur les différentes interfaces :

```
# ip -br link
lo            UNKNOWN        00:00:00:00:00:00 <LOOPBACK,UP,LOWER_UP>
enp38s0       UP             e4:11:5b:50:13:32
<BROADCAST,MULTICAST,UP,LOWER_UP>
wlo1          DOWN           e6:7e:b5:40:84:e8 <NO-
CARRIER,BROADCAST,MULTICAST,UP>
```

⇨ Le système dispose de deux interfaces réseau, en plus de celle de bouclage interne lo.

Affichage des informations de routage :

```
# ip route
default via 192.168.1.254 dev enp38s0 proto dhcp metric 100
10.1.0.0/16 dev enp38s0 proto kernel scope link src 10.1.0.1
192.168.1.0/24 dev enp38s0 proto kernel scope link src 192.168.1.108 metric
100
```

⇨ Le système participe à deux réseaux IP, 192.168.1.0/24 et 10.1.0.0/16. La passerelle par défaut (Destination = 0.0.0.0) est à l'adresse 192.168.1.254.

Affichage des informations sur les sockets réseau, y compris celles sur lesquelles des processus sont en attente, avec les processus associés :

```
# ss -f inet -nap
Netid     State      Recv-Q     Send-Q                Local Address:Port
Peer Address:Port     Process
udp       UNCONN     0          0                     0.0.0.0:5353
0.0.0.0:*             users:(("avahi-daemon",pid=929,fd=15))
udp       UNCONN     0          0                     0.0.0.0:53008
0.0.0.0:*             users:(("avahi-daemon",pid=929,fd=17))
udp       ESTAB      0          0                     192.168.1.108%enp38s0:68
192.168.1.254:67      users:(("NetworkManager",pid=984,fd=26))
udp       UNCONN     0          0                     0.0.0.0:111
0.0.0.0:*             users:(("rpcbind",pid=848,fd=5),("systemd",pid=1,fd=95)
)
tcp       LISTEN     0          128                   0.0.0.0:111
0.0.0.0:*             users:(("rpcbind",pid=848,fd=4),("systemd",pid=1,fd=94)
)
tcp       LISTEN     0          128                   0.0.0.0:22
0.0.0.0:*             users:(("sshd",pid=1001,fd=5))
```

```
tcp      LISTEN    0         5                     127.0.0.1:631
0.0.0.0:*              users:(("cupsd",pid=1002,fd=10))
tcp      ESTAB     0         0                     192.168.1.108:22
192.168.1.141:63681    users:(("sshd",pid=1853,fd=5),("sshd",pid=1835,fd=5))
tcp      ESTAB     0         0                     192.168.1.108:22
192.168.1.141:64368    users:(("sshd",pid=4466,fd=5),("sshd",pid=4462,fd=5))
tcp      ESTAB     0         0                     10.1.0.1:44730
10.1.0.2:22            users:(("ssh",pid=4391,fd=5))
```