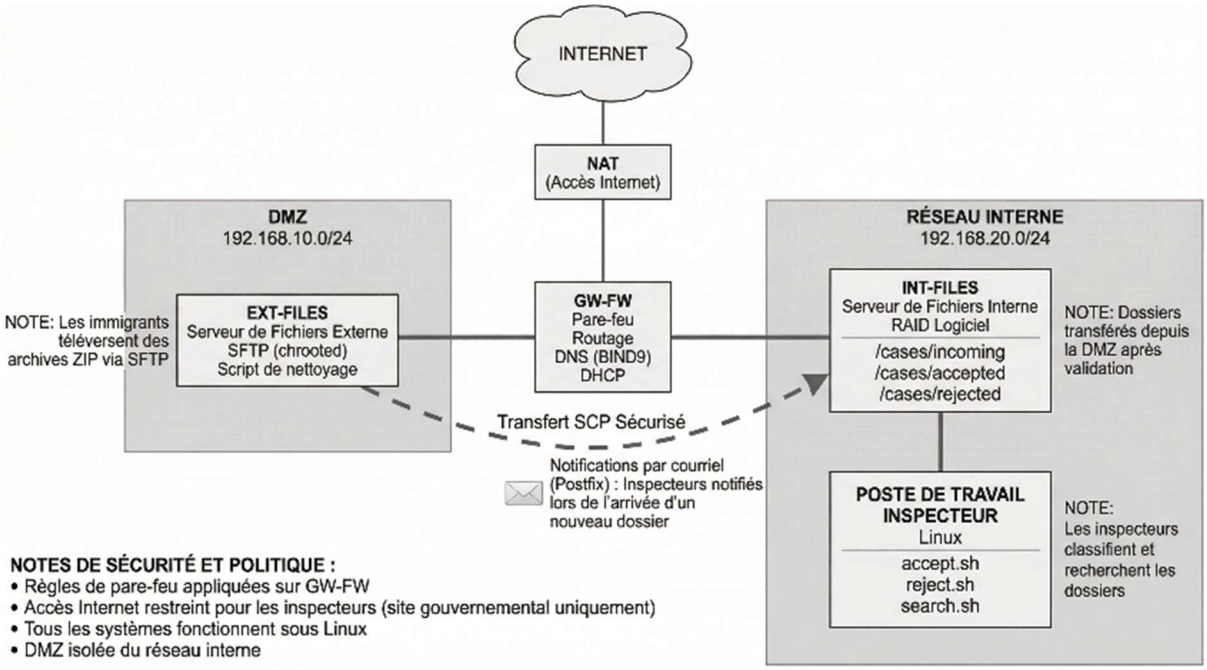
Ahmadou DIALLO

PGE.P

Documentation technique pLPIC2 “Papers Please”

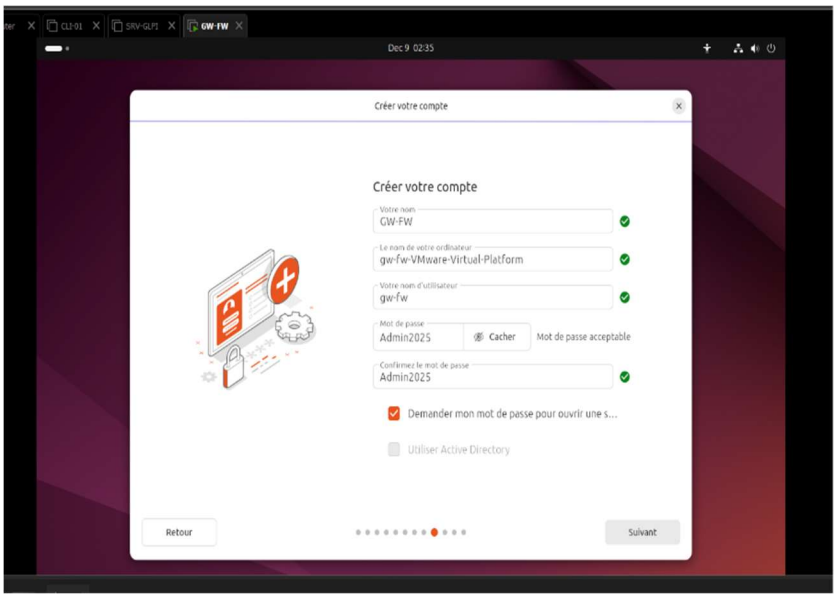
1) Objectif

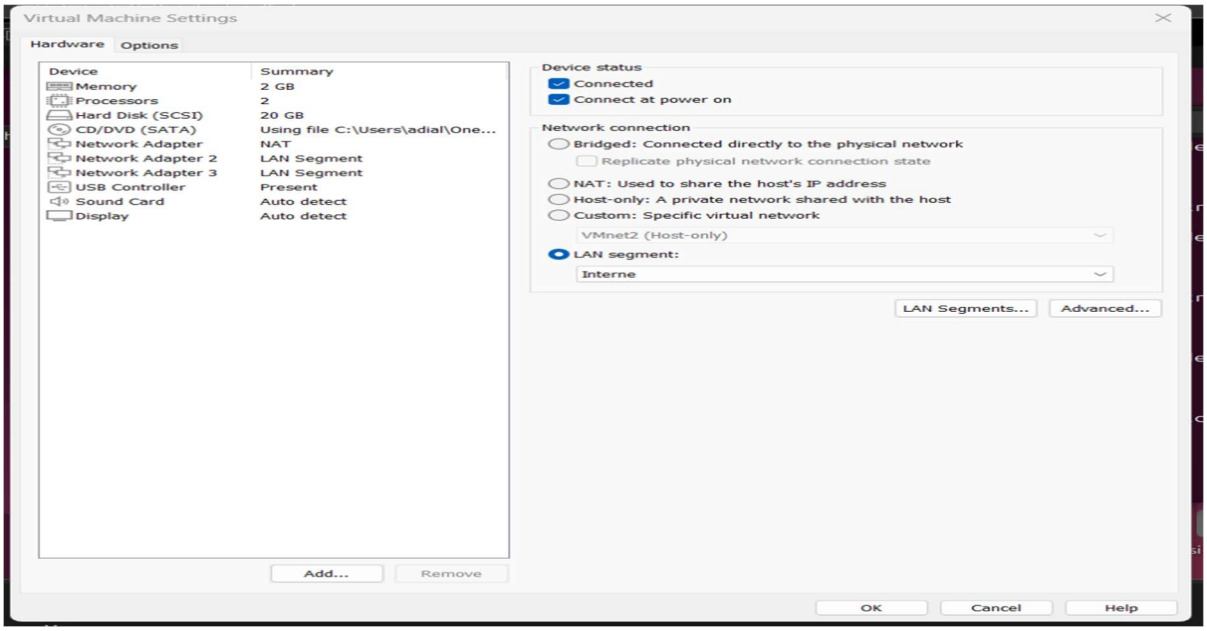
Ce projet met en place une chaîne complète permettant aux “immigrants” de déposer des dossiers sous forme d’archives ZIP, d’en contrôler automatiquement la conformité, de transférer uniquement les cas valides vers un serveur interne, puis de permettre aux “inspectors” de classer et rechercher des cas par identifiant. L’ensemble est sécurisé par une segmentation réseau (DMZ / interne), un pare-feu central et des services réseau internes (DNS/DHCP) ainsi qu’une notification mail à l’arrivée de nouveaux dossiers.



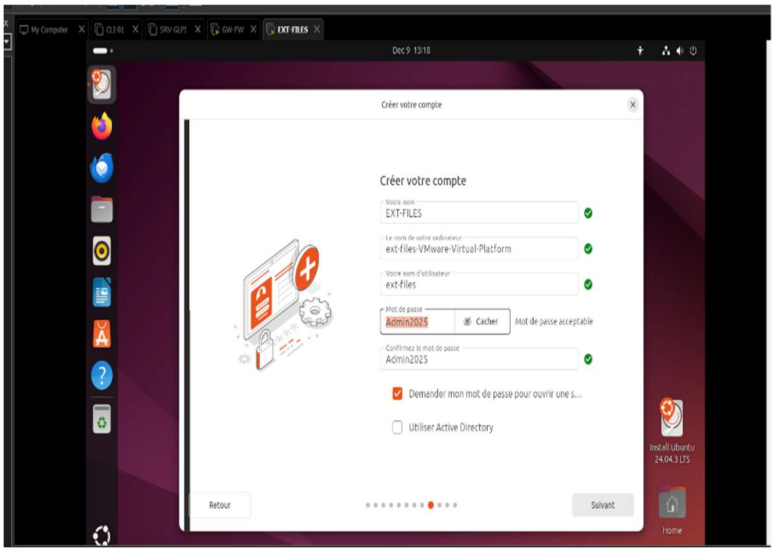
2) Architecture réseau

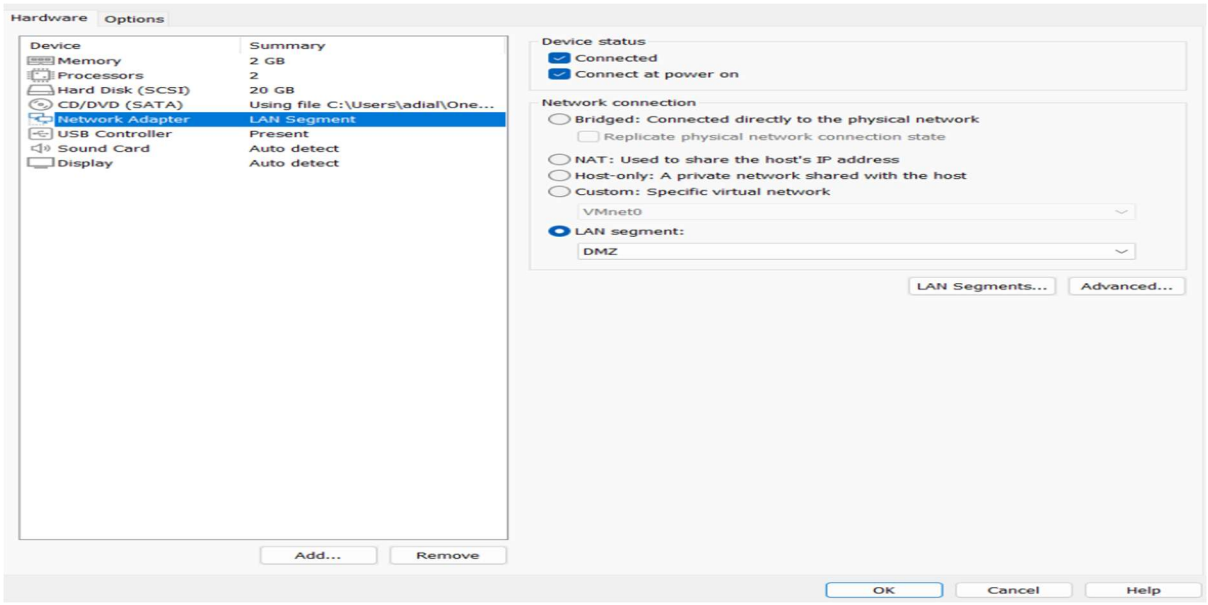
L’infrastructure est segmentée en trois zones : un accès Internet via NAT, une DMZ en 192.168.10.0/24 dédiée au dépôt externe, et un réseau interne en 192.168.20.0/24 pour le stockage et le poste inspector. Cette séparation permet d’exposer uniquement le strict nécessaire (dépôt SFTP en DMZ) tout en isolant le stockage interne et les outils de décision. Le serveur GW-FW sert de point de passage unique : il route, filtre et applique les politiques de sécurité entre les réseaux.

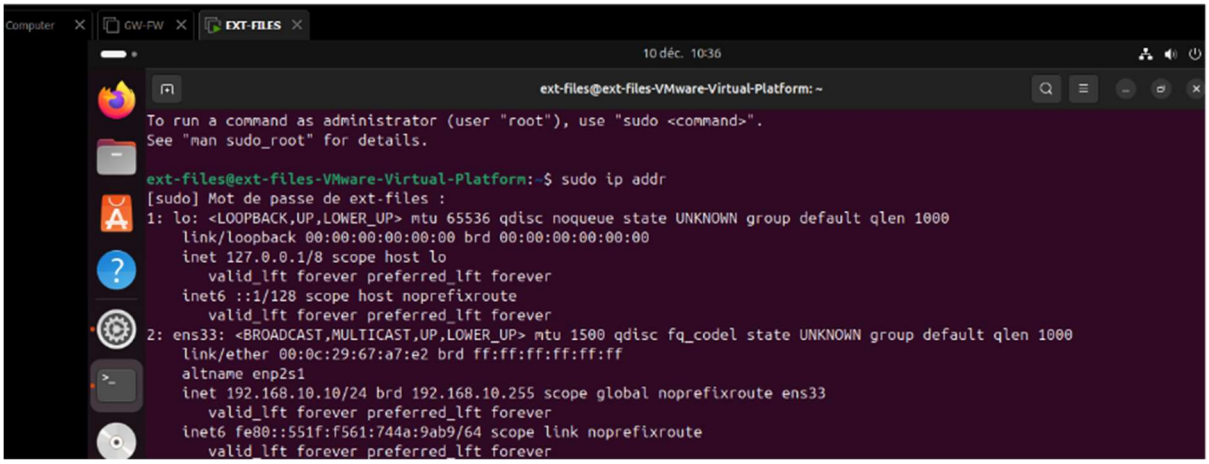


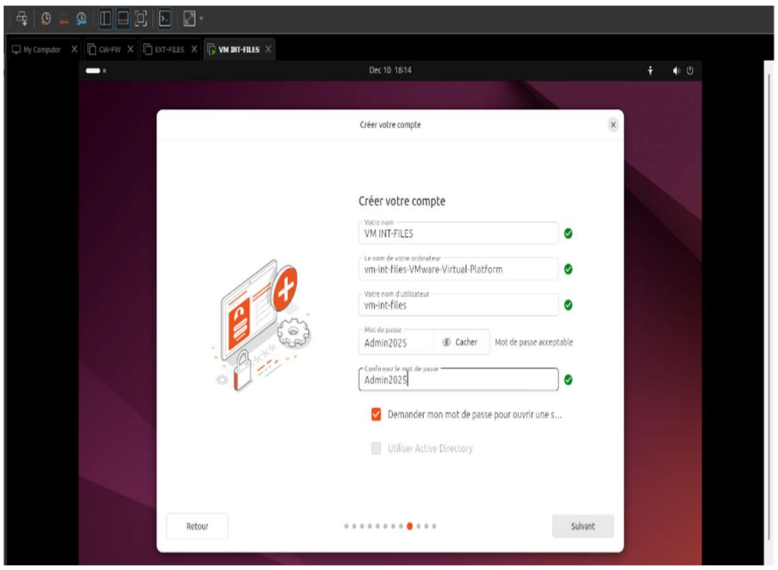


```
gw-fw@gw-fw-VMware-Virtual-Platform:~$
gw-fw@gw-fw-VMware-Virtual-Platform:~$ sudo ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:9c:40:6d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.25.154/24 brd 192.168.25.255 scope global dynamic noprefixroute ens33
       valid_lft 1583sec preferred_lft 1583sec
    inet6 fe80::6e9e:fcfe:931d:cad/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:9c:40:77 brd ff:ff:ff:ff:ff:ff
    altname enp2s2
    inet 192.168.10.1/24 brd 192.168.10.255 scope global noprefixroute ens34
       valid_lft forever preferred_lft forever
4: ens35: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:9c:40:81 brd ff:ff:ff:ff:ff:ff
    altname enp2s3
    inet 192.168.20.1/24 brd 192.168.20.255 scope global noprefixroute ens35
       valid_lft forever preferred_lft forever
    inet6 fe80::456:9b2f:59e6:efa4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
gw-fw@gw-fw-VMware-Virtual-Platform:~$
```




Hardware
Options
Device
Summary
Memory
2 GB
Processors
2
Hard Disk (SCSI)
20 GB
CD/DVD (SATA)
Using file C:\Users\adial\One...
Network Adapter
LAN Segment
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
DMZ
LAN Segments...
Advanced...
OK
Cancel
Help


Computer
GW-FW
EXT-FILES
10 déc. 10:36
ext-files@ext-files-VMware-Virtual-Platform: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ext-files@ext-files-VMware-Virtual-Platform:~$ sudo ip addr
[sudo] Mot de passe de ext-files :
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 noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
link/ether 00:0c:29:67:a7:e2 brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 192.168.10.10/24 brd 192.168.10.255 scope global noprefixroute ens33
valid_lft forever preferred_lft forever
inet6 fe80::551f:f561:744a:9ab9/64 scope link noprefixroute
valid_lft forever preferred_lft forever



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\Users\adial\One...
Network Adapter	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

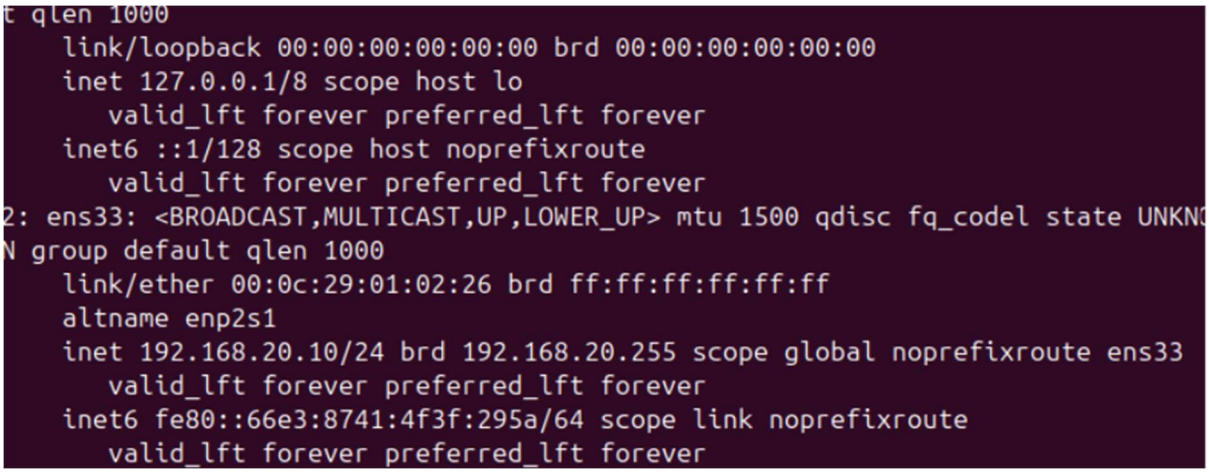
Add... Remove

Device status
- [x] Connected
- [x] Connect at power on

Network connection
- ( ) Bridged: Connected directly to the physical network
  - [ ] Replicate physical network connection state
- ( ) NAT: Used to share the host's IP address
- ( ) Host-only: A private network shared with the host
- ( ) Custom: Specific virtual network
  - VMnet0
- (•) LAN segment:
  - Interne

LAN Segments... Advanced...

OK Cancel Help



3) Serveur GW-FW : routage, firewall, DNS, DHCP

Le serveur GW-FW joue un rôle central, il assure le routage entre les interfaces (NAT, DMZ et interne) et constitue l'unique point de contrôle des flux. Le forwarding IPv4 est activé afin de permettre le transit inter-réseaux, et la table de routage garantit que la DMZ et l'interne utilisent GW-FW comme passerelle par défaut.

La sécurité est appliquée via des règles sur GW-FW. L'objectif est de limiter les communications au strict nécessaire : la DMZ ne doit pas pouvoir accéder librement au réseau interne, à l'exception des flux indispensables (par exemple, transfert SCP depuis EXT-FILES vers INT-FILES). Côté interne, les inspectors disposent d'un accès Internet restreint (uniquement vers le site gouvernemental autorisé), ce qui réduit fortement le risque d'exfiltration ou d'usage non conforme.

Le service DNS interne est fourni par sur GW-FW via le domaine gov.local. Les hôtes internes (int-files.gov.local, ext-files.gov.local, etc.) sont résolus par ce DNS afin de simplifier la configuration. Les clients internes utilisent GW-FW comme serveur DNS, ce qui garantit une résolution cohérente et centralisée.

```
gw-fw@gw-fw-VMware-Virtual-Platform:~$ dig @127.0.0.1 int-files.gov.local

; <<>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <<>> @127.0.0.1 int-files.gov.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58786
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 85a15ec5288a3bfe01000000693acc91ce05bbc7ef1cb7ea (good)
;; QUESTION SECTION:
;int-files.gov.local.           IN      A

;; ANSWER SECTION:
int-files.gov.local.    604800  IN      A       192.168.20.10

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Dec 11 14:52:17 CET 2025
;; MSG SIZE  rcvd: 92

gw-fw@gw-fw-VMware-Virtual-Platform:~$
```

Vérifications :

```
Global
         Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub
       DNS Servers: 192.168.20.1
        DNS Domain: gov.local

Link 2 (ens33)
    Current Scopes: DNS
         Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
       DNS Servers: 192.168.20.1
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$ ping gw-fw.gov.local
ping int-files.gov.local
PING gw-fw.gov.local (192.168.20.1) 56(84) bytes of data.
64 bytes from _gateway (192.168.20.1): icmp_seq=1 ttl=64 time=0.627 ms
64 bytes from _gateway (192.168.20.1): icmp_seq=2 ttl=64 time=0.604 ms
64 bytes from _gateway (192.168.20.1): icmp_seq=3 ttl=64 time=0.685 ms

--- gw-fw.gov.local ping statistics ---
^C3 packets transmitted, 3 received, 0% packet loss, time 2050ms
rtt min/avg/max/mdev = 0.604/0.638/0.685/0.034 ms
PING int-files.gov.local (192.168.20.10) 56(84) bytes of data.
64 bytes from vm-int-files-VMware-Virtual-Platform (192.168.20.10): icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from vm-int-files-VMware-Virtual-Platform (192.168.20.10): icmp_seq=2 ttl=64 time=0.080 ms
^C
--- int-files.gov.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.058/0.069/0.080/0.011 ms
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$
```

Enfin, le DHCP est également centralisé sur GW-FW afin de simplifier le déploiement des postes inspectors. Il attribue automatiquement une adresse IP au poste, ainsi que la passerelle et le DNS.

```
gw-fw@gw-fw-VMware-Virtual-Platform:~$ sudo apt install isc-dhcp-server
[sudo] Mot de passe de gw-fw :
Désolé, essayez de nouveau.
[sudo] Mot de passe de gw-fw :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  isc-dhcp-common
Paquets suggérés :
  isc-dhcp-server-ldap policycoreutils
Les NOUVEAUX paquets suivants seront installés :
  isc-dhcp-common isc-dhcp-server
0 mis à jour, 2 nouvellement installés, 0 à enlever et 121 non mis à jour.
Il est nécessaire de prendre 1 281 ko dans les archives.
Après cette opération, 4 281 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-server amd64 4.4.3-P1-4ubuntu2 [1 236 kB]
Réception de :2 http://archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-common amd64 4.4.3-P1-4ubuntu2 [45,8 kB]
1 281 ko réceptionnés en 4s (298 ko/s)
Préconfiguration des paquets...
Sélection du paquet isc-dhcp-server précédemment désélectionné.
(Lecture de la base de données... 207938 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../isc-dhcp-server_4.4.3-P1-4ubuntu2_amd64.deb ...
Dépaquetage de isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Sélection du paquet isc-dhcp-common précédemment désélectionné.
Préparation du dépaquetage de .../isc-dhcp-common_4.4.3-P1-4ubuntu2_amd64.deb ...
Dépaquetage de isc-dhcp-common (4.4.3-P1-4ubuntu2) ...
Paramétrage de isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Generating /etc/default/isc-dhcp-server...
```

```
subnet 192.168.20.0 netmask 255.255.255.0 {
     range 192.168.20.100 192.168.20.200;
     option routers 192.168.20.1;
     option domain-name-servers 8.8.8.8;
}
```

```
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-12-11 13:38:50 CET; 60ms ago
       Docs: man:dhcpd(8)
   Main PID: 5449 (dhcpd)
      Tasks: 1 (limit: 2130)
     Memory: 2.6M (peak: 2.6M)
        CPU: 27ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─5449 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf ens35
```

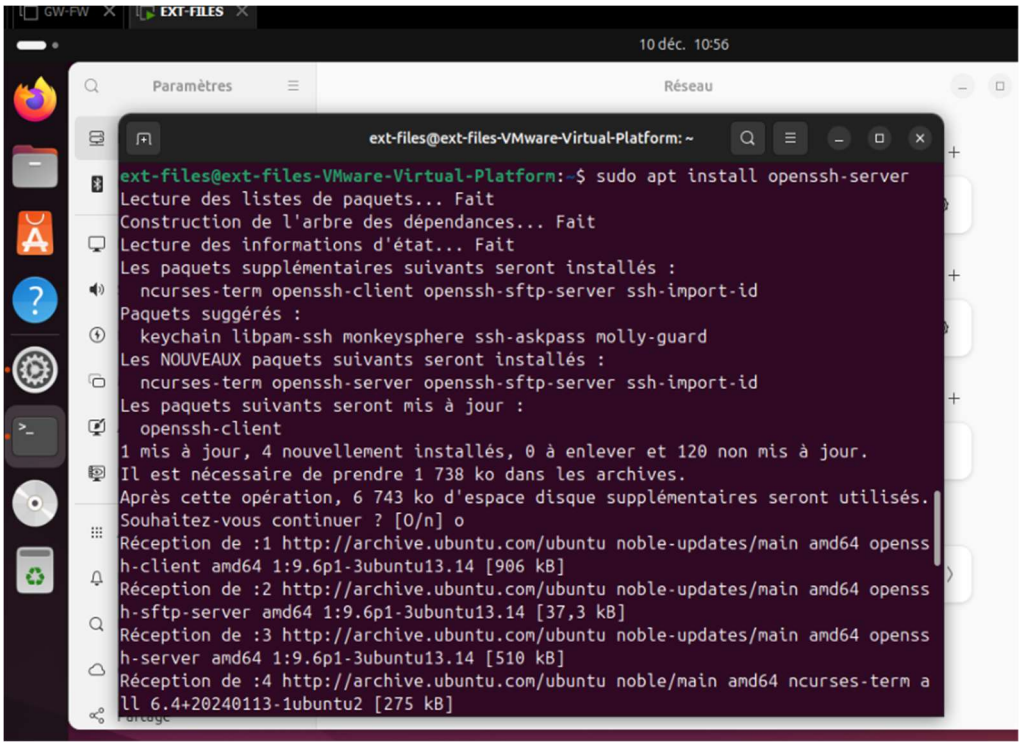
Vérification DHCP :

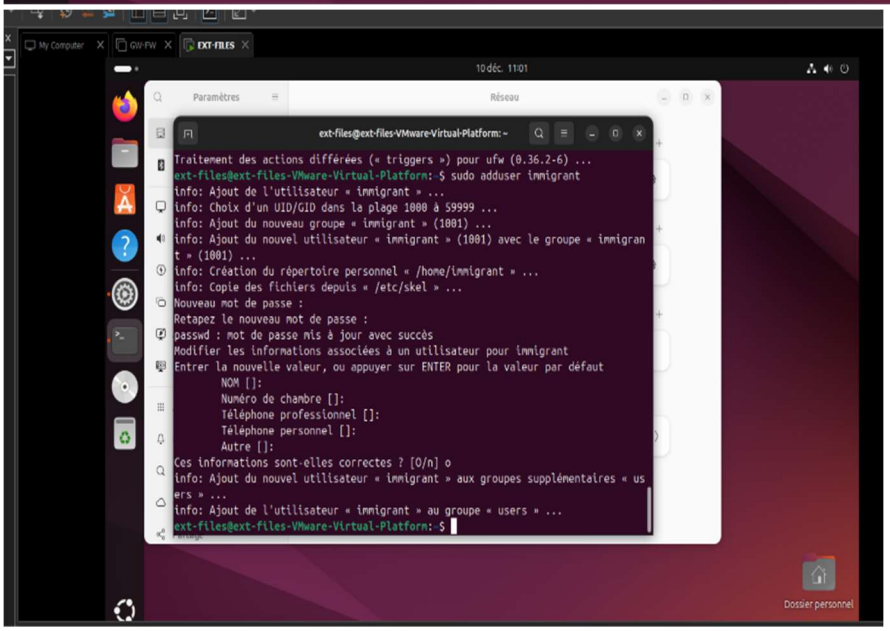
Sur le serveur int files après avoir mis l'IP en automatique on peut voir que le DHCP est fonctionnel :

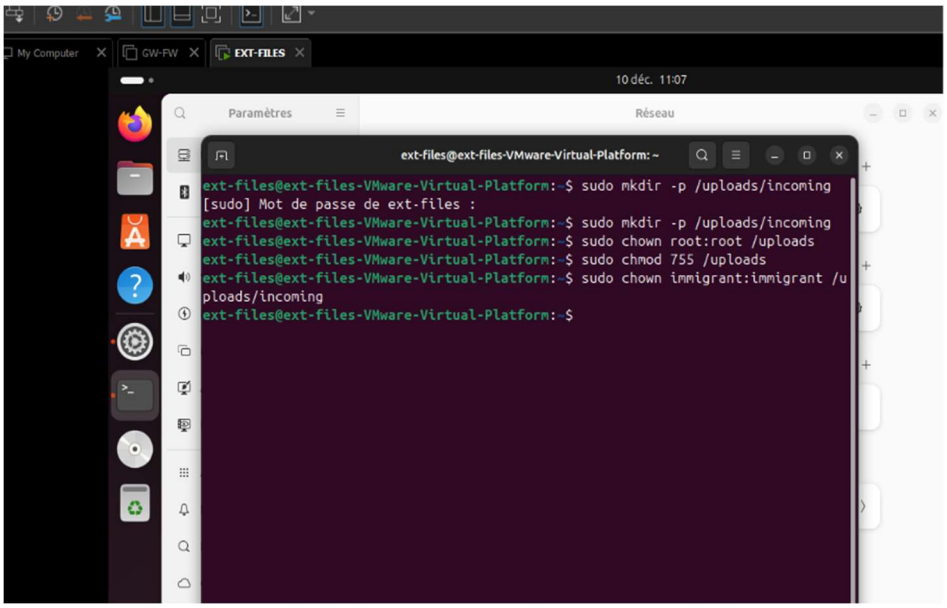
```
ip addr
Warning: The unit file, source configuration file or drop-ins of NetworkManager.service changed on disk. Run 'sys
s.
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:01:02:26 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.100/24 brd 192.168.20.255 scope global dynamic noprefixroute ens33
       valid_lft 573sec preferred_lft 573sec
    inet6 fe80::66e3:8741:4f3f:295a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$
```

4) EXT-FILES (DMZ) : dépôt SFTP chroot + contrôle automatique

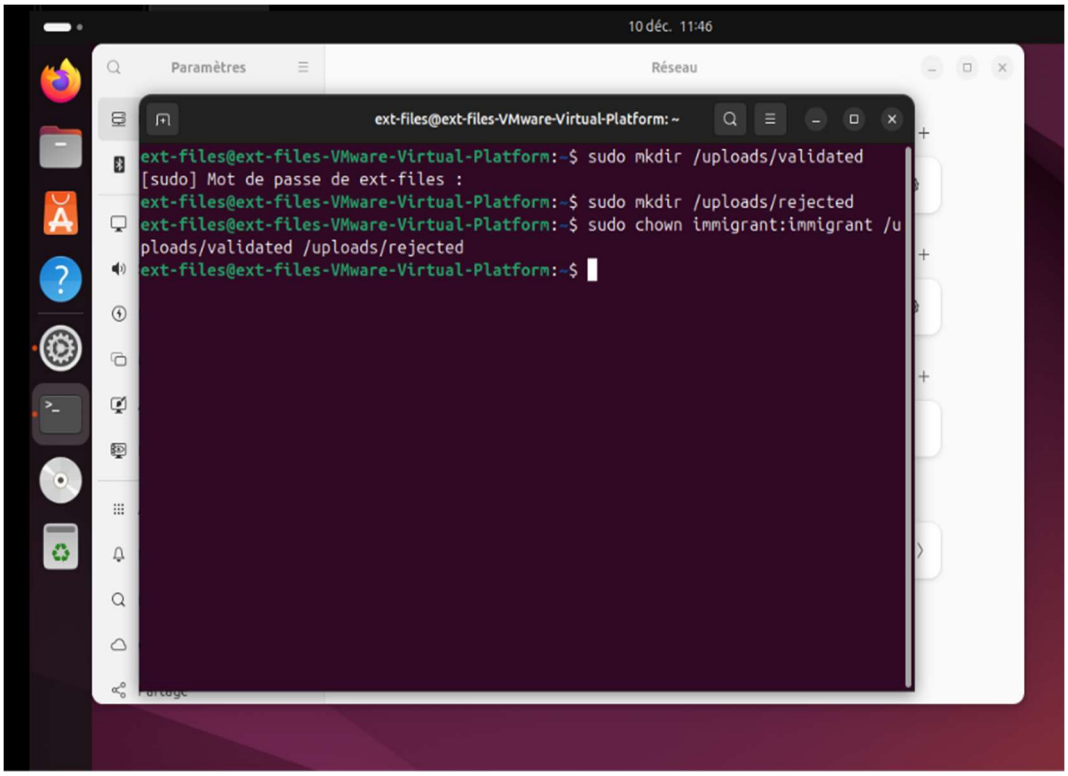
Le serveur EXT-FILES, placé en DMZ, est dédié au dépôt des immigrants. L’accès se fait via SFTP, avec un chroot et un compte restreint afin d’empêcher toute interaction avec le système de fichiers en dehors du répertoire d’upload. Cette approche limite l’exposition et réduit l’impact potentiel d’un compte compromis.

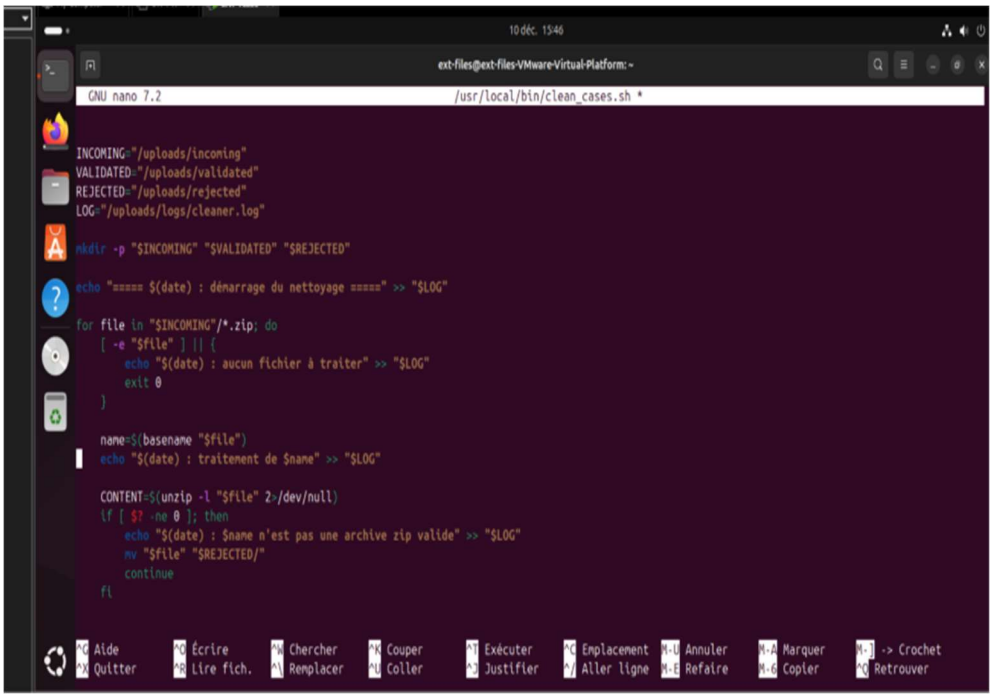

GW-FW
EXT-FILES
10 déc. 10:56
Paramètres
Réseau
ext-files@ext-files-VMware-Virtual-Platform: ~
ext-files@ext-files-VMware-Virtual-Platform:~$ sudo apt install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
ncurses-term openssh-client openssh-sftp-server ssh-import-id
Paquets suggérés :
keychain libpam-ssh monkeysphere ssh-askpass molly-guard
Les NOUVEAUX paquets suivants seront installés :
ncurses-term openssh-server openssh-sftp-server ssh-import-id
Les paquets suivants seront mis à jour :
openssh-client
1 mis à jour, 4 nouvellement installés, 0 à enlever et 120 non mis à jour.
Il est nécessaire de prendre 1 738 ko dans les archives.
Après cette opération, 6 743 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-client amd64 1:9.6p1-3ubuntu13.14 [906 kB]
Réception de :2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.14 [37,3 kB]
Réception de :3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.14 [510 kB]
Réception de :4 http://archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]


My Computer
GW-FW
EXT-FILES
10 déc. 11:01
Paramètres
Réseau
ext-files@ext-files-VMware-Virtual-Platform: ~
Traitement des actions différées (« triggers ») pour ufw (0.36.2-6) ...
ext-files@ext-files-VMware-Virtual-Platform:~$ sudo adduser immigrant
info: Ajout de l'utilisateur « immigrant » ...
info: Choix d'un UID/GID dans la plage 1000 à 59999 ...
info: Ajout du nouveau groupe « immigrant » (1001) ...
info: Ajout du nouvel utilisateur « immigrant » (1001) avec le groupe « immigrant » (1001) ...
info: Création du répertoire personnel « /home/immigrant » ...
info: Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour immigrant
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
NOM []:
Numéro de chambre []:
Téléphone professionnel []:
Téléphone personnel []:
Autre []:
Ces informations sont-elles correctes ? [O/n] o
info: Ajout du nouvel utilisateur « immigrant » aux groupes supplémentaires « users » ...
info: Ajout de l'utilisateur « immigrant » au groupe « users » ...
ext-files@ext-files-VMware-Virtual-Platform:~$
Dossier personnel

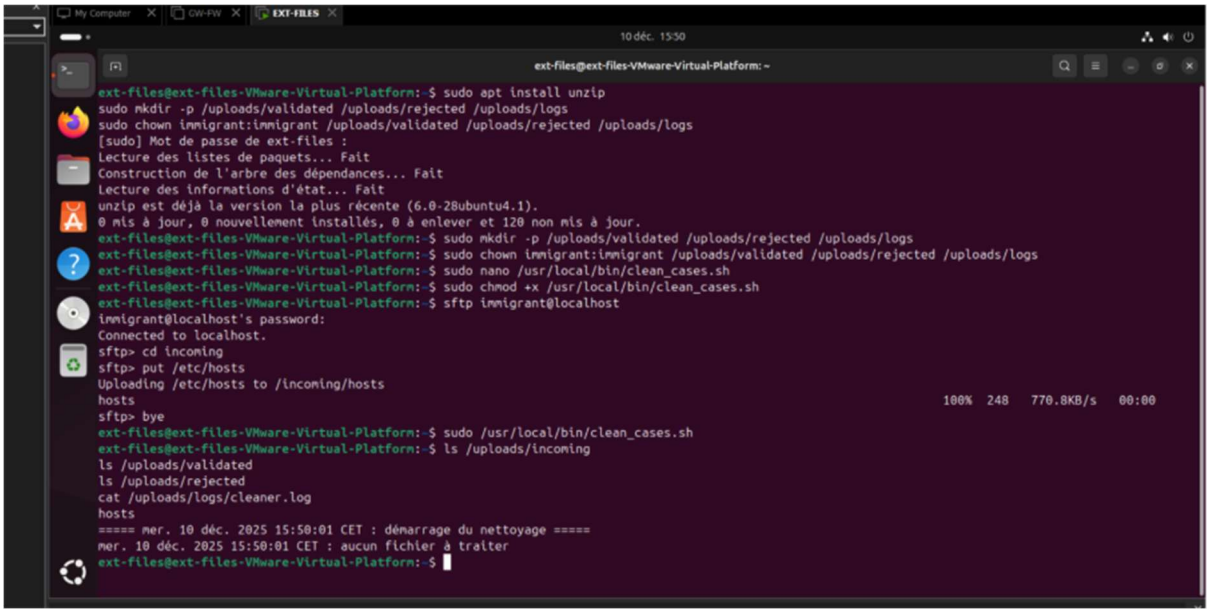


Les immigrants déposent leurs ZIP dans une arborescence dédiée. Un script de clean-up analyse automatiquement chaque archive : il vérifie le format ZIP, la présence des fichiers requis et la cohérence de l'identifiant immigrant dans les noms de fichiers. Les archives conformes sont déplacées vers un répertoire "validated" tandis que les non conformes sont isolés dans "rejected".





Test du script :



5) Transfert sécurisé DMZ → Interne

Une fois validés, les ZIP sont transférés depuis EXT-FILES vers le serveur interne INT-FILES via SCP. Ce choix fournit un canal chiffré et simple à automatiser (cron), et garantit que seuls les dossiers passés par le contrôle de conformité atteignent la zone interne.

```
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$ sudo apt install openssh-server
sudo mkdir -p /cases/incoming /cases/accepted /cases/rejected
sudo chown -R vm-int-files:vm-int-files /cases
[sudo] Mot de passe de vm-int-files :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Paquets suggérés :
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
Les NOUVEAUX paquets suivants seront installés :
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
Les paquets suivants seront mis à jour :
  openssh-client
1 mis à jour, 4 nouvellement installés, 0 à enlever et 147 non mis à jour.
Il est nécessaire de prendre 1 738 ko dans les archives.
Après cette opération, 6 743 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-client amd64 1:9.6p1-3ubuntu13.14 [906 kB]
Réception de :2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.14 [37,3 kB]
Réception de :3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.14 [510 kB]
Réception de :4 http://archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]
Réception de :5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 ssh-import-id all 5.11-0ubuntu2.24.04.1 [10,1 kB]
1 738 ko réceptionnés en 4s (389 ko/s)
Préconfiguration des paquets...
(Lecture de la base de données... 190885 fichiers et répertoires déjà installés.
)
```

```
ext-files@ext-files-VMware-Virtual-Platform:~$ ssh vm-int-files@192.168.20.10
The authenticity of host '192.168.20.10 (192.168.20.10)' can't be established.
ED25519 key fingerprint is SHA256:9jnJBynKJHXd8hyZUaochRBzDKCpKGwXpWPOtDRjaCY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.20.10' (ED25519) to the list of known hosts.
vm-int-files@192.168.20.10's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

La maintenance de sécurité étendue pour Applications n'est pas activée.

145 mises à jour peuvent être appliquées immédiatement.
25 de ces mises à jour sont des mises à jour de sécurité.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Activez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires.
Visitez https://ubuntu.com/esm ou executez : sudo pro status

*** Le système doit être redémarré ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
```

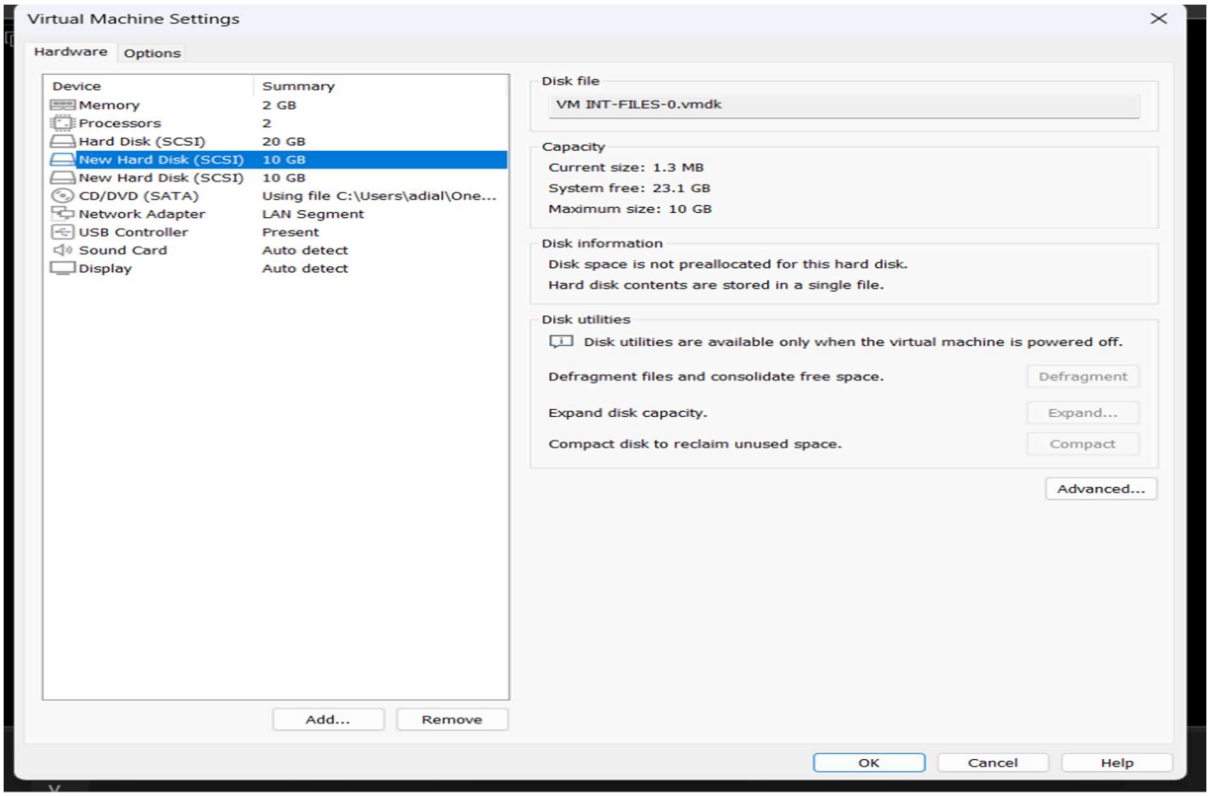
Le **transfert EXT-FILES → INT-FILES fonctionne:**

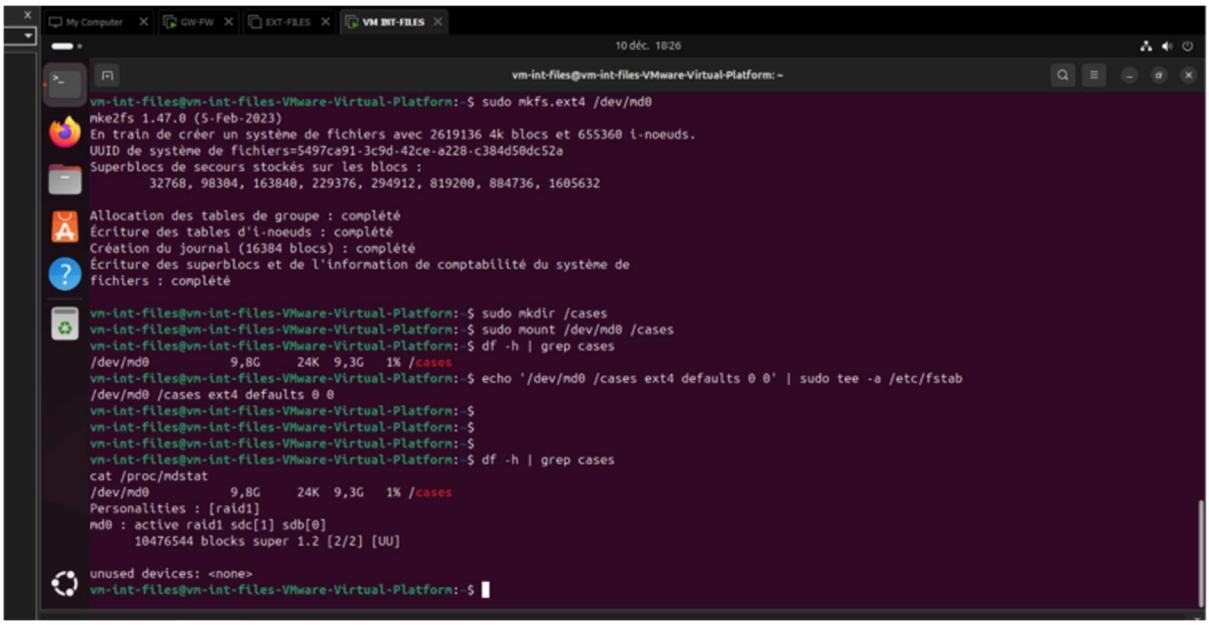
```
ext-files@ext-files-VMware-Virtual-Platform:~$ scp /uploads/validated/dossier_test.zip vm-int-files@192.168.20.10:/cases/incoming/
vm-int-files@192.168.20.10's password:
dossier_test.zip                                              100%  326    61.1KB/s   00:00
ext-files@ext-files-VMware-Virtual-Platform:~$
```

```
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$ ls /cases/incoming
dossier_test.zip
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$
```

6) INT-FILES (Interne) : RAID, stockage des cas, notifications

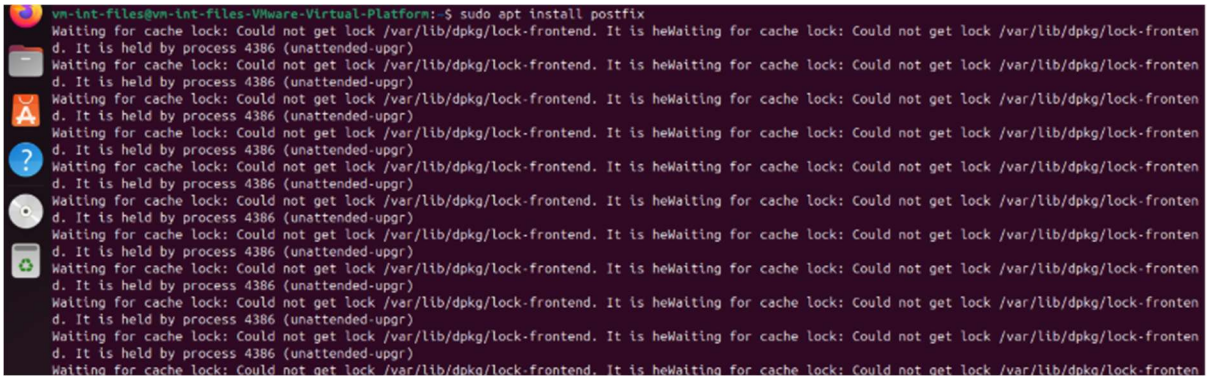
Le serveur INT-FILES héberge la base de dossiers internes et doit résister aux pannes disque. Un RAID logiciel est mis en place afin d'assurer la tolérance de panne et la continuité de service.



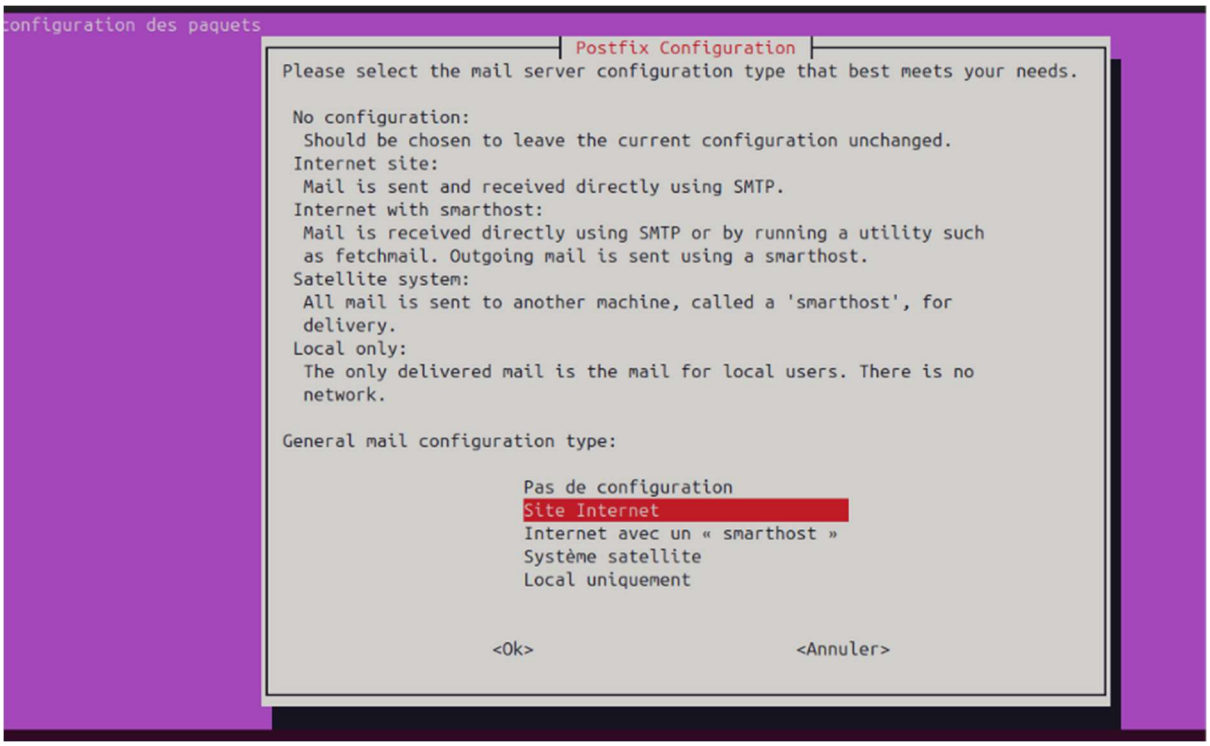


Un service mail basé sur Postfix est utilisé pour notifier automatiquement les inspectors lorsqu'un nouveau dossier arrive en attente de validation. Cette notification est déclenchée par les scripts (ou par le transfert) et permet de réduire la latence opérationnelle sans surveillance manuelle.

Configuration serveur mail interne :



On choisi local uniquement :



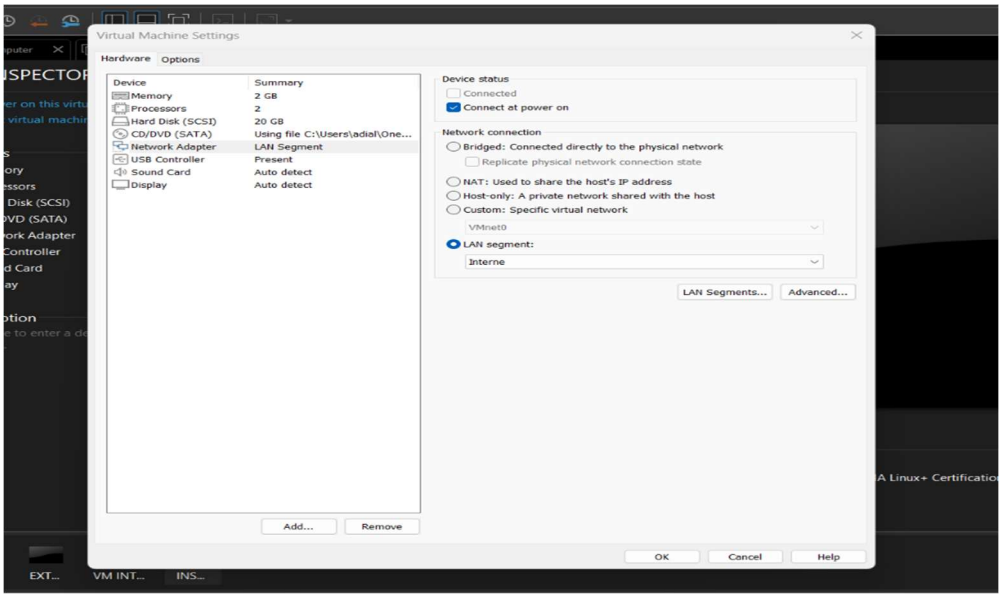
Test :

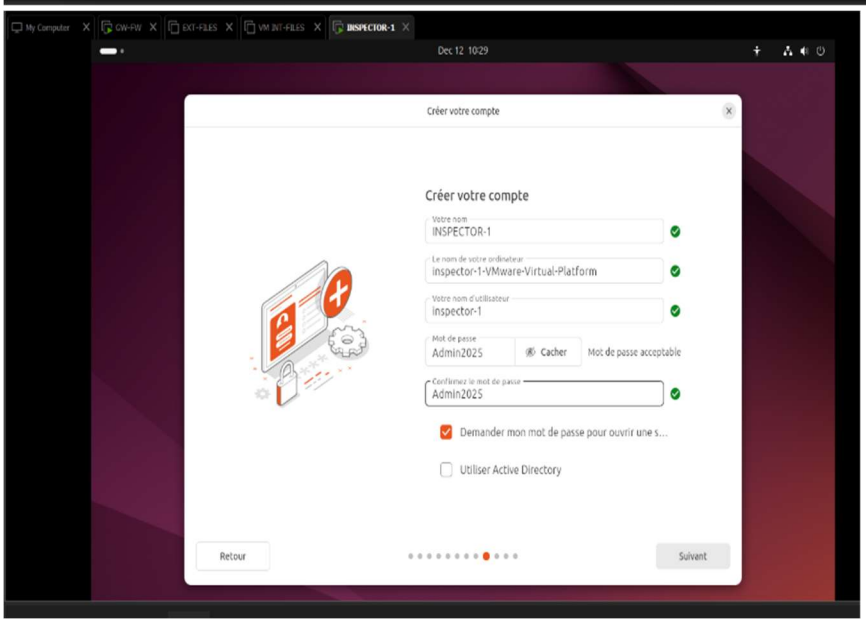
```
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$ echo "Test mail OK" | mail -s "Nouveau dossier reçu" vm-int-files
mail
"/var/mail/vm-int-files": 2 messages 2 nouveaux
>N   1 VM INT-FILES       jeu. déc. 11 16  12/585   Nouveau dossier reçu
 N   2 VM INT-FILES       jeu. déc. 11 16  13/598   Nouveau dossier reçu
? 1
Return-Path: <vm-int-files@vm-int-files-VMware-Virtual-Platform>
X-Original-To: vm-int-files
Delivered-To: vm-int-files@int-files.gov.local
Received: by vm-int-files-VMware-Virtual-Platform.gov.local (Postfix, from userid 1000)
        id 79D45A00AB; Thu, 11 Dec 2025 16:09:47 +0100 (CET)
Subject: Nouveau dossier reçu
To: vm-int-files@int-files.gov.local
User-Agent: mail (GNU Mailutils 3.17)
Date: Thu, 11 Dec 2025 16:09:47 +0100
Message-Id: <20251211150947.79D45A00AB@vm-int-files-VMware-Virtual-Platform.gov.local>
From: VM INT-FILES <vm-int-files@vm-int-files-VMware-Virtual-Platform>

? q
1 message sauvegardé dans /home/vm-int-files/mbox
1 message conservé dans /var/mail/vm-int-files
vm-int-files@vm-int-files-VMware-Virtual-Platform:~$
```

7) Poste INSPECTOR : accès aux dossiers + scripts accept/reject/search

Le poste INSPECTOR, situé sur le réseau interne, obtient sa configuration réseau via DHCP et utilise le DNS interne pour résoudre les serveurs par nom. Il accède directement aux répertoires du serveur INT-FILES afin de traiter les dossiers. Les scripts accept.sh et reject.sh permettent de déplacer un dossier depuis /cases/incoming vers /cases/accepted ou /cases/rejected. Le script search.sh permet de vérifier rapidement le statut d'un identifiant immigrant (accepté, rejeté, en attente, inconnu).

Création poste inspecteur :





Inspector 1 est bien dans le domaine gov.local et son a eu son ip via le dhcp

```
inspector-1@inspector-1-VMware-Virtual-Platform:~$ resolvectl status
Global
         Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (ens33)
    Current Scopes: DNS
         Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
       DNS Servers: 192.168.20.1
        DNS Domain: gov.local
inspector-1@inspector-1-VMware-Virtual-Platform:~$ ip addr
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 noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:63:7d:a7 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.101/24 brd 192.168.20.255 scope global dynamic noprefixroute ens33
       valid_lft 383sec preferred_lft 383sec
    inet6 fe80::7777:82ad:2145:370e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
inspector-1@inspector-1-VMware-Virtual-Platform:~$
```

Scripts INSPECTEUR :

Test script :

```
inspector-1@inspector-1-VMware-Virtual-Platform:~$ ls ~/cases/incoming
./accept.sh     # ou ./reject.sh
./search.sh
auto_test.zip  dossier_test.zip
Nom du dossier à ACCEPTER: auto_test.zip
ACCEPTÉ: auto_test.zip
ID à rechercher: 67890
grep: /home/inspector-1/cases/accepted/auto_test.zip : fichiers binaires correspondent
ACCEPTÉ
inspector-1@inspector-1-VMware-Virtual-Platform:~$ ls ~/cases/accepted
ls ~/cases/rejected
auto_test.zip
inspector-1@inspector-1-VMware-Virtual-Platform:~$
```

Test pour un rejet :

```
inspector-1@inspector-1-VMware-Virtual-Platform:~$ ./reject.sh
dossier_test.zip
Nom du dossier à REJETER: dossier_test.zip
REJETÉ: dossier_test.zip
inspector-1@inspector-1-VMware-Virtual-Platform:~$ ls ~/cases/rejected
dossier_test.zip
inspector-1@inspector-1-VMware-Virtual-Platform:~$
```

L'accès Internet depuis le poste inspector est volontairement restreint par le firewall sur GW-FW. Pour que ce point soit incontestable à la soutenance, il faut montrer une preuve : une navigation réussie vers le site gouvernemental autorisé, et un accès bloqué vers un site non autorisé.

8) Scripts livrés :

Les scripts suivants sont utilisés :

cleanup.sh : analyse les archives déposées sur EXT-FILES, vérifie la conformité puis classe les ZIP dans **validated** ou **rejected** et écrit un log.

transfer_cases.sh : transfère uniquement les ZIP validés vers le serveur interne INT-FILES via **SCP**, évite les doublons, archive le ZIP dans **transferred** et déclenche l'envoi d'une notification mail.

Pipeline.sh : exécute successivement cleanup.sh puis transfer_cases.sh. Ce script est appelé automatiquement par cron.

Accept.sh : utilisé sur le poste inspector pour déplacer un cas depuis **incoming** vers **accepted** et journaliser la décision.

Reject.sh : utilisé sur le poste inspector pour déplacer un cas depuis **incoming** vers **rejected** et journaliser la décision.

Search.sh : permet de rechercher un identifiant immigrant et d'afficher son statut (**ACCEPTÉ / REJETÉ / EN ATTENTE / INCONNU**).

9) Conclusion

Ce projet met en place un système complet de contrôle dématérialisé : dépôt des archives en DMZ, vérification automatique (clean-up), transfert sécurisé vers le serveur interne, puis traitement par les inspectors (accept/reject/search). La segmentation réseau et le serveur GW-FW (firewall, routage, DNS, DHCP) assurent la sécurité et l'isolation des zones. Les logs et notifications par mail garantissent la traçabilité et une prise en charge rapide des dossiers. L'ensemble est simple, robuste, et prêt à être démontré.