

Projet en pLPIC2

Contexte : Il y a des problèmes d'immigration, et pour contrôler les frontières, on nous demande de numériser le processus de contrôle des immigrés. Tous doivent être fait sous Linux.

Les immigrés déposent une archive (zip ou autre) sur un serveur de fichier. Dans cette archive il y a un :

- Un fichier **TXT** avec les infos personnelles : pays, raison de visite, durée, taille, poids, etc.
- Des **documents PDF** contenant tout le numéro **d'identification** de la personne.

Le serveur doit automatiquement nettoyer et **supprimer** les archives non conformes. Et **Transférer** les fichiers valides vers un **serveur interne** (sécurisé).

Le serveur de base de fichier doit être résistant à une panne (RAID) et comporte 3 dossiers : en attente, refuser, accepter. Les inspecteurs sont **notifiés par mail** lorsqu'un nouveau dossier arrive.

Poste des inspecteurs :

- Accès direct au **serveur interne**.
- Un programme leur permet de :
 - Ouvrir et examiner les documents.
 - Accepter ou refuser les dossiers.
- Accès :
 - à la **messagerie interne**,
 - et à **Internet**, mais **seulement au site du gouvernement**.
- Un outil de recherche permet de vérifier si un **identifiant d'immigré** est autorisé à entrer.

Pour réaliser ce projet nous avons décidé 2 machine virtuelle qui vont s'occuper de ces tâches.

La 1ère est le 'serveur' :

A. Router-Grestin : Le Cerveau Réseau et la Sécurité

Cette machine joue le rôle de **routeur, serveur DNS, serveur DHCP, et pare-feu**.

Objectif	Service/Configuration	Rôle dans l'Infrastructure
Passerelle & Sécurité	UFW (Firewall)	Sécurise le réseau en bloquant tout trafic non essentiel. Seuls les services nécessaires (DNS, DHCP, Mail, Samba) sont autorisés à circuler.
Nommage (DNS)	Bind9	Permet à tous les équipements du réseau de trouver les services du serveur interne en utilisant son nom (<code>server-internal.grestin.gov</code>) au lieu de son IP (<code>192.168.10.2</code>).
Adresses IP	ISC DHCP Server	Distribue automatiquement des adresses IP aux clients (bien que le serveur utilise une IP statique).

Bien sûr pour respecter les consignes de l'énoncé, il faut installer et configurer le routeur, le DNS, le DHCP et pare-feu etc... Qui seront un peu plus en bas.

La 2eme machine a pour rôle 'service interne' :

2. Server-Internal : Stockage, Données et Automatisation

Cette machine est le cœur du système. Elle gère le stockage sécurisé des archives, les services de messagerie, et la logique d'automatisation.

A. Stockage et Accès

Objectif	Service/Configuration	Rôle dans l'Infrastructure
Redondance des Données	RAID 1 (mdadm)	Combine deux disques physiques en un volume logique (<code>/dev/md0</code>) monté sur <code>/srv/files</code> . Si un disque tombe en panne, les données restent intactes sur l'autre.
Partage de Fichiers	Samba	Permet aux inspecteurs de se connecter et d'accéder au volume RAID (<code>/srv/files</code>) pour déposer et récupérer des archives.
Utilisateurs	<code>adduser</code>	Création des comptes comme <code>inspector1</code> pour la gestion des accès et des permissions.

Pour répondre aux demandes de gestion des fichiers, nous avons décidé de faire ainsi :

B. Flux d'Archives et Automatisation

Objectif	Service/Configuration	Rôle dans l'Infrastructure
Gestion des Tâches	Cron (crontab)	Planifie l'exécution des scripts de maintenance et de flux à des heures précises (par exemple, minuit).
Scripts de Flux	<code>transfer.sh</code>	<i>La logique métier.</i> Déplace les archives du dossier d'entrée (<code>inbound</code>) vers les dossiers de classification (<code>classified</code> ou <code>rejected</code>) en fonction de critères de contenu (ex: présence de mots-clés).
Scripts de Maintenance	<code>cleanup.sh</code>	Supprime automatiquement les fichiers trop anciens (par exemple, plus de 10 jours) pour nettoyer le volume RAID.
Preuve de Logique	<code>find_case.sh</code>	Script de validation qui permet à un inspecteur de vérifier rapidement où se trouve une archive donnée (dans <code>PENDING</code> , <code>ACCEPTED</code> , ou <code>REJECTED</code>).

Pour envoyer les mails, on a choisi de faire ainsi :

C. Messagerie

Objectif	Service/Configuration	Rôle dans l'Infrastructure
Envoi de Mails	Postfix	Installé et configuré pour utiliser le domaine <code>grestin.gov</code> . Il est utilisé pour envoyer des notifications (comme des alertes du système ou des confirmations de statut aux inspecteurs).

Configuration :

(L'adresse IP et la carte de sous réseaux ont déjà été faite)

On teste une connectivité entre les 2 machines (car sont dans le même sous réseaux) :

```
sysadmin@Router-Grestin: ~  
sysadmin@Router-Grestin:~$ ping -c 3 192.168.10.2  
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.  
64 bytes from 192.168.10.2: icmp_seq=1 ttl=64 time=5.61 ms  
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=2.31 ms  
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=1.22 ms  
  
--- 192.168.10.2 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 1.221/3.047/5.608/1.864 ms  
sysadmin@Router-Grestin:~$
```

Configure le DHCP : Affiche le sous-réseau 192.168.10.0/24, la plage d'IP, et le DNS pointant vers le routeur (192.168.10.1)

```
sysadmin@Router-Grestin:~$ cat /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
authoritative;
# Le reste du fichier doit être commenté ou supprimé

# Déclaration autoritaire
authoritative;

# Subnet interne pour les clients (inspecteurs)
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.100 192.168.10.200;
    option routers 192.168.10.1;
    option domain-name-servers 192.168.10.1;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Teste le DHCP :

```
sysadmin@Router-Grestin:~$ systemctl status isc-dhcp-server
● 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 Sat 2025-12-06 23:40:53 CET; 46min ago
     Docs: man:dhcpd(8)
    Main PID: 1780 (dhcpd)
      Tasks: 1 (limit: 2205)
     Memory: 5.3M (peak: 5.6M)
        CPU: 305ms
    CGroup: /system.slice/isc-dhcp-server.service
            └─1780 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

Dec 07 00:21:50 Router-Grestin dhcpd[1780]: DHCPREQUEST for 192.168.10.100 from 00:0c:29:3d:a8:49 (krishna-VMware)
Dec 07 00:21:50 Router-Grestin dhcpd[1780]: DHCPACK on 192.168.10.100 to 00:0c:29:3d:a8:49 (krishna-VMware)
Dec 07 00:26:21 Router-Grestin dhcpd[1780]: DHCPINFORM from 192.168.10.101 via ens34
Dec 07 00:26:21 Router-Grestin dhcpd[1780]: DHCPACK to 192.168.10.101 (00:50:56:c0:00:01) via ens34
Dec 07 00:26:21 Router-Grestin dhcpd[1780]: DHCPINFORM from 192.168.10.101 via ens34
Dec 07 00:26:21 Router-Grestin dhcpd[1780]: DHCPACK to 192.168.10.101 (00:50:56:c0:00:01) via ens34
Dec 07 00:26:23 Router-Grestin dhcpd[1780]: DHCPREQUEST for 192.168.10.101 from 00:50:56:c0:00:01 (DESKTOP-0KU1QL)
Dec 07 00:26:23 Router-Grestin dhcpd[1780]: DHCPACK on 192.168.10.101 to 00:50:56:c0:00:01 (DESKTOP-0KU1QL)
Dec 07 00:26:34 Router-Grestin dhcpd[1780]: DHCPREQUEST for 192.168.10.100 from 00:0c:29:3d:a8:49 (krishna-VMware)
Dec 07 00:26:34 Router-Grestin dhcpd[1780]: DHCPACK on 192.168.10.100 to 00:0c:29:3d:a8:49 (krishna-VMware)
```

(Il distribue bien des adresses IP)

Création du domaine :

```
sysadmin@Router-Grestin:~$ sudo cat /etc/bind/db.grestin.gov
[sudo] password for sysadmin:

;
$TTL 604800
@      IN  SOA  router-grestin.grestin.gov. sysadmin.grestin.gov. (
                        2025120602 ; <--- SERIAL (À incrémenter !)
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@      IN  NS   router-grestin.grestin.gov.
@      IN  A    192.168.10.1      ; IP du domaine (optionnel)

; Enregistrements A
router-grestin  IN A 192.168.10.1
server-internal IN A 192.168.10.2

; Enregistrement Mail Exchange (MX)
@      IN  MX   10 server-internal.grestin.gov.
```

Validation DNS (Résolution) : La résolution du nom de domaine vers l'IP interne (192.168.10.2) fonctionne, validant Bind9 :

```

sysadmin@Router-Grestin:~$ dig @127.0.0.1 server-internal.grestin.gov

; <<>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <<>> @127.0.0.1 server-internal.grestin.gov
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18854
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d6f6bf69bf5e97e1010000006934bc4590b5805e8a663037 (good)
;; QUESTION SECTION:
;server-internal.grestin.gov.      IN      A

;; ANSWER SECTION:
server-internal.grestin.gov. 604800 IN A      192.168.10.2

;; Query time: 43 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Dec 07 00:29:09 CET 2025
;; MSG SIZE rcvd: 100

```

Validation DNS (Syntaxe) : Les fichiers de zone DNS sont syntaxiquement corrects et ont été chargés :

```

sysadmin@Router-Grestin:~$ sudo named-checkzone grestin.gov /etc/bind/db.grestin.gov
[sudo] password for sysadmin:
zone grestin.gov/IN: loaded serial 2025120602
OK

```

Statut Firewall (Sécurité) : Le pare-feu est actif et autorise seulement les services nécessaires (DNS, DHCP, Mail, Samba) sur le réseau interne :

```

sysadmin@Router-Grestin:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To Action From
--
53/udp on ens34 ALLOW IN Anywhere
67/udp on ens34 ALLOW IN Anywhere
68/udp on ens34 ALLOW IN Anywhere
25/tcp on ens34 ALLOW IN Anywhere
445/tcp on ens34 ALLOW IN Anywhere
22/tcp on ens34 ALLOW IN Anywhere
53/udp (v6) on ens34 ALLOW IN Anywhere (v6)
67/udp (v6) on ens34 ALLOW IN Anywhere (v6)
68/udp (v6) on ens34 ALLOW IN Anywhere (v6)
25/tcp (v6) on ens34 ALLOW IN Anywhere (v6)
445/tcp (v6) on ens34 ALLOW IN Anywhere (v6)
22/tcp (v6) on ens34 ALLOW IN Anywhere (v6)

```

Statut RAID et Montage : Le volume RAID (/dev/md0) est correctement formaté et monté sur le point de montage des archives :

```

krishna@krishna-VMware-Virtual-Platform: ~
krishna@krishna-VMware-Virtual-Platform:~$ df -h /srv/files
Filesystem      Size  Used Avail Use% Mounted on
/dev/md0        4.9G   8.0K  4.6G   1% /srv/files

```

Création d'Utilisateur : L'utilisateur inspector1 (nécessaire pour Samba et les scripts) existe :

```

krishna@krishna-VMware-Virtual-Platform:~$ id inspector1
uid=1002(inspector1) gid=1002(inspector1) groups=1002(inspector1),100(users)
krishna@krishna-VMware-Virtual-Platform:~$

```

Statut Samba : Le service de partage de fichiers est actif et prêt à accepter les connexions (permet aux inspecteurs d'accéder à /srv/files) :

```
krishna@krishna-VMware-Virtual-Platform:~$ systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smbd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-12-06 17:58:25 CET; 6h ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Main PID: 3888 (smbd)
    Status: "smbd: ready to serve connections..."
     Tasks: 3 (limit: 2207)
    Memory: 7.6M (peak: 8.5M)
       CPU: 7.419s
    CGroup: /system.slice/smbd.service
            └─3888 /usr/sbin/smbd --foreground --no-process-group
              └─3891 "smbd: notifyd"
                └─3892 "smbd: cleanupd"

Dec 06 17:58:25 krishna-VMware-Virtual-Platform systemd[1]: Starting smbd.service - Samba SMB Daemon...
Dec 06 17:58:25 krishna-VMware-Virtual-Platform (smbd)[3888]: smbd.service: Referenced but unset environme>
Dec 06 17:58:25 krishna-VMware-Virtual-Platform systemd[1]: Started smbd.service - Samba SMB Daemon.
lines 1-19/19 (END)
```

Nom de Domaine Mail : Le serveur de messagerie Postfix est correctement configuré pour utiliser le domaine grestin.gov :

```
krishna@krishna-VMware-Virtual-Platform:~$ postconf myhostname
myhostname = grestin.gov
```

Planification (Cron) : Les deux scripts de flux et de maintenance sont planifiés pour s'exécuter automatiquement chaque jour :

```
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow  command
# Nettoyage à minuit
0 0 * * * /usr/local/bin/cleanup.sh
# Transfert à minuit et 15 minutes
15 0 * * * /usr/local/bin/transfer.sh
```

Logique du Script de Flux : Affiche la logique de tri (recherche de mot-clé, déplacement vers classified ou rejected, journalisation) :

```
krishna@krishna-VMware-Virtual-Platform:~$ cat /usr/local/bin/transfer.sh
#!/bin/bash

INBOUND_DIR="/srv/files/inbound"
CLASSIFIED_DIR="/srv/files/classified"
REJECTED_DIR="/srv/files/rejected"
LOG_FILE="/var/log/transfer.log"

# Traiter chaque fichier dans inbound
for file in "$INBOUND_DIR"/*; do
    if [ -f "$file" ]; then # Vérifie que c'est un fichier et non un répertoire
        filename=$(basename "$file")

        # Logique de Classification : Recherche du mot "Arms"
        if grep -q "Arms" "$file"; then
            # Déplace vers REJECTED et log
            mv "$file" "$REJECTED_DIR/$filename"
            echo "$(date) REJECTED: $filename (Contient Arms)" >> "$LOG_FILE"
        else
            # Déplace vers CLASSIFIED et log
            mv "$file" "$CLASSIFIED_DIR/$filename"
            echo "$(date) CLASSIFIED: $filename" >> "$LOG_FILE"
        fi
    fi
done
```

Logique Script de Nettoyage : Affiche la logique pour supprimer les fichiers anciens (maintenance) :

```
krishna@krishna-VMware-Virtual-Platform:~$ cat /usr/local/bin/cleanup.sh
#!/bin/bash

# Supprime les fichiers (non répertoires) de plus de 10 jours
find /srv/files/ -type f -mtime +10 -delete

# Supprime les répertoires vides
find /srv/files/ -type d -empty -delete
```

Preuve de Logique Inspecteur : Le script de recherche confirme que le système est capable de dire si une archive est ACCEPTED, REJECTED, ou PENDING (prouve l'exploitabilité de la logique de flux) :

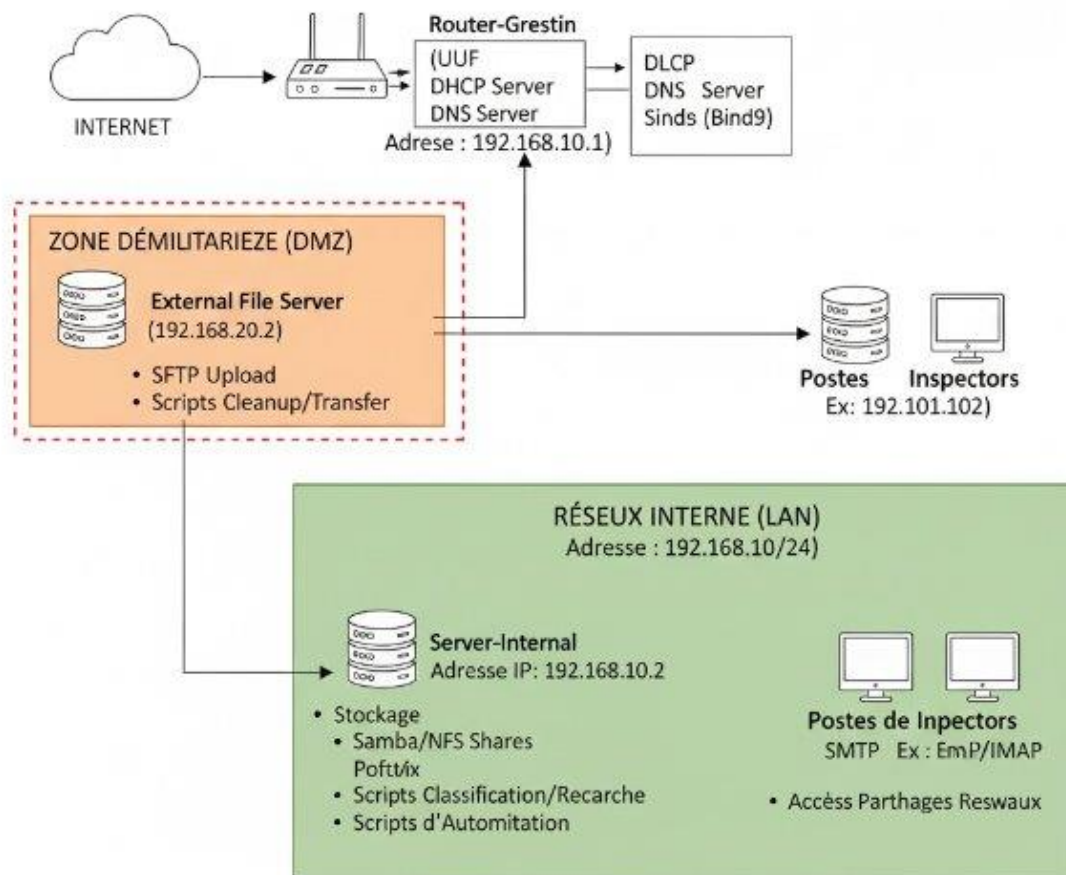
```
krishna@krishna-VMware-Virtual-Platform:~$ cat /usr/local/bin/find_case.sh

#!/bin/bash
ID=$1
if [ -z "$ID" ]; then
    echo "Usage: $0 [ID_DU_CAS]"
    exit 1
fi

if [ -d "/srv/files/classified/$ID" ]; then
    echo "ARCHIVE $ID : ACCEPTED"
elif [ -d "/srv/files/rejected/$ID" ]; then
    echo "ARCHIVE $ID : REJECTED"
elif [ -d "/srv/files/inbound/$ID" ]; then
    echo "ARCHIVE $ID : PENDING"
else
    echo "ARCHIVE $ID : INCONNUE"
fi
```

Structure du réseau :

Architecture du Système d'Control Frontalier Numériquee de Grestin



Schema based ou Linux Distribution (ex. Ubuntu Server)

Objectiv : Sécurité, Redomaitation