RAPPORT PROJET LPIC 102

Ensemble des commandes, des fichiers de configuration, des tests concernant le projet.

CHARPIGNON NICOLAS ET CHAPRON MAXIME

Nous avons installé deux systèmes débian, un serveur debian 12 sans interface graphique (Comme cela se produit dans le milieu professionnel) et un debian client avec GUI.

Sur un system débian, il n'y a pas sudo d'installé en mode minimum :

```
max@debian:~$ su -
Password:
root@debian:~# apt install sudo
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sudo is already the newest version (1.9.13p3-1+deb12u2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@debian:~# usermod -aG max sudo
usermod: user 'sudo' does not exist
root@debian:~# usermod -aG sudo max
root@debian:~#
```

Nous avons fixé l'ip comme cela est d'usage sur un serveur :

```
max@debian:~$ sudo nano /etc/network/interfaces
max@debian:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
        address 192.168.120.130/24
        gateway 192.168.120.2
        dns-nameserver 8.8.8.8 8.8.4.4
```

1 – NTP : Installation via le script suivant :

```
max@debian:~$ nano chrony.sh
max@debian:~$ chmod +x chrony.sh
```

Exécution avec privilèges :

```
max@debian:~$ ./chrony.sh
Veuillez exécuter ce script avec sudo ou en tant que root.
```

```
  GNU nano 7.2                                                    chrony.sh
#!/bin/bash

# Arrête le script immédiatement si une commande échoue
set -e

# -- Vérification des droits root --
if [ "$(id -u)" -ne 0 ]; then
  echo "Veuillez exécuter ce script avec sudo ou en tant que root." >&2
  exit 1
fi

# --- 1. Installation ---
echo "Installation de Chrony..."
sudo apt-get update
sudo apt-get install -y chrony

# --- 2. Configuration des serveurs NTP ---
echo "Configuration des serveurs NTP dans /etc/chrony/chrony.conf..."
CONF_FILE="/etc/chrony/chrony.conf"

# Commente les lignes "pool" et "server" existantes pour éviter les conflits
sudo sed -i 's/^\(pool\|server\)/#\1/' "$CONF_FILE"

# Ajoute les nouveaux serveurs à la fin du fichier
# Note : on utilise "tee -a" pour écrire dans un fichier avec sudo
echo "
# Serveurs NTP pour la France
server 0.fr.pool.ntp.org iburst
server 1.fr.pool.ntp.org iburst
server 2.fr.pool.ntp.org iburst
server 3.fr.pool.ntp.org iburst
" | sudo tee -a "$CONF_FILE" > /dev/null

# --- 3. Configuration de l'accès local ---
echo "Autorisation du réseau local..."
ALLOW_LINE="allow 192.168.120.0/24"

# Vérifie si la ligne existe déjà avant de l'ajouter
if grep -qFx "$ALLOW_LINE" "$CONF_FILE"; then
    echo "La règle d'autorisation existe déjà."
else
    echo "$ALLOW_LINE" | sudo tee -a "$CONF_FILE" > /dev/null
    echo "Règle d'autorisation ajoutée."
fi

# --- 4. Redémarrage et vérification ---
echo "Redémarrage du service Chrony..."
sudo systemctl restart chrony
# Laisse un peu de temps à Chrony pour se connecter
sleep 20

echo "Vérification du statut de Chrony :"
sudo chronyc tracking
echo "-------------------------------------"
echo "Sources de synchronisation actuelles :"
sudo chronyc sources
echo "Clients connectés au serveur :"
sudo chronyc clients


echo "Configuration de Chrony terminée avec succès !"
```

```
max@debian:~$ sudo ./chrony.sh
Installation de Chrony...
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
chrony is already the newest version (4.3-2+deb12u1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Configuration des serveurs NTP dans /etc/chrony/chrony.conf...
Autorisation du réseau local...
La règle d'autorisation existe déjà.
Redémarrage du service Chrony...
Vérification du statut de Chrony :
Reference ID    : 253B3F7D (37.59.63.125)
Stratum         : 3
Ref time (UTC)  : Thu Jul 24 19:41:49 2025
System time     : 0.000006166 seconds fast of NTP time
Last offset     : +0.000006223 seconds
RMS offset      : 0.000006223 seconds
Frequency       : 0.742 ppm fast
Residual freq   : +68.840 ppm
Skew            : 0.537 ppm
Root delay      : 0.023938555 seconds
Root dispersion : 0.002282159 seconds
Update interval : 1.8 seconds
Leap status     : Normal
-------------------------------------
Sources de synchronisation actuelles :
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- 82-64-81-218.subs.proxad>     2   6    17    13  +2212us[+2212us] +/-   67ms
^+ vps-mrs1.orleans.ddnss.de     2   6    17    14   -170us[ -164us] +/-   19ms
^* 37.59.63.125                  2   6    17    13   -598us[ -592us] +/-   13ms
^+ ntp.tuxfamily.net             2   6    17    14  +1315us[+1321us] +/-   38ms
Clients connectés au serveur :
Hostname                      NTP   Drop Int IntL Last     Cmd   Drop Int  Last
===============================================================================
192.168.120.131                 1      0   -   -    18       0      0   -     -
Configuration de Chrony terminée avec succès !
max@debian:~$
```

Synchro OK + client en 192.168.120.131 connecté au serveur car le réseau local est autorisé

Vérification du service :

```
max@debian:~$ sudo systemctl status chrony
● chrony.service - chrony, an NTP client/server
     Loaded: loaded (/lib/systemd/system/chrony.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-07-24 19:41:42 UTC; 11min ago
       Docs: man:chronyd(8)
             man:chronyc(1)
             man:chrony.conf(5)
    Process: 7104 ExecStart=/usr/sbin/chronyd $DAEMON_OPTS (code=exited, status=0/SUCCESS)
   Main PID: 7106 (chronyd)
      Tasks: 2 (limit: 2258)
     Memory: 1.4M
        CPU: 63ms
     CGroup: /system.slice/chrony.service
             ├─7106 /usr/sbin/chronyd -F 1
             └─7107 /usr/sbin/chronyd -F 1
```

2- Postfix :

Création d'un fichier secret.env protégé pour ne pas mettre les infos dans le script :

```
max@debian:~$ sudo nano /root/secret.env
max@debian:~$ sudo chmod 600 /root/secret.env
```

```
  GNU nano 7.2                                                    /root/secret.env
GMAIL_USER="le[redacted]@gmail.com"
GMAIL_APP_PASS="[redacted]
MAIL_TEST="chap[redacted]@gmail.com"
```

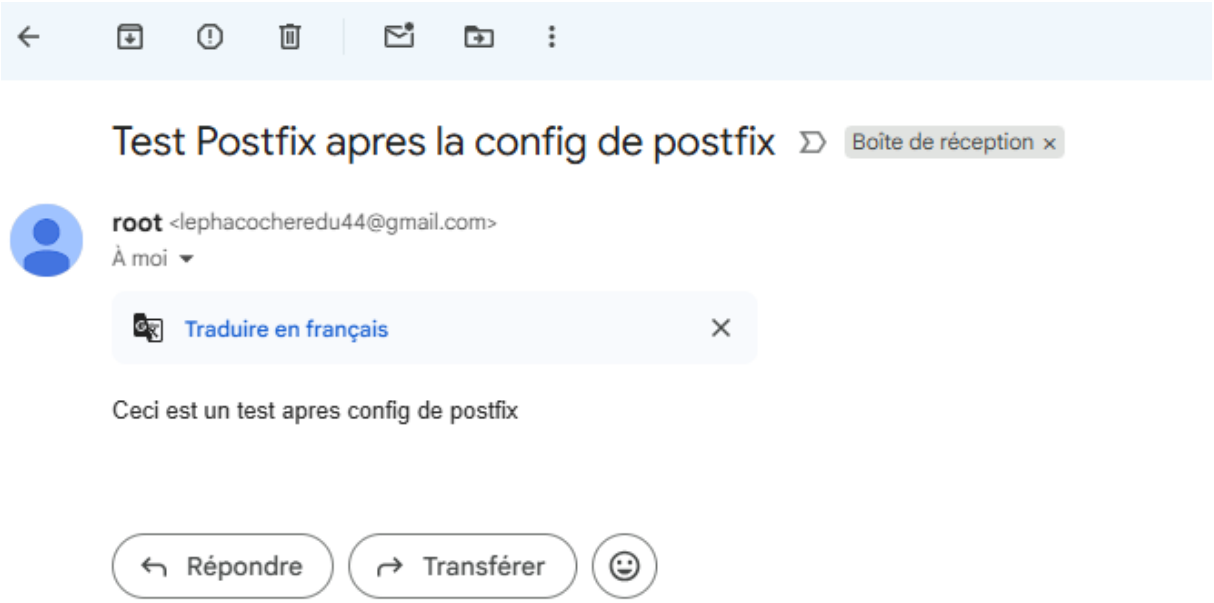
```
max@debian:~$ nano postfix.sh
max@debian:~$ chmod +x postfix.sh
```

```
  GNU nano 7.2                                                    postfix.sh
#!/bin/bash

set -e

# -- Chargement des secrets
if [ ! -f /root/secret.env ]; then
  echo "Fichier /root/secret.env introuvable." >&2
  exit 1
fi

source /root/secret.env

# -- Variables fixes
RELAY_HOST="[smtp.gmail.com]:587"
MY_HOSTNAME="debian.localdomain"
MY_NETWORKS="127.0.0.0/8 192.168.120.0/24 [::ffff:127.0.0.0]/104 [::1]/128"

# -- Vérification des droits root
if [ "$(id -u)" -ne 0 ]; then
  echo "Veuillez exécuter ce script avec sudo ou en tant que root." >&2
  exit 1
fi

echo "--- Début de la configuration de Postfix ---"
echo "Installation de Postfix..."

debconf-set-selections <<< "postfix postfix/main_mailer_type select Satellite system"
debconf-set-selections <<< "postfix postfix/mailname string $MY_HOSTNAME"
debconf-set-selections <<< "postfix postfix/relayhost string $RELAY_HOST"

apt-get update
apt-get install -y postfix mailutils

echo "Configuration des paramètres principaux (main.cf)..."
postconf -e "myhostname = $MY_HOSTNAME"
postconf -e "alias_maps = hash:/etc/aliases"
postconf -e "alias_database = hash:/etc/aliases"
postconf -e "mydestination = \$myhostname, debian, localhost.localdomain, , localhost"
postconf -e "relayhost = $RELAY_HOST"
postconf -e "mynetworks = $MY_NETWORKS"
postconf -e "inet_interfaces = all"
postconf -e "inet_protocols = ipv4"
postconf -e "smtp_sasl_auth_enable = yes"
postconf -e "smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd"
postconf -e "smtp_sasl_security_options = noanonymous"
postconf -e "smtp_use_tls = yes"
postconf -e "smtp_tls_CApath = /etc/ssl/certs"

echo "Création du fichier de mot de passe SASL..."
echo "$RELAY_HOST    $GMAIL_USER:$GMAIL_APP_PASS" > /etc/postfix/sasl_passwd
chmod 600 /etc/postfix/sasl_passwd
postmap /etc/postfix/sasl_passwd

echo "Redémarrage de Postfix..."
systemctl restart postfix

echo "Configuration de Postfix terminée avec succès."
echo "mail de test envoyé sur $MAIL_TEST"
echo "Ceci est un test apres config de postfix" | mail -s "Test Postfix apres la config de postfix" "$MAIL_TEST"
```

```
max@debian:~$ sudo ./postfix.sh
--- Début de la configuration de Postfix ---
Installation de Postfix...
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://security.debian.org/debian-security bookworm-security InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
postfix is already the newest version (3.7.11-0+deb12u1).
mailutils is already the newest version (1:3.15-4).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Configuration des paramètres principaux (main.cf)...
Création du fichier de mot de passe SASL...
Redémarrage de Postfix pour appliquer toutes les configurations...
Configuration de Postfix terminée avec succès !
Email de test envoyé
max@debian:~$
```

```
2025-07-24T19:51:25.953781+00:00 debian postfix/master[8341]: daemon started -- version 3.7.11, configuration /etc/postfix
2025-07-24T19:51:26.013391+00:00 debian postfix/pickup[8342]: 032B62964F: uid=0 from=<root@debian>
2025-07-24T19:51:26.019023+00:00 debian postfix/cleanup[8349]: 032B62964F: message-id=<20250724195126.032B62964F@debian.localdomain>
2025-07-24T19:51:26.019802+00:00 debian postfix/qmgr[8343]: 032B62964F: from=<root@debian>, size=403, nrcpt=1 (queue active)
2025-07-24T19:51:27.028139+00:00 debian postfix/smtp[8351]: 032B62964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1, del
ays=0.01/0.02/0.48/0.51, dsn=2.0.0, status=sent (250 2.0.0 OK  1753386687 ffacd0b85a97d-3b76fcad29dsm2973286f8f.49 - gsmtp)
2025-07-24T19:51:27.028767+00:00 debian postfix/qmgr[8343]: 032B62964F: removed
max@debian:~$
```

Mail reçu sur Gmail :



Vérification du service ok:

```
max@debian:~$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/lib/systemd/system/postfix.service; enabled; preset: enabled)
     Active: active (exited) since Thu 2025-07-24 19:51:25 UTC; 1min 21s ago
       Docs: man:postfix(1)
    Process: 8344 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 8344 (code=exited, status=0/SUCCESS)
        CPU: 989us

Jul 24 19:51:25 debian systemd[1]: Starting postfix.service - Postfix Mail Transport Agent...
Jul 24 19:51:25 debian systemd[1]: Finished postfix.service - Postfix Mail Transport Agent.
```

Script d'envoi de mail :

```
root@debian:/usr/local/bin# nano send_alert.sh
root@debian:/usr/local/bin# chmod +x send_alert.sh
```

```
  GNU nano 7.2                                                    send_alert.sh
#!/bin/bash

EVENT_TYPE="$1"
RECIPIENT="chapron.maxime@gmail.com"
SENDER="lephacocheredu44@gmail.com"

# Utilise une structure "case" pour gérer les différents événements
case "$EVENT_TYPE" in
  "login_failure")
    SUBJECT="Alerte de Sécurité: Connexion échouée"
    BODY="Une tentative de connexion a échoué.
Utilisateur: $PAM_USER
Depuis l'IP: $PAM_RHOST
Service: $PAM_SERVICE"
    ;;
  "password_change")
    SUBJECT="Alerte de Sécurité: Mot de passe modifié"
    BODY="Le mot de passe a été changé pour l'utilisateur: $PAM_USER
Service: $PAM_SERVICE"
    ;;
  "reboot")
    SUBJECT="Information: Redémarrage du serveur"
    # Note: les variables PAM ne sont pas disponibles ici
    BODY="Le serveur a redémarré le $(date)"
    ;;
  *)
    # Au cas où le type d'événement est inconnu
    SUBJECT="Alerte Système Inconnue"
    BODY="Un événement non identifié a été déclenché."
    ;;
esac

# Envoi du mail
echo "$BODY" | mail -s "$SUBJECT" -a "From: Serveur Debian <$SENDER>" "$RECIPIENT"
```

Ce script est appelé plus tard (partie 4 dans sécurité avec PAM).

Nous avons dû créer un service :

```
max@debian:~$ sudo nano /etc/systemd/system/reboot-alert.service
max@debian:~$
```

```
  GNU nano 7.2                                  /etc/systemd/system/reboot-alert.service
[Unit]
Description=Envoi d'une alerte mail au redémarrage
After=network-online.target

[Service]
Type=oneshot
ExecStart=/usr/local/bin/send_alert.sh reboot

[Install]
WantedBy=multi-user.target
```

```
max@debian:~$ sudo systemctl status reboot-alert.service
o reboot-alert.service - Envoi d'une alerte mail au redémarrage
     Loaded: loaded (/etc/systemd/system/reboot-alert.service; enabled; preset: enabled)
     Active: inactive (dead) since Thu 2025-07-24 15:34:45 UTC; 4h 26min ago
   Main PID: 696 (code=exited, status=0/SUCCESS)
        CPU: 121ms

Jul 24 15:34:42 debian systemd[1]: Starting reboot-alert.service - Envoi d'une alerte mail au redémarrage...
Jul 24 15:34:45 debian systemd[1]: reboot-alert.service: Deactivated successfully.
Jul 24 15:34:45 debian systemd[1]: Finished reboot-alert.service - Envoi d'une alerte mail au redémarrage.
max@debian:~$
```

3- Fuseau hoaire :

```
max@debian:~$ sudo timedatectl set-timezone Asia/Tokyo
max@debian:~$ timedatectl
               Local time: Fri 2025-07-25 05:04:55 JST
           Universal time: Thu 2025-07-24 20:04:55 UTC
                 RTC time: Thu 2025-07-24 20:04:55
                Time zone: Asia/Tokyo (JST, +0900)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
max@debian:~$
```

```
max@debian:~$ sudo apt install locales -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
locales is already the newest version (2.36-9+deb12u10).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
max@debian:~$ sudo nano /etc/locale.gen
```

On décommente les lignes

```
de_DE.UTF-8 UTF-8
```

```
es_ES.UTF-8 UTF-8
```

```
it_IT.UTF-8 UTF-8
```

On génere et on check si c’est ok :

```
max@debian:~$ sudo locale-gen
Generating locales (this might take a while)...
  de_DE.UTF-8... done
  en_US.UTF-8... done
  es_ES.UTF-8... done
  it_IT.UTF-8... done
Generation complete.
max@debian:~$ locale -a
C
C.utf8
POSIX
de_DE.utf8
en_US.utf8
es_ES.utf8
it_IT.utf8
max@debian:~$
```

4 – PAM

Securisation du changement de mdp :

```
max@debian:~$ sudo apt install libpam-pwquality
```

```
max@debian:~$ sudo nano /etc/pam.d/common-password
```

#ucredit 1 majuscule minimum, lcredit 1 minuscule minimum, dcredit 1 chiffre minimum, ocredit 1 caractere special minimum.

```
# here are the per-package modules (the "Primary" block)
#ucredit maj, lcredit minusc, dcredit chiffre, ocredit caract special
password        requisite                       pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config

password   optional   pam_exec.so /usr/local/bin/send_alert.sh password_change
```

Modification de ces fichiers pour le blocage des comptes :

```
max@debian:~$ sudo nano /etc/pam.d/common-auth
```

```
auth required pam_faillock.so preauth silent deny=3 unlock_time=600
auth [success=2 default=ignore] pam_unix.so nullok
auth optional pam_exec.so /usr/local/bin/send_alert.sh Failed Login A failed login attempt has occurred
auth [default=die] pam_faillock.so authfail deny=3 unlock_time=600
auth sufficient pam_faillock.so authsucc deny=3 unlock_time=600
```

```
max@debian:~$ sudo nano /etc/security/time.conf
```

Paramétrage ici pour le groupe étudiant qui a le droit de se connecter uniquement du lundi au jeudi de 8h a 18h (pour la démo du vendredi à la soutenance)

Les fichiers /etc/pam.d/sshd et /etc/pam.d/login sont modifié pour que time.d s'applique uniquement au groupe etudiant. (Bonne pratique de géré par groupe et non par user ou pour tout le monde)

Explication de la logique pour /etc/pam.d/sshd et /etc/pam.d/login en commentaire dans les fichiers.

```
  GNU nano 7.2                    /etc/security/time.conf
sshd;*;*;MoTuWeTh0800-1800
login;*;*;MoTuWeTh0800-1800
```

```
  GNU nano 7.2                                                    /etc/pam.d/sshd *
# PAM configuration for the Secure Shell service

# Standard Un*x authentication.
@include common-auth

# Disallow non-root logins when /etc/nologin exists.
account    required     pam_nologin.so

# Si l'utilisateur N'EST PAS un étudiant, on saute la règle de temps suivante
account [success=1 default=ignore] pam_succeed_if.so user notingroup etudiants
# Cette règle de temps ne s'applique donc QUE pour le groupe "etudiants"
account required     pam_time.so

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account  required     pam_access.so

# Standard Un*x authorization.
@include common-account

# SELinux needs to be the first session rule.  This ensures that any
# lingering context has been cleared.  Without this it is possible that a
# module could execute code in the wrong domain.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so close

# Set the loginuid process attribute.
session    required     pam_loginuid.so

# Create a new session keyring.
session    optional     pam_keyinit.so force revoke

# Standard Un*x session setup and teardown.
@include common-session

# Print the message of the day upon successful login.
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional     pam_motd.so  motd=/run/motd.dynamic
session    optional     pam_motd.so noupdate

# Print the status of the user's mailbox upon successful login.
session    optional     pam_mail.so standard noenv # [1]

# Set up user limits from /etc/security/limits.conf.
session    required     pam_limits.so

# Read environment variables from /etc/environment and
# /etc/security/pam_env.conf.
session    required     pam_env.so # [1]
# In Debian 4.0 (etch), locale-related environment variables were moved to
# /etc/default/locale, so read that as well.
session    required     pam_env.so user_readenv=1 envfile=/etc/default/locale

# SELinux needs to intervene at login time to ensure that the process starts
# in the proper default security context.  Only sessions which are intended
# to run in the user's context should be run after this.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so open

# Standard Un*x password updating.
@include common-password
```

```
  GNU nano 7.2                                                    /etc/pam.d/login *
#
# The PAM configuration file for the Shadow `login' service
#

# Enforce a minimal delay in case of failure (in microseconds).
# (Replaces the `FAIL_DELAY' setting from login.defs)
# Note that other modules may require another minimal delay. (for example,
# to disable any delay, you should add the nodelay option to pam_unix)
auth       optional   pam_faildelay.so  delay=3000000

# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth       required   pam_issue.so issue=/etc/issue

# Disallows other than root logins when /etc/nologin exists
# (Replaces the `NOLOGINS_FILE' option from login.defs)
auth       requisite  pam_nologin.so

# SELinux needs to be the first session rule. This ensures that any
# lingering context has been cleared. Without this it is possible
# that a module could execute code in the wrong domain.
# When the module is present, "required" would be sufficient (When SELinux
# is disabled, this returns success.)
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so close

# Sets the loginuid process attribute
session    required     pam_loginuid.so

# Prints the message of the day upon successful login.
# (Replaces the `MOTD_FILE' option in login.defs)
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional   pam_motd.so motd=/run/motd.dynamic
session    optional   pam_motd.so noupdate

# SELinux needs to intervene at login time to ensure that the process
# starts in the proper default security context. Only sessions which are
# intended to run in the user's context should be run after this.
# pam_selinux.so changes the SELinux context of the used TTY and configures
# SELinux in order to transition to the user context with the next execve()
# call.
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so open
# When the module is present, "required" would be sufficient (When SELinux
# is disabled, this returns success.)

# This module parses environment configuration file(s)
# and also allows you to use an extended config
# file /etc/security/pam_env.conf.
#
# parsing /etc/environment needs "readenv=1"
session       required   pam_env.so readenv=1
# locale variables are also kept into /etc/default/locale in etch
# reading this file *in addition to /etc/environment* does not hurt
session       required   pam_env.so readenv=1 envfile=/etc/default/locale

# Standard Un*x authentication.
@include common-auth

# This allows certain extra groups to be granted to a user
# based on things like time of day, tty, service, and user.
# Please edit /etc/security/group.conf to fit your needs
# (Replaces the `CONSOLE_GROUPS' option in login.defs)
auth       optional   pam_group.so

# Uncomment and edit /etc/security/time.conf if you need to set
# time restraint on logins.
# (Replaces the `PORTTIME_CHECKS_ENAB' option from login.defs
# as well as /etc/porttime)

# Si l'utilisateur N'EST PAS un étudiant, on saute la règle de temps suivante
account [success=1 default=ignore] pam_succeed_if.so user notingroup etudiants
# Cette règle de temps ne s'applique donc QUE pour le groupe "etudiants"
account    requisite  pam_time.so

# Uncomment and edit /etc/security/access.conf if you need to
# set access limits.
# (Replaces /etc/login.access file)
account  required       pam_access.so
```

```
max@debian:~$ sudo nano /etc/login.defs
```

```
PASS_MAX_DAYS   60
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

5 – X11

```
root@debian:/etc/pam.d# sudo apt install -y xauth x11-apps
```

```
X11Forwarding yes
X11DisplayOffset 10
X11UseLocalhost yes
```

```
root@debian:/etc/pam.d# sudo systemctl restart ssh
```

Script .py

```
  GNU nano 7.2                                                    postfix_pam_logs.py
import tkinter as tk
from tkinter import ttk, filedialog
import time
import psutil
import json
import csv

def get_time():
    return time.strftime("%Y-%m-%d %H:%M:%S", time.localtime())

def get_system_info():
    cpu = psutil.cpu_percent()
    ram = psutil.virtual_memory().percent
    return f"CPU: {cpu}% | RAM: {ram}% | Réseau: {current_net_speed:.2f} Mo/s"

def update_dashboard():
    time_var.set(get_time())
    system_var.set(get_system_info())
    root.after(1000, update_dashboard)

def read_logs(file_path, filter_text=""):
    try:
        with open(file_path, 'r') as f:
            lines = f.readlines()
            if filter_text:
                lines = [line for line in lines if filter_text in line]
            return lines[-50:]
    except:
        return ["Impossible de lire le fichier."]

def refresh_logs():
    pam_logs = read_logs("/var/log/auth.log", pam_filter.get())
    postfix_logs = read_logs("/var/log/mail.log", postfix_filter.get())
    pam_text.delete(1.0, tk.END)
    postfix_text.delete(1.0, tk.END)
    pam_text.insert(tk.END, "".join(pam_logs))
    postfix_text.insert(tk.END, "".join(postfix_logs))

def export_logs(format_):
    logs = {
        "pam": read_logs("/var/log/auth.log", pam_filter.get()),
        "postfix": read_logs("/var/log/mail.log", postfix_filter.get())
    }
    path = filedialog.asksaveasfilename(defaultextension=f".{format_}")
    if not path:
        return
    with open(path, 'w') as f:
        if format_ == "json":
            json.dump(logs, f, indent=4)
        else:
            writer = csv.writer(f)
            for key, lines in logs.items():
                writer.writerow([f"### {key.upper()} ###"])
                for line in lines:
                    writer.writerow([line.strip()])

# Initialisation interface
root = tk.Tk()
root.title("Tableau de bord système")

time_var = tk.StringVar()
system_var = tk.StringVar()
pam_filter = tk.StringVar()
postfix_filter = tk.StringVar()

tk.Label(root, textvariable=time_var, font=("Arial", 14)).pack()
tk.Label(root, textvariable=system_var, font=("Arial", 12)).pack()

frame = tk.Frame(root)
frame.pack(pady=5)

tk.Label(frame, text="Filtre PAM:").grid(row=0, column=0)
tk.Entry(frame, textvariable=pam_filter).grid(row=0, column=1)
tk.Label(frame, text="Filtre Postfix:").grid(row=0, column=2)
tk.Entry(frame, textvariable=postfix_filter).grid(row=0, column=3)

tk.Button(frame, text="Actualiser les logs", command=refresh_logs).grid(row=1, column=0, columnspan=2)
tk.Button(frame, text="Exporter en CSV", command=lambda: export_logs("csv")).grid(row=1, column=2)
tk.Button(frame, text="Exporter en JSON", command=lambda: export_logs("json")).grid(row=1, column=3)
```

```python
pam_text = tk.Text(root, height=10, width=100)
pam_text.pack(pady=5)
postfix_text = tk.Text(root, height=10, width=100)
postfix_text.pack(pady=5)

graph_canvas = tk.Canvas(root, width=800, height=250, bg="white")
graph_canvas.pack(pady=10)

legend = tk.Label(root, text="CPU (rouge, %), RAM (bleu, %), Réseau (vert, x3 zoom, Mo/s)", font=("Arial", 10))
legend.pack()

# Historique des données système
cpu_history = []
ram_history = []
net_history = []

last_net_bytes = psutil.net_io_counters().bytes_sent + psutil.net_io_counters().bytes_recv
current_net_speed = 0.0  # Mo/s

def update_graph():
    global last_net_bytes, current_net_speed

    cpu = psutil.cpu_percent()
    ram = psutil.virtual_memory().percent
    total_now = psutil.net_io_counters().bytes_sent + psutil.net_io_counters().bytes_recv
    current_net_speed = (total_now - last_net_bytes) / 1024 / 1024  # en Mo/s
    last_net_bytes = total_now

    cpu_history.append(cpu)
    ram_history.append(ram)
    net_history.append(current_net_speed)
    if len(cpu_history) > 100:
        cpu_history.pop(0)
        ram_history.pop(0)
        net_history.pop(0)

    graph_canvas.delete("all")

    net_max = max(1, max(net_history, default=1))
    net_zoom_factor = 3.0

    width = int(graph_canvas['width'])
    height = int(graph_canvas['height'])
    step = width / 100

    # Axes Y CPU/RAM
    for val in [0, 25, 50, 75, 100]:
        y = height - (val / 100) * height
        graph_canvas.create_line(0, y, width, y, fill="#eee")
        graph_canvas.create_text(10, y, anchor="nw", text=f"{val}%", font=("Arial", 8), fill="gray")

    # Axes Y réseau (échelle après zoom)
    for val in range(1, int(net_max) + 1):
        y = height - ((val * net_zoom_factor) / net_max) * height
        graph_canvas.create_line(0, y, width, y, fill="#f0f0f0")
        graph_canvas.create_text(width - 50, y, anchor="nw", text=f"{val} Mo/s", font=("Arial", 8), fill="gray")

    def draw_line(data, color, max_val, zoom=1.0):
        for i in range(1, len(data)):
            x1 = (i - 1) * step
            x2 = i * step
            y1 = height - ((data[i - 1] * zoom) / max_val) * height
            y2 = height - ((data[i] * zoom) / max_val) * height
            graph_canvas.create_line(x1, y1, x2, y2, fill=color, width=2)

    draw_line(cpu_history, "red", 100)
    draw_line(ram_history, "blue", 100)
    draw_line(net_history, "green", net_max, zoom=net_zoom_factor)

    root.after(1000, update_graph)

# Lancer les mises à jour
update_dashboard()
update_graph()
root.mainloop()
```

Connexion en SSH depuis mon debian client :

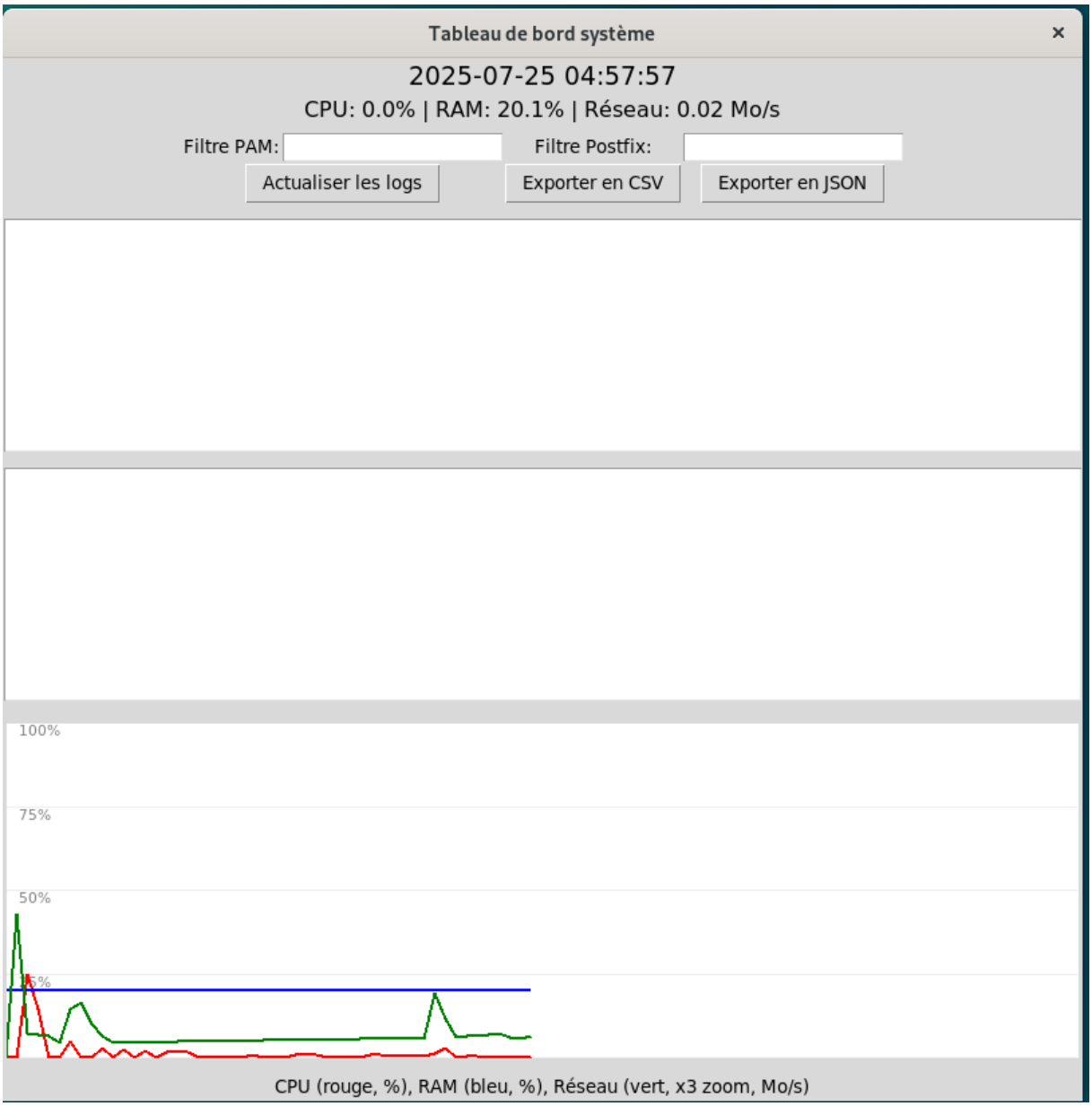
Ubuntu 64-bit | Debian 12 S6 | Debian12-client

Activities Terminal

max@debian: ~

```
client@debian-client:~$ hostname
debian-client
client@debian-client:~$ ip a
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:29:63:27:1e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.120.131/24 brd 192.168.120.255 scope global dynamic noprefixroute ens33
       valid_lft 1107sec preferred_lft 1107sec
    inet6 fe80::20c:29ff:fe63:271e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
client@debian-client:~$ ssh -X max@192.168.120.130
max@192.168.120.130's password:
Linux debian 6.1.0-37-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.140-1 (2025-05-22) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Jul 25 04:54:27 2025 from 192.168.120.131
max@debian:~$ python3
.cache/              .local/              .ssh/                postfix_pam_logs.py
max@debian:~$ python3 postfix_pam_logs.py
```

Ouverture de ma fenetre X11 :



Choix de mots clés pour filtrer les logs, et les variables cpu, ram et réseau (consommation de bande passante en temps réel s'affichent en valeur et sur des courbes) :

Test export JSON ET CSV :

Tableau de bord système

2025-07-25 05:02:22

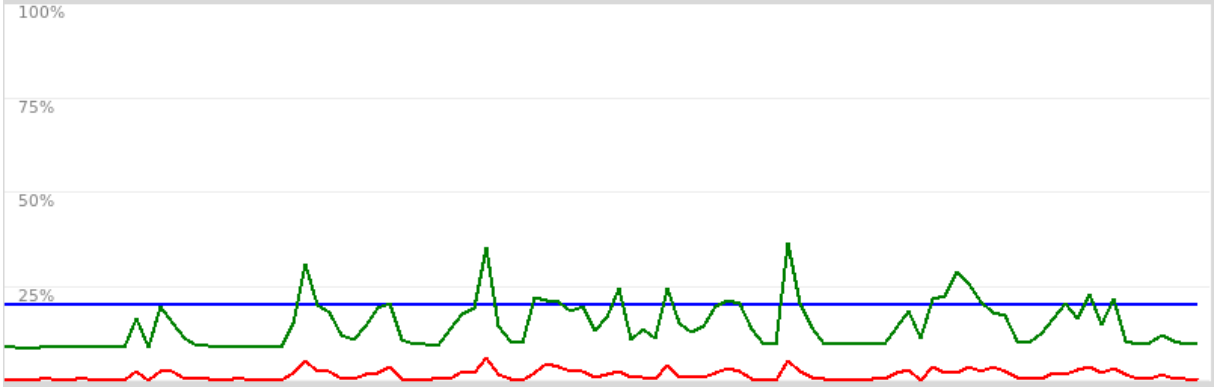
CPU: 60.0% | RAM: 20.0% | Réseau: 0.03 Mo/s

Filtre PAM: user2 Filtre Postfix: relayS

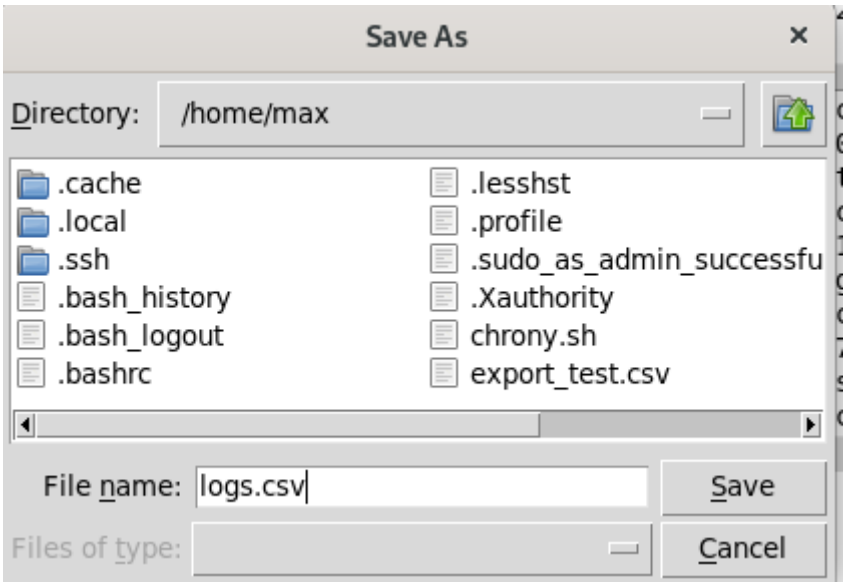
Actualiser les logs | Exporter en CSV | Exporter en JSON

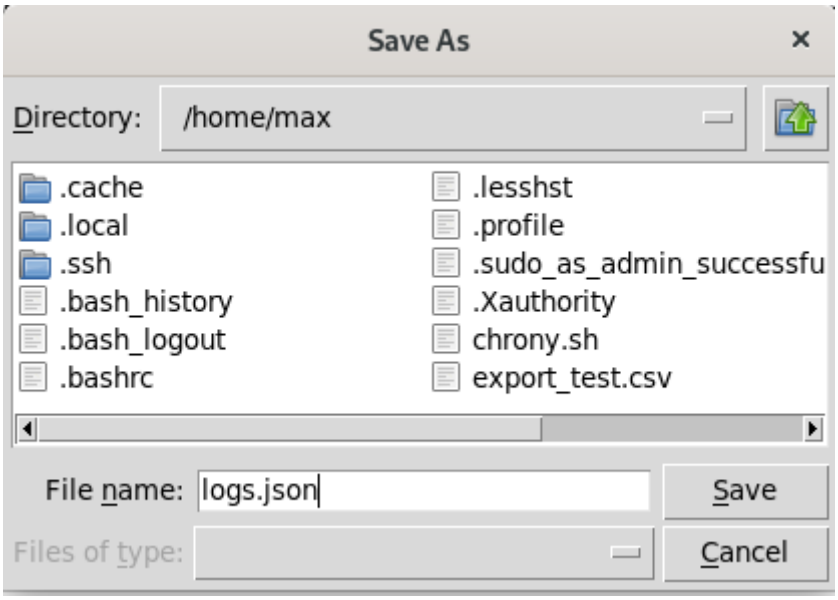
```
2025-07-25T04:07:05.312012+02:00 debian sudo:      max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COM
MAND=/usr/sbin/faillock --user user2
2025-07-25T04:07:52.659783+02:00 debian sshd[2782]: Failed password for user2 from 192.168.120.1 por
t 60650 ssh2
2025-07-25T04:09:31.770103+02:00 debian sshd[2782]: Failed password for user2 from 192.168.120.1 por
t 60650 ssh2
2025-07-25T04:09:38.866304+02:00 debian sshd[2782]: Connection closed by authenticating user user2 1
92.168.120.1 port 60650 [preauth]
2025-07-25T04:09:59.346490+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 por
t 60673 ssh2
```

```
2025-07-24T16:18:52.342950+00:00 debian postfix/smtp[1857]: 4D2822964D: to=<chapron.maxime@gmail.com
>, relay=smtp.gmail.com[64.233.184.109]:587, delay=1, delays=0.02/0.01/0.42/0.58, dsn=2.0.0, status=
sent (250 2.0.0 OK  1753373932 5b1f17b1804b1-4587291b461sm2724635e9.28 - gsmtp)
2025-07-24T16:30:08.397246+00:00 debian postfix/smtp[3134]: 171D82964F: to=<chapron.maxime@gmail.com
>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1.3, delays=0.02/0.03/0.41/0.86, dsn=2.0.0, statu
s=sent (250 2.0.0 OK  1753374608 ffacd0b85a97d-3b76fcc3fefsm2688828f8f.82 - gsmtp)
2025-07-24T16:35:20.620204+00:00 debian postfix/smtp[3181]: 8164C2964F: to=<chapron.maxime@gmail.com
>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1.1, delays=0.02/0.01/0.37/0.7, dsn=2.0.0, status
=sent (250 2.0.0 OK  1753374920 ffacd0b85a97d-3b76fcad22asm2665653f8f.53 - gsmtp)
2025-07-24T16:37:51.432322+00:00 debian postfix/smtp[3209]: 732AF2964F: to=<chapron.maxime@gmail.com
```



CPU (rouge, %), RAM (bleu, %), Réseau (vert, x3 zoom, Mo/s)






```
max@debian:~$ ls
chrony.sh  export_test.csv  logs.json  logs_serveur.csv  ntp.sh  postfix.sh  postfix_pam_logs.py  test_json.json
```

```
  GNU nano 7.2                                                    logs.json
{
    "pam": [
        "2025-07-25T04:07:05.312012+02:00 debian sudo:      max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COMMAND=/usr/sbin/faillock --user user2\n",
        "2025-07-25T04:07:52.659783+02:00 debian sshd[2782]: Failed password for user2 from 192.168.120.1 port 60650 ssh2\n",
        "2025-07-25T04:09:31.770103+02:00 debian sshd[2782]: Failed password for user2 from 192.168.120.1 port 60650 ssh2\n",
        "2025-07-25T04:09:38.866304+02:00 debian sshd[2782]: Connection closed by authenticating user user2 192.168.120.1 port 60650 [preauth]\n",
        "2025-07-25T04:09:59.346490+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2\n",
        "2025-07-25T04:10:08.939793+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2\n",
        "2025-07-25T04:10:42.518166+02:00 debian sshd[2804]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168
        "2025-07-25T04:10:44.778245+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2\n",
        "2025-07-25T04:11:21.994683+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2\n",
        "2025-07-25T04:11:25.636283+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2\n",
        "2025-07-25T04:11:28.596475+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2\n",
        "2025-07-25T04:11:29.250731+02:00 debian sshd[2804]: error: maximum authentication attempts exceeded for user2 from 192.168.120.1 port 60673 ssh2 [p
        "2025-07-25T04:11:29.250976+02:00 debian sshd[2804]: Disconnecting authenticating user user2 192.168.120.1 port 60673: Too many authentication failu
        "2025-07-25T04:11:29.251093+02:00 debian sshd[2804]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.120.1  u
        "2025-07-25T04:11:35.087233+02:00 debian sudo:      max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COMMAND=/usr/sbin/faillock --user user2\n",
        "2025-07-25T04:12:09.960065+02:00 debian sshd[2847]: Failed password for user2 from 192.168.120.1 port 60698 ssh2\n",
        "2025-07-25T04:12:51.558206+02:00 debian sshd[2847]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168
        "2025-07-25T04:12:53.604450+02:00 debian sshd[2847]: Failed password for user2 from 192.168.120.1 port 60698 ssh2\n",
        "2025-07-25T04:13:02.019989+02:00 debian sshd[2847]: Connection closed by authenticating user user2 192.168.120.1 port 60698 [preauth]\n",
        "2025-07-25T04:16:11.753588+02:00 debian sshd[2864]: pam_succeed_if(sshd:account): requirement \"user notingroup etudiants\" was met by user \"user2
        "2025-07-25T04:16:11.756042+02:00 debian sshd[2864]: Accepted password for user2 from 192.168.120.1 port 60722 ssh2\n",
        "2025-07-25T04:16:11.761199+02:00 debian sshd[2864]: pam_unix(sshd:session): session opened for user user2(uid=1006) by (uid=0)\n",
        "2025-07-25T04:16:11.788981+02:00 debian systemd-logind[564]: New session 8 of user user2.\n",
        "2025-07-25T04:16:11.880152+02:00 debian (systemd): pam_unix(systemd-user:session): session opened for user user2(uid=1006) by (uid=0)\n",
        "2025-07-25T04:16:14.364730+02:00 debian sshd[2864]: pam_unix(sshd:session): session closed for user user2\n",
        "2025-07-25T04:16:27.338318+02:00 debian sshd[2893]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168
        "2025-07-25T04:16:29.967552+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2\n",
        "2025-07-25T04:16:35.196911+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2\n",
        "2025-07-25T04:16:37.268425+02:00 debian sshd[2893]: pam_faillock(sshd:auth): Consecutive login failures for user user2 account temporarily locked\n
        "2025-07-25T04:16:39.167499+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2\n",
        "2025-07-25T04:16:43.107517+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2\n",
        "2025-07-25T04:16:46.229896+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2\n",
        "2025-07-25T04:16:51.366438+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2\n",
        "2025-07-25T04:16:51.603491+02:00 debian sshd[2893]: error: maximum authentication attempts exceeded for user2 from 192.168.120.1 port 60723 ssh2 [p
        "2025-07-25T04:16:51.603960+02:00 debian sshd[2893]: Disconnecting authenticating user user2 192.168.120.1 port 60723: Too many authentication failu
        "2025-07-25T04:16:51.604234+02:00 debian sshd[2893]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.120.1  u
        "2025-07-25T04:19:17.025653+02:00 debian sudo:      max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COMMAND=/usr/sbin/faillock --user user2\n",
        "2025-07-25T04:19:44.341466+02:00 debian sshd[2946]: Failed password for user2 from 192.168.120.1 port 60748 ssh2\n",
        "2025-07-25T04:19:52.154138+02:00 debian sshd[2946]: Failed password for user2 from 192.168.120.1 port 60748 ssh2\n",
        "2025-07-25T04:23:49.408851+02:00 debian sshd[2974]: Failed password for user2 from 192.168.120.1 port 60770 ssh2\n",
        "2025-07-25T04:24:04.192462+02:00 debian sshd[2974]: Connection closed by authenticating user user2 192.168.120.1 port 60770 [preauth]\n",
        "2025-07-25T04:42:00.173485+02:00 debian sshd[1659]: Failed password for user2 from 192.168.120.1 port 63857 ssh2\n",
        "2025-07-25T04:43:33.277796+02:00 debian sshd[1659]: Failed password for user2 from 192.168.120.1 port 63857 ssh2\n",
        "2025-07-25T04:43:35.074096+02:00 debian sshd[1659]: Connection closed by authenticating user user2 192.168.120.1 port 63857 [preauth]\n",
        "2025-07-25T04:44:02.674349+02:00 debian sshd[1725]: pam_succeed_if(sshd:account): requirement \"user notingroup etudiants\" was met by user \"user2
        "2025-07-25T04:44:02.676377+02:00 debian sshd[1725]: Accepted password for user2 from 192.168.120.1 port 63865 ssh2\n",
        "2025-07-25T04:44:02.683440+02:00 debian sshd[1725]: pam_unix(sshd:session): session opened for user user2(uid=1006) by (uid=0)\n",
        "2025-07-25T04:44:02.742396+02:00 debian systemd-logind[530]: New session 5 of user user2.\n",
        "2025-07-25T04:44:02.804997+02:00 debian (systemd): pam_unix(systemd-user:session): session opened for user user2(uid=1006) by (uid=0)\n",
        "2025-07-25T04:44:07.818827+02:00 debian sshd[1725]: pam_unix(sshd:session): session closed for user user2\n"
    ],
    "postfix": [
        "2025-07-24T16:18:52.342950+00:00 debian postfix/smtp[1857]: 4D2822964D: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, de
        "2025-07-24T16:30:08.397246+00:00 debian postfix/smtp[3134]: 171D82964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, de
        "2025-07-24T16:35:20.620204+00:00 debian postfix/smtp[3181]: 8164C2964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, de
        "2025-07-24T16:37:51.432322+00:00 debian postfix/smtp[3209]: 732AF2964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, de
        "2025-07-24T16:43:04.692337+00:00 debian postfix/smtp[3825]: A2CB426454: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, de
        "2025-07-24T17:32:47.835523+00:00 debian postfix/smtp[4892]: A08202C1C2: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, de
        "2025-07-24T19:18:21.033541+00:00 debian postfix/smtp[5815]: E8E252964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, de
        "2025-07-24T19:48:31.278578+00:00 debian postfix/smtp[7750]: 399AB2C1C2: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, de
        "2025-07-24T19:51:27.028139+00:00 debian postfix/smtp[8351]: 032B62964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, de
        "2025-07-24T20:19:58.298567+00:00 debian postfix/smtp[8906]: 0B02F29650: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, de
        "2025-07-24T20:31:18.080902+00:00 debian postfix/smtp[8987]: 14F2F26451: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, de
        "2025-07-24T21:15:28.642471+00:00 debian postfix/smtp[9540]: 80EAF2822F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, de
```

```
  GNU nano 7.2                                                    logs_serveur.csv
### PAM ###
2025-07-25T04:07:05.312012+02:00 debian sudo:      max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COMMAND=/usr/sbin/faillock --user user2
2025-07-25T04:07:52.659783+02:00 debian sshd[2782]: Failed password for user2 from 192.168.120.1 port 60650 ssh2
2025-07-25T04:09:31.770103+02:00 debian sshd[2782]: Failed password for user2 from 192.168.120.1 port 60650 ssh2
2025-07-25T04:09:38.866304+02:00 debian sshd[2782]: Connection closed by authenticating user user2 192.168.120.1 port 60650 [preauth]
2025-07-25T04:09:59.346490+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2
2025-07-25T04:10:08.939793+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2
2025-07-25T04:10:42.518166+02:00 debian sshd[2804]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.120.1
2025-07-25T04:10:44.778245+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2
2025-07-25T04:11:21.994683+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2
2025-07-25T04:11:25.636283+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2
2025-07-25T04:11:28.596475+02:00 debian sshd[2804]: Failed password for user2 from 192.168.120.1 port 60673 ssh2
2025-07-25T04:11:29.250731+02:00 debian sshd[2804]: error: maximum authentication attempts exceeded for user2 from 192.168.120.1 port 60673 ssh2 [preauth]
2025-07-25T04:11:29.250976+02:00 debian sshd[2804]: Disconnecting authenticating user user2 192.168.120.1 port 60673: Too many authentication failures [pre
2025-07-25T04:11:29.251093+02:00 debian sshd[2804]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.120.1  user=user
2025-07-25T04:11:35.087233+02:00 debian sudo:      max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COMMAND=/usr/sbin/faillock --user user2
2025-07-25T04:12:09.960065+02:00 debian sshd[2847]: Failed password for user2 from 192.168.120.1 port 60698 ssh2
2025-07-25T04:12:51.558206+02:00 debian sshd[2847]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.120.1
2025-07-25T04:12:53.604450+02:00 debian sshd[2847]: Failed password for user2 from 192.168.120.1 port 60698 ssh2
2025-07-25T04:13:02.019989+02:00 debian sshd[2847]: Connection closed by authenticating user user2 192.168.120.1 port 60698 [preauth]
"2025-07-25T04:16:11.753588+02:00 debian sshd[2864]: pam_succeed_if(sshd:account): requirement ""user notingroup etudiants"" was met by user ""user2"""
2025-07-25T04:16:11.756042+02:00 debian sshd[2864]: Accepted password for user2 from 192.168.120.1 port 60722 ssh2
2025-07-25T04:16:11.761199+02:00 debian sshd[2864]: pam_unix(sshd:session): session opened for user user2(uid=1006) by (uid=0)
2025-07-25T04:16:11.788981+02:00 debian systemd-logind[564]: New session 8 of user user2.
2025-07-25T04:16:11.880152+02:00 debian (systemd): pam_unix(systemd-user:session): session opened for user user2(uid=1006) by (uid=0)
2025-07-25T04:16:14.364730+02:00 debian sshd[2864]: pam_unix(sshd:session): session closed for user user2
2025-07-25T04:16:27.338318+02:00 debian sshd[2893]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.120.1
2025-07-25T04:16:29.967552+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2
2025-07-25T04:16:35.196911+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2
2025-07-25T04:16:37.268425+02:00 debian sshd[2893]: pam_faillock(sshd:auth): Consecutive login failures for user user2 account temporarily locked
2025-07-25T04:16:39.167499+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2
2025-07-25T04:16:43.107517+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2
2025-07-25T04:16:46.229896+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2
2025-07-25T04:16:51.366438+02:00 debian sshd[2893]: Failed password for user2 from 192.168.120.1 port 60723 ssh2
2025-07-25T04:16:51.603491+02:00 debian sshd[2893]: error: maximum authentication attempts exceeded for user2 from 192.168.120.1 port 60723 ssh2 [preauth]
2025-07-25T04:16:51.603960+02:00 debian sshd[2893]: Disconnecting authenticating user user2 192.168.120.1 port 60723: Too many authentication failures [pre
2025-07-25T04:16:51.604234+02:00 debian sshd[2893]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.120.1  user=user
2025-07-25T04:19:17.025653+02:00 debian sudo:      max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COMMAND=/usr/sbin/faillock --user user2
2025-07-25T04:19:44.341466+02:00 debian sshd[2946]: Failed password for user2 from 192.168.120.1 port 60748 ssh2
2025-07-25T04:19:52.154138+02:00 debian sshd[2946]: Failed password for user2 from 192.168.120.1 port 60748 ssh2
2025-07-25T04:23:49.408851+02:00 debian sshd[2974]: Failed password for user2 from 192.168.120.1 port 60770 ssh2
2025-07-25T04:24:04.192462+02:00 debian sshd[2974]: Connection closed by authenticating user user2 192.168.120.1 port 60770 [preauth]
2025-07-25T04:42:00.173485+02:00 debian sshd[1659]: Failed password for user2 from 192.168.120.1 port 63857 ssh2
2025-07-25T04:43:33.277796+02:00 debian sshd[1659]: Failed password for user2 from 192.168.120.1 port 63857 ssh2
2025-07-25T04:43:35.074096+02:00 debian sshd[1659]: Connection closed by authenticating user user2 192.168.120.1 port 63857 [preauth]
"2025-07-25T04:44:02.674349+02:00 debian sshd[1725]: pam_succeed_if(sshd:account): requirement ""user notingroup etudiants"" was met by user ""user2"""
2025-07-25T04:44:02.676377+02:00 debian sshd[1725]: Accepted password for user2 from 192.168.120.1 port 63865 ssh2
2025-07-25T04:44:02.683440+02:00 debian sshd[1725]: pam_unix(sshd:session): session opened for user user2(uid=1006) by (uid=0)
2025-07-25T04:44:02.742396+02:00 debian systemd-logind[530]: New session 5 of user user2.
2025-07-25T04:44:02.804997+02:00 debian (systemd): pam_unix(systemd-user:session): session opened for user user2(uid=1006) by (uid=0)
2025-07-25T04:44:07.818827+02:00 debian sshd[1725]: pam_unix(sshd:session): session closed for user user2
### POSTFIX ###
"2025-07-24T16:18:52.342950+00:00 debian postfix/smtp[1857]: 4D2822964D: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, delay=1,
"2025-07-24T16:30:08.397246+00:00 debian postfix/smtp[3134]: 171D82964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1.3
"2025-07-24T16:35:20.620204+00:00 debian postfix/smtp[3181]: 8164C2964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1.1
"2025-07-24T16:37:51.432322+00:00 debian postfix/smtp[3209]: 732AF2964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=0.9
"2025-07-24T16:43:04.692337+00:00 debian postfix/smtp[3825]: A2CB426454: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1,
"2025-07-24T17:32:47.835523+00:00 debian postfix/smtp[4892]: A08202C1C2: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1.2
"2025-07-24T19:18:21.033541+00:00 debian postfix/smtp[5815]: E8E252964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, delay=1.1
"2025-07-24T19:48:31.278578+00:00 debian postfix/smtp[7750]: 399AB2C1C2: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, delay=1,
"2025-07-24T19:51:27.028139+00:00 debian postfix/smtp[8351]: 032B62964F: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=1,
"2025-07-24T20:19:58.298567+00:00 debian postfix/smtp[8906]: 0B02F29650: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=3.3
"2025-07-24T20:31:18.080902+00:00 debian postfix/smtp[8987]: 14F2F26451: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, delay=1,
"2025-07-24T21:15:29.642471+00:00 debian postfix/smtp[9540]: 90FAE282AF: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.109]:587, delay=1.1
```

II.

1

NTP : /etc/chrony.chrony.conf (192.168.120.130 = ip du serveur)

```
  GNU nano 7.2                                                    /etc/chrony/chrony.conf
# Welcome to the chrony configuration file. See chrony.conf(5) for more
# information about usable directives.

# Include configuration files found in /etc/chrony/conf.d.
confdir /etc/chrony/conf.d

# Use Debian vendor zone.
#pool 2.debian.pool.ntp.org iburst
server 192.168.120.130 iburst
```

On change l’heure du serveur pour tester la synchro :

Coupe chrony pour changer l’heure, pour on restart

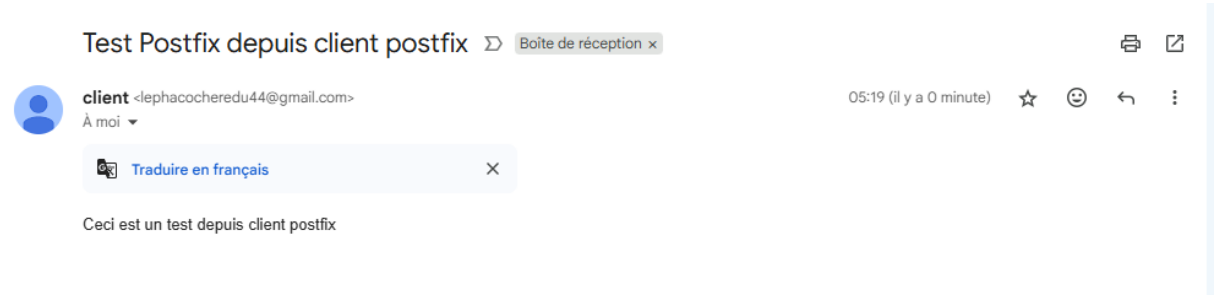
```
client@debian-client:~$ sudo systemctl stop chrony
sudo date -s "2025-07-25 10:00:00"  # change l'heure artificiellement
[sudo] password for client:
Fri Jul 25 10:00:00 AM CEST 2025
client@debian-client:~$ date
Fri Jul 25 10:00:02 AM CEST 2025
client@debian-client:~$ sudo systemctl start chrony
[sudo] password for client:
client@debian-client:~$ date
Fri Jul 25 05:13:01 AM CEST 2025
client@debian-client:~$ date
Fri Jul 25 05:13:09 AM CEST 2025
client@debian-client:~$ chronyc tracking
chronyc sources -v
Reference ID    : C0A87882 (192.168.120.130)
Stratum         : 3
Ref time (UTC)  : Fri Jul 25 03:12:52 2025
System time     : 0.000000011 seconds slow of NTP time
Last offset     : +0.000010263 seconds
RMS offset      : 0.000010263 seconds
Frequency       : 3.945 ppm slow
Residual freq   : -2.886 ppm
Skew            : 12.317 ppm
Root delay      : 0.024193965 seconds
Root dispersion : 0.003157849 seconds
Update interval : 2.0 seconds
Leap status     : Normal

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current best, '+' = combined, '-' = not combined,
| /             'x' = may be in error, '~' = too variable, '?' = unusable.
||                                                 .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured offset,
||                                \     |          |  zzzz = estimated error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 192.168.120.130               2   6    17    27    +16us[  +26us] +/-   15ms
client@debian-client:~$
```

Postfix client : ip du serveur relais ajouté dans /etc/postfix/main.cf

```
  GNU nano 7.2                                                    /etc/postfix/main.cf
# See /usr/share/postfix/main.cf.dist for a commented, more complete version


# Debian specific:  Specifying a file name will cause the first
# line of that file to be used as the name.  The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6



# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache


smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = debian-client.local
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, debian-client, localhost.localdomain, , localhost
relayhost = [192.168.120.130]:25
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4
```

Log du serveur : On voit que l'ip de mon client s'est connecté (client = 192.168.120.131) et que le mail a été relayé

```
2025-07-25T05:19:30.322252+02:00 debian postfix/smtpd[2034]: connect from unknown[192.168.120.131]
2025-07-25T05:19:30.355873+02:00 debian postfix/smtpd[2034]: 56CE52968E: client=unknown[192.168.120.131]
2025-07-25T05:19:30.357653+02:00 debian postfix/cleanup[2037]: 56CE52968E: message-id=<20250725031930.1C829443770@debian-client.local>
2025-07-25T05:19:30.359781+02:00 debian postfix/qmgr[1653]: 56CE52968E: from=<client@debian-client>, size=610, nrcpt=1 (queue active)
2025-07-25T05:19:30.360344+02:00 debian postfix/smtpd[2034]: disconnect from unknown[192.168.120.131] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=
7
2025-07-25T05:19:32.044433+02:00 debian postfix/smtp[2038]: 56CE52968E: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.167.109]:587, delay=1.7, d
elays=0.01/0.02/0.43/1.2, dsn=2.0.0, status=sent (250 2.0.0 OK  1753413572 5b1f17b1804b1-4586ec7944lsm30582745e9.2 - gsmtp)
2025-07-25T05:19:32.045662+02:00 debian postfix/qmgr[1653]: 56CE52968E: removed
max@debian:~$
```



Comparaison NTP :

```
client@debian-client:~$ sudo timedatectl set-timezone UTC
client@debian-client:~$ timedatectl
               Local time: Fri 2025-07-25 03:24:12 UTC
           Universal time: Fri 2025-07-25 03:24:12 UTC
                 RTC time: Fri 2025-07-25 03:24:12
                Time zone: UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
client@debian-client:~$ chronyc tracking
Reference ID    : C0A87882 (192.168.120.130)
Stratum         : 3
Ref time (UTC)  : Fri Jul 25 03:23:37 2025
System time     : 0.000001233 seconds slow of NTP time
Last offset     : +0.000989228 seconds
RMS offset      : 0.001875717 seconds
Frequency       : 4.894 ppm slow
Residual freq   : +0.762 ppm
Skew            : 7.282 ppm
Root delay      : 0.024247043 seconds
Root dispersion : 0.002695441 seconds
Update interval : 64.8 seconds
Leap status     : Normal
client@debian-client:~$ date
Fri Jul 25 03:25:16 AM UTC 2025
client@debian-client:~$ ^C
client@debian-client:~$
```

4 – TESTS

Test sur étudiants :

```
max@debian:~$ sudo groupadd etudiants
```

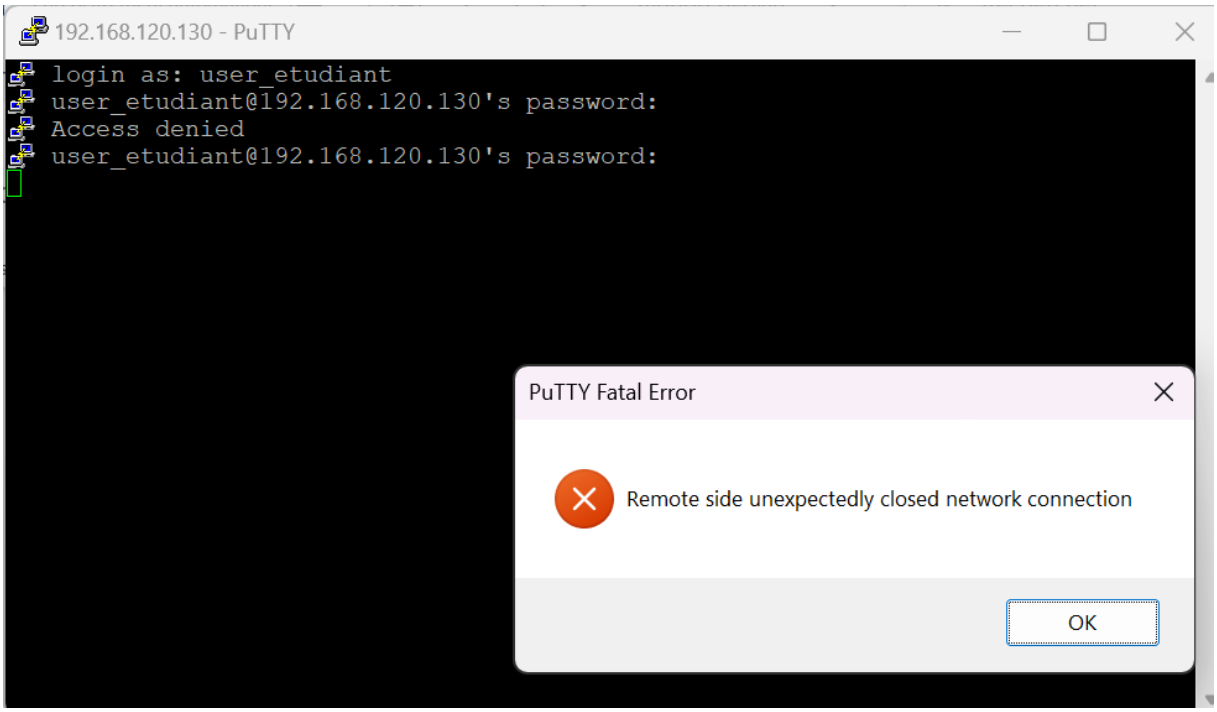
```
max@debian:~$ sudo adduser user_etudiant
```

```
max@debian:~$ sudo usermod -aG user_etudiant etudiants
```

```
user_etudiant : user_etudiant users etudiants
```

Test de connexion en dehors des heures autorisées :

```
2025-07-24T21:22:41.302415+00:00 debian login[9610]: pam_succeed_if(login:account): requirement "user notingroup etudiants" not met by user "user_etudiant"
2025-07-24T21:22:41.302880+00:00 debian login[9610]: Permission denied
2025-07-24T21:22:43.393626+00:00 debian (sd-pam): pam_unix(systemd-user:session): session closed for user user_etudiant
```



Log depuis l'application .py présentée plus bas : on lit que la condition notingroup étudiants est fausse donc la connexion est refusé car il est 18h passé

```
2025-07-24T22:15:49.528262+00:00 debian sshd[9803]: pam_succeed_if(sshd:account): requirement "user
notingroup etudiants" not met by user "user_etudiant"
2025-07-24T22:15:49.529212+00:00 debian sshd[9803]: Failed password for user_etudiant from 192.168.1
20.1 port 58823 ssh2
2025-07-24T22:15:49.529257+00:00 debian sshd[9803]: fatal: Access denied for user user_etudiant by P
AM account configuration [preauth]
```

Test de changement de mot de passe :

```
max@debian:~$ sudo adduser user2
```

Je me connecte en user2 :

```
user2@debian:~$
```

Je tente 3 tentatives différentes en ne respectant pas les contraintes de sécurité de mots de passe : ça fonctionne et ça quitte le changement grâce au parametre retry 3

```
user2@debian:~$ passwd
Changing password for user2.
Current password:
New password:
BAD PASSWORD: The password contains less than 1 digits
New password:
BAD PASSWORD: The password contains less than 1 uppercase letters
New password:
BAD PASSWORD: The password contains less than 1 non-alphanumeric characters
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
user2@debian:~$
```

Réuisste de changement de mdp :

```
user2@debian:~$ passwd
Changing password for user2.
Current password:
New password:
BAD PASSWORD: The password is the same as the old one
New password:
Retype new password:
passwd: password updated successfully
user2@debian:~$
```

Réussite :

```
2025-07-25T03:52:59.301996+02:00 debian sshd[2670]: pam_succeed_if(sshd:account): requirement "user notingroup etudiants" was met by user "user2"
2025-07-25T03:52:59.302832+02:00 debian sshd[2670]: Accepted password for user2 from 192.168.120.1 port 60536 ssh2
2025-07-25T03:52:59.309855+02:00 debian sshd[2670]: pam_unix(sshd:session): session opened for user user2(uid=1006) by (uid=0)
2025-07-25T03:52:59.357831+02:00 debian systemd-logind[564]: New session 6 of user user2.
2025-07-25T03:52:59.418904+02:00 debian (systemd): pam_unix(systemd-user:session): session opened for user user2(uid=1006) by (uid=0)
2025-07-25T03:52:59.700043+02:00 debian sshd[2670]: pam_env(sshd:session): deprecated reading of user environment enabled
2025-07-25T03:57:24.036254+02:00 debian passwd[2709]: pam_unix(passwd:chauthtok): authentication failure; logname=user2 uid=1006 euid=0 tty= ruser= rhost=  u
ser=user2
2025-07-25T03:58:07.877742+02:00 debian passwd[2711]: pam_unix(passwd:chauthtok): password changed for user2
2025-07-25T03:58:42.807944+02:00 debian sudo:     max : TTY=pts/0 ; PWD=/home/max ; USER=root ; COMMAND=/usr/bin/tail -n 20 /var/log/auth.log
2025-07-25T03:58:42.809946+02:00 debian sudo: pam_unix(sudo:session): session opened for user root(uid=0) by max(uid=1000)
```

On voit dans les logs : user2 pas membre du groupe étudiant donc peut se connecter (il est après 18h)

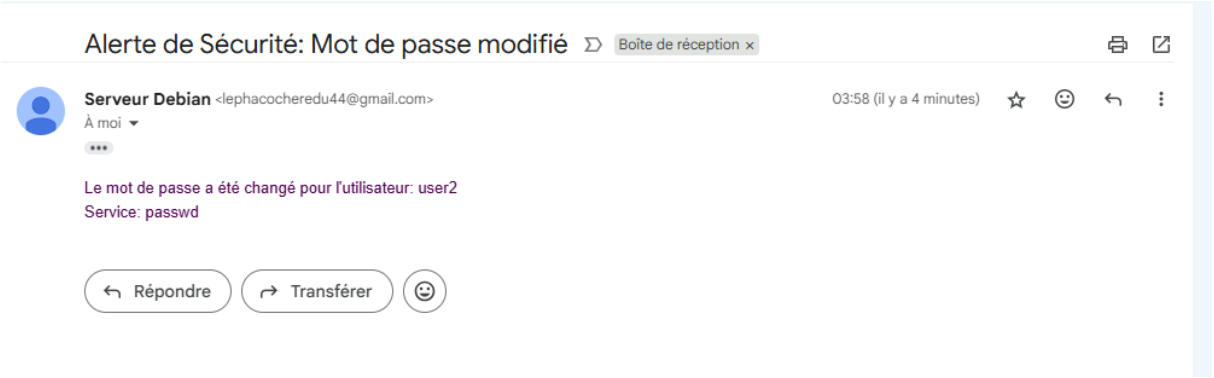
Il a fait une erreur de mdp on le voit dans les logs

On voit également le changement de mdp

On voit dans /var/mail.mail.log l'envoi d'un mail à la même heure :

```
2025-07-25T03:58:08.063883+02:00 debian postfix/pickup[2491]: 0F6F12C1C3: uid=1006 from=<lephacocheredu44@gmail.com>
2025-07-25T03:58:08.078764+02:00 debian postfix/cleanup[2717]: 0F6F12C1C3: message-id=<20250725015808.0F6F12C1C3@debian.localdomain>
2025-07-25T03:58:08.081871+02:00 debian postfix/qmgr[2492]: 0F6F12C1C3: from=<lephacocheredu44@gmail.com>, size=470, nrcpt=1 (queue active)
2025-07-25T03:58:10.913273+02:00 debian postfix/smtp[2719]: 0F6F12C1C3: to=<chapron.maxime@gmail.com>, relay=smtp.gmail.com[64.233.184.108]:587, delay=2.9, d
elays=0.03/0.03/0.55/2.3, dsn=2.0.0, status=sent (250 2.0.0 OK  1753408690 ffacd0b85a97d-3b76fcb87b9sm3546166f8f.66 - gsmtp)
2025-07-25T03:58:10.914008+02:00 debian postfix/qmgr[2492]: 0F6F12C1C3: removed
```

Mail reçu :



Test erreur de connexion : compte bloqué :

```
max@debian:/etc/pam.d$ sudo faillock --user user3
user3:
When                Type  Source                                           Valid
2025-07-25 12:06:15 RHOST 192.168.120.1                                        V
2025-07-25 12:06:20 RHOST 192.168.120.1                                        V
2025-07-25 12:06:25 RHOST 192.168.120.1                                        V
```

```
2025-07-25T12:07:09.259537+02:00 debian sudo:     max : TTY=pts/0 ; PWD=/etc/pam.d ; USER=root ; COMMAND=/usr/sbin/faillock --user user3
2025-07-25T12:07:09.262527+02:00 debian sudo: pam_unix(sudo:session): session opened for user root(uid=0) by max(uid=1000)
2025-07-25T12:07:09.266357+02:00 debian sudo: pam_unix(sudo:session): session closed for user root
max@debian:/var/log$
```

Mail pour chaque tentative :

Serveur Debian <lephacocheredu44@gmail.com> 12:06 (il y a 1 minute)
À moi

Une tentative de connexion a échoué.
Utilisateur: user3
Depuis l'IP: 192.168.120.1
Service: sshd

Serveur Debian <lephacocheredu44@gmail.com> 12:06 (il y a 1 minute)
À moi

Une tentative de connexion a échoué.
Utilisateur: user3
Depuis l'IP: 192.168.120.1
Service: sshd

Serveur Debian <lephacocheredu44@gmail.com> 12:06 (il y a 1 minute)
À moi

Une tentative de connexion a échoué.
Utilisateur: user3
Depuis l'IP: 192.168.120.1
Service: sshd