

## Script alert SSH

C'est script en **Python** qui envoie une notification par **e-mail** chaque fois qu'un utilisateur se connecte à **Guacamole** ou tente une connexion SSH. Il utilise **Postfix** pour intercepter les connexions et **SMTP** pour envoyer l'alerte

```
zafar@apache-guaca:~# sudo apt update && sudo apt install postfix mailutils -y
[sudo] password for zafar:
Sorry, try again.
[sudo] password for zafar:
Sorry, try again.
[sudo] password for zafar:
Atteint :1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Atteint :2 http://archive.ubuntu.com/ubuntu jammy InRelease
Atteint :3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
```

```
zafar@apache-guaca:~# sudo apt install python3 python3-pip -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
python3 est déjà la version la plus récente (3.10.6-1~22.04.1).
python3 passé en « installé manuellement ».
```

```
zafar@apache-guaca:/opt/scripts# sudo nano monitor_guacamole_ssh.py
```

```
zafar@apache-guaca:/opt/scripts# sudo chmod +x monitor_guacamole_ssh.py
```

```
GNU nano 6.2 monitor_guacamole_ssh.py
import smtplib
import time
import re
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

# Configuration SMTP
SMTP_SERVER = "smtp-mibc-fr-07.mailinblack.com"
SMTP_PORT = 25
MAIL_TO = "stagiaire-it@daudruy.fr"
MAIL_FROM = "stagiaire-it@daudruy.fr" # À remplacer par un mail valide

# Fonction d'envoi d'alerte
def send_alert(subject, message):
    try:
        msg = MIMEMultipart()
        msg['From'] = MAIL_FROM
        msg['To'] = MAIL_TO
        msg['Subject'] = subject

        msg.attach(MIMEText(message, 'plain'))

        with smtplib.SMTP(SMTP_SERVER, SMTP_PORT) as server:
            server.sendmail(MAIL_FROM, MAIL_TO, msg.as_string())
        print("[+] Notification envoyée avec succès !")
    except Exception as e:
        print(f"[-] Erreur d'envoi de l'email: {e}")

# Surveillance des logs SSH et Guacamole
def monitor_logs():
    auth_log = "/var/log/auth.log"
    guac_log = "/var/log/tomcat9/catalina.out"

    with open(auth_log, "r") as ssh_log, open(guac_log, "r") as guac:
        ssh_log.seek(0, 2)
        guac.seek(0, 2)

    while True:
        ssh_line = ssh_log.readline()
        guac_line = guac.readline()
```

## Test :

```
zafar@apache-guaca:/opt/scripts# nohup: ignoring input and appending output to '/home/zafar/nohup.out'
```

Je me connecte en ssh sur serveur

```
*** System restart required ***
Last login: Tue Feb  4 13:35:49 2025 from 192.168.40.65

zafar@apache-guaca:~#
```

Mail si je tape mal le mot de passe

The screenshot shows an email client interface. On the left, a list of emails from 'stagiaire-it@daudruy.fr' is visible. The selected email is titled 'Tentative SSH échouée' (Failed SSH Attempt) and has a timestamp of 14:44. The main content area shows the email body: 'À : Stagiaire IT' and 'Tentative de connexion SSH échouée depuis 192.168.40.65'. Below the body are buttons for 'Répondre' (Reply) and 'Transférer' (Forward).

La je me suis connecté en ssh

The screenshot shows the same email client interface. The selected email is titled 'Alerte Connexion SSH' (SSH Connection Alert) and has a timestamp of 14:44. The main content area shows the email body: 'Connexion SSH détectée : Utilisateur : zafar IP : 192.168.40.65'. Below the body are buttons for 'Répondre' (Reply) and 'Répondre à tous' (Reply All).

## Automatiser ce script avec systemd

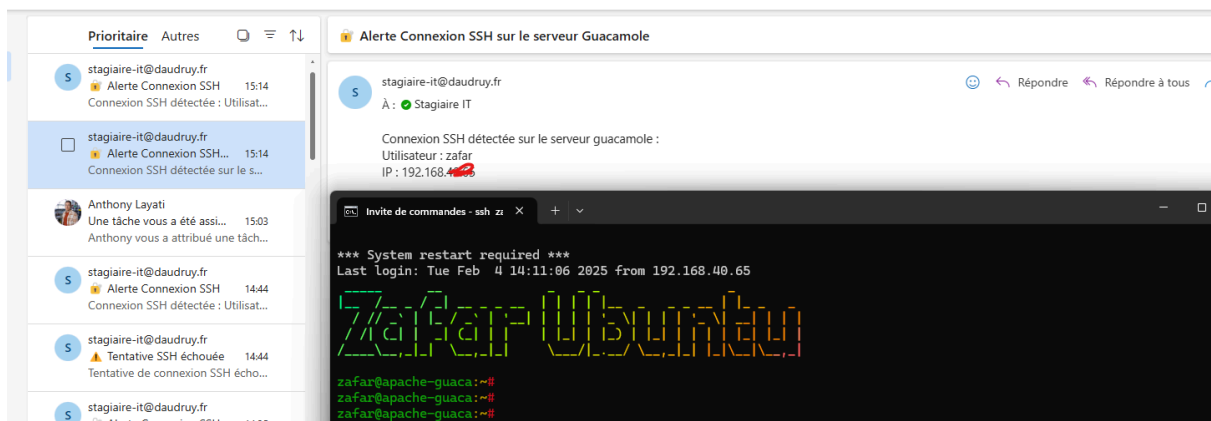
```
GNU nano 6.2 /etc/systemd/system/monitor.service
[Unit]
Description=Surveillance des connexions SSH et Guacamole
After=network.target

[Service]
ExecStart=/usr/bin/python3 /opt/scripts/monitor_guacamole_ssh.py
Restart=always
User=root

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

```
zafar@apache-guaca: /etc/systemd/system# sudo nano /etc/systemd/system/monitor.service
zafar@apache-guaca: /etc/systemd/system# sudo systemctl daemon-reload
zafar@apache-guaca: /etc/systemd/system# sudo systemctl enable monitor.service
zafar@apache-guaca: /etc/systemd/system# sudo systemctl start monitor.service
zafar@apache-guaca: /etc/systemd/system# sudo systemctl status monitor.service
● monitor.service – Surveillance des connexions SSH et Guacamole
   Loaded: loaded (/etc/systemd/system/monitor.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-02-04 14:09:14 UTC; 3s ago
     Main PID: 102321 (python3)
       Tasks: 1 (limit: 9394)
```

✓ **Parfait !** Mon service **monitor.service** fonctionne maintenant et tourne bien en arrière-plan. 🎉



The screenshot shows an email interface with a list of messages on the left and a detailed view of an alert on the right. The alert is titled "Alerte Connexion SSH sur le serveur Guacamole" and is from "stagiaire-it@daudruy.fr". The body of the email states: "Connexion SSH détectée sur le serveur guacamole : Utilisateur : zafar IP : 192.168.40.65". Below the email content, there is a terminal window titled "Invite de commandes - ssh zi" showing a system message: "\*\*\* System restart required \*\*\*" and "Last login: Tue Feb 4 14:11:06 2025 from 192.168.40.65". The terminal also displays the name "Zafar Ubuntu" in a stylized font and the prompt "zafar@apache-guaca:~#".

## le scripte complet :

```
import smtplib
import time
import re
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

# Configuration SMTP
SMTP_SERVER = "smtp-mibc-fr-07.mailinblack.com"
SMTP_PORT = 25
MAIL_TO = "stagiaire-it@daudruy.fr"
MAIL_FROM = "alert@yourdomain.com" # À remplacer par un mail valide

# Fonction d'envoi d'alerte
def send_alert(subject, message):
    try:
        msg = MIMEMultipart()
        msg['From'] = MAIL_FROM
        msg['To'] = MAIL_TO
        msg['Subject'] = subject

        msg.attach(MIMEText(message, 'plain'))

        with smtplib.SMTP(SMTP_SERVER, SMTP_PORT) as server:
            server.sendmail(MAIL_FROM, MAIL_TO, msg.as_string())
            print("[+] Notification envoyée avec succès !")
    except Exception as e:
        print(f"[-] Erreur d'envoi de l'email: {e}")

# Surveillance des logs SSH et Guacamole
def monitor_logs():
    auth_log = "/var/log/auth.log"
    guac_log = "/var/log/tomcat9/catalina.out"

    with open(auth_log, "r") as ssh_log, open(guac_log, "r") as guac:
        ssh_log.seek(0, 2)
        guac.seek(0, 2)

        while True:
            ssh_line = ssh_log.readline()
            guac_line = guac.readline()

            # Détection des connexions SSH réussies
            if ssh_line and "Accepted password" in ssh_line:
                user = re.search(r'Accepted password for (\w+)', ssh_line)
                ip = re.search(r'from ([\d\.]+)', ssh_line)
                if user and ip:
                    msg = f"Connexion SSH détectée : \nUtilisateur : {user.group(1)} \nIP : {ip.group(1)}"
                    send_alert("🚨 Alerte Connexion SSH", msg)

            # Détection des échecs SSH
            if ssh_line and "Failed password" in ssh_line:
                ip = re.search(r'from ([\d\.]+)', ssh_line)
                if ip:
                    msg = f"Tentative de connexion SSH échouée depuis {ip.group(1)}"
                    send_alert("⚠ Tentative SSH échouée", msg)

            # Détection des connexions Guacamole
            if guac_line and "User \\" in guac_line and "connected from" in guac_line:
                user = re.search(r'User \"(.*)\"', guac_line)
                ip = re.search(r'from ([\d\.]+)', guac_line)
                if user and ip:
                    msg = f"Connexion Guacamole détectée : \nUtilisateur : {user.group(1)} \nIP : {ip.group(1)}"
                    send_alert("🖥 Connexion Guacamole", msg)

            time.sleep(1)

if __name__ == "__main__":
    monitor_logs()
```

