Script de notification

1. Installer msmtp

```
root@apache-guaca:~# sudo apt-get install msmtp
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 :
  libsecret-1-0 libsecret-common
Paquets suggérés :
  msmtp-mta
Les NOUVEAUX paquets suivants seront installés :
```

```
 GNU nano 6.2                                    /home/zafar/.msmtprc
# Paramètres par défaut
defaults
auth            off
tls             off
logfile         ~/.msmtp.log

# Configuration du compte par défaut
account default
host            smtp-mibc-fr-07.mailinblack.com
port            25
from            stagiaire-it@daudruy.fr
```

```
root@apache-guaca:/opt/scripts# chmod 600 /home/zafar/.msmtprc
```

Puisque le script tourne sous `root`, la config a été copiée dans `/root/.msmtprc` :
sudo cp /home/zafar/.msmtprc /root/
sudo chown root:root /root/.msmtprc
sudo chmod 600 /root/.msmtprc

zafar

Mise en place du script de surveillance des logs

```
  GNU nano 6.2                                  /opt/scripts/watch_guac_log.sh
#!/bin/bash
#
# Script qui surveille les logs de Guacamole et envoie une notification lors d'une connexion.

LOGFILE="/var/log/tomcat9/catalina.out"
KEYWORD="User .* connected to connection"

# Suivi en temps réel des logs
tail -n0 -F "$LOGFILE" | while read -r LINE; do
    # Vérifie si la ligne contient le mot-clé indiquant une connexion
    echo "$LINE" | grep -E "$KEYWORD" > /dev/null
    if [ $? -eq 0 ]; then
        # Extraction du nom de l'utilisateur et de la connexion
        USER_NAME=$(echo "$LINE" | awk -F'"' '{print $2}')
        CONNECTION_ID=$(echo "$LINE" | awk -F'connected to connection "' '{print $2}' | awk -F'"' '{print $1}')
        DATE_CONNEXION=$(date '+%Y-%m-%d %H:%M:%S')

        # Log local (pour debug)
        echo "$(date '+%Y-%m-%d %H:%M:%S') - Connexion détectée : $USER_NAME sur connexion $CONNECTION_ID" >> /tmp/guac_notify_watch.log

        # Appel du script de notification
        /opt/scripts/guac_notify.sh "$USER_NAME" "$CONNECTION_ID"
    fi
done
```

On le rende executable : chmod +x /opt/scripts/watch_guac_log.sh

```
root@apache-guaca:/opt/scripts# ls -l watch_guac_log.sh
-rwxr-xr-x 1 root root 1001 févr.  3 14:48 watch_guac_log.sh
root@apache-guaca:/opt/scripts#
```

Mise en place du script de notification (`guac_notify.sh`)
Ce script est déclenché par `watch_guac_log.sh` pour envoyer un email.

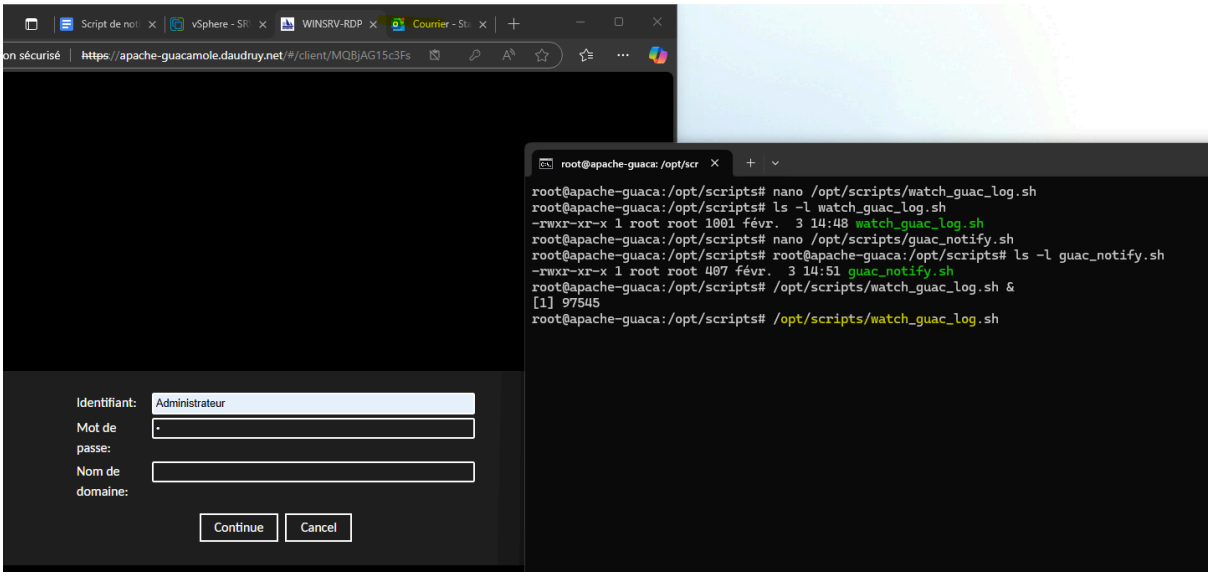
```
  GNU nano 6.2                                  /opt/scripts/guac_notify.sh
#!/bin/bash

USER_NAME="$1"
CONNECTION_ID="$2"
DATE_CONNEXION=$(date '+%Y-%m-%d %H:%M:%S')

SUBJECT="Connexion Guacamole - Utilisateur: $USER_NAME"
BODY="Salut,\n\nL'utilisateur $USER_NAME s'est connecté à Guacamole.\nDate et heure: $DATE_CONNEXION\nConnexion ID: $CONNECTION_ID\n\nÀ plus !"

echo -e "Subject: $SUBJECT\n\n$BODY" | /usr/bin/msmtp --file=/root/.msmtprc -a default stagiaire-it@daudruy.fr
```

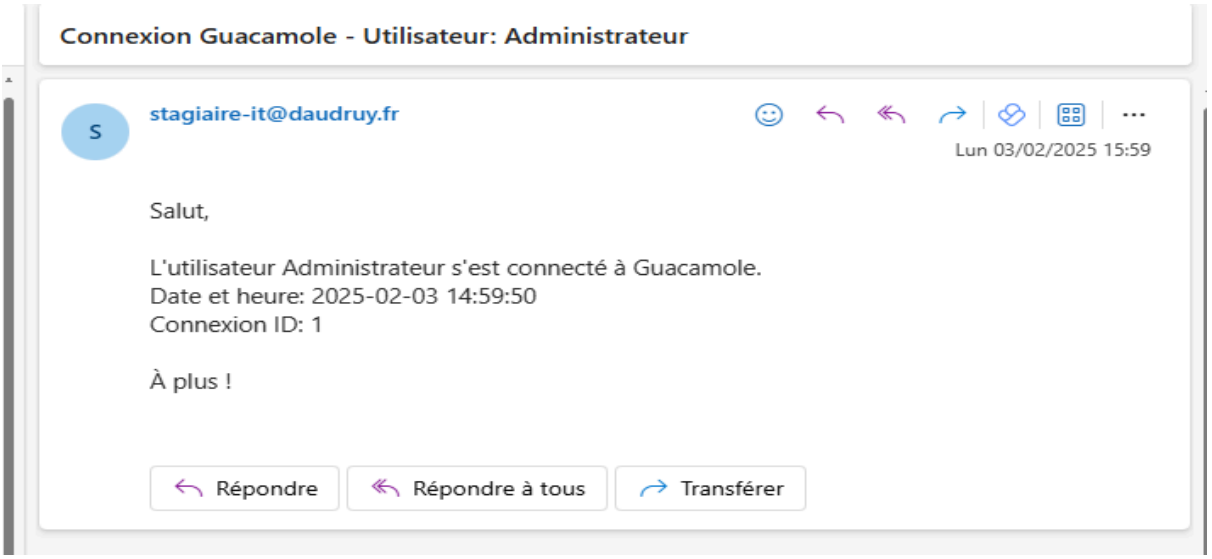
Rendre le script exécutable: `chmod +x /opt/scripts/guac_notify.sh`

```
root@apache-guaca:/opt/scripts# root@apache-guaca:/opt/scripts# ls -l guac_notify.sh
-rwxr-xr-x 1 root root 407 févr.  3 14:51 guac_notify.sh
root@apache-guaca:/opt/scripts#
```

zafar

Lancer manuellement pour le teste :





Pour s'assurer que le script démarre automatiquement au redémarrage.

```
  GNU nano 6.2          /etc/systemd/system/watch_guac.service *
[Unit]
Description=Surveillance des connexions Guacamole et envoi de notifications
After=network.target

[Service]
ExecStart=/opt/scripts/watch_guac_log.sh
Restart=always
User=root

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

Activer et démarrer le service

```
root@apache-guaca:/opt/scripts# sudo systemctl daemon-reload
root@apache-guaca:/opt/scripts# sudo systemctl enable watch_guac.service
root@apache-guaca:/opt/scripts# sudo systemctl start watch_guac.service
root@apache-guaca:/opt/scripts# sudo systemctl status watch_guac.service
● watch_guac.service - Surveillance des connexions Guacamole et envoi de notifications
     Loaded: loaded (/etc/systemd/system/watch_guac.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-02-03 15:02:51 UTC; 55s ago
   Main PID: 98240 (watch_guac_log.)
      Tasks: 3 (limit: 9394)
     Memory: 740.0K
        CPU: 2ms
     CGroup: /system.slice/watch_guac.service
             ├─98240 /bin/bash /opt/scripts/watch_guac_log.sh
             ├─98241 tail -n0 -F /var/log/tomcat9/catalina.out
             └─98242 /bin/bash /opt/scripts/watch_guac_log.sh
```

Vérifier les logs du script

```
root@apache-guaca:/opt/scripts# cat /tmp/guac_notify_watch.log
2025-02-03 14:49:25 - Connexion détectée : Administrateur sur connexion 1
2025-02-03 14:49:36 - Connexion détectée : Administrateur sur connexion 1
2025-02-03 14:51:58 - Connexion détectée : Administrateur sur connexion 1
2025-02-03 14:52:32 - Connexion détectée : Administrateur sur connexion 1
2025-02-03 14:59:50 - Connexion détectée : Administrateur sur connexion 1
2025-02-03 14:59:50 - Connexion détectée : Administrateur sur connexion 1
root@apache-guaca:/opt/scripts#
```

Vérifier les logs systemd

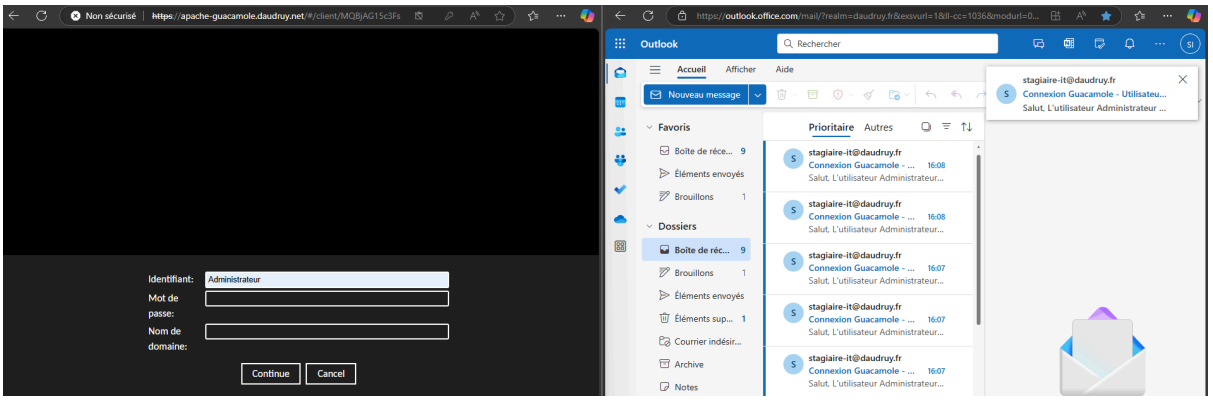
```
root@apache-guaca:/opt/scripts# sudo journalctl -u watch_guac.service --no-pager | tail -n 5
0
févr. 03 15:02:51 apache-guaca systemd[1]: Started Surveillance des connexions Guacamole et
envoi de notifications.
root@apache-guaca:/opt/scripts#
```

zafar

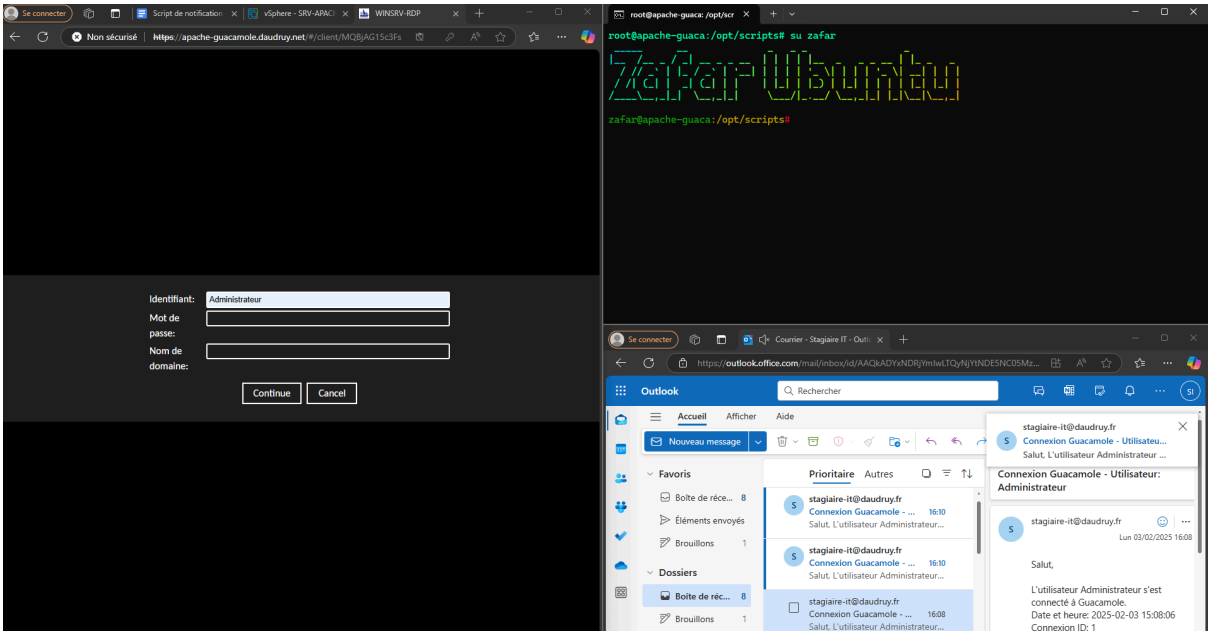
```
root@apache-guaca:/opt/scripts# /opt/scripts/guac_notify.sh testuser 1234.
root@apache-guaca:/opt/scripts# cat ~/.msmtp.log
févr. 03 14:51:58 host=smtp-mibc-fr-07.mailinblack.com tls=off auth=off from=stagiaire-it@daudruy.fr r
ecipients=stagiaire-it@daudruy.fr mailsize=257 smtpstatus=250 smtpmsg='250 2.0.0 Ok: queued as 39E1412
007F' exitcode=EX_OK
févr. 03 14:52:32 host=smtp-mibc-fr-07.mailinblack.com tls=off auth=off from=stagiaire-it@daudruy.fr r
ecipients=stagiaire-it@daudruy.fr mailsize=257 smtpstatus=250 smtpmsg='250 2.0.0 Ok: queued as 6AB9D12
0083' exitcode=EX_OK
```

🎉 Tout est maintenant automatisé.

Dèse que le utilisateur met son identifiant les scrippte les detecte et envoite un notification



Et ca marche en étant user normal :

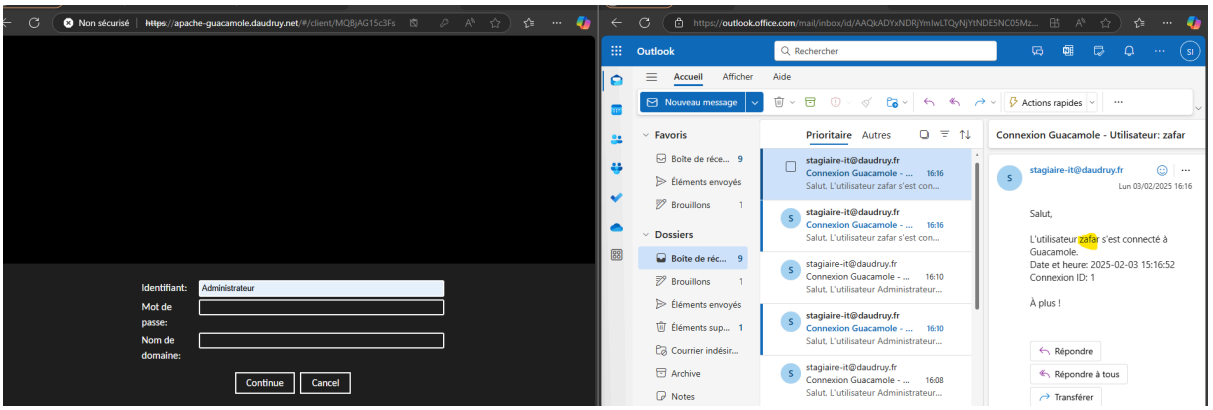


zafar

Les droit :

```
zafar@apache-guaca:/opt/scripts# ls -l /opt/scripts/
total 16
-rwxr-xr-x 1 zafar root 3618 janv. 28 11:48 envoie_et_nettoie.sh
-rwxr-xr-x 1 root  root  407 févr.  3 14:51 guac_notify.sh
-rwxr-xr-x 1 root  root  417 janv. 28 13:54 nas_supprime.sh
-rwxr-xr-x 1 root  root 1001 févr.  3 14:48 watch_guac_log.sh
```

Teste avec autre utilisateur :



Test script un jours après config :