Zafar sio2

05/01/2025

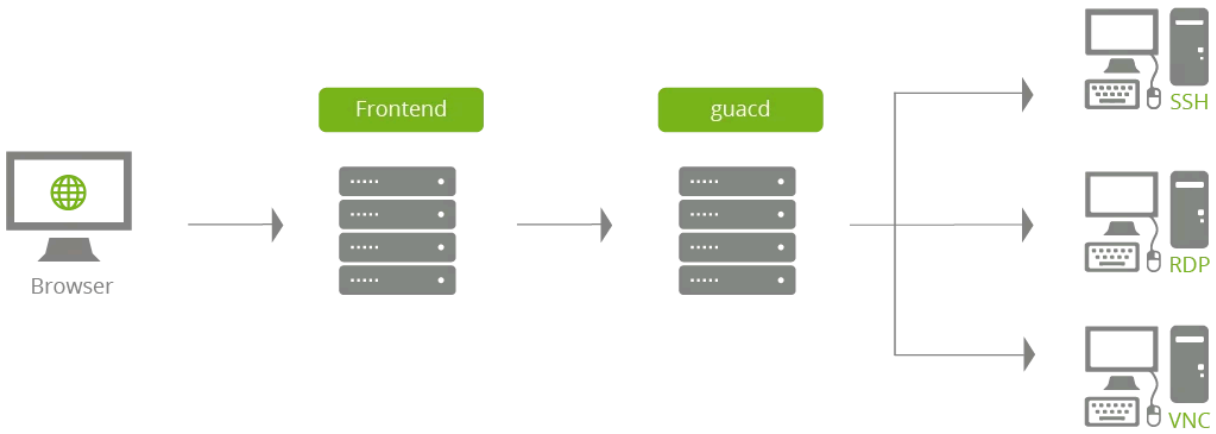
Projet Apache-Guacamole

Contexte et Objectif du Projet

Dans ce rapport nous allons installer et configurer Apache Guacamole, une solution open source et gratuite que l'on peut mettre en place en tant que bastion d'administration, passerelle d'accès ou encore serveur de rebond.
Une machine sous Ubuntu 24.05 sera utilisée pour héberger l'application.

Configuration
Apache Guacamole

Le serveur Apache Guacamole sera utilisé comme point d'entrée unique la zone DMZ de Daudruy pour accéder aux serveurs et équipements de l'infrastructure que ce soit via les protocoles RDP, SSH, VNC et Telnet, et même Kubernetes. Que l'on soit en externe ou en interne, les connexions aux serveurs vont obligatoirement passer par l'hôte Apache Guacamole.



Apache Guacamole devient un élément central de l'infrastructure puisqu'il sert de passerelle pour administrer les machines. il est possible d'avoir plusieurs hôtes Apache Guacamole pour répartir la charge et assurer la haute disponibilité mais dans notre cas on as pas trop de charge 10 utilisateur sur 8 serveur.

Enfin, les règles de pare-feu doivent aussi être adaptées : l'hôte Apache Guacamole doit être le seul à pouvoir se connecter en RDP/SSH/VNC/Etc. sur les machines de l'infrastructure.

II. Les fonctions clés d'Apache Guacamole

- Centralisation et suivi des connexions : qui, quand, où, combien de temps, depuis où
- Aucun client lourd à installer, l'accès s'effectue en mode web grâce au HTML5
- Authentification multi-facteurs pour l'accès aux connexions, via un code TOTP
- Authentification SSO, compatible avec SAML, OpenID Connect, CAS ou encore LDAP
- Enregistrements vidéos des sessions, c'est-à-dire quand une connexion est en cours d'utilisation
- Gestion des autorisations pour l'accès aux connexions, par groupes ou par utilisateurs

III. Installer Apache Guacamole sur Debian

A. Installer les prérequis d'Apache Guacamole

Tout d'abord, nous devons installer un ensemble de paquets indispensables au bon fonctionnement d'Apache Guacamole. Certains paquets sont spécifiques à certaines fonctionnalités, comme les connexions RDP par exemple. Cette liste de dépendance est consultable dans la documentation.

[Installing Guacamole natively — Apache Guacamole Manual v1.5.5]

Sur la machine Ubuntu, on commence par installer ces fameuses dépendances avec les bonne version de 2025 avec la commande suivante :

Créer un super utilisateur pour travailler la dessu :

```
zafar@apache-guaca:~$
```

B. Compiler et installer Apache Guacamole "Server"

La partie "Serveur Apache Guacamole" doit être téléchargée et compilée en local pour s'installer. La dernière version sera utilisée, à savoir la version 1.5.5. Pour identifier la dernière version, nous pouvons nous appuyer sur ces deux liens :

- Historique des versions d'Apache Guacamole
- Télécharger les sources d'installation d'Apache Guacamole

On va se positionner dans le répertoire "/tmp" et télécharger l'archive tar.gz :

```
zafar@apache-guaca:/tmp$ wget https://downloads.apache.org/guacamole/1.5.5/source/guacamole-server-1.5.5.tar.gz
z
--2025-01-17 12:53:41--  https://downloads.apache.org/guacamole/1.5.5/source/guacamole-server-1.5.5.tar.gz
Resolving downloads.apache.org (downloads.apache.org)... 135.181.214.104, 88.99.208.237, 2a01:4f9:3a:2c57::2, .
..
Connecting to downloads.apache.org (downloads.apache.org)|135.181.214.104|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1136892 (1,1M) [application/x-gzip]
Saving to: ‘guacamole-server-1.5.5.tar.gz’

guacamole-server-1.5.5.tar. 100%[=========================================>]   1,08M  3,39MB/s    in 0,3s

2025-01-17 12:53:42 (3,39 MB/s) - ‘guacamole-server-1.5.5.tar.gz’ saved [1136892/1136892]
```

Une fois le téléchargement terminé, on décompresse l'archive tar.gz et on se positionne dans le répertoire obtenu :

```
zafar@apache-guaca:/tmp$ tar -xzf guacamole-server-1.5.5.tar.gz
zafar@apache-guaca:/tmp$ cd guacamole-server-1.5.5/
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$
```

On exécute la commande ci-dessous pour se préparer à la compilation, ce qui va permettre de vérifier la présence des dépendances :

```
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo ./configure --with-systemd-dir=/etc/systemd/system/
```

```
  Services / tools:

     guacd ..... yes
     guacenc .... yes
     guaclog .... yes

  FreeRDP plugins: /usr/lib/x86_64-linux-gnu/freerdp2
  Init scripts: no
  Systemd units: /etc/systemd/system/

Type "make" to compile guacamole-server.

zafar@apache-guaca:/tmp/guacamole-server-1.5.5$
```

Enfin, on termine par installer le composant Guacamole Server :

```
Type "make" to compile guacamole-server.

zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo make
make  all-recursive
make[1]: Entering directory '/tmp/guacamole-server-1.5.5'
Making all in src/libguac
```

```
make[2]: Leaving directory '/tmp/guacamole-server-1.5.5/src/guaclog'
make[2]: Entering directory '/tmp/guacamole-server-1.5.5'
make[2]: Leaving directory '/tmp/guacamole-server-1.5.5'
make[1]: Leaving directory '/tmp/guacamole-server-1.5.5'
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo make install
Making install in src/libguac
make[1]: Entering directory '/tmp/guacamole-server-1.5.5/src/libguac'
Making install in .
```

Voilà, la partie serveur d'Apache Guacamole est installée ! 👍

La commande ci-dessous sert à mettre à jour les liens entre guacamole-server et les librairies (cette commande ne retourne aucun résultat) :

```
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo ldconfig
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$
```

Ensuite, on va démarrer le service "guacd" correspondant à Guacamole et activer son démarrage automatique. La première commande sert à prendre en compte le nouveau service.

```
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo systemctl daemon-reload
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo systemctl enable --now guacd
Created symlink /etc/systemd/system/multi-user.target.wants/guacd.service → /etc/systemd/system/guacd.service.
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$
```

Enfin, on vérifie le statut d'Apache Guacamole Server :

```
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo systemctl status guacd
● guacd.service - Guacamole Server
     Loaded: loaded (/etc/systemd/system/guacd.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-01-17 12:59:01 UTC; 25s ago
       Docs: man:guacd(8)
   Main PID: 23804 (guacd)
      Tasks: 1 (limit: 9394)
```

C. Créer le répertoire de configuration

Dernière étape avant de passer à la partie cliente d'Apache Guacamole, on crée l'arborescence pour la configuration d'Apache Guacamole. Cela va donner le répertoire "/etc/guacamole" avec les sous-répertoires "extensions" et "lib". Nous en aurons besoin par la suite pour mettre en place le stockage des données dans une base de données MariaDB / MySQL.

```
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo mkdir -p /etc/guacamole/{extensions,lib}
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$
```

D. Installer Guacamole Client (Web App)

Pour exécuter **Guacamole Web App**, un **serveur Tomcat 9** est nécessaire. Il permet d'héberger l'application Java et de gérer les connexions utilisateurs via un navigateur.

On install le paquet tomcat9

```
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ sudo apt-get install tomcat9 tomcat9-admin tomcat9-common tomca
t9-user
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 :
  ca-certificates-java default-jre-headless java-common libapr1 libeclipse-jdt-core-java liblcms2-2
  libpcsclite1 libtcnative-1 libtomcat9-java openjdk-11-jre-headless
Paquets suggérés :
```

Puis, nous allons télécharger la dernière version de la Web App d'Apache Guacamole depuis le dépôt officiel:

```
zafar@apache-guaca:/tmp/guacamole-server-1.5.5$ cd /tmp
zafar@apache-guaca:/tmp$ wget https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-1.5.5.war
--2025-01-17 13:03:02--  https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-1.5.5.war
Resolving downloads.apache.org (downloads.apache.org)... 135.181.214.104, 88.99.208.237, 2a01:4f9:3a:2c57::2, .
..
Connecting to downloads.apache.org (downloads.apache.org)|135.181.214.104|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17401039 (17M)
Saving to: ‘guacamole-1.5.5.war’

guacamole-1.5.5.war         100%[=======================================>]  16,59M  25,1MB/s    in 0,7s

2025-01-17 13:03:03 (25,1 MB/s) - ‘guacamole-1.5.5.war’ saved [17401039/17401039]

zafar@apache-guaca:/tmp$
```

Une fois que le fichier est téléchargé, on le déplace dans la librairie de Web App de Tomcat9 avec cette commande :

```
zafar@apache-guaca:/tmp$ sudo mv guacamole-1.5.5.war /var/lib/tomcat9/webapps/guacamole.war
zafar@apache-guaca:/tmp$ sudo systemctl restart tomcat9 guacd
zafar@apache-guaca:/tmp$
```

05/01/2025

Voilà, Apache Guacamole Client est installé ! 👍

Base de données MariaDB pour l'authentification

Guacamole utilise **MariaDB Server** sur **Ubuntu** pour stocker les informations des utilisateurs, les connexions et les configurations.

Exemple : Lorsqu'un utilisateur se connecte, Guacamole récupère ses droits et paramètres depuis MariaDB.

✅ Pourquoi MariaDB ?

- Compatible avec MySQL et Guacamole
- Rapide et sécurisé
- Facile à gérer sur Ubuntu

```
zafar@apache-guaca:/tmp$ sudo apt-get install mariadb-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  galera-4 libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifi
  libdbi-perl libencode-locale-perl libfcgi-bin libfcgi-perl libfcgi0ldb
  libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-me
  liblwp-mediatypes-perl libmariadb3 libmysqlclient21 libtimedate-perl l
```

Création de base et utilisateur :

```
zafar@apache-guaca:/tmp$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 46
Server version: 10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE guacadb;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> CREATE USER 'userdb'@'localhost' IDENTIFIED BY 'zafar';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> GRANT SELECT, INSERT, UPDATE, DELETE ON guacadb.* TO 'userdb'@'localhost';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> EXIT;
Bye
zafar@apache-guaca:/tmp$
```

05/01/2025

La suite va consister à ajouter l'extension MySQL à Apache Guacamole ainsi que le connecteur correspondant.Toujours depuis le dépôt officiel, on télécharge cette extension :

```
zafar@apache-guaca:/tmp$ wget https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-auth-jdbc-1.5.5.tar
.gz
--2025-01-17 13:11:32--  https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-auth-jdbc-1.5.5.tar.gz
Resolving downloads.apache.org (downloads.apache.org)... 88.99.208.237, 135.181.214.104, 2a01:4f9:3a:2c57::2, .
..
Connecting to downloads.apache.org (downloads.apache.org)|88.99.208.237|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33099128 (32M) [application/x-gzip]
Saving to: ‘guacamole-auth-jdbc-1.5.5.tar.gz’

guacamole-auth-jdbc-1.5.5.t 100%[=========================================>]  31,57M  37,2MB/s    in 0,8s

2025-01-17 13:11:33 (37,2 MB/s) - ‘guacamole-auth-jdbc-1.5.5.tar.gz’ saved [33099128/33099128]

zafar@apache-guaca:/tmp$
```

On décompresser le fichier puis on déplace le fichier ".jar" de l'extension dans le répertoire "/etc/guacamole/extensions/" créé précédemment :

```
zafar@apache-guaca:/tmp$ tar -xzf guacamole-auth-jdbc-1.5.5.tar.gz
zafar@apache-guaca:/tmp$ sudo mv guacamole-auth-jdbc-1.5.5/mysql/guacamole-auth-jdbc-mysql-1.5.5.jar /etc/guaca
mole/extensions/
zafar@apache-guaca:/tmp$
```

Ensuite, le connecteur MySQL doit être téléchargé depuis le site de MySQL (peu importe si vous utilisez MariaDB ou MySQL).
On copie (ou déplace) le fichier .jar du connecteur vers le répertoire "lib" d'Apache Guacamole :

```
zafar@apache-guaca:/tmp$ wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-9.1.0.tar.gz
--2025-01-17 13:13:57--  https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-9.1.0.tar.gz
Resolving dev.mysql.com (dev.mysql.com)... 23.54.143.15, 2a02:26f0:2b00:3a2::2e31, 2a02:26f0:2b00:387::2e31
Connecting to dev.mysql.com (dev.mysql.com)|23.54.143.15|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://cdn.mysql.com//Downloads/Connector-J/mysql-connector-j-9.1.0.tar.gz [following]
--2025-01-17 13:13:58--  https://cdn.mysql.com//Downloads/Connector-J/mysql-connector-j-9.1.0.tar.gz
Resolving cdn.mysql.com (cdn.mysql.com)... 2.18.132.71, 2a02:26f0:2b00:382::1d68, 2a02:26f0:2b00:386::1d68
Connecting to cdn.mysql.com (cdn.mysql.com)|2.18.132.71|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4485702 (4,3M) [application/x-tar-gz]
Saving to: ‘mysql-connector-j-9.1.0.tar.gz’

mysql-connector-j-9.1.0.tar 100%[=========================================>]   4,28M  --.-KB/s    in 0,09s

2025-01-17 13:13:58 (48,9 MB/s) - ‘mysql-connector-j-9.1.0.tar.gz’ saved [4485702/4485702]

zafar@apache-guaca:/tmp$ tar -xzf mysql-connector-j-9.1.0.tar.gz
zafar@apache-guaca:/tmp$ sudo cp mysql-connector-j-9.1.0/mysql-connector-j-9.1.0.jar /etc/guacamole/lib/
zafar@apache-guaca:/tmp$
```

Les dépendances sont déployées, mais nous n'avons pas encore fini cette intégration avec MariaDB.

En effet, il faut importer la structure de la base de données Apache Guacamole dans notre base de données "guacadb". Pour cela, on va importer tous les fichiers SQL situés dans le répertoire "guacamole-auth-jdbc-1.5.5/mysql/schema/". Le mot de passe root de MariaDB doit être saisi pour effectuer l'import.

```
zafar@apache-guaca:/tmp$ sudo cp mysql-connector-j-9.1.0/mysql-connector-j-9.1.0.jar /etc/guacamole/lib/
zafar@apache-guaca:/tmp$ cd guacamole-auth-jdbc-1.5.5/mysql/schema/
zafar@apache-guaca:/tmp/guacamole-auth-jdbc-1.5.5/mysql/schema$ cat *.sql | mysql -u root -p guacadb
Enter password:
zafar@apache-guaca:/tmp/guacamole-auth-jdbc-1.5.5/mysql/schema$ ls -l
total 28
-rw-r--r-- 1 zafar zafar 20174 juil. 21  2021 001-create-schema.sql
-rw-r--r-- 1 zafar zafar  2876 juil. 21  2021 002-create-admin-user.sql
drwxr-xr-x 2 zafar zafar  4096 juil. 21  2021 upgrade
zafar@apache-guaca:/tmp/guacamole-auth-jdbc-1.5.5/mysql/schema$
```

Une fois que c'est fait, on va créer et éditer le fichier guacamole.properties" pour déclarer la connexion à MariaDB. Ce fichier peut être utilisé pour d'autres paramètres, selon vos besoins.

```
 GNU nano 6.2                          /etc/guacamole/guacamole.properties *
#declaration de de la connexion a Mariadb
#ce fichier est utile aussi pour d'autre parametres

# MySQL ------------------------
mysql-hostname: 127.0.0.1
mysql-port: 3306
mysql-database: guacadb
mysql-username: userdb
mysql-password: zafar
#------------------------------
```

Tant que l'on est dans la configuration, éditez le fichier "guacd.conf" pour déclarer le serveur Guacamole (ici, on déclare une connexion locale sur le port par défaut, à savoir 4822).
Communication interne : La Web App Guacamole (sur Tomcat) se connecte à **Guacd** via ce port.

```
 GNU nano 6.2                                  /etc/guacamole/guacd.conf *
#Declaration de une connexion local par defaut sur le port 4822
[server]
bind_host = 0.0.0.0
bind_port = 4822
#-----------------------------------------------------------------------
```

On redemarre tous les service

```
zafar@apache-guaca:/tmp/guacamole-auth-jdbc-1.5.5/mysql/schema$ sudo systemctl restart tomcat9 guacd mariadb
zafar@apache-guaca:/tmp/guacamole-auth-jdbc-1.5.5/mysql/schema$
```

Voilà, l'installation de base est terminée ! 👍

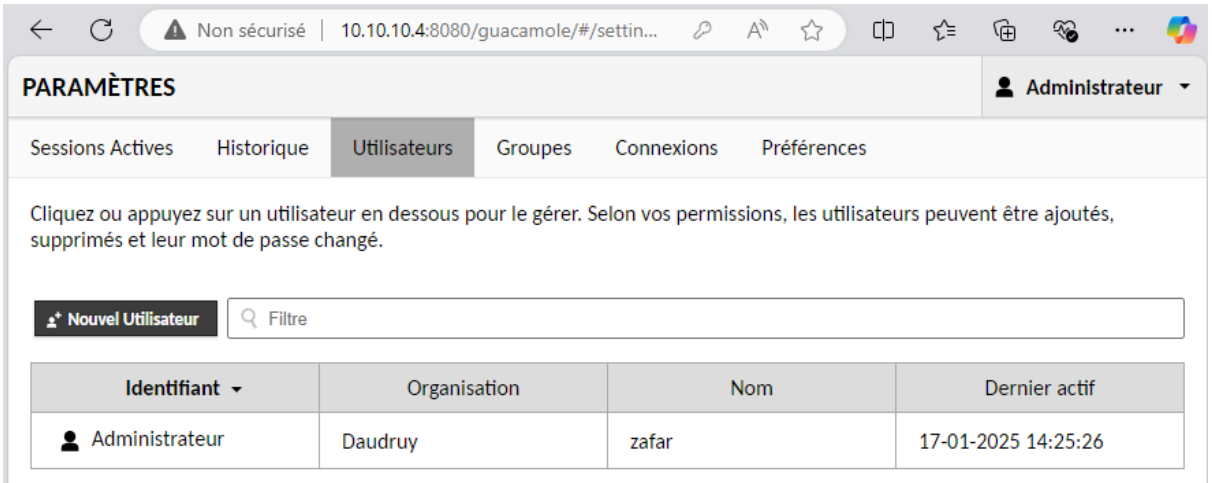
Zafar sio2

05/01/2025

Premiers pas avec Apache Guacamole

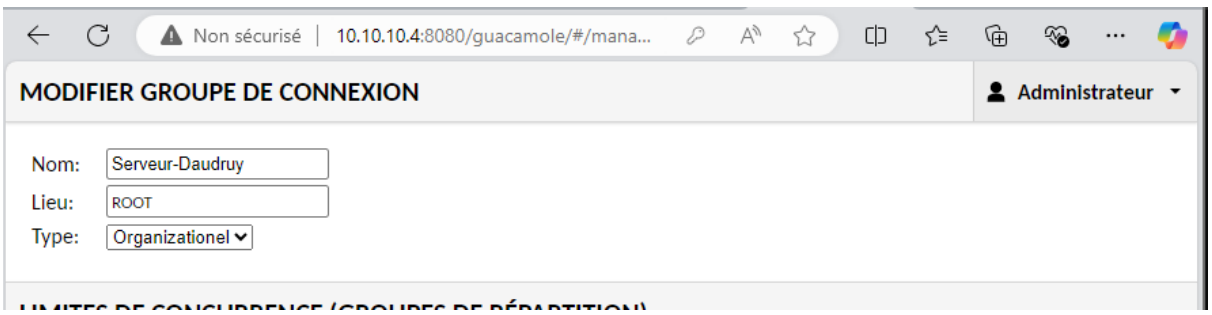
Pour se connecter, on va utiliser les identifiants par défaut : Utilisateur : guacadmin Mot de passe : guacadmin

Créer un nouveau compte admin



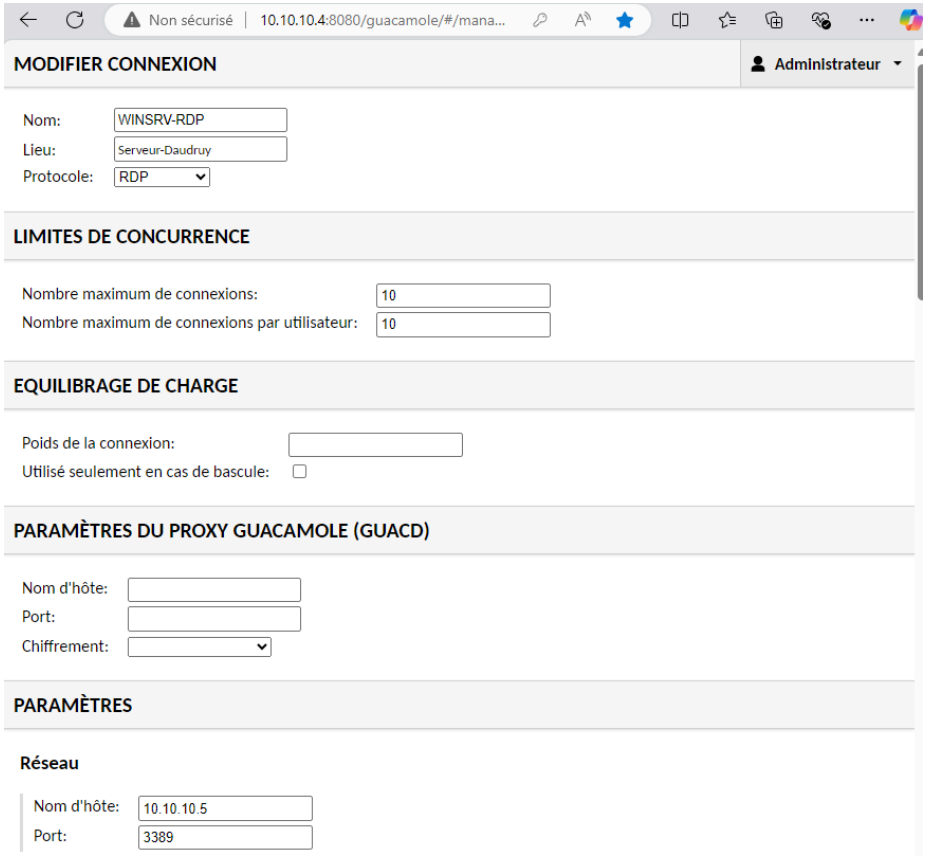
Ajouter une connexion RDP

on va créer un nouveau groupe pour organiser les machine 👍

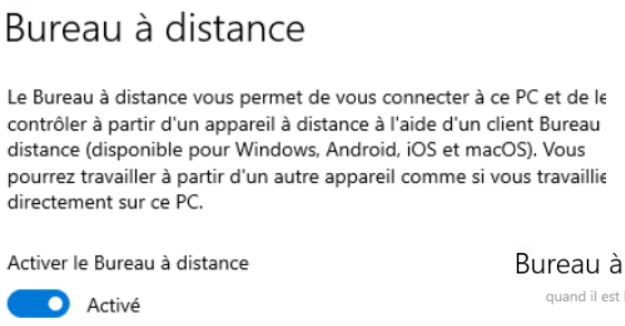


Zafar sio2

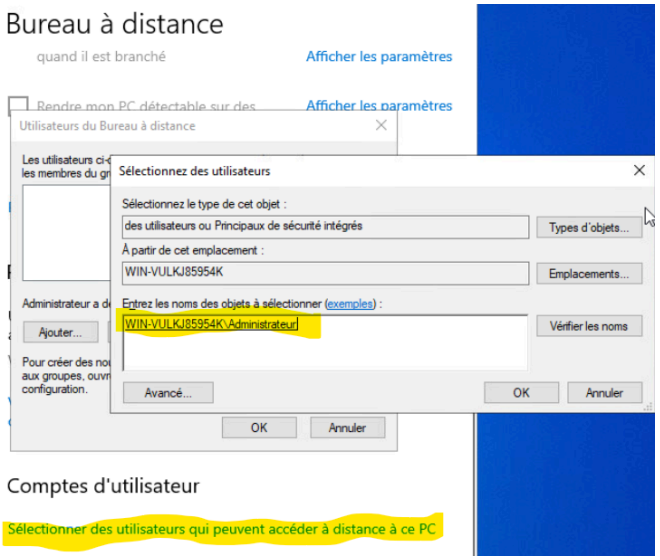
05/01/2025



Activer le Bureau à Distance (RDP) sur Windows :



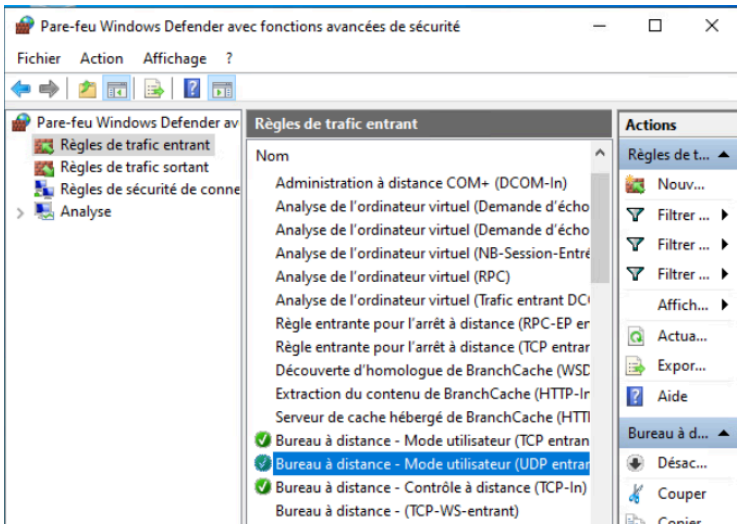
Autorise les utilisateurs RDP :



Zafar sio2

05/01/2025

Configurer le pare-feu Windows :

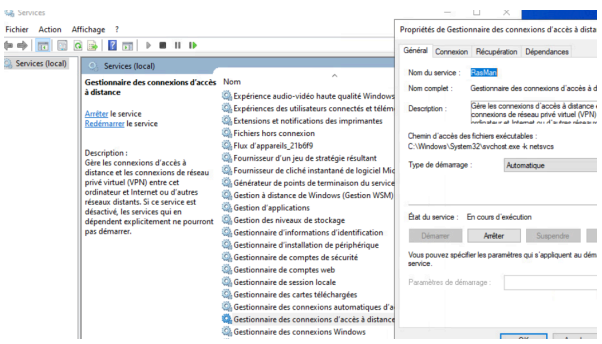


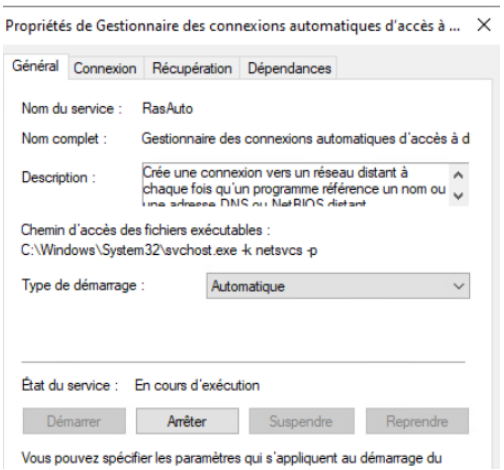

```
zafar@apache-guaca:~$ ping 10.10.10.5
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.
64 bytes from 10.10.10.5: icmp_seq=1 ttl=128 time=0.196 ms
64 bytes from 10.10.10.5: icmp_seq=2 ttl=128 time=0.195 ms
64 bytes from 10.10.10.5: icmp_seq=3 ttl=128 time=0.212 ms
```

```
C:\Users\Administrateur>ping 10.10.10.4

Envoi d'une requête 'Ping'  10.10.10.4 avec 32 octets de données :
Réponse de 10.10.10.4 : octets=32 temps<1ms TTL=64
Réponse de 10.10.10.4 : octets=32 temps<1ms TTL=64
```

```
zafar@apache-guaca:~$ sudo systemctl restart guacd
zafar@apache-guaca:~$ sudo ufw allow 3389
Rules updated
Rules updated (v6)
zafar@apache-guaca:~$ sudo ufw allow 4822
Rules updated
Rules updated (v6)
zafar@apache-guaca:~$ sudo ufw allow 8080
Rules updated
Rules updated (v6)
zafar@apache-guaca:~$
```

On vérifie le statut du service RDP:
Services.msc puis on démarre le RDP en mode **Automatique**.



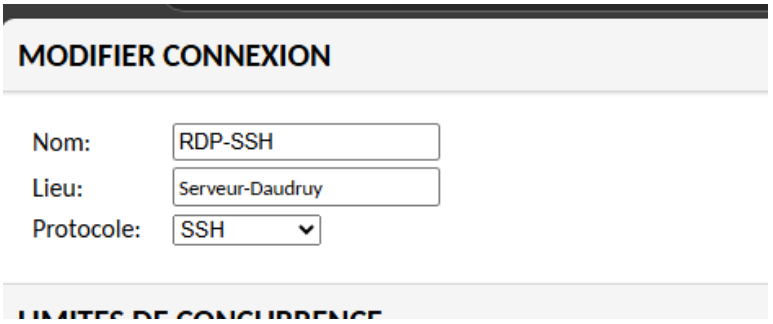


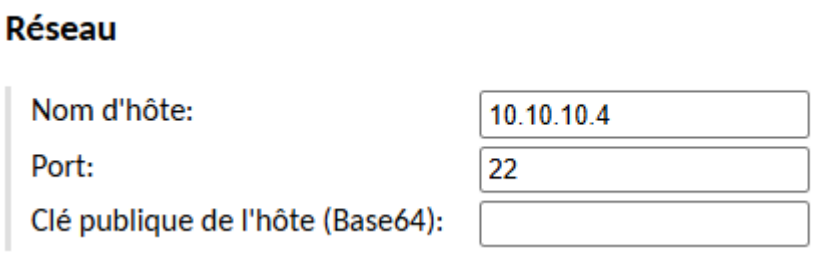
Zafar sio2

05/01/2025

Voilà nous avons une connexion en RDP sur un machine win 👍

Nous allons maintenant configurer la connexion en SSH





Jusqu' ici nous avons des configuré par défaut et des connexion et ssh et rdp

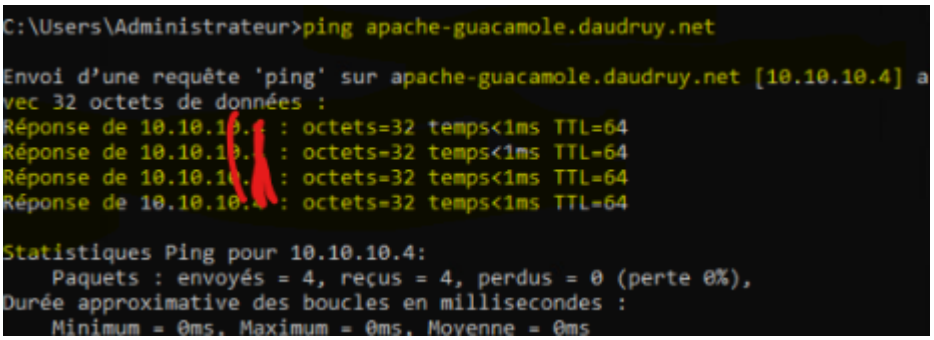
Maintenant nous allons configurer les configue avancé comme DNS Https Certificate SSL

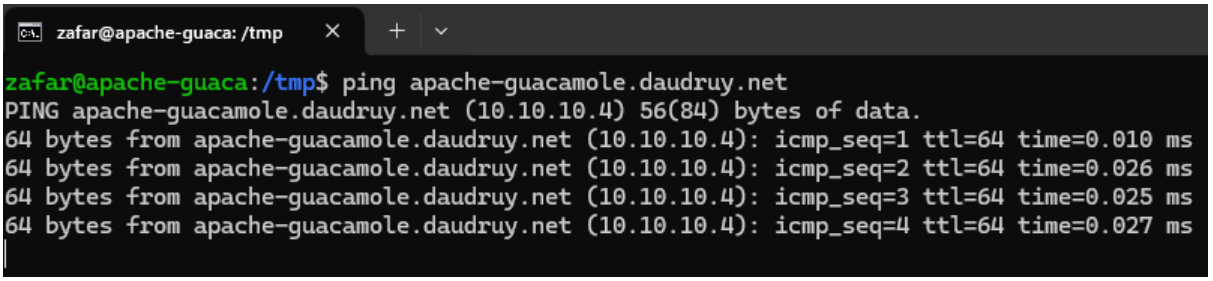
Zafar sio2

05/01/2025

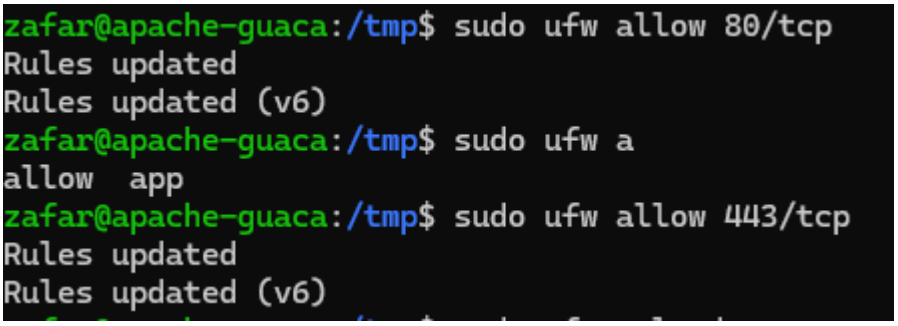
Configuration Avancé Guacamole

Le DNS est déjà configuré sur le serveur DNS, Nous allons configurer le dsn sur apache pour qu' il réponde en local

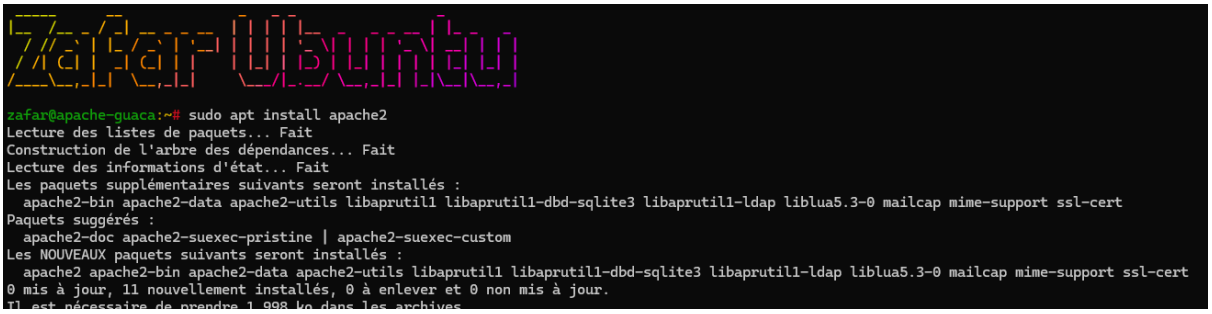




Configure firewall :



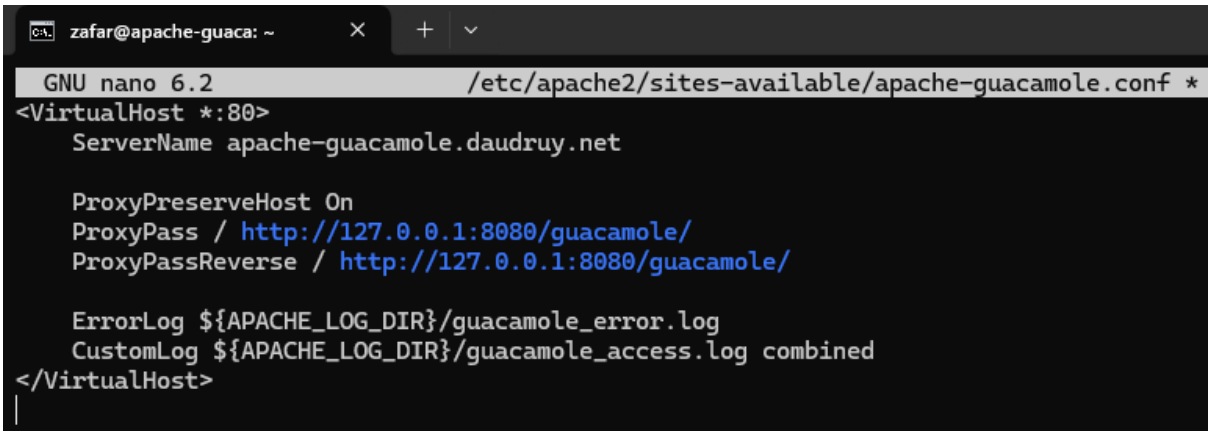
Pour la configure DNS on a besoin d'un Apache2

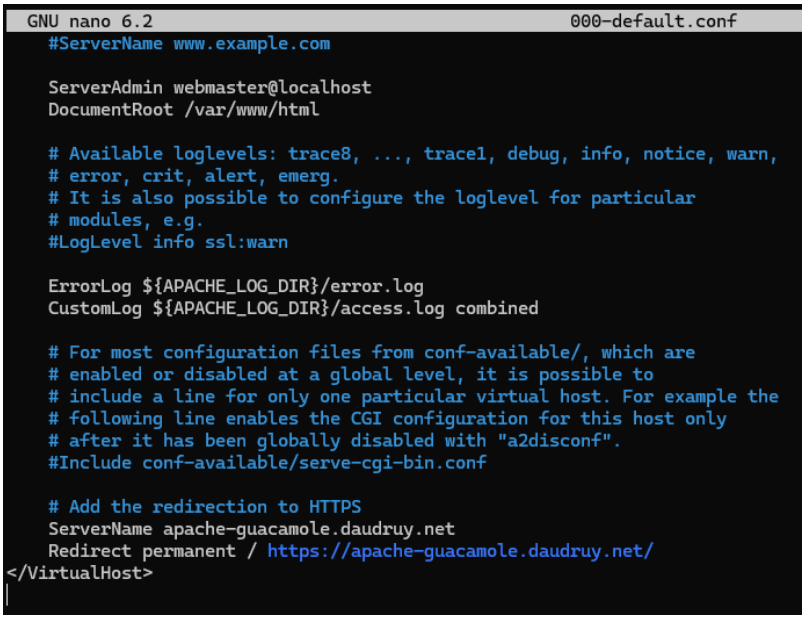


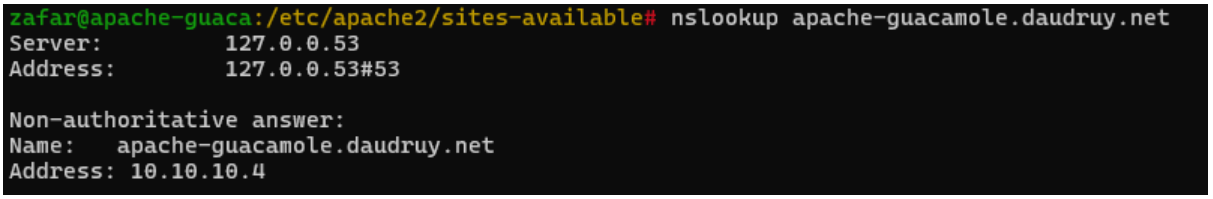
Zafar sio2

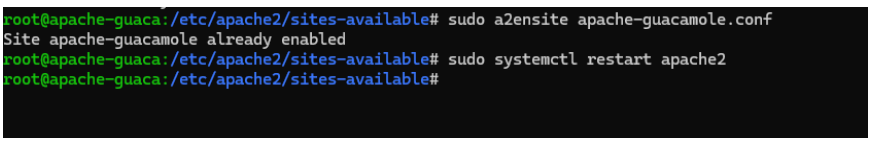
05/01/2025

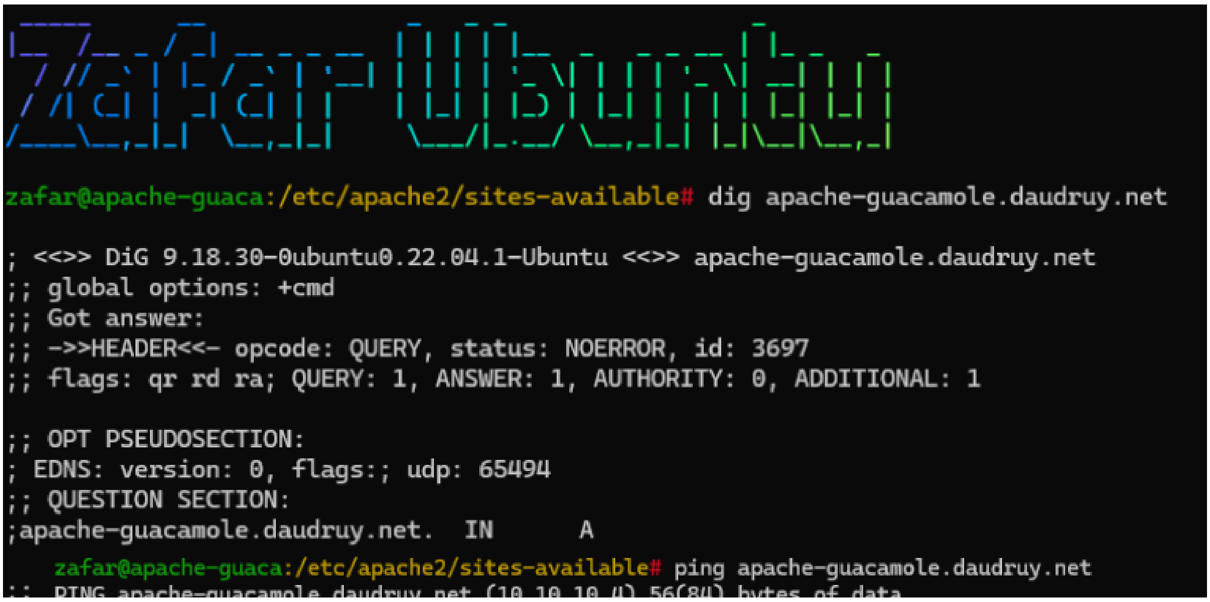
Sur Apache, la configuration des DNS se fait généralement dans les fichiers de configuration des hôtes virtuels, plus précisément dans les fichiers **`000-default.conf`** ou dans des fichiers personnalisés dans le répertoire **`/etc/apache2/sites-available/`**.
Ces fichiers sont utilisés pour définir des hôtes virtuels (Virtual Hosts) et peuvent inclure des directives qui spécifient les noms de domaine pour lesquels le serveur doit répondre.

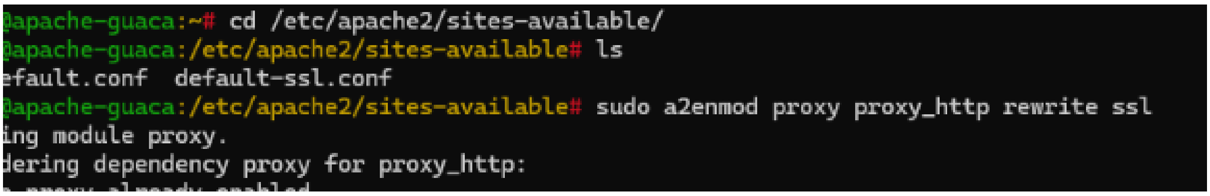




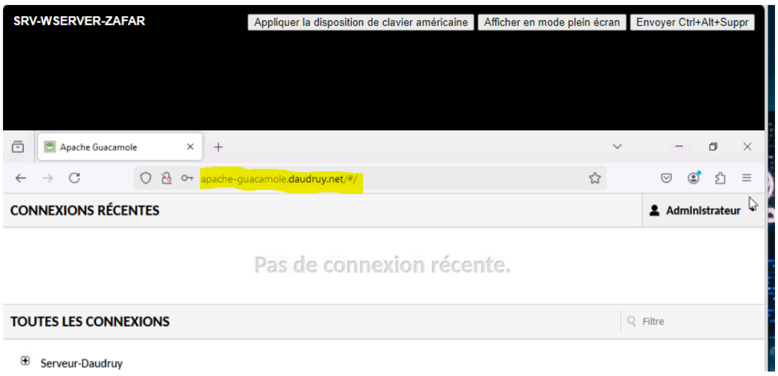








Nous allons tester la connexion DNS sur machine virtuelle en Local et la ca marche 👍

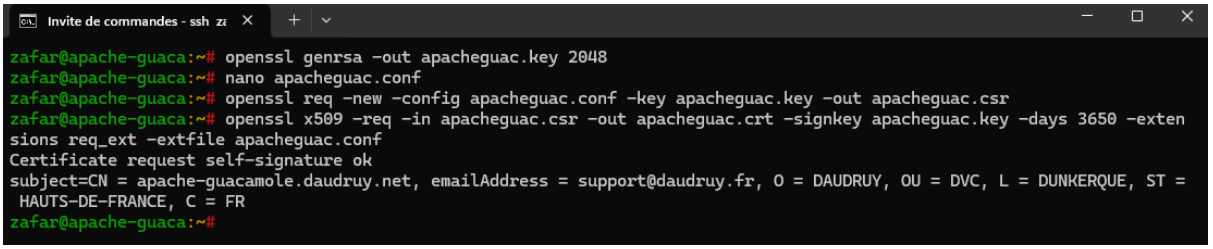


Le domaine `apache-guacamole.daudruy.net` est correctement résolu vers l'adresse IP `10.10.10.4`, confirmant que la configuration DNS est fonctionnelle.

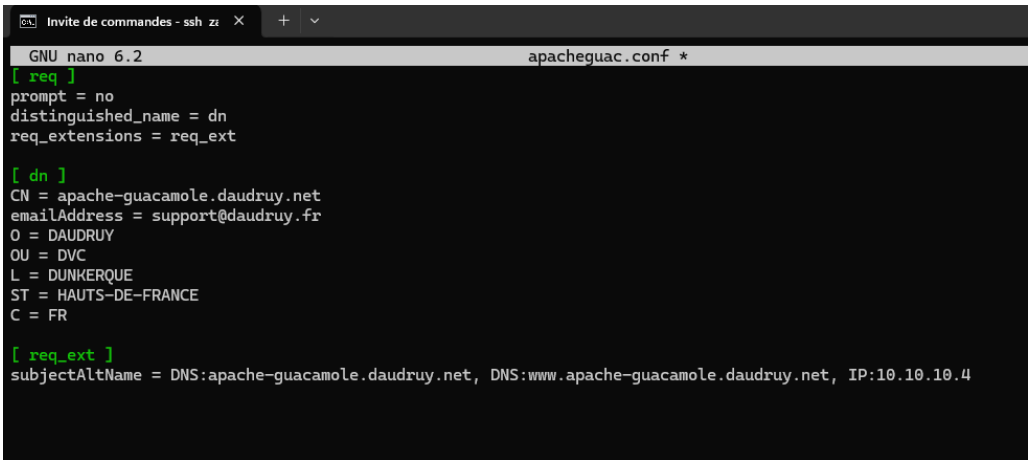
Certification SSL-HTTPS - HTTP

Solution pour avoir une connexion https sans le message de erreur de connexion https

On exécute cette commande pour générer une clé privée de 2048 bits :



On crée le fichier apache.conf Il contient la configuration **OpenSSL** pour créer un certificat auto-signé.

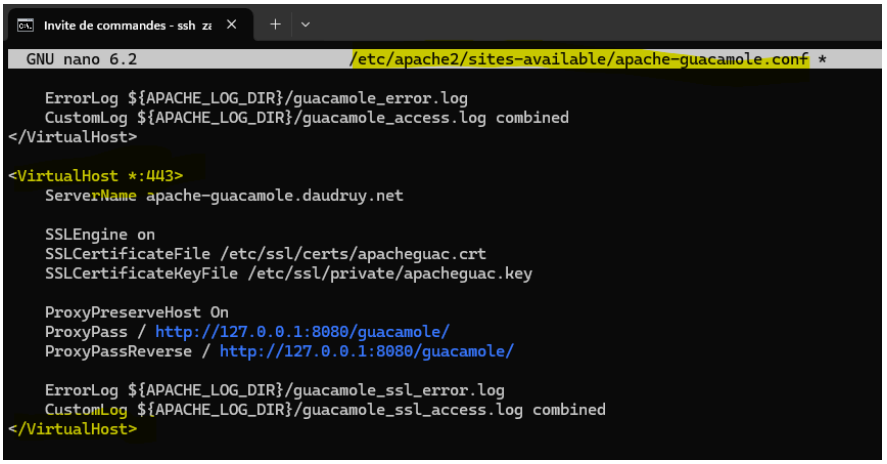


Configurer Apache pour utiliser le certificat

On déplace les fichiers générés dans les dossiers SSL d'Apache :

```
zafar@apache-guaca:~# sudo cp apacheguac.key /etc/ssl/private/
[sudo] password for zafar:
zafar@apache-guaca:~# sudo cp apacheguac.crt /etc/ssl/certs/
zafar@apache-guaca:~# sudo nano /etc/apache2/sites-available/apache-guacamole.conf
zafar@apache-guaca:~# sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
zafar@apache-guaca:~# sudo systemctl restart apache2
```

On modifié le fichier de configuration Apache et on ajoute les lignes suivantes :



Active le module SSL et redémarre Apache :

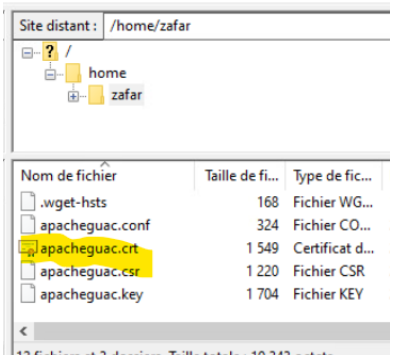
```
zafar@apache-guaca:~# sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
zafar@apache-guaca:~# sudo systemctl restart apache2
```

Zafar sio2

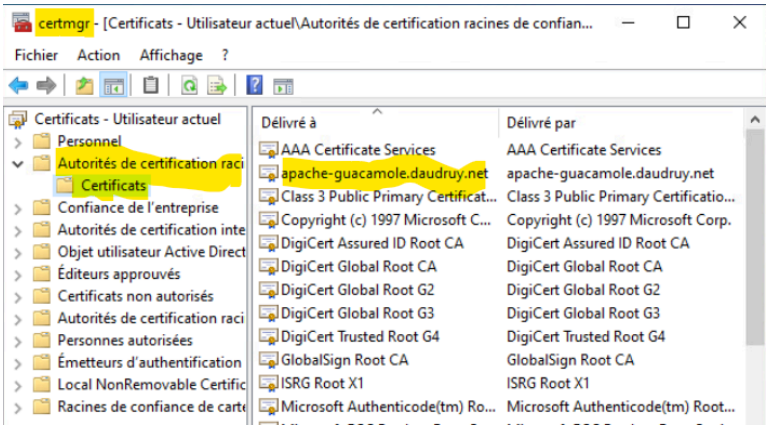
05/01/2025

Exporter le certificat et l'importer dans Windows

On récupère le certificate depuis filezilla:



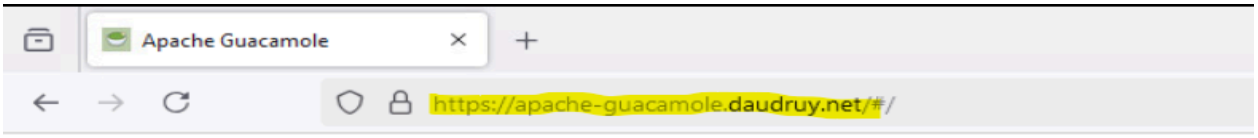
Importer le certificate dans Windows :



Zafar sio2

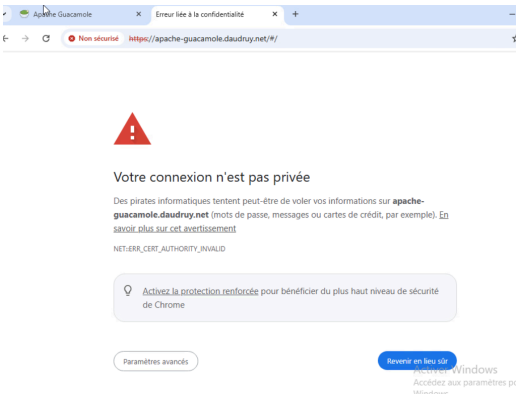
05/01/2025

On teste l'accès 👍



En résumé : On crée une clé privée, on génère un certificat SSL avec SAN via un fichier de configuration (`apacheguac.conf`), on configure Apache pour utiliser le certificat, on redémarre Apache, puis on exporte et importe le certificat dans Windows.

C'est un bon methode si on veut avoir des accès https en local sans avoir le massage sur la photo



Zafar sio2

05/01/2025

Mettre en place la double authentification TOTP

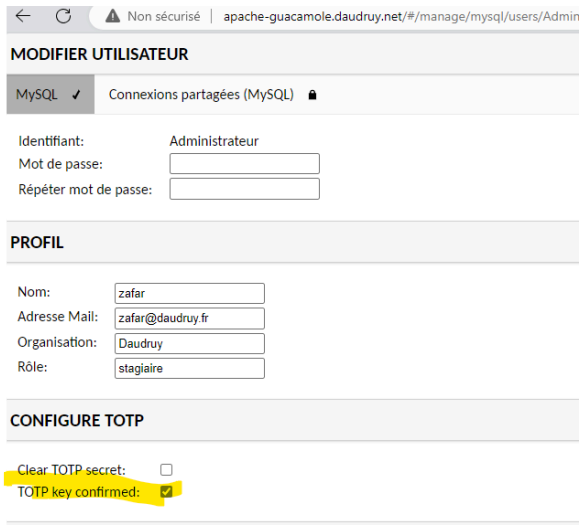
Pour bénéficier de la double authentification avec un code TOTP comme second facteur, une extension doit être ajoutée à Apache Guacamole.

```
zafar@apache-guaca:~# cd /tmp
zafar@apache-guaca:/tmp# wget https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-auth-totp-1.5.5.tar.gz
--2025-01-20 15:11:12--  https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-auth-totp-1.5.5.tar.gz
Resolving downloads.apache.org (downloads.apache.org)... 88.99.208.237, 135.181.214.104, 2a01:4f8:10a:39da::2, ...
Connecting to downloads.apache.org (downloads.apache.org)|88.99.208.237|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4923857 (4,7M) [application/x-gzip]
Saving to: 'guacamole-auth-totp-1.5.5.tar.gz'

guacamole-auth-totp-1.5.5.tar 100%[=============================================>]   4,70M  19,6MB/s    in 0,2s

2025-01-20 15:11:13 (19,6 MB/s) - 'guacamole-auth-totp-1.5.5.tar.gz' saved [4923857/4923857]

zafar@apache-guaca:/tmp#
```

```
zafar@apache-guaca:/tmp# tar -xzf guacamole-auth-totp-1.5.5.tar.gz
zafar@apache-guaca:/tmp# sudo mv guacamole-auth-totp-1.5.5/guacamole-auth-totp-1.5.5.jar /etc/guacamole/extensions/
[sudo] password for zafar:
zafar@apache-guaca:/tmp# sudo nano /etc/guacamole/guacamole.properties
zafar@apache-guaca:/tmp# sudo systemctl restart tomcat9
zafar@apache-guaca:/tmp# sudo nano /etc/guacamole/guacamole.properties
zafar@apache-guaca:/tmp# sudo systemctl restart tomcat9
zafar@apache-guaca:/tmp# sudo nano /etc/guacamole/guacamole.properties
zafar@apache-guaca:/tmp#
```

Invite de commandes - ssh zz

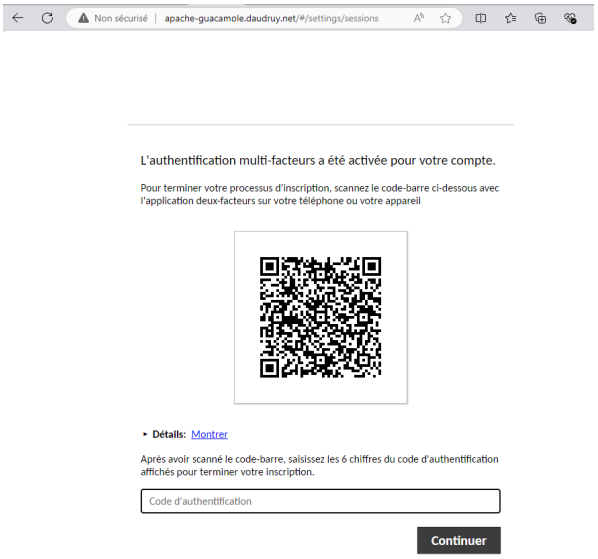
```
 GNU nano 6.2                                /etc/guacamole/guacamole.properties *
#declaration de de la connexion a Mariadb
#ce fichier est utile aussi pour d'autre parametres

# MySQL ------------------------
mysql-hostname: 127.0.0.1
mysql-port: 3306
mysql-database: guacadb
mysql-username: userdb
mysql-password: zafar
#-------------------------------



# TOTP
#ici on ajoute le nome de chaque utilisateur déja cree sur apache-guacamole
#pou le moment j'ai un compte admin
totp-issuer: Administrateur
totp-digits: 6
totp-period: 30
totp-mode: sha1
```

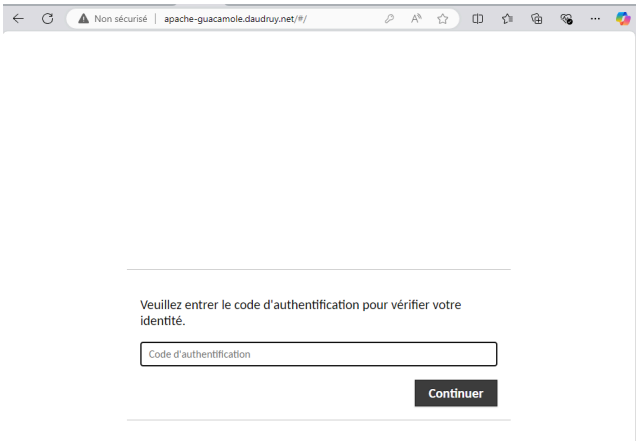


Zafar sio2

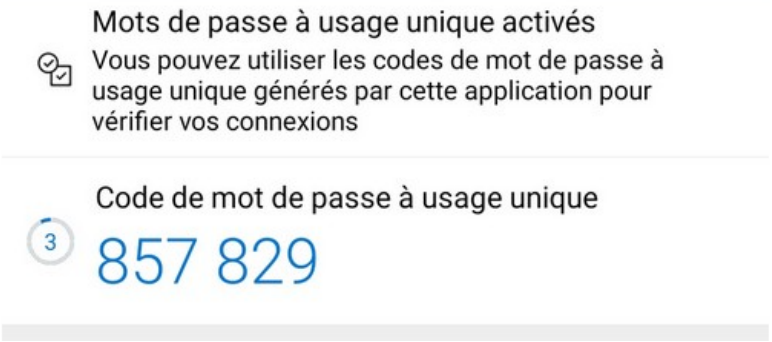
05/01/2025

On scan le code bar puis à chaque connexion il nous demande le code qui est dans le Microsoft authentificateur





Code reçu sur téléphone



05/01/2025

Configure avancé Apache-GUACAMOLE

Redirection de HTTP vers HTTPS

Objectif : Configurer Apache pour rediriger automatiquement les requêtes HTTP vers HTTPS pour le domaine `apache-guacamole.daudruy.net`.

Ici on redirige tout le trafic HTTP vers HTTPS
Ce fichier **gère les requêtes HTTP non sécurisées (port 80)** et contient :

```
zafar@apache-guaca:~# sudo nano /etc/apache2/sites-available/000-default.conf
zafar@apache-guaca:~#
```

```
  GNU nano 6.2                                          000-default.conf *
<VirtualHost *:80>

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html


    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined


    # Add the redirection to HTTPS
    ServerName apache-guacamole.daudruy.net
    Redirect permanent / https://apache-guacamole.daudruy.net/
</VirtualHost>
```

➡ Cela signifie que toutes les requêtes HTTP sont automatiquement redirigées vers HTTPS.

Zafar sio2

05/01/2025

Configuration du Proxy et SSL pour Guacamole (`apache-guacamole.conf`)

📌 But

Active le proxy vers Guacamole (port 8080)
Active **HTTPS avec un certificat SSL**
Redirige **HTTP → HTTPS**

```
 GNU nano 6.2                                    apache-guacamole.conf
<VirtualHost *:80>
    ServerName apache-guacamole.daudruy.net

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:8080/guacamole/
    ProxyPassReverse / http://127.0.0.1:8080/guacamole/

    ErrorLog ${APACHE_LOG_DIR}/guacamole_error.log
    CustomLog ${APACHE_LOG_DIR}/guacamole_access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerName apache-guacamole.daudruy.net

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apacheguac.crt
    SSLCertificateKeyFile /etc/ssl/private/apacheguac.key

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:8080/guacamole/
    ProxyPassReverse / http://127.0.0.1:8080/guacamole/

    ErrorLog ${APACHE_LOG_DIR}/guacamole_ssl_error.log
    CustomLog ${APACHE_LOG_DIR}/guacamole_ssl_access.log combined
</VirtualHost>


<VirtualHost *:80>
    ServerName apache-guacamole.daudruy.net
    Redirect permanent / https://apache-guacamole.daudruy.net/
</VirtualHost>
```

Activation ssl configure

```
zafar@apache-guaca:~# sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
zafar@apache-guaca:~#   systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to reload 'apache2.service'.
Authenticating as: admin (zafar)
Password:
==== AUTHENTICATION COMPLETE ===
zafar@apache-guaca:~#
```

Zafar sio2

05/01/2025

Configuration du Proxy pour l'IP locale (`guacamole.conf`)

📌 **But :** Accès à Guacamole via internet avec son IP et le port

```
 GNU nano 6.2                                    guacamole.conf *
<VirtualHost *:443>
    ServerName 10.10.10.4  # Remplace par ton IP publique ou nom de domaine
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/ton-certificat.crt  # Remplace avec certificat autorite le jours de mise en produ>
    SSLCertificateKeyFile /etc/ssl/private/ton-certificat.key

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:8080/  # Guacamole tourne sur Tomcat sur le port 8080
    ProxyPassReverse / http://127.0.0.1:8080/

    ErrorLog ${APACHE_LOG_DIR}/guacamole_error.log
    CustomLog ${APACHE_LOG_DIR}/guacamole_access.log combined
</VirtualHost>
```

Pare-feu :

```
zafar@apache-guaca:~# sudo systemctl start apache2
zafar@apache-guaca:~# sudo systemctl start tomcat9
zafar@apache-guaca:~# sudo netstat -tuln | grep 8080
sudo: netstat: command not found
zafar@apache-guaca:~# sudo ufw allow 80
Rule added
Rule added (v6)
zafar@apache-guaca:~# sudo ufw allow 443
Rule added
Rule added (v6)
zafar@apache-guaca:~# sudo ufw allow 8080
Skipping adding existing rule
Skipping adding existing rule (v6)
zafar@apache-guaca:~# sudo ufw reload
Firewall reloaded
```

Résultat Final

✅ **HTTP (port 80) → HTTPS (port 443)** automatique.
✅ **Guacamole accessible via https://apache-guacamole.daudruy.net**. En local
✅ **Sécurisation avec un certificat SSL**.
✅ **Reverse Proxy fonctionnel avec Apache vers Tomcat (Guacamole sur port 8080)**.

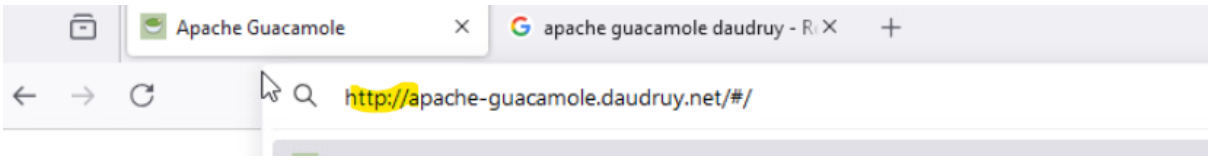
Tests réalisés

La redirection HTTP vers HTTPS est opérationnelle.
Le site est accessible uniquement via une connexion sécurisée HTTPS en local , sur internet il faut avoir un certificate

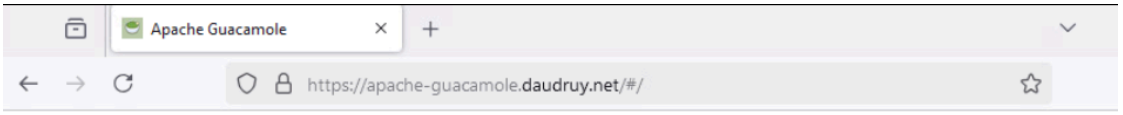
Zafar sio2

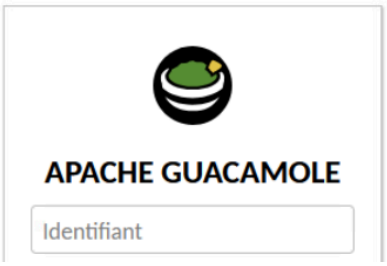
05/01/2025

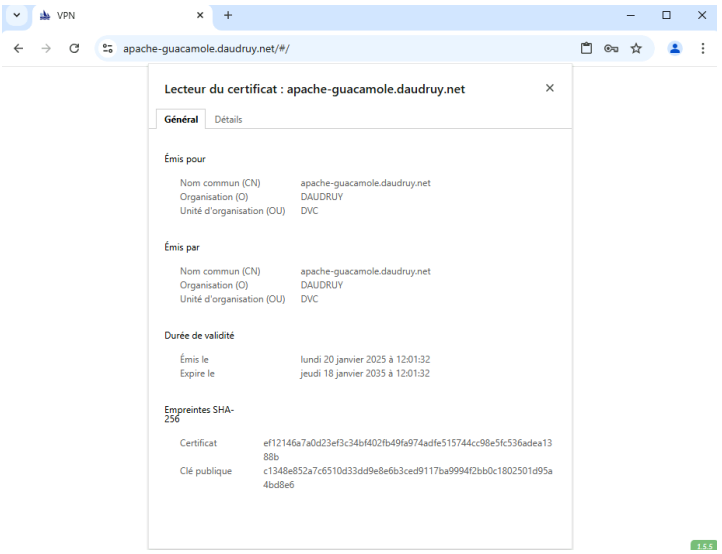
On tape http://



Et on est dirigé vers https://







Personalisation Guacamole

```
root@apache-guaca:/var/lib# su zafar
zafar@apache-guaca:/var/lib# su -
Password:
root@apache-guaca:~# cd /var/lib/tomcat9/webapps/guacamole/translations/
root@apache-guaca:/var/lib/tomcat9/webapps/guacamole/translations# ls
ca.json  de.json  es.json  it.json  ko.json  no.json  ru.json
cs.json  en.json  fr.json  ja.json  nl.json  pt.json  zh.json
```

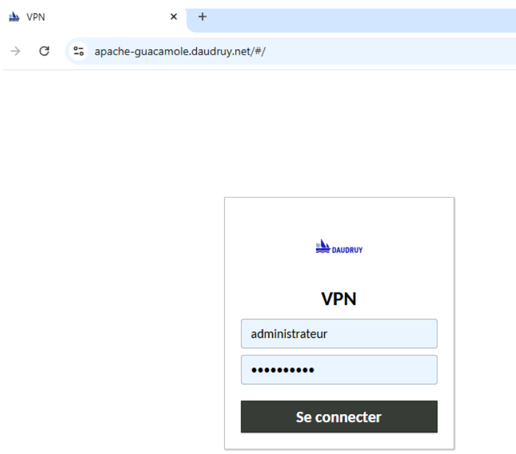
```
  GNU nano 6.2
{
    "NAME" : "English",

    "APP" : {

        "NAME"    : "VPN-GETWAY",
        "VERSION" : "1.5.5",
```

Changer le logo

```
root@apache-guaca:/var/lib/tomcat9/webapps/guacamole/images# chown tomcat logo-64.svg
root@apache-guaca:/var/lib/tomcat9/webapps/guacamole/images# chgrp tomcat logo-64.svg
root@apache-guaca:/var/lib/tomcat9/webapps/guacamole/images# systemctl restart guacd
root@apache-guaca:/var/lib/tomcat9/webapps/guacamole/images# systemctl restart tomcat9
root@apache-guaca:/var/lib/tomcat9/webapps/guacamole/images# ls -l
```

```
total 124
drwxr-x--- 2 tomcat tomcat 4096 janv. 17 13:03 action-icons
drwxr-x--- 2 tomcat tomcat 4096 janv. 17 13:03 arrows
-rw-r----- 1 tomcat tomcat  359 mars  29  2024 checker.svg
-rw-r----- 1 tomcat tomcat  369 mars  29  2024 checkmark.svg
-rw-r----- 1 tomcat tomcat 1408 mars  29  2024 circle-arrows.svg
-rw-r----- 1 tomcat tomcat  924 mars  29  2024 cog.svg
-rw-r----- 1 tomcat tomcat  994 mars  29  2024 drive.svg
-rw-r----- 1 tomcat tomcat  609 mars  29  2024 file.svg
-rw-r----- 1 tomcat tomcat  689 mars  29  2024 folder-closed.svg
-rw-r----- 1 tomcat tomcat  691 mars  29  2024 folder-open.svg
-rw-r----- 1 tomcat tomcat  984 mars  29  2024 folder-up.svg
drwxr-x--- 2 tomcat tomcat 4096 janv. 17 13:03 group-icons
-rw-rw-r-- 1 tomcat tomcat 2782 janv. 23 13:40 guac-tricolor.svg
-rw-r----- 1 tomcat tomcat 1180 mars  29  2024 lock.svg
-rw-r----- 1 tomcat tomcat 9167 mars  29  2024 logo-144.png
-rw-rw-r-- 1 zafar  zafar  2782 janv. 23 13:48 logo-64.svg
-rw-r----- 1 tomcat tomcat  647 mars  29  2024 magnifier.svg
```

On peut aller plus loin dans la configuration des interfaces personnalisées, mais comme ce n'est pas ma spécialité et que Guacamole utilise des langages comme JSON, JavaScript, etc., que je ne maîtrise pas totalement, cela complique les modifications. D'ailleurs, rien que la mise en place des logos m'a pris tout un après-midi à chercher dans les fichiers.



Zafar sio2

05/01/2025

Mise en place du Fail2Ban

Pour empêcher les attaques par force brute deviennent une menace sérieuse sur guacamole je me en place fail2ban

Commencez par installer Fail2Ban

```
zafar@apache-guaca:~# sudo apt update
[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
Lecture des informations d'état... Fait
1 paquet peut être mis à jour. Exécutez « apt list --upgradable » pour le voir.
zafar@apache-guaca:~# sudo apt install fail2ban -y
```

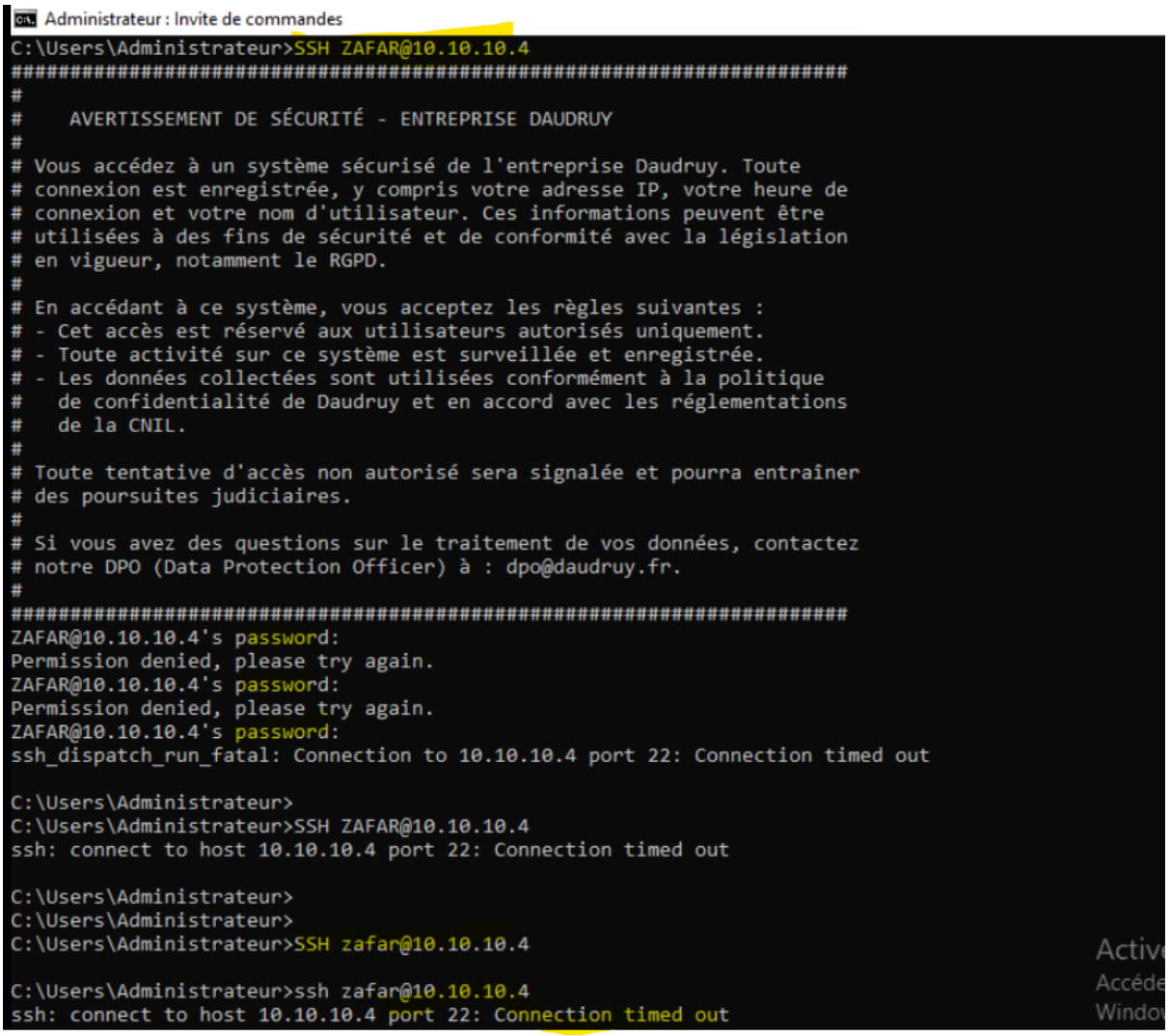
```
zafar@apache-guaca:~# cd /etc/fail2ban/
zafar@apache-guaca:/etc/fail2ban# ls
action.d  fail2ban.conf  fail2ban.d  filter.d  jail.conf  jail.d  paths-arch.conf  paths-common.conf  paths-debian.conf  paths-opensuse.conf
zafar@apache-guaca:/etc/fail2ban# sudo cp jail.conf jail.local
zafar@apache-guaca:/etc/fail2ban# sudo nano jail.local
```

```
  GNU nano 6.2                                                                jail.local
#
# SSH servers
#

[sshd]
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600
findtime = 600
```

```
zafar@apache-guaca:/etc/fail2ban# sudo systemctl enable fail2ban.service
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
zafar@apache-guaca:/etc/fail2ban# sudo systemctl restart fail2ban
zafar@apache-guaca:/etc/fail2ban# sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-01-23 10:49:35 UTC; 2s ago
       Docs: man:fail2ban(1)
   Main PID: 48431 (fail2ban-server)
      Tasks: 5 (limit: 9394)
```

Test

05/01/2025



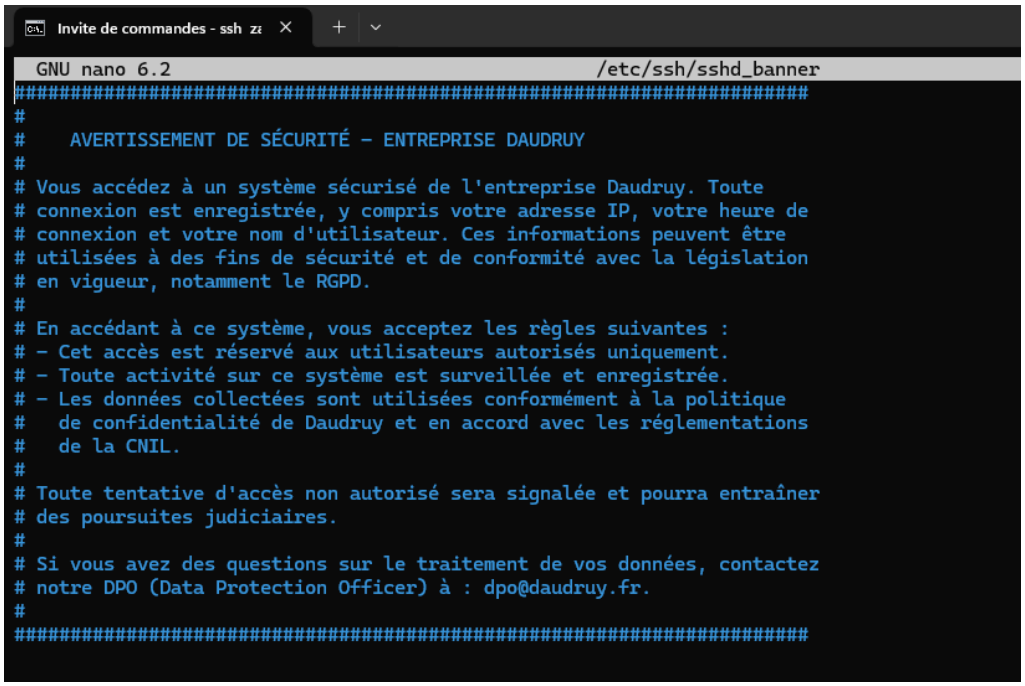

```
zafar@apache-guaca:/etc/fail2ban# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     2
   `- Banned IP list:   10.10.10.5
zafar@apache-guaca:/etc/fail2ban#
```

```
zafar@apache-guaca:/etc/fail2ban# sudo tail -f /var/log/fail2ban.log
2025-01-23 11:21:39,076 fail2ban.filter         [48752]: INFO    Added logfile: '/var/log/auth.log' (pos = 94190, ha
2025-01-23 11:21:39,079 fail2ban.jail           [48752]: INFO    Jail 'sshd' started
2025-01-23 11:21:39,277 fail2ban.actions        [48752]: NOTICE  [sshd] Restore Ban 10.10.10.5
2025-01-23 11:27:08,249 fail2ban.actions        [48752]: NOTICE  [sshd] Unban 10.10.10.5
2025-01-23 11:31:31,230 fail2ban.filter         [48752]: INFO    [sshd] Found 10.10.10.5 - 2025-01-23 11:31:31
2025-01-23 11:31:42,318 fail2ban.filter         [48752]: INFO    [sshd] Found 10.10.10.5 - 2025-01-23 11:31:41
2025-01-23 11:31:47,885 fail2ban.filter         [48752]: INFO    [sshd] Found 10.10.10.5 - 2025-01-23 11:31:47
2025-01-23 11:31:48,581 fail2ban.actions        [48752]: NOTICE  [sshd] Ban 10.10.10.5
```

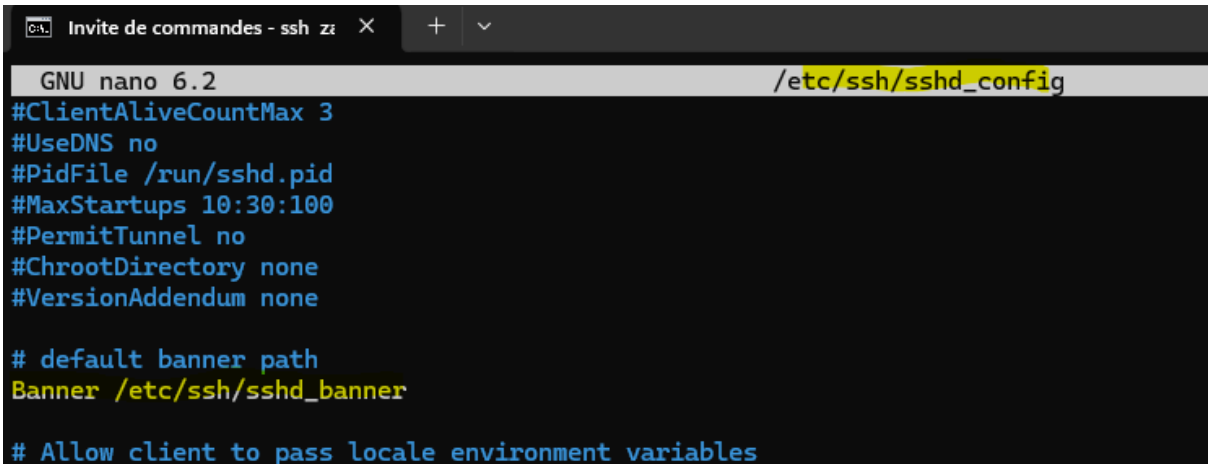
Bannière de connexion SSH avec conformité RGPD

05/01/2025

```
zafar@apache-guaca:/etc/fail2ban# sudo nano /etc/ssh/sshd_banner
```




```
zafar@apache-guaca:/etc/fail2ban# sudo nano /etc/ssh/sshd_config
```



05/01/2025

B. Créer un enregistrement vidéo des sessions

Téléchargement de l'extension

```
root@apache-guaca:/tmp# wget https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-history-recording-storage-1.5.5.tar.gz
--2025-01-15 09:08:00--  https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-history-recording-storage-1.5.5.tar.gz
Resolving downloads.apache.org (downloads.apache.org)... 88.99.208.237, 135.181.214.104, 2a01:4f9:3a:2c57::2, ...
Connecting to downloads.apache.org (downloads.apache.org)|88.99.208.237|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15894 (16K) [application/x-gzip]
Saving to: 'guacamole-history-recording-storage-1.5.5.tar.gz'

guacamole-history-recording-storage-1.5.5.tar.gz     100%[=============================================================================================================>]  15,52K  --.-KB/s    in 0,02s

2025-01-15 09:08:00 (661 KB/s) - 'guacamole-history-recording-storage-1.5.5.tar.gz' saved [15894/15894]

root@apache-guaca:/tmp#
```

Puis, on décompresse l'archive tar.gz , On déplace le fichier .jar de l'extension vers le répertoire "extensions" de Guacamole :

```
root@apache-guaca:/tmp# sudo mv guacamole-history-recording-storage-1.5.5/guacamole-history-recording-storage-1.5.5.jar /etc/guacamole/extensions/
```

On redémarre le service puis crée un répertoire pour l' enregistrement

```
root@apache-guaca:/etc/guacamole/extensions# ls
guacamole-auth-jdbc-mysql-1.5.5.jar  guacamole-history-recording-storage-1.5.5.jar
```

```
root@apache-guaca:/etc/guacamole/extensions# ls -ld /var/lib/guacamole/recordings
drwxrws--- 2 tomcat tomcat 4096 janv. 15 09:10 /var/lib/guacamole/recordings
root@apache-guaca:/etc/guacamole/extensions# sudo chown -R root:tomcat /var/lib/guacamole/recordings
root@apache-guaca:/etc/guacamole/extensions# sudo chmod -R 770 /var/lib/guacamole/recordings
root@apache-guaca:/etc/guacamole/extensions# sudo usermod -aG tomcat $(ps -o user= -p $(pgrep guacd))
root@apache-guaca:/etc/guacamole/extensions# sudo systemctl restart guacd
```

```
root@apache-guaca: /etc/gua
  GNU nano 6.2                                  guacamole.properties
# MySQL
mysql-hostname=127.0.0.1
mysql-port=3306
mysql-database=guacadb
mysql-username=db-user
mysql-password=zafar

#activer les logs en mode débogage
guacd-hostname: localhost
guacd-port: 4822
log-level: debug



recording-path: /var/lib/guacamole/recordings
recording-name: ${GUAC_DATE}-${GUAC_TIME}-${GUAC_USERNAME}
create-recording-path: true
```

Il faut juste faire attention au droit de différent fichier et utilisateur

guacadmin	15-01-2025 12:45:22	24 secondes	ssh-apache	192.168.40.65	
guacadmin	15-01-2025 12:32:51	28 secondes	win-rdp-test	192.168.40.65	View
guacadmin	15-01-2025 12:32:29	3 secondes	ssh-apache	192.168.40.65	

Pour ssh : il vas utiliser la meme dossier que rdp et la meme chemins

Créer automatiquement le chemin typescript : ☐

Enregistrement Ecran

Chemin de l'enregistrement:	${HISTORY_PATH}/${HIST
Nom de l'enregistrement:	${GUAC_DATE}-${GUAC_
Exclure les graphiques/flux:	☐
Exclure la souris:	☐
Inclure les événements clavier:	☐
Créer automatiquement le chemin d'enregistrement:	☑

guacadmin	15-01-2025 14:22:25	22 secondes	ssh-apache	192.168.40.65	View
guacadmin	15-01-2025 14:21:14	15 secondes	ssh-apache	192.168.40.65	View

Les enregistrements des video de session utilisateur ont été sauvegardées le PC

Conclusion

Durant ces trois semaines de stage, j'ai pu rechercher et configurer **Guacamole**, en passant par :

✅ **Installation et base de données**
✅ **Mise en place de l'authentification TOTP**
✅ **Configuration DNS et certificat SSL auto-généré**
✅ **Déploiement du certificat sur PC**
✅ **Activation de HTTPS et redirection HTTP → HTTPS**
✅ **Enregistrement des sessions**
✅ **Sécurisation avec Fail2Ban**

Tout au long de cette configuration, j'ai rencontré plusieurs problématiques, mais j'ai pu les résoudre en m'appuyant sur la documentation et des ressources adaptées. Ce stage m'a permis de renforcer mes compétences en administration système linux et en sécurisation des services.