MK-Guacamole

01 - Description

Une description :

Nom DNS interne :
Nom DNS Externe :
Type de serveur (Physique, VMware, LXC, Docker...) : Conteneur LXC
OS : Ubuntu 22.04
CPU :
RAM :
Disque LVM :
/ :

Réseaux :

Adresse IP :
Masque : 255.255.255.0
Passerelle :
DNS : 192.168.1.50
VLAN :

1. Checklist - Création du serveur :

Domaine :

[*] Configuration de l'enregistrement A sur v.sdem.fr
[*] Configuration de l'enregistrement PTR sur v.sdem.fr
[*] Configuration de l'enregistrement A sur sdem.fr (interne)
[x] Configuration de l'enregistrement A sur sdem.fr (externe)
[x] Ajout du serveur dans la zone DNS morbihan-energies.fr avec un enregistrement CNAME

Sécurité :

[*] Création compte adminme
[*] Changement mot de passe root
[*] Changement mot de passe adminme
[*] Sécurisation des mots de passe (20 caractères minimum et 3 types de caractères différents)
[*] Mise à jour du coffre fort de mot de passe
[*] Déploiement clé SSH
[*] Paramétrage du SUDO NOPASSWORD
Liste des Ports ouverts :

Sauvegarde :

[*] Configurer la sauvegarde locale
[*] Configurer la sauvegarde sur le PRA (si serveur critique)
[ ] Configurer la sauvegarde de Base de données (Dump local)

Autres :

[*] Ajout du serveur dans Guacamole
[*] Ajout du serveur dans la supervision
[*] Ajout de la documentation d'installation et de paramétrage de la VM dans ZIM
[ ] Configuration du NTP

A - Qu'est ce que Guacamole:

Le serveur Apache Guacamole sera utilisé comme point d'entrée unique 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 passer obligatoirement par l'hôte Apache Guacamole.

Dans l'exemple ci-dessous, l'hôte Apache Guacamole est positionné en DMZ puisqu'il doit être accessible depuis l'extérieur. L'accès depuis l'extérieur n'est pas obligatoire puisque l'on pourrait imposer une connexion VPN au réseau de l'entreprise avant de permettre la connexion sur l'interface de Guacamole. De la même manière pour publier l'hôte Guacamole sur Internet, il est recommandé de s'appuyer sur un reverse proxy en frontal (le pare-feu pourrait très bien assurer cette fonction), ce qui permettra en même temps de passer les flux en HTTPS.

image.png
Image not found or type unknown

Apache Guacamole devient un élément central de l'infrastructure puisqu'il sert de **passerelle pour administrer les machines**. Rassurez-vous, il est possible d'avoir plusieurs hôtes Apache Guacamole pour **répartir la charge et assurer la haute disponibilité**.

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.

02 - Installation

A - Installation de Guacamole :

1. Installation des Dépendances :

```
sudo apt-get install libcairo2-dev libjpeg-turbo8-dev libpng-dev libtool-bin uuid-dev libossp-uuid-dev
libwebsockets-dev libssl-dev libavcodec-dev freerdp2-dev libpango1.0-dev libssh2-1-dev libtelnet-dev
libwebsockets-dev libpulse-dev libvorbis-dev libwebp-dev libavcodec-dev libavformat-dev libavutil-dev
libswscale-dev
```

2. Télécharger Serveur Guacamole :

```
wget https://downloads.apache.org/guacamole/1.5.3/source/guacamole-server-1.5.3.tar.gz
```

3. Décompression :

```
tar -xvf guacamole-server-1.5.3.tar.gz
cd guacamole-server-1.5.3
autoreconf -fi
```

4. Script de Configuration :

```
./configure --with-init-dir=/etc/init.d
```

5. Compilation et installation :

```
make
make install
```

6. Liens :

```
ldconfig
```

Redémarrage des services 1

```
systemctl restart guacd
```

B - Installation de Tomcat :

1. Installation de Tomcat :

```
sudo apt-get install tomcat9 tomcat9-admin tomcat9-common tomcat9-user
sudo mkdir /etc/guacamole/
sudo wget https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-1.5.3.war -O
/etc/guacamole/guacamole.war
```

2. Lien symbolique avec Tomcat :

```
sudo wget https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-1.5.3.war -O
/etc/guacamole/guacamole.war
```

Redémarrer Guac Tomcat 1

```
systemctl restart tomcat9
systemctl restart guacd
```

3. Extension du répertoire :

```
mkdir /etc/guacamole/{extensions,lib}
```

C-MYSQL :

1. Installation de MySQL :

```
apt install mariadb-server
mysql_secure_installation
```

2. Création d'une base de données Guacamole :

```
mysql -u root -p
CREATE DATABASE guacamole_db;
CREATE USER 'guacamole_user'@'localhost' IDENTIFIED BY 'Testeur';
GRANT SELECT,INSERT,UPDATE,DELETE ON guacamole_db.* TO 'guacamole_user'@'localhost';
FLUSH PRIVILEGES;
quit;
```

3. Module Mysql/Guacamole :

```
wget https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-auth-jdbc-1.5.3.tar.gz
tar -xvf guacamole-auth-jdbc-1.5.3.tar.gz
```

4. Extension Mysql/Guacamole :

```
cp guacamole-auth-jdbc-1.5.3/mysql/guacamole-auth-jdbc-mysql-1.5.3.jar /etc/guacamole/extensions/
```

5. Importer le schéma dans la base de donné :

```
cat guacamole-auth-jdbc-1.5.3/mysql/schema/*.sql | mysql -u root -p guacamole_db
```

6. Pilote Mysql/Guacamole :

```
wget https://cdn.mysql.com//Downloads/Connector-J/mysql-connector-j-8.0.33.tar.gz
tar -xvzf mysql-connector-j-8.0.33.tar.gz
cp mysql-connector-j-8.0.33/mysql-connector-j-8.0.33.jar /etc/guacamole/lib/
```

Redémarrage Mysql 1

```
systemctl restart mariadb.service
```

7. Fichier de propriété Guacamole :

```
touch /etc/guacamole/guacamole.properties
nano /etc/guacamole/guacamole.properties

echo "
# Hostname and Guacamole server port
guacd-hostname: localhost
guacd-port: 4822

# MySQL properties
mysql-hostname: localhost
mysql-port: 3306
mysql-database: guacamole_db
mysql-username: guacamole_user
mysql-password: Testeur
" > /etc/guacamole/guacamole.properties
```

Redémarrer Guac Tomcat 2

```
systemctl restart tomcat9
systemctl restart guacd
```

8. Connexion via l'interface :

http://adresseIP:8080/guacamole/

D - Connexion LDAP :

1. Installation du LDAP :

Tout d'abord, connectez-vous sur le serveur Guacamole en ligne de commande afin d'installer l'extension LDAP.

Ensuite, positionnez-vous dans "/tmp" et téléchargez l'archive tar.gz de l'extension :

```
cd /tmp
wget https://downloads.apache.org/guacamole/1.5.2/binary/guacamole-auth-ldap-1.5.2.tar.gz
```

Une fois que c'est fait, décompressez cette archive tar.gz :

```
tar -xzf guacamole-auth-ldap-1.5.2.tar.gz
```

Puis, déplacez le fichier JAR de l'extension vers le répertoire "extensions" de Guacamole.

```
sudo mv guacamole-auth-ldap-1.5.2/guacamole-auth-ldap-1.5.2.jar /etc/guacamole/extensions
```

Pour que cette extension soit prise en charge, il convient de redémarrer Tomcat9 :

```
sudo systemctl restart tomcat9
```

2. Connexion au LDAP :

Toujours sur le serveur Apache Guacamole, ouvrez le fichier de configuration :

```
sudo nano /etc/guacamole/guacamole.properties
```

Dans ce fichier, il y a déjà d'autres propriétés définies, notamment les informations de connexion à la base de données MySQL (MariaDB). Vous devez configurer l'extension LDAP.

Tout d'abord, vous devez indiquer le nom du contrôleur de domaine, le port LDAP (*389* par défaut) et la méthode de chiffrement (*none* avec du LDAP classique). Ce qui donne les lignes suivantes à ajouter dans le fichier :

```
### Active Directory
# Controleur de domaine
ldap-hostname: ldap.v.sdem.fr
ldap-port: 389
ldap-encryption-method: none
```

Deuxièmement, à la suite, vous devez ajouter les informations sur le compte à utiliser pour s'authentifier auprès de l'annuaire Active Directory. Ce compte sert uniquement à lire le contenu de l'annuaire (utilisateurs, groupes et membre des groupes). Dans l'exemple ci-dessous, le compte « *Sync_Guacamole@it-connect.local* » est utilisé.

```
# Utilisateur pour connexion AD
ldap-search-bind-dn: cn=LDAP Administrator,ou=DIT Roles,dc=sdem,dc=fr
ldap-search-bind-password: PASSWORD
```

Troisièmement, vous devez indiquer **comment rechercher les utilisateurs dans l'Active Directory** . Comme base DN, c'est-à-dire comme **base de recherche** , on évite de mettre la racine de l'annuaire Active Directory.

Ici, l'OU " *OU=Tiering,OU=IT,DC=it-connect,DC=local* " qui contient d'autres sous-OU ainsi que les comptes d'administration seront ciblés. Tout ce qui est en dehors de cette racine " *ne sera pas vu* " par Guacamole. Ceci correspond au paramètre " **ldap-user-base-dn** ". Ensuite, le paramètre " **ldap-username-attribute** " sert à préciser l'attribut AD utilisé pour les noms d'utilisateurs.

Enfin, le paramètre « **ldap-user-search-filter** » permet de déclarer le filtre de recherche. Ici, on prend tous les utilisateurs qui sont membres du groupe de sécurité Active Directory « **GDL-Guacamole-Access** ».

```
# Recherche des utilisateurs
ldap-user-base-dn: ou=People,dc=sdem,dc=fr
ldap-username-attribute: uid
#ldap-user-search-filter:
(&(objectClass=User)(sAMAccountName=*)(memberOf:1.2.840.113556.1.4.1941:=CN=GDL-Guacamole-A>
```

Quatrièmement, vous devez **ajouter des paramètres de recherche pour les groupes** . Si vous souhaitez rechercher uniquement les utilisateurs, cette partie n'est pas obligatoire. Sur le même principe, on indique la base de recherche et le filtre. Ici, on prend tous les groupes situés sous la base DN.

```
# Recherche des groupes
#ldap-group-base-dn: OU=Tiering,OU=IT,DC=it-connect,DC=local
#ldap-group-search-filter: (objectClass=Group)
```

Le fichier de configuration est prêt ! Sauvegardez et fermez le fichier. Il ne reste plus qu'à relancer Tomcat9 :

```
sudo systemctl restart tomcat9
```