
TITRE DU PROJET

**Déploiement d'un Bastion d'Administration Apache Guacamole sous
Debian 12**

BTS SIO – Option SISR

Projet professionnel E6

Réalisé par : Amir Tajik-Heulin

1. Présentation du projet

Dans le cadre de ma formation BTS SIO option SISR, j'ai réalisé la mise en place d'un serveur Apache Guacamole sous Debian 12 afin de centraliser et sécuriser l'accès aux serveurs de l'infrastructure.

L'objectif était de déployer une solution de bastion permettant aux administrateurs de se connecter aux équipements informatiques via une interface Web unique, sans installer de client spécifique.

Cette solution permet l'utilisation des protocoles :

- RDP
- SSH
- VNC
- Telnet

ainsi que la centralisation des accès administrateurs.

2. Contexte professionnel

L'entreprise souhaite améliorer la sécurité des accès administratifs.

Avant le projet :

- connexions directes RDP
- absence de traçabilité
- pas de centralisation
- risque élevé en cas de compromission

Après le projet :

- point d'accès unique
 - journalisation
 - authentification renforcée
 - contrôle des connexions
-

3. Analyse des besoins

Les besoins identifiés étaient :

Sécurité

- limiter les accès administrateurs
- supprimer les connexions RDP directes

Administration

- centraliser l'accès aux serveurs

Traçabilité

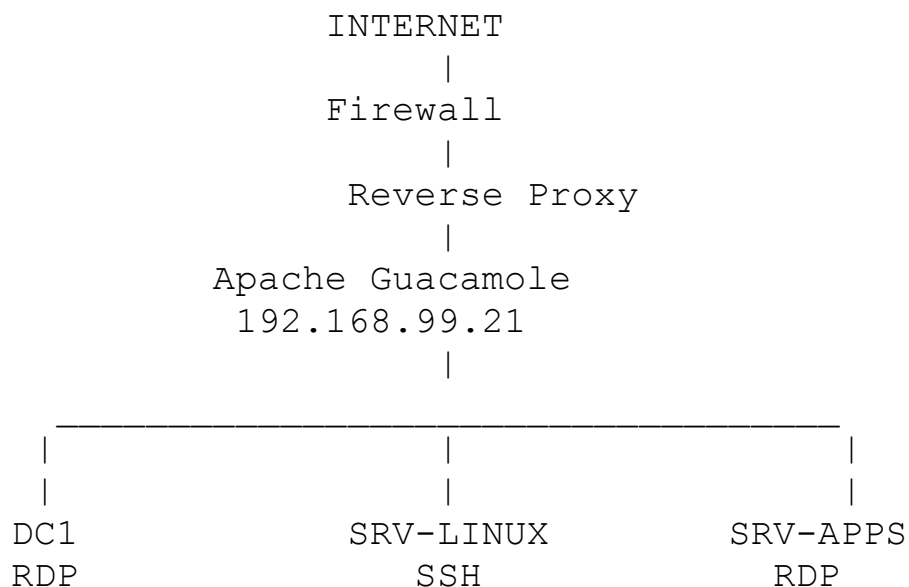
- connaître :
 - qui
 - quand
 - combien de temps
 - depuis quelle adresse IP

Haute disponibilité

- possibilité d'ajouter plusieurs bastions Guacamole

4. Architecture technique

Schéma d'architecture



Machines utilisées

Machine	OS
Guacamole	Debian 12
DC1	Windows Server 2022
SRV-LINUX	Debian
Client	Windows 11

5. Pourquoi Apache Guacamole ?

Apache Guacamole offre plusieurs avantages :

Accès Web

Aucun client RDP n'est nécessaire.

Gestion centralisée

Toutes les connexions passent par le bastion.

MFA

Authentification à deux facteurs.

Historique

Traçabilité complète.

Enregistrement vidéo

Possibilité d'enregistrer les sessions administrateur.

6. Installation de Debian 12

Machine virtuelle créée sous VMware :

Ressource	Valeur
CPU	2 vCPU
RAM	4 Go
Disque	40 Go

Installation minimale Debian 12.

Mise à jour :

```
apt update  
apt upgrade -y
```

7. Installation de Guacamole Server

Installation des dépendances :

```
apt-get install build-essential  
libcairo2-dev  
freerdp2-dev  
libssh2-1-dev  
libvncserver-dev
```

Compilation :

```
./configure  
make  
make install
```

Activation du service :

```
systemctl enable guacd  
systemctl start guacd
```

8. Installation de Tomcat

Installation :

```
apt install tomcat9
```

Déploiement du fichier :

```
guacamole.war
```

Redémarrage :

```
systemctl restart tomcat9
```

9. Base de données MariaDB

Installation :

```
apt install mariadb-server
```

Création :

```
CREATE DATABASE guacadb;
```

Création utilisateur :

```
CREATE USER 'guacamole';
```

Import du schéma SQL.

10. Configuration Apache Guacamole

Fichier :

```
/etc/guacamole/guacamole.properties
```

Configuration :

```
mysql-hostname  
mysql-port  
mysql-database  
mysql-username  
mysql-password
```

11. Création des comptes administrateurs

Actions réalisées :

- création d'un nouveau compte administrateur
- suppression du compte guacadmin
- définition d'un mot de passe complexe

Cette étape est importante car :

`guacadmin / guacadmin`

est le compte par défaut.

12. Mise en place des connexions RDP

Connexion créée :

DC1

Paramètre	Valeur
Protocole	RDP
IP	192.168.10.10
Port	3389
Domaine	expertv.local

13. Authentification Multi-Facteurs (MFA)

Extension installée :

`guacamole-auth-totp`

Configuration :

```
totp-issuer  
totp-digits  
totp-period  
totp-mode
```

Chaque administrateur doit :

- scanner un QR Code
 - enregistrer son compte dans Microsoft Authenticator
-

14. Journalisation des accès

Guacamole enregistre :

- utilisateur
- heure
- date
- durée
- adresse IP

Cela permet :

- audit
 - conformité
 - investigation sécurité
-

15. Enregistrement vidéo des sessions

Extension installée :

`guacamole-history-recording-storage`

Fonction :

- enregistrement des sessions RDP
- lecture depuis l'interface Web
- export vidéo

Utilité :

- audit
 - supervision
 - preuve d'intervention
-

16. Tests réalisés

Test	Résultat
Accès Web Guacamole	OK
Connexion RDP DC1	OK
Connexion SSH Linux	OK
Historique	OK
MFA	OK
Enregistrement vidéo	OK
Base MariaDB	OK

17. Sécurité mise en œuvre

MFA

Double authentification.

Bastion

Suppression des accès directs.

Historique

Traçabilité complète.

Comptes administrateurs

Suppression du compte par défaut.

Journalisation

Suivi de toutes les actions.

18. Difficultés rencontrées

- compilation de guacamole-server
- installation Tomcat 9
- connexion MariaDB
- configuration RDP
- MFA TOTP

Solutions :

- analyse des logs
 - documentation Apache
 - validation progressive des services
-

19. Compétences BTS SIO mobilisées

Compétence	Mise en œuvre
Gérer le patrimoine informatique	Déploiement Debian
Mettre à disposition un service	Apache Guacamole
Sécuriser les équipements	MFA
Répondre aux incidents	Analyse des logs
Travailler en mode projet	Déploiement complet
Organiser son développement professionnel	Documentation Apache

20. Améliorations futures

- Reverse Proxy Nginx
 - HTTPS avec Let's Encrypt
 - LDAP Active Directory
 - SSO
 - Cluster Guacamole
 - Haute disponibilité
 - Supervision Zabbix
-

Conclusion

Ce projet m'a permis de découvrir et de déployer une solution de bastion d'administration moderne basée sur Apache Guacamole.

J'ai acquis des compétences en administration Linux, gestion de bases de données MariaDB, sécurisation des accès administrateurs, mise en place du MFA et supervision des connexions.

Cette solution répond aux besoins actuels des entreprises en matière de cybersécurité et de contrôle des accès privilégiés, tout en simplifiant l'administration des infrastructures Windows et Linux.