

Épreuve E6 :
Administration des systèmes et des réseaux

Situation Numéro 2

Mise en place d'un bastion Guacamole
pour l'accès sécurisé aux ressources internes

Lycée Le Castel - Promo 2025



DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 2
Nom, prénom : PAUCHET Jarod		N° candidat : 02217576504
Épreuve ponctuelle	<input checked="" type="checkbox"/> Contrôle en cours de formation	Date : .06. / .05. /..2025..
Organisation support de la réalisation professionnelle - GSB		
Intitulé de la réalisation professionnelle - Mise en place d'un bastion Guacamole		
Période de réalisation : 14/04/2025 au 06/04/2025 Lieu : Lycée Le Castel		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation ¹ (ressources fournies, résultats attendus)		
Ressources fournies: <ul style="list-style-type: none"> - Ova gsb2025 - Dépôt gitea gsb2025 - Schéma réseau Résultats attendus (sous virtualbox): <ul style="list-style-type: none"> - Correction des playbooks - Infrastructure opérationnelle - Guacamole fonctionnel - Connexion RDP et SSH fonctionnel 		
Description des ressources documentaires, matérielles et logicielles utilisées ²		
Matériels utilisés: <ul style="list-style-type: none"> - ordinateur bat13-lab213, ordinateur perso - Principaux logiciels utilisés : VirtualBox, Ansible, Guacamole - Gestion de versions: Git - Guacamole (Bastion) - pfSense (pare-feu) - Environnement de travail collaboratif: Github, Gitea, Google Drive - Ova: Debian 12 gsb2025, pfSense Vierge, Debian Vierge - Ansible (déploiement) 		
Modalités d'accès aux productions ³ et à leur documentation ⁴		

¹ En référence aux conditions de réalisation et ressources nécessaires du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

⁴ Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Contexte : Le laboratoire Galaxy Swiss Bourdin (GSB) issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) a fait appel à nos services pour l'installation d'un Bastion Guacamole.

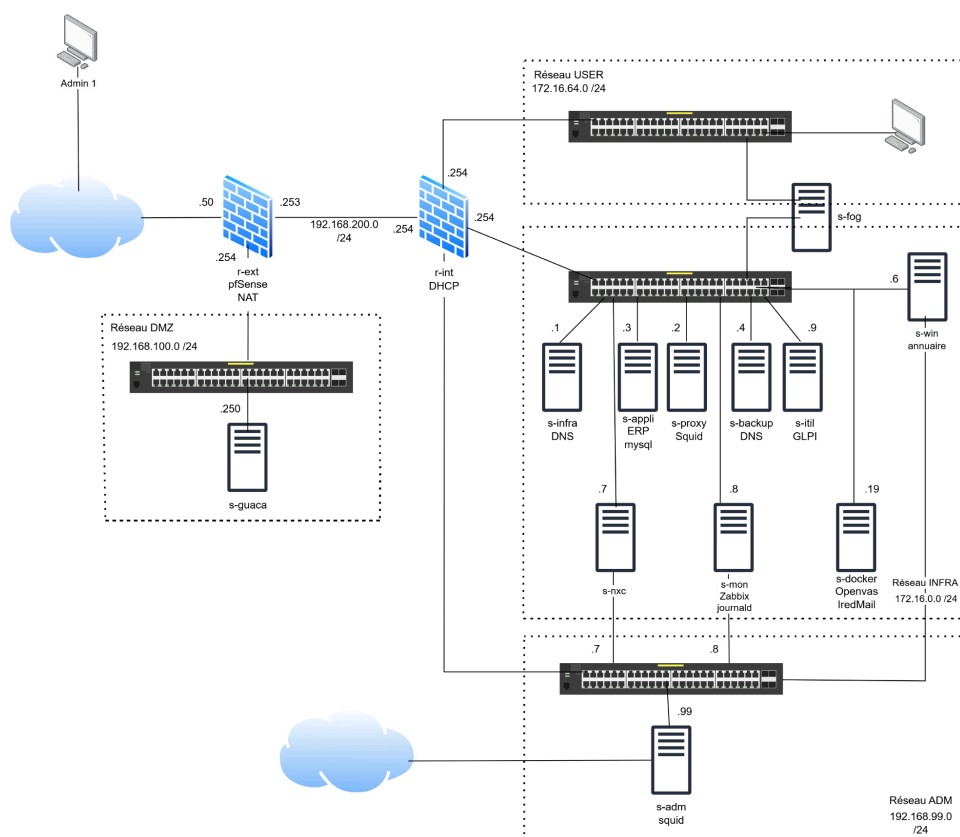
Existant : Dépôt Git, description du contexte, description de l'existant, expression des besoins, machine existante, playbook Ansible, Ova VirtualBox, schéma réseau.

Machines :

- **s-adm** : serveur d'administration/déploiement (accès SSH avec clé publique) squid/routage NAT
- **s-infra** : DNS (bind, autoconfiguration clients Web)
- **r-ext (pfSense)** : routage/NAT, Filtrage, Redirection
- **r-int** : routage, DHCP
- **s-win** : Contrôleur de domaine AD
- **s-guaca** : Nouveau serveur (Bastion Guacamole)
- **xfce-cli** : Nouveau Client Debian 12 XFCE
- **w10-cli** : Nouveau Client Windows 10

Mission : Mise en œuvre d'un serveur Guacamole

Contrainte : Respect de la structure du réseau GSB, respect des systèmes d'exploitation déjà existant.



Objectif

Le secteur administratif de GSB a fait appel à nos services pour la mise en place d'une solution d'accès sécurisé aux ressources internes (LAN) depuis un réseau potentiellement non sécurisé (DMZ).

L'objectif principal est de permettre la mise en place d'un bastion **Guacamole** pour que les techniciens puissent administrer à distance un serveur Windows (par Bureau à Distance avec **RDP** - Remote Desktop Protocol) et un serveur Linux (par ligne de commande avec **SSH** - Secure Socket Shell) de manière sécurisée.

Objectifs techniques

- Configuration d'un pare-feu **pfSense** (NAT) qui sépare internet du réseau interne
- Installation et configuration d'un Bastion **Guacamole** conteneurisé avec **Podman** situé en DMZ
- Mise en place d'un reverse proxy **Nginx** conteneurisé
- Création et gestion des utilisateurs du service **Guacamole**
- Configuration des machines à administrer (**s-win** et **s-infra**)
- Accès par **RDP** à la machine windows **s-win** et accès par **SSH** à la machine **s-infra**
- Preuve de log de connexion récupérer par le Bastion **Guacamole**

Les outils utilisés

Outils d'accès à distance Guacamole

Guacamole est une passerelle d'accès distant open-source, qui permet de se connecter à des machines via un navigateur web, sans avoir besoin d'installer de client spécifique. Il supporte plusieurs protocoles comme **RDP**, **SSH** et **VNC**.

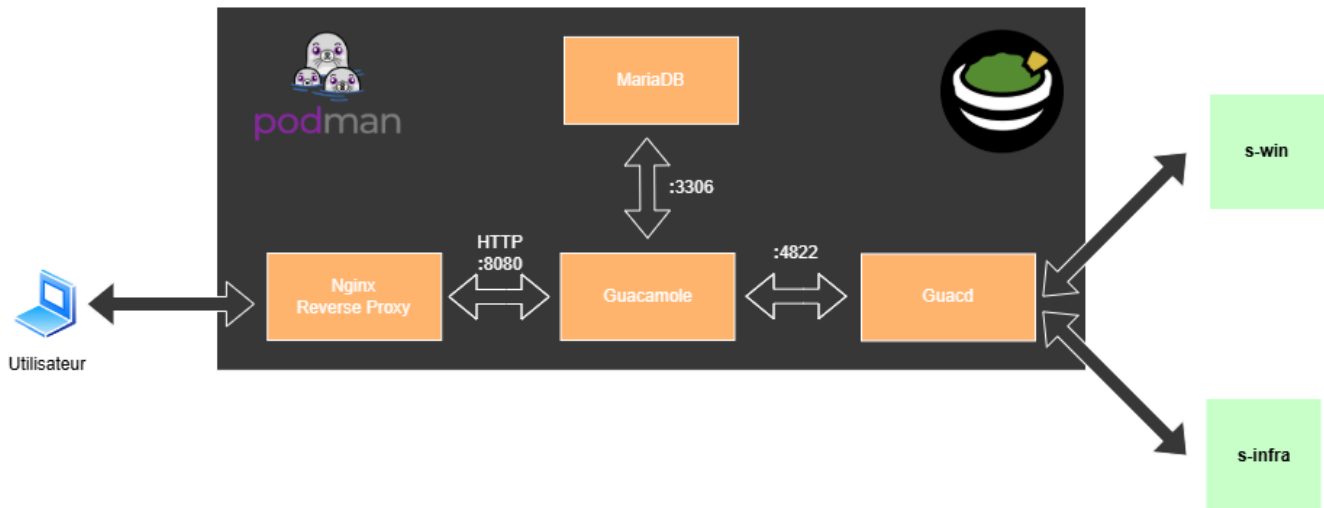
Dans un rôle de bastion, **Guacamole** agit comme un point d'entrée sécurisé et centralisé pour accéder aux serveurs d'une infrastructure. Les utilisateurs s'authentifient via une interface web, puis accèdent aux machines cibles en toute sécurité.

Les principaux avantages

- Aucun client requis (tout se fait via un navigateur)
- Contrôle des accès utilisateurs
- Journalisation des connexions
- Idéal pour les environnements cloisonnés ou sécurisés



Schéma du fonctionnement du bastion Guacamole



La solution a été déployée à l'aide de **Podman**, en structurant un pod composé des conteneurs suivants :

- **Guacamole** (interface web d'accès distant)
- **Guacd** (daemon qui gère les connexions aux machines distantes)
- **MariaDB** (base de données utilisée par **Guacamole** pour stocker les utilisateurs, connexions et paramètres)
- **Nginx** (sécurise l'accès web avec HTTPS, redirige le trafic vers **Guacamole**)

Outils de conteneurisation Podman

Podman (Pod Manager) est un moteur de conteneur open-source, compatible avec **Docker** mais **sans démon** (daemonless).

Il permet de créer, gérer et exécuter des conteneurs et des pods de manière sécurisée.

Caractéristiques principales

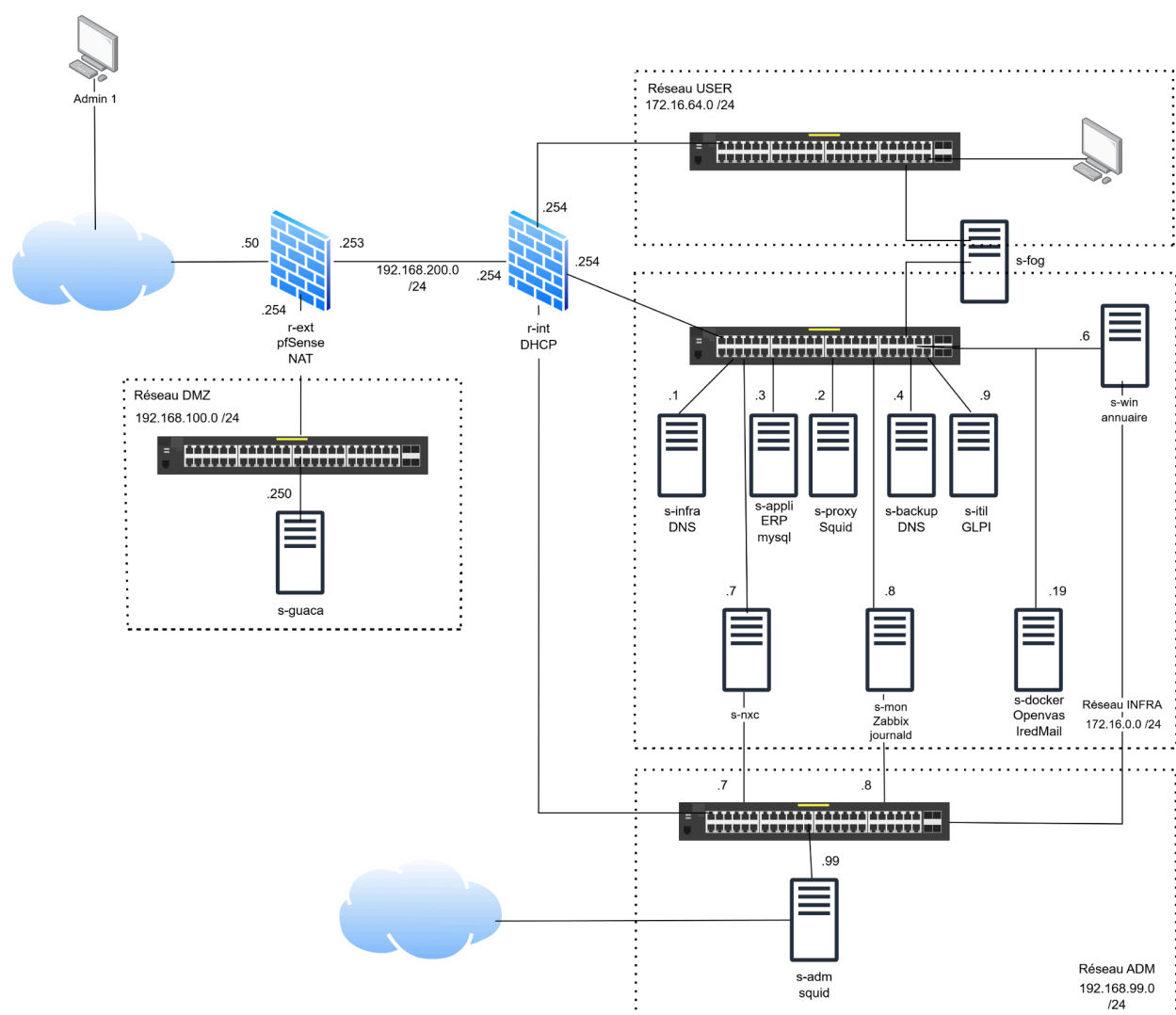
- Compatible avec les commandes Docker (*alias docker=podman*)
- Fonctionne **sans root** (rootless), idéal pour la sécurité
- Gère des **pods** (groupes de conteneurs partageant le même réseau et espace de noms)
- Intégration native avec **systemd** pour les services

Les principaux avantages

- Plus sécurisé (pas besoin de démon en arrière-plan)
- Meilleur contrôle des permissions



Schéma Réseau



Prérequis

Rôles des machines :

- **s-adm** : serveur d'administration/déploiement (accès **SSH** avec clé publique) squid/routage NAT
- **r-ext** : routeur externe (via **pfSense**), routage/NAT, filtrage
- **r-int** : routeur interne, DHCP pour les réseaux internes.
- **s-guaca** : bastion d'accès distant sécurisé via **Guacamole**
- **s-infra** : DNS (serveur distant pour tester le **SSH**)
- **s-win** : serveur windows Active Directory (serveur distant pour tester le **RDP**)
- **xfce-cli** : client graphique léger, utilisé pour la configuration de **pfSense** et du bastion **Guacamole**

Rôles des réseaux :

- **n-adm** : réseau d'administration dédié à l'installation et au déploiement initial des machines
- **n-infra** : réseau réservé aux serveurs internes
- **n-user** : réseau simulant l'environnement des utilisateurs
- **n-link** : réseau de transit reliant les routeurs r-ext et r-int.
- **n-dmz** : zone démilitarisé dans laquelle est déployé le bastion s-guaca
- **bridge** : réseau simulant l'accès à Internet

Étapes clés

- Installation de **Podman**
- Automatisation du déploiement d'un pod contenant les services suivants :
 - **Guacamole** (interface web d'accès distant)
 - **Guacd** (gestion des connexions RDP/SSH)
 - **MariaDB** (stockage des données de configuration)
 - **Nginx** (reverse proxy assurant la terminaison HTTPS)
- Déploiement du pod via **Podman**
- Création des tables **MariaDB** pour **Guacamole**
- Déploiement de la machine virtuelle **s-guaca** dans la DMZ
- Configuration du pfSense
- Création de connexion distantes dans **Guacamole**
- Phase de tests et journalisation

Etape 1 : Installation de Podman

À partir d'une OVA Debian 12.10 vierge dans le réseau *n-adm*, effectuer la mise à jour de liste des paquets et l'installation du paquet **Podman**.

```
apt update
apt install -y podman git sudo
```

Etape 2 : Automatisation du déploiement

1 - Création du dossier de configuration

Le dossier *~/template* contient les **fichiers de configuration nécessaires à la génération du pod Guacamole** ; il est utilisé par le script *guacpod.sh* pour initialiser correctement les volumes, les secrets et les paramètres du conteneur.

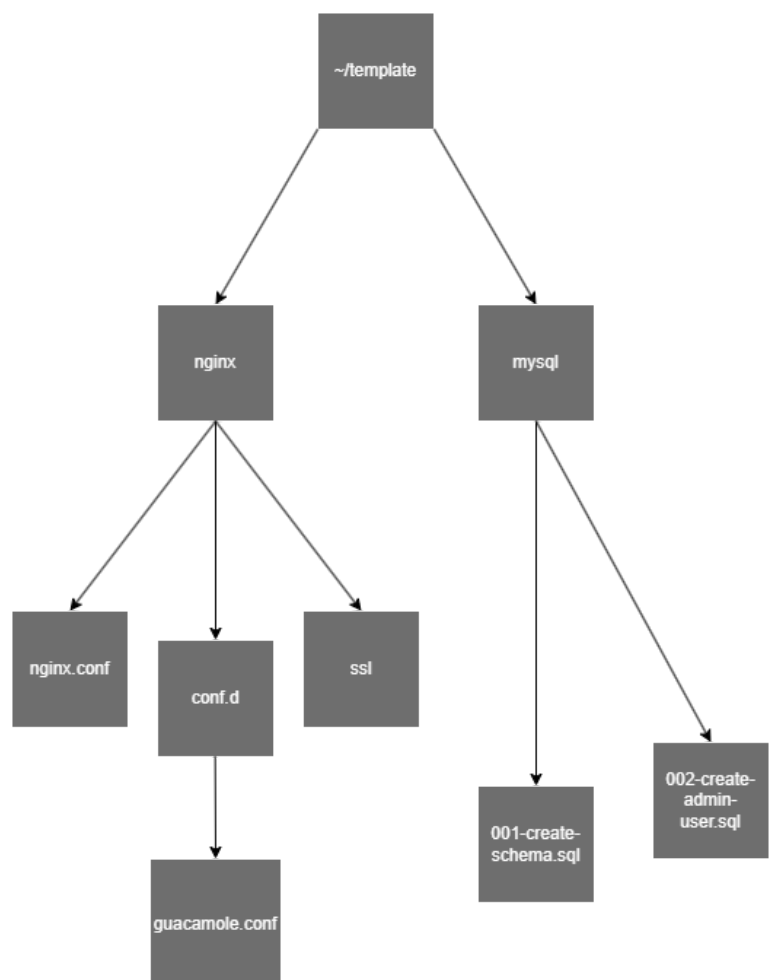
Le schéma ci-dessous illustre l'arborescence et la répartition des fichiers dans ce répertoire.

nginx : Contient la configuration du reverse proxy **Guacamole** en HTTPS

- *nginx.conf* : Fichier principal de configuration du serveur **nginx**.
- *conf.d/guacamole.conf* : Fichier pour la redirection HTTPS
- *ssl/* : Répertoire prévu pour les certificats SSL (clé privée, certificat).

mysql/ : Contient les scripts SQL d'initialisation de la base de données.

- *001-create-schema.sql* : Crée la structure de la base de données **Guacamole**.
- *002-create-admin-user.sql* : Crée un utilisateur admin par défaut.



Exemple de nginx.conf

Voici un extrait de configuration du *nginx.conf* contenu dans *~/template/nginx*

```
user  nginx;
worker_processes  auto;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;

events {
    worker_connections  1024;
}

http {
    include      /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile      on;
    keepalive_timeout  65;

    include /etc/nginx/conf.d/*.conf; # Inclut tous les fichiers de configuration de
    type .conf du dossier /etc/nginx/conf.d
}
```

Exemple du guacamole.conf

Voici un extrait de configuration du *guacamole.conf* contenu dans *~/template/nginx/conf.d/*

```
server {
    listen 443 ssl http2; # Écoute sur le port 443 avec SSL
    server_name gsb.lan;

    ssl_certificate /etc/nginx/ssl/self.cert; # Chemin vers le certificat SSL
    ssl_certificate_key /etc/nginx/ssl/self-ssl.key; # Clé privée correspondant au
    certificat

    . . .

    location / {
        proxy_pass http://localhost:8080/guacamole/; # Reverse proxy vers l'application
        Guacamole
        proxy_buffering off;
        proxy_http_version 1.1;
        proxy_set_header Host $host;
        . . .
    }

server {
    listen 80; # Serveur HTTP, port 80
    server_name gsb.lan;
    return 301 https://$host$request_uri; # Redirige automatiquement tout HTTP vers
    HTTPS
}
```

2 - Création du certificat et de la clé SSL

```
openssl req -x509 -nodes -days 365 \
    -newkey rsa:2048 \
    -keyout ~/template/nginx/ssl/self-ssl.key \
    -out ~/template/nginx/ssl/self.cert \
    -subj "/C=FR/ST=Bourgogne/L=Dijon/O=GSB/OU=IT/CN=gsb.lan"
```

> Exemple de commande utilisant **Openssl** (open-source)

3 - Récupération des fichiers de schéma SQL pour Guacamole

Cloner le dépôt officiel de **Guacamole** pour accéder aux fichiers nécessaires

```
git clone https://github.com/apache/guacamole-client.git
```

Copie des fichiers de création du schéma MySQL

Une fois le dépôt cloné, copiez les fichiers SQL permettant de créer le schéma et l'utilisateur administrateur dans `~/template/mysql`

```
cp ./guacamole-client/extensions/guacamole-auth-jdbc/modules/guacamole-auth-jdbc-mysql/schema/001-create-schema.sql ~/template/mysql/

cp ./guacamole-client/extensions/guacamole-auth-jdbc/modules/guacamole-auth-jdbc-mysql/schema/002-create-admin-user.sql ~/template/mysql/
```

> Le premier script crée la structure des tables nécessaires, tandis que le second ajoute un utilisateur administrateur par défaut **"guacadmin"**.

4 - Création du script bash de déploiement

Voici un extrait de configuration du `guacpod.sh`

```
#!/bin/bash

# Créé le pod
podman pod create --name Bastion_Guacamole --publish 80:80 --publish 443:443 --publish 8080:8080

# Conteneur guacamole
podman run -d --name GSB_guacamole --pod Bastion_Guacamole \
-v /etc/timezone:/etc/timezone:ro \
-v /etc/localtime:/etc/localtime:ro \
-e TZ=Europe/Paris \
-e TOTP_ENABLED=true \
-e GUACD_HOSTNAME=GSB_guacd \
-e GUACD_PORT=4822 \
-e MYSQL_HOSTNAME=GSB_mariadb \
-e MYSQL_PORT=3306 \
-e MYSQL_DATABASE=guacamoledb \
-e MYSQL_USER=guacamole \
-e MYSQL_PASSWORD=changeme \
-e RECORDING_SEARCH_PATH=/var/lib/guacamole/recordings \
-e HEADER_ENABLED=true \
docker.io/guacamole/guacamole
```

```
# Conteneur nginx
podman run -d --name GSB_nginx_ssl --pod Bastion_Guacamole \
-v ~/template/nginx/nginx.conf:/etc/nginx/nginx.conf:ro \
-v ~/template/nginx/conf.d:/etc/nginx/conf.d \
-v ~/template/nginx/ssl:/etc/nginx/ssl:ro \
-v /etc/timezone:/etc/timezone:ro \
-v /etc/localtime:/etc/localtime:ro \
-e TZ=Europe/Paris \
docker.io/library/nginx:latest
```

Étape 3 : Déploiement du Pod

Exécution du script

Lancer le déploiement automatisé du pod **Guacamole** avec un *sudo bash*

```
sudo bash guacpod.sh
```

Étape 4 : Création des tables MariaDB

Accéder au conteneur **MariaDB** pour lancer la configuration de la base de données

```
podman exec -it GSB_mariadb mariadb -u root -p
```

> Il faut saisir le mot de passe administrateur de la base de données **MariaDB**.

Se placer dans la base de données dédiée à **Guacamole** avec la commande *USE*

```
USE guacamoledb;
```

> Il faut saisir le nom de la base de données **MariaDB** utilisée par **Guacamole**.

Exécuter les scripts SQL pour créer les tables et l'utilisateur administrateur "guacadmin".

```
SOURCE /tmp/mysql-scripts/001-create-schema.sql;
SOURCE /tmp/mysql-scripts/002-create-admin-user.sql;
```

> Il faut indiquer le chemin exact où sont stockés les deux fichiers **.sql** du conteneur **MariaDB**.

Vérifier que les tables ont bien été créées avec la commande *SHOW TABLES*

```
SHOW TABLES;
```

Étape 5 : Déploiement de *s-guaca* dans la DMZ

Éteindre la machine, changer le mode d'accès réseau en interne *n-dmz*

Réseau

Adapter 1 Adapter 2 Adapter 3 Adapter 4

☒ Activer l'interface réseau

Mode d'accès réseau : Réseau interne

Name: n-dmz

Type d'interface : Intel PRO/1000 MT Desktop (82540EM)

Mode Promiscuité : Refuser

Adresse MAC : 080027B701F5

☒ Câble branché

Étape 6 : Configuration du pfSense

Afin d'avoir accès au réseau *n-infra* depuis *s-guaca*, il nous faut configurer le pare-feu.

Voici un tableau récapitulatif des paramètres nécessaire pour le bon fonctionnement de *s-guaca* dans la DMZ

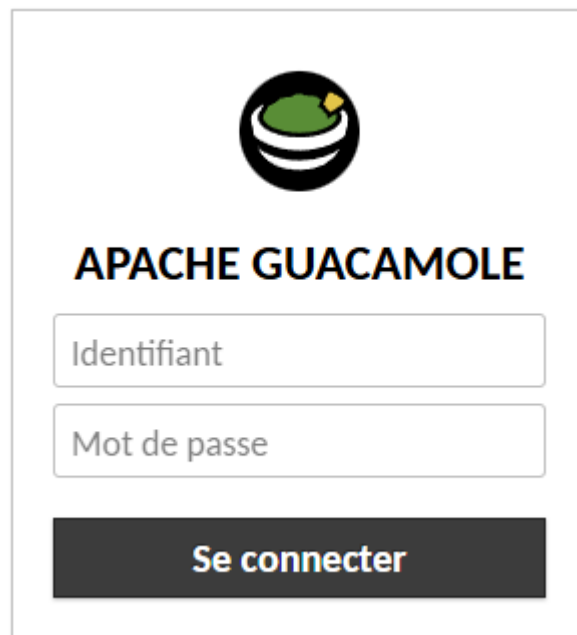
NAT - Port Forwarding							
Interface	Protocole	Destination	Port	IP de redirection	Port de redirection	Description	
WAN	TCP	This Firewall (self)	HTTPS → HTTPS	192.168.100.250	HTTPS	Rediriger HTTPS vers DMZ depuis le WAN	
Règles Firewall - WAN							
Interface	Action	État	Protocole	Source	Destination	Port	Description
WAN	Pass	✓ Activée	TCP	Any	192.168.100.250	HTTPS → HTTPS	NAT Rediriger HTTPS vers DMZ (auto créée)
Règles Firewall - LAN							
Interface	Action	État	Protocole	Source	Destination	Port	Description
LAN	Pass	✓ Activée	TCP	172.16.64.0/24	192.168.100.250	HTTPS → HTTPS	HTTPS Réseau User vers Guacamole
LAN	Pass	✗ Désactivée	ICMP	172.16.64.0/24	192.168.100.250	-	Ping Réseau User vers Guacamole (test uniquement)
LAN	Pass	✗ Désactivée	ICMP	Any	This Firewall (self)	-	Ping vers le pare-feu depuis le LAN (test)
Règles Firewall - DMZ							
Interface	Action	État	Protocole	Source	Destination	Port	Description
DMZ	Pass	✓ Activée	TCP	192.168.100.250	172.16.64.0/24	HTTPS → HTTPS	Guacamole vers Réseau User
DMZ	Pass	✓ Activée	TCP	192.168.100.250	172.16.0.0/24	MS RDP → MS RDP	Guacamole RDP vers Réseau Infra
DMZ	Pass	✓ Activée	TCP	192.168.100.250	172.16.0.0/24	SSH → SSH	Guacamole SSH vers Réseau Infra
DMZ	Pass	✗ Désactivée	ICMP	DMZ Subnets	This Firewall (self)	-	Ping DMZ vers le pare-feu (test uniquement)
Routeage - Gateways							
Interface	Nom	Gateway	Description				
LAN	RextToRint	192.168.200.254	R-ext vers R-int				
Routeage - Routes statiques							
Réseau destination	Gateway	Description					
172.16.0.0/24	RextToRint	Route vers réseau Infra					
172.16.64.0/24	RextToRint	Route vers réseau User					

Étape 7 : Création de connexion distantes

1 - Connexion à l'interface web

L'interface web du serveur **s-guaca** est accessible via l'adresse suivante :

https://adresse_ip_guacamole/

The image shows the Apache Guacamole login interface. At the top center is the Apache Guacamole logo, which consists of a black circle containing a green bowl with a yellow spoon. Below the logo, the text "APACHE GUACAMOLE" is displayed in a bold, black, sans-serif font. Underneath the text are two input fields: the first is labeled "Identifiant" and the second is labeled "Mot de passe". Both fields are white with a light gray border. At the bottom of the form is a dark gray button with the text "Se connecter" in white, bold, sans-serif font.

> Interface d'authentification de **Guacamole** permettant l'accès à la console d'administration

Identifiants par défaut :

Nom d'utilisateur : `guacadmin`

Mot de passe : `guacadmin`

2 - Activation de la TOTP

Un QR code sera présent lors de la première connexion, il suffira de le scanner à l'aide d'une application mobile pour **TOTP (Time-based One-time Password)** tel que **Aegis** ou **Google/Microsoft Authenticateur** (Android) et **FreeOTP** (IOS)

L'authentification multi-facteurs a été activée pour votre compte.

Pour terminer votre processus d'inscription, scannez le code-barre ci-dessous avec l'application deux-facteurs sur votre téléphone ou votre appareil

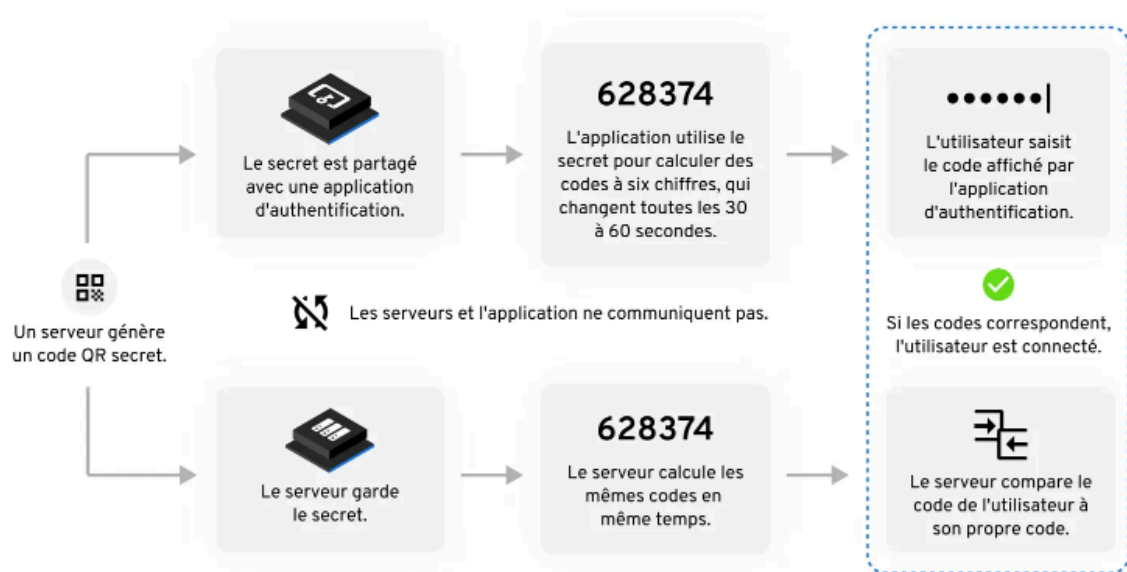


► Détails: [Montrer](#)

Après avoir scanné le code-barre, saisissez les 6 chiffres du code d'authentification affichés pour terminer votre inscription.

Continuer

Pour rappel, voici un schéma du processus de fonctionnement de la **TOTP** :



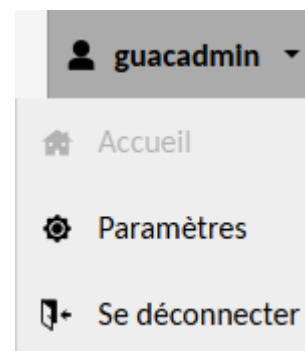
3 - Création des connexions

Accéder au **"paramètres"** disponible dans le coin droit de l'interface.

Ensuite onglet **"Connexions"**, choisissez **"Nouvelle Connexion"**

Entrer les paramètres nécessaires pour les onglets suivants :

- **Modifier Connexion**
- **Paramètres - Réseau**



MODIFIER CONNEXION

Nom:
Lieu:
Protocole:

PARAMÈTRES

Réseau

Nom d'hôte:
Port:
Clé publique de l'hôte (Base64):

> Voici un exemple de configuration nécessaire pour l'accès **SSH** de **s-infra**.

MODIFIER CONNEXION

Nom:
Lieu:
Protocole:

PARAMÈTRES

Réseau

Nom d'hôte:
Port:

> Voici un exemple de configuration nécessaire pour l'accès **RDP** de **s-infra**

Cochez la case “**Ignorer le certificat du serveur**” et choisissez votre agencement clavier “**AZERTY**” (seulement pour les connexions **RDP**), et le fuseau horaire **Europe/Paris**.

Étape 8 : Phase de tests et journalisation

1 - Connexion SSH - **s-infra**

Une fois les connexions vers **s-infra** (SSH) et **s-win** (RDP) ajoutées, revenir à la page d'accueil de l'interface **Guacamole** afin de vérifier leur bon fonctionnement.

Sélectionner la connexion **s-infra**, puis entrer les identifiants d'authentification de cette machine.

Login as: Password:

```
Linux s-infra 6.1.0-33-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.133-1 (2025-04-10) x86_64

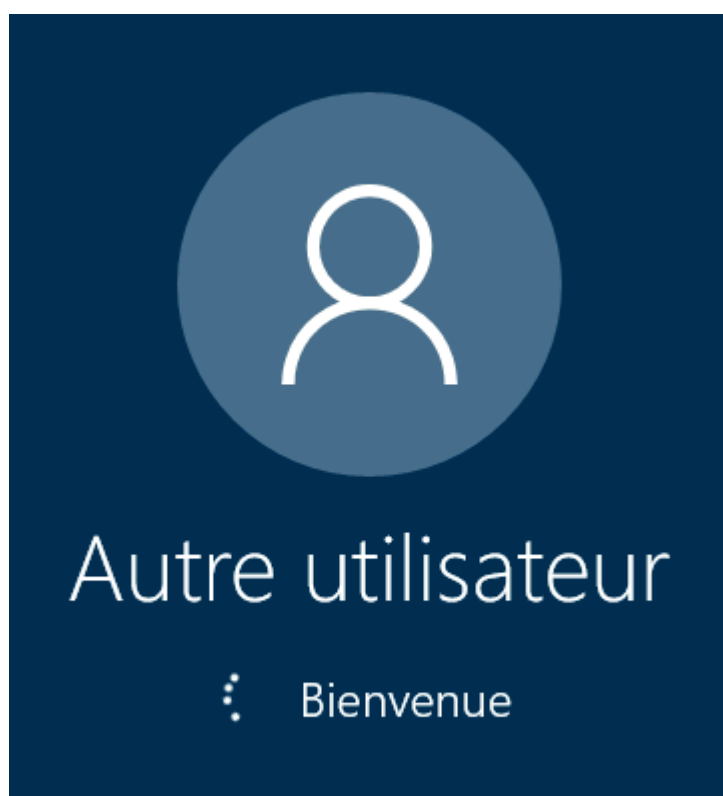
Plan your installation, and FAI installs your plan.

Last login: Fri Apr 25 18:11:48 2025 from 192.168.100.250
sio@s-infra:~$
```

> Aperçu d'une connexion **SSH** réussie.

2 - Connexion RDP - *s-win*

Sélectionner la connexion **s-win**, puis entrer les identifiants d'authentification de cette machine.

A dark-themed dialog box for RDP authentication. It contains three input fields with labels: 'Identifiant:', 'Mot de passe:', and 'Nom de domaine:'. Below the fields are two buttons: 'Continue' and 'Cancel'.

> **Guacamole** procède à l'établissement de la connexion **RDP** avec le serveur distant.

3 - Journalisation de Guacamole

Pour visualiser les connexions qui ont été effectuées sur nos différentes machines, accéder aux paramètres de l'interface **Guacamole** puis dans l'onglet **"Historique"** afin d'avoir un aperçu des connexions.

Sessions Actives Historique Utilisateurs Groupes Connexions Préférences

L'historique des dernières connexions est listé ici et peut être trié en cliquant sur l'en-tête des colonnes. Pour rechercher des enregistrements spécifiques, entrez un filtre et cliquez sur "Rechercher". Seuls les enregistrements correspondants au filtre renseigné seront

🔍 Filtre

Rechercher

Identifiant	Ouvert depuis ▲	Durée	Nom de connexion	Hôte distant
guacadmin	25-04-2025 18:42:56	--	s-infra	
guacadmin	25-04-2025 18:42:14	--	s-win	
guacadmin	25-04-2025 18:19:08	23.1 minutes	s-win	
guacadmin	25-04-2025 18:18:38	29 secondes	s-win	
guacadmin	25-04-2025 18:16:04	2.3 minutes	s-win	
guacadmin	25-04-2025 18:11:59	30.2 minutes	s-infra	
guacadmin	25-04-2025 18:09:36	2.4 minutes	s-infra	
guacadmin	25-04-2025 17:51:52	27.1 minutes	s-win	
guacadmin	25-04-2025 17:51:47	51.1 minutes	s-infra	

> Aperçu d'un historique de connexions **Guacamole**.

Dans la machine **Guacamole**, il est possible d'utiliser la commande **journalctl -f** afin de récupérer les connexions entrantes.

```
avril 25 19:01:24 Bastion systemd[1]: 8c9c17ad5f21833de4a73f0fba7e97f6d5430c1e6dd13b8ca2bcc7529f2fd083.service: Deactivated successfully.
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[1]: INFO: Creating new client for protocol "rdp"
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[1]: INFO: Connection ID is "$53af8a07-db97-49a0-91ec-632ac2fcdcef"
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[269]: INFO: No security mode specified. Defaulting to security mode negotiation with server.
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[269]: INFO: Resize method: none
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[269]: INFO: No clipboard line-ending normalization specified. Defaulting to preserving the format of all
line endings.
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[269]: INFO: User "@0fb1ef51-eab2-4bab-9698-4c8ff43e3c7d" joined connection "$53af8a07-db97-49a0-91ec-632
ac2fcdcef" (1 users now present)
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[269]: INFO: Loading keymap "base"
avril 25 19:03:38 Bastion GSB_guacd[1044]: guacd[269]: INFO: Loading keymap "en-us-qwerty"
avril 25 19:03:38 Bastion GSB_guacamole[1072]: 19:03:38.929 [http-nio-8080-exec-8] INFO o.a.g.tunnel.TunnelRequestService - User "guacadmin" connected to conne
ction "1".
avril 25 19:03:56 Bastion GSB_guacd[1044]: guacd[269]: INFO: Connected to RDPDR 1.13 as client 0x0003
avril 25 19:03:57 Bastion GSB_guacd[1044]: guacd[269]: INFO: RDPDR user logged on
```

> Aperçu d'une connexion **RDP** réussie.