

# **SRV-GUACAMOLE**

Noah MAILLET Projet-SANDBOX



# Table of contents

1	Preface		3
1.1	Present	ation Technologies	3
1.2	Configu	ıration minimal	4
1.3	Configu	ıration mise en place:	4
2	Créatio	n de la machine virtuelle	5
3	Installa	tion Debian	8
3.1	Configu	ırer le réseau	8
3.2	Configu	ırer l'outil de gestion des paquets	11
4	Configu	ıration Debian	13
4.1	Configu	ıration du réseau :	13
4.2	Configu	ıration dépot	14
4.3	Ajout e	t configuration d'un disque :	15
5	Installa	tion guacamole	18
5.1	Installa	tion des prérequis d'apache guacamole	18
5.2	Compila	ation et installation Apache Guacamole « Server »	19
5.3	Créatio	n repertoire de configuration	22
5.4	Installa	tion Guacamole Client (Web app)	22
5.5	Installa	tion d'une base de données MariaDB pour l'authentification	23
6	Premie	r pas avec Apache Guacamole	27
6.1	Créatio	n d'un nouveau compte admin	27
6.2	Ajout d	'une connexion	29
	6.2.1	Connexion SSH	29
	6.2.1.1	Configuration	29
	6.2.1.2	Test de la connexion	31
	6.2.2	Connexion RDP	31
	6.2.2.1	Configuration	31
	6.2.2.2	Test de la connexion	33
7	Sécurite	é d'Apache Guacamole	34
7.1	Créer u	n enregistrement video des sessions	34
7.2	Configu	ıration enregistrement d'une connexions	36
7.3	Configu	ıration HTTPS de guacamole	37
	7.3.1	Génération du keystore	37
	7.3.2	Création du connecteur SSL	
8	Synchro	onisation LLDAP	40
8.1	Installa	tion extension LDAP pour Apache Guacamole	40
8.2	Connex	ion Guacamole à LLDAP	41
8.3	Créatio	n d'un compte administrateur pour la synchronisation	42
8.4	Verifica	tion de la synchronisation	43
9	Schéma	a des Flux Apache Guacamole	44



# 1 Preface

# **1.1 Presentation Technologies**

Apache Guacamole est une passerelle d'accès à distance open-source qui révolutionne la manière dont les utilisateurs se connectent et interagissent avec leurs applications et leurs bureaux à distance. Conçu pour la simplicité, la sécurité et la flexibilité, Guacamole offre une solution unifiée pour accéder à des ressources informatiques dispersées sur différents réseaux, systèmes d'exploitation et dispositifs.

Fonctionnalités principales :

- 1. Accès universel : Guacamole élimine les barrières entre les utilisateurs et leurs applications en permettant un accès à distance à partir de n'importe quel appareil disposant d'un navigateur web compatible.
- 2. Intégration transparente : Grâce à ses protocoles standard, Guacamole s'intègre facilement avec une large gamme de systèmes d'exploitation, de protocoles de connexion et de solutions d'authentification, éliminant ainsi les silos informatiques et simplifiant la gestion des accès.
- 3. Sécurité renforcée : En mettant l'accent sur la sécurité, Guacamole offre un accès à distance sécurisé grâce au cryptage des communications, à l'authentification à plusieurs facteurs et à des fonctionnalités de gestion des identités robustes.
- 4. Gestion centralisée : Avec une interface d'administration intuitive, Guacamole permet une gestion centralisée des connexions et des utilisateurs, simplifiant ainsi la configuration et la surveillance de l'ensemble du système.
- 5. Personnalisation et Extensibilité : Guacamole offre une flexibilité inégalée en permettant la personnalisation de l'interface utilisateur, l'extension des fonctionnalités grâce à des plug-ins et le développement d'intégrations personnalisées pour répondre aux besoins spécifiques de chaque organisation.

Cas d'Utilisation :

- Accès à Distance pour les Employés : Les organisations peuvent fournir à leurs employés un accès sécurisé à leurs applications et bureaux virtuels depuis n'importe où, ce qui facilite le travail à distance et l'accès aux ressources internes.
- 2. Support technique : Les équipes de support technique peuvent utiliser Guacamole pour accéder aux ordinateurs des utilisateurs à distance, diagnostiquer les problèmes et fournir une assistance technique en temps réel.
- 3. Hébergement de Desktops virtuels : Guacamole peut être utilisé pour fournir un accès à distance à des bureaux virtuels hébergés dans le cloud ou sur site, offrant ainsi une solution économique pour le déploiement de postes de travail virtuel.
- 4. Développement et Tests : Les développeurs et les testeurs peuvent utiliser Guacamole pour accéder à des environnements de développement et de test à distance, ce qui facilite la collaboration et l'itération rapide.

### Conclusion :

Avec sa simplicité d'utilisation, sa sécurité renforcée et sa flexibilité, Apache Guacamole est bien plus qu'une simple passerelle d'accès à distance : c'est un outil essentiel pour la transformation numérique des entreprises, offrant un accès transparent et sécurisé à toutes les ressources informatiques, où que vous soyez.



# 1.2 Configuration minimal.

La configuration minimale du serveur guacamole est la suivante :

- Processeur :
- o 2 cœurs
- RAM :
  - o **4 Go**
- Espace disque :
  - $_{\odot}$  50 Go (à voir en fonction des enregistrements de sessions).

# 1.3 Configuration mise en place:

La configuration que je vais utiliser pour ce projet est la suivante :

- Processeur:
  - 2 cœurs,
- RAM :
  - o 4 Go
- Stockage :
  - $\circ$  32 Go stockage système (SSD)
  - o 100 Go stockage enregistrement (HDD).
- Réseau :
  - o 1 carte Réseau VLAN SERVER.
  - 1 carte Réseau VLAN DMZ.



# 2 Création de la machine virtuelle.

Dans le cadre du projet sandbox, l'outil de virtualisation qui a été retenue est Proxmox.

Vous pouvez installer Apache Guacamole dans tout autre environnement de virtualisation tant que vous respectez la configuration minimale.

- 1. Je me connecte à ma ferme de serveur ProxMox.
- 2. Créer une VM.



3. Je renseigne le nom de la machine virtuelle « SRV-GUACAMOLE », le pool de ressource : « Sandbox-Training ». → Suivant.

Cre	éer: Mach	ine virtuelle						$\otimes$
G	énéral S	Système d'exploitation	Système	Disques	Processeur	Mémoire	Réseau	Confirmation
Nœ	eud:	pve		$\sim$	Pool de	SANDBO	X-TRAINING	× ~
VM	1 ID:	103		$\bigcirc$	ressources:			
No	m:	SRV-GUACAMOLE	E					

4. Je sélectionne l'ISO (Debian 11 DVD). → Suivant.

Cr	éer: Machine	virtuelle						$\otimes$	
G	Sénéral Syste	ème d'exploitation	Système	Disques	Processeur	Mémoire	Réseau	Confirmation	
(	Utiliser une image de média (ISO)     Système d'exploitation de l'invité:								
	Stockage	storage		$\sim$	Туре:	Linux		$\sim$	
	Image ISC	DEB-11.8.0-amd	164-DVD-1.iso	$\sim$	Version:	6.x - 2.6 K	Cernel	$\sim$	
c (	Utiliser le lec	teur CD/DVD de l'hó	ôte						
e (	○ N'utiliser auc	un média							

5. Je laisse les paramètres par défaut → suivant.

Créer: Machine	Créer: Machine virtuelle									
Général Syst	ème d'exploitation Système	Disques	Processeur	Mémoire	Réseau	Confirmation				
Carte graphique:	Par défaut	$\sim$	Contrôleur SCSI:	VirtIO SC	SI single	$\sim$				
Machine:	Par défaut (i440fx)	$\sim$	Agent QEMU:							
Micrologiciel										
BIOS:	Par défaut (SeaBIOS)	$\sim$	Ajouter un module TPM:							



6. Je laisse les paramètres par défaut → suivant.

(On ajoutera le Disque supplémentaire après l'installation du système d'exploitation).

Créer: Ma	chine virtu	elle						$\otimes$
Général	Système	d'exploitation	Système	Disques	Proces	seur Mé	moire Ré	éseau Confirmation
scsi0	Û	Disque Ba	ande passa	nte				
		Bus/périphériq	ue: SCSI		0 🗘	Cache:	Pa	ır défaut (Aucun ca ∨
		Stockage:	local-l	vm	$\sim$	IO thread:		
		Taille du disque (Gio):	<sup>e</sup> 32		$\hat{\mathbf{v}}$			
		Format:	Image	disque brut	e (r 🗸			

7. J'alloue 2 cœurs de processeur et je sélectionne host en type → suivant.

Créer: Mac	hine virtuelle				$\otimes$		
Général	Système d'exploitation	Système	Disques	Processeur	Mémoire	Réseau	Confirmation
Supports de	1		$\hat{}$	Туре:	host		× ~
Cœurs:	2		$\bigcirc$	Total de cœurs:	2		

8. J'alloue 4 Go de mémoire → Suivant.

Créer: Ma	Créer: Machine virtuelle										
Général	Système d'exp	loitation	Système	Disques	Processeur	Mémoire	Réseau	Confirmation			
Mémoire (MiB):		4192		$\hat{\mathbf{Q}}$							

9. Je choisis « Intel E1000 » comme carte réseau et je l'ajoute au VLAN 1, je désactive le pare-feu → suivant.

Créer: Machine virtuelle									
Général	Système d'exploitation	Système	Disques	Processeur	Mémoire	Réseau	Confirmation		
Aucun périphérique réseau									
Pont (bridge)	): vmbr0		$\sim$	Modèle:	Intel E100	00	$\sim$		
Étiquette de VLAN:	1		$\hat{\mathbf{x}}$	Adresse MAC:	auto				
Pare-feu:									



Général Systèr	me d'exploitation	Système	Disques	Processeur	Mémoire	Réseau	Confirmatio			
Key 个	Value									
cores	2									
сри	host									
ide2	storage:is	:iso/DEB-11.8.0-amd64-DVD-1.iso,media=cdrom								
memory	4192	4192								
name	SRV-GUA	CAMOLE								
net0	e1000,bri	e1000,bridge=vmbr0,tag=1								
nodename	pve									
numa	0									
ostype	126									
pool	SANDBO	X-TRAINING								
scsi0	local-lvm:	32,iothread=c	on							
scsihw	virtio-scsi-	virtio-scsi-single								
sockets	1									
vmid	103									
] Demaner apres	CIECUIUI									

10. Je m'assure que les informations sont correctes  $\rightarrow$  terminer.

Une fois la machine virtuelle créée.

- 11. Je me rends sur la configuration de la machine.
- 12. J'ajoute une carte réseau avec la configuration suivante : Modèle Intel E1000, VLAN 100, Firewall désactiver.

Ajouter: Carte réseau									
Pont (bridge): Étiquette de VLAN:	vmbr0 100	$\sim$	Modèle: Adresse MAC:	Intel E1000 ~					
Pare-feu:				Avancé 🗌 Ajouter					



# 3 Installation Debian.

- 1. Je me connecte à ma ferme de serveur.
- 2. Je démarre la machine virtuelle.
- 3. Je choisis installé.



<Revenir en arrière>

# 3.1 Configurer le réseau.

8. Échec de la configuration automatique → continuer.





9. Configurer le réseau vous-mêmes.



10. Je rentre l'@IP de mon serveur ainsi que son masque sous réseau.

11. Je rentre l'@Passerrelle → continuer.

[!!] Configurer le réseau -

La passerelle est une adresse IP (quatre nombres séparés par des points) qui indique la machine qui joue le rôle de routeur ; cette machine est aussi appelée le routeur par défaut. Tout le trafic qui sort du réseau (p. ex. vers Internet) passe par ce routeur. Dans quelques rares circonstances, vous n'avez pas besoin de routeur. Si c'est le cas, vous pouvez laisser ce champ vide. Consultez votre administrateur si vous ne connaissez pas la réponse correcte à cette question.

Passerelle :

10.16.1.14

<Revenir en arrière>

<Continuer>



12. Je rentre l'@IP du DNS → continuer.



13. Je rentre le nom de la machine  $\rightarrow$  continuer.

	[!] Configurer le réseau					
Veuillez indiquer le nom de ce	système.					
Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez–le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.						
Nom de machine :						
srv-guacamole						
<revenir arrière="" en=""></revenir>		<continuer></continuer>				

14. Je renseigne le nom de domaine  $\rightarrow$  continuer.

[!] Configurer le réseau

Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvez mettre ce que vous voulez mais assurez-vous d'employer le même nom sur toutes les machines.

Domaine :

sandbox.local

<Revenir en arrière>

<Continuer>

- 15. <u>Configuration mot de passe root</u>  $\rightarrow$  je rentre le mot de passe et je le confirme  $\rightarrow$  continuer.
- 16. <u>Création utilisateur</u> → Je rentre le nom complet de l'utilisateur → je rentre le pseudo de l'utilisateur → je rentre le mot de passe et je le confirme → continuer.
- Portionner les disques → assisté Utliser un disque entier → SDA → tout dans une seul partition → Terminer le partionnement → OUI.



<Oui>

# 3.2 Configurer l'outil de gestion des paquets.

18. <u>Analyse d'autres support</u> → « Non ».

[!] Configurer l'outil de gestion des paquets 🚽

L'analyse des supports d'installation a trouvé l'étiquette :

Debian GNU/Linux 11.8.0 \_Bullseye\_ - Official amd64 DVD Binary-1 20231007-14:05

Vous pouvez maintenant analyser des médias supplémentaires qui seront utilisés par l'outil de gestion des paquets (APT). En principe, ils devraient appartenir au même ensemble que le média d'amorçage. Si vous n'avez pas d'autres supports disponibles, vous pouvez passer cette étape.

Si vous souhaitez analyser d'autres supports, veuillez en insérer un autre maintenant.

Faut-il analyser d'autres supports d'installation ?

<Revenir en arrière>

19. <u>Miroir réseau</u> → « Oui ».

[!] Configurer l'outil de gestion des paquets		
L'utilisation d'un miroir sur le réseau peut permettre de compléter présents sur le support d'installation. Il peut également donner acc plus récentes.	les logici ès à des v	els ersions
Vous effectuez actuellement une installation depuis une image DVD. E paquets soient présents, certains peuvent manquer. Si vous disposez bonne qualité à Internet, vous devriez utiliser un miroir réseau de vous souhaitez installer un environnement graphique de bureau, .	lien que de d'une conn la distrib	nombreux exion de ution si
Faut–il utiliser un miroir sur le réseau ?		
<revenir arrière="" en=""></revenir>	<mark>KOui&gt;</mark>	<non></non>

- 20. <u>Pays miroir</u> → France.
- 21. <u>Choix du miroir</u> → deb.debian.org
- 22. <u>Mandataire Proxy</u> → Je n'ai pas de proxy → Continuer.
- 23. <u>Configuration popularity-contest</u> → Non.



24. Je choisie : « Serveur SSH & Utilitaire du système » → Continuer

25. Installation Grub → Oui.

[!] Installer le programme de démarrage GRUB	
Il semble que cette nouvelle installation soit le seul système d'explo sur cet ordinateur. Si c'est bien le cas, il est possible d'installer démarrage GRUB sur le disque principal (partition UEFI ou secteur d'an	Ditation existant le programme de morçage).
Attention : si le programme d'installation ne détecte pas un système d installé sur l'ordinateur, cela empêchera temporairement ce système de Toutefois, le programme de démarrage GRUB pourra être manuellement rec pour permettre ce démarrage.	d'exploitation e démarrer. configuré plus tard
Installer le programme de démarrage GRUB sur le disque principal ?	
<revenir arrière="" en=""></revenir>	<mark>KOui&gt;</mark> <non></non>

26. <u>Installé le programme de démarrage</u> → /dev/sda.

[!] Installer le programme de démarrage GRUB Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode habituelle pour cela est de l'installer sur le disque principal (partition UEFI ou secteur d'amorçage). Vous pouvez, si vous le souhaitez, l'installer ailleurs sur un autre disque, une autre partition, ou même sur un support amovible. Périphérique où sera installé le programme de démarrage : Choix manuel du périphérique /dev/sda (scsi-OQEMU\_QEMU\_HARDDISK\_drive-scsio) <Revenir en arrière>



# 4 Configuration Debian.

- 1. Je démarre le serveur debian.
- 2. Je me connecte avec le compte root.

# 4.1 Configuration du réseau :

3. Je me rends dans /etc/network/

### Commandes :

cd /etc/network

4. Je modifie le fichier interfaces et j'ajoute la configuration si dessous.

<u>Commandes :</u>	
nano interfaces	
Configuration :	
allow-hotplug ens19	
iface ens19 inet static	
address 10.16.100.253/30	
gateway 10.16.100.254	
<pre># The primary network interface allow-hotplug ens18 iface ens18 inet static</pre>	

```
# dns-* options are implemented by the resolvconf package, if installed
dns-nameservers 10.16.1.2
dns-search sandbox.local
allow-hotplug ens19
iface ens19 inet static
```

- address 10.16.100.253/30 gateway 10.16.100.254
- 5. Je modifie le fichier de configuration DNS.

## Commandes :

```
nano /etc/resolv.conf
Configuration:
search sandbox.local
nameserver 10.16.1.2
nameserver 192.168.1.254 #Remplacé cette valeur par votre DNS interne
nameserver 1.1.1.1
```



6. Je protège contre l'écriture les fichiers de configuration : resolv.conf & interfaces.

<u>Commandes :</u>						
chattr +i /etc/resolv.conf						
<pre>chattr +i /etc/network/interfaces</pre>						

7. Je redémarre le serveur.

# 4.2 Configuration dépot.

- 1. Je me connecte en root sur le serveur.
- 2. Je me rends dans /etc/apt.

## Commandes :

cd /etc/apt

3. Je modifie le fichier sources.list → Je commente les lignes CDrom.

# deb co # <u>d</u> eb co	drom:[Debian drom:[Debian	GNU/Linux GNU/Linux	11.8.0 11.8.0	_Bullseye _Bullseye	· Official · Official	amd64 D∖ amd64 D∖	D Binary–1 D Binary–1	20231007-14:05]/ 20231007-14:05]/	bullseye bullseye	contrib contrib	main main
deb http deb–src	o://deb.debi http://deb.	an.org/deb debian.org	ian/ <mark>bul</mark> ] /debian/	lseye main bullseye ma	in						
deb htt: deb–src	o://security http://secu	.debian.or: rity.debia	g/debian- h.org/deb	-security <mark>bu</mark> Dian-securit	ıllseye−se y bullsey	curity ma e-securit	in contrib y main con	trib			
# bulls@ # see hi deb htt; deb–src	eye–updates, ttps://www.d o://deb.debi http://deb.	to get up ebian.org/u an.org/deb debian.org,	dates bef doc/manua ian/ bull /debian/	fore a point als/debian–r lseye–update bullseye–up	: release reference/ es main co odates mai	is made; ch02.en.h ntrib n contrib	tml#_updat	es_and_backports			

4. Je protège contre l'écriture « sources.list ».

# Commandes :

chattr +i /etc/apt/sources.list

5. Je mets à jour les paquet.

### Commandes :

apt update && apt upgrade

```
root@srv-guacamole:/etc/apt# apt update && apt upgrade
Atteint :1 http://deb.debian.org/debian bullseye InRelease
Atteint :2 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
```



# 4.3 Ajout et configuration d'un disque :

Source : https://artheodoc.wordpress.com/2015/05/29/ajouter-un-nouveau-disque-dur-sous-linux/

1. Je me connecte au serveur Debian et je l'éteins.

## <u>Commandes :</u>

Shutdown #Eteint le serveur 1 minutes après l'exécution du serveur.

Init 0 #Eteint le serveur immédiatement.

- 2. Je vais dans proxmox → Matériel → Ajouter → Disque Dur.
- 3. J'allloue 100Go au disque dur → Ajouter.

🗭 Machine	Par	detau	it (14401x)	
Ajouter: Disque	dur			$\otimes$
Disque Band	e passante			
Bus/périphérique:	SCSI V 1	$\hat{}$	Cache:	Par défaut (Aucun cache 🗸
Contrôleur SCSI:	VirtIO SCSI single		Abandonner:	
Stockage:	storage	$\sim$	IO thread:	
Taille du disque (Gio):	100	$\hat{}$		
Format:	Image au format QEMU	$\sim$		
Aide				Avancé 🗌 Ajouter

- 4. Je démarre et je me connecte au serveur.
- 5. J'affiche les table de partition des périphériques :

# Commandes :

fdisk -1 | more

root@srv-guacamole:~# fdisk –1   more
Disque /dev/sda : 32 GiB, 34359738368 octets, 67108864 secteurs
Modèle de disque : QEMU HARDDISK
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0xea43f3a8
Périphérique Amorçage Début Fin Secteurs Taille Id Type
/dev/sda1 * 2048 65107967 65105920 31G 83 Linux
/dev/sda2 65110014 67106815 1996802 975M 5 Étendue
/dev/sda5 65110016 67106815 1996800 975M 82 partition d'échange Linux / Solaris
Disque /dev/sdb : 100 GiB, 107374182400 octets, 209715200 secteurs
Modèle de disque : QEMU HARDDISK
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets



Ici on peut voir que le disque /dev/sdb est mon nouveau disque.

### Commandes :

fdisk -l /dev/sdb

```
root@srv-guacamole:~# fdisk –1 /dev/sdb
Disque /dev/sdb : 100 GiB, 107374182400 octets, 209715200 secteurs
Modèle de disque : QEMU HARDDISK
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
```

6. Je modifie le type de partition :

### Commandes :

fdisk /dev/sdb

```
Bienvenue dans fdisk (util-linux 2.36.1).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.
Le périphérique ne contient pas de table de partitions reconnue.
Création d'une nouvelle étiquette pour disque de type DOS avec identifiant de disque 0xb54e4c06.
Commande (m pour l'aide) : n
Type de partition
        p primaire (0 primaire, 0 étendue, 4 libre)
        e étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) : 2
Premier secteur, the secteurs ou the table (K,M,G,T,P) (2048-209715199, 209715199 par défaut) :
Une nouvelle partition 2 de type « Linux » et de taille 100 GiB a été créée.
Commande (m pour l'aide) : w_
```

### 7. Je formate le disque en ext4.

# Commandes :

mkfs.ext4 /dev/sdb

8. Je vais dans le dossier /srv et je créée le dossier guaca-rec pour le point de montage.

<u>Commandes :</u>

cd /srv/

mkdir guaca-rec



9. J'édite le fichier fastb pour que le montage soit prise en charge au démarrage de la machine.

Commandes :								
nano /etc/f	stab							
<u>Configuration</u>	<u>n :</u>							
/dev/sdb	/srv/guaca-rec	ext4	defaults	0	0			
# /etc/fsta	ab: static file syste	em infor	mation.					
# # Use 'hlk:	id' to print the univ	versallu	unique ider	tifier	for a			
# device; 1	this may be used with	h UUID=	as a more ro	bust wa	iy to n	ame devices		
# that work	ks even if disks are	added a	and removed.	See fst	ab(5).			
۳ # systemd ۽	generates mount units	s based	on this file	e, see s	systemd	.mount(5).		
# Please ru	un 'systemotl daemon-	-reload'	after makir	ng chang	(es her	e.		
# <file sys<="" th=""><td>stem&gt; <mount point=""></mount></td><td><type></type></td><th><pre><options></options></pre></th><th></th><th>(dump&gt;</th><td><pass></pass></td><td></td><td></td></file>	stem> <mount point=""></mount>	<type></type>	<pre><options></options></pre>		(dump>	<pass></pass>		
# / was on	/dev/sda1 during ins	stallati	.on					
UUID=e1d2b8	319-8d2d-401a-89f8-f(	ca141ba1	.65c /		ext4	errors=rer	nount-ro O	1
W Swap was	0A /uev/Sua5 uuring 197–464e–4fbc–95b6–5	3da73d5d	l3e2 none		suan	SIII	0	0
/dev/sr0	/media/cdromO	udf,is	09660 user,r	noauto	0	0		× i
/dev/sdb	/srv/guaca-rec	ext4	defaults	C	)	0		

10. Je monte le disque :

<u>Commandes :</u>	
mount /srv/guaca-rec/	



# 5 Installation guacamole.

Source : https://www.it-connect.fr/tuto-apache-guacamole-bastion-rdp-sshdebian/#III Installer Apache Guacamole sur Debian

# 5.1 Installation des prérequis d'apache guacamole.

1. Mise à jour des dépôts.

### Commandes :

Apt-get update

2. Installation des dépendances.

### Commandes :

apt-get install build-essential libcairo2-dev libjpeg62-turbo-dev libpng-dev libtool-bin uuiddev libossp-uuid-dev libavcodec-dev libavformat-dev libavutil-dev libswscale-dev freerdp2-dev libpango1.0-dev libssh2-1-dev libtelnet-dev libvncserver-dev libwebsockets-dev libpulse-dev libssl-dev libvorbis-dev libwebp-dev sudo wget

root@srv-guacamole:~# apt-get install build-essential libcairo2-dev libjpeg62
ormat-dev libavutil-dev libswscale-dev freerdp2-dev libpango1.0-dev libssh2-1
vorbis-dev libwebp-dev sudo wget
Lecture des listes de paquets Fait
Construction de l'arbre des dépendances Fait
Lecture des informations d'état Fait
build-essential est déjà la version la plus récente (12.9).
libcairo2-dev est déjà la version la plus récente (1.16.0-5).
libavcodec-dev est déjà la version la plus récente (7:4.3.6-0+deb11u1).
libavformat-dev est déjà la version la plus récente (7:4.3.6-0+deb11u1).
libavutil-dev est déjà la version la plus récente (7:4.3.6-0+deb11u1).
libswscale-dev est déjà la version la plus récente (7:4.3.6-0+deb11u1).
freerdp2-dev est déjà la version la plus récente (2.3.0+dfsg1-2+deb1lu1).
libjpeg62-turbo-dev est déjà la version la plus récente (1:2.0.6-4).
libpng-dev est déjà la version la plus récente (1.6.37-3).
libssh2-1-dev est déjà la version la plus récente (1.9.0-2).
libtelnet-dev est déjà la version la plus récente (0.21-5+b1).
libtool-bin est déjà la version la plus récente (2.4.6-15).
libvncserver-dev est déjà la version la plus récente (0.9.13+dfsg-2+deb11u1).
libvorbis-dev est déjà la version la plus récente (1.3.7-1).
libwebp-dev est déjà la version la plus récente (0.6.1-2.1+deb11u2).
libwebsockets-dev est déjà la version la plus récente (4.0.20-2).
libssl-dev est déjà la version la plus récente (1.1.1w-0+deb11u1).
libossp-uuid-dev est déjà la version la plus récente (1.6.2-1.5+b9).
libpangol.0-dev est déjà la version la plus récente (1.46.2-3).
libpulse-dev est déjà la version la plus récente (14.2-2).
sudo est déjà la version la plus récente (1.9.5p2-3+deb11u1).
uuid-dev est déjà la version la plus récente (2.36.1-8+deb11u1).
wget est déjà la version la plus récente (1.21-1+deb11u1).
0 mis à jour, 0 nouvel <u>l</u> ement installés, 0 à enlever et 0 non mis à jour.



# 5.2 Compilation et installation Apache Guacamole « Server ».

1. Je me positionne dans le fichier « /tmp ».

### Commandes :

/tmp

2. Téléchargement du fichier guacamole.

## Commandes :

wget <a href="https://downloads.apache.org/guacamole/1.5.3/source/guacamole-server-1.5.3.tar.gz">https://downloads.apache.org/guacamole/1.5.3/source/guacamole-server-1.5.3.tar.gz</a>

3. Je décompresse l'archive tar.gz et je me positionne dans repertoire obtenue.

### Commandes :

tar -xzf guacamole-server-1.5.3.tar.gz

cd guacamole-server-1.5.3/

root@srv-guacamole:/tmp# tar -xzf guacamole-server-1.5.3.tar.gz root@srv-guacamole:/tmp# cd guacamole-server-1.5.3/



4. Je prépare la compilation de guacamole.

# Commandes: sudo ./configure --with-init-dir=/etc/init.d freerdp2 .....yes pango ....yes libavcodec ...yes libavformat...yes libssh2 ....yes libssh2 ...yes libtelnet ...yes libtelnet ...yes libvrDis ...yes libvescale ...yes libtelnet ...yes libvurbis ...yes libvescale ...yes libtelnet ...yes libvurbis ...yes libverbis ...yes libwebsockets ...yes libwebp ....yes wsock32 .....no

Protocol support:

Kubernetes yes RDP yes SSH yes Telnet yes
VNC yes Services / tools:
guacd yes guacenc yes guaclog yes
FreeRDP plugins: /usr/lib/x86_64-linux-gnu/freerdp2 Init scripts: /etc/init.d Systemd units: no
/pe "make" to compile guacamole-server.

5. Je compile le code source de guacamole-server.

# Commandes :

sudo make

6. J'installe le composant Guacamole Server.

## Commandes :

sudo make install

7. Je mets à jour les liens entre les guacamole-server et les libraires :

# Commandes :

sudo ldconfig



8. Je démarre le service « guacd ».

## Commandes :

```
sudo systemctl daemon-reload
```

sudo systemctl start guacd # Démarrage service guacamole.

sudo systemctl enable guacd # Activation service guacamole.

```
root@srv-guacamole:/tmp/guacamole-server-1.5.3# systemctl daemon-reload
root@srv-guacamole:/tmp/guacamole-server-1.5.3# systemctl start guacd.service
root@srv-guacamole:/tmp/guacamole-server-1.5.3# systemctl enable guacd.service
guacd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable guacd
root@srv-guacamole:/tmp/guacamole-server-1.5.3#
```

9. Je vérifie le statut du serveur Apache Guacamole.

### Commandes :

systemctl status guacd

```
root@srv-guacamole:/tmp/guacamole-server-1.5.3# systemctl status guacd.service

guacd.service - LSB: Guacamole proxy daemon

Loaded: loaded (/etc/init.d/guacd; generated)

Active: active (running) since Wed 2024-03-13 11:17:51 CET; 1min 25s ago

Docs: man:systemd-sysv-generator(8)

Tasks: 1 (limit: 4767)

Memory: 11.9M

CPU: 15ms

CGroup: /system.slice/guacd.service

L14752 /usr/local/sbin/guacd -p /var/run/guacd.pid

mars 13 11:17:51 srv-guacamole systemd[1]: Starting LSB: Guacamole proxy daemon...

mars 13 11:17:51 srv-guacamole guacd[14750]: Guacamole proxy daemon (guacd) version 1.5.3 started

mars 13 11:17:51 srv-guacamole guacd[14749]: Starting guacd:

mars 13 11:17:51 srv-guacamole guacd[14749]: Starting guacd:

mars 13 11:17:51 srv-guacamole guacd[14749]: Starting guacd:

mars 13 11:17:51 srv-guacamole guacd[14749]: SUCCESS

mars 13 11:17:51 srv-guacamole guacd[14752]: Listening on host ::1, port 4822
```



# 5.3 Création repertoire de configuration.

Je crée le répertoire de configuration.

## Commandes :

sudo mkdir -p /etc/guacamole/{extensions, lib}

# 5.4 Installation Guacamole Client (Web app).

1. J'installe Tomcat9.

### Commandes :

sudo apt-get install tomcat9 tomcat9-admin tomcat9-common tomcat9-user

2. Je télécharge la dernière version de l'application Web Apache Guacamole.

<u>Commandes :</u>
cd /tmp
wget <a href="https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-1.5.3.war">https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-1.5.3.war</a>
root@srv-guacamole:/tmp# wget https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-1.5.3.war 2024-03-13 11:55:13 https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-1.5.3.war Résolution de downloads.apache.org (downloads.apache.org)… 135.181.214.104, 88.99.208.237, 2a01:4f9:3a:2c57::2, Connexion à downloads.apache.org (downloads.apache.org)… 135.181.214.104/ 88.99.208.237, 2a01:4f9:3a:2c57::2, requéte HTTP transmise, en attente de la réponse… 200 OK Taille : 13631953 (13M) Sauvegarde en : « guacamole-1.5.3.war »
guacamole-1.5.3.war 100%[===================================

24-03-13 11:55:14 (12,3 MB/s) – « guacamole-1.5.3.war » sauvegardé [13631953/13631953]

3. Je déplace déplace le fichier dans dans la librairie Web app de tomcat9.

### Commandes :

sudo mv guacamole-1.5.3.war /var/lib/tomcat9/webapps/guacamole.war

4. Je redemarre le service tomtcat9 et apache Guacamole.

### Commandes :

sudo systemctl restart tomcat9 guacd





# 5.5 Installation d'une base de données MariaDB pour l'authentification.

- 1. Je me connecte au serveur.
- 2. J'installe le paquet « MariaDB Server » :

# Commandes :

sudo apt-get install mariadb-server

root@srv-guacamole:/tmp# 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 gawk libaio1 libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libencode-locale-perl
libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl
liblwp-mediatypes-perl libmariadb3 libterm-readkey-perl libtimedate-perl liburi-perl mariadb-client-10.5 mariadb-client-core-10.5 mariadb-common
mariadb-server-10.5 mariadb-server-core-10.5 mysql-common psmisc rsync socat
Paquets suggérés :
gawk-doc libmldbm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl libipc-sharedcache-perl libwww-perl mailx mariadb-test
Les NOUVEAUX paquets suivants seront installés :
galera-4 gawk libaiol libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libencode-locale-perl
libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl
liblwp-mediatypes-perl libmariadb3 libterm-readkey-perl libtimedate-perl liburi-perl mariadb-client-10.5 mariadb-client-core-10.5 mariadb-common
mariadb-server mariadb-server-10.5 mariadb-server-core-10.5 mysql-common psmisc rsync socat
0 mis à jour, 34 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 17,8 Mo dans les archives.
Après cette opération, 160 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n]

3. Configuration sécuriser de mariadb :

# Commandes:

sudo mysql\_secure\_installation

# **Configuration :**

https://www.it-connect.fr/installer-un-serveur-lamp-linux-apache-mariadb-php-sous-debian-11/

4. Connexion à la base de données :

# Commandes :

mariadb -u root -p

5. Création de la base de donnée :

# Commandes :

CREATE DATABASE guacadb;

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



6. Création de l'utilisateurs et configuration des droits de la base de données.

# Commandes :

CREATE USER 'guaca\_nachos'@'localhost' IDENTIFIED BY 'VotreMot2P@sse!';

GRANT SELECT, INSERT, UPDATE, DELETE ON guacadb.\* TO 'guaca\_nachos'@'localhost';

FLUSH PRIVILEGES;

EXIT;

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

MariaDB [(none)]> FLUSH PRIVILEGES; Query OK, 0 rows affected (0,001 sec)

4ariaDB [(none)]> EXIT;

7. Téléchargement et installation de l'extension MySQL à Apache Guacamole.

### Commandes :

cd /tmp

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

8. Extraction de l'extension.

# Commandes :

tar -xzf guacamole-auth-jdc.1.5.3.tar.gz

oot@srv-guacamole:/tmp# tar -xzf guacamole-auth-jdbc-1.5.3.tar.gz					
root@srv-guacamole:/tmp# ls -lh					
total 32M					
drwxr-xr-x 6 sandbox sandbox 4,0K 26 juil.  2023 guacamole-auth-jdbc-1.5.3					
-rw-rr 1 root    root       32M 26 juil.  2023 guacamole-auth-jdbc-1.5.3.tar.gz					
drwx 3 root root 4,0K 14 mars 09:39 systemd-private-1f7dacf564a640999fde707a90d7b582-systemd-logind.service-ABpChi					
drwx 3 root root 4,0K 14 mars 09:39 systemd-private-1f7dacf564a640999fde707a90d7b582-systemd-timesyncd.service-zWPucj					
drwx 3 root root 4,0K 14 mars 09:46 systemd-private-1f7dacf564a640999fde707a90d7b582-tomcat9.service-Fcs23e					
root@srv-guacamole:/tmp#					

9. Déplacement de l'extension dans le repertoire « /etc/guacamole/extensions/ » :

<u>Commandes :</u>		
sudo	mv	<pre>guacamole-auth-jdbc-1.5.3/mysql/guacamole-auth-jdbc-mysql-1.5.3.jar</pre>
/etc/guacamol	e/extensions	/



10. Téléchargement du connector mysql.

# Commandes:wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-8.3.0.tar.gzroot@srv.guacamole:/tmp# wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-8.3.0.tar.gz-:2024-03-14 10:26:27-- https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-8.3.0.tar.gzroot@srv.guacamole:/tmp# wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-8.3.0.tar.gzroot@srv.guacamole:/tmp# wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-8.3.0.tar.gzroot@srv.guacamole:/tmp# wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-j-8.3.0.tar.gzRésolution de dev.mysql.com (dev.mysql.com/get/Downloads/Connector-J/mysql-23::22610:1b00:226:226:1200:22610:1200:22610:1200:22610:1200:2201120:22011

11. Decompression de l'archive.

### Commandes :

```
tar -xzf mysql-connector-j-8.3.0.tar.gz
```

12. Copie du connecteur vers le fichier « lib » d'apache Guacamole.

## Commandes :

sudo cp mysql-connector-j-8.3.0/mysql-connector-j-8.3.0.jar /etc/guacamole/lib/

13. Importation de la structure de la base de donnée apache Guacamole dans la base de donnée « Guacadb ».

### Commandes :

```
cd guacamole-auth-jdbc-1.5.3/mysql/schema/
```

```
cat *.sql | mariadb -u root -p guacadb
```

14. Création et modification du fichier « guacamole.properties » pour déclarer la connexion à la base de donnée.

# Commandes :

sudo nano /etc/guacamole/guacamole.properties

### **Configuration :**

# Mariadb :

mariadb-hostname : 127.0.0.1

mariadb-port : 3306

mariadb-database : guacadb

```
mariadb-username : guaca_nachos
```

mariadb-password : VotreMot2P@sse!



15. Création et modification du fichier « guacd.conf » pour déclarer le serveur guacamole.

Commandes :
sudo nano /etc/guacamole/guacd.conf
Configuration :
[server]
pind_host = 0.0.0.0
pind_port = 4822
[server]

pind host = 0.0.0.0

bind port = 4822

16. Redémarrage des services lier à Apache Guacamole.

# Commandes :

sudo systemctl restart tomcat9 guacd mariadb

### Tomcat9:

tomcat9.se	rvice - Apache Tomcat 9 Web Application Server
Loaded:	loaded (/lib/systemd/system/tomcat9.service; enabled; vendor preset: enabled)
Active:	active (running) since Thu 2024-03-14 11:34:51 CET; 13s ago
Docs:	https://tomcat.apache.org/tomcat-9.0-doc/index.html
Process:	2699 ExecStartPre=/usr/libexec/tomcat9/tomcat-update-policy.sh (code=exited, status=0/SUCCESS)
Main PTD.	2703 (java)

Guacd :

### MariaDB :

mariadb.se	rvice - MariaDB 10.5.23 database server
Loaded:	<pre>loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)</pre>
Active:	active (running) since Thu 2024-03-14 11:34:52 CET; 13s ago
Docs:	man:mariadbd(8)
	https://mariadb.com/kb/en/library/systemd/
Process:	2729 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld
Process:	2730 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION
Process:	2732 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR=    VA
Process:	2799 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITIC
Process:	2801 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
Main PID:	2779 (mariadbd)
Status:	"Taking your SQL requests now"
Tasks:	19 (limit: 4767)
Memory:	73.6M
CPU:	323ms
CGroup:	/system.slice/mariadb.service
	└─2779 /usr/sbin/mariadbd



# 6 Premier pas avec Apache Guacamole.

https://www.it-connect.fr/tuto-apache-guacamole-bastion-rdp-sshdebian/#IV Premiers pas avec Apache Guacamole

1. Je me connecte sur l'application apache guacamole.

URL : http://srv-guacamole.sandbox.local:8080/guacamole/#/

•	9	Apache G	iuacamole	×	+	-	-	٥	×
←	$\rightarrow$	C	A Not secure	srv-gua	icamole.sandbox.local:8080/guacamole/#/	☆	д		:
<i>pf</i> P	fsense								



2. Je me connecte avec le compte admin par défaut.

Username : guacadmin

Mot de passe : guacadmin

# 6.1 Création d'un nouveau compte admin.

- 1. Je me connecte à apache Guacamole
- 2. Je me rends dans Setting → Users → New Users.

SETTINGS								💄 guacadmin 👻
Active Sessions	History	Users	Groups	Connections	Preferences			
Click or tap on a u	Click or tap on a user below to manage that user. Depending on your access level, users can be added and deleted, and their passwords can be changed.							
<u>∎</u> * New User	* New User Q Filter							
	Usernar	me 🕶			Organization	Full name	Last active	
💄 guacadmin	ı						2024-03-14 15:29:20	

3. Edit User : Je rentre les informations de l'utilisateurs.

EDIT USER						
Username:	noah.maillet					
Password:						
Re-enter Password:						

4. Profile : Je rentre les informations.



# PROFILE

Full name:	Noah MAILLET Local
Email address:	noah.maillet@sandbox.local
Organization:	Sandbox
Role:	Administrateur System Local

5. Permissions : Je coche tout les droit pour donner accès à l'utilisateurs.

# PERMISSIONS

Administer system:	~
Create new users:	~
Create new user groups:	<b>~</b>
Create new connections:	<b>~</b>
Create new connection groups:	<b>~</b>
Create new sharing profiles:	<b>~</b>
Change own password:	~

6. Test de de connexion avec le nouvel utilisateur.

RECENT CONNECTIONS

No recent connections.

💄 noah.maillet 👻



# 6.2 Ajout d'une connexion.

# 6.2.1 Connexion SSH.

# 6.2.1.1 Configuration.

- 1. Je me connecte sur Apache Guacamole.
- 2. Je me rends dans Paramètres  $\rightarrow$  Connexion  $\rightarrow$  Nouvelle connexion.

J'ai au préalable créer un groupe pour répartir mes connexions.

3. Modifier la connexion.

Nom:	SRV-LLDAP
Lieu:	Administration
Protocole:	SSH 🗸

4. Paramètres – Réseau.

# Réseau

Nom d'hôte:

srv-lldap.sandbox.local

Port:

22

Clé publique de l'hôte (Base64):



5. Paramètres – Authentification.

# Authentification

Identifiant:	sandbox	]
Mot de passe:	•••••	] 🖬
Clé privée:		
		6
Phrase secrète:		] 🖬

# 6. Paramètres – Session Environnement.

# Session / Environnement

Exécuter une commande:			
Langue/Locale (\$LANG):			
Fuseau horaire (\$TZ):	Europe	✓ Paris	~
Intervalle keepalive Serveur:			

7. Enregistrer.



# 6.2.1.2 Test de la connexion.

1. Je me rends sur la page d'acceuil de guacamole.

# TOUTES LES CONNEXIONS Administration Administration S SRV-LLDAP 2. Je clique sur « SRV-LLDAP ». 3. La connexion est fonctionnelle. Linux SRV-LLDAP 6.5.13-1-pve #1 SMP PREEMPT\_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50Z) x86\_64 The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright. Debian GNU/Linux comes with ABSOLUTELY NO WAPPANTY to the extent

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Thu Mar 14 15:39:44 2024 from 10.16.1.1 sandbox@SRV-LLDAP:~\$

# 6.2.2 Connexion RDP.

# 6.2.2.1 Configuration.

- 1. Je me connecte sur Apache Guacamole.
- 2. Je me rends dans Paramètres → Connexion → Nouvelle connexion.
- 3. Modifier connexion :



4. Paramètres – Réseau :

# Réseau

Nom d'hôte:host-admin.sandbox.localPort:3389



5. Paramètres – Authentification :

# Authentification

Identifiant:	
Mot de passe:	
Nom de domaine:	
Mode de Sécurité:	[
Désactiver l'authentification:	
Ignorer le certificat du serveur:	

sandbox-admin	
•••••	
	~

~

6. Paramètres – Paramètres de base :

# Paramètres de base

Programme de démarrage:		]
Nom du Client:		]
Agencement clavier:	Français (Azerty)	~
Fuseau horaire:	Europe V Paris	~
Enable multi-touch:		
Console Administrateur:		

# 7. Paramètres – Presse-papiers :

# **Presse-papiers**

Line endings:Windows (CRLF)Désactiver la copie depuis l'ordinateur distant:Désactiver coller à partir du client:

8. Enregistrer.



# 6.2.2.2 Test de la connexion.

- 1. Je me rends sur la page d'acceuil d'apache Guacamole.
- 2. Je clique sur « Host-Admin ».



3. La connexion à « Host-Admin » est fonctionnelle.





# 7 Sécurité d'Apache Guacamole.

# 7.1 Créer un enregistrement video des sessions.

- 1. Je me connecte en ssh sur le serveur guacamole.
- 2. Je vais dans /tmp et je télécharge l'extension D'enregistrement de guacamole.

### Commandes :

cd /tmp

wget <u>https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-history-recording-storage-</u> 1.5.3.tar.gz



3. Je décompresse l'extensions.

### Commandes :

Tar -xzf guacamole-history-recording-storage-1.5.3.tar.gz

4. Je déplace le fichier .jar de l'extension dans le répertoire extenstions de guacamole.

### Commandes :

sudo mv guacamole-history-recording-storage-1.5.3/guacamole-history-storage-1.5.3.jar
/etc/guacamole/extensions

5. Je redémarre le service Tomcat9.

### Commandes :

sudo systemctl restart tomcat9

```
root@srv-guacamole:/tmp# systemctl status tomcat9.service
● tomcat9.service - Apache Tomcat 9 Web Application Server
Loaded: loaded (/lib/systemd/system/tomcat9.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2024-03-15 lo:26:33 CET; 12s ago
Docs: https://tomcat.apache.org/tomcat-9.0-doc/index.html
Process: 862 ExecStartPre=/usr/libexec/tomcat9/tomcat-update-policy.sh (code=exited, status=0/SUCCESS)
Main PTD: 866 (java)
Tasks: 37 (limit: 4661)
Memory: 250.9M
CPU: 13.274s
CGroup: /system.slice/tomcat9.service
______866 /usr/lib/jvm/default-java/bin/java -Djava.util.logging.config.file=/var/lib/tomcat9/conf/logging.properties -Djava.util.logging.manager=or
```



6. Je créer le fichiers « Recordings » sur mon deuxième disque.

# Commandes :

Cd /srv/guaca-rec

Mkdir recordings

```
root@srv-guacamole:/tmp# cd /srv/guaca-rec/
root@srv-guacamole:/srv/guaca-rec# mkdir recordings
root@srv-guacamole:/srv/guaca-rec# ls -lh
total 20K
drwx----- 2 root root 16K 14 mars 14:26 lost+found
drwxr-xr-x 2 root root 4,0K 15 mars 10:32 recordings
root@srv-guacamole:/srv/guaca-rec#
```

7. Je change les permissions du repertoire « recordings ».

### Commandes :

```
sudo chown root:tomcat /srv/guaca-rec/recordings
```

```
sudo chmod 2750 /srv/guaca-rec/recordings
```

```
root@srv-guacamole:/srv/guaca-rec# sudo chown root:tomcat /srv/guaca-rec/recordings/
root@srv-guacamole:/srv/guaca-rec# sudo chmod 2750 /srv/guaca-rec/recordings/
root@srv-guacamole:/srv/guaca-rec# ls -lh
total 20K
drwx----- 2 root root 16K 14 mars 14:26 lost+found
drwxr-s--- 2 root root 16K 15 mars 10:32 recordings
```

8. Je configure le chemin de stockage des enregistrements « guacamole.properties ».

<u>Commandes :</u>
cd /etc/guacamole/
nano guacamole.properties
Configuration :
# Recording path.
Recording-search-path : /srv/guaca-rec/recordings

```
GNU nano 5.4

# Mariadb :

mysql-hostname: 127.0.0.1

mysql-port: 3306

mysql-database: guacadb

mysql-username: guaca_nachos

mysql-password:

# Recording Path :

recording-search-path: /srv/guaca-rec/recordings
```



# 7.2 Configuration enregistrement d'une connexions.

- 1. Je me connecte à apache guacamole.
- 2. Je vais dans paramètres  $\rightarrow$  Connexion  $\rightarrow$  « Nom de la connexion ».



3. Paramètres - Enregistrement Ecran.

# **Configuration :**

Chemin de l'enregistrement: \${HISTORY\_PATH}/\${HISTORY\_UUID}

Nom de l'enregistrement: \${GUAC\_DATE}-\${GUAC\_TIME} - [Protocole] - \${GUAC\_USERNAME}

Je coche : « Créer automatiquement un chemin d'enregistrement ».

### **Enregistrement Ecran**

Chemin de l'enregistrement:	\${HISTORY_PATH}/\${HIST
Nom de l'enregistrement:	\${GUAC_DATE}-\${GUAC_1
Exclure les graphiques/flux:	
Exclure la souris:	
Inclure les événements clavier:	
Créer automatiquement le chemin d'enregistrement:	

4. Test du bon fonctionnement de l'enregistrement.

PARAMÈTRES					💄 noah.maillet 👻		
Sessions Actives Historique	Utilisateurs Groupes Connexions Préf	érences					
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 listés.							
Identifiant	Ouvert depuis 🔺	Durée	Nom de connexion	Hôte distant	Logs		
noah.maillet	15-03-2024 11:08:34	30 secondes	SRV-LLDAP		<u>View</u> •		



# 7.3 Configuration HTTPS de guacamole.

# 7.3.1 Génération du keystore.

- 1. Je me connecte au serveur guacamole.
- 2. Je me déplace dans « /etc /tomcat9 » et je génère le keystore.

### Commandes :

cd /etc/tomcat9

sudo keytool -genkey -alias tomcat -keyalg RSA -keystore /etc/tomcat9/keystore



Le fichier keystore a bien été créer :

root@srv-gua	camol	e:/etc/i	tomcat	t9#	ls -lł	า	
total 216K							
drwxrwxr-x 3	root	tomcat	4,0K	14	mars	14:39	Catalina
-rw-r 1	root	tomcat	7,1K	28	janv.	2021	catalina.properties
-rw-r 1	root	tomcat	1,4K	28	janv.	2021	context.xml
-rw-r 1	root	tomcat	1,2K	28	janv.	2021	jaspic-providers.xml
-rw-rr 1	root	root	2,7K	15	mars	13:53	keystore
-rw-r 1	root	tomcat	2,8K	16	oct.	14:51	logging.properties
drwxr-xr-x 2	root	tomcat	4,0K	14	mars	14:39	policy.d
-rw-r 1	root	tomcat	7,5K	16	oct.	14:51	server.xml
-rw-r 1	root	tomcat	2,2K	28	janv.	2021	tomcat-users.xml
-rw-r 1	root	tomcat	169K	28	<u>j</u> anv.	2021	web.xml



# 7.3.2 Création du connecteur SSL.

- 1. Je me connecte au serveur Guacamole.
- 2. Je copie le fichier « server.xml » pour avoir une sauvegarde en cas de problème.

root@srv-gua	camole:/etc/	tomcat9#	cp sei	rver.xr	nl server.xml-old
root@srv-gua	<pre>camole:/etc/</pre>	tomcat9#	ls -lł		
total 224K					
drwxrwxr-x 3	root tomcat	4,0K 14	mars	14:39	Catalina
-rw-r 1	root tomcat	7,1K 28	janv.	2021	catalina.properties
-rw-r 1	root tomcat	1,4K 28	janv.	2021	context.xml
-rw-r 1	root tomcat	1,2K 28	janv.	2021	jaspic-providers.xml
-rw-rr 1	root root	2,7K 15	mars	13:53	keystore
-rw-r 1	root tomcat	2,8K 16	oct.	14:51	logging.properties
drwxr-xr-x 2	root tomcat	4,0K 14	mars	14:39	policy.d
-rw-r 1	root tomcat	7,5K 16	oct.	14:51	server.xml
-rw-r 1	root root	7,5K 15	mars	14:17	server.xml-old
-rw-r 1	root tomcat	2,2K 28	janv.	2021	tomcat-users.xml
-rw-r 1	root tomcat	169K 28	<u>j</u> anv.	2021	web.xml
root@srv-gua	camole:/etc/	tomcat9#			

3. Je modifie le fichier « server.xml » et j'ajoute le connecteur SSL.

# Commandes :

nano server.xml

### **Configuration :**

<Connector protocol="org.apache.coyote.http11.Http11AprProtocol"

port="8443" maxThreads="200"

scheme="https" secure="true" SSLEnabled="True"

keystoreFile="/etc/tomcat9/keystore"

keystorePass="VotreMot2P@sse!"

clientAuth="false" sslProtocol="TLS"/>

<connector< th=""><th><pre>protocol="org.apache.coyote.http11.Http11AprProtocol"</pre></th></connector<>	<pre>protocol="org.apache.coyote.http11.Http11AprProtocol"</pre>
	port="8443" maxThreads="200"
	<pre>scheme="https" secure="true" SSLEnabled="True"</pre>
	keystoreFile="/etc/tomcat9/keystore"
	keystorePass=""
	<pre>clientAuth="false" sslProtocol="TLS"/&gt;</pre>

4. Je redémarre tomcat9

# <u>Commandes :</u>

sudo systemctl restart tomcat9.service



# 5. Test de la connexion en SSL.

~	e Apache Guacan	mole	×	+		-	٥	×
÷	→ C (01	Not secure http	<b>16</b> ://s	srv-guacamole.sandbox.local.8443/guacamole/#/	☆	д		:
pf	Pfsense 🚯 LLDAP /	Administrati	🖲 Ap	pache Guazamole				



Activate Windows Go to Settings to activate Windows.

15.3



# 8 Synchronisation LLDAP.

https://www.it-connect.fr/apache-guacamole-configurer-authentification-active-directory-ldap/

# 8.1 Installation extension LDAP pour Apache Guacamole.

- 1. Je me connecte au serveur guacamole.
- 2. Je me déplace dans le fichier « /tmp » et je télécharge l'extension « Authentification LDAP ».

### Commandes :

/tmp

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

```
srv-guacamole:=# cd /tmp
srv-guacamole:/tmpW wget https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-auth-ldap-1.5.3.tar.gz
4-03-21 11:04:21-- https://downloads.apache.org/guacamole/1.5.3/binary/guacamole-auth-ldap-1.5.3.tar.gz
ution de downloads.apache.org (downloads.apache.org). 135.181.214.104, 88.99.208.237, 2a01:4f8:10a:39da::2, ...
xion à downloads.apache.org (downloads.apache.org)|135.181.214.104|:443... connecté.
te HTTP transmise, en attente de la réponse... 200 OK
e : 13100655 (12M) [application/x-gzip]
garde en : « guacamole-auth-ldap-1.5.3.tar.gz »
```

3. Je décompresse l'archive.

# Commandes :

tar -xzf guacamole-auth-ldap-1.5.3.tar.gz

4. Je déplace l'extensions dans le répertoire « extensions » de « guacamole ».

# Commandes:

sudo mv guacamole-auth-ldap-1.5.3/guacamole-auth-ldap-1.5.3.jar /etc/guacamole/extensions

5. Je redémarre le service « tomcat9 ».

Commandes:

sudo systemctl restart tomcat9.service

```
mcat9.Service - Apache Tomcat 9 Web Application Server
Loaded: loaded (/lib/systemd/system/tomcat9.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2024-03-21 li-06:46 CET; 12s ago
Docs: https://tomcat.apache.org/tomcat-9.0-doc/index.html
Process: 720 ExecStartPre=/usr/libexec/tomcat9/tomcat-update-policy.sh (code=exited, status=0/SUCCESS)
ain PID: 724 (java)
Tasks: 50 (limit: 4661)
Memory: 300.4M
CPU: j3.841<</pre>
                                     8415
stem.slice/tomcat9.service
24 /usr/lib/jvm/default-java/bin/java -Djava.util.logging.config.file=/var/lib/tomcat9/conf/logging.properties -Djava.util.logging.manager=on
24 /usr/lib/jvm/default-java/bin/java -Djava.util.logging.config.file=/var/lib/tomcat9/conf/logging.properties -Djava.util.logging.manager=on
```



# 8.2 Connexion Guacamole à LLDAP.

https://github.com/lldap/lldap/blob/main/example\_configs/apacheguacamole.md

1. Je modifie la configuration du serveur guacamole et j'ajoute le connecteur LLDAP.

<u>Commandes :</u>
cd /etc/guacamole
nano guacamole.properties
Configuration :
# LDAP Properties :
ldap-hostname: 10.16.1.1
ldap-port: 3890
ldap-user-base-dn: ou=people, dc=sandbox, dc=local
ldap-username-attribute: uid
ldap-search-bind-dn: uid=admin,dc=sandbox,dc=local
ldap-search-bind-password: VotreMot2P@sse!
# LDAP Properties :
ldap-hostname: 10.16.1.1
ldap-port: 3890
<pre>ldap-user-base-dn: ou=people,dc=sandbox,dc=local</pre>
ldap-username-attribute: uid
ldap-search-bind-dn: uid=admin ou=people dc=sandbox dc=local

- dap-search-bind-password:
  - 2. Je redemarre le service guacamol, tomcat et mariadb.

# Commandes :

Systemtcl restart guacd.service, tomcat9.service, mariadb.service



# 8.3 Création d'un compte administrateur pour la synchronisation.

1. Edit User → Je rentre l'identifiant et le mot de passe.

# EDIT USER

Username:	admin
Password:	
Re-enter Password:	

2. Profile → Je rentre le nom de l'utilisateur, l'organisation et le Role.

PROFILE					
Full name:	ADMIN-LDAP				
Email address:					
Organization:	Sandbox				
Role:	Synchronisation LDAP				

3. Permissions  $\rightarrow$  J'alloue les permissions.

# PERMISSIONS

Administer system:	✓
Create new users:	✓
Create new user groups:	✓
Create new connections:	✓
Create new connection groups:	✓
Create new sharing profiles:	✓
Change own password:	✓



# 8.4 Verification de la synchronisation.

- 1. Je me connecte avec le compte administrateur de mon LLDAP.
- 2. Je me rends dans utilisateurs et je peux voir les utilisateurs de mon Domaine.

<b>▲</b> * New User Q Filter						
Username 👻	Organization	Full name	Last active			
💄 admin	Sandbox	ADMIN-LDAP	2024-03-21 11:20:47			
💄 guacadmin			2024-03-14 15:29:20			
🛓 nmaillet						
L noah.maillet	Sandbox	Noah MAILLET Local	2024-03-21 11:13:40			

3. Je me connecte avec un utilisateur du domaine.

RECENT CONNECTIONS

💄 nmalllet 👻

Q Filter

No recent connections.

### ALL CONNECTIONS

- Administration HOST-ADMIN
  - >\_ SRV-DNS
- >\_ SRV-GUACAMOLE >\_ SRV-LLDAP



# 9 Schéma des Flux Apache Guacamole.





# About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | <u>www.capgemini.com</u>



This document contains information that may be privileged or confidential and is the property of the Capgemini Group.

Company Confidential. Copyright © 2023 Capgemini. All rights reserved.