

Documentation technique : Bastion Apache Guacamole

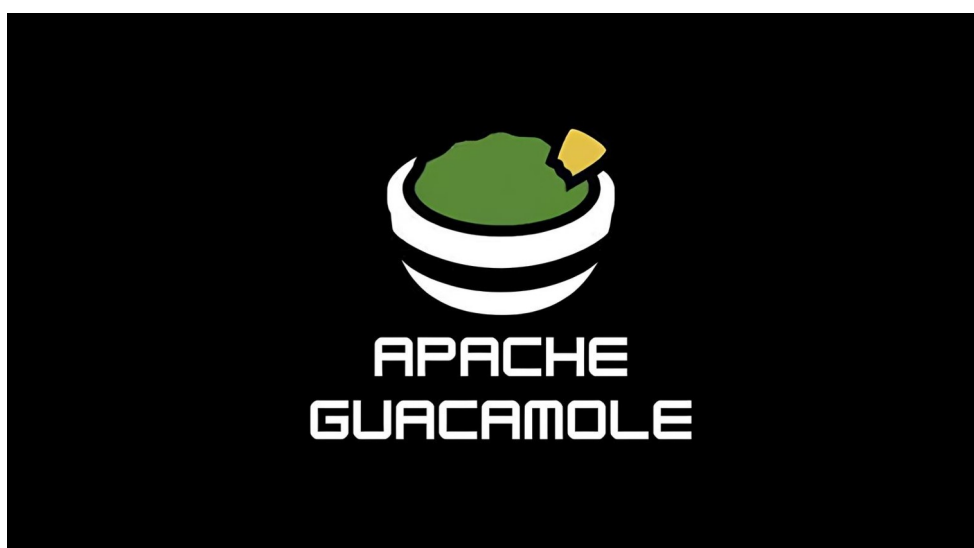
Mission Bastion :

Dans le cadre de la gestion de l'infrastructure réseau de l'organisation **Tiers-Lieux**, la société souhaite tester un outil de type **bastion** afin d'administrer son réseau de manière centralisée et sécurisée. Le responsable technique hésite entre plusieurs solutions logicielles, dont **Wallix** et **Guacamole**, et m'a confié la mission de mettre en place une maquette d'évaluation pour tester les fonctionnalités de base d'un logiciel de bastion.

Le projet consiste à choisir une solution adaptée et à la configurer pour qu'elle réponde aux besoins d'administration des équipements réseaux et des serveurs, tout en garantissant une gestion sécurisée et centralisée des connexions.

Objectifs :

- **Centraliser l'administration des équipements réseau et serveurs** (Linux, Windows, commutateurs, pare-feu, etc.).
- **Assurer un accès sécurisé aux serveurs depuis une machine externe** au réseau de Tiers-Lieux pour permettre aux techniciens d'ITS d'intervenir à distance.
- Mettre en place un système de **gestion des rôles utilisateurs** pour restreindre les droits d'accès en fonction des responsabilités (ex. administrateurs, utilisateurs spécifiques, etc.).
- Lier les comptes d'administration du bastion à **Active Directory** pour une gestion centralisée des utilisateurs.
- Tester la solution choisie et évaluer son efficacité pour l'administration des systèmes.



Installation d'Apache Guacamole

Les ressources nécessaires, de la version 1.5.2, sont disponibles ici : (dernière version actuel)_

<https://downloads.apache.org/guacamole/>

Nous allons télécharger l'archive guacamole-server et l'extraire vers /etc/guacamole qu'il faut créer :

```
#wget https://downloads.apache.org/guacamole/1.5.2/source/guacamole-server-1.5.2.tar.gz
#tar -xzf guacamole-server-1.5.2.tar.gz
#mv guacamole-server-1.5.2 /etc/guacamole
```

Étant donné que nous allons installer Apache Guacamole à partir des fichiers sources, nous aurons besoin d'installer au préalable des paquets qui permettront de compiler cette solution :

```
#aptitude install -y build-essential libpng-dev libjpeg-dev libcairo2-dev_
```

Pour connaître le reste des paquets à installer pour le bon fonctionnement des protocoles, nous pouvons utiliser la commande suivante dans notre dossier Guacamole :

```
#./configure --with-systemd-dir=/etc/systemd/system/
```

```
-----
guacamole-server version 1.5.2
-----

Library status:

 freerdp2 ..... no
  pango ..... no
 libavcodec ..... no
 libavformat..... no
 libavutil ..... no
 libssh2 ..... no
 libssl ..... no
 libswscale ..... no
 libtelnet ..... no
 libVNCServer ..... no
 libvorbis ..... no
 libpulse ..... no
 libwebsockets ..... no
 libwebp ..... no
 wsock32 ..... no
```

```
#aptitude install -y freerdp2-dev libpango1.0-dev libavcodec-dev libavformat-dev  
libavformat-dev libssh2-1-dev libssl-dev libswscale-dev libtelnet-dev libvncserver-dev  
libvorbis-dev libpulse-dev libwebsockets-dev libwebp-dev_
```

Refaire la commande pour configurer les paramètres afin de prendre en compte les nouveaux paquets installés :

```
#./configure --with-systemd-dir=/etc/systemd/system/
```

Une fois les dépendances installées nous pouvons compiler les fichiers sources et initialiser le service guacamole qui est « guacd » :

```
#make && make install && ldconfig
```

```
#systemctl enable guacd
```

```
root@debian:/etc/guacamole# systemctl status guacd.service  
● guacd.service - Guacamole Server  
   Loaded: loaded (/etc/systemd/system/guacd.service; enabled; vendor preset: enabled)  
   Active: inactive (dead)  
     Docs: man:guacd(8)
```

Le service orienté serveur (Guacamole-Server) étant correctement installé il faut maintenant configurer le service orienté client (Guacamole-Client). Dans cette partie nous utiliserons le service tomcat9 en tant que serveur web et le service mariadb pour stocker les données :

```
#aptitude install -y tomcat9 tomcat9-common tomcat9-admin tomcat9-user
```

Spécifier le répertoire principal de Guacamole pour l'environnement Tomcat. Tomcat se basera sur ce chemin pour les fichiers de configuration :

```
#echo GUACAMOLE_HOME=/etc/guacamole > /etc/default/tomcat9
```

La page web de guacamole est contenu dans guacamole-1.4.0.war, il faut donc l'installer dans le dossier web de tomcat :

```
# wget https://downloads.apache.org/guacamole/1.5.5/binary/guacamole-1.5.5.war  
#mv guacamole-1.5.5.war /var/lib/tomcat9/webapps/guacamole.war
```

Étant un nouveau fichier il faut affecter les droits à tomcat sur celui-ci et redémarrer les services :

```
#chown tomcat:tomcat /var/lib/tomcat9/webapps/guacamole.war  
#systemctl restart tomcat9.service guacd.service
```

Pour accéder à la page web de guacamole il faut renseigner son port et le chemin complet > <http://X.X.X.X:8080/guacamole> :



Dans cette partie nous utiliserons le service mariadb pour stocker les données. Guacamole fonctionne grâce à des librairies et à des extensions. Il faut donc créer deux dossier dans le /etc/guacamole :

```
#mkdir /etc/guacamole/{lib,extensions}  
#aptitude install -y mariadb-server mariadb-client
```

```
CREATE DATABASE guacamole;  
CREATE USER 'guacamole'@'localhost' IDENTIFIED BY 'guacamole';  
GRANT ALL PRIVILEGES ON guacamole.* TO 'guacamole'@'localhost';  
FLUSH PRIVILEGES;
```

Une fois ceci fait il faut importer des tables pré-configurées. Nous téléchargerons une extension MYSQL dans notre dossier précédemment créé :

```
#cd /etc/guacamole/extensions/  
#wget https://downloads.apache.org/guacamole/1.5.2/binary/guacamole-auth-jdbc-1.5.2.tar.gz  
#tar -xzf guacamole-auth-jdbc-1.5.2.tar.gz  
#cat guacamole-auth-jdbc-1.5.2/mysql/schema/*.sql | mysql guacamole  
#cp guacamole-auth-jdbc-1.5.2/mysql/guacamole-auth-jdbc-mysql-1.5.2.jar  
/etc/guacamole/extensions/
```

Installation du driver JDBC dans le dossier lib. Ce driver permet à Java (utilisé par l'interface web de guacamole) d'interagir avec la base de données :

```
#cd /etc/guacamole/lib  
#wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-java-8.0.30.tar.gz  
#tar -xzf mysql-connector-java-8.0.30.tar.gz  
#mv mysql-connector-java-8.0.30/mysql-connector-java-8.0.30.jar ./
```

Le dernier fichier à configurer est « guacamole.properties » dans /etc/guacamole Celui-ci permet définir les paramètres à utiliser par notre service « guacd » :

```
#Guacamole  
guacd-hostname: localhost  
guacd-port: 4822  
#Mysql  
mysql-hostname: localhost  
mysql-port: 3306  
mysql-database: guacamole  
mysql-username: guacamole  
mysql-password: guacamole
```

Une fois terminé il faut lier le dossier guacamole à Tomcat et redémarrer les services :

```
#ln -s /etc/guacamole /usr/share/tomcat9/.guacamole  
systemctl restart tomcat9.service  
guacd.service guacd
```

```
root@debian:/etc/guacamole/lib# ln -s /etc/guacamole /usr/share/tomcat9/.guacamole  
systemctl restart tomcat9.service guacd.service  
guacd  
guacd[38844]: INFO:      Guacamole proxy daemon (guacd) version 1.5.2 started
```

Si nous retournons sur notre page web, nous pouvons nous connecter avec l'utilisateur guacadmin/guacadmin, ce compte est le super-utilisateur dans Guacamole :



APACHE GUACAMOLE

guacadmin

Se connecter

CONNEXIONS RÉCENTES

guacadmin

La connexion est réussi !

Opérations de base à réaliser

1. Administration des équipements réseau :

- Configuration du bastion pour administrer les équipements réseau tels que les **routeurs, commutateurs et pare-feu**. (SSH)

MODIFIER CONNEXION

Nom:
Lieu:
Protocole:

Nom, lieu de l'équipement
et le protocole

LIMITES DE CONCURRENCE

Nombre maximum de connexions:
Nombre maximum de connexions par utilisateur:

EQUILIBRAGE DE CHARGE

Poids de la connexion:
Utilisé seulement en cas de bascule: ☐

PARAMÈTRES DU PROXY GUACAMOLE (GUACD)

Nom d'hôte:
Port:
Chiffrement:

PARAMÈTRES

Réseau

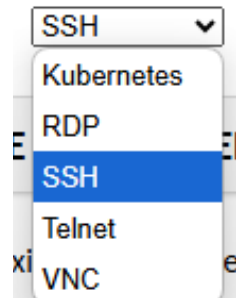
Nom d'hôte:
Port:
Clé publique de l'hôte (Base64):

IP de connexion et le port
(22 = SSH)

Authentification

Identifiant:
Mot de passe:

Identifiant de connexion
SSH de l'équipement



Réseau & Commutateurs

- + > SW-BUREAU
- + > SW-COEUR
- + > SW-DMZ-SRV

Sécurité & Pare-feu

- + > FW-STORMSHIELD

Mes équipements réseau sont
maintenant tous administrable

← → ↻ Non sécurisé https://guacamole.pod3.local/#/client/MwBjAG15c3Fs

🍱 | 🌐 Apache Guacamole 🖥️ Connexion - VMwar... 🌐 172.23.3.250 Admini... 🖥️ Interface standard -... 📺 SRV-Zabl

```
***** SWITCH DU M ET DU J *****
***** W A R N I N G *****
UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED !!!
IF YOU'RE NOT AUTHORIZED TO ACCESS THIS SYSTEM
!!! DISCONNECT NOW !!!
*****
***** A T T E N T I O N *****
LES ACCES NON SOLLICITES SONT STRICTEMENT INTERDITS
SI VOUS N'AVEZ PAS ETE AUTORISE A ACCEDER A CE SYSTEME
!!! DECONNECTEZ VOUS MAINTENANT !!!
*****

2-BUREAU#
```

← → ↻ Non sécurisé https://guacamole.pod3.local/#/client/OQBjAG15c3Fs

🍱 | 🌐 Apache Guacamole 🖥️ Connexion - VMwar... 🌐 172.23.3.250 Admini... 🖥️ Interface standard -... 📺 SRV-Zabbio

```
ast login: Thu Mar 6 09:14:18 2025 from 172.23.3.99
N310A41FJ942A7: FW SN310 (S / EUROPE)
irewall software version 4.3.32 RELEASE
ystem Name: SN310_POD3

ort      name      NS-BSD   state  addressIPv4      addressIPv6
1        out       eth0     up     10.10.103.250/16
2        in        eth1     up     192.168.23.250/24
3        dmz1      eth2     up     172.23.3.250/24
4        dmz2      eth3     down
5        dmz3      eth4     down
6        dmz4      eth5     down
7        dmz5      eth6     down
8        dmz6      eth7     down

N310_POD3-SN310A41FJ942A7>
```

Si nous retournons sur la page d'accueil il est désormais possible de se connecter a mes équipements en SSH.

2. Administration des serveurs :

- Accès aux serveurs **Windows via RDP** et **Linux via SSH** à travers le bastion.

MODIFIER CONNEXION

Nom:
Lieu:
Protocole:

Nom, lieu de l'équipement
et le protocole

LIMITES DE CONCURRENCE

Nombre maximum de connexions:
Nombre maximum de connexions par utilisateur:

EQUILIBRAGE DE CHARGE

Poids de la connexion:
Utilisé seulement en cas de bascule: ☐

PARAMÈTRES DU PROXY GUACAMOLE (GUACD)

Nom d'hôte:
Port:
Chiffrement:

PARAMÈTRES

Réseau

Nom d'hôte:
Port:

IP de connexion et le port
(3389 = RDP)

Authentification

Identifiant:
Mot de passe:
Nom de domaine:

Identifiant de connexion
SSH de l'équipement

Infrastructure Windows

+  SRV-AD01

+  SRV-AD02

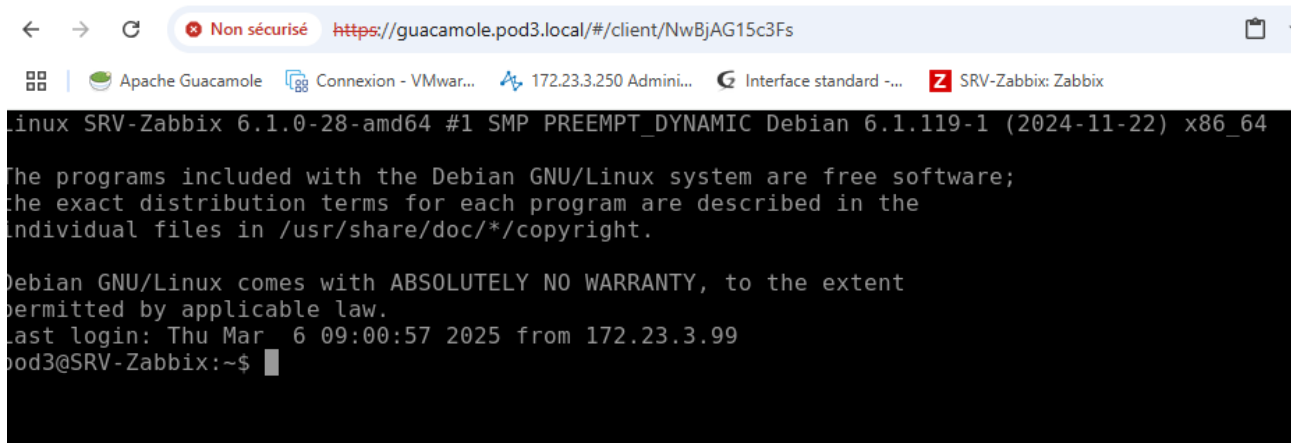
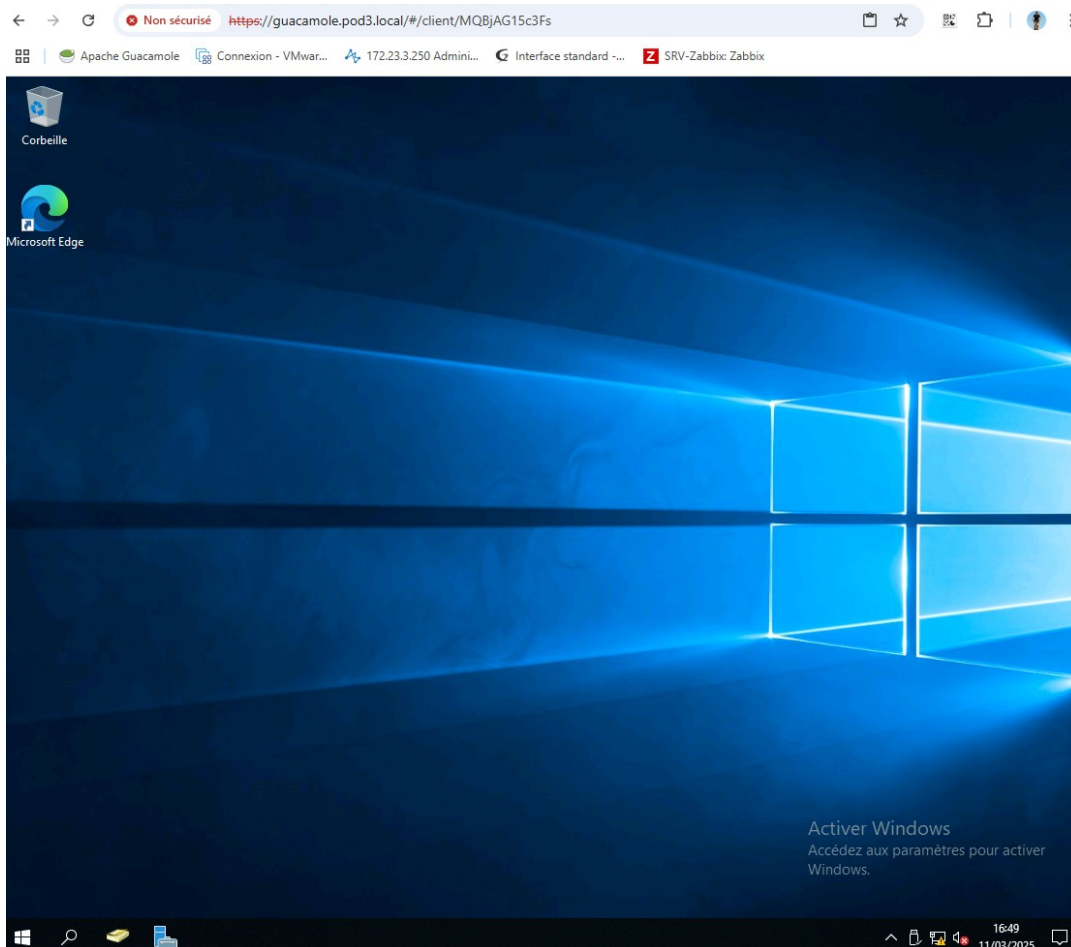
Serveurs de Supervision & Gestion

+ > SRV-GLPI-RSYSLOG-NTP

+ > SRV-GUACAMOLE

+ > SRV-ZABBIX

Mes équipements réseau sont
maintenant tous administrable



Si nous retournons sur la page d'accueil il est désormais possible de se connecter a mes serveurs en RDP et SSH.

3. Intégration avec Active Directory :

- Lier le système de gestion des utilisateurs du bastion à Active Directory pour simplifier l'administration et garantir une gestion sécurisée des comptes.

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

Requêtes enregistrées

pod3.local

- AuditME
- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Keys
- LostAndFound
- Managed Service Accounts
- Program Data
- System
- TiersLieux**
 - Bureau
 - Compta
 - IT**
- Users
- NTDS Quotas
- TPM Devices

Nom

- GG_IT
- Jean PEUPLUS

Utilisateur IT administrateur sur guacamole

OU lier a guacamole

Identifiant ▾	Organisation	Nom	Dernier actif
GG_bureau			
GG_compta_tiers_lieux			
GG_IT			
JEANP			11-03-2025 14:13:33
LUCASF			
MELANIEZ			

Utilisateur de l'AD sur guacamole

Nom Groupe ▾
GG_bureau
GG_compta
GG_IT

Groupe de l'AD (OU : Tiers-Lieux) sur guacamole

Installation et configuration d'un service Rsyslog

Installer et configurer un service Rsyslog sur le serveur GLPI pour centraliser les logs des activités d'administration du réseau et des serveurs, y compris les accès via le bastion.

Installation du serveur Rsyslog :

Installer Rsyslog sur une distribution Debian

```
sudo apt -y install rsyslog
```

Le fichier de paramétrage se nomme **/etc/rsyslog.conf**.

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="10514")
```

Choix des journaux en commentant ou décommentant les lignes

```
auth,authpriv.* /var/log/auth.log
*.*,auth,authpriv.none -/var/log/syslog
#cron.* /var/log/cron.log
daemon.* -/var/log/daemon.log
kern.* -/var/log/kern.log
lpr.* -/var/log/lpr.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log
mail.info -/var/log/mail.info
mail.warn -/var/log/mail.warn
mail.err /var/log/mail.err
```

Les lignes suivantes permettent d'indiquer quels réseaux pourront accéder au serveur de logs (protocole UDP ou TCP)

```
AllowedSender UDP, 127.0.0.1, 192.168.1.0/24

# OU

AllowedSender TCP, 127.0.0.1, 192.168.1.0/24
```

Redémarrer le service Rsyslog

```
sudo systemctl restart rsyslog
```

Paramétrage du client

Installer Rsyslog sur une distribution Debian

```
sudo apt -y install rsyslog
```

Le fichier de paramétrage se nomme **/etc/rsyslog.conf**.

```
*. * @IP_SERVEUR:10514 (pour TCP)
*. * @IP_SERVEUR:514 (pour UDP)
```

Client Rsyslog maintenant visible sur le serveur :

```
root@SRV-GLPI:/var/log/syslogclients# ls
172.23.3.1-syslog.log    172.23.3.254-syslog.log  SRV-GLPI-syslog.log
172.23.3.250-syslog.log  172.23.3.2-syslog.log
172.23.3.252-syslog.log  172.23.3.99-syslog.log
```

Log du serveur Guacamole : Connexion au site web guacamole

```
root@SRV-GLPI:~# cd /var/log/syslogclients
root@SRV-GLPI:/var/log/syslogclients# tail -f 172.23.3.99-syslog.log
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: guacd[10150]: WARNING:#011No known host keys provided, host identity will not be verified.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: guacd[10150]: WARNING:#011No known host keys provided, host identity will not be verified.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: Unable to set the timezone: SSH server refused to set "TZ" variable.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: guacd[10150]: WARNING:#011Unable to set the timezone: SSH server refused to set "TZ" variable.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: Unable to set the timezone: SSH server refused to set "TZ" variable.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: guacd[10150]: WARNING:#011Unable to set the timezone: SSH server refused to set "TZ" variable.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: SSH connection successful.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: guacd[10150]: INFO:#011SSH connection successful.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: SSH connection successful.
2025-03-11T15:12:35+01:00 SRV-DEBIAN-GUACAMOLE guacd[10150]: guacd[10150]: INFO:#011SSH connection successful.
```

Installation et configuration d'un service NTP :

Déployer un service NTP sur l'infrastructure pour synchroniser les horodatages des logs avec un serveur NTP externe comme ntp.univ-tln.fr ou fr.pool.ntp.org.

Installation du serveur NTP :

Installer Chrony sur une distribution Debian

```
apt install chrony
```

Il faut démarrer et activer le service

```
systemctl enable --now chronyd
```

Le fichier de config est : /etc/chrony.conf

```
pool fr.pool.ntp.org iburst
pool ntp.univ-tln.fr iburst
```

Pour configurer Chrony en tant que serveur NTP

```
allow 172.23.3.0/24
deny all
logdir /var/log/chrony
```

Il faut relancer le service

```
systemctl restart chronyd
```

Afficher le statut NTP

```
chronyc tracking
```

```
root@SRV-GLPI:~# chronyc tracking
Reference ID    : 81FA23FB (y.ns.gin.ntt.net)
Stratum        : 3
Ref time (UTC) : Tue Mar 11 14:52:59 2025
System time    : 0.000459237 seconds fast of NTP time
Last offset    : +0.000304481 seconds
RMS offset     : 0.000228919 seconds
Frequency      : 7.530 ppm slow
Residual freq  : +0.002 ppm
Skew           : 0.109 ppm
Root delay     : 0.154714793 seconds
Root dispersion : 0.012706457 seconds
Update interval : 1037.2 seconds
Leap status    : Normal
```

Installation du client NTP :

Installer Chrony sur une distribution Debian

```
apt install chrony
```

Le fichier de config est : /etc/chrony.conf

```
server 172.23.3.245 iburst      #IP SERVEUR CHRONY
```

Il faut relancer le service

```
systemctl restart chronyd
```

Serveur Chrony dans la liste des sources (172.23.3.245)

```
root@SRV-DEBIAN-GUACAMOLE:~# chronyc sources -v

.- Source mode '^' = server, '=' = peer, '#' = local clock.
/ .- Source state '*' = current best, '+' = combined, '-' = not combined,
/      'x' = may be in error, '~' = too variable, '?' = unusable.
||
||      Reachability register (octal) -.          |      .- xxxx [ yyyy ] +/- zzzz
||      Log2(Polling interval) --.          |      |      xxxx = adjusted offset,
||      \              |          |      |      yyyy = measured offset,
||      \              |          |      |      zzzz = estimated error.
||
||
MS Name/IP address         Stratum Poll Reach LastRx Last sample
=====
^* neel.ch                  1 10    375   70m  -5774us[-5777us] +/- 18ms
^+ vps-f60b2d25.vps.ovh.net 2 10    377   48m  +1153us[+1153us] +/- 20ms
^+ 27.ip-51-68-44.eu        3 10    377   516  -387us[ -387us] +/- 17ms
^- main.arcanite.ch         3 10    377   418  -1485us[-1485us] +/- 53ms
^- 172.23.3.245             3 6     377    3   +929us[ +929us] +/- 90ms
```

Client connectés au serveur Chronyc

```
root@SRV-GLPI:~# chronyc clients
Hostname                NTP      Drop Int IntL Last      Cmd      Drop Int Last
=====
172.23.3.99             7600     0 6 - 21      0        0 - -
172.23.3.1              7168     0 6 - 8      0        0 - -
SN310_POD3.pod3.local   1562     0 10 - 55     0        0 - -
172.23.3.254            5674     0 6 - 19     0        0 - -
172.23.3.2              7169     0 6 - 1      0        0 - -
WIN-1LTB5B5JMTN.pod3.loc> 505     0 10 - 187   0        0 - -
172.23.3.101            506     0 10 - 575     0        0 - -
```

Comparatif entre Wallix Bastion et Apache Guacamole

L'administration des infrastructures IT nécessite souvent un accès sécurisé aux équipements et serveurs. Les bastions d'administration jouent un rôle clé dans la gestion et la sécurisation des accès. Ce document compare **Wallix Bastion** et **Apache Guacamole** sur plusieurs critères :

1. Présentation des solutions

- **Wallix Bastion** : Solution commerciale de **PAM (Privileged Access Management)**, Wallix Bastion offre un contrôle strict des accès aux systèmes critiques en assurant une traçabilité complète et une gestion fine des droits d'accès.
- **Apache Guacamole** : Solution open-source permettant un accès distant via **RDP, SSH et VNC** via un navigateur web, sans client à installer.

2. Sécurité et authentification

Critère	Wallix Bastion	Apache Guacamole
Authentification multi-facteurs (MFA)	Oui (Intégré)	Oui (via extensions)
Gestion des identités	Avancée (AD, LDAP, SAML, etc.)	Basique (LDAP, base interne)
Traçabilité des accès	Journaux détaillés, enregistrement des sessions	Logs de connexion (moins détaillés)
Chiffrement des connexions	Élevé (AES, TLS)	Dépend des protocoles utilisés (TLS pour HTTPS, SSH pour accès SSH)
Isolation des accès	Oui (Proxy d'accès)	Non (connexion directe)

3. Fonctionnalités et cas d'usage

Fonctionnalité	Wallix Bastion	Apache Guacamole
Accès sans client	Interface web	Interface web
Protocoles supportés	SSH, RDP, Telnet, VNC, HTTPS	RDP, SSH, VNC
Gestion des droits	Granulaire par utilisateur, rôle et ressource	Basique (groupes et utilisateurs)
Enregistrement des sessions	Oui	Non (à configurer avec d'autres outils)
Intégration avec AD / LDAP	Oui	Oui

4. Déploiement et administration

Critère	Wallix Bastion	Apache Guacamole
Mode de déploiement	Appliance, VM, Cloud	Serveur applicatif (Docker, Tomcat)
Facilité de mise en place	Déploiement guidé mais complexe	Simple, dépend des besoins
Maintenance	Support éditeur	Communauté open-source
Coût	Licence payante	Gratuit (open-source)

5. Adaptabilité aux besoins

- **Wallix Bastion** est adapté aux **grandes entreprises** ayant des exigences élevées en matière de conformité et de sécurité, nécessitant une gestion avancée des accès privilégiés.
- **Apache Guacamole** est idéal pour les **PME et Home Labs** recherchant une solution simple et rapide à mettre en place pour un accès distant sécurisé.

6. Conclusion

Le choix entre **Wallix Bastion** et **Apache Guacamole** dépend des besoins et du niveau de sécurité recherché :

- **Wallix Bastion** est une solution **professionnelle et complète** pour la gestion des accès sécurisés aux infrastructures critiques.
- **Apache Guacamole** est une alternative **souple et open-source** qui facilite l'accès distant sans nécessiter de client lourd.