Guacamole with partially Podman / CentOS 8

Das Guacamole Projekt ist eine **HTML5 Remote-Access Applikation**, die als zentrale Verwaltungskonsole entfernter Computer verwendet werden kann. Unterstützt werden derzeit die Protokolle **VNC**, **RDP**, **SSH** wie auch **Telnet**.

Hier, für eine Installation von Guacamole auf CentOS 7

Alternative zu guacamole: Installation von Glyptodon Enterprise (Webpage) oder https://www.os-js.org/

Installation von Guacamole 1.3.0

Die folgende Installation wurde für Red Hat / CentOS 8 geschrieben.

Vorbereitungen für Guacamole

Um einen funktionierenden Betrieb von Guacamole zu gewährleisten, werden zu Beginn erst einmal alle *von Guacamole benötigten Packete* installiert:

```
# dnf install epel-release -y
# dnf update -y
# dnf install @container-tools -y

# dnf install mariadb-server wget java-11-openjdk-devel -y
```

Direkt nach der Installation der Packete, wird als erstes die lokale MySQL Datenbank abgesichert.

Generieren eines neuen MaiaDB-Root Passwortes:

```
# openssl rand -base64 30 > /root/.mariadb-root-pw && cat /root/.mariadb-root-pw
```

```
Tb/qprITSryJDHEp29XHr7/IuxMxZhGke/LZXEEJ
```

```
# systemctl enable mariadb.service --now
```

```
# mysql_secure_installation
```

```
Enter current password for root (enter for none): Enter
Set root password? [Y/n]: Y
New password: ******************************
Re-enter new password: ******************************
Remove anonymous users? [Y/n]: Y
Disallow root login remotely? [Y/n]: Y
Remove test database and access to it? [Y/n]: Y
Reload privilege tables now? [Y/n]: Y

All done!
```

Zum Schluss der Vorbereitungen werden noch die Guacamole Kern-Komponenten heruntergeladen sowie der MySQL Connector zum herstellen der Guacamole Datenbankverbindung installiert.

```
# cd /tmp

# wget https://www.blackgate.org/guac/guacamole-auth-jdbc-1.3.0.tar.gz
# wget https://www.blackgate.org/guac/guacamole-auth-duo-1.3.0.tar.gz

##DOWNLOAD JUST ONE VERSION, HARDENED BY MICHAEL OR ORIGINAL VERSION:##
# wget https://www.blackgate.org/guac/guacamole-1.3.0.war
# wget https://www.blackgate.org/guac/guacamole-1.3.0_hardened.war

##MYSQL CONNECTOR
# dnf install
https://cdn.mysql.com//Downloads/Connector-J/mysql-connector-java-8.0.24-1.e
l8.noarch.rpm
```

Kompilieren und einrichten von Tomcat 9 für Guacamole

```
# useradd -m -U -d /opt/tomcat -s /bin/false tomcat

# VERSION=9.0.45
# wget
https://www-eu.apache.org/dist/tomcat/tomcat-9/v${VERSION}/bin/apache-tomcat
-${VERSION}.tar.gz -P /tmp

# tar -xf /tmp/apache-tomcat-${VERSION}.tar.gz -C /opt/tomcat/
# ln -s /opt/tomcat/apache-tomcat-${VERSION} /opt/tomcat/latest
# chown -R tomcat: /opt/tomcat
# sh -c 'chmod +x /opt/tomcat/latest/bin/*.sh'

# mkdir -p /etc/guacamole/extensions
```

```
# mkdir /etc/guacamole/lib
```

```
# vim /etc/systemd/system/tomcat.service
```

```
[Unit]
Description=Tomcat 9 servlet container
After=network.target

[Service]
Type=forking

User=tomcat
Group=tomcat

Environment="JAVA_HOME=/usr/lib/jvm/jre"
Environment="GUACAMOLE_HOME=/etc/guacamole"
Environment="JAVA_OPTS=-Djava.security.egd=file:///dev/urandom"

Environment="CATALINA_BASE=/opt/tomcat/latest"
Environment="CATALINA_HOME=/opt/tomcat/latest"
Environment="CATALINA_PID=/opt/tomcat/latest/temp/tomcat.pid"
Environment="CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC"

ExecStart=/opt/tomcat/latest/bin/startup.sh
ExecStop=/opt/tomcat/latest/bin/shutdown.sh

[Install]
WantedBy=multi-user.target
```

```
# systemctl daemon-reload

# systemctl enable tomcat --now
# systemctl status tomcat
```

```
# setsebool -P tomcat_can_network_connect_db on

# firewall-cmd --zone=public --add-port=8080/tcp --permanent
# firewall-cmd --reload
```

Einrichten und starten des Guacamole Protokoll Servers

```
# setsebool -P container_manage_cgroup on
```

```
# vim /etc/systemd/system/guacamole-guacd-container.service
```

```
```

```
[Unit]
Description=Guacamole guacd-Container
After=network.target

[Service]
Type=simple
TimeoutStartSec=60s

ExecStartPre=-/usr/bin/podman rm "guacamole-protocol-server"
ExecStart=/usr/bin/podman run --name guacamole-protocol-server --net=host
guacamole/guacd

ExecReload=-/usr/bin/podman stop "guacamole-protocol-server"
ExecReload=-/usr/bin/podman rm "guacamole-protocol-server"

ExecStop=-/usr/bin/podman stop "guacamole-protocol-server"
Restart=always
RestartSec=30

[Install]
WantedBy=multi-user.target
```

```
# systemctl daemon-reload

# systemctl start guacamole-guacd-container.service
# systemctl enable guacamole-guacd-container.service

# systemctl status guacamole-guacd-container.service
# netstat -tulpn
```

Einrichten der Guacamole Datenbank

In diesem Schritt wird mit dem **DB-root** Benutzer auf den **MySQL Server** verbunden und die Datenbank **Guacamole** erstellt und abgefüllt. Weiter wird aus Security Grünen einen eigenen Benutzer dazu erstellt, welcher ausschliesslich auf die Guacamole DB berechtigt wird. So wird verhindert, dass dieser Benutzer Veränderungen an der Server eigenen DB Struktur vornehmen kann.

```
# mysql -u root --password=$(cat /root/.mariadb-root-pw)
```

```
CREATE DATABASE guacamole_db1;
CREATE USER 'guacamole'@'localhost' IDENTIFIED BY
'v2gjMrY/2XmgJwhNE56scymqTiC337XkVKOHtYw9';
GRANT SELECT,INSERT,UPDATE,DELETE ON guacamole_db1.* TO
'guacamole'@'localhost';
FLUSH PRIVILEGES;
quit
```

Hier wird das Guacamole ***DB Authentifizierungs-Tool*** **jdbc** entpackt, in die Installation integriert und anschliessend die Datenbank abgefüllt. Zum Schluss wird dann noch der offizielle MySQL Connector driver ebenfalls mit einbezogen.

```
# tar -xvf guacamole-auth-jdbc-1.3.0.tar.gz
# cd guacamole-auth-jdbc-1.3.0/mysql/

# cp guacamole-auth-jdbc-mysql-1.3.0.jar /etc/guacamole/extensions/
# cat schema/*.sql | mysql -u root --password=$(cat /root/.mariadb-root-pw)
guacamole_db1
# cd ../..

# ln -s /usr/share/java/mysql-connector-java.jar /etc/guacamole/lib/
```

Einrichten des Web-Clients für Tomcat

Nun kann der Web-Client *(das User Interface)* von Guacamole auf dem System eingerichtet werden. Hierzu wird das selbst-entpackende *.war File welches den Client beinhaltet ins Webverzeichnis von **Tomcat 9** verlinkt.

```
# cp guacamole-1.3.0.war /etc/guacamole/guacamole.war
# ln -s /etc/guacamole/guacamole.war /opt/tomcat/latest/webapps/
# mkdir /opt/tomcat/latest/.guacamole

# touch /etc/guacamole/guacamole.properties
# ln -s /etc/guacamole/guacamole.properties /opt/tomcat/latest/.guacamole/
```

Befüllen der Haupt-Konfigurationsdatei von Guacamole. Alle Änderungen die hier hineingeschrieben werden, überschreiben lediglich den default Wert von Guacamole.

```
# vim /etc/guacamole/guacamole.properties
```

```
# MySQL properties
mysql-hostname: localhost
mysql-port: 3306
mysql-database: guacamole_db1
mysql-username: guacamole
mysql-password: v2gjMrY/2XmgJwhNE56scymqTiC337XkVKOHtYw9
```

Installation abschliessen

Folgende SELinux Boolean muss für die Kommunikation zwischen Guacamole und der Datenbank aktiviert werden:

```
# setsebool -P tomcat_can_network_connect_db on
```

Zum Schluss, wird noch den Autostart der Services aktiviert und das System anschliessend neugestartet!

```
# systemctl enable tomcat.service --now (oder restart!)
# firewall-cmd --zone=public --add-port=8080/tcp --permanent
# firewall-cmd --reload

# systemctl reboot
```

Der Server sollte nun unter folgendem Link erreichbar sein: http://your_IP:8080/guacamole

Für weitere Details, Hilfestellungen: Offizielles Guacamole Manual

***ACHTUNG:* Das Standard Passwort von Guacamole muss unbedingt noch geändert werden!**

- **Username**: guacadmin
- **Passwort**: guacadmin

Einrichten einer Two Level Authentication

- Wie wird die Two Level Authentication aktiviert?

Upgrade auf neue Version von Guacamole

Um auf die neue Version von Guacamole zu upgraden, kann wie oben bei der Neuinstallation vorgegangen werden. Es wird jedoch empfohlen, das Upgrade wie unten in den einzelnen Schritten beschrieben durchzuführen; Um auch alle gespeicherten Verbindungen und User zu erhalten, braucht es nämlich trotzdem die einte oder andere kleine Abänderung.

WICHTIG: Ein grosser unterschied besteht darin, dass der gesammte DB Create Part übersprungen wird und anstelle von diesem Abschnittes hier die Schritte aus dem Punkt **MySQL-DB Upgrade** durchgeführt werden.

Vorbereitung und Durchführung des Upgrades

Vor dem Beginn werden die zwei **Haupt-Services**, welche Guacamole auszeichnen **gestoppt** und das System aktualisiert.

```
# systemctl stop tomcat.service
# systemctl stop guacamole-guacd-container.service
```

```
# yum update -y
```

Anschliessend, werden die *alten Dateien / Verzeichnisse gelöscht,* welche nicht mehr von der neuen Guacamole Version unterstützt, gebraucht werden:

```
# rm -rf /etc/guacamole/extensions/*
# rm -f /opt/tomcat/latest/webapps/guacamole.war
# rm -rf /opt/tomcat/latest/webapps/guacamole
# rm -f /etc/guacamole/guacamole.war
```

Zum durchführen des Upgrades, wird folgendermassen vorgegangen:

1. **Herunterladen der neuen Versionen** (**`Server`**, **`WebClient`**, **`jdbc`** und *falls gebraucht* **duo**)

```
# cd /tmp
# wget https://www.blackgate.org/guac/guacamole-auth-jdbc-1.2.0.tar.gz

##DOWNLOAD JUST ONE VERSION, HARDENED BY MICHAEL OR ORIGINAL VERSION:##
# wget https://www.blackgate.org/guac/guacamole-1.2.0.war
# wget https://www.blackgate.org/guac/guacamole-1.2.0_hardened.war

# wget https://www.blackgate.org/guac/guacamole-auth-duo-1.2.0.tar.gz
```

2. **Entpacken** der Sourcecodes der Extensionßs

```
# tar -xvf guacamole-auth-jdbc-1.2.0.tar.gz
# tar -xvf guacamole-auth-duo-1.2.0.tar.gz
```

3. Aktualisieren des Guacamole Protokoll Servers

```
# podman pull guacamole/guacd:latest
```

4. Neue Versionen der Erweiterungen, aus den Source Ordnern in /ect/guacamole/extension kopieren! (z.B. auth-jdbc & auth-duo)

```
# cp guacamole-auth-jdbc-1.2.0/mysql/guacamole-auth-jdbc-
mysql-1.2.0.jar /etc/guacamole/extensions/

# cp guacamole-auth-duo-1.2.0/guacamole-auth-duo-1.2.0.jar
/etc/guacamole/extensions/
```

5. **Neuer Web-Client** nach **/etc/guacamole/** kopieren und Symlinks erneuern. **ACHTUNG: Nur eine Version kopieren!**

```
##COPY JUST ONE VERSION, SAME YOU DESIDED ABOVE!: (HARDENED BY MICHAEL
OR ORIGINAL VERSION)##

# cp guacamole-1.2.0_hardened.war /etc/guacamole/guacamole.war
# cp guacamole-1.2.0.war /etc/guacamole/guacamole.war

# ln -s /etc/guacamole/guacamole.war /opt/tomcat/latest/webapps/
```

6. Falls nötig, **DB-Upgrade durchführen**. Ansonsten Dienste (wie ganz unten beschrieben) wieder starten.

MySQL-DB Upgrade (Für 1.2.0 nicht nötig)

Um nun (falls Nötig → *wenn Files vorhanden*) das MySQL Upgrade durchzuführen, muss wie folgt vorgehen werden:

```
# cd guacamole-auth-jdbc-1.2.0/mysql/schema/upgrade

# cat upgrade-pre-1.2.0.sql | mysql -u root --password=$(cat /root/.mariadb-root-pw) $(awk -v FS="mysql-database: " 'NF>1{print $2}' /etc/guacamole/guacamole.properties)
```

ACHTUNG: Wenn zwei db Aktualisierungen notwendig sind; z.B. beim Upgrade von Guacamole 0.9.15 auf 1.1.x, muss die DB IMMER zuerst auf die erste vorherige Version in dem Fall 1.0.0 upgedated werden, noch bevor, schlussendlich auf die neuste Release Version 1.1.x aktualisiert werden kann!

Upgrade Abschliessen

Nach dem erfolgreichen Upgrade, kann der Guacamole Server (nach einem daemon-reload) sowie der Tomcat Webserver anschliessend wieder gestartet werden!

```
# systemctl stop guacamole-guacd-container.service
# systemctl start tomcat.service
```

Problemlösung

White Screen auf Loginpage von Guacamole

Error aus Logfile: `/opt/tomcat/latest/logs/catalina.out`

```
09:45:51.118 [http-nio-8080-exec-11] WARN
o.a.g.e.AuthenticationProviderFacade - The "mysql" authentication provider
has encountered an internal error which will halt the authentication
process. If this is unexpected or you are the developer of this
authentication provider, you may wish to enable debug-level logging. If this
is expected and you wish to ignore such failures in the future, please set
"skip-if-unavailable: mysql" within your guacamole.properties.
09:45:51.118 [http-nio-8080-exec-11] ERROR o.a.g.rest.RESTExceptionMapper -
Unexpected internal error:
### Error querying database.  Cause: java.sql.SQLException: The server time
zone value 'CEST' is unrecognized or represents more than one time zone. You
must configure either the server or JDBC driver (via the 'serverTimezone'
configuration property) to use a more specifc time zone value if you want to
```

```
utilize time zone support.
### The error may exist in
org/apache/guacamole/auth/jdbc/user/UserMapper.xml
### The error may involve
org.apache.guacamole.auth.jdbc.user.UserMapper.selectOne
### The error occurred while executing a query
### Cause: java.sql.SQLException: The server time zone value 'CEST' is
unrecognized or represents more than one time zone. You must configure
either the server or JDBC driver (via the 'serverTimezone' configuration
property) to use a more specifc time zone value if you want to utilize time
zone support.
```

Lösung: Timezone/Zeitzone des MariaDB/MySQL Servers ändern

1. Die Standardtabellen für die Zeitzonen des Systems laden:

   ```
   # mysql_tzinfo_to_sql /usr/share/zoneinfo | mysql -u root --
   password=$(cat /root/.mariadb-root-pw) mysql
   ```

2. Anpassen der Zone im Config-file:

   ```
   vim /etc/my.cnf.d/mariadb-server.cnf
   ```

   ```
   # Settings user and group are ignored when systemd is used.
   # If you need to run mysqld under a different user or group,
   # customize your systemd unit file for mysqld/mariadb according to the
   # instructions in http://fedoraproject.org/wiki/Systemd
   [mysqld]
   max_allowed_packet=64M
   datadir=/var/lib/mysql
   socket=/var/lib/mysql/mysql.sock
   log-error=/var/log/mariadb/mariadb.log
   pid-file=/run/mariadb/mariadb.pid

   # Timezone
   default_time_zone=Europe/Zurich
   ```

3. Restart Service:

   ```
   systemctl restart mysql
   ```

Last update: **2021/05/03 15:19**