Geneious Server Database 2023.0 Installation Manual

Biomatters Ltd

February 3, 2023

Contents

1 Server Setup **7**

1.1 Prerequisites 7

1.2 Document Scope 8

1.3 Red Hat Enterprise Linux or CentOS Server Installation 8

2 Installing Geneious Server Database **11**

2.1 Preparation 11

2.2 Installing Geneious Server Database 12

3 Configure the Server **15**

3.1 Start/stop/restart Geneious Server Database via Tomcat 15

3.2 Configure the server's local database 15

3.3 User configuration 18

4 Geneious Server Database settings **19**

4.1 Activating the license 19

4.2 Connecting to Geneious Server Database from Geneious Prime 19

4.3 Creating the First Database Admin Geneious Server Database 19

5 Upgrading from Geneious Server Database 6.0 or later **21**

5.1 Preparation 21

5.2 Upgrade the package 22

6 LDAP with TLS or SSL configuration **23**

7 TLS/SSL Server Authentication **25**

7.1 Using TLS/SSL secure communication 25

8 Backing up Geneious Server Database **29**

Chapter 1

Server Setup

IMPORTANT: PLEASE READ!

Upgrading to Geneious Server Database 2022.0.1 and Beyond

The upgrade to Geneious Server Database 2022 included upgrading the server to run on Java 11 instead of Java 8. This change had the following significant effects:

- Geneious Server Database is no longer supported on CentOS/RedHat 6.
- The included Tomcat server was upgraded from Tomcat 7 to Tomcat 9.
- The installation scripts were streamlined into a single `install.sh`.

As a result, there are some changes to the commands included in this manual, and a careful read is recommended before execution.

It is **highly recommended** that you backup your existing server and/or database before commencing the upgrade. How to do that is beyond the scope of this document - but note that you will need to backup both the server and the database if you have large-file support enabled.

1.1 Prerequisites

Your hardware must be a 64 bit Intel/AMD (x86_64) system meeting the requirements to run the selected operating system. The shared database provided by Geneious Server Database may be configured to use an existing external SQL database server or the Postgres server that

is installed on the Geneious Server Database machine. Either way, there must be enough disk space on the Geneious Server Database machine to accommodate large datasets that the shared database will store on the file system instead of directly in the SQL database. Due to the complexities of potential library conflicts we require that Geneious Server Database is installed on a dedicated machine (which could be virtual) with no pre-existing software installed. The operating system should be RHEL Server or CentOS version 7.

It is assumed that Geneious Server Database will be installed by someone who has the expertise for basic administration of a RHEL/CentOS system, including working on the command line and adding user accounts.

1.2 Document Scope

This document covers installing Geneious Server Database with additional sections that describe configuring Geneious Server Database to use network authentication (with LDAP and Kerberos examples).

The document **does not cover** the following:

- Installing Red Hat EL or CentOS operating systems, other than configuration requirements
- Network configuration steps required to obtain a static IP address for your machine
- Configuration steps required to enable network authentication for linux login for your machine

1.3 Red Hat Enterprise Linux or CentOS Server Installation

Geneious Server Database should be installed on a generic RHEL/CentOS **Server** system **without virtualization options**.

- **Configure the disk partition layout** so that there is sufficient space for large data sets that will be sent to the server and stored on it. The default layout is often not suitable. Data sets that are uploaded are temporarily stored in files under directory `/var/cache`. The shared database stores files under `HOSTNAME` home directory. Do not accept the default disk partitioning of the OS install which often supplies minimal space to the `/` directory. One simple configuration is to create a `/boot` partition with 1GB, swap partition of suitable size, and the rest in the `/` root partition containing enough space for multiple large data sets even if there is another large network share allocated for the HOSTNAME home directory to hold the shared database files.

- **Configuration of the firewall and SELinux** is outside the scope of this document. The default configuration for Tomcat uses port `8080` for HTTP and `8443` for HTTPS. It may be simplest to disable the firewall and SELinux before installing Geneious Server, then enable and configure them after everything else is working, or leave them disabled to rely on the security of the local network.
- **If using Red Hat EL** rather than CentOS, add the Optional channel as instructed at `https://access.redhat.com/solutions/392003` (Red Hat subscription login is required to access the link).
- **Network configuration**: The Geneious Server Database machine should have a static IP address and its hostname on DNS. The command line `hostname -i` should show at least one IP address other than `127.0.0.1`
- **Run yum -y upgrade** to ensure OS is up to date before installing Geneious Server Database.
- As a final step, run through this check list and tick each item if you're sure they are done:

Firewall disabled or properly configured	
SELinux disabled or properly configured	
All updates applied	
Host registered on network	
One big / partition big enough to handle your data	
RHEL (not applicable for CentOS) – Optional channel sub	

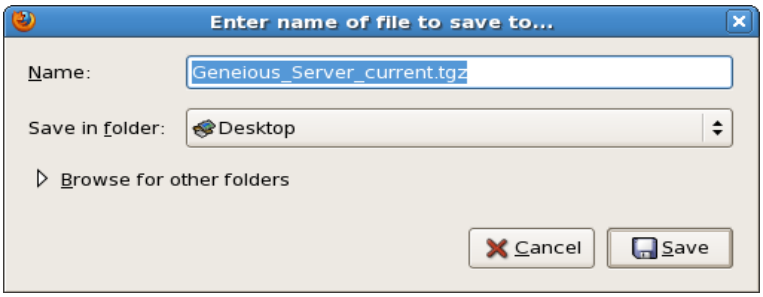
- You're now ready to install Geneious Server Database itself.

Chapter 2

Installing Geneious Server Database

2.1 Preparation

- This manual assumes you're logged in as `root` because Geneious Server Database needs to be installed by the `root` user. You may use `sudo su -` to get full `root` access.
- Using the URL provided, download the Geneious Server Database tarball to a convenient location such as `/root/Desktop`. The file shown below as `Geneious_Server_current.tar.gz` will have the current version number instead of `current` in the file name but will unpack into a directory named `Geneious_Server_current`.



- Once the file is downloaded, open the terminal (`Applications` → `System Tools` → `Terminal`) and type the following:

  ```
  cd /root/Desktop
  ```

- You can now unpack the file using the following command:

  ```
  tar xzvf Geneious_Server_current.tar.gz
  ```

- This will create a directory. Type the following to go into it:

  ```
  cd Geneious_Server_current
  ```

- For a quick overview of installation options, you can execute:

  ```
  sh ./install.sh --help
  ```

2.2 Installing Geneious Server Database

RHEL only - not CentOS – if you still haven't been to the RHN website and added the Optional channel subscription you must do that now because the following script requires that subscription.

For the most basic installation of Geneious Server Database , use:

```
sh ./install.sh --database-only --install-server
```

This will perform a few automated tasks, as well as pausing to ask for extra information as required. It is possible to automate the installation by providing a few extra options:

- For a quiet install (minimal interaction):

  ```
  --quiet
  ```

- To specify the database password:

  ```
  --password PASSWORD
  ```

  Note that for a pre-existing installation/upgrade, the password can be found in `/home/<hostname>/.geneiousServerConfig/database.properties`

- Automatically agree with the license:

  ```
  --agree
  ```

- Configure proxy settings:

  ```
  --setup-proxy http://USERNAME:PASSWORD@PROXY:PORT
  ```

  Note that this is the full string, you may only need to provide relevant parts.

The installation script verifies that compatible options are selected - for example, you cannot specify `--quiet` without `--password`. It is also possible to break the automation up into its constituent parts, if you wish. The main options are:

- Prerequisites only (including the backing database):

  ```
  sh ./install.sh --database-only --install-prerequisites
  ```

- The host server:

```
sh ./install.sh --database-only --install-server
```

Further partitioning is possible - read `install.sh` if interested.

Chapter 3

Configure the Server

3.1 Start/stop/restart Geneious Server Database via Tomcat

Geneious Server Database runs as a Java application under the Apache Tomcat application server. To start, stop or restart the Geneious Server Database application, run the appropriate command from the terminal command line, specifying either `start`, `stop`, or `restart`. The command must be run as `root` or using `sudo`.

```
systemctl start tomcat
```

The error and debugging logs for Geneious Server Database are written to the Tomcat logs in the following locations:

- `/var/log/tomcat/catalina.out` - The general Tomcat logs.
- `/var/log/geneiousserver/*` - Geneious Server Database specific logs.
- `/var/log/geneiousserverinstall.log` - The installation log.

3.2 Configure the server's local database

This section describes configuration changes that can be made in files that are located in the `/home/<hostname>/.geneiousServerConfig` directory. For changes to these files to take effect you will need to restart Tomcat.

- **Network login only** – In order to use network authentication with Geneious Server Database you can use any authentication system for which there is a Java JAAS login module. We will give examples using kerberos and LDAP.

  To use Kerberos you need to perform two steps, the first of which is documented below: Open the file `geneious_auth.conf` in the `/home/<hostname>/.geneiousServerConfig` directory. Find the following section:

  ```
  Geneious {
    com.biomatters.plugins.serverDatabase.webservice.GeneiousDatabaseLogin
  Module sufficient;
  };
  ```

  Change this to the following:

  ```
  Geneious {
    com.sun.security.auth.module.Krb5LoginModule sufficient;
  };
  ```

- **Network login only** – To use LDAP the JAAS Login Module requires the LDAP configuration to be consistent with linux login authentication and the following two additional conditions:
  - The LDAP server must be configured to use plain text or `ldaps` protocol, not `STARTTLS`
  - The user objects containing the `uid` and `userPassword` attributes must be stored in a single table, i.e. no nested directory structures are permitted for those user objects

- **Network login only** – If your LDAP configuration meets the above conditions you may configure Geneious Server Database to authenticate against LDAP.

  To use LDAP authentication open the file `geneious_auth.conf` in the `/home/<hostname>/.geneiousServerConfig` directory. Find the following section:

```
Geneious {
  com.biomatters.plugins.serverDatabase.webservice.GeneiousDatabaseLogin
Module sufficient;
};
```

  Change this to the following (substituting your LDAP urls for `yourLdapValue` and the DN for your user objects for `yourDNforUser`):

```
Geneious {
    com.sun.security.auth.module.LdapLoginModule sufficient
userProvider="yourLdapValue"
authIdentity="yourDNforUser";
};
```

  For example biomatters' entry would look like:

```
Geneious {
  com.sun.security.auth.module.LdapLoginModule sufficient
userProvider="ldaps://ldap.biomatters.com:636/ou=people,dc=biomatters,dc=com"
authIdentity="uid={USERNAME},ou=people,dc=biomatters,dc=com";
};
```

  For more information on LDAP with SSL, go to Chapter 6.

- If after installation you find Geneious Server Database running slowly, you may also want to tune your `postgreSQL` server to take better advantage of the server's hardware. Here are a few links on the topic:
  http://linuxfinances.info/info/quickstart.html
  http://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server

- Restart Tomcat to enable the new configuration:

```
systemctl restart tomcat
```

- To enable SSL support in Tomcat, first get it working without SSL and then refer to Chapter 7.

3.3 User configuration

- Every user who will connect to Geneious Server Database must have a linux login account under their user name. Either configure the Geneious Server Database machine for network login or create local linux accounts.

Chapter 4

Geneious Server Database settings

4.1 Activating the license

- Go to `http://<hostname>:8080/GeneiousServerAdmin` (replacing `<hostname>` with the real hostname)
- Login to the admin console using username **admin** and password **g3n3i0us**
- Change the admin password from the default by clicking on `Administration` and entering the old password and new password
- Click on `Server Licensing` and enter the Licensee Name and License Key you were sent; click `activate license`

4.2 Connecting to Geneious Server Database from Geneious Prime

- Click on Shared Databases in the Sources panel in Geneious Prime
- Click **New Database Connection**.
- Select **Geneious Server Database** tab
- Enter the connection details to connect to the Geneious Server Database.

4.3 Creating the First Database Admin Geneious Server Database

If there are no database admins in Geneious Server Database any user can set themselves as a database admin with the option **Make the current user a Database Admin** in Geneious Prime.

This option is only available when there are no database admins. As database admins can access all folders in the database, it is important that the first database admin is set by the appropriate person as soon as possible.

- To create the first database admin user, start Geneious, connect to your Geneious Server Database from within Geneious, right click on the root folder of the database and select **Make the current user a Database Admin**.
- A database admin can make additional users database admins by setting the user's role in the group Everybody to Admin.
- By default, all folders in the database will be added to a user's Private Group, meaning that documents will not be shared, and all users may create groups. Right click on the root folder and select **Administration** to see the menu items for changing from the default settings.

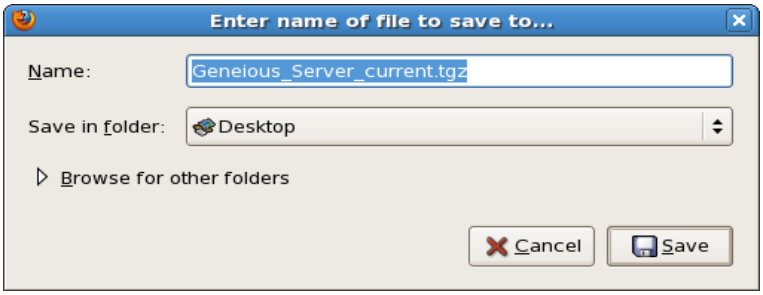
More information on the administration of Geneious Server Databases from Geneious Prime can be found in Geneious Prime user manual

Chapter 5

Upgrading from Geneious Server Database 6.0 or later

5.1 Preparation

- This manual assumes you're logged in as `root` because Geneious Server needs to be installed by the `root` user. You may use `sudo su -` to get full `root` access.
- Using the URL provided, download the Geneious Server Database tarball to a convenient location such as `/root/Desktop`.
  The file shown below as `Geneious_Server_current.tar.gz` will have the current version number instead of `current` in the file name but will unpack into a directory named `Geneious_Server_current`.



- Once the file is downloaded, open the terminal (`Applications` → `System Tools` → `Terminal`) and type the following:

  ```
  cd /root/Desktop
  ```

- There may already be a `Geneious_Server_current` directory on your desktop from your previous install. You should rename this or delete it prior to unpacking the new version.

- You can now unpack the file using the following command:

  ```
  tar xzvf Geneious_Server_current.tar.gz
  ```

- This will create a directory. Type the following to go into it:

  ```
  cd Geneious_Server_current
  ```

5.2 Upgrade the package

- Upgrade Geneious Server Database by running the following installation script:

  ```
  sh ./install.sh --database-only --install-prerequisites --install-server
  ```

- Once your server has updated and Tomcat has restarted, you should get your users to upgrade to the new version of Geneious included in the tar ball you downloaded. These can be found in the `Geneious_Server_current/geneious_installers` directory.

Chapter 6

LDAP with TLS or SSL configuration

The are two ways that an LDAP server can be configured to use TLS or SSL. One way wraps all communication with the LDAP server in a TLS connection. If your server administrator has configured it that way, the URL to reference the server must start with `ldaps://`, and typically will specify port `636`.

The other configuration of an LDAP server with TLS or SSL does not enable TLS/SSL for the initial communication, starting it when it is time to send a password. This mode requires you to specify the URL as starting with `ldap://`, usually using port `389`. Your configuration file must contain the line `UseSSL=true`.

With either mode of SSL on the LDAP server, the operating system on the Geneious Server Database machine must be configured to accept the server's public key certificate. If the certificate was obtained from a recognized commercial Certificate Authority, no extra configuration is likely to be required on the Geneious Server Database machine. Otherwise, refer to the `update-ca-trust` command for installing a public certificate as a trusted CA root.

Chapter 7

TLS/SSL Server Authentication

7.1 Using TLS/SSL secure communication

Geneious Server Database uses Java's JAAS modules for user authentication with, for example, an LDAP or Kerberos server. Geneious does not itself secure the connection between it and Geneious Server Database. If you cannot trust the physical security of a local network connection or use a VPN, then security between the Geneious client and Geneious Server Database computers can be accomplished by configuring them to use SSL.

The two general steps required for SSL are

- Install SSL certificates in Tomcat on the Geneious Server Database computer
- Specify use of SSL in the login dialog in the Geneious client

How to obtain SSL certificates is outside the scope of this document. Your systems administrator or IT department should know how. A self-signed certificate can be used, but will require the Geneious user to disable verification of the certificate, a slight reduction in security. Best practice will be to obtain a certificate from a Certificate Authority that is recognized by the major operating systems.

In the following instructions the private and public certificate files will be referred to as `server.crt` and `server.pem`, but the names are arbitrary.

The next commands must be done as root, either by being logged in root or using `sudo` in the commands:

copy `server.crt` and `server.pem` to a new directory named `/opt/tomcat/latest/ssl/`

```
mkdir -p /opt/tomcat/latest/ssl
```

```
cp server.crt server.pem /opt/tomcat/latest/ssl/
```

Edit the file `/opt/tomcat/latest/conf/server.xml`

The default version of the file after Tomcat has been installed contains a number of sections that begin with `<Connector` and end with a corresponding `/>`.

Some of them are preceded with `<!--` and followed by `-->`.

Those sections are commented out so as to have no effect. They are there as examples which you can modify to your needs and enable by removing the `<!--` and `-->` that surround them.

There will be one connector definition that is not commented out, specifying a non-SSL connector on port `8080`. If you want to require all connections between Geneious and Geneious Server Database to be over encrypted SSL, restrict the port `8080` connector specification to work with localhost only (required for use by the admin console) by inserting `address="127.0.0.1"` between `Connector` and `port="8080"`. For example:

```
<Connector address="127.0.0.1" port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

To enable SSL using the `server.crt` and `server.pem` files that you created, insert the following connector definition after one of the existing ones in `server.xml`.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector port="8443" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
SSLCertificateFile="/opt/tomcat/latest/ssl/server.crt"
SSLCertificateKeyFile="/opt/tomcat/latest/ssl/server.pem"
SSLProtocol="all"/>
```

You can use a different port other than the standard Tomcat default of `8443`, but the Geneious client users must enter the same port number in their login dialog.

Save the edited `/opt/tomcat/latest/conf/server.xml` file and restart Tomcat:

```
systemctl restart tomcat
```

Check the log files in `/var/log/tomcat/` to see if there were any errors starting up Tomcat.

To use Geneious to login to a Geneious Server Database over SSL, in the login dialog in Geneious, specify as the host name the exact name that was specified in the certificate when it was created,

select the Use SSL checkbox, and set the port number correctly (default `8443`). If the certificate is self-signed, unselect the Require valid SSL cert path checkbox.

Chapter 8

Backing up Geneious Server Database

There are two parts to backing up Geneious Server Database:

- Backup the sql database using the standard backup procedure for your choice of SQL database. The default SQL database name is `geneiousserver` but the actual name used is specified in the `database.properties` configuration file found in `/home/<hostname>/.geneiousServerConfig/` where `<hostname>` is the real hostname.
- Backup the following directory on the Geneious Server: `/home/<hostname>/.geneiousServerNN.Ndata` where `NN.N` is the major and minor version number of Geneious Server, e.g.,`/home/<hostname>/.geneiousServer2023.0data`. This directory contains the contents of Geneious documents that are too large to store completely in the SQL database.