Zabbix 7.4 Installation on Debian 12 (Vanilla Setup)

1. Configure Locales

- Set up `en_US.UTF-8` and any additional locales for multi-language support in Zabbix.

`dpkg-reconfigure locales`

2. Install MariaDB (Zabbix Database Backend)

- Install the default MariaDB server package:

`apt install default-mysql-server`

3. Secure MariaDB Setup

- Run as `root` to improve database security:

`mariadb-secure-installation`

- Recommended to carefully read each prompt and avoid default answers where security is impacted.

4. Add Zabbix Repository

- Download and install official Zabbix APT package:

`wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb`

```
`dpkg -i zabbix-release_latest_7.4+debian12_all.deb`
`apt update`
```

5. Install Zabbix Components

- Install server, frontend (PHP), Apache configuration, SQL scripts, and agent:

`apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent`

6. Create Zabbix Database and Import Schema

- Connect to MariaDB and create database/user:

`mysql -uroot -p`

```
  ```
  create database zabbix character set utf8mb4 collate utf8mb4_bin;
  create user zabbix@localhost identified by 'password';
  grant all privileges on zabbix.* to zabbix@localhost;
  set global log_bin_trust_function_creators = 1;
  quit;
  ```
* Import initial schema:
  `zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix`
* Disable trust function flag after import:
  `mysql -uroot -p`
  ```
  set global log_bin_trust_function_creators = 0;
  quit;
  ```
```

7. Configure Zabbix Server

- Set the database password in `/etc/zabbix/zabbix_server.conf`:

`DBPassword=password`

8. Start and Enable Zabbix Services

- Start and enable server, agent, and Apache:

`systemctl restart zabbix-server zabbix-agent apache2`

```
  `systemctl enable zabbix-server zabbix-agent apache2`
```

9. Access Zabbix Web UI

- Open Zabbix frontend in a browser:

`http://your-server-ip/zabbix`

SSL Setup

1. Generate Self-Signed Certificate

- Create directory:

`sudo mkdir -p /etc/ssl/zabbix`

- Generate cert:

`sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/zabbix/zabbix.key -out /etc/ssl/zabbix/zabbix.crt -subj “/C=CA/ST=Quebec/L=Boisbriand/O=ZabbixLAN/CN=zabbix.local”`

2. Configure Apache for SSL

- Enable SSL module and default SSL site:

`sudo a2enmod ssl`

```
  `sudo a2ensite default-ssl`
* Edit SSL virtual host:
  `sudo nano /etc/apache2/sites-available/default-ssl.conf`
  Add or update:
  ```
  SSLEngine on
  SSLCertificateFile /etc/ssl/zabbix/zabbix.crt
  SSLCertificateKeyFile /etc/ssl/zabbix/zabbix.key
  DocumentRoot /usr/share/zabbix
  ```
```

3. Force HTTP to Redirect to HTTPS

- Edit HTTP virtual host:

`sudo nano /etc/apache2/sites-available/000-default.conf`

```
  Inside `<VirtualHost *:80>` add:
  ```
  Redirect "/" "https://your-server-ip/zabbix"
  ```
  Replace ''your-server-ip'' with your actual server IP or hostname.
```

4. Apply Changes

- Restart Apache:

`sudo systemctl restart apache2`

5. Access the Frontend

- Use:

`https://your-server-ip/zabbix`

```
Accept browser warning for the self-signed cert.
```

From:
https://dulib.re/wiki/ - **Le Goût du Libre**

Permanent link:
https://dulib.re/wiki/doku.php/zabbix_7.4_sur_debian_12_avec_ssl?rev=1751926986

Last update: **2025/07/07 15:23**