Zabbix 7.4 Installation on Debian 12 with SSL

These instructions make the assumption :

- You have a Debian 12 “vanilla” setup, only SSH server and no desktop environment
- No root account, all commands are run as `sudo` - this usually starts with `sudo -s` after login.
- Zabbix server is NOT Internet-facing, and runs in a LAN, isolated environment

For an Internet-facing install, consider setting up an SSL certificate with certbot, and configuring two-factor authentication (2FA).

Full official documentation is available at Zabbix.com.

Credits

- Fabian Rodríguez, François Baillargeon (review) - Le Goût du Libre
- Sources:
  - Official Zabbix installation instructions
  - Debian Zabbix insstallation instructions

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
```

Answer 'n' to the first two questions, assuming you have no `root` account setup.

4. Add Zabbix Repository

Download and install official Zabbix APT package - whis will add Zabbix repositories to your servers', and update the repositories database:

```
wget
https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/z
abbix-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
```

(press enter as your `root` user is not defined)

Important : The second statement should be changed to use a password of your choice.

```
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` (replace with the password set in step 6 above):

```
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 to test the installation has completed well (don't finish it just yet, SSL setup is next!):

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

SSL Setup

Using SSL in a LAN environment helps protect sensitive data like login credentials from being intercepted or tampered with—even on internal networks where threats can arise from compromised devices or curious users.

While self-signed certificates aren't trusted publicly, they're perfectly acceptable in closed systems where you control the environment and trust the endpoints.

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
```

Update config:

```
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

This prevents accidentally using http (plain-text) to connect to your server.

Edit HTTP virtual host:

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

Add inside `<VirtualHost *:80>`:

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

Replace `your-server-ip` with your actual IP or hostname.

4. Apply Changes

Restart Apache:

```
sudo systemctl restart apache2
```

5. Access the Frontend

Use:

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

Accept the browser warning for the self-signed certificate.

The default access credentials are :

- User : **Admin**
- Password : **zabbix**