Installasi osTicket dari How To Forge

How to Install osTicket on Ubuntu 22.04

On this page

1. Prerequisites
2. Install Apache, MariaDB, and PHP
3. Create a Database for osTicket
4. Download osTicket
5. Create Apache Virtual Host
6. Launch osTicket Installation Wizard
7. Secure osTicket with Let's Encrypt SSL
8. Conclusion

osTicket is an open-source and one of the most widely used ticketing systems by small and medium-sized businesses. It is a simple and easy-to-use web-based customer support portal that helps you to manage and track all tickets. osTicket allows you to define ticket routing rules to send tickets to the correct person. You can customize and add your logo, images, and videos to tickets. osTicket supports many database types, such as MySQL and PostgreSQL, and can be integrated with LDAP/Active directory for central authentication.

This post will explain how to install osTicket with Apache on Ubuntu 22.04.

Prerequisites

- A server running Ubuntu 22.04.
- A valid domain name is pointed to your server IP.

- A root password is configured on the server.

Install Apache, MariaDB, and PHP

First, you will need to install the Apache web server, MariaDB, PHP, and other PHP extensions to your server. You can install all the packages using the following command.

```
apt install apache2 mariadb-server php libapache2-mod-php php-mysql php-cgi php-fpm php-cli php-curl php-gd php-imap php-mbstring php-pear php-intl php-apcu php-common php-bcmath -y
```

Once all the packages are installed, start and enable the Apache and MariaDB service using the following command.

```
systemctl start apache2
systemctl enable apache2
systemctl start mariadb
systemctl enable mariadb
```

Create a Database for osTicket

First, secure the MariaDB installation with the following command.

```
mysql_secure_installation
```

Answer all the questions to set a MariaDB root password and secure the installation:

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!

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
```

Next, log in to the MariaDB shell with the following command.

```
mysql -u root -p
```

Once logged in, create a database and user for osTicket with the following command.

```
MariaDB [(none)]> CREATE DATABASE osticket;
MariaDB [(none)]> CREATE USER 'osticket'@'localhost' IDENTIFIED BY 'securepassword';
```

Next, grant all the privileges to the osTicket database with the following command.

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON osticket.* TO osticket@localhost IDENTIFIED BY "securepassword";
```

Next, flush the privileges and exit from the MariaDB shell with the following command.

```
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> EXIT;
```

Once you are done, you can proceed to the next step.

Download osTicket

First, download the latest version of osTicket with the following command.

```
wget https://github.com/osTicket/osTicket/releases/download/v1.17.2/osTicket-v1.17.2.zip
```

Once the osTicket is downloaded, create a directory of osTicket and extract the downloaded file inside that directory.

```
mkdir /var/www/html/osticket
unzip osTicket-v1.17.2.zip -d /var/www/html/osticket
```

Next, change the ownership and permission of the osTicket directory with the following command:

```
chown -R www-data:www-data /var/www/html/osticket
chmod -R 755 /var/www/html/osticket
```

Now, rename the osTicket sample configuration file using the command given below:

```
mv /var/www/html/osticket/upload/include/ost-sampleconfig.php /var/www/html/osticket/upload/include/ost-config.
```

Once you are finished, you can proceed to the next step.

Create Apache Virtual Host

Next, you will need to create an Apache virtual host configuration file for osTicket. You can create it with the following command.

```
nano /etc/apache2/sites-available/osticket.conf
```

Add the following lines:

```
<VirtualHost *:80>
        ServerName osticket.example.com
        ServerAdmin admin@localhost
        DocumentRoot /var/www/html/osticket/upload

        <Directory /var/www/html/osticket/upload>
                Require all granted
                Options FollowSymlinks
                AllowOverride All
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/osticket.error.log
        CustomLog ${APACHE_LOG_DIR}/osticket.access.log combined
</VirtualHost>
```

Save and close the file when you are done. Then, activate the osTicket virtual host and enable the Apache rewrite module with the following command:

```
a2ensite osticket.conf
a2enmod rewrite
```

Next, restart the Apache service to apply the configuration changes:

```
systemctl restart apache2
```

You can check the Apache status with the following command.

```
systemctl status apache2
```

You should get the following output.

```
? apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2022-12-21 07:20:15 UTC; 3s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 62019 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 62023 (apache2)
      Tasks: 6 (limit: 2238)
     Memory: 15.4M
        CPU: 42ms
     CGroup: /system.slice/apache2.service
```

```
        ??62023 /usr/sbin/apache2 -k start
        ??62024 /usr/sbin/apache2 -k start
        ??62025 /usr/sbin/apache2 -k start
        ??62026 /usr/sbin/apache2 -k start
        ??62027 /usr/sbin/apache2 -k start
        ??62028 /usr/sbin/apache2 -k start

Dec 21 07:20:15 ubuntu2204 systemd[1]: apache2.service: Deactivated successfully.
Dec 21 07:20:15 ubuntu2204 systemd[1]: Stopped The Apache HTTP Server.
Dec 21 07:20:15 ubuntu2204 systemd[1]: Starting The Apache HTTP Server...
```

Launch osTicket Installation Wizard

You can now launch the osTicket installation wizard using the URL **http://osticket.example.com.** You should see the following page.

Click on the **Continue.** You should see the basic installation page.

Define your helpdesk URL, name, email, database name, username, password, then click on the **Install Now** button to start the installation. Once the osTicket is installed, you should see the following page.

To access the osTicket control panel, type the URL **http://osticket.example.com/scp** in your web browser. You should see the osTicket login page.

Provide your admin username, password and click on the **Login** button. You should see the osTicket dashboard on the following screen.

You can also access the osTicket default page using the URL **http://osticket.example.com**

Secure osTicket with Let's Encrypt SSL

To secure your website with the Let's Encrypt SSL, you will need to install the certbot package on your server.

First, install the Snap package manager with the following command:

```
apt install snapd
```

Next, update the Snap package to the latest version:

```
snap install core
snap refresh core
```

Next, install the certbot package using the following command:

```
snap install --classic certbot
```

Next, create a symbolic link for Certbot binary to the system location:

```
ln -s /snap/bin/certbot /usr/bin/certbot
```

Next, run the following command to download and install Let's Encrypt SSL certificates:

```
certbot --apache -d osticket.example.com
```

You will be asked to provide your email address and accept the term of service:

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): hitjethva@gmail.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
```

Type Y and press the Enter key to download and install the SSL certificates for your domain:

```
Account registered.
Requesting a certificate for osticket.example.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/osticket.example.com/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/osticket.example.com/privkey.pem
This certificate expires on 2023-03-22.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for osticket.example.com to /etc/apache2/sites-enable/osticket.conf
Congratulations! You have successfully enabled HTTPS on https://osticket.example.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Conclusion

In this post, we showed you how to install osTicket with Apache on Ubuntu 22.04 server. You can now deploy osTicket in your organization to scale and streamline your customer service and drastically improve your customer experience.

Revision #5
Created 20 August 2024 06:00:09 by Admin Diskominfo
Updated 22 August 2024 04:53:21 by Admin Diskominfo