Deploy Umami on Centos 7 server using Docker compose

Pre-request:

* Access to the server with root privilege to server.

Installation :

Install Docker on the server:

Update the packages:

sudo yum update

install the dependency:

sudo yum install -y yum-utils device-mapper-persistent-data lvm2

Add Docker repository to yum:

sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo

Install Docker:

sudo yum install -y docker-ce

Enable and Start Docker:

systemctl enable --now docker

check the service is running and healthy:

systemctl status docker

install docker compose:

Download the latest version of Docker Compose:

sudo curl -L "https://github.com/docker/compose/releases/latest/download/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

Make the Docker Compose binary executable:

sudo chmod +x /usr/local/bin/docker-compose

Verify the installation:

docker-compose –version

Deploying:

Deploy the service using docker compose file, we change the listing port to be 8080:

docker-compose -f ansible/umami-docker-compose.yaml up -d

this will create two containers: one for the PostgreSQL database, with default credentials, and the second container is the official Umami container with the latest updates.

Open the port 8080 on firewalld:

firewall-cmd --add-port=8080/tcp –permanent

Reload the firewall to apply the changes by running the following command:

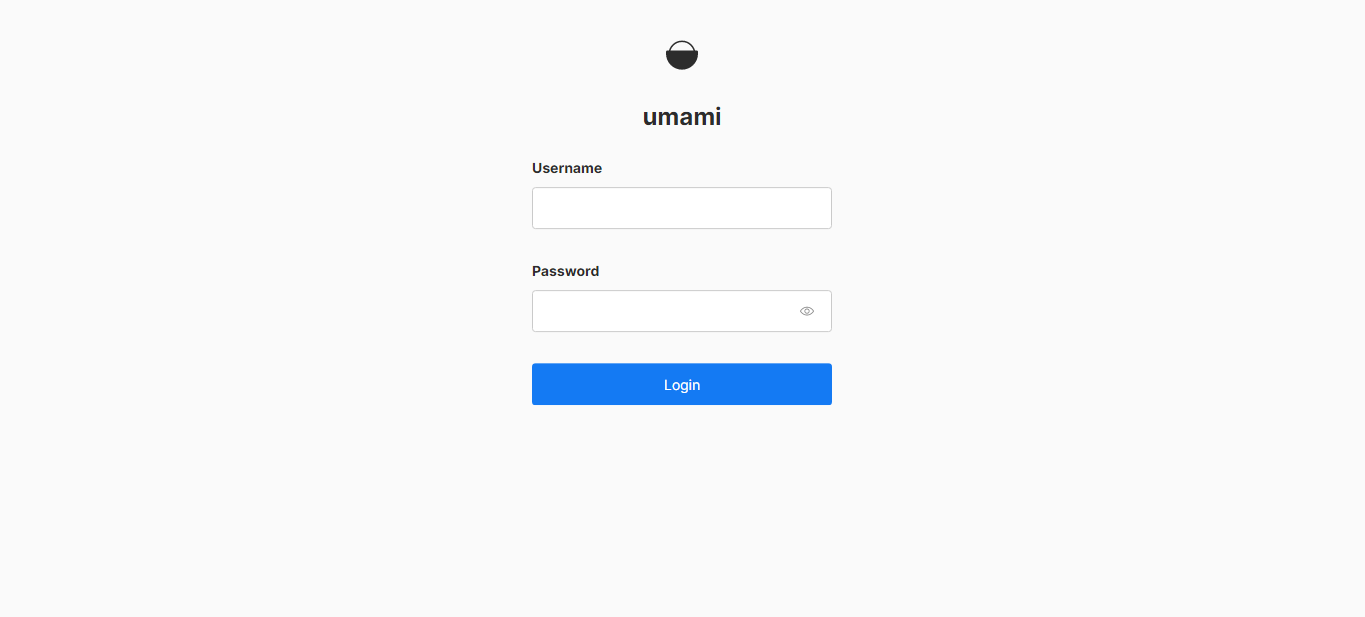
firewall-cmd –reload

Verify that port 8080 is now open by running the following command:

firewall-cmd --list-all | grep 8080

we can test the application now by type is the browser:

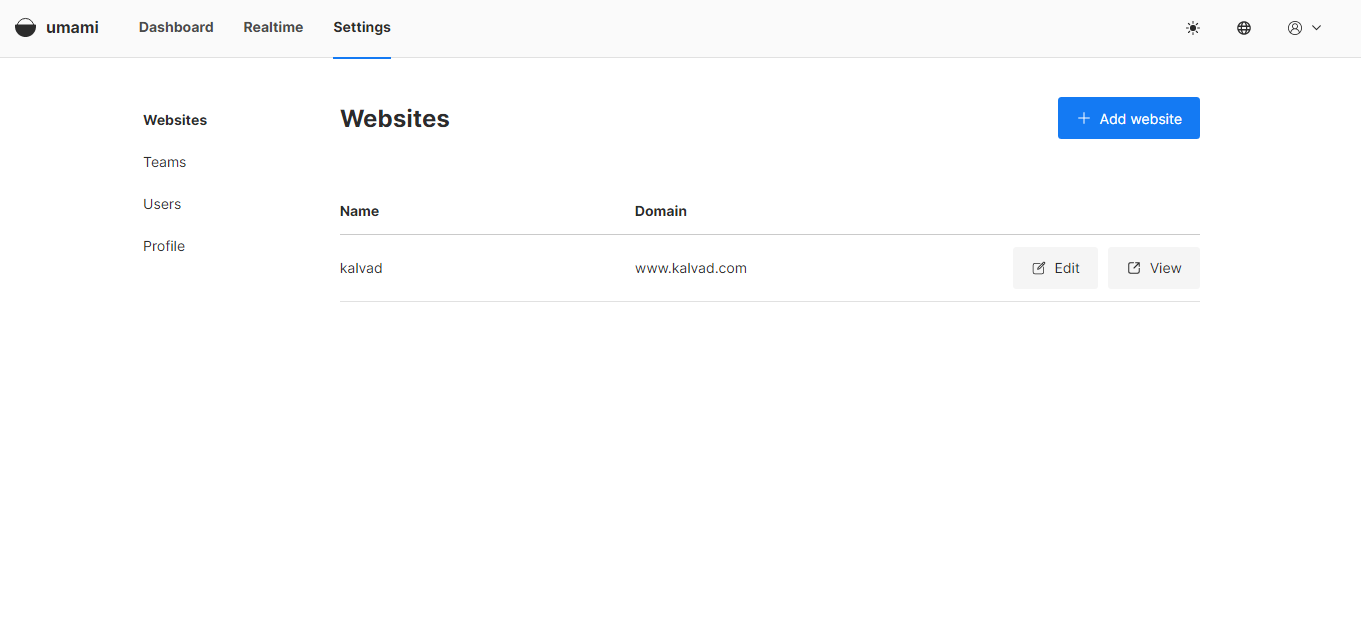
<http://Ip-of-the-server:8080>



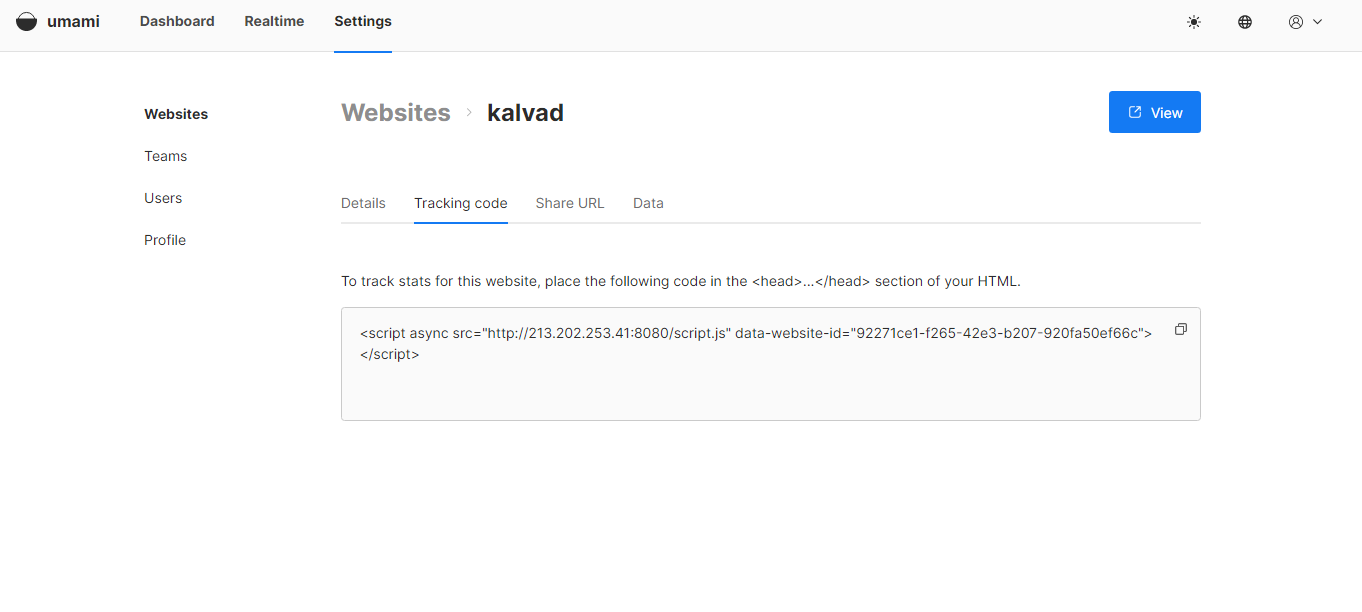
The default credential is username: admin and password: umami

Change the credential immediately after first login.

to add website go to sitting and press add website:



Then press edit and go to tracking code



place the following code in the <head>...</head> section of your HTML

securer the connection:

we need to be mapping the ip address to specific domain or sub domain,

after that we can install SSL certificate to secure the communication:

install nginx as reverse proxy:

sudo yum install nginx

enable and start nginx service

systemctl enable –now nginx

virefy the service is running and healthy:

systemctl status nginx