Automated Deployment of WordPress Website on Nginx using GitHub Actions on AWS Cloud

*This documentation outlines the steps to set up an automated deployment process for a WordPress website using Nginx as the web server, LEMP (Linux, Nginx, MySQL, PHP) stack, and GitHub Actions as the CI/CD automation tool. The deployment process follows security best practices and ensures optimal performance of the website.*

**Website URL –** *https://demo.binbash.website/*

**Github Repo URL -** *https://github.com/eashan98/wordpress*

**## Table of Contents**

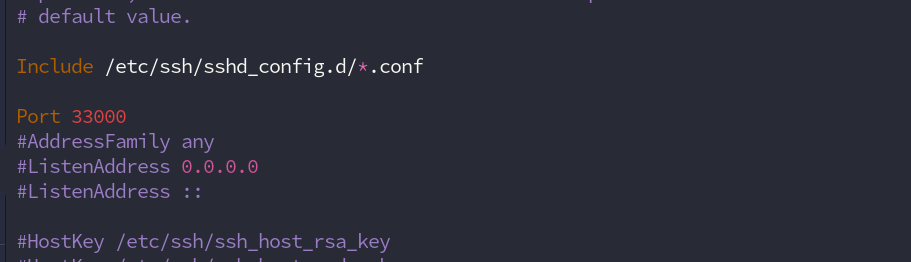
1. Server Provisioning
2. Package Installtion
3. Website Configuration & Security
4. GitHub Repository Setup

**1- Ubuntu Server Provisioning**

• I have choosed a cloud provider of AWS and provision an EC2 Server of Ubuntu Linux 22.04

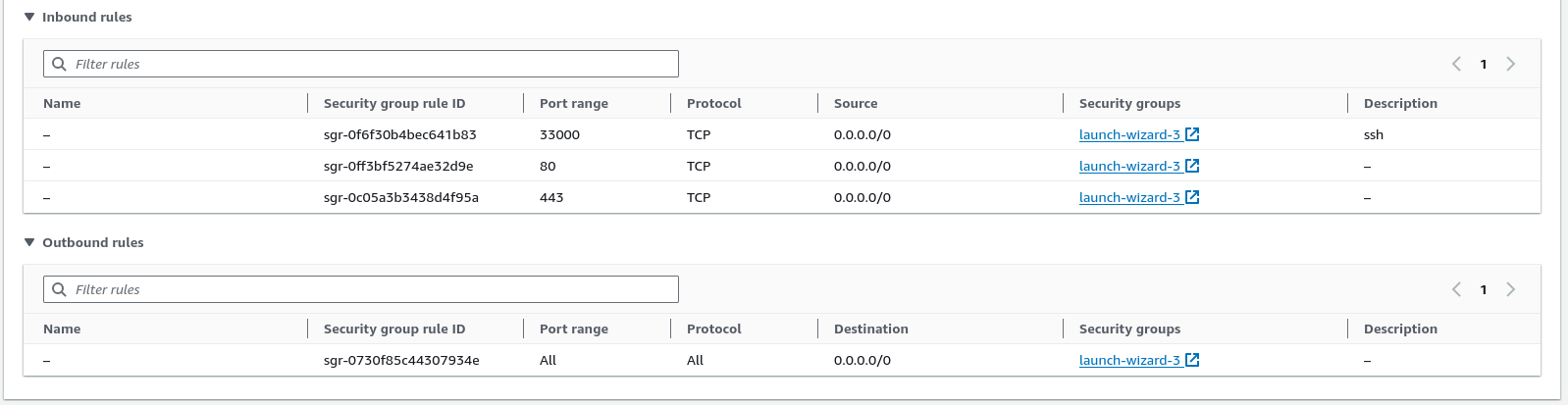
• Set the firewall rules as stated below

◦ Open the port of 33000 only on my IP for secure connection of SSH



◦ Open the port 80 & 443 for the https traffic

• Setup SSH service for only key-based authentication and disable root login for secure remote access



**2. Packages Installation**

• Install Nginx as the web server.

◦ Created Nginx config file for the configuration

▪ URL – *https://github.com/eashan98/wordpress/blob/main/nginx.conf*

◦ setup the project directory at /var/www/html/wordpress

◦ change the owner ship of the /var/www/html/wordpress dir so that nginx can access this directory

• Install MySQL as the database.

◦ Mysql version – 5.7

• Install PHP for processing dynamic content.

◦ Php version – 7.4

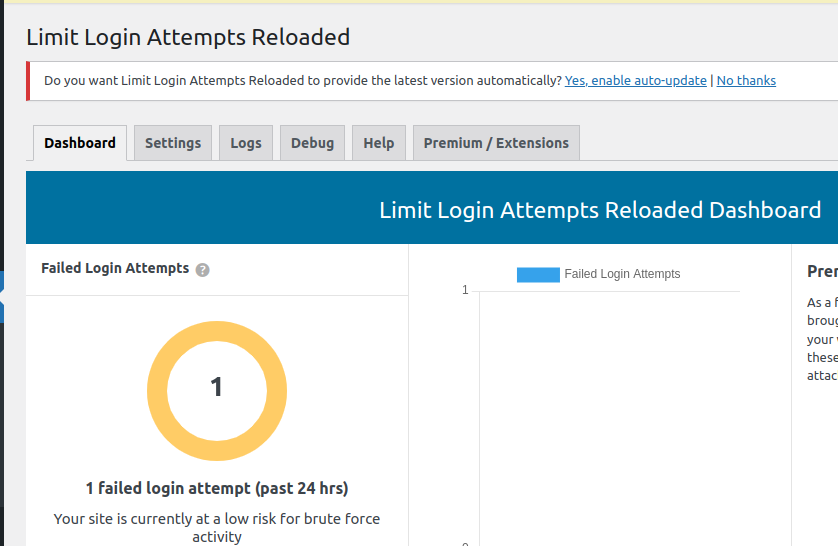
**3. Website Configuration & Security**

• Set up WordPress

◦ Install and configure WordPress in VPS

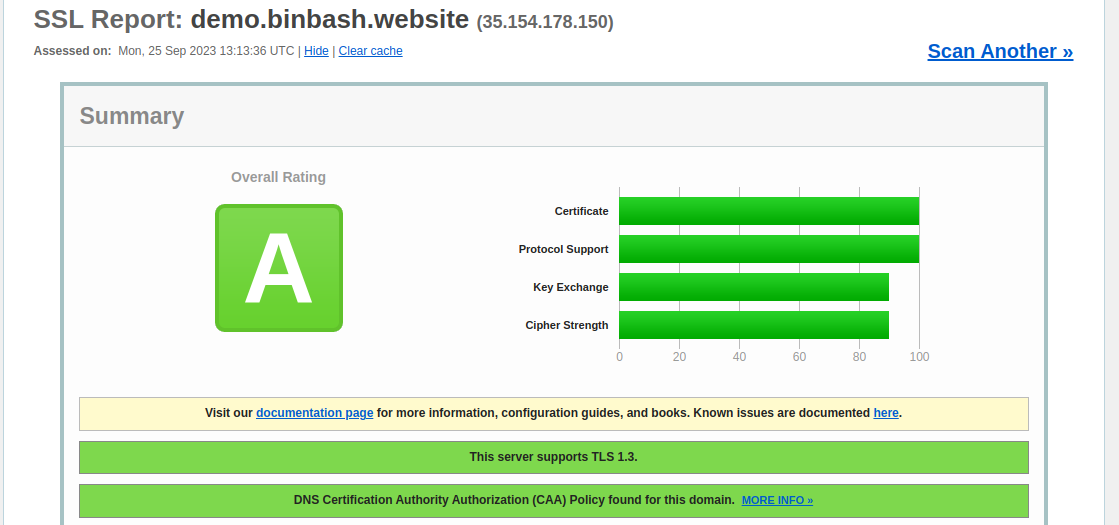
◦ Setup WordPress with strong password

◦ Limit Login Attempts on admin panel to lock after 3 login attempts



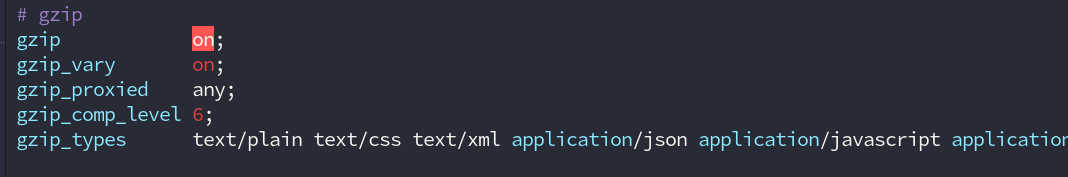
◦ Add Wordpress plugin to protect from XSS, Brute Force Attack & Anti-Spam: Spam Protection, Disable XML-RPC-API (Lightweight plugin to disable XML-RPC API and Pingbacks,Trackbacks for faster and more secure website.)

• Implemented SSL Certificate with LetsEncrypt for Secure HTTPS connection and setup LetsEncrypt for auto-renewal of certificate. (here is a report from [www.ssllabs.com](http://www.ssllabs.com))



• Optimized Nginx Configuration

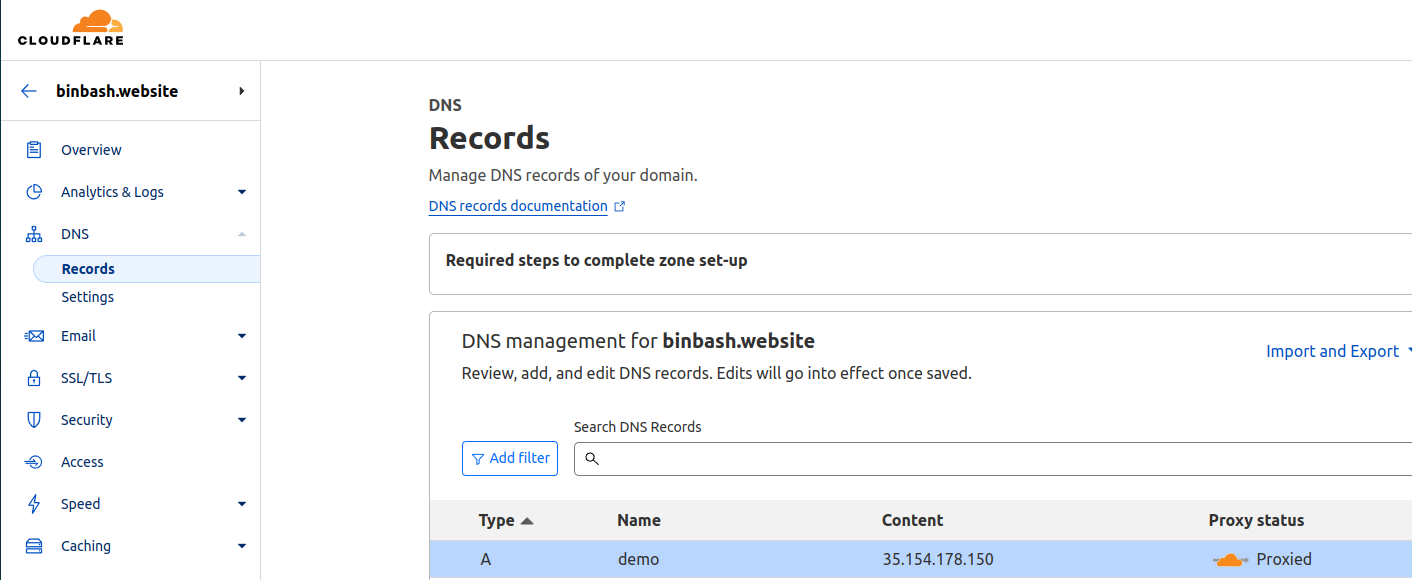
◦ Optimized the Nginx server configuration to enhance website performance using caching, gzip compression, and added Security Headers to increase security.





**4. CloudFlare Setup**

* Cloudflare will protect your site from threats, improve performance, and provide analytics.
* It enhances security by shielding against DDoS attacks and threats
* It optimizes website performance with content delivery, improving user experience.
* Config -
  + Added a “A” record with the name demo.binbash.website that points to the wordpress server IP.
  + Also update the name server of cloud flare in domain registrar name server setting .

****

**4. GitHub Repository Setup**

• Created a GitHub Repository to save the WordPress project.

• Create the GitHub Actions yaml for the automated deployment of project and securely transfer project files to the VPS also install dependency (if required)

◦ ci-yaml - *https://github.com/eashan98/wordpress/blob/main/.github/workflows/main.yml*

• Here you can find the instruction to setup this enviroment locally

◦ README.md – *https://github.com/eashan98/wordpress/blob/main/README.md*