HOSTNEXTRA

AFTER SERVER SETUP **CHECKLIST**

When we provide you the login credentials of the your new server, it is recommended to follow some initial steps to get the server secure and performing optimally.

In this guide, we'll show you some of our recommendations for securing the server at the initial stage. We offer server management service where we do hardening and monitoring of the server if you want us to take care of that task.

1

Change Root Password

It is always recommended to change the root user password of the server when you receive new server credentials and should store in a secure password manager.

For Linux: Use **passwd** command to set new password

2

Create A New Admin User

To perform system or root level tasks, you should never run it using root user access. It is a safe way to create a new user with sudo rights so that the user can perform the system-level task.

For Linux:

```
adduser -G wheel admin
passwd admin
```

3

Disable Root Login

The attacker target root user in a brute-force attack, disabling root user can lower the risk of brute-force attack to the server. It is the best practice to do.

Open the SSH configuration file.
sudo vi /etc/ssh/sshd_config
Set **permissionRootLogin=no**
Restart sshd service: sudo systemctl restart sshd

4

Modify The Default SSH Port

Modifying the default SSH Port 22 can reduce automated connections. The automated bot tries and brute-force on default SSH port. So it's recommend to modify the port.

Open the SSH configuration file.
sudo vi /etc/ssh/sshd_config
Set **Port= [new port]**
Restart sshd service: sudo systemctl restart sshd

5

Use SSH Key to Login

SSH key based authentication is always a best practice to do. It will secure most common interruption point into a server.

Use the **ssh-keygen** command to create an SSH key on your computer and the **ssh-copy-id** command to copy the SSH key to the server:
ssh-copy-id root@SERVER-IP

6

Keep The Server Up-To-Date

Always keep the server updated, it will help to prevent many common attacks. There is no better method to secure a server than to ensure it is consistently updated OS, kernel, and application programming.

apt-get upgrade -y (Ubuntu Based)
yum update -y (Fedora Based)

7

Enable and Configure the Firewall

Firewall plays an important role in server security. With dedicated server firewalld is pre-installed but in VPS, it need to install firewall. We recommend you to use CSF firewall.

sudo apt install ufw (Ubuntu Based).
To install CSF on CentOS
It is a detail article about the CSF.

8

Set the System Time

To record activities with the proper time, it is crucial to set a system time. It will help to troubleshoot the issues.

```
sudo timedatectl set-time YYYY-MM-DD
```

NEED HELP WITH YOUR SERVER MANAGEMENT?

Our server administration services cover server hardening, 3rd party software installations, 24/7 server monitoring, reboot assistance, server migrations, backup configuration. Our expert server Engineers work round-the-clock to ensure excellent performance.

SERVER MANAGEMENT

CONTACT US