

# Server Hardening

Wie sichern wir unseren BFFH Server ab und verhindern Angriffe? Auf dieser Seite finden sich Ansätze für ein stabiles, sicheres Setup in einer Linux-Umgebung.

## Offene Ports prüfen

```
netstat -an | grep LISTEN | grep -v LISTENING
```

## Unattended Upgrades

Automatische Updates per apt

```
sudo apt update
sudo apt upgrade -y
sudo apt install unattended-upgrades -y
sudo dpkg-reconfigure -plow unattended-upgrades
```

## Fail2ban

Basiert auf <https://www.digitalocean.com/community/tutorials/how-to-protect-an-nginx-server-with-fail2ban-on-ubuntu-20-04>

```
sudo apt install fail2ban
sudo systemctl enable fail2ban.service
```

```
cd /etc/fail2ban/
sudo cp jail.conf jail.local
```

```
sudo vim /etc/fail2ban/jail.local
```

```
[DEFAULT]
...
findtime = 10m
maxretry = 5
...
```

```
sudo vim /etc/fail2ban/jail.d/defaults-debian.conf
```

```
[DEFAULT]
```

```
banaction = nftables
```

```
banaction_allports = nftables[type=allports]
```

```
backend = systemd
```

```
[sshd]
```

```
enabled = true
```

```
sudo systemctl restart fail2ban.service
```

---

Version #2

Erstellt: 28 Dezember 2024 02:14:38 von Mario Voigt (Stadtfabrikanten e.V.)

Zuletzt aktualisiert: 28 Dezember 2024 02:52:59 von Mario Voigt (Stadtfabrikanten e.V.)