# Sicherheit

## Absichern eines Ubuntu Servers

Eine Anleitung für die Basisababsicherung findest du hier

## Besucher pro Land sperren

Eine Anleitung findest du hier

## ClamAV Antivirus

Eine Installationsanleitung inkl. Konfiguration für Nextcloud findest du hier.

ClamAV restarten:

```
service clamav-daemon restart
```

überprüfen, ob der Daemon läuft:

```
/etc/init.d/clamav-daemon status
netstat -a |grep clam
```

Verbraucht der Clamav Daemon zuviel CPU Ressourcen, so kann man diie CPU Last begrenzen:

Edit `/lib/systemd/system/clamav-daemon.service` to include this line in the `[Service]` section:

```
CPUQuota=20%

Then restart the service
```

```
sudo systemctl daemon-reload
```

Starte einen manuellen Scan:

```
sudo clamscan -r -i /pfad/zum/verzeichnis
```

Achtung: Je nach Größe kann das länger dauern!

# Lynis:

ist eine Applikation, mit deren Hilfe man Autdits des Systems durchführen kann. Es ändert keine Einstellungen am System. Eine Anleitung findest du hier

Eine Anlaeitung für die Installation der letzten Version findest du hier

# fail2ban

Es ist ratsam fail2ban für die Absicherung eines Linux-Servers einzusetzen. Eine umfangreiche Anleitung findest du hier. Diese Anleitung ist auch sehr gut, ebenso diese

Will man IP Adressen auch nach einem Restart permanent bannen, hilft diese Anleitung.

Für Owncloud/Nextcloud gibt es diese Absicherung

Gute Beispiele, um einen Apache Webserver abzusichern findest du hier

## fail2ban bricht bei einem Start mit einem Fehler ab

Eine aussagekräftige Fehlerinformation findest du bei eingabe in die CLI: `fail2ban-client -x start`

## Hier ein Beispiel, wie man eine regex testen kann (apache-404.conf)

```
fail2ban-regex /var/log/apache2/error.log /etc/fail2ban/filter.d/apache-auth.conf
```

## Will man eine IP unblocken:

```
sudo fail2ban-client set Jailname unbanip IP-Adresse
```

### Wichtige fail2ban client Kommandos:

### fail2ban-client COMMAND

| Kommando | Erklärung |
|---|---|
| start | startet alle Jails |
| reload | liest die Konfigurationsfiles neu ein |
| relead JAIL | liest die Konfiguration des mit JAIL benannten Jails ein |
| stop | stoppt den Server |
| status | zeigt den Status des Servers und aller aktiven Jails |
| status JAIL | zeigt den Status des mit JAIL bezeichneten Jails an |

# Stoppen von DDoS Attacken (kleine)

Eine gute Anleitung findest du hier

# UFW

Die UFW = uncomlicated Firewall ist ein leicht zu bedienendes Werkzeug zum Bearbeiten der Firewallregeln.

### Grundeinstellungen:

```
$ sudo ufw allow ssh/tcp
$ sudo ufw logging on
$ sudo ufw enable
$ sudo ufw status (numbered)
```

Die Reihenfolge der Kette ist wichtig. Daher sind die offenen Ports hinten in der Kette zu reichen. Mit insert kann man die zu blockierenden IPs vorher in der Kette plazieren.

```
sudo ufw insert [position] [theRule]
```

### eine ganze IP-Range sperren

```
sudo ufw deny from 195.96.129.0/24 to any
```

### Firewall aus- und wieder einschalten

```
$ sudo ufw disable
$ sudo u□fw enable
```

### grafisches Interface

für U'FW = gufw

### welcher Prozess nutzt welchen Port

```
sudo ss -tulnpa | grep (portnummer)
```