

Pakete:

- Debian (ab 7): fail2ban

Per default überwacht fail2ban bei debian ssh:

```
egrep -A7 '\[sshd?\]' /etc/fail2ban/jail.conf
less /etc/fail2ban/filter.d/sshd.conf
```

[/etc/fail2ban/jail.conf](#)

```
...
[DEFAULT]
...
banaction = iptables-multiport
...
```

```
less /etc/fail2ban/action.d/iptables-multiport.conf
```

fail2ban Zusammenfassung der Konfiguration anzeigen:

```
fail2ban-client status
fail2ban-client status sshd
```

Apache Basic Auth

Pakete: apache2 fail2ban (Debian 9)

```
mkdir -p /srv/www/fail2ban
htpasswd -c /srv/www/htpasswd_fail2ban heinz
```

[/etc/apache2/conf-available/fail2ban-apache-auth-test.conf](#)

```
<directory /srv/www/fail2ban>
  AllowOverride AuthConfig
  AuthType      Basic
  AuthName      "Bitte Username und Passwort"
  AuthBasicProvider file
  AuthUserFile  /srv/www/htpasswd_fail2ban
  Require       valid-user
</directory>
```

[/srv/www/fail2ban/index.html](#)

```
<html>
<head>
```

```
<title>Hello fail2ban!</title>
</head>
<body>
  Hello fail2ban
</body>
</html>
```

Zugriff lokal testen:

```
wget --user heinz --password xxx -nv -O -
http://127.0.0.1/fail2ban-test/index.html
```

[/etc/fail2ban/jail.local](#)

```
[apache-auth]
enabled = true
```

```
fail2ban-client reload
fail2ban-client status
fail2ban-client status apache-auth
```

Von einem anderen Rechner aus:

```
ab -n 10 -A heinz:nono http://192.168.212.11/fail2ban-test/index.html
```

```
less /var/log/fail2ban.log
```

From:
<https://wiki.lab.linuxhotel.de/> - **Linuxhotel Wiki**

Permanent link:
<https://wiki.lab.linuxhotel.de/doku.php/lpi2:fail2ban>

Last update: **2018/02/02 11:16**

