fail2ban - Abfragen

Alle gebannten IP's und in welchem jail herrauszufinden ist bei fail2ban ziemlich aufwending ud unübersichtlich.
Deshalb hier ein paar Möglichkeiten

```
fail2ban-client status | grep "Jail list:" | sed "s/ //g" | awk '{split($2,a,",");fo
r(i in a) system("fail2ban-client status " a[i])}' | grep "Status\|IP list"
```

Fail2ban nutzt die Daenbank sqlite3.
Diese lässt sich natürlich abfragen:

```
sqlite3 /var/lib/fail2ban/fail2ban.sqlite3 \
"select datetime(timeofban, 'unixepoch', 'localtime') as startofban,
datetime(timeofban + bantime, 'unixepoch', 'localtime') as endofban,
ip, jail, bantime, bancount, data from bips
where endofban > datetime('now', 'localtime')
order by jail, endofban
limit 10"
```

Show all IP address and its jail:

```
sqlite3 /var/lib/fail2ban/fail2ban.sqlite3 "select ip,jail from bips"
```

Show all unique IP address:

```
sqlite3 /var/lib/fail2ban/fail2ban.sqlite3 "select distinct ip from bips"
```

Show all unique IP address in sshd jail:

```
sqlite3 /var/lib/fail2ban/fail2ban.sqlite
3 "select distinct ip from bips where jail='sshd'"
```

Show top 20 most banned IP address in all jails:

```
sqlite3 /var/lib/fail2ban/fail2ban.sqlite
3
"select jail,ip,count(*) as count from bips group by ip order by count desc limit 20
"
```

Eindeutige ID: #1129
Verfasser: n/a
Letzte Änderung: 2023-02-05 14:54