Security

I see many access attempts in the log files of my SSH server, what can I do about it?

The many access attempts indicate that someone wants to gain unauthorized access to your system. On the one hand, it makes sense to change the default port of the SSH server, for this you can also find a FAQ entry in our system.

In addition to the port change you have the possibility to install a program which works in cooperation with "iptables" and keeps unwanted guests away.

The tool fail2ban notices unauthorized access attempts and blocks the connections from the attacking IP using added rules in iptables.

The installation of fail2ban does not require any further configuration and is ready to use. Under Debain / Ubuntu it runs as follows:

root@server:~# apt-get install fail2ban

For other operating systems, use the system's package manager. fail2ban is now preconfigured for incoming SSH connections.

Unique solution ID: #1433
Author: Bettina Brauer
Last update: 2021-04-01 06:20