Network: fail2ban

Fail2ban is very important, as it will detect brute force intrusions tries and prevent attackers from accessing the system.

Here ar some small docs on how to setup and us fail2ban in brief.

Installation

The original Version in SuSe 15.6 is 0.11 - what is horribly old and will not work any more.

So add the Security- Repo from the Build- Service to have at least V1.1.0 from here:

https://build.opensuse.org/repositories/security

Then, install with:

```
zypper install fail2ban
```

Configuring

The most work should already be done by fail2ban or by your distribution - for example on how to setup the rules in detail.

So in my case for a small setup, it was enough to extend the file /etc/fail2ban/jail.local :

```
# Do all your modifications to the jail's configuration in jail.local!
[DEFAULT]
#
# MISCELLANEOUS OPTIONS
#

# "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
```

```
ignoreip = 127.0.0.1/8 ::1 192.168.178.0/24
# "bantime" is the number of seconds that a host is banned.
bantime  = 48h
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 4h
# "maxretry" is the number of failures before a host get banned.
maxretry = 3

[sshd]
enabled = true
port    = ssh
filter  = sshd
logpath = %(sshd_log)s
backend = systemd
```

This alread enabled SSH.

Monitoring fail2ban

For an overview: `fail2ban-client status`
Or for a Service (called Jail): `fail2ban-client status sshd`

This will show all banned ips.

From:
http://dokuwiki.obel1x.de/ - **obel1x.de**

Permanent link:
http://dokuwiki.obel1x.de/content:serverbasics:network-fail2ban

Last update: **2025/08/07 10:56**