

fail2ban (0.9.6)

•
•
•
•
•
•
•

fail2ban , , . ,

:

- Astra Linux Common Edition 2.12

fail2ban (. synaptic) :

```
sudo apt install fail2ban
```

fail2ban :

0	
/etc/fail2ban/fail2ban.conf /etc/fail2ban/fail2ban.local	" "
/etc/fail2ban/filter.d/*.conf /etc/fail2ban/filter.d/*.local	, . , .
/etc/fail2ban/action.d/*.conf /etc/fail2ban/action.d/*.local /etc/fail2ban/action.d/*.py	, /. , Python (*.py).
/etc/fail2ban/jail.conf /etc/fail2ban/jail.local /etc/fail2ban/jail.d/*.conf /etc/fail2ban/jail.d/*.local	. .conf/.local.

*.conf , , *.local , *.conf, .. , *.conf.

fail2ban sshd. /etc/fail2ban/jail.d/defaults-debian.conf.
C " ":

[sshd]
enabled = true

10 , 5 10 , /etc/fail2ban/jail.conf.

:

maxretry	
findtime	,
bantime	, findtime maxretry

, , /etc/fail2ban/jail.conf. (,), () /etc/fail2ban/jail.d/ .local , , /etc/fail2ban/jail.d/00-orel.local:

 [DEFAULT]
bantime = 300
maxretry = 10
findtime = 3600
ignoreip = 10.0.15.0/24

:

- [DEFAULT], ;
- 5 (300);
- 10 ;
- (3600);
- 10.0.15.0/24.

fail2ban , ,

```
sudo systemctl restart fail2ban
```

```
fail2ban , , /etc/fail2ban/filters.d/ (, dovecot /etc/fail2ban/filters.d/dovecot.conf).  
 , ssh, /etc/fail2ban/jail.d .local, enabled=true.
```

, dovecot /etc/fail2ban/jail.d/dovecot.local:

 [dovecot]
enabled = true
bantime = 120

. [dovecot] (- bantime), dovecot, (2 (120)). (filter).

/etc/fail2ban/filter.d/ /etc/fail2ban/action.d/, , .local.

, :

```
fail2ban-client set < > unbanip <IP- >
```

, ssh 10.0.15.35 :

```
fail2ban-client set sshd unbanip 10.0.15.35
```

man:

 man fail2ban
man fail2ban-server
man fail2ban-client
man jail.conf