

Documentatie fail2ban installeren in virtuele omgeving en deployment on bare-metal

Documentatie type	Link
Online markdown documentation	github.com
Online pdf documentation	github.com

Table of contents

- [Documentatie fail2ban installeren in virtuele omgeving en deployment on bare-metal](#)
 - [Table of contents](#)
 - [Installatie fail2ban op ubuntu server](#)
 - [Configuratie fail2ban op ubuntu server](#)
 - [Findtime](#)
 - [Maxretry](#)
 - [Bantime](#)
 - [Configureer fail2ban opdracht](#)
 - [Testen van fail2ban service](#)
 - [Resultaten bans / jails](#)

Installatie fail2ban op ubuntu server

```
sudo apt install fail2ban -y
```

Configuratie fail2ban op ubuntu server

```
sudo cp jail.conf jail.local
```

Findtime

```
103 # A host is banned if it has generated "maxretry" during the last "findtime"
104 # seconds.
105 findtime = 10m
```

Maxretry

```
107 # "maxretry" is the number of failures before a host get banned.
108 maxretry = 5
```

Bantime

```
100 # "bantime" is the number of seconds that a host is banned.  
101 bantime = 10m
```

Configureer fail2ban opdracht

```
[DEFAULT]  
bantime = 15m  
findtime = 3m  
maxretry = 6  
  
[sshd]  
port = ssh  
logpath = %(sshd_log)s  
backend = %(sshd_backend)s
```

Aangezien de service al actief was moet deze herstart worden zodat de aanpassingen in de config file kunnen worden opgenomen.

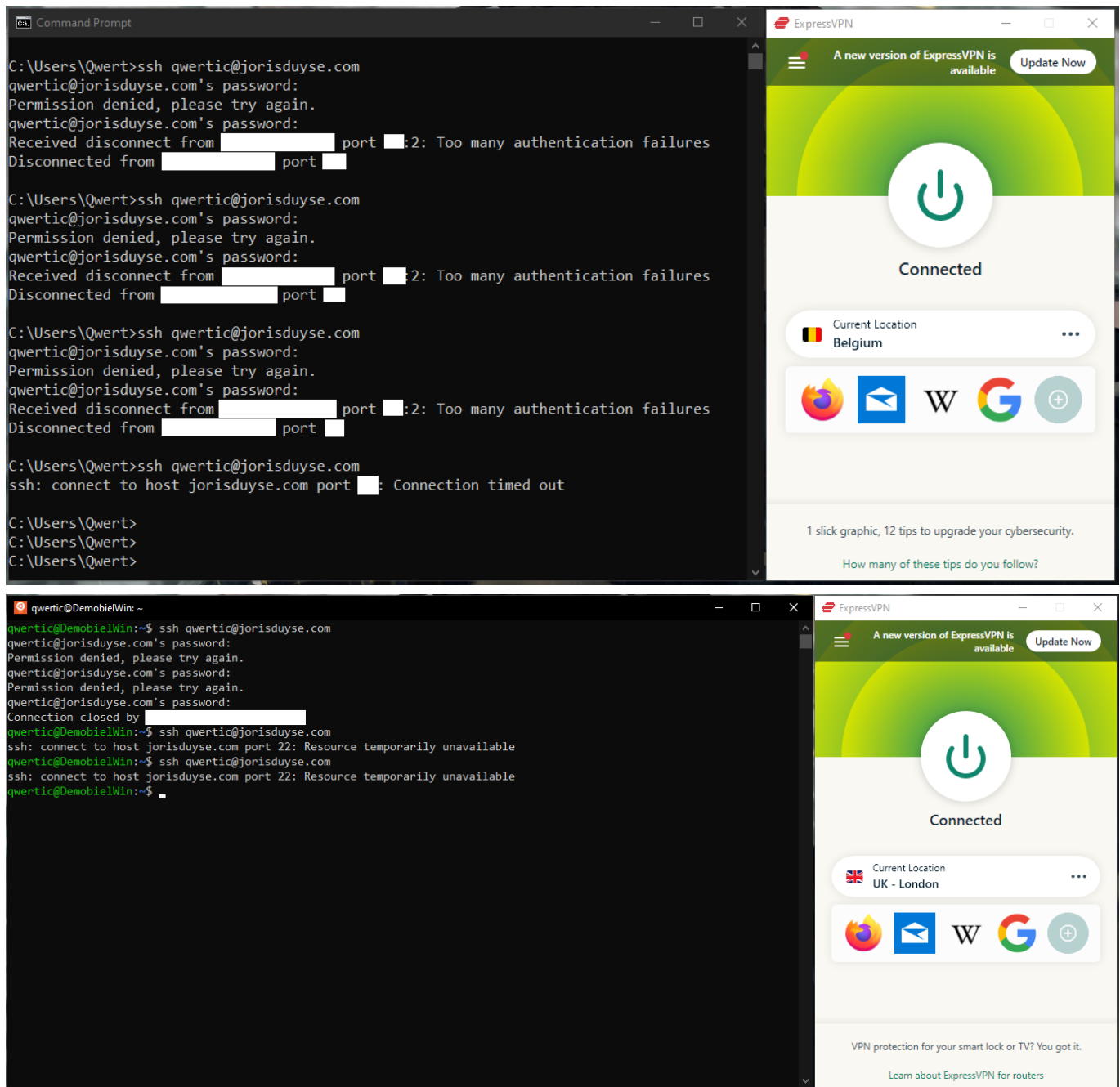
```
systemctl status fail2ban.service
```

```
qwertic@cplex: ~  
qwertic@cplex:~$ systemctl status fail2ban.service  
● fail2ban.service - Fail2Ban Service  
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)  
   Active: active (running) since Sat 2022-03-19 13:21:28 UTC; 1h 19min ago  
     Docs: man:fail2ban(1)  
  Main PID: 24241 (f2b/server)  
    Tasks: 5 (limit: 9306)  
  Memory: 18.0M  
   CGroup: /system.slice/fail2ban.service  
           └─24241 /usr/bin/python3 /usr/bin/fail2ban-server -xf start  
  
Mar 19 13:21:28 cplex systemd[1]: Starting Fail2Ban Service...  
Mar 19 13:21:28 cplex systemd[1]: Started Fail2Ban Service.  
Mar 19 13:21:28 cplex fail2ban-server[24241]: Server ready  
qwertic@cplex:~$
```

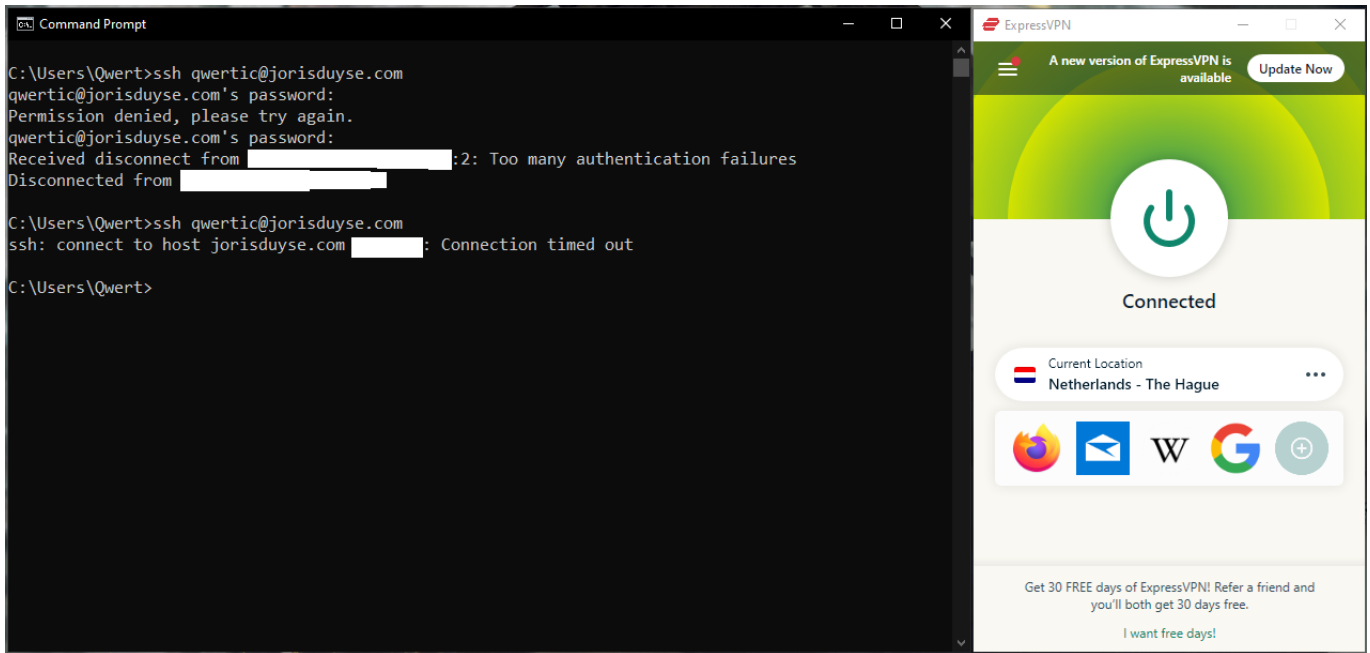
```
$ sudo systemctl reload fail2ban.service #ssh connection crashed; sign it works?  
[sudo] password for qwertic:  
client_loop: send disconnect: Connection reset
```

Testen van fail2ban service

Wanneer het ip wordt gemerkt toont ssh in **cmd** echter **Connection timed out** in plaats van **ssh: connect to host server.hostname.com port 2022: Connection refused**. In **Ubuntu 20.04 on Windows** komt de error **ssh: connect to host jorisduyse.com port 22: Resource temporarily unavailable**



"Test wanner **maxretry** in jail.local op 6 staat"



"Test wanner **maxretry** in jail.local op **1** staat"

Resultaten bans / jails

```
sudo iptables -n -L #list of banned ip addresses
```

