

Fail2ban

installazione :

```
sudo apt install fail2ban
```

verificare la versione :

```
fail2ban-client --version
```

Fail2ban è dotato di file di configurazione predefiniti che puoi personalizzare in base alle tue esigenze. Il file di configurazione principale si trova in **/etc/fail2ban/jail.conf** .

Tuttavia, si consiglia di creare una copia locale (**/etc/fail2ban/jail.local**) per evitare che le modifiche vengano sovrascritte durante gli aggiornamenti.

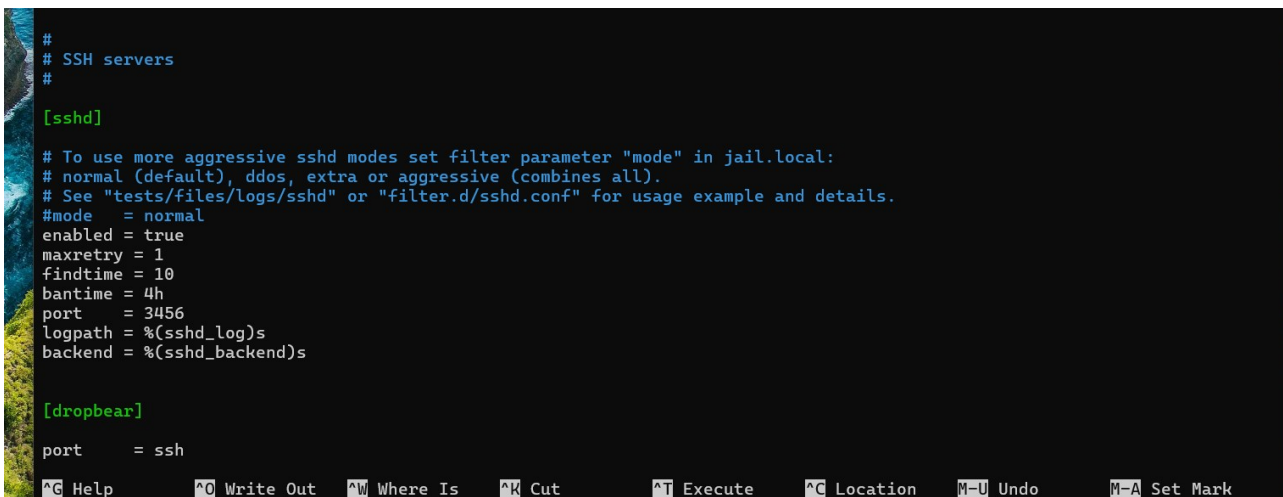
Il comando :

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

apri un editor di testo che vuoi esempio nano,vim,ecc. :

```
sudo nano /etc/fail2ban/jail.local
```

nel file di configurazione immetti le seguenti diciture :



```
#
# SSH servers
#

[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode = normal
enabled = true
maxretry = 1
findtime = 10
bantime = 4h
port = 3456
logpath = %(sshd_log)s
backend = %(sshd_backend)s

[dropbear]

port = ssh

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set Mark
```

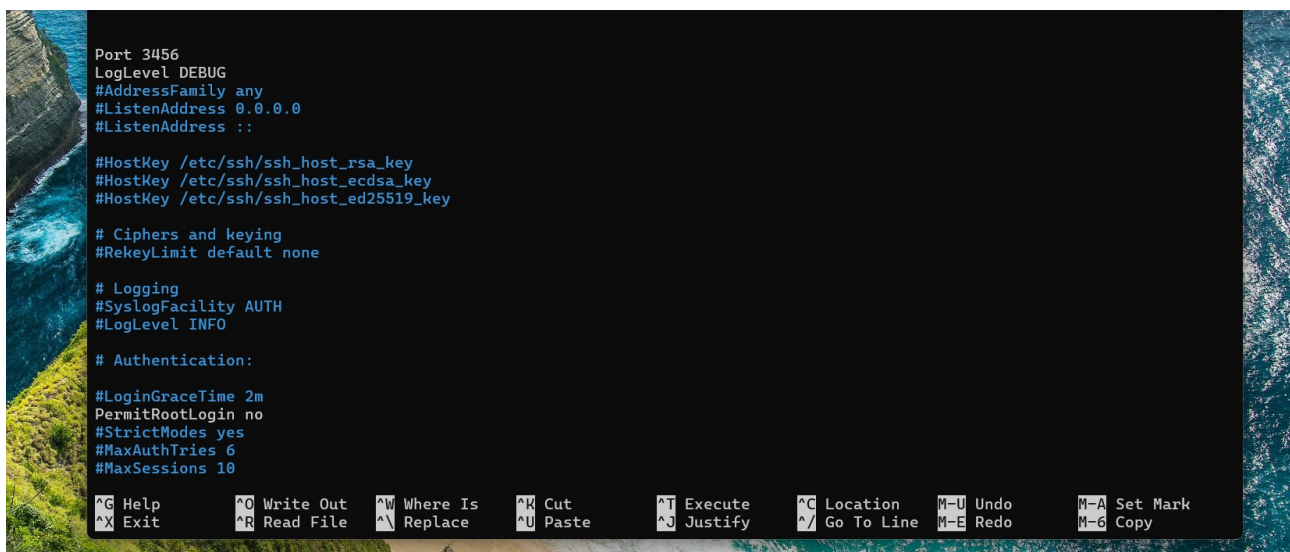
installare ssh

ssh è un servizio che permette gli utenti di connettersi a una macchina/pc/server da remoto :

- 1) `sudo apt install openssh-server`
- 2) `sudo systemctl start ssh`
- 3) `sudo systemctl enable ssh`
- 4) `sudo systemctl status ssh` --- → visualizza se il servizio è in running

di norma l'ssh è la porta 22 ma cambiandola nel file di configurazione in ssh puoi mettere in sicurezza il server, eppure negare il login con root indispensabile, puoi aumentare la verbosità dei log con il DEBUG, il file di configurazione è :

`sudo nano /etc/ssh/sshd_config` :

A screenshot of a terminal window showing the configuration file /etc/ssh/sshd_config. The file is being edited with the nano text editor. The configuration includes settings for port (3456), log level (DEBUG), address family (any), listen address (0.0.0.0), host keys (rsa, ecdsa, ed25519), ciphers and keying (rekey limit default none), logging (syslog facility AUTH, log level INFO), and authentication (login grace time 2m, permit root login no, strict modes yes, max auth tries 6, max sessions 10). The bottom of the screen shows the nano editor's command palette with various shortcuts like ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^C Location, ^M Undo, ^A Set Mark, ^X Exit, ^R Read File, ^\ Replace, ^U Paste, ^J Justify, ^_ Go To Line, ^E Redo, and ^G Copy.

dopo di che esegui il riavvio del servizio e fallo partire, enable fa sì che il servizio partirà alla accensione della macchina/server con questi comandi :

- 1) `sudo systemctl restart fail2ban`
- 2) `sudo systemctl start fail2ban`
- 3) `sudo systemctl enable fail2ban`
- 4) `sudo systemctl status fail2ban`

in ufw che sarebbe il firewall di linux abilitare il transito con di connessioni :

1) `sudo ufw status` -- → vedrà se il servizio è attivo se non lo è usare -- → `sudo ufw enable`

2) abilitare la porta 3456 --- → `sudo ufw allow 3456/tcp`

3) accesso in ssh sarà : `ssh -p 3456 server@192.168.200.122`

oppure loggarsi con la verbosità :

`ssh -vvv -p 3456 server@192.168.200.122` o `ssh -v -p 3456 server@192.168.200.122`

esempio immagini accesso in -v o -vvv :

```
server@ubuntu: ~  
debug1: Trying private key: C:\\Users\\UTENTE/.ssh/id_ecdsa  
debug1: Trying private key: C:\\Users\\UTENTE/.ssh/id_ecdsa_sk  
debug1: Trying private key: C:\\Users\\UTENTE/.ssh/id_ed25519  
debug1: Trying private key: C:\\Users\\UTENTE/.ssh/id_ed25519_sk  
debug1: Trying private key: C:\\Users\\UTENTE/.ssh/id_xmss  
debug1: Trying private key: C:\\Users\\UTENTE/.ssh/id_dsa  
debug1: Next authentication method: password  
server@192.168.1.52's password:  
Authenticated to 192.168.1.52 ([192.168.1.52]:3456) using "password".  
debug1: channel 0: new session [client-session] (inactive timeout: 0)  
debug1: Requesting no-more-sessions@openssh.com  
debug1: Entering interactive session.  
debug1: pledge: filesystem  
debug1: ENABLE_VIRTUAL_TERMINAL_INPUT is supported. Reading the VTSequence from console  
debug1: ENABLE_VIRTUAL_TERMINAL_PROCESSING is supported. Console supports the ansi parsing  
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0  
debug1: client_input_hostkeys: searching C:\\Users\\UTENTE/.ssh/known_hosts for [192.168.1.52]:3456 / (none)  
debug1: client_input_hostkeys: searching C:\\Users\\UTENTE/.ssh/known_hosts2 for [192.168.1.52]:3456 / (none)  
debug1: client_input_hostkeys: hostkeys file C:\\Users\\UTENTE/.ssh/known_hosts2 does not exist  
debug1: client_input_hostkeys: host key found matching a different name/address, skipping UserKnownHostsFile update  
debug1: pledge: fork  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
System information as of Wed Jan  8 07:52:29 PM UTC 2025  
  
System load:  0.12          Processes:          113
```

```
server@ubuntu: ~  
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0  
debug1: client_input_hostkeys: searching C:\\Users\\UTENTE/.ssh/known_hosts for [192.168.1.52]:3456 / (none)  
debug1: client_input_hostkeys: searching C:\\Users\\UTENTE/.ssh/known_hosts2 for [192.168.1.52]:3456 / (none)  
debug1: client_input_hostkeys: hostkeys file C:\\Users\\UTENTE/.ssh/known_hosts2 does not exist  
debug1: client_input_hostkeys: host key found matching a different name/address, skipping UserKnownHostsFile update  
debug1: pledge: fork  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
System information as of Wed Jan  8 07:52:29 PM UTC 2025  
  
System load:  0.12          Processes:          113  
Usage of / :  33.7% of 18.62GB  Users logged in:    1  
Memory usage: 5%             IPv4 address for enp0s3: 192.168.1.52  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
Last login: Wed Jan  8 19:51:27 2025 from 192.168.1.40  
server@ubuntu:~$
```

4) buttare giù la porta 22 : `sudo ufw deny 22/tcp`

5) se vuoi e se necessiti di tale cosa.... Bloccare tutto il traffico in entrata tranne per un solo IP a piacere. bloccare tutto il traffico in entrata :

`sudo ufw default deny incoming`

6) **Consentire tutto il traffico in uscita:**

`sudo ufw default allow outgoing`

7) Consenti l'accesso sulla porta 3456 solo dall'IP specifico :

`sudo ufw allow from 192.168.200.122 to any port 3456 proto tcp`

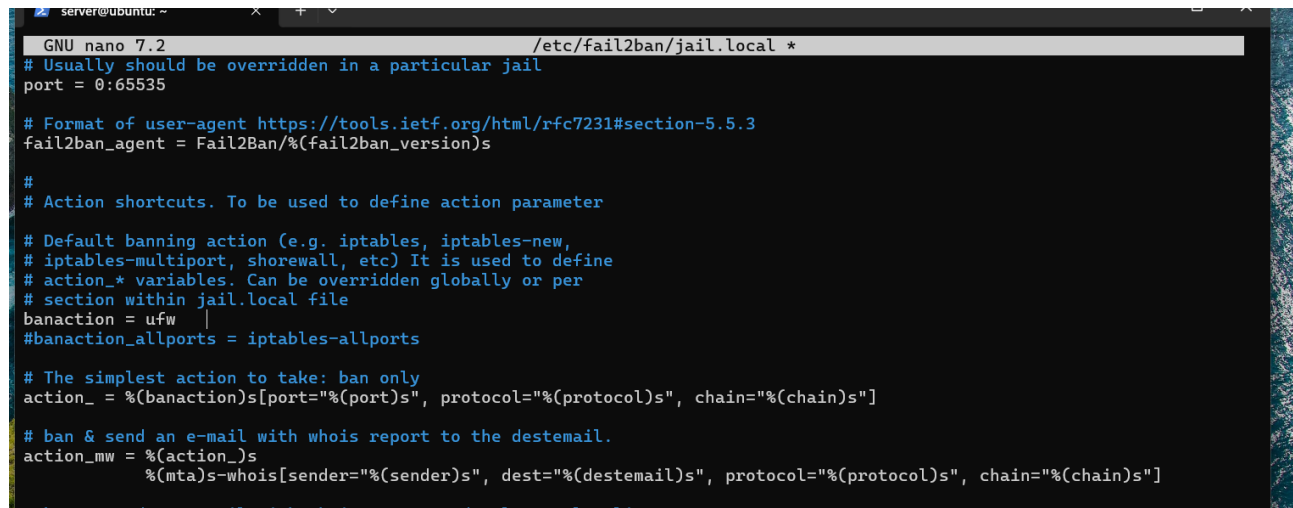
8) verificare con la verbosità lo stato delle regole immesse :

`sudo ufw status verbose`

9) visualizzare gli ip bannati :

`sudo fail2ban-client status sshd`

10) configurazione di ipv6 ed ipv4 per i ban, togliendo iptables perché lavoriamo su ufw :



```
GNU nano 7.2 /etc/fail2ban/jail.local *
# Usually should be overridden in a particular jail
port = 0:65535

# Format of user-agent https://tools.ietf.org/html/rfc7231#section-5.5.3
fail2ban_agent = Fail2Ban/(fail2ban_version)s

#
# Action shortcuts. To be used to define action parameter
#
# Default banning action (e.g. iptables, iptables-new,
# iptables-multiport, shorewall, etc) It is used to define
# action_* variables. Can be overridden globally or per
# section within jail.local file
banaction = ufw
#banaction_allports = iptables-allports

# The simplest action to take: ban only
action_ = %(banaction)s[port=%(port)s", protocol=%(protocol)s", chain=%(chain)s"]

# ban & send an e-mail with whois report to the destemail.
action_mw = %(action_)s
            %(mta)s-whois[sender=%(sender)s", dest=%(destemail)s", protocol=%(protocol)s", chain=%(chain)s"]

# ban & send an e-mail with whois report and relevant log lines
```

fail2ban per myadmin e apache2

installazione apache2 e configurazione:

`sudo apt install apache2`

attivazione servizi :

`sudo systemctl start apache2`

`sudo systemctl status apache2`

`sudo systemctl enable apache2`

accertarsi che funzioni :

<http://192.168.1.55/>

installazione mysql / phpmyadmin:

`sudo apt install mysql-server -y`

`sudo systemctl start mysql`

`sudo systemctl enable mysql`

installazione :

`sudo apt install phpmyadmin -y`

creare un link simbolico nel server web Apache per poterlo accedere facilmente via browser:

1) `sudo ln -s /usr/share/phpmyadmin /var/www/html/phpmyadmin`

2) `sudo systemctl restart apache2`

accesso al browser :

<http://192.168.1.55/phpmyadmin>

creazione database mysql :

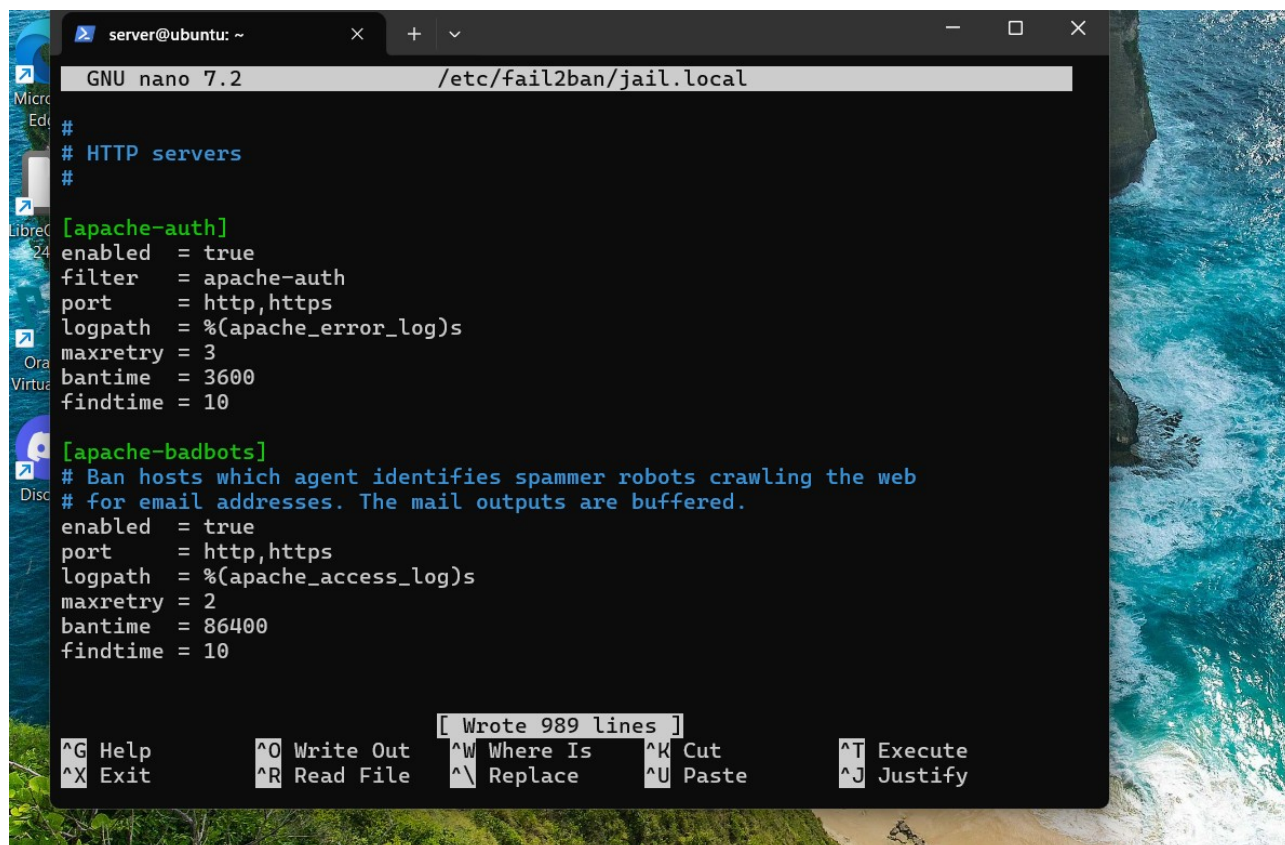
1) `sudo mysql -u root -p`

2) `CREATE DATABASE ilmiodatabasecillone;`

- 3) CREATE USER 'alessandro'@'localhost' IDENTIFIED BY 'passwordforte';
- 4) GRANT ALL PRIVILEGES ON ilmiodatabasecillone.* TO 'alessandro'@'localhost';
- 5) FLUSH PRIVILEGES;

ora immettere le regole jail su fail2ban :

1) regola apache2 :



```

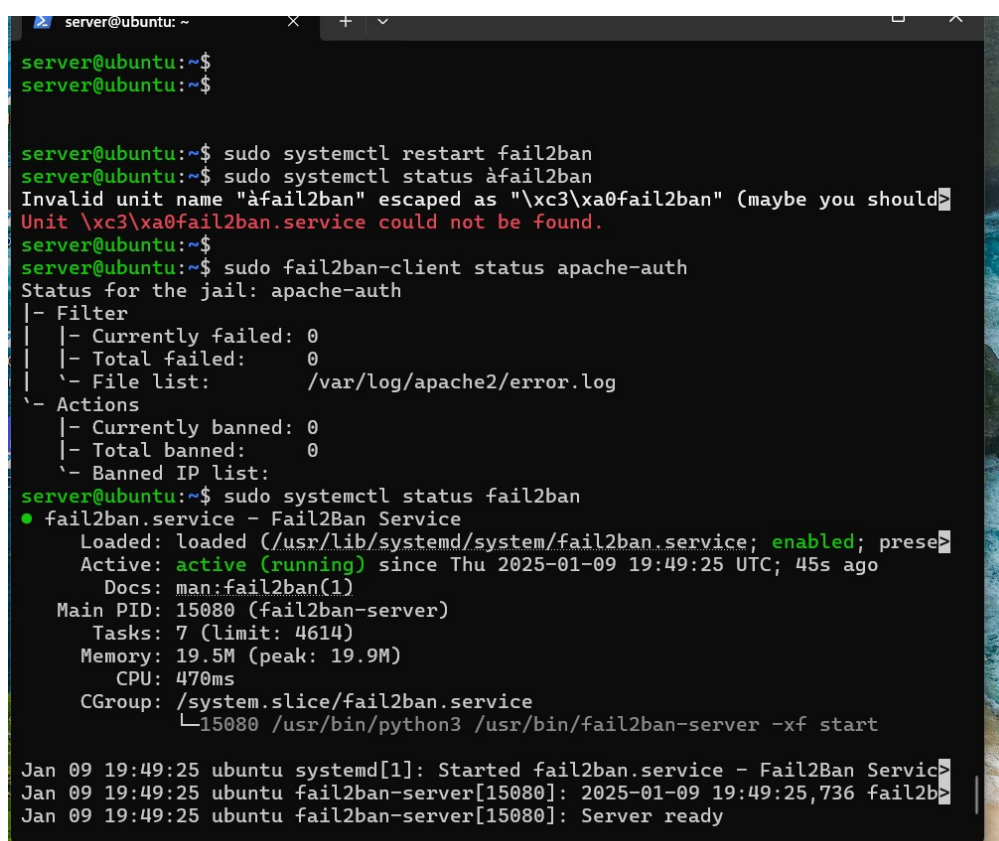
server@ubuntu: ~
GNU nano 7.2 /etc/fail2ban/jail.local

#
# HTTP servers
#

[apache-auth]
enabled = true
filter = apache-auth
port = http,https
logpath = %(apache_error_log)s
maxretry = 3
bantime = 3600
findtime = 10

[apache-badbots]
# Ban hosts which agent identifies spammer robots crawling the web
# for email addresses. The mail outputs are buffered.
enabled = true
port = http,https
logpath = %(apache_access_log)s
maxretry = 2
bantime = 86400
findtime = 10

[ Wrote 989 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
  
```



```

server@ubuntu:~$
server@ubuntu:~$

server@ubuntu:~$ sudo systemctl restart fail2ban
server@ubuntu:~$ sudo systemctl status fail2ban
Invalid unit name "fail2ban" escaped as "\xc3\xa0fail2ban" (maybe you should
Unit \xc3\xa0fail2ban.service could not be found.
server@ubuntu:~$
server@ubuntu:~$ sudo fail2ban-client status apache-auth
Status for the jail: apache-auth
|- Filter
|  |- Currently failed: 0
|  |- Total failed: 0
|  \- File list: /var/log/apache2/error.log
\-- Actions
    |- Currently banned: 0
    |- Total banned: 0
    \- Banned IP list:
server@ubuntu:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; prese
   Active: active (running) since Thu 2025-01-09 19:49:25 UTC; 45s ago
     Docs: man:fail2ban(1)
   Main PID: 15080 (fail2ban-server)
      Tasks: 7 (limit: 4614)
     Memory: 19.5M (peak: 19.9M)
          CPU: 470ms
    CGroup: /system.slice/fail2ban.service
            └─15080 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jan 09 19:49:25 ubuntu systemd[1]: Started fail2ban.service - Fail2Ban Servic
Jan 09 19:49:25 ubuntu fail2ban-server[15080]: 2025-01-09 19:49:25,736 fail2b
Jan 09 19:49:25 ubuntu fail2ban-server[15080]: Server ready
  
```

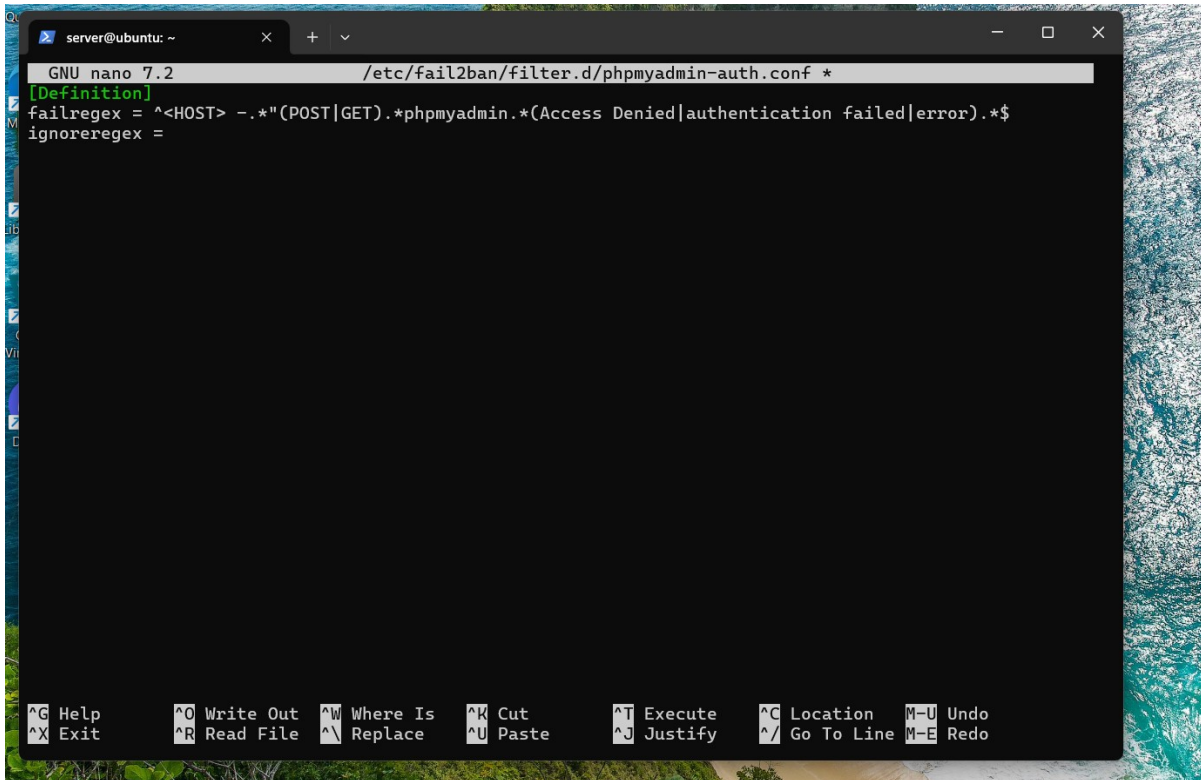

regola phpmyadmin :

```
[phpmyadmin-syslog]
enabled = true
port     = http,https
logpath  = %(syslog_authpriv)s
backend  = %(syslog_backend)s
filter   = phpmyadmin-syslog
bantime  = 4h
findtime = 10
maxretry = 3
```

prova testata :

```
Jan 09 20:03:06 ubuntu systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jan 09 20:03:06 ubuntu fail2ban-server[15225]: 2025-01-09 20:03:06,167 fail2ban.configreader [15225]
Jan 09 20:03:06 ubuntu fail2ban-server[15225]: Server ready
server@ubuntu:~$ sudo fail2ban-client status phpmyadmin-syslog
Status for the jail: phpmyadmin-syslog
|- Filter
| |- Currently failed: 0
| |- Total failed:    1
| \- File list:       /var/log/auth.log
\-- Actions
   |- Currently banned: 1
   |- Total banned:    1
   \- Banned IP list:   192.168.1.40
server@ubuntu:~$
```

creazione di una definizione dettagliata nell'elencare un ban :



The image shows a terminal window with a dark background. At the top, the window title is "server@ubuntu: ~". Below it, the nano text editor is open, editing the file "/etc/fail2ban/filter.d/phpmyadmin-auth.conf". The editor's status bar at the top indicates "GNU nano 7.2" and the file path. The main content area shows the following configuration:

```
[Definition]
failregex = ^<HOST> -.*(POST|GET).*phpmyadmin.*(Access Denied|authentication failed|error).*$
ignoreregex =
```

At the bottom of the terminal, there is a row of keyboard shortcuts for nano:

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location	M-U Undo
^X Exit	^R Read File	^N Replace	^U Paste	^J Justify	^_ Go To Line	M-E Redo