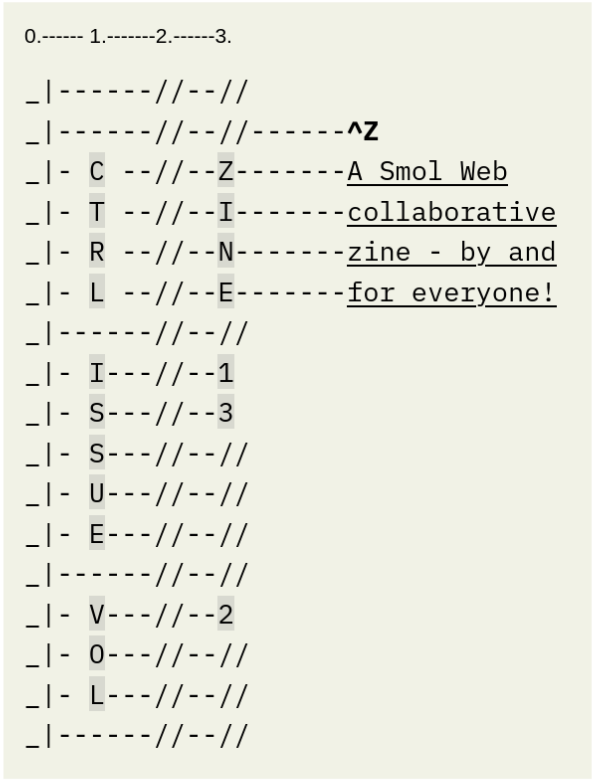


```
2024-02-04 13:37:30,946 fail2ban.filtersystemd  [97557]: INFO     [sshd] Added
journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2024-02-04 13:37:30,946 fail2ban.filter         [97557]: INFO     maxRetry: 5
2024-02-04 13:37:30,946 fail2ban.filter         [97557]: INFO     findtime:
600
2024-02-04 13:37:30,946 fail2ban.actions        [97557]: INFO     banTime: 600
2024-02-04 13:37:30,946 fail2ban.filter         [97557]: INFO     encoding:
UTF-8
2024-02-04 13:37:30,953 fail2ban.jail           [97557]: INFO     Jail 'sshd'
started
2024-02-04 13:37:31,156 fail2ban.filter         [97557]: INFO     [sshd] Found
218.92.0.31 - 2024-02-05 06:35:41
[...]
2024-02-04 13:37:31,194 fail2ban.filtersystemd  [97557]: INFO     [sshd] Jail
is in operation now (process new journal entries)
2024-02-04 13:37:31,553 fail2ban.actions        [97557]: NOTICE   [sshd] Ban
218.92.0.31
2024-02-04 13:37:31,582 fail2ban.actions        [97557]: NOTICE   [sshd] Ban
118.193.35.41
2024-02-04 13:37:31,591 fail2ban.actions        [97557]: NOTICE   [sshd] Ban
103.119.3.178
2024-02-04 13:37:31,599 fail2ban.actions        [97557]: NOTICE   [sshd] Ban
180.101.88.201
2024-02-04 13:37:31,608 fail2ban.actions        [97557]: NOTICE   [sshd] Ban
218.92.0.118
2024-02-04 13:37:31,617 fail2ban.actions        [97557]: NOTICE   [sshd] Ban
103.236.192.222
```

On the example server Fail2Ban didn't wait long to start banning bad actors. If you don't have any activity in your log, test by attempting to SSH in from another system to an invalid username.

Updating Time Zone Information (Optional)

Check Current Time Zone

Use the `timedatectl` command to check the current time zone.

shell-session

Mid-2009: YouTubers are annoying, musicians should put music videos on YouTube, MTV should have music videos again, Retweets should be a feature, not a manual task, celebrities are dumb. Look at this stupid celebrity! Oh my God, so and so celebrity responded to me! <3

2010: Taylor Swift is extremely popular. Twitter is extremely popular. Did you hear Facebook has 1 billion members now? Will Twitter get that big? Fail Whale. Twitter should host video. Which Twitter app do do use? Android or iPhone? BOO!, either way.

2011: Man, everybody is a hipster. Gotye is great. Adele is great. YouTube musicians are great. Glad some artists have videos on YouTube now. So and so blog is becoming a book? Cool! So and so blog got bought out and is being retired? Not cool! People can jus Tweet news stories now, no need to have publications.

2012: Shit, ads. Why is my Timeline no longer chronological? No one has responded in a while. Do celebrities just NOT talk to anyone anymore?

2013: Wow, this journalist has more followers than this Oscar nominee! Let's LiveTweet The Oscars! Let's LiveTweet ALL the big events and shows! Cambridge Analytica? Yea I heard of it - glad I don't use Facebook. Snowden was right, I suppose.

Early-2014: Look at these segments of Twitter - politics Twitter, technology Twitter, Infosec Twitter, YouTube Twitter - so many things going on, still...

Late-2014: BLM. This world is unjust. So many people documenting everything - everything is on video, everything vulnerable. Hope things work out.

INTRO

And here we are!

We made it - Volume 2, Issue 13. One full year of Ctrl-ZINE! Amazing we kept it going this long (and longer) :)

^C has been amazing. As is the Smol Web. Where the large/main Web as a whole was (is) once disregarded as "cluttered" by some (me, certainly), it is now something to take apprehension to to do simple things. I love companies, ambition, new products - but JS crushing Web sites, pop-ups, newsletters, and data load lead me to just opt opposite.

The Smol Web gives me a place to *be* that opposite. IRC, cli-based activities, nixing boradband for a simple tethering plan through my carrier, slow, slo-fi, deliberate use of technology, as well as a near analog lifestyle away from the computer - my mind stays clear, I focus on what matters - ME!

I hope all take care to do the same.

Issue 13 brings two entries - one from me and one from basilmori. Rushed and busy this month, the zine is smaller than previous issues. More next time.

Punch in to this issue, share (and Sharealike). Happy, free, ambiguous, principled.

Your compiler,

~loghead

2015: New Media Twitter, Content Creator Twitter, Journalism Twitter, Meme Account Twitter, anyone who does anything that garners a Verified badge Twitter – the pendulum has swung. Twitter and it's Internet superiority has won. The World Wide Web of Twitter – cancel your phone number, give them your Twitter handle, instead.

Early-2016: Trump? President? Pfff! His show sucked, he'll die of a cocaine overdose before he manages to get nominated. Have you read the news anyway? Then entire Western world “knows” Hilary will win, so...

Late-2016: Oh. His ego will likely be gratified now that he has high office. A sane approach to politics, perhaps? In honor of the sacred seat of office of the POTUS? No? Ok. Hey, where did my Twitter Timeline go? Hundreds of them left!

2017, 2018: Trump, everything sucks, news is centralized, people want Instagram for sanity, Twitter can/should be good, but f** Twitter

2019: Ffs I have to leave Twitter. Account closed. Re-opened. Account closed and obscured password so I don't remember it. Recover via e-mail. I am too addicted to this shit. I will die of depression if I do not leave Twitter. Closing account now, Sept 1 2019.

The End

And it was, I haven't been back since then. That's a decade recap of things happening when I could have been doing better things.

Here's to tiny blogs, the Smol Web and real communities!

```
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset:
enabled)
     Active: active (running) since Mon 2024-02-04 13:37:30 UTC; 11s ago
     Docs: man:fail2ban(1)
   Main PID: 97557 (fail2ban-server)
     Tasks: 5 (limit: 1092)
     Memory: 33.6M
     CPU: 530ms
     CGroup: /system.slice/fail2ban.service
           └─97557 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Feb 04 13:37:30 example systemd[1]: Started fail2ban.service - Fail2Ban
Service.
Feb 04 13:37:30 example fail2ban-server[97557]: 2024-02-04 13:37:30,660
fail2ban.configreader   [97557]: WARNING 'allow>
Feb 04 13:37:30 example fail2ban-server[97557]: Server ready
```

Fail2Ban is running. Now, `tail` the log to watch activity and make sure it's reacting to intrusion attempts.

```
shell-session
guide@example:~$ sudo tail -f /var/log/fail2ban.log
2024-02-04 13:37:30,691 fail2ban.server         [97557]: INFO
--------------------------------------------------
2024-02-04 13:37:30,691 fail2ban.server         [97557]: INFO     Starting
Fail2ban v1.0.2
2024-02-04 13:37:30,692 fail2ban.observer       [97557]: INFO     Observer
start...
2024-02-04 13:37:30,697 fail2ban.database       [97557]: INFO     Connected to
fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2024-02-04 13:37:30,700 fail2ban.database       [97557]: WARNING New database
created. Version '4'
2024-02-04 13:37:30,700 fail2ban.jail           [97557]: INFO     Creating new
jail 'sshd'
2024-02-04 13:37:30,929 fail2ban.jail           [97557]: INFO     Jail 'sshd'
uses systemd {}
2024-02-04 13:37:30,930 fail2ban.jail           [97557]: INFO     Initiated
'systemd' backend
2024-02-04 13:37:30,931 fail2ban.filter         [97557]: INFO     maxLines: 1
```

INDEX:


```
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local
file.
# See man 5 jail.conf for details.
#
guide@example:~$
```

Create and edit `/etc/fail2ban/jail.local` with `sudo nano /etc/fail2ban/jail.local` so that it looks like the following.

```
systemd
[DEFAULT]
backend = systemd
# Fixes: ERROR Failed during configuration: Have not found any log file for
sshd jail

[Definition]
allowipv6 = true
# Fixes: WARNING 'allowipv6' not defined in 'Definition'. Using default one:
'auto'

[sshd]
enabled = true
# Enables the SSH jail.
```

If you install software in later guides, you may need to update `/etc/fail2ban/jail.local` with additional configuration information.

Finishing Up

Start the server and check the status.

```
shell-session
guide@example:~$ sudo systemctl start fail2ban
guide@example:~$ sudo systemctl status fail2ban
```

Setting up a Debian 12 VPS by *kmc*

This guide will walk you through initial configuration and securing of a Debian 12 VPS. The guide is written for someone familiar with connecting via SSH and command lines. If you're unsure of a concept, please consult your vendor's documentation and technical support.

Change Root Password

Log in to the root account. Your provider will either prompt you for, or generate a root password during VPS creation. Immediately change this to a different strong password after logging in with the `passwd` command.

```
shell-session
Linux example 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1
(2023-12-30) x86_64

The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@example:~# passwd
New password:
Retype new password:
passwd: password updated successfully
root@example:~#
```

Update Software

Old Things by *~basilmori*

I love owning old devices.

In many ways, they're no longer relevant,
These bygone relics of an era long past,
Whether that era was a decade ago or three.
Once electronic masterpieces of their time,
Now they're little more than novelties.
Collector's items, of little practical use.

You usually don't need to own old devices.
New devices can do everything they once did.
So powerful are these new computers of ours
That they can simulate them down to circuits
And do everything which once was brand new,
And which made the old device so exciting.

But the older devices have a magic to them.
They're coarser. Focused. Not like the new,
Ever more powerful, ever finding fresh uses,
Bringing together a lifetime of new inventions
Into simulating a lifetime of old inventions
And doing everything we could ever want.

They used to be the new devices, of course.
But they felt something different at the time.
These old machines, with less power or polish,
Had to do more with what they were given,
And often had to pretend they were better for it.
It gave them character, and made them unique.

I like to use my old devices to do old things.
A computer built for writing and nothing else,
Unable to open a modern website without slowing,

And there it is - the start of Volume 2!

Zines, community, ups, downs, everywheres (ha), it’s all in fun and game

Remember to tip your local devs, start a small site, or delete your site ;)

Credit Blacklisted 411 magazine for inspiration to start ^Z, credit to all who continue to contribute, who continue to read.

Stay well!

~loghead

Your next immediate step is to check and update software with `apt update && apt upgrade` to make sure the most recently available security patches are applied.

```
shell-session
root@example:~# apt update && apt upgrade
Hit:1 https://dl.example.com/debian universal InRelease
Hit:2 https://deb.debian.org/debian bookworm InRelease
Get:3 https://deb.debian.org/debian-security bookworm-security InRelease [48.0
kB]
Get:4 https://deb.debian.org/debian bookworm-updates InRelease [52.1 kB]
Hit:5 https://dl.example.com/debian bookworm InRelease
Get:6 https://deb.debian.org/debian-security bookworm-security/main Sources
[73.0 kB]
Get:7 https://deb.debian.org/debian-security bookworm-security/main amd64
Packages [134 kB]
Fetched 307 kB in 1s (421 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@example:~#
```

The example machine is up to date.

Uncomplicated Firewall (UFW)

Debian 12 installs UFW by default. For this guide, you are only using SSH and that is all you should allow with `ufw`. Review the rules currently in effect with `ufw status`.

```
shell-session
root@example:~# ufw status
Status: active
```

```
Feb 04 13:12:27 example fail2ban-server[92217]: 2024-02-04 13:12:27,178
fail2ban                [92217]: ERROR   Failed during configuration: Have not
found any log file for sshd jail
Feb 04 13:12:27 example fail2ban-server[92217]: 2024-02-04 13:12:27,185
fail2ban                [92217]: ERROR   Async configuration of server failed
Feb 04 13:12:27 example systemd[1]: fail2ban.service: Main process exited,
code=exited, status=255/EXCEPTION
Feb 04 13:12:27 example systemd[1]: fail2ban.service: Failed with result
'exit-code'.
guide@example:~$
```

Your First Error

The errors relate to Debian 12's migration from plaintext log files to a centralized journal maintained by `journald`. Fail2Ban can't start because it expects log files that aren't there. You'll fix that in the configuration.

Configuration

Review Fail2Ban's configuration first. Fail2Ban stores its default configuration in `/etc/fail2ban/jail.conf`. Don't edit it directly. The beginning of `jail.conf` tells you why.

```
shell-session
guide@example:~$ head /etc/fail2ban/jail.conf -n 19
#
# WARNING: heavily refactored in 0.9.0 release.  Please review and
#          customize settings for your setup.
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in jail.local file,
#           or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
```

Execute the `timedatectl` command again to verify the time zone is set correctly.

```
shell-session
guide@example:~$ timedatectl
           Local time: Tue 2024-02-06 21:20:23 MST
           Universal time: Wed 2024-02-07 04:20:23 UTC
                 RTC time: Wed 2024-02-07 04:20:23
           Time zone: US/Mountain (MST, -0700)
System clock synchronized: yes
           NTP service: n/a
      RTC in local TZ: no
guide@example:~$
```

The example system's time zone is now set to US/Mountain.

Conclusion

Congratulations! You have configured and secured a Debian 12 VPS. You now have a strong base to build out your desired system.

OUTRO

```
The following additional packages will be installed:
  python3-pyinotify python3-systemd whois
Suggested packages:
  mailx system-log-daemon monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify python3-systemd whois
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 589 kB of archives.
After this operation, 2,901 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 https://deb.debian.org/debian bookworm/main amd64 fail2ban all 1.0.2-2
[451 kB]
[...]
Processing triggers for man-db (2.11.2-2) ...
guide@example:~$
```

By default, Fail2Ban should start upon installation. Check that with `sudo systemctl status fail2ban`.

```
shell-session
guide@example:~$ sudo systemctl status fail2ban
× fail2ban.service - Fail2Ban Service
      Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset:
enabled)
      Active: failed (Result: exit-code) since Sun 2024-02-04 13:12:27 UTC;
3min 39s ago
   Duration: 238ms
      Docs: man:fail2ban(1)
      Process: 92217 ExecStart=/usr/bin/fail2ban-server -xf start
(code=exited, status=255/EXCEPTION)
   Main PID: 92217 (code=exited, status=255/EXCEPTION)
      CPU: 107ms

Feb 04 13:12:26 example systemd[1]: Started fail2ban.service - Fail2Ban
Service.
Feb 04 13:12:27 example fail2ban-server[92217]: 2024-02-04 13:12:27,155
fail2ban.configreader   [92217]: WARNING 'allowipv6' not defined in
'Definition'. Using default one: 'auto'
```

Feels better for writing than my fancy new one.
And the older games, I feel, are always more fun
When they're being held back by the old hardware.

We still make old devices today, sometimes.
We don't realize, because they aren't old yet.
But when you build a device made to do one thing,
A little underpowered, maybe with older hardware,
Designed with features that are a little bit odd,
It'll be remembered enough to one day become old.

```
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

root@example:~#
```

SSH and nothing else is currently configured in `ufw`. You will notice `Status: active`. That means `ufw` is already on. If it had said `Status: inactive` you would turn it on with `ufw enable`. If you install software in later guides, you may need to update UFW's rules.

Create User Account and Grant Sudo Privileges

Now create your user account with `adduser [username]`. You will be doing your administrative tasks from your user account after this. Following the Principle of Least Privilege (PoLP), users and processes should have the bare minimum privileges required to perform their function.

```
shell-session
root@example:~# adduser guide
Adding user `guide' ...
Adding new group `guide' (1001) ...
Adding new user `guide' (1001) with group `guide (1001)' ...
Creating home directory `/home/guide' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for guide
Enter the new value, or press ENTER for the default
      Full Name []:
      Room Number []:
      Work Phone []:
      Home Phone []:
```

Flipping The Bird - *~loghead*

(a Twitter prevailing narrative (as I saw it) mid-2009 - late-2019)

Mmm, I remember AOL chats in 1998. Talk about a dopamine rich adrenaline rush every time I say at my PC w/ espresso in hand! It was game time - everyone. Everywhere. Let's chat and party!

Se La Vie AOL

Enter Twitter, 2009. I refrained from social media until then. MySpace seemed addictive. Facebook looked monstrously lame. Twitter, “let's try it out”, I thought.

A few moments in and I knew if be there a min (a min being a decade). People talking, celebrities talking. Celebrities talking TO ME! (WTF?!) And not like a popular Twitch streamer, I mean like a celebrity I just watched on HBO the night before. “What was this world?”

So after jamming it up on the new-New Media platform for a while, I realized that I would restart my coffee addiction and caffeine intake. To do a thing it must be done right.

A dusk-lit stroll saw me to the Save a Lot down the road. Starbucks espresso roast purchased. A full coffee filters worth of grounds brewed a mug full, and I began the deep dive to Dopamine Ocean. Tila Tequila (prior to her batshittiness) had a large following, as did Ashton Kurcher and Kat Von D. Tommy Lee of Motley Crue, a few tech journalists, and the litany of gossip bloggers I knew over the years populated my feed.

Here's how it (the narrative) went - in a loose timeline

```
guide@example:~$ timedatectl
           Local time: Wed 2024-02-07 04:11:17 UTC
           Universal time: Wed 2024-02-07 04:11:17 UTC
                 RTC time: Wed 2024-02-07 04:11:17
           Time zone: UTC (UTC, +0000)
System clock synchronized: yes
           NTP service: n/a
       RTC in local TZ: no
```

The clock of the example system is set to the Coordinated Universal Time (UTC).

Find Your Time Zone

Find your time zone by `timedatectl list-timezones` at the command line. A scrollable list of time zones will be shown. Find and note your desired time zone for the next step.

```
shell-session
US/Mountain
```

The example machine's clock will be set to US/Mountain time zone.

Setting the Time Zone

`timedatectl` is used to set the time zone as well. Set the time zone to the one you recorded in the previous step.

```
shell-session
guide@example:~$ sudo timedatectl set-timezone US/Mountain
guide@example:~$
```

Verification

```
      Other []:
Is the information correct? [Y/n] Y
Adding new user `guide' to supplemental / extra groups `users' ...
Adding user `guide' to group `users' ...
root@example:~#
```

Now add your user to the `sudo` group so they can run administrative commands with `usermod`.

```
shell-session
root@example:~# usermod -aG sudo guide
root@example:~#
```

The `usermod` command only outputs a message if it fails. It's time to log out as root.

```
shell-session
root@example:~# logout
Connection to example.org closed.
```

It's important that you have your newly created user log in to remove root's access in the next step. Logging in and disabling root's SSH login with your user ensures you're able to fix any errors related to that account before you lock yourself out.

Disable Root Login

It's time to disable root's ability to log in via SSH. You'll be editing `/etc/ssh/sshd_config` with the text editor of your choice. By default Debian installs `nano` and `vim`.

```
shell-session
guide@example:~$ sudo nano /etc/ssh/sshd_config
```

Find the line that says `PermitRootLogin yes`. Change this line to `PermitRootLogin no`. Save and exit from your text editor.

Restart the SSH service to make sure the that change takes effect with `sudo systemctl restart ssh`.

Trying to log to to the root account via SSH to the shell machine should now fail.

```
shell-session
guide@localhost:~$ ssh root@example.org
root@example.org password:
Permission denied, please try again.
root@example.org password:
Permission denied, please try again.
root@example.orgs password:
root@example.org Permission denied (publickey,password).
guide@localhost:~$
```

Installing and Configuring Fail2Ban

Fail2Ban prevents intrusions by monitoring the system's logs for authentication or other definable events. This helps prevent brute force attacks. Fail2Ban is highly configurable and as you add additional services you can add rules to protect them. For now, we're just worried about brute force attacks via SSH.

Installation

First, install Fail2Ban. It has dependencies which apt, the package manager, detects and automatically installs.

```
shell-session
guide@example:~$ sudo apt install fail2ban
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```