Using Fedora CoreOS to Ship Your FOSS Project

You can easily self-host your projects!

Who am I...

- Joe Doss (jdoss)
- 23 year Linux user
- Fedora package maintainer and Fedora Cloud / CoreOS SIG member
- Former Director of Engineering Operations at Kenna Security, Inc (now Cisco)
- Principal Systems Architect at Forem (FOSS software behind dev.to)

And what is Forem?

- FOSS for building communities
  - https://github.com/forem/forem
  - 17k+ Stars on GitHub
  - Powers dev.to
- Monolithic Ruby application
  - Puma
  - Sidekiq
- Requirements
  - PostgreSQL
  - Redis
  - imgproxy
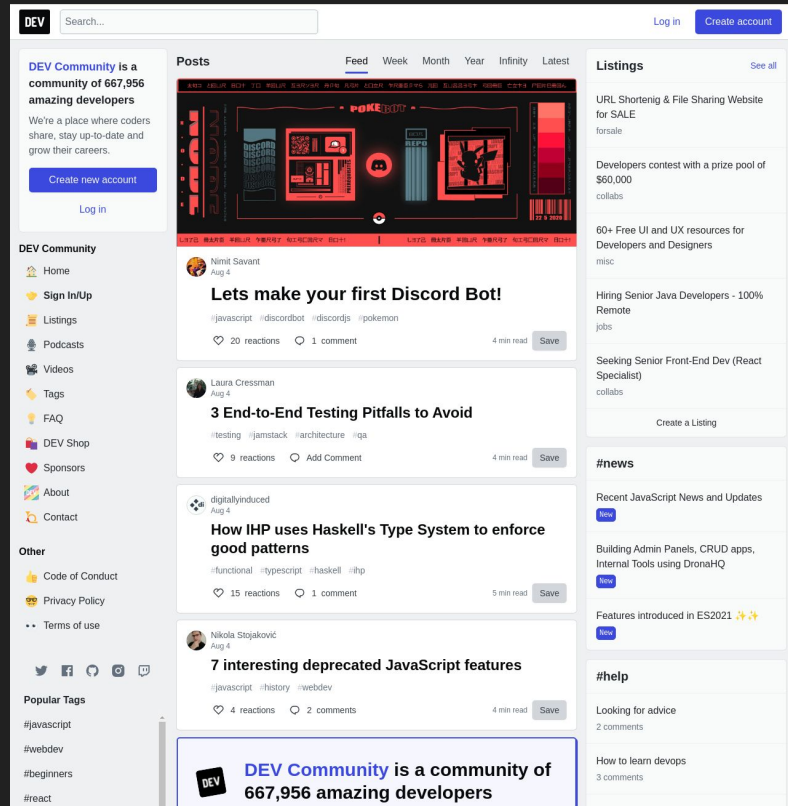
Forem Self-Host Goals

- Affordable
- Provider agnostic
- Reproducible deployments
- Easy to deploy/update Forem code
- Safe updates for the underlying OS
- Modern tooling but not Enterprise tooling (but... why not k8s???)
- Features from Forem Cloud easy to translate to Self-Host (and vice versa)
- Not a bunch of services shoved into a single container
- More than just the code

Why Fedora CoreOS?

- Immutable
- Secure
- Container Centric
- Rolling Release
- Updates and Rollbacks
- Define configuration at boot
- Modern system tooling
  - systemd
  - Podman
- Great cloud provider coverage
- Bare metal support

Forem Self-Host Repo

- FCOS Ansible Role
- Butane Ansible Role
- Three different Cloud provider playbooks
  - DigitalOcean
  - AWS
  - Google Compute
- QEMU Playbook for local development
- Butane Template for setting up Forem
  - systemd-oomd
  - swap-on-zram
  - Python 3 support
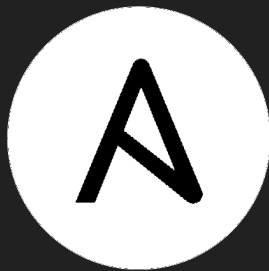
Ansible

The rubber stamp

```yaml
---
all:
  hosts:
  vars:
    ssh_key: "{{ lookup('file', '~/.ssh/forem.pub') }}"
    app_protocol: https://
    database_pool_size: 10
    force_ssl_in_rails: "true"
    lang: en_US.UTF-8
    node_env: "{{ forem_environment }}"
    rack_env: "{{ forem_environment }}"
    rack_timeout_service_timeout: 300
    rack_timeout_wait_timeout: 300
    rails_env: "{{ forem_environment }}"
    rails_log_to_stdout: "true"
    rails_serve_static_files: enabled
    redis_sessions_url: redis://localhost:6379
    redis_sidekiq_url: redis://localhost:6379
    redis_url: redis://localhost:6379
    session_expiry_seconds: 1209600
    web_concurrency: 2
    forem_context: selfhost
    forem_container_tag: quay.io/forem/forem:latest
  children:
    forem:
      hosts:
        example:
          ansible_connection: local
          ansible_python_interpreter: /usr/bin/python3
          forem_domain_name: forem.wtf
          forem_subdomain_name: community
          forem_server_hostname: forem
          default_email: systems@forem.com
          app_domain: "{{ forem_subdomain_name }}.{{ forem_domain_name }}"
          secret_key_base: "{{ vault_secret_key_base }}"
          session_key: _FOREMSELFHOST_Session
          imgproxy_key: "{{ vault_imgproxy_key }}"
          imgproxy_salt: "{{ vault_imgproxy_salt }}"
          forem_version: latest
          forem_environment: production
          dd_api_key: "{{ vault_dd_api_key }}"
          honeybadger_api_key: "{{ vault_honeybadger_api_key }}"
          honeybadger_js_api_key: "{{ vault_honeybadger_js_api_key }}"
          honeycomb_api_key: "{{ vault_honeycomb_api_key }}"
          postgres_user: forem_production
          postgres_password: "{{ vault_forem_postgres_password }}"
          postgres_host: localhost
          pusher_app_id: "{{ vault_pusher_app_id }}"
          pusher_beams_id: "{{ vault_pusher_beams_id }}"
          pusher_beams_key: "{{ vault_pusher_beams_key }}"
          pusher_cluster: us2
          pusher_key: "{{ vault_pusher_key }}"
          pusher_secret: "{{ vault_pusher_secret }}"
```

Butane / Ignition

Configuration on boot!

```yaml
1  variant: fcos
2  version: 1.3.0
3  passwd:
4    users:
5      - name: core
6        ssh_authorized_keys:
7          - ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPekWj19MJiQ0iZLS9ed6Fq7TI52FcNWm
8
9  storage:
10   directories:
11     - path: /opt/ansible
12       mode: 0755
13
14     - path: /opt/forem/envs
15       mode: 0750
16
17     - path: /opt/forem/configs
18       mode: 0750
19
20     - path: /opt/forem/data
21       mode: 0750
22
23     - path: /opt/forem/data/postgresql
24       mode: 0750
25
26     - path: /opt/forem/data/redis
27       mode: 0750
28
29     - path: /opt/forem/data/uploads
30       mode: 0750
31
32     - path: /opt/forem/configs/traefik
33       mode: 0750
34
35     - path: /opt/forem/tmp
36       mode: 0755
37
```

```json
1 {"ignition":{"config":{"replace":{"compression":"gzip","source":"
  data:;base64,H4sIAAAAAAAC/+y8abOb2LI2+Fd2u9vRH3S2mafqcEQjJoEQIAYx3H2iLqOYZxBw4
  /z3jj3YtT1UlX3sevu9N8ofLG3IXCtXDg+5ciV6818Pb7JrnY1ZUz+8+eW/
  Ht7McT88//HwBnkHvwMf3vzrHw9vWn8YbtEzyTTE/fDw5pf/+K+HN7VfxU+0YdPHD2/+8fBmGGFJ6Gt
  Omz7Y40sbrE+XT5fs4gjEMou5omqYZRNl8Bio9VoQUk8Mer41aXNg5RJ2k7AxmnmxQcYTzHWGKGMyHil
  1VkYYkh2uCE9Rd3sT/79CUWeRHVVa/C5vq4c0///XPR2GHsen9a/wsbZT1cTg2fRZ/kLn1x/
  RJZqBpR8Cvhywon2WvmuiRC6WQf/3jC8Kk6eMKi0t5+ISWJH+XNmzqJLt+M3nkj/
  730AJtM4zXPh668rvY+jjKvksoYGrLxo++d93A2PtxkhXfyjZW7edW+Oc/
  Ht4kWfkV08Vj+MI2xP2chfEAvLjus5hhU49xPQ7PThA2VdvHw0fPvm7Z81xDM/Xhswc/rvSX/
  yfwhxhH/3FAB5F+/scA6KaBVs+e9gaNJgO5qaVxNpyrHl1yJuhgSS5Vl1XdvE0dnLiVeE2D0d65Ulc
  60RDAtB0EuI7TYa5VhRj3AxW0LRkTObiE4hC1h7av13bRYW6tqsy5ZU2UjK7WO5tOwksf5qRBhlqcILz
  qdpsY8ygS6Q5hufE0+lfATRTUiuKVuHDlaXdirLI1WbRjyMUUFBFPW1vkLMAVkvM0wN4Y5OfMqMsmM0W
  ByHg7z01UUnZzxrhwdNodeEu5ELSh3Tia1gDgapmJW9z2NE2/
  f0aCD9aBwd815EcM+cIOn6v7H4yqmLSocPpbhO0mf32XNW9h/mmYj58IXfpjPIxvQfpPRRHh0imGKmr
  gf3kXPwvx0Z8CN89l+dIY9T201LysTg3Yo63QphFuBtdSuuHeVc3ngRpmbO4PuFeI8KSzGnjfjJiDzlP
```

systemd + podman

A "not terrible" way to run services

```
976  - name: forem-rails.service
977    enabled: true
978    contents: |
979      [Unit]
980      Description=Forem Rails Service
981      Wants=network.target
982      After=network-online.target
983      Wants=forem-openresty.service
984      BindsTo=forem-pod.service forem.service
985      After=forem-pod.service forem.service forem-postgresql.service forem-redis.s
986      Before=forem-openresty.service
987
988      [Service]
989      LimitNOFILE=1048576
990      Environment=PODMAN_SYSTEMD_UNIT=%n
991      Restart=on-failure
992      RestartSec=30
993      TimeoutStartSec=600
994      ExecStartPre=/usr/bin/podman image exists localhost/forem/forem:current
995      ExecStartPre=/usr/bin/podman run \
996        --name forem-rails-bootstrap \
997        --pod forem-pod \
998        --log-driver journald \
999        --replace --rm \
1000       --sdnotify ignore \
1001       --env-file /opt/forem/envs/rails.env \
1002       --volume /opt/forem/data/uploads:/opt/apps/forem/public/uploads:U,z \
1003       localhost/forem/forem:current bootstrap
1004     ExecStart=/usr/bin/podman run \
1005       --name %N \
1006       --pod forem-pod \
1007       --log-driver journald \
1008       --replace --rm -d \
1009       --sdnotify conmon \
1010       --env-file /opt/forem/envs/rails.env \
1011       --volume /opt/forem/data/uploads:/opt/apps/forem/public/uploads:z \
1012       localhost/forem/forem:current
1013     ExecStop=/usr/bin/podman stop -t 10 %N
1014     ExecStopPost=/usr/bin/podman stop -i -t 10 %N
1015     ExecStopPost=/usr/bin/podman rm -i -v %N
1016     Type=notify
1017     NotifyAccess=all
1018     Delegate=true
1019     SyslogIdentifier=%N
1020     Slice=machine-forem-pod.slice
1021
1022     [Install]
1023     WantedBy=multi-user.target default.target
1024
```

"The next five years are going to be full of amazing self-hosted solutions for all sorts of things, pretty excited to see this."

_____

- @deathbypapercut

Self hosting FOSS applications securely and easily is something everyone can do with Fedora CoreOS!

Thanks!

Contact me! or don't…
I am not your sysadmin!

joe@solidadmin.com
twitter.com/jdoss
github.com/jdoss

Super cool URLs…

getfedora.org/en/coreos
github.com/forem/selfhost