



Getting stuff done with



fedora
COREOS

Software Engineer
At Smallstep

Joe Doss



Who am I?

Twitter: [@jdoss](#)

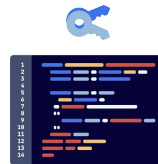
GitHub: [@jdoss](#)

IRC: `jdoss`

joe@solidadmin.com

joedoss.com

Software Engineer, deep in Public Key Infrastructure and making certificates easy at Smallstep



Fedora package maintainer

FCOS and Fedora Cloud SIG member



Longggg time Linux user

I do cool sh*t with FCOS on a daily basis



You know about FCOS.

This talk is all about how to use it to do cool things!



We are gonna chat about...

- Tooling
- Workflows
- Butane design patterns
- Real world use

Take This, It's Dangerous to Go Alone

Tooling

[Bupy](#) – Local development tool with QEMU

[Terraform-provider-ct](#) – Use this in Terraform to convert butane to ignition with template and snippet support.

[Matchbox](#) – PXE server with built in Butane/Ignition support

[Terraform-provider-matchbox](#) – Provider for managing Matchbox in Terraform

[Butane Schema](#) for Editor LSPs

Butane design patterns

- Templates
- Reusable Butane snippets
- Premade systemd units with systemd overrides

My typical workflow...

- 1 Identify what you are trying to build



My typical workflow...

2 Write Butane to define that workload



My typical workflow...

3 Convert to Ignition and launch to test



My typical workflow...

4 Iterate to ideal configuration



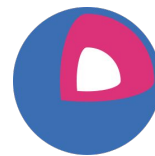
My typical workflow...

5 Deploy to production
(or your basement)



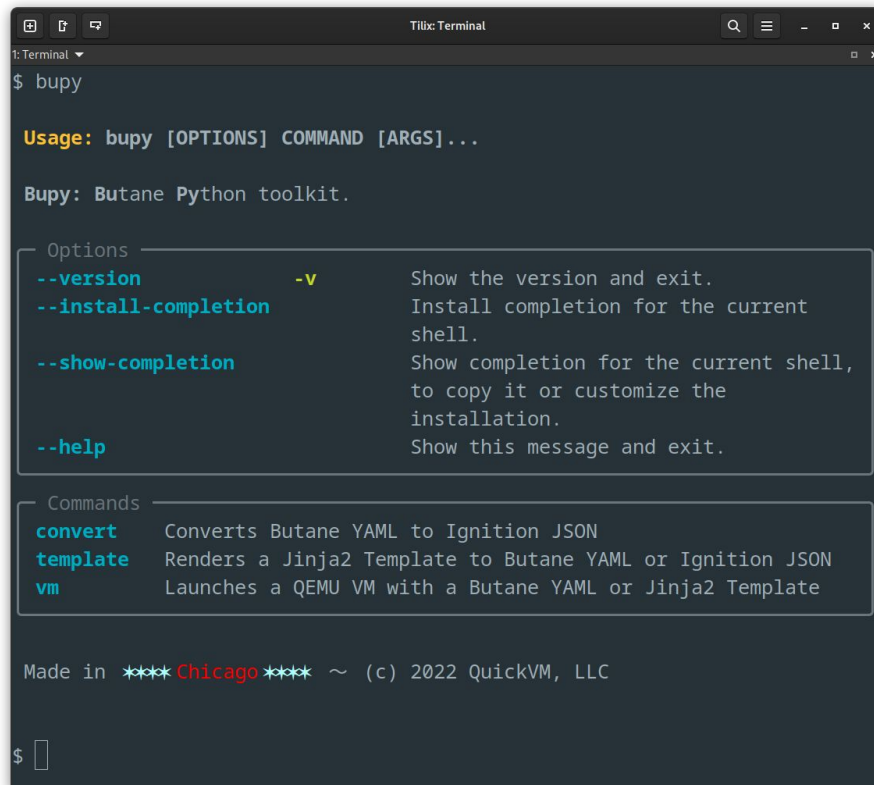
My typical workflow...

6 Back to step 2 if you need to iterate as your workload evolves over time



Bupy

The Butane Python Toolkit
for quickly developing and
testing Butane
configurations.



```
Tilix Terminal
1: Terminal
$ bupy

Usage: bupy [OPTIONS] COMMAND [ARGS]...

Bupy: Butane Python toolkit.

Options
  --version          -v          Show the version and exit.
  --install-completion  Install completion for the current
                             shell.
  --show-completion    Show completion for the current shell,
                             to copy it or customize the
                             installation.
  --help             Show this message and exit.

Commands
  convert  Converts Butane YAML to Ignition JSON
  template Renders a Jinja2 Template to Butane YAML or Ignition JSON
  vm       Launches a QEMU VM with a Butane YAML or Jinja2 Template

Made in ***Chicago*** ~ (c) 2022 QuickVM, LLC

$
```

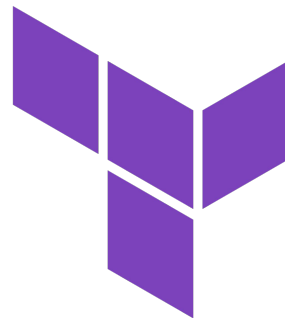
```
<name>: {{ item.name }}  
{{%- if item.groups %}  
    groups:  
{{%- for item in item.groups %}}  
$ head examples/bupyvars.yaml  
---  
passed:  
users:  
- name: core  
sshkey:  
  - ssh-ed25519 AAAAC3NzaC1lZDI1NTU5AAAAEEntTqUp0YDfXkgCEVcbCNzkaI25rjBHIrhdcFKAJH51 bupy@quickvm.com  
  - ssh-ed25519 AAAAC3NzaC1lZDI1NTU58BBBIEntTqUp0YDfXkgCEVcbCNzkaI25rjBHIrhdcFKAJH51 bupy@quickvm.com  
  - sk-ssh-ed25519@openssh.com AAAGnRtLWkzcClIZDi1NTE5QGwZW5zc2guY29tAAAIKLu74gMTQdEs/3Jhq2JIKQPwSUC5UX4AGF22Gr1RDAAAABHWzdDo= jdoos@quickvm.com  
  
- name: bluey  
groups:  
$ bupy template examples/justssh.bu.j2 examples/bupyvars.yaml  
{'ignition': {'version': '3.3.0'}, 'passwd': {'groups': [{'name': 'gooddogs'}, {'name': 'devs'}, {'name': 'managers'}], 'users': [{'name': 'core', 'sshAuthorizedKeys': [\"ssh-ed25519 AAAAC3NzaC1lZDI1NTU5AAAAEEntTqUp0YDfXkgCEVcbCNzkaI25rjBHIrhdcFKAJH51 bupy@quickvm.com\", \"ssh-ed25519 AAAAC3NzaC1lZDI1NTU58BBBIEntTqUp0YDfXkgCEVcbCNzkaI25rjBHIrhdcFKAJH51 bupy@quickvm.com\", \"sk-ssh-ed25519@openssh.com AAAGnRtLWkzcClIZDi1NTE5QGwZW5zc2guY29tAAAIKLu74gMTQdEs/3Jhq2JIKQPwSUC5UX4AGF22Gr1RDAAAABHWzdDo=jdoos@quickvm.com\"]}, {'groups': ['sudo', 'wheel', 'gooddogs'], 'name': 'bluey', 'sshAuthorizedKeys': [\"ssh-ed25519 AAAAC3NzaC1lZDI1NTU5AAAAEEntTqUp0YDfXkgCEVcbCNzkaI25rjBHIrhdcFKAJH51 bupy@quickvm.com\"]}], 'groups': ['gooddogs'], 'name': 'bingo', 'sshAuthorizedKeys': [\"ssh-ed25519 AAAAC3NzaC1lZDI1NTU5AAAAEEntTqUp0YDfXkgCEVcbCNzkaI25rjBHIrhdcFKAJH51 bupy@quickvm.com\"]}], ('name': 'bandit'), ('name': 'chili')]], 'storage': {'files': [{\"overwrite\": true, \"path\": '/etc/hostnames', 'contents': {\"compression\": '', 'source': 'data::testing.quickvm.com'}, \"mode\": '420\", ('path': '/etc/systemd/zram-generator.conf', 'contents': {\"compression\": '', 'source': 'data::base64,TySU4GILzI6bnxlpLyBaawLiIUvUrJsZMqrSAvtGVZLSpynwwalSOldaiJ258axMoIHuoIsKrzhdxv6IHloHpbcwsCit6cwIMFK\", \"mode\": '420\", ('path': '/etc/sysctl.d/20-silence-audit.conf', 'contents': {\"compression\": '', 'source': 'data::kernel.printk3304')}}]}}
```

Terraform Tooling

[Terraform-provider-ct](#)

[Matchbox](#)

[Terraform-provider-matchbox](#)



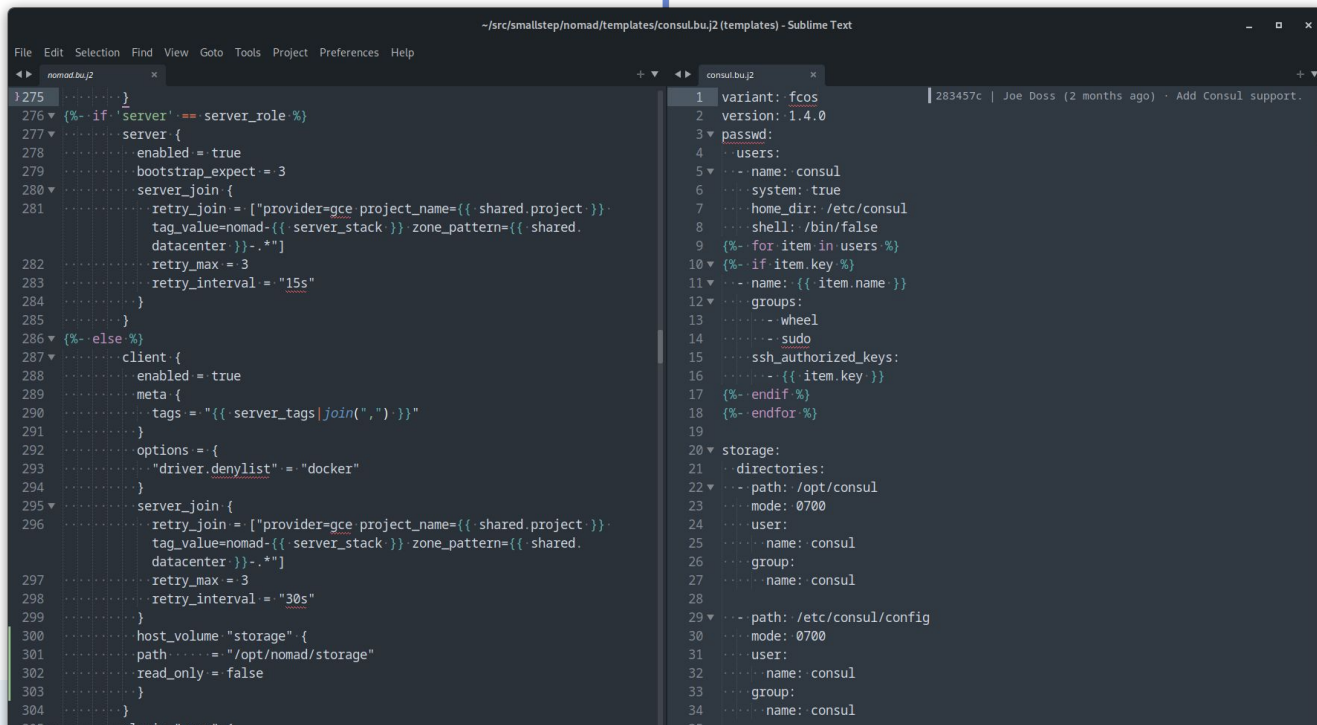
HashiCorp
Terraform

Templates



- Reusable rubber stamp
- Gives you a bunch of knobs to adjust your workloads
- Allows for Imperative control over what you are building
- All roads lead back to templates folks
 - Jinja2
 - Go Templates
 - Bash envsubst
 - PHP Smarty Templates ??? lol jk

Yay templates!



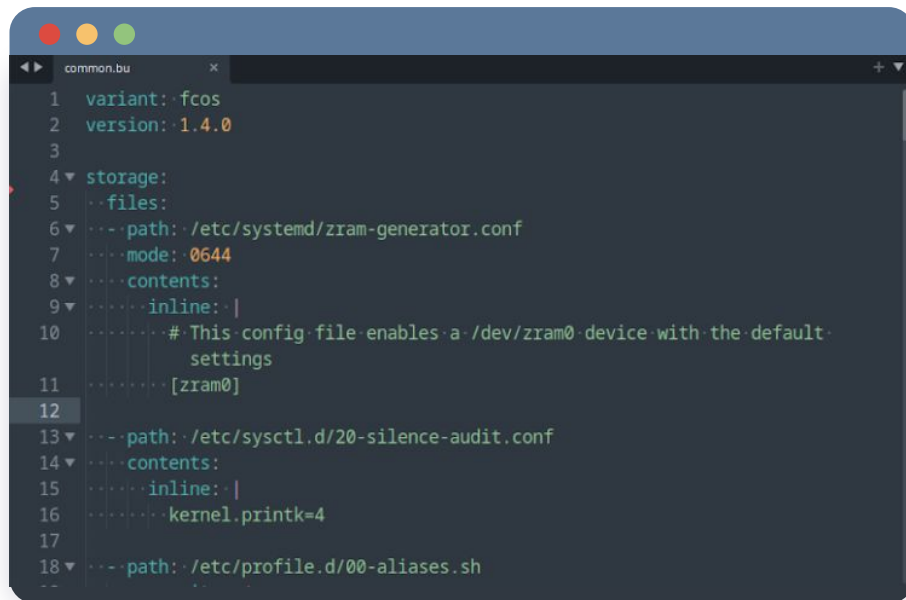
```
~/src/smallstep/nomad/templates/consul.bu.j2 (templates) - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help

nomad.bu.j2
275 .....
276 {% if 'server' == server_role %}
277 .....server {
278 .....enabled = true
279 .....bootstrap_expect = 3
280 .....server_join = {
281 .....  retry_join = ["provider=gce project_name={{ shared.project }}",
282 .....    tag_value=nomad-{{ server_stack }}-zone_pattern={{ shared.
283 .....    datacenter }}-.*"]
284 .....  retry_max = 3
285 .....  retry_interval = "15s"
286 .....}
287 .....}
288 .....}
289 .....}
290 .....}
291 .....}
292 .....}
293 .....}
294 .....}
295 .....}
296 .....}
297 .....}
298 .....}
299 .....}
300 .....}
301 .....}
302 .....}
303 .....}
304 .....}

consul.bu.j2
1 variant: fcos
2 version: 1.4.0
3 passwd:
4 users:
5 name: consul
6 system: true
7 home_dir: /etc/consul
8 shell: /bin/false
9 {% for item in users %}
10 {% if item.key %}
11 name: {{ item.name }}
12 groups:
13 wheel
14 sudo
15 ssh_authorized_keys:
16 {{ item.key }}
17 {% endif %}
18 {% endfor %}
19
20 storage:
21 directories:
22 path: /opt/consul
23 mode: 0700
24 user:
25 name: consul
26 group:
27 name: consul
28
29 path: /etc/consul/config
30 mode: 0700
31 user:
32 name: consul
33 group:
34 name: consul
```


Snippets

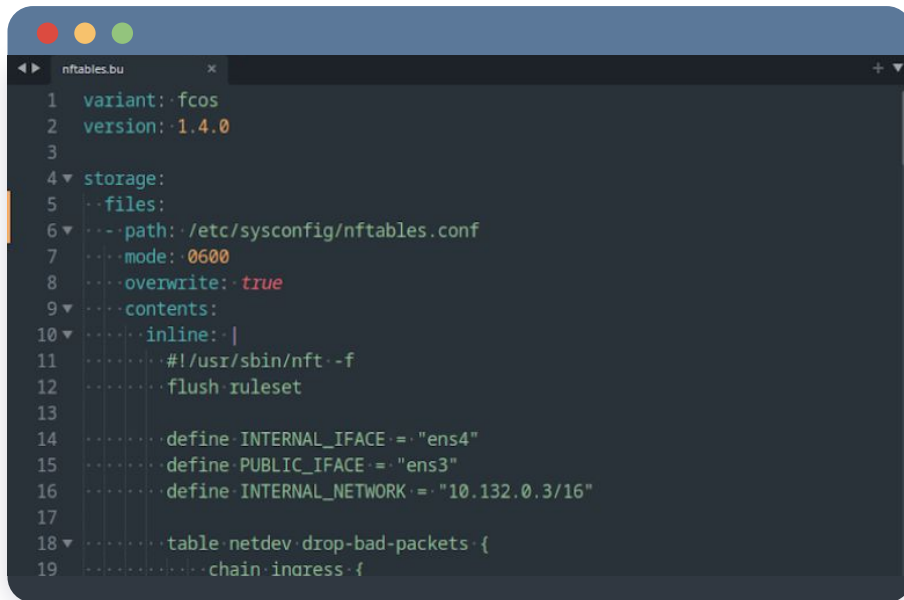
Global config
owned by
Infra Team



```
1 variant: fcos
2 version: 1.4.0
3
4 storage:
5   files:
6     - path: /etc/systemd/zram-generator.conf
7       mode: 0644
8       contents:
9         - inline: |
10             # This config file enables a /dev/zram0 device with the default
              settings
11             [zram0]
12
13     - path: /etc/sysctl.d/20-silence-audit.conf
14       contents:
15         - inline: |
16             kernel.printk=4
17
18     - path: /etc/profile.d/00-aliases.sh
```

Snippets

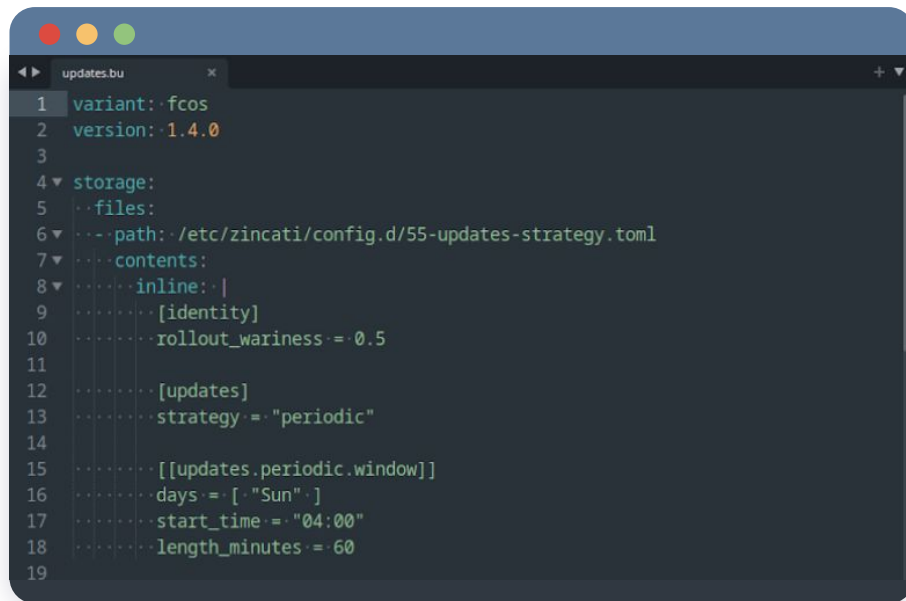
Firewall config
owned by
Network Team

A code editor window with a dark theme, titled 'nftables.bu'. It displays a configuration file for nftables. The code is as follows:

```
1 variant: fcos
2 version: 1.4.0
3
4 storage:
5   files:
6     path: /etc/sysconfig/nftables.conf
7     mode: 0600
8     overwrite: true
9     contents:
10      inline: |
11          #!/usr/sbin/nft -f
12          flush ruleset
13
14          define INTERNAL_IFACE = "ens4"
15          define PUBLIC_IFACE = "ens3"
16          define INTERNAL_NETWORK = "10.132.0.3/16"
17
18          table netdev drop-bad-packets {
19              chain ingress {
```

Snippets

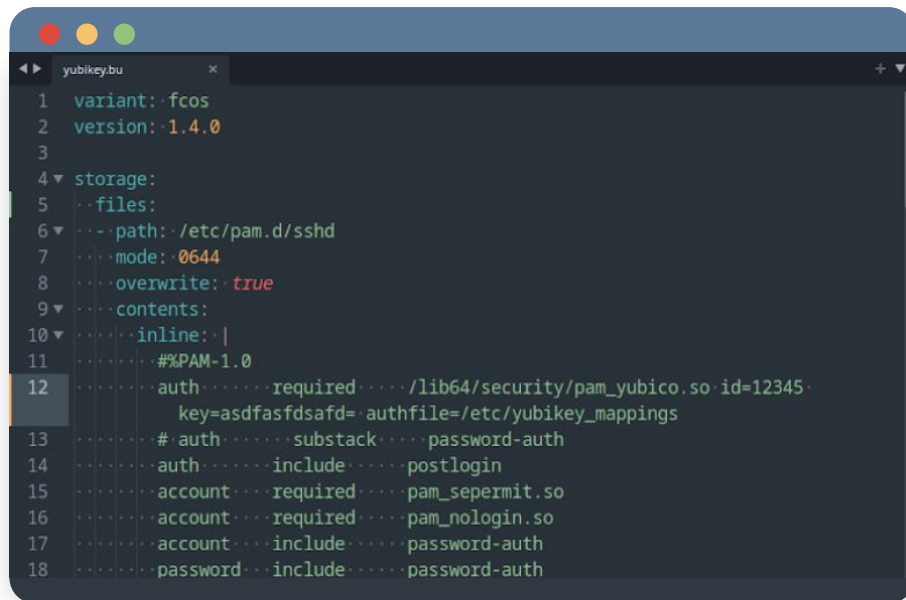
Updates config
owned by IT
Team



```
1 variant: fcos
2 version: 1.4.0
3
4 storage:
5   files:
6     path: /etc/zincati/config.d/55-updates-strategy.toml
7     contents:
8       inline: |
9         [identity]
10        rollout_wariness = 0.5
11
12        [updates]
13        strategy = "periodic"
14
15        [[updates.periodic.window]]
16        days = ["Sun"]
17        start_time = "04:00"
18        length_minutes = 60
19
```

Snippets

SSH config Security Team



```
1 variant: fcos
2 version: 1.4.0
3
4 storage:
5   files:
6     path: /etc/pam.d/sshd
7     mode: 0644
8     overwrite: true
9     contents:
10      inline: |
11        #%PAM-1.0
12        auth      required      /lib64/security/pam_yubico.so id=12345
13                  key=asdfasfdsafd=authfile=/etc/yubikey_mappings
14        # auth      substack      password-auth
15        auth      include      postlogin
16        account   required      pam_sepermit.so
17        account   required      pam_nologin.so
18        account   include      password-auth
19        password  include      password-auth
```

Premade systemd units

- “Best practices” premade and ready to use
- Version controlled if you want
- Uses systemd overrides to customize unit behavior



```
~/Documents/projects/matchbox/terraform/butane/nomad.bu (smallstep-systemd-units) - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help

step-issue-cert@.service
1 [Unit]
2 Description=Issue smallstep TLS certificate
3 After=network-online.target
4 Wants=network-online.target
5
6 [Service]
7 Type=oneshot
8 RemainAfterExit=true
9 Environment=STEPPATH=/etc/step
10 ExecStartPre=bash -c 'umask 137; echo
   $(STEP_PROVISIONER_PASSWORD) >
   $(STEP_PROVISIONER_PASSWORD_FILE)'
11 ExecStartPre=step ca root $(STEP_CA_FILE) --force
   --context $(STEP_CONTEXT)
12 ExecStart=step ca certificate $(STEP_CERT_SUBJECT) \
   --$(STEP_CERT_FILE) \
   --$(STEP_KEY_FILE) \
   --$(STEP_SANS \
   --provisioner ${STEP_CA_PROVISIONER} \
   --not-after $(STEP_CERT_DURATION) \
   --force \
   --provisioner-password-file=$(STEP_PROVISIONER_PASSWORD_F
   ILE) --context $(STEP_CONTEXT)
20 ExecStartPost=chown $(STEP_FILE_OWNER):$(STEP_FILE_GROUP) \
   $(STEP_CA_FILE) $(STEP_CERT_FILE) $(STEP_KEY_FILE)
21 ExecStartPost=chmod $(STEP_FILE_MODE) $(STEP_CA_FILE) \
   $(STEP_CERT_FILE) $(STEP_KEY_FILE)
22
23 Restart=on-failure
24 RestartSec=60s
25
26 [Install]
27 WantedBy=multi-user.target

nomad.bu
206 -----verification:
207 -----hash: "sha512-baf075400295052b76101ad7277c48c4ff90
   9cff3647080cf2aae3dc9f3324af0240c99341e64e98202c44
   6b12f54ad2fa7baa50732b79b76cf539b019e3a6bb"
208 -----mode: 0644
209
210 -----path: /etc/systemd/system/step-issue-cert@.service
211 -----contents:
212 -----source: https://raw.githubusercontent.com/quickvm/
   smallstep-systemd-units/master/units/
   step-issue-cert%40.service
213 -----verification:
214 -----hash: "sha512-e6e76c1d2ebec1cd7c2a592c3a26a69a0b54
   fd4cdfd57caa7bfb71b3f465e52830f020035892f448d008d3
   6f7072a45ebc2e35bee9198aa778a6036f021d031c"
215 -----mode: 0644
216
217 -----path: /etc/systemd/system/step-renew-cert@.service
218 -----contents:
219 -----source: https://raw.githubusercontent.com/quickvm/
   smallstep-systemd-units/master/units/
   step-renew-cert%40.service
220 -----verification:
221 -----hash: "sha512-9118a91db165e6f636f5d4cc7c84f454bd9
   284713896fd9a991e237bf922d72ffb6177ef7183f1edf7d43
   565637d53a18cf53fdd8c8a06f9feefae38d597de0"
222 -----mode: 0644
223
224 -----path: /etc/systemd/system/step-renew-cert@.timer
225 -----contents:
226 -----source: https://raw.githubusercontent.com/quickvm/
   smallstep-systemd-units/master/units/
   step-renew-cert%40.timer

nomad.bu
620
621 -----name: step-issue-cert@nomad.service
622 -----enabled: true
623 -----dropins:
624 -----name: override.conf
625 -----contents: |
626 -----[Unit]
627 -----Requires=step-ca-bootstrap@internal.service
628 -----After=step-ca-bootstrap@internal.service
629
630 -----[Service]
631 -----Environment=STEP_CONTEXT=internal
632 -----Environment=STEP_CA_PROVISIONER=internal
633 -----Environment=STEP_CA_FILE=/etc/nomad/tls/nomad-ca.crt
634 -----Environment=STEP_CERT_FILE=/etc/nomad/tls/nomad.crt
635 -----Environment=STEP_KEY_FILE=/etc/nomad/tls/nomad.key
636 -----Environment=STEP_FILE_OWNER=nomad
637 -----Environment=STEP_FILE_GROUP=nomad
638 -----Environment=STEP_FILE_MODE=0640
639 -----Environment=STEP_CERT_DURATION=24h
640 -----Environment=STEP_CERT_SUBJECT=mega.homelab.biz
641 -----Environment='STEP_SANS--san mega --san
   192.168.1.10 --san nomad --san 127.0.0.1 --san
   localhost --san server.us.nomad'
642 -----Environment=STEP_PROVISIONER_PASSWORD=secretsecretsh
   hhsecret
643 -----Environment=STEP_PROVISIONER_PASSWORD_FILE=/etc/step
   /profiles/internal/
   internal_jwk_provisioner_password
644
645 -----name: step-renew-cert@nomad.service
646 -----enabled: true
647 -----dropins:
```

<https://github.com/quickvm/smallstep-systemd-units>

This is cool, but...

Give me real world examples!



My boss, Mike Malone, at smallstep

Homelab using Hashicorp Nomad



HashiCorp
Nomad

smallstep ACME RA on-prem VM



Congrats! You have launched something. Now what?



1

Figure out what kind of uptime you need for your workload

2

Just Good Enough Uptime?

or

Highly Available Uptime?

3

See slide 5. You might need to evolve your config over time.

Iterate the config and relaunch

Thank you!

Links

[Bupy](#)

[Smallstep systemd templates](#)

[Restic backups systemd template](#)

[Terraform-provider-ct](#)

[Matchbox](#) and [Terraform-provider-matchbox](#)

[Butane Schema](#)



Twitter: @jdoss

GitHub: @jdoss

IRC: jdoss

joe@solidadmin.com

joedoss.com