cfgmgmt for cfgmgmt

fosdem 2019

```
❯ tree -L 1 .
.
├── 00_intro
├── 01_whoami
├── 02_olindata
├── 03_contents
├── 04_problem
├── 05_solution
├── 06_tools
├── 07_setup
├── 08_bootstrap
├── 09_create_host
├── 10_push_package
├── 11_openscap
├── 12_image_based
├── 13_extensions
├── 14_outro
└── 15_shutdown
```

```
❯ tree 00_intro
00_intro
├── 00_fosdem2019
├── 01_welcome
└── 02_cfgmgmt_for_cfgmgmt
```

```
❯ tree 01_whoami
01_whoami
├── 00_enschede
│   ├── 00_born_raised
│   ├── 01_cs1.5
│   ├── 02_shockmedia
│   └── 03_takeaway
├── 01_hobbies
│   ├── 00_hip_hop
│   ├── 01_true_crime
│   ├── 02_architecture
│   ├── 03_interior_design
│   ├── 04_concerts
│   └── 05_it
├── 02_openwrt
│   ├── 00_strict_nat
│   └── 01_amazing
└── 03_den_haag
    ├── 00_new_challenge
    └── 01_olindata
```

```
❯ tree 02_olindata
02_olindata
├── 00_foss
├── 01_devops
├── 02_aws
├── 03_puppet
├── 04_terraform
└── 05_training
```

```
❯ tree 03_contents
03_contents
├── 00_config-management^2
├── 01_scope
├── 02_setup
├── 03_verify
└── 04_next
```

```
❯ tree 04_problem
04_problem
├── 00_puppet
├── 01_ntp
├── 02_kubernetes
├── 03_foreman
└── 04_katello
```

❯ manage application configurations

❯ "All animals are equal, but some animals are more equal than others."

❯ puppetserver(s) are often set up manually

❯ puppetserver(s) grow with business

❯ puppetserver(s) scale horizontally/vertically

❯ puppetserver(s) do not support HA

```
❯ cat ntp.pp

class { 'ntp':
  servers => [ 'ntp1.corp.com', 'ntp2.corp.com' ],
}
```

01_ntp

```
❯ cat k8s-controller.pp
class {'kubernetes':
  controller => true,
}

❯ cat k8s-worker.pp
class {'kubernetes':
  worker => true,
}
```

❯ manage virtual and physical host lifecycles

❯ manage services via smart proxy -> dns/dhcp/tftp/pxe/puppet/etc

❯ configuration management via puppet and enc

❯ monitoring of host statuses

❯ reporting of applicable patches/statuses/custom

❯ webui/cli/api

❯ 7400+ commits, 10th anniversary this year

- content management
- subscriptions (via rh cdn)
- products (groups)
- repositories
- gpg keys
- sync management
- lifecycle environments
- content views (snapshots)
- content view versions
- activation keys
- openscap
- patch management via errata
- combines multiple projects
- katello pulp candlepin
- together over 50k commits

```
❯ tree 05_solution
05_solution
└── 00_config-management^2
```

```
❯ puppet module install theforeman-puppet --modulepath .

❯ cat > install.pp <<EOF
class { '::puppet': server => true }
EOF

❯ puppet apply install.pp --modulepath .

❯ or foreman-installer --scenario foreman/katello

❯ or foreman forklift

❯ and foreman-ansible-modules
```

```
❯ tree 06_tools
06_tools
├── 00_chicken-egg
├── 01_lxd
├── 02_cloud-init
├── 03_foreman
├── 04_katello
├── 05_ansible
├── 06_fam
├── 07_git
├── 08_hammer
├── 09_libvirt
├── 09_openscap
└── 10_distrobuilder
```

❯ ‘pre-loaded’ via custom image

❯ installed during first boot

❯ prepare configuration management up front

❯ delegation: cloud-init to foreman-installer to puppet to ansible

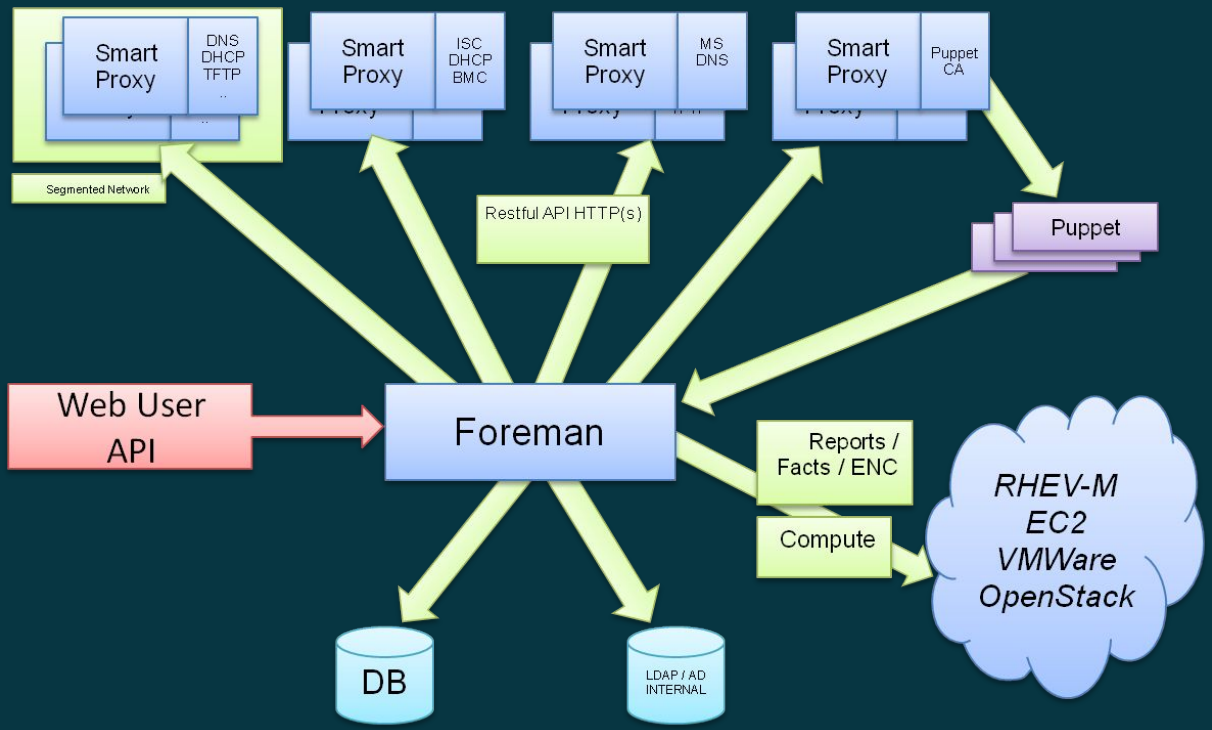
- cloud-init via nocloud provider
- easy cloud-init testing -> sudo cloud-init clean --logs --reboot (*)
- containers with pid1
- simple and fast proof-of-concept
- meant to consolidate homelab machines for power/money saving reasons

01_lxd
02_cloud-init

```
❯ cat cloud-init-host-config.yml
hostname: mynode
fqdn: mynode.example.com
manage_etc_hosts: true

❯ cat cloud-init-bridge.yml
version: 1
config:
  - type: physical
    name: eth0
  - type: bridge
    name: br0
    bridge_interfaces:
      - eth0
    subnets:
      - type: dhcp
```

- provisioning and configuration management
- content management
- pulp
- candlepin



03_foreman
04_katello

- configuration management via ssh
- supports many applications via ansible modules (python)
- foreman-ansible-modules project
- ansible module for foreman/katello mgmt
- team effort
- strict workflow with checks and balances
- foreman -- hammer -> cli

- api for qemu/lxc/xen/hyper-v/more
- nested via lxd
- connect via ssh/tcp/socket
- insecure for demo
- ovirt/proxmox/openstack/aws/gcp/more

- audit your environment
- generate reports
- scap workbench
- profiles for CIS/PCI-DSS/STIG/CJIS/NIST/more
- build our custom centos lxd image with cloud-init support
- no pre-built binaries available

10_openscap
11_distrobuilder

```
❯ tree 07_setup
07_setup
├── 00_lxd
├── 01_cloud-init
└── 02_ansible
```

```
❯ lxc-checkconfig

❯ lxc profile edit default
...
config:
  raw.lxc: |-
    lxc.cgroup.devices.allow = a
    lxc.cap.drop=
...

❯ lxc network edit lxdbr0
...
config:
  raw.dnsmasq: |
    dhcp-boot=pxelinux.0,fosdem.10.132.8.100.nip.io,10.132.8.100
    dhcp-option=66,10.132.8.100
...
```

```
❯ cat cloud-init-centos-katello-ssh.yml
hostname: fosdem
fqdn: fosdem.10.132.8.100.nip.io
manage_etc_hosts: true
users:
  - name: centos
    groups: sudo
    sudo: ['ALL=(ALL) NOPASSWD:ALL']
    ssh_authorized_keys:
      - ssh-rsa AAAAB3Nz... foo@bar
write_files:
- path: /root/bootstrap.sh
  permissions: '0755'
  content: |
    #!/bin/bash
    /usr/sbin/foreman-installer --scenario "katello" \
...
      --verbose
```

```
runcmd:
  - yum -y localinstall
http://fedorapeople.org/groups/katello/releases/yum/3.10/katello/el7/x8
6_64/katello-repos-latest.rpm
  - yum -y localinstall
http://yum.theforeman.org/releases/1.20/el7/x86_64/foreman-release.rpm
  - yum -y localinstall
https://yum.theforeman.org/client/1.20/el7/x86_64/foreman-client-releas
e.rpm
  - yum -y localinstall
https://yum.puppetlabs.com/puppet5/puppet5-release-el-7.noarch.rpm
  - yum -y localinstall
http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  - yum -y install foreman-release-scl python-django
  - yum -y update
  - yum -y install katello
  - bash /root/bootstrap.sh
```

```
❯ lxc init sig-cloud-generic fosdem -c security.privileged=true \
    --config=user.user-data="$(cat cloud-init-centos-katello-ssh.yml)"

❯ lxc network attach lxdbr0 fosdem eth0

❯ lxc config device set fosdem eth0 ipv4.address 10.132.8.25

❯ lxc config set fosdem environment.LANG en_US.UTF-8

❯ lxc config show fosdem (--expanded)

❯ ansible-playbook setup.yml

❯ bundle install
```

01_cloud-init
02_ansible

```
❯ tree 08_bootstrap
08_bootstrap
├── 00_issues
├── 01_workflow
├── 02_start
└── 03_playbook
```

- run ansible a couple of times
- centos version ‘flips’
- some hardcoded values in playbook
- forked version of fam, already fixed upstream

❯ lxc network config

❯ lxc container config

❯ ansible/bundle setup

❯ populate vars file

❯ start lxc container

❯ apply playbook

```
❯ lxc start fosdem

❯ lxc exec fosdem -- journalctl -f

... wait ~20m

❯ lxc exec fosdem -- journalctl -f | grep admin

❯ lxc snapshot fosdem
```

```
❯ ansible-playbook -vvv seed.yml -e configure_ssh=true -e
configure_r10k=true -e run_puppet=true; ansible-playbook -vvv seed.yml
-e sync_repos=true

❯ lxc exec fosdem -- tail -f /var/log/foreman/production.log

... wait ~60m

❯ lxc snapshot fosdem

❯ ansible-playbook -vvv seed.yml -e dangling=true -e
configure_backups=true -e configure_errata=true

❯ lxc exec fosdem -- bash /root/pulp_errata_sync.sh

... wait ~60m

❯ lxc snapshot fosdem
```

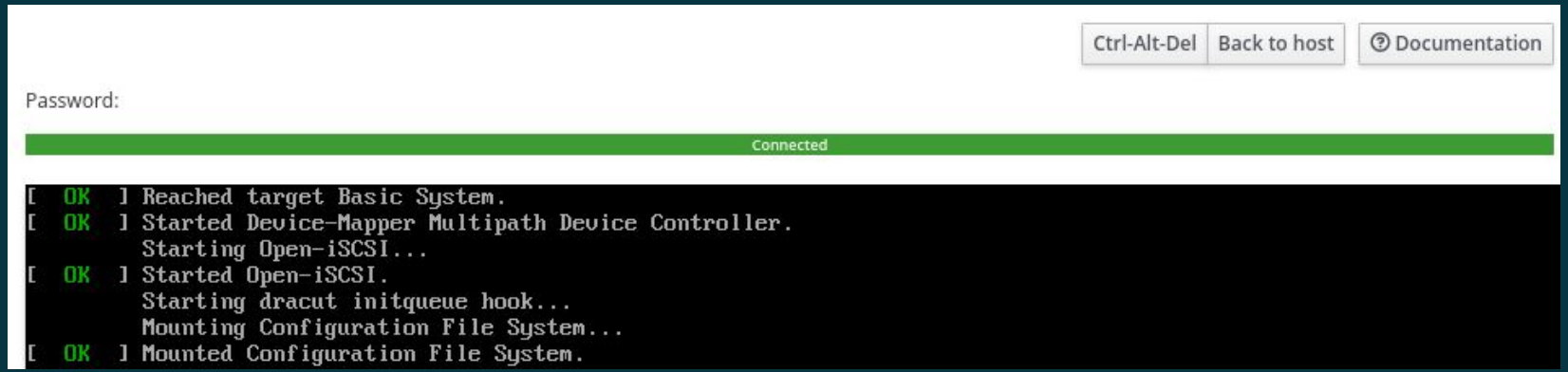
```
❯ tree 09_create_host
09_create_host
├── 00_hammer-cli
└── 01_webui-vnc
```

```
❯ hammer host create --name "kittycat.lxd" \
--location "wim-ws2" \
--organization-id 1 \
--hostgroup "el7_group" \
--interface
"type=interface,managed=true,primary=true,provision=true,compute_bridge
=br0" \
--volume="capacity=32G" \
--compute-attributes "start=1"
```

❯ foreman doesn’t enable the autostart option for libvirt vms, use a hook

❯ http://www.uberobert.com/autostart-libvirt-vms-in-foreman/

❯ https://fosdem.10.132.8.100.nip.io



❯ hosts -> target -> console -> f12 -> copy wss link -> paste in new tab, change to https -> accept insecure certificate -> f5 console

00_webui-vnc

```
❯ tree 10_push_package
10_push_package
├── 00_content-host
├── 01_errata
└── 02_host-collection
```

```
❯ tree 11_openscap
11_openscap
├── 00_compliance
└── 01_assessment
```

```
❯ hammer policy create --period custom --cron-line "5 1 * * *"
--description pci --hostgroups el7_group --name pci --scap-content 'Red
Hat centos7 default content' --scap-content-profile-id 18 --location
wim-ws2 --organization lxd
```

```
❯ tree 12_image_based
12_image_based
├── 00_packer
├── 01_importing
└── 02_ssh
```

❯ packer with a qemu builder

❯ gitlab-ci -> preconfigured builder with loop devices and dependencies

❯ builder runs libvirt, via lxd

❯ gitlab-ci has 2 jobs: build the image and upload it to a libvirt host

❯ hammer compute-resource image create --name centos76-master-95283ce5 --operatingsystem "CentOS 7.6.1810" --username foreman-builder --password foreman-builder --uuid /data/centos76-master-95283ce5 --compute-resource-id 2 --architecture x86_64

❯ using snippets via foreman requires ssh -> prepared ‘builder’ user

❯ requires dhcp orchestration -> foreman needs to know the ip to ssh to

❯ can’t demo the actual login because no dhcp orchestration in lab env

00_packer 02_ssh
01_importing

```
❯ tree 13_extensions
13_extensions
├── 00_freeipa
├── 01_awx
├── 02_ovirt
├── 03_cicd
├── 04_graylog
├── 05_mco_choria
└── 06_foreman_addons
```

```
❯ tree 14_outro
14_outro
├── 00_conclusion
└── 01_questions
```

❯ Apply configmanagement to your core services for host lifecycle management makes life easier:

- centralized interface
- quickly spin up new environments
- provision multiple organizations
- insight into host statuses for monitoring and reporting
- aligned workflow
- tons of existing resources (modules) which help

```
❯ tree 15_shutdown
15_shutdown
├── 00_resources
└── 01_sigkill
```

- https://theforeman.org/
- #theforeman on irc.freenode.net
- https://community.theforeman.org/
- https://github.com/theforeman
- https://github.com/furhouse/fosdem2019
- https://www.lisenet.com/tag/katello/
- https://developers.redhat.com/

❯ ` exit

so long and thanks for all the fish
w.bonthuis - fosdem 2019

01_sigkill