Core Compute Services

Config management

Giacomo Tenaglia - CSC on IT Services - 2024-11-08

IaC

Infrastructure as Code

ai / it-puppet-hostgroup-lxplus / Merge requests / !224

Enable twofa volunteers and service accounts

Edit | Code

Merged **Steve Traylen** requested to merge `OTG0150912` into `qa` 2 months ago

Overview 0 | Commits 1 | Pipelines 2 | **Changes 4** | Add a to do

Compare **qa** and **latest version** — 4 files +6 −3

data/hostgroup/lxplus/nodes/test.yaml +0 −1 Viewed

```
1  1  ---
2  2
3     - hg_lxplus::enable_twofa: 'plus'
4  3
5  4  # Cannary the pkg updates here.
6  5  osrepos::distro_sync_retry: false
```

data/hostgroup/lxplus/tunnel/test.yaml deleted 100644 → 0 +0 −2 Viewed

```
1     - ---
2     -  hg_lxplus::enable_twofa: 'tunnel'
```

data/hostgroup/lxplus/nodes.yaml +3 −0 Viewed

```
1  1  ---
2  2
      3  + # Enable the plus variant of twofa
      4  + hg_lxplus::enable_twofa: 'plus'
      5  +
```

CERN Config Management Services

"Agile Infrastructure"

- Early 2000s: home-grown toolset
- 2012: the "AI" project
  - Puppet & Foreman
  - Openstack
  - Centralised logging & monitoring

CERN Config Management Services

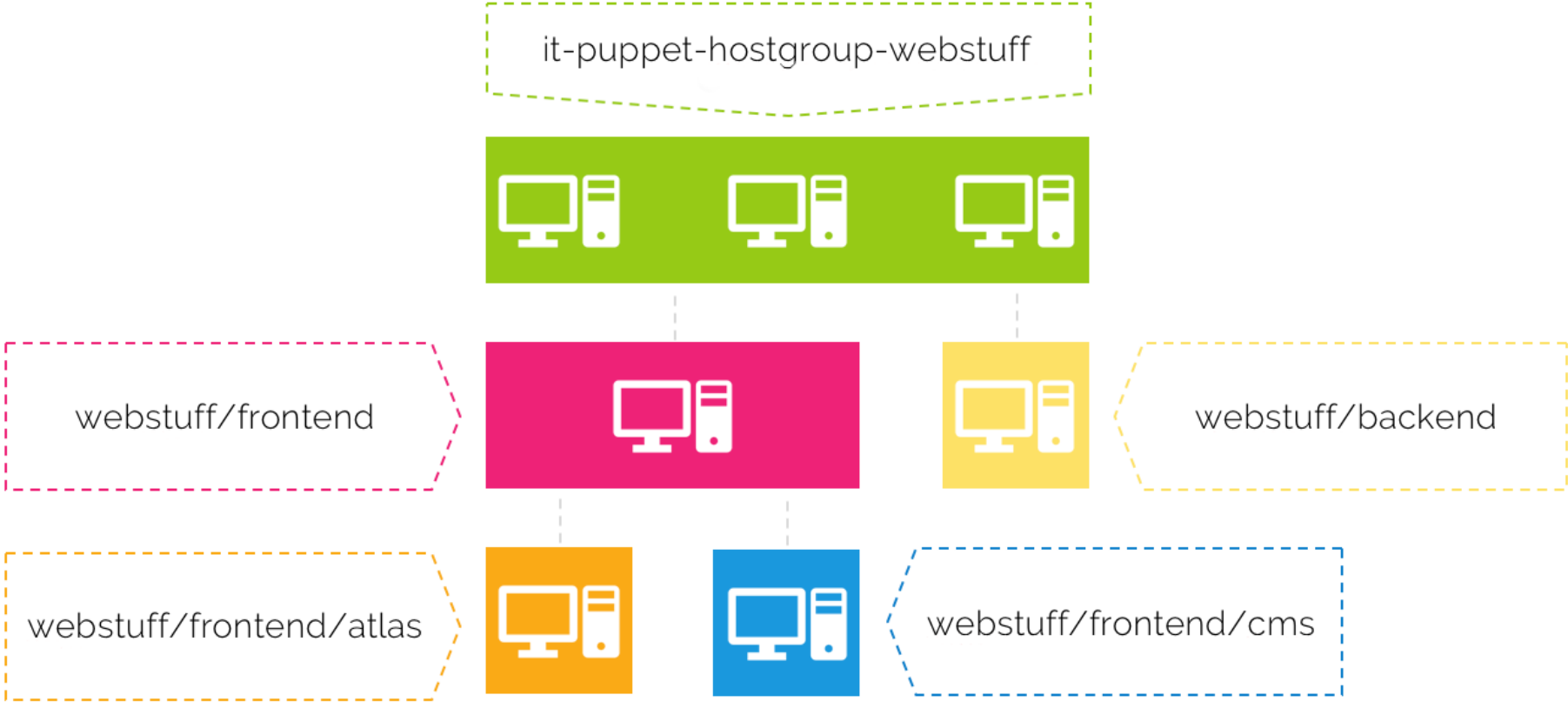
- Sources of Truth ™
  - HR databases -> e-groups -> Active Directory -> LDAP
  - LanDB (including CERN perimeter Firewall)
  - CERN Certificate Authority
  - Windows/Linux “blessed” configs
  - …
- Config Services:
  - Configure Windows/Linux virtual/physical servers
  - Wrap around all of the above
  - Leverage Openstack
  - Provide IaC

Technology stack

-  Puppet (open-source, mostly single-company):
  - Centralised configuration management system
  - Based on Ruby
  - Client/server architecture
-  Foreman:
  - Inventory/classifier
-  Gitlab:
  - Configuration repositories

Classifying nodes

Foreman & hostgroups

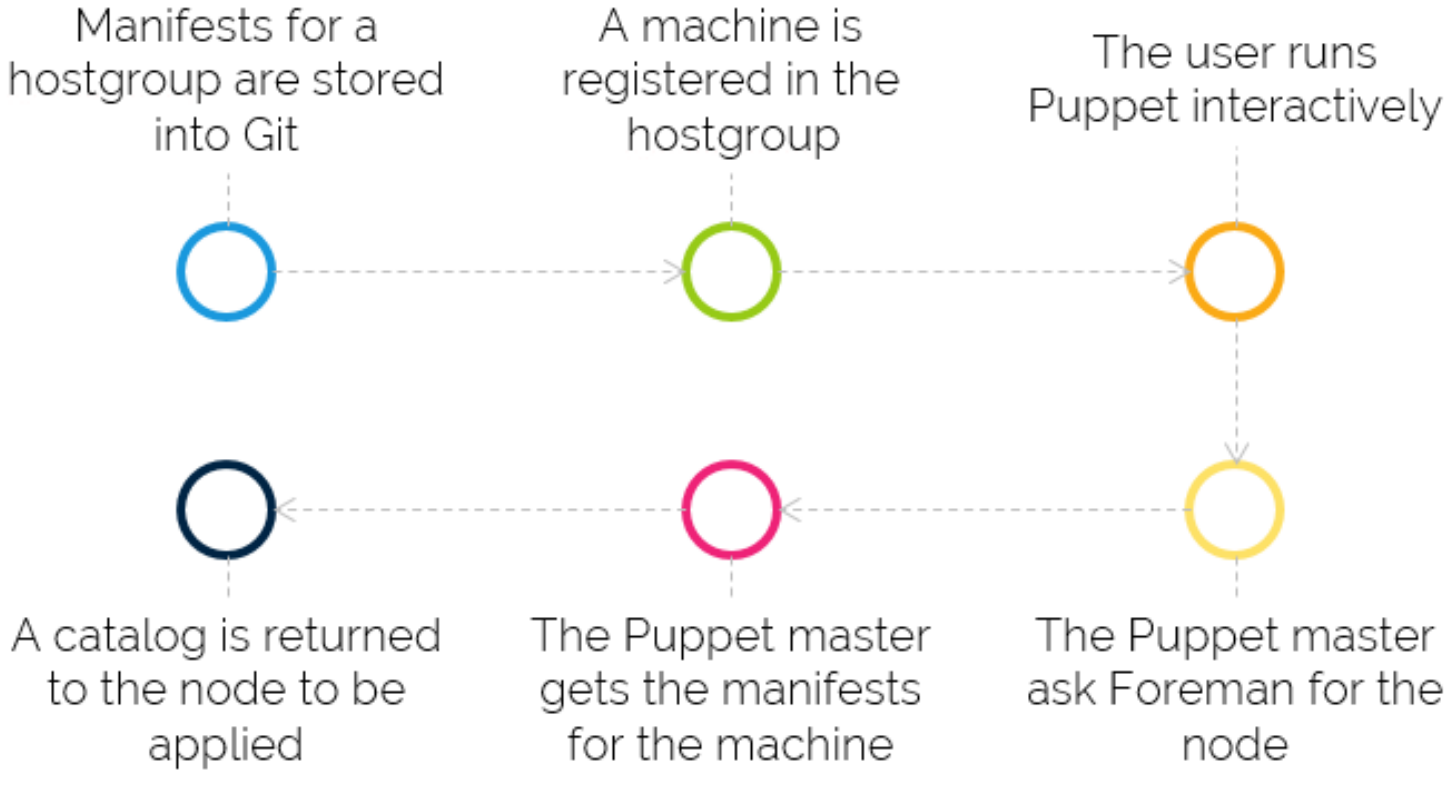


Classifying nodes

Foreman & hostgroups

- Foreman: https://judy.cern.ch
- Hostgroups: Gitlab repos

The Puppet Agent



Managing change

Gitlab & environments

- `aiadm`: “management/reference service”
- Environments:
  - “Pointer” to feature branches
  - Allow separated testing of config changes
  - Homegrown ‘Puppet librarian service’

Managing change

Your nodes only

- `csc-config-{1..6}.cern.ch`
- `playground/csc`

```
ssh aiadm.cern.ch
git clone https://:@gitlab.cern.ch:8443/ai/it-puppet-hostgroup-playground.git
git checkout csc_X
...
git push
ssh root@csc-config-X.cern.ch
puppet agent -tv
```

Configuring services

Modules

- Goal: do not reinvent the wheel
- https://gitlab.cern.ch/ai/it-puppet-module-training/

```
include training
```

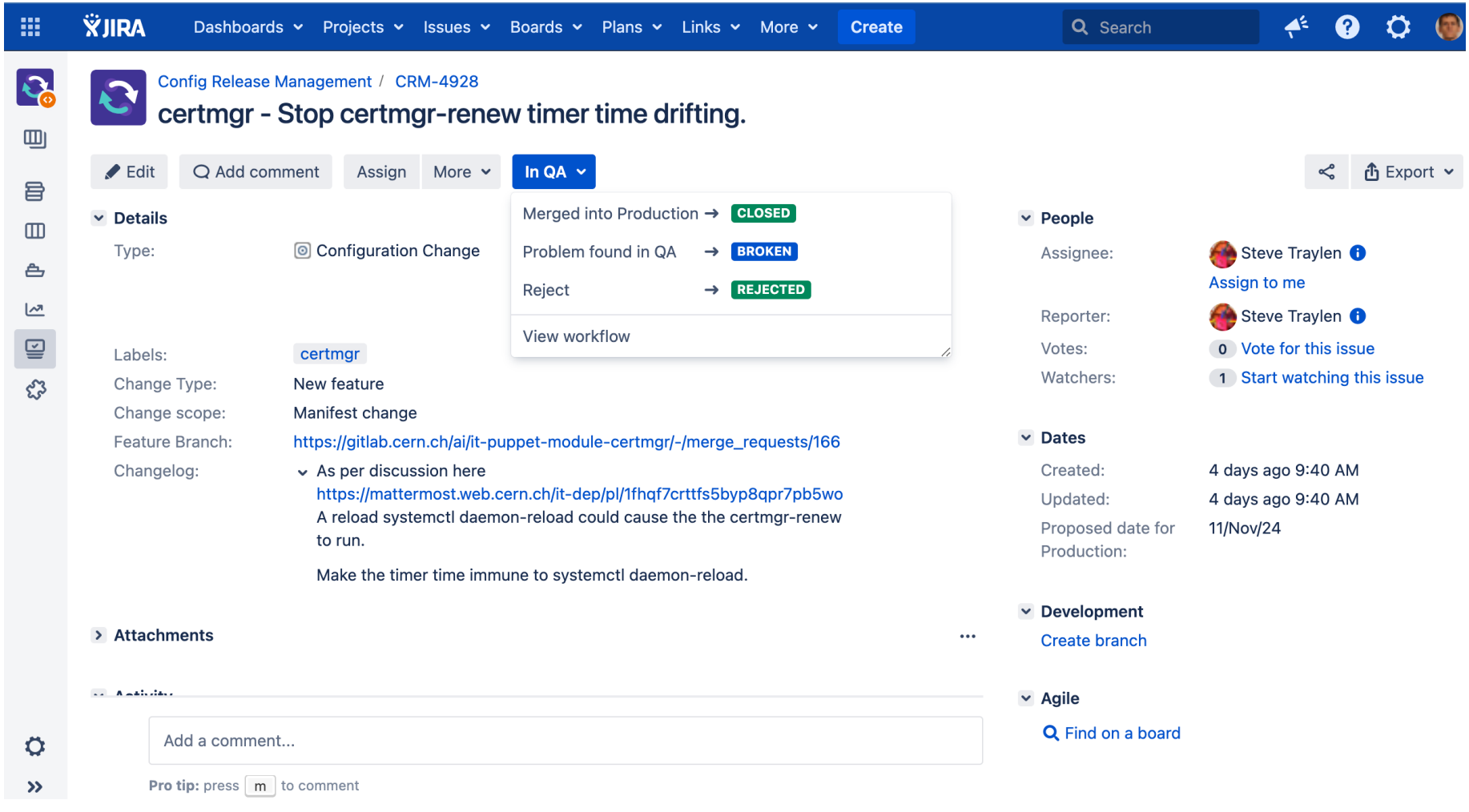
Separating data

Hiera

- Store the configuration data in key-value pairs
- Look up needed data during catalog compilation
- HIERArchic structure: https://gitlab.cern.ch/ai/it-puppet-hostgroup-punch

Centralised change control

CERN-wide QA process



Extras

Secrets, certificates, alarms etc

- Secrets management: `teigi` vs Vault
- Certificates: `certmgr`
- Alarms & server state: `roger` (MONIT)

Wrapping up

```
+------------------+-------------------------------------------------------
|         Hostname: | csc-config-1.cern.ch
|         Hardware: | virtual, 1 cores, 1.56 GiB memory, - swap, 1 disks
|        Hostgroup: | playground
|          Comment: | This is for short-term playing and testing. Machines in he
|                   | should have no expectation of being stable and may be dele
|                   | without warning.
|      Environment: | csc_1
|      Responsible: | tcsc-it-services-2024-students@cern.ch
|        Main user: | tcsc-it-services-2024-students@cern.ch
|  FE Responsible: | Ignore
|               OS: | RedHat 9.4 x86_64 (5.14.0-427.42.1.el9_4.x86_64)
|          Project: | CSC IT Services
|          Flavour: | m2.small
|       Avail zone: | cern-geneva-a
|        LANDBsets: | -
|       LB aliases: | -
|    CNAME aliases: | -
|             IPv4: | 188.184.84.135 (GPN) (S513-A-VM75)
```

To know more

- https://cern.ch/config
- Self-service config training
- it-dep/~Puppet Mattermost
- https://gitlab.cern.ch/ai/
- `aiadm:/mnt/puppetnfsdir/environments/production/`