MASS-MIGRATION OF 5000 SERVERS TO FOREMAN/KATELLO WITH BOOTSTRAP.PY

Evgeni Golov
$ WHOAMI

Evgeni Golov
Software Engineer at Red Hat
ex-Consultant at Red Hat
Debian and Grml Developer

♥ FOSS ♥
♥ automation ♥
SITUATION

- 10k RHEL (5k RHEL5, 4k RHEL6, 1k RHEL7)
- most of them subscribed to Satellite5/Spacewalk
- want to move to Satellite6/Foreman
- this requires a plan
TOOLING

- Satellite 6.1 (Foreman 1.7, Katello 2.2)
  - this was done about a year ago
  - the learnings also apply to Foreman itself
- bootstrap.py
  - script for registration of machines to Foreman/Katello
  - at that time not even part of the Katello project
  - mimicks the idea of bootstrap.sh from Spacewalk
BOOTSTRAP.PY

- install katello-ca-consumer RPM
- subscribe the machine using subscription-manager or rhn-migrate-classic-to-rhsm
- configure katello-agent
- configure Puppet
STEP 1: EL5?!  
- ain't nobody got time for that  
- just let it bit-rot on the old infra  
- there is an migration to EL6/7 planned anyways  
- (guess who is still up and running today?)  
- no need to care for the old content  
- but also no insight if there are any gotchas
STEP 2: SIZE THE INFRASTRUCTURE

- main VM: 12vCore, 32GB RAM, 1TB flash
- 6 proxies: 8vCore, 24GB RAM, 500G flash
- rough setup:
  - no machines connect directly to Foreman
  - no more than 1000 clients per proxy
  - most machines don't do Puppet
STEP 3: WAIT FOR FIREWALLS

• there is always a firewall somewhere
• and it for sure will make you unhappy
• request the new firewall rules early and broadly (allow ALL the networks!)
STEP 4: DESIGN CONTENT

- the old setup provided almost only RHEL, apps were delivered from other sources
- this makes an easy setup with one CCV per RHEL release, containing CVs for:
  - RHEL + SatTools
  - admin software (backup, monitoring, etc)
STEP 5: REGISTER ALL THE MACHINES

piece of cake, right?
STEP 5.1: FIND THE RIGHT PROXY

- most machines are subscribed to Spacewalk
  - find the old Spacewalk proxy in `/etc/sysconfig/rhn/up2date`
  - have a map of old proxy to new proxy
- machine is not subscribed?
  - try guessing based on host/domainname
  - try guessing based on IPv4 subnet
- if everything fails, use a "default" proxy
STEP 5.2: FIND AN EXECUTOR

- you need to run a script on every single machine
- Spacewalk has a function for that, but it was disabled
- when a problem occurs during migration, Spacewalk might not be able to control the machine anymore
- today everybody would have used Ansible
- we had BMC BladeLogic, as that was what the customer had for all platforms
STEP 5.3: CHECK THAT FIREWALL

- nobody wants to schedule 5000 jobs that will fail
- run a quick pre-check job before doing the actual work
  - can the host resolve itself (and get a FQDN?)
  - can the host reach the old proxy
  - can the host reach the new proxy (on 80, 443, 5671)
STEP 5.4: WAIT FOR EVERYBODY

- the previous step will identify a lot of machines as "broken"
- enjoy your coffee while waiting for the firewalls, machine owners, etc
STEP 5.5: TEST WHILE WAITING

- figure out which `bootstrap.py` parameters you need
- figure out which patches for `bootstrap.py` you need
- submit everything upstream
- become the de-facto maintainer of `bootstrap.py` upstream
STEP 5.6: REGISTER!

- we run batches of 1000 per day, so we would not affect too many departments
- --skip foreman as we did not care for Foreman/Puppet, just content
- --force as we sometimes just re-run the same machine multiple times
- --legacy-purge to remove the machine from Spacewalk
STEP 5.7: COLLECT THE PIECES

- Sometimes `rhsmcertd` would hang, blocking `subscription-manager`, blocking `yum`
- Some machines have broken clocks, SSL terribly fails
- Yes, we served "wrong" content to a couple boxes, but that was found quickly (missing repos)
- (Broken) proxies in `yum.conf` make it hard to fetch packages
RANDOM FINDINGS

- BMC BladeLogic injects an own libssl using LD_LIBRARY_PATH, breaking yum
- EL6.4 (and older) has a nasty Python bug, making all syslog calls EMERG
- People hate monitoring filesystems
- It is considered OK to leave a machine with broken dependencies
THANKS!

✉️ evgeni@golov.de
🌐 die-welt.net
🐦 @zhenech
🌐 +EvgeniGolov
🌐 @evgeni
🌐 zhenech