

Migrating to OpenVox at CERN

Daniel Juárez

Voxconf 2026 - 16th July 2026

Who am I?

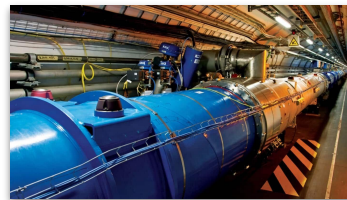


→ **Daniel Juárez**

- ↳ **Spaniard, from the north, so not used to hot summers**
- ↳ **DevOps, Cloud engineer, Sysadmin**
- ↳ **Former employee of CERN, Proton, SonarSource**
- ↳ **Configuration Management (among other services) service manager since Jan 2025 together with Giacomo Tenaglia**
 - **We both are relatively new on the service**

and we also do not have AC

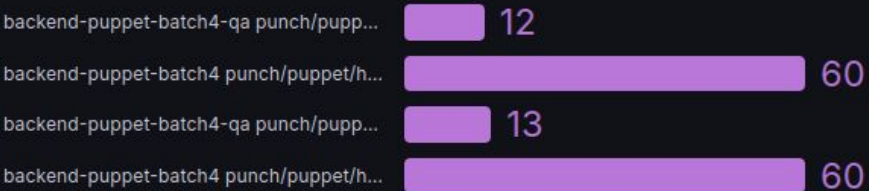
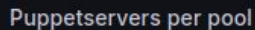
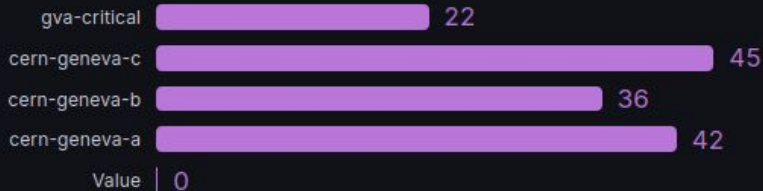
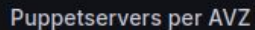
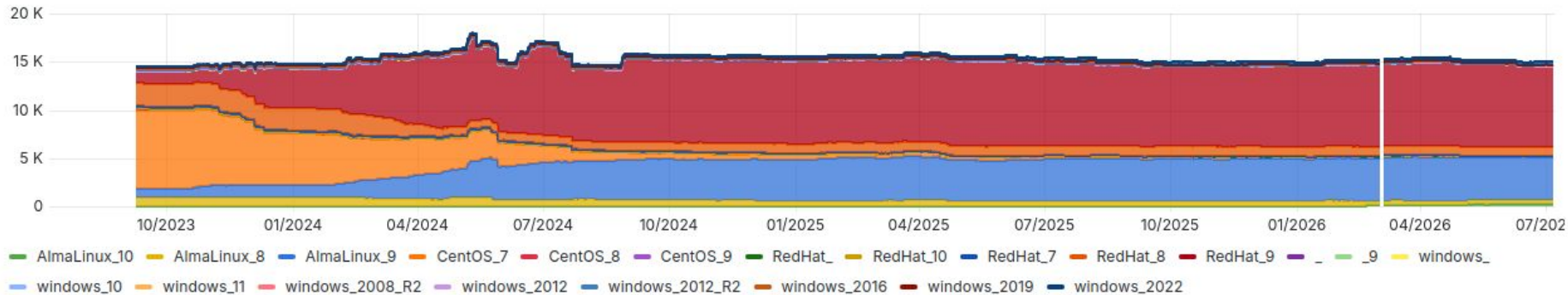
What is CERN (just in case)



→ European Organization for Nuclear Research

- ↳ **Between France and Switzerland, operating since 1954**
- ↳ **High-energy physics research but not only**
- ↳ **Large Hadron Collider, largest and highest energy particle collider so far. 27 Km circumference**
- ↳ **Where WWW was invented, the Higgs boson was discovered and where the single antimatter factory in the world is**
- ↳ **CERN employs about 2500 people from nationalities all around the world (plus hosts 12K users yearly)**
- ↳ **We do not create black holes nor do rituals**

What are we dealing with



Who we are and what we run

→ CERN IT: Configuration Management & Ops

- ↳ The team behind CERN's “Agile Infrastructure” (AI, yes... I know) config layer
- ↳ We keep computing in a known, reproducible state

→ Puppet is the backbone of the data-centre fleet

- ↳ 15K nodes: lxplus, lxbatch/HTCondor, HPC, service nodes
 - Used to have 40K+ some years ago until K8s raised in popularity and Batch service switched to bigger but less machines
- ↳ 400 administrators
- ↳ Foreman as ENC → Foreman hostgroup → Puppet site includes hostgroups
- ↳ Split into
 - 266 Hostgroups (which include modules)
 - 492 Modules

PART 1

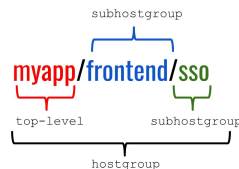
How CERN does config management

Agile Infrastructure: Foreman + Puppet + a lot of home-grown glue

A quick CERN-ism glossary

→ **hostgroup** - our top-level node classification unit

↳ Hierarchical path → maps to Puppet classes



→ **JENS** - git → Puppet environments compiler (since 2013)

↳ Think of it as a r10k, before it existed

→ **teigi / tbag**: our secret store; **certmgr**: host certificates

↳ Moving to Vault/OpenBao and checking the certmgr future

→ **roger**: machine appstate & alarm state; **Foreman**: our ENC + inventory

→ **ai-*** CLIs - ai-bs (bootstrap), ai-foreman, ai-rc, ai-kill ...

→ **mco** - mcollective for fleet orchestration, kept alive by manual building

Hostgroups & Hiera: the CERN data model

→ Everything hangs off the hostgroup hierarchy

- ↳ Hiera is keyed by hostgroup path: data/hostgroup/punch/puppet/ps/v4/...
- ↳ A node inherits data top-down along its hostgroup path

→ Foreman is the External Node Classifier (ENC)

- ↳ Membership in a hostgroup → which Puppet classes a node includes
- ↳ site.pp translates hostgroups into classes: if \$hg_hostgroup == ...
- ↳ We of course use Foreman for all the rest of features it provides
 - Kickstart templates, partitioning tables → OpenStack Ironic nodes
 - Integration with monitoring, openDCIM

JENS: our git → environments engine

- **Reminder: our r10k-like tool**
- **Turns git branches into ready-to-serve Puppet environments**
 - ↳ Inputs: repository metadata + environment definitions
 - ↳ Environments = trees of symlinks to per-branch module/hostgroup clones
 - ↳ Mounting a NFS on Puppet servers + mounted on admin nodes for people to debug
- **jens-update runs; does CRUD on environments**
 - ↳ Push code → JENS refreshes NFS content → Puppet masters serve it to nodes
 - ↳ Based on GitLab Webhooks for what changed
- **Home-grown & open source (github.com/cernops/jens), in prod since 2013**
 - ↳ If JENS is down, users' pushes simply don't reach their machines

PUNCH: the hostgroup that runs the infra

→ PUNCH = the control plane for config management itself

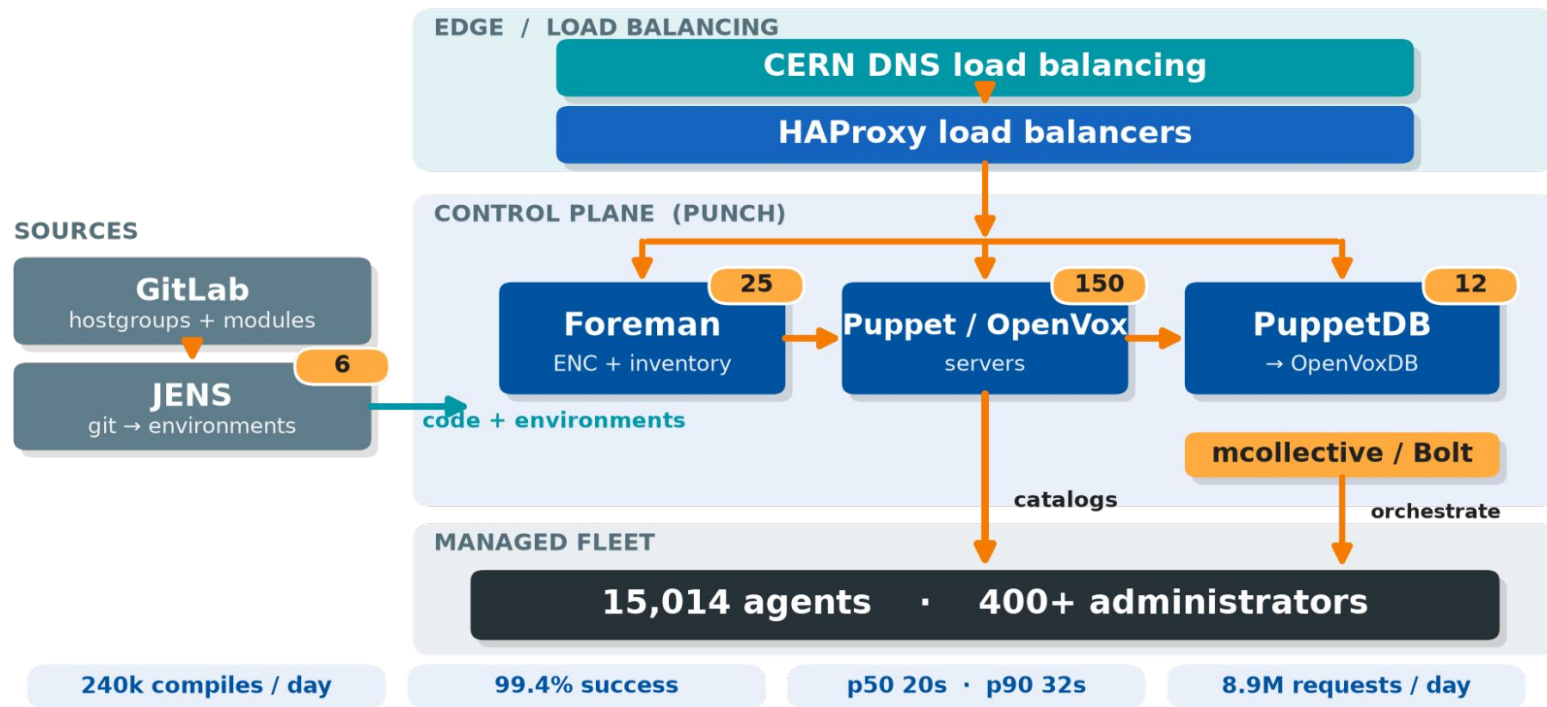


- ↳ 215 nodes run the whole config service
- ↳ 150 Puppet / OpenVox servers behind HAProxy (pools batch a/b, devel a/b/c)
 - Will probably reduce the fleet this year, it is now overdimensioned
- ↳ 25 Foreman nodes (UI, API, ENC, reports); 6 PuppetDB nodes + LBs & garbage collectors
- ↳ 6 JENS, 6 cache, 2 CI runners, 2 Rundeck (crund), 1 general tooling machine

→ Everything HA & load-balanced via CERN DNS-LB + HAProxy

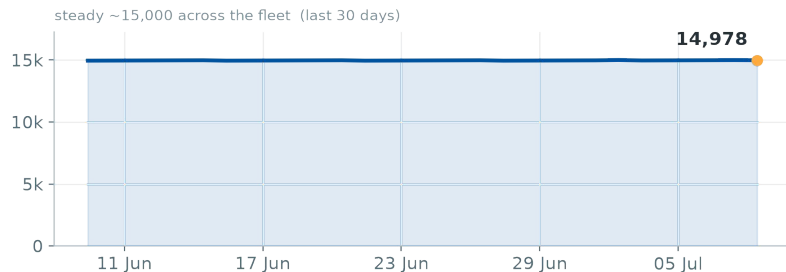
- ↳ Flume-based log enrichment ships component logs for monitoring

Anatomy of the PUNCH control plane

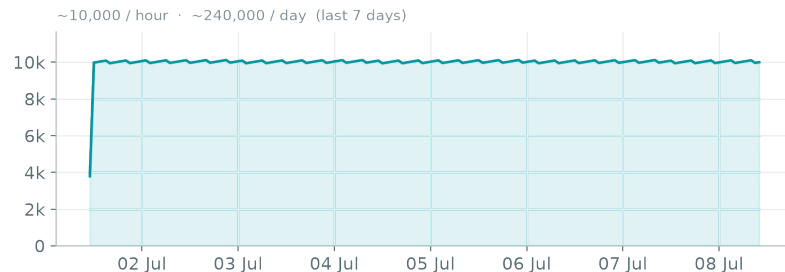


PUNCH by the numbers

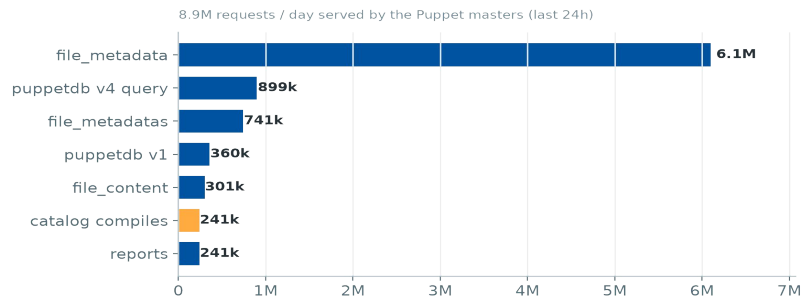
Distinct agents managed per day



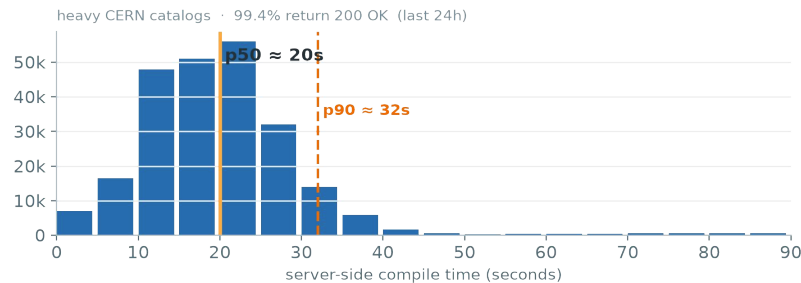
Catalog compilations per hour



HAProxy requests by endpoint



Catalog compile time distribution



Foreman as our ENC (and our fork)



- **Puppet masters call Foreman as the external node classifier**
 - ↳ `external_nodes = /usr/local/bin/foreman-enc.rb --no-cache-fallback`
 - ↳ `foreman-enc.rb` is CERN-written; we push facts to Foreman directly
- **We wrap Foreman with our own ai-foreman CLI**
- **We still run an old Foreman (2.4), heavily patched for our scale**
 - ↳ A stack of `foreman-cern-*.patch` carried on top of upstream
 - ↳ Plans on upgrading, with the drawback of losing features on host visualization

PuppetDB at CERN scale

→ 6 PuppetDB nodes; v8

- ↳ Separate sync / async / gc roles, all HAProxy-balanced
- ↳ Fed by 240k catalog compilations a day across 146 masters

→ We patched the PDB terminus to filter facts before storage

- ↳ Beyond facts-blocklist, works for structured facts too
- ↳ Upstreamed as puppetlabs/puppetdb PR #4021
- ↳ Ideally we will try to push this onto openvoxdb later on

→ Real-world load: certain users hammer PDB

- ↳ ~170 parallel 2 to 3 min queries exhaust the connection pool



mcollective: still alive, still maintained

- **Fleet orchestration still runs on marionette-collective**
 - ↳ `mco puppet disable` / service stop across a hostgroup in one command
- **We keep the ecosystem alive on our GitLab, rebuilt for EL10**
- **Those gems ship in our meta packages, see the migration next**
- **Our goal is to productionise the use of Bolt, PoC worked fine, we need to properly deploy and document; many teams have mco all over their operational docs**

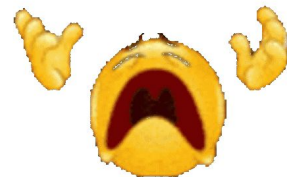
↳ We announced the removal and everyone got nervous



PART 2

Migrating to OpenVox

One meta-package to flip a fleet



For most, a repo swap. For us, an archaeological dig

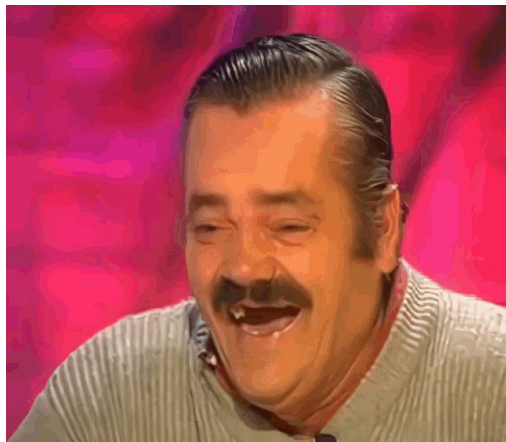
- 15,000+ machines · 400+ administrators · ~15 years of config history
 - ↳ Data centres, accelerator controls, physics analysis grids
- OpenVox itself was the easy part
- The real debt was in the abstractions we built on top of Puppet
 - ↳ JENS, hostgroups, ai-* tooling, mcollective, home-grown ENC glue
- A post-mortem and a mid-mortem, tied to CERN's long-term open-source strategy
- New service managers, adventure time



Switching to Openvox



→ Go through <https://voxpupuli.org/openvox/install/> switch repos, switch package names, done



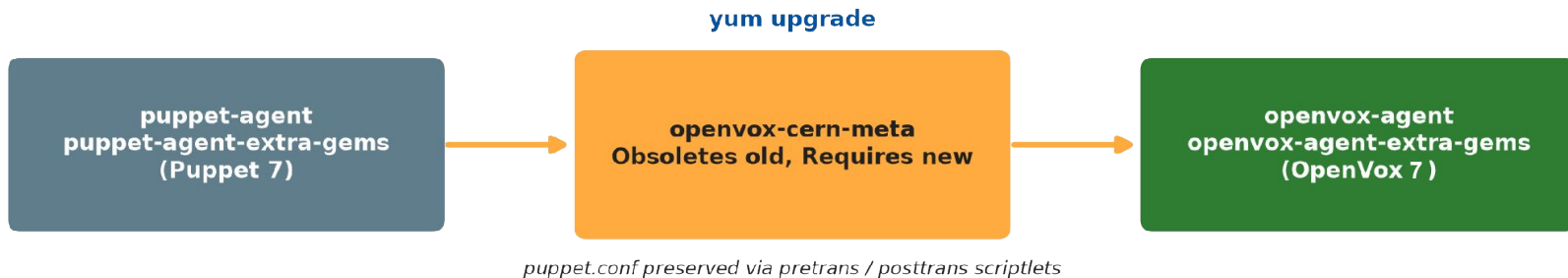
... Maybe not ...

No more building our own agent

- We use the OpenVox agent RPM from upstream (mirrored)
 - ↳ Will start using it for Windows installers soon
- Was: rebuild puppet-agent with extra deps such as mco
 - ↳ Now: consume upstream openvox + a thin CERN meta on top
- Less carry, same guarantees, reproducible
- Since we had to support RHEL10/Alma10, we did it from the ground for them, then extrapolate for 8 and 9

openvox-cern-meta: one package to rule them all

- A single meta-RPM flips a node from Puppet to OpenVox
 - ↳ Obsoletes: puppet-agent < 8.0.0, puppet-agent-extra-gems < 8.0.0
 - ↳ Requires: openvox-agent, openvox-agent-extra-gems, virt-what, pciutils
- Config is preserved across the swap, with no re-bootstrap
 - ↳ %pre backs up puppet.conf; %posttrans restores it
- A plain dnf upgrade' does the migration, driven by Obsoletes



openvox-cern-meta + extra gems

```
Name:      openvox-cern-meta
Version:   2.0.1
Release:   5%{?dist}
Summary:   CERN transition meta-package: migrates puppet-agent to openvox-agent
License:   MIT
URL:       https://gitlab.cern.ch/ai-config-team/openvox
BuildArch: noarch
```

```
Requires:  openvox-agent
Requires:  openvox-agent-extra-gems
Requires:  virt-what
Requires:  pciutils
%if 0%{?el10}
Requires:  python3
Requires:  python3-setuptools
%endif
```

```
Obsoletes: puppet-agent < 8.0.0
Obsoletes: puppet-agent-extra-gems < 8.0.0
```

```
%description
Transition meta-package for CERN that migrates machines from puppet-agent to
openvox-agent. When installed, it obsoletes puppet-agent and
puppet-agent-extra-gems, pulling in openvox-agent and openvox-agent-extra-gems
as replacements. It preserves the existing puppet.conf configuration across the
transition so that agent settings are not lost when puppet-agent is removed.
```

```
%pre -p /usr/bin/bash
if [ -f /etc/puppetlabs/puppet/puppet.conf ]; then
    cp -a /etc/puppetlabs/puppet/puppet.conf /etc/puppetlabs/puppet/puppet.conf.openvox-transition
    echo "openvox-cern-meta: backed up puppet.conf to puppet.conf.openvox-transition"
fi
```

```
%posttrans -p /usr/bin/bash
if [ -f /etc/puppetlabs/puppet/puppet.conf.openvox-transition ]; then
    if [ ! -f /etc/puppetlabs/puppet/puppet.conf ]; then
        mv /etc/puppetlabs/puppet/puppet.conf.openvox-transition /etc/puppetlabs/puppet/puppet.conf
        echo "openvox-cern-meta: restored puppet.conf from openvox-transition backup"
    else
        rm -f /etc/puppetlabs/puppet/puppet.conf.openvox-transition
        echo "openvox-cern-meta: puppet.conf still present, removed transition backup"
    fi
fi
```

```
# Meta-package: nothing to prep, build, or install
```

```
# Octocat stuff
Source20: https://rubygems.org/downloads/diffy-%{diffy_version}.gem
Source21: https://rubygems.org/downloads/hashdiff-%{hashdiff_version}.gem
Source22: https://rubygems.org/downloads/httparty-%{httparty_version}.gem
Source23: https://rubygems.org/downloads/mime-types-data-%{mime_types_data_version}.gem
Source24: https://rubygems.org/downloads/mime-types-%{mime_types_version}.gem
Source25: https://rubygems.org/downloads/multi_xml-%{multi_xml_version}.gem
Source27: https://rubygems.org/downloads/octocatalog-diff-%{octocatalog_diff_version}.gem
Source28: https://rubygems.org/downloads/parallel-%{parallel_version}.gem
Source29: https://rubygems.org/downloads/rack-%{rack_version}.gem
```

```
# Mcollective stuff
Source30: https://rubygems.org/downloads/sshkeyauth-%{sshkeyauth_version}.gem
Source31: https://rubygems.org/downloads/ed25519-%{ed25519_version}.gem
Source34: https://rubygems.org/downloads/bcrypt_pbkdf-%{bcrypt_pbkdf_version}.gem
Source36: https://rubygems.org/downloads/net-ssh-%{net_ssh_version}.gem
Source37: https://rubygems.org/downloads/stomp-%{stomp_version}.gem
Source38: https://rubygems.org/downloads/socksify-%{socksify_version}.gem
```

```
# rubygem-ipaddress for network module.
Source40: https://rubygems.org/downloads/ipaddress-%{ipaddress_version}.gem
```

```
# rubygem-puppet-pson to replace vendored parallel_version
Source50: https://rubygems.org/downloads/puppet-pson-%{puppet_pson_version}.gem
```

```
# Ruby 3.2 support to sshkeyauth
# https://github.com/jordansissel/ruby-sshkeyauth/pull/7
Patch0: sshkeyauth-7.patch
```

```
# Support signatures beyond rsa-ssh
# https://github.com/jordansissel/ruby-sshkeyauth/pull/8
Patch1: sshkeyauth-8.patch
```

```
# Always sign with rsa-sha2-256
# https://github.com/jordansissel/ruby-sshkeyauth/pull/9
Patch2: sshkeyauth-9.patch
```

```
BuildRequires: gcc
BuildRequires: libffi-devel
BuildRequires: cmake
BuildRequires: make
BuildRequires: libgit2-devel
BuildRequires: libxml2-devel
BuildRequires: libxslt-devel
BuildRequires: chrpath
BuildRequires: openvox-agent >= 7.35.0
%if 9%{?el6}%{?el7}
BuildRequires: pkgconfig
%else
BuildRequires: pkgconf-pkg-config
%endif
```

```
Requires: openvox-agent >= 7.35.0
```

```
%description
Extra gems that are installed openvox-agent space
```



openvox-agent-extra-gems: the CERN extras



- The gems our tooling needs beyond the base agent
 - ↳ mcollective stack: stomp, net-ssh, sshkeyauth, ed25519, bcrypt_pbkdf
 - ↳ puppet-pson replaces the PSON gem dropped in Puppet 8
 - ↳ octocatalog-diff for catalog diffing in CI and change review
- New direction: extras now depend on the agent, not the reverse
 - ↳ Kills the old circular build dep
- mcollective itself now ships here, not as a fat agent patch
 - ↳ Patched gems ride with upstream PRs (sshkeyauth [#7](#)/[#8](#)/[#9](#))

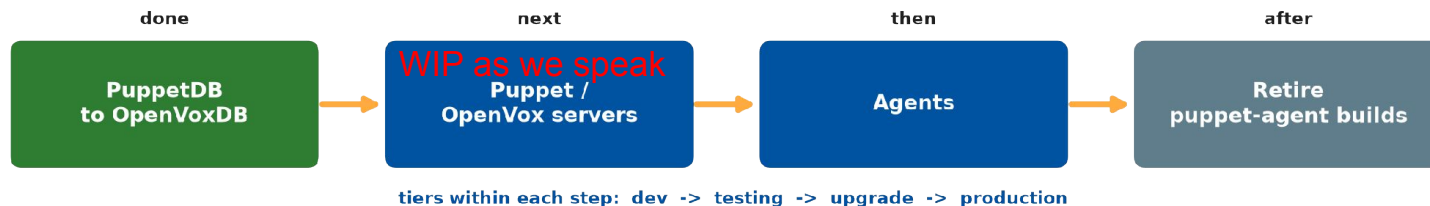
How we're doing it: our principles

- **Stop building & patching our own agent RPM**
 - ↳ It blocked point-release upgrades and “made us special”
- **Server-side: patch via the Puppet `patch` module, not the RPM**
 - ↳ Only two patches left: `plugin_sync` + `skip node resources`
 - `Plugin_sync` allows us to avoid no matter what module from bringing custom facts in your hostgroup. Service managers control what they allow to run on their fleet.
- **Extras depend on the agent, not the reverse**
 - ↳ Removes the circular build dep; `mcollective` moves into extras
- **Servers before agents (reversed only during dev)**
- **Keep legacy facts (`include_legacy_facts=true`) until 8 is steady**

Rolling it out across the fleet



- Phased by hostgroup, control plane (PUNCH) validated first
 - ↳ dev / qa / upgrade hostgroups before production
- roger appstate gates disruptive steps; alarms silenced during moves
- No big-bang: nodes flip as they pick up the meta-package
- puppet.conf preserved → no mass re-signing / re-bootstrap

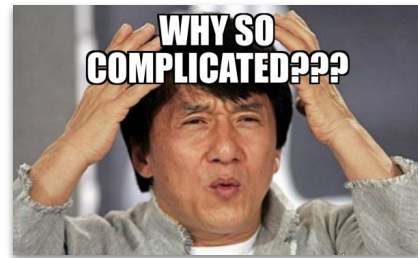


tiers within each step: dev -> testing -> upgrade -> production

Note: the whole switch has already been validated, but it is awaiting for holidays season to be over

First real switch: PuppetDB → OpenVoxDB

- In production since 11 Jun 2026 (full PDB downtime)
- Forced to go first: openvoxdb requires openvox-agent ≥ 8.26
 - ↳ So PDB nodes crossed to the OpenVox agent + OpenVox 8 ahead of the fleet
 - ↳ But the rest of our infra runs with Puppet/Openvox agent 7!
- D-day = a bundle-switch of three modules
 - ↳ Osrepos: where we switch the repos from puppet to voxpupuli
 - ↳ Cernmco: where we control our MCollective setup to use our RPM
 - ↳ Cernpuppet: where we control our Puppet package versions and config
- Upstreamed: [puppet-openvoxdb PR #48](#), merged before go-live



Crossing to Puppet 8 / Ruby 3: the fun bugs

- CA-refresh storms after agent 8 → `ca_refresh_interval` workaround
 - ↳ Reported upstream as [OpenVox issue #435](#). We do not refresh certs like this. Fixed a few days ago!
- Ruby 3.2 removed `FileTest.exists?`
 - ↳ Bit custom facts and `mcollective` core → `mco 2.13.3`
- Vendored PSON gone → `teigi autoload` broke
 - ↳ Ship `puppet-pson` via `openvox-agent-extra-gems` (for now)
- RPM churn: `obsoletes`, `version-locks`, vanished `systemd` units
 - ↳ Pin `openvox-agent` to `openvoxdb`'s version; re-link `puppetdb.service`

Funny current state

- OpenVoxDB 8 running openvox-agent 8
- QA: Openvox-server 7 running openvox-agent 7
- PROD: Puppet-server 7 running openvox-agent 7
- Some clients running openvox-agent 7
- Others running puppet-agent 7



We upstream, but want to give back more

- OpenVox core: CA-refresh bug report, [issue #435](#)
- puppet-openvoxdb: [PR #48](#), our OpenVoxDB module fixes (merged)
- in the good ol' days:
 - ↳ Foreman
 - ↳ mcollective ecosystem
- PuppetDB terminus fact-filter, [PR #4021](#)
- Goal: shrink our patch set, keep the OpenVox ecosystem healthy
- A great kudos to Steve Traylen, our Puppet guru who contributes to upstream regularly

Status & lessons learned



→ Where we are (Jul 2026)

- ↳ PuppetDB DONE, Puppet masters DONE in QA (which serve real production load), Agents TESTED and ready

→ What worked: OpenVox behaved as a drop-in, Obsoletes meta-package = low drama

- ↳ Preserving puppet.conf was the single most important detail

→ Lessons: patch via modules, stop forking the agent RPM

- ↳ Servers before agents; keep legacy facts until 8 is steady state

→ Next: finish agents, retire puppet-agent builds, docs, Bolt

- ↳ Windows team will handle the agent switch separately

And then?

- Upgrade Foreman to something recent
- Migrate to OpenVox 8 all over the place
 - ↳ CI validation before deadline
 - ↳ Pushing all service managers
 - ↳ And finally drop all CentOS 7 support we kept on a best effort basis for some use cases...Yes, we know.
- Evaluate Ansible integrations
- Evaluate more options to give back to VoxPupuli
 - ↳ Initial internal discussions (the mills of God grind slowly)



THANK YOU

Questions?

Daniel Juárez · CERN IT-CD-CC · dajuarez@cern.ch

