A not-so-bumpy road to Puppet 4 at CERN
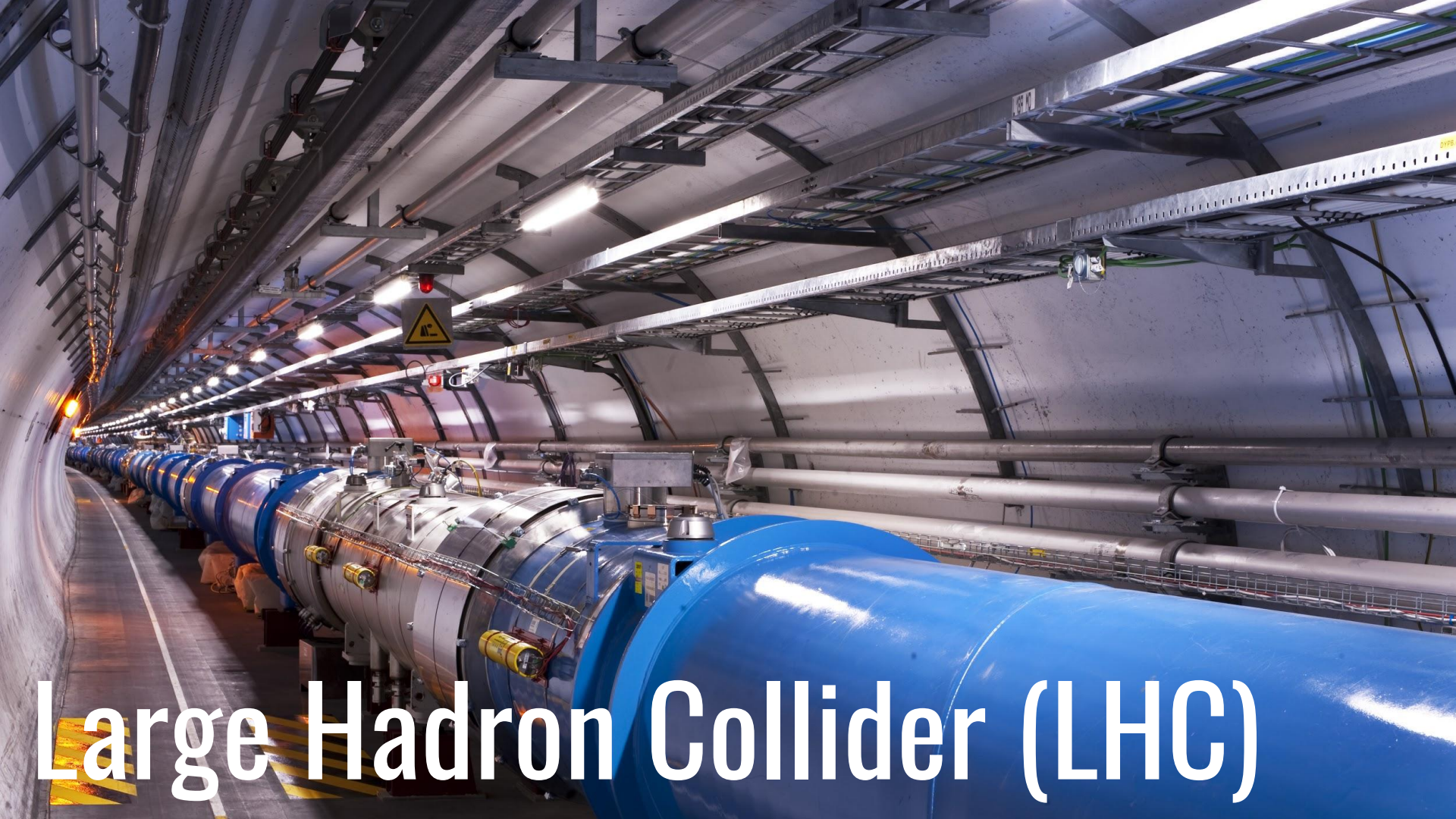
nacho.barrientos@cern.ch
CERN IT Department

On the French-Swiss border
22 member states
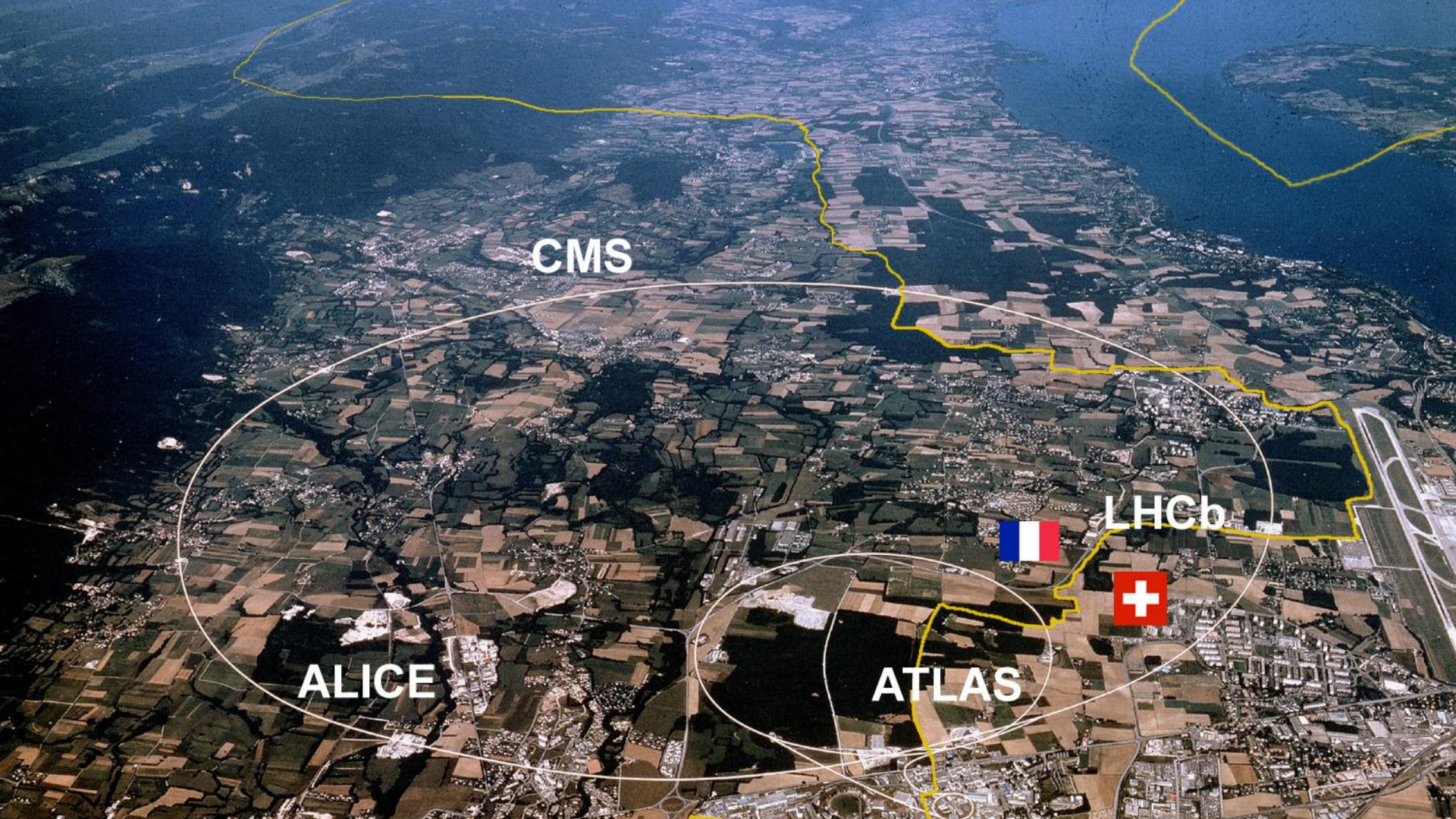Collaborators from all around the world
What do we do?

Large Hadron Collider (LHC)

Compact Muon Solenoid (CMS)
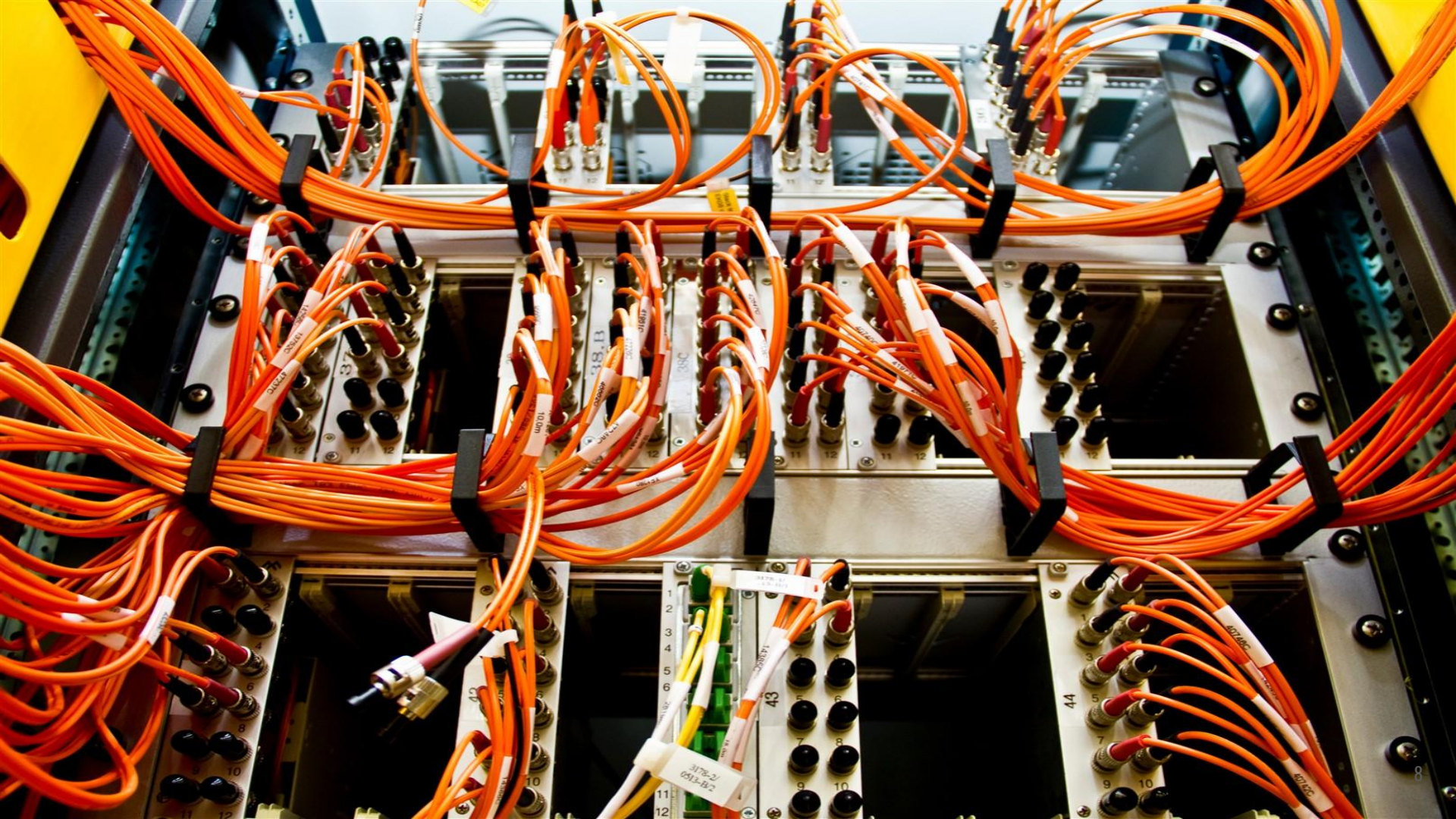
https://home.cern
https://visit.cern

CERN Service Portal
easy access to services at CERN

Home   News ▾   Service Information ▾   Navigate Catalogue ▾   Contacts   My Profile ▾   Site Guide

⊕ Service Availability Overview

✓ Service Available   ⚠ Service Degraded   ⊖ Service Unavailable   ℹ Informational Message   ? No Information

Public screens view | Minimal view | FAQ

Batch Services
- Batch
- BOINC
- HPC

Collaboration Services
- Conference Rooms
- E-Mail
- Eduroam
- Lync
- Sharepoint

Computer Security Services
- Certificate Authority
- Single Sign On and Account Management

Data Analytics Services
- HADOOP

Database Services
- Accelerator Database
- Administration Database
- Database on Demand
- Database Replication
- Experiment Database
- General Purpose Database

Desktop Services
- Windows Desktop

Development Services
- Git
- JIRA
- SVN

Document Management Services
- CDS

Engineering Software Services
- Electronics Design Software
- Mathematics Software
- Mechanical Design Software

GRID Services
- File Transfer
- GRID Compute Element
- GRID Development
- GRID Information
- GRID Infrastructure Monitoring
- MyProxy
- VOMS

Infrastructure Application Services
- Indico Event Application Support

Interactive Services
- LXPLUS
- Windows Terminal Servers

IT Infrastructure Services
- ACRON
- Centralised Elasticsearch
- Configuration Management
- Linux Operating System
- Load Balancing
- Messaging
- Monitoring
- Server Provisioning

Network Services
- Campus Network
- CIXP
- Datacenter Network
- Network Database and Registration
- Network for Projects and Experiments
- Technical Network
- WIFI
- WLCG Network

Printing Services
- Printing and Copying

Storage Services
- AFS
- Backup and Restore
- CASTOR
- Ceph
- CERNBox
- CVMFS
- DFS
- EOS
- FILER

Telephone Services
- E-Fax
- Fixed Line Phone

Text and Media Services
- Alerter
- MultiMedia
- Public Information Display

Web Services
- AFS Web Hosting
- CERN Search
- Databases Applications
- Drupal
- IIS Web Hosting
- Java Web Hosting
- PaaS Web Application Hosting
- Twiki

34k active nodes in PuppetDB

Base catalog contains **1.2k** resources

350 catalogs compiled per minute

191 changes* per day

350 puppeteers

CONFIG TEAM
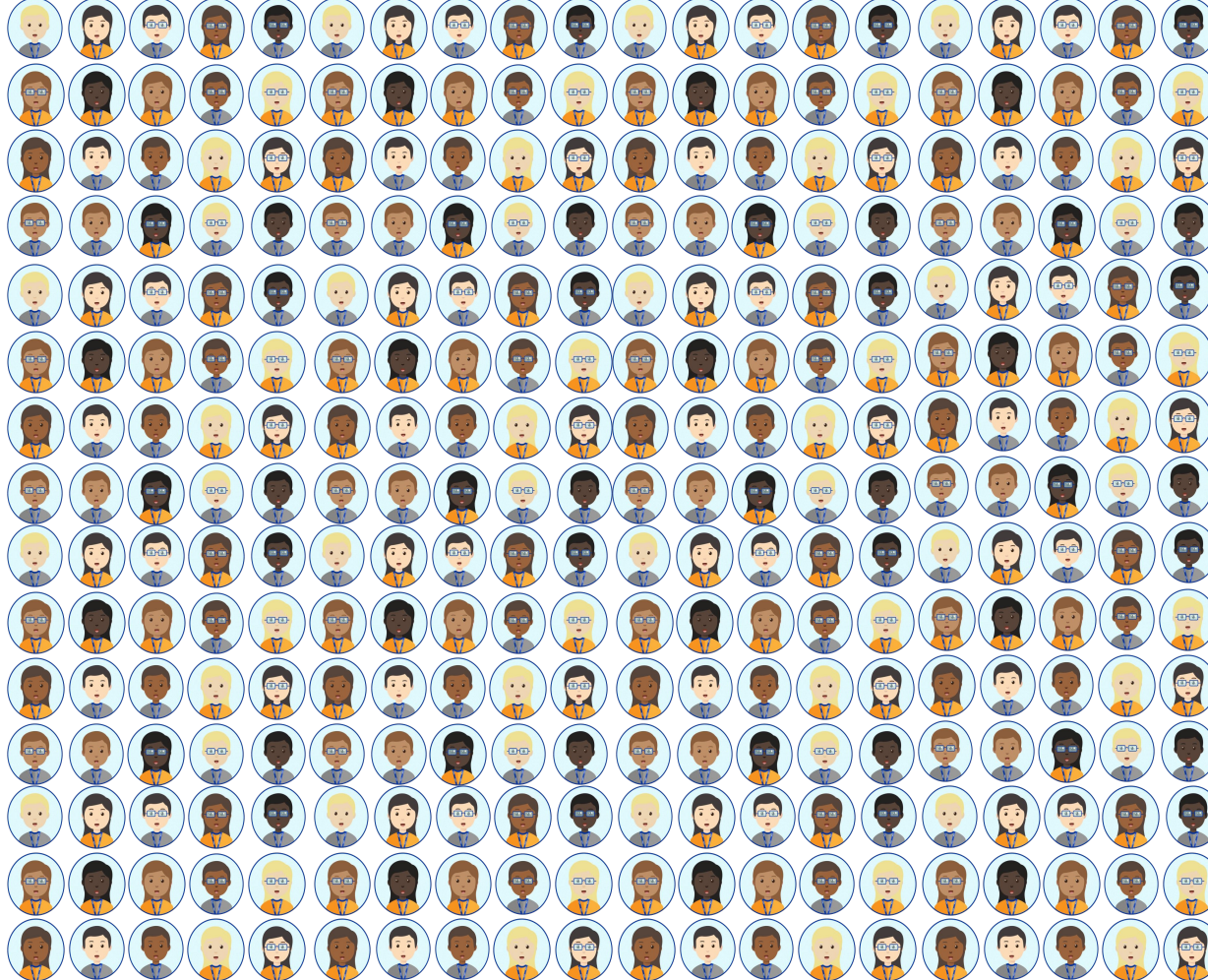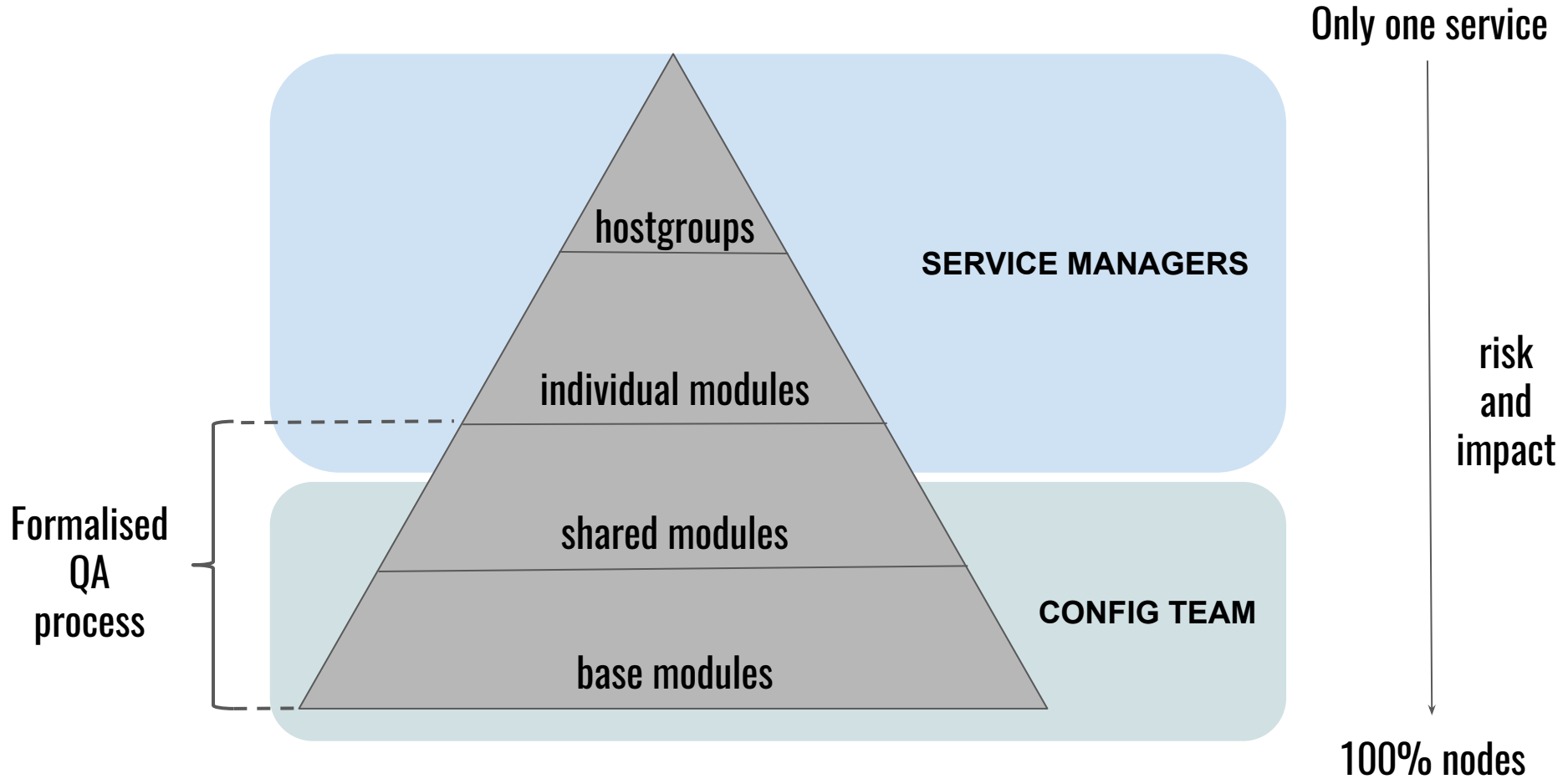
CONFIG TEAM

CONFIG TEAM

SERVICE MANAGERS

16

Only one service

risk and impact

100% nodes

SERVICE MANAGERS

CONFIG TEAM

hostgroups

individual modules

shared modules

base modules

Formalised QA process

Changes to QA are <u>announced</u> publicly
Typical QA duration: 1 week
All service managers can <u>stop</u> them

https://github.com/cernops/jens

Our trip from Puppet 3 to Puppet 4

The preps…

Parallel server infrastructure

CI framework

Base configuration dual compatibility

Planning and communication

1 Volunteer runs against Puppet 4 servers
CI preaching

2

3

When the ground started to shake

Castings that became errors

```
2. if $::operatingsystemmajrelease <= 6 {
3.     ...
4. }
```

Changed boolean interpretation ('')

```
3. if $variable {
4.     ... you are running puppet 4.
5. } else {
6.     ... you are running puppet 3.
7. }
```

Variable scope and nested classes

```
class outer {
  $var = 'dynamic'
  include inner
}
```

```
class inner {
  notice(inline_template('<%= @var %>'))
}
```

Hiera variable names (dots)

```
$stream_prune_log_max    = hiera('snort.stream_prune_log_max', '0')
```

```
34 task test: [
35    :metadata_lint,
36    :syntax,
37    :lint,
38    :spec,
39 ]
```

Status	Build ID	Name	
⊘ passed	#201467 `docker`	puppet3	⏱ 01:09 📅 36 minutes ago
⊘ passed	#201468 `docker`	puppet4	⏱ 01:12 📅 36 minutes ago
⊗ failed	#201469 `docker` `allowed to fail`	puppet4_latest	⏱ 00:51 📅 36 minutes ago

Status   **Build ID**   **Name**

⊘ **Tests**

1 Volunteer runs against Puppet 4 servers
CI preaching
Bugging people!

2

3

RECENT ACTIVITY IN PUPPET LAND

Bigger is more recent. Includes topic branches. *Modules are represented in blueish*, *hostgroups in yellowish*.

Countdown to Puppet 4 in QA

0	16	44	02
Days	Hours	Minutes	Seconds

cloud_monitoring cloud_monitoring dbnetworkconfig voatlasrucio

dbhwbunchconfig grid_wlmanagement appserver aistools aiadm gfal2 hdp cloud_baremetal

vopanda sts na62_rc aimon hadoop monitoring dmaas

puppetserver its bi lemon ofed cloud_identity voatlasmisc

gridftp playground fence etf fts vocmsdb asterisk

compass tone it_es xrootd cds keystone kamailio

cloud_compute mdm dpm jens

drupal_service shibboleth phmicdm creamce database

streaming metricmgr paas acronsvc mpi boinc slurm

vocmsglidein procurement pentaho

dbcoreconfig

27

1

2 Agents (still Puppet 3) pointed to Puppet 4

3

(in the meantime)
Preparing the agent upgrade...

1

2

3

puppet-3.8.7cern5

puppet-3.8.7cern6
puppet-agent-0.0.0

puppet-agent-1.8.2.10

(in the meantime)
Preparing the agent upgrade...

Custom facts (Facter 2.x → Facter 3.x)

```
m/params.pp
1  class landb::params {
2
3    if versioncmp($::puppetversion,'4') >= 0 {
4      $default_landb_config = '/etc/puppetlabs/puppet/landb_config.yaml'
5    } else {
6      $default_landb_config = '/etc/puppet/landb_config.yaml'
7    }
8
```

```
if Gem::Version.new(Facter[:puppetversion].value) >= Gem::Version.new('4')
  config_path  = '/etc/puppetlabs/puppet/landb_config.yaml'
else
  config_path  = '/etc/puppet/landb_config.yaml'
end
```

Dual configuration ([/etc/puppet, /etc/mcollective] ↔ /etc/puppetlabs/*)

1

2

3 Agent upgrade to Puppet 4

QA

24H PRODUCTION ROLL-OUT

3.5 months

1

2

3

Puppet 3.x

Puppet 4.x

And that 5%?

broken catalog, Puppet disabled, broken software updates…

please rebuild/reinstall 😊

Puppet 3.x

Puppet 4.x

Unable! 😎

unpin software repositories,
fix dependency problems,
copy puppet.conf and run Puppet…

...usually helped

What did go wrong?

User crontabs removed from CVMFS Stratum 0 release manager machines

Type:
Service Incident

Incident Status:
Resolved

Begin:
Wed, Mar 29, 2017 13:48

Service Impact:
Degraded

Sixtrack user cronjobs lost

SE: BOINC Service, FE: BOINC Support,

As a consequence of the change of Puppet behaviour to purge all non-puppet managed cron jobs (CRM-2188),

Root Cause: Puppet 3 to Puppet 4 upgrade, and change of default behaviour with respect to cron. (CRM-2188), not detected in QA,

cron jobs removed for AIS

SE: Oracle Web Hosting Service, FE: Application Middleware Infrastructure,

As a side effect of Puppet 4 agent installation, crontab jobs have been removed from AIS main job scheduling machine.

What could we have done better?

Earlier CI

Module or Hostgroup	Master Brach	QA Branch	Modulesync Branch
it-puppet-hostgroup-acronsvc	build success	build success	build success
it-puppet-hostgroup-afssrv	build success	build success	build unknown
it-puppet-hostgroup-aiadm	build success	build success	build success
it-puppet-hostgroup-aimon	build success	build success	build failed
it-puppet-hostgroup-appserver	build success	build success	build success
it-puppet-hostgroup-backup	build success	build success	build success
it-puppet-hostgroup-batchmon	build unknown	build unknown	build failed

it-puppet-module-security	build success	build success	build unknown
it-puppet-module-selinux	build success	build success	build success
it-puppet-module-sendmail	build success	build success	build success
it-puppet-module-serf	build failed	build failed	build failed
it-puppet-module-shibboleth	build success	build success	build unknown
it-puppet-module-singularity	build success	build success	build success
it-puppet-module-slurm	build success	build success	build success

Catalog diffs (octocatalog-diff?)

Ongoing activities

SERVICE MANAGERS

Multi-tenancy

Packing problem
Auto-scaling
Auto-creation
Low maintenance

www.cern.ch

Backup slides

but ... what about development?

Create topic branches as neccesary → Create environment → **Can reuse node?**

Can reuse node? — Yes → Move node to new environment
Can reuse node? — No → Create node in new environment

→ Make changes on topic branches → Run Puppet and tests → **More changes needed?**

More changes needed? — Yes → (back to Make changes on topic branches)
More changes needed? — No → Create MR (or update) to qa → Review MR (somebody else)

Review MR → **Is it a shared module?**
Is it a shared module? — No → Merge to qa
Is it a shared module? — Yes → Announce change → Merge to qa

Merge to qa → **Side effects?**
Side effects? — No → **Is a shared module?**
Side effects? — Yes → (back to Make changes on topic branches)

Is a shared module? — No → Create MR to master
Is a shared module? — Yes → **Is QA time over?**

Is QA time over? — Yes → Create MR to master
Is QA time over? — No → (back to Merge to qa)

Create MR to master → Merge to master → **Reused node?**
Reused node? — No → Delete node
Reused node? — Yes → Move node to old environment

Delete node / Move node to old environment → Delete topic branches and environment

45

```
ibarrien@aiadm13: (master)
~/it-puppet-environments $ cat ai4632.yaml
---
default: qa
notifications: nacho.barrientos@cern.ch
overrides:
  modules:
    flume: monit564
  hostgroups:
    punch: ai4632
ibarrien@aiadm13: (master)
~/it-puppet-environments $
```

```
ibarrien@aiadm13: (master)
~/it-puppet-environments $ cat ai4632.yaml
---

default: qa
notifications: nacho.barrientos@cern.ch
overrides:
  modules:
    flume: monit564
  hostgroups:
    punch: ai4632
ibarrien@aiadm13: (master)
~/it-puppet-environments $ ai-foreman -l punch/aijens showhost
+-------------------+----------------------------+-------------+-------------+
| Name              | Hostgroup                  | Environment | OS          |
+-------------------+----------------------------+-------------+-------------+
|       -dev01.cern.ch | punch/aijens/b/live/secondary | ai4632      | CentOS 7.2 |
|       101.cern.ch | punch/aijens/a/live/primary   | production  | CentOS 7.2 |
|       103.cern.ch | punch/aijens/a/live/secondary | production  | CentOS 7.2 |
|       112.cern.ch | punch/aijens/b/live/primary   | production  | CentOS 7.2 |
|       113.cern.ch | punch/aijens/b/live/secondary | qa          | CentOS 7.2 |
+-------------------+----------------------------+-------------+-------------+

ibarrien@aiadm13: (master)
~/it-puppet-environments $ 
```

```yaml
# Snapshot created on 2016-10-31 11:01:04.352940 based on production
---
notifications: foo@cern.ch
overrides:
  common:
    hieradata: commit/86e0d3c6636e78813fe5e924742c94da0f1216d9
    site: commit/c5ea298afec55e67de6bad8e47a1a2d9fd3aed11
  hostgroups:
    appserver: master
    database: master
    dblc: master
  modules:
    aodh: commit/e0b021f79c9f4629a884badbe82dddf630c5a60e
    apache: commit/79b49ed69d729dcbe82f9b96ec366d2f45a743d4
    archive: commit/8999548ab4f8d3dad8e8bef18f1f4abc5e7adf29
    augeasproviders_base: commit/80c16064f233976f8b28b515d3edc97c72f036fd
    augeasproviders_ssh: commit/0ae3fa412df4c3cddba6362d8e457d996bc733d6
    augeasproviders_sysctl: commit/402de8dcfd0b62cf482a48a775d6bd80e170b9da
    authwrapper: master
    # etc
```
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"ai434.yaml" 20L, 763C written   20,1   All

A node belongs to a hostgroup

backup/server/tape/lib0
punch/fore/balance/external
cloud_compute/level2/kvm/gva_project_002

it-puppet-hostgroup-myapp
  code
    manifests
      init.pp
      frontend.pp
      frontend
        sso.pp
  data
    hostgroup
      myapp.yaml
      myapp
        frontend.yaml
        frontend
          sso.yaml

myapp

it-puppet-hostgroup-myapp
  code
    manifests
      init.pp
      frontend.pp
      frontend
        sso.pp
  data
    hostgroup
      myapp.yaml
      myapp
        frontend.yaml
        frontend
          sso.yaml

myapp/frontend

it-puppet-**hostgroup**-myapp
  code
    manifests
      init.pp
      frontend.pp
      frontend
        sso.pp
  data
    hostgroup
      myapp.yaml
    myapp
      frontend.yaml
      frontend
        sso.yaml

it-puppet-**module**-apache
  files
  lib
  manifests
    init.pp
    vhost.pp
      …
  templates

frontend.pp

```
class hg_myapp::frontend {
…
  class {'apache':
    server_signature => 'off'
    …
  }
  apache::vhost {
    …
  }
  …
}
```

54

```
it-puppet-hostgroup-myapp
 code
  manifests
   init.pp
   frontend.pp
   frontend
    sso.pp
 data
  hostgroup
   myapp.yaml
   myapp
    frontend.yaml
    frontend
     sso.yaml
  fqdns
   appc003.cern.ch.yaml
```

sso.pp

```
class hg_myapp::frontend::sso {
…
   include shibboleth
…
}
```

sso.yaml

```
shibboleth::session_storage: 'memcache'
shibboleth::memcached_servers:
  - foomc01.cern.ch
  - foomc02.cern.ch
shibboleth::memcached_prefix: "MY_PREFIX:"
shibboleth::remote_user: 'ADFS_LOGIN'
shibboleth::application_name: foo_application
shibboleth::site_name: foo.bar.cern.ch
```
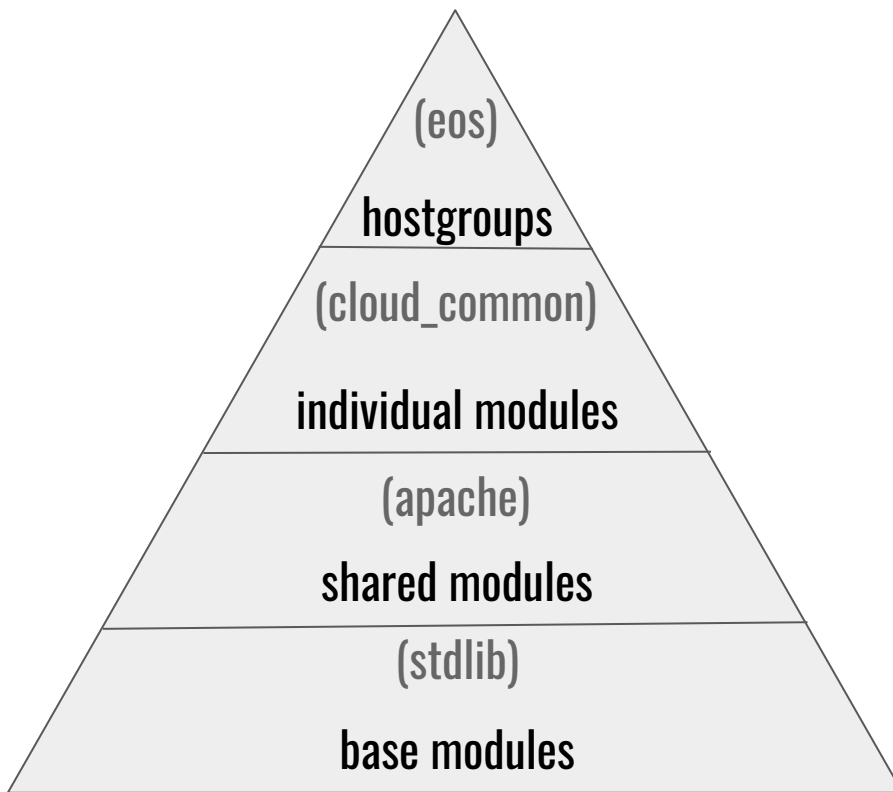
393 <u>modules</u> (upstream and homegrown)

206 top-level <u>hostgroups</u> (services)

Only one service

risk
and
impact

100% nodes

(eos)

hostgroups

(cloud_common)

individual modules

(apache)

shared modules

(stdlib)

base modules

```
[root@nachodev06 ~]# yum clean all
Loaded plugins: kernel-module, priorities, rpm-warm-cache, securit
Cleaning repos: ai6-qa ai6-stable epel epel-testing lemon6-qa lemo
              : slc6-testing slc6-updates
Cleaning up Everything
[root@nachodev06 ~]# puppet --version
3.8.7
[root@nachodev06 ~]# /usr/local/sbin/distro_sync.sh
[root@nachodev06 ~]# puppet
-bash: /usr/bin/puppet: No such file or directory
[root@nachodev06 ~]# source /etc/profile.d/puppet-agent.sh
[root@nachodev06 ~]# puppet --version
4.8.1
[root@nachodev06 ~]# []
```

Or just log in and out!

USERS