
CERN

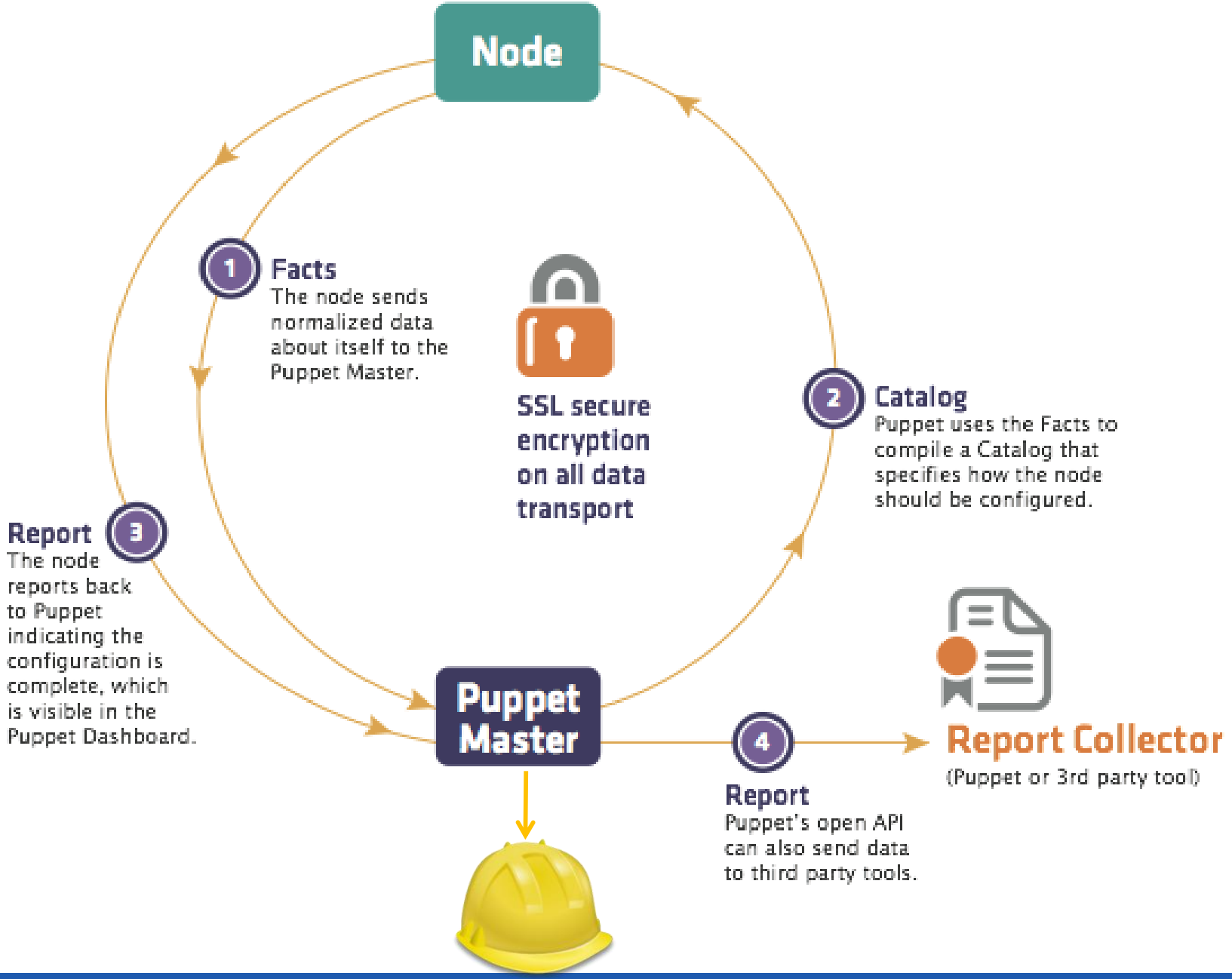
Configuration Management at CERN

Nacho Barrientos <nacho.barrientos@cern.ch>
on behalf of <ai-config-team@cern.ch>

Configuration Management

- Description of the state of IT infrastructure
- Manages everything configuration-wise
- Desirable in tiny data centres, a must in the rest
- CERN IT: From Quattor to Puppet. Why?
  - *Development* started Q1 2012
  - Quattor was fully shutdown Q3 2015

CERN IT's CM infrastructure


Node
1
Facts
The node sends normalized data about itself to the Puppet Master.
SSL secure encryption on all data transport
2
Catalog
Puppet uses the Facts to compile a Catalog that specifies how the node should be configured.
3
Report
The node reports back to Puppet indicating the configuration is complete, which is visible in the Puppet Dashboard.
Puppet Master
4
Report
Puppet's open API can also send data to third party tools.
Report Collector
(Puppet or 3rd party tool)

What describes a node?

- The **hostgroup** to which it belongs

```
+-----------------+-------------------------------------------------------------+
|       Hostname: | p05798818h00153.cern.ch                                     |
|       Hardware: | physical, 32 cores, 62.87 GB memory, 2.00 GB swap, 50 disks |
|      Hostgroup: | castor/c2atlas/diskserver/t0atlas                           |
```

Hierarchical:

castor (top-level)

- c2atlas
  - diskserver
    - t0atlas

- And the **environment**

Can code be reused? Yes!

- Hostgroup ~ service-specific code
- Common config -> modules

46% of our Puppet code is meant to be reused

Challenges

1. Scaling
   - ~18000 agents (physical and virtual)
   - 77 octocore Puppet masters
2. Administratively distinct admins that formally don't trust each other
   - 207 environments
   - 152 hostgroups (or "services")
   - 287 modules (CERN and upstream)

When upstream is not enough

1. Scaling
   - With lots of puppet masters...
   - Code distribution and sync becomes a problem
2. Distinct admins
   - Single repository approach is not viable
   - Need for ACLs and independent Git histories

In-house development, open source:
https://github.com/cernops/jens

Change management

- Distinct services sharing code (via modules)
- Changes to shared code have to be validated
- Workflow:
  - Change announcement
  - In the QA environment for a week
  - Auto merged if nobody has complained

10% rejection rate in QA

Puppet & Openstack @ CERN

```
ibarrien@aiadm205: (~)
~ $ ai-bs-vm --cc7 -g playground/ibarrien nec2015.cern.ch
Trying to bootstrap 'nec2015.cern.ch'...
VM flavor: m1.small
Booting from image: cc7
VM tenant: Personal ibarrien
Foreman environment: production
Foreman hostgroup: playground/ibarrien
Puppet master: it-puppet-masters-public.cern.ch
Certmgr server: baby02.cern.ch
Certmgr port: 8008
Roger server: woger.cern.ch
Roger port: 8201
Preparing dynamic user data...
Using '/usr/share/ai-tools/userdata/puppetinit' as userdata script template to init Pu
Adding host 'nec2015.cern.ch' to Foreman...
Host 'nec2015.cern.ch' created in Foreman
Staging host 'nec2015.cern.ch' on Certmgr...
Host 'nec2015.cern.ch' staged
Using auth plugin: v3kerberos
Using 'CC7 Base - x86_64 [2015-06-12]' as the latest 'CC7' image available
Creating virtual machine 'nec2015'...
Request to create VM 'nec2015' sent
Adding 'nec2015.cern.ch' to Roger
------------------------------------------------------------------------
* Your machine is booting and the network is being configured right now,
  Puppet will run immediately after a successful boot process.
* It typically takes around 30 minutes between this command is
  executed and the first Puppet report arrives to Foreman:
  https://judy.cern.ch/hosts/nec2015.cern.ch/reports
  (although this depends a lot on the complexity of your configuration)
```

The future

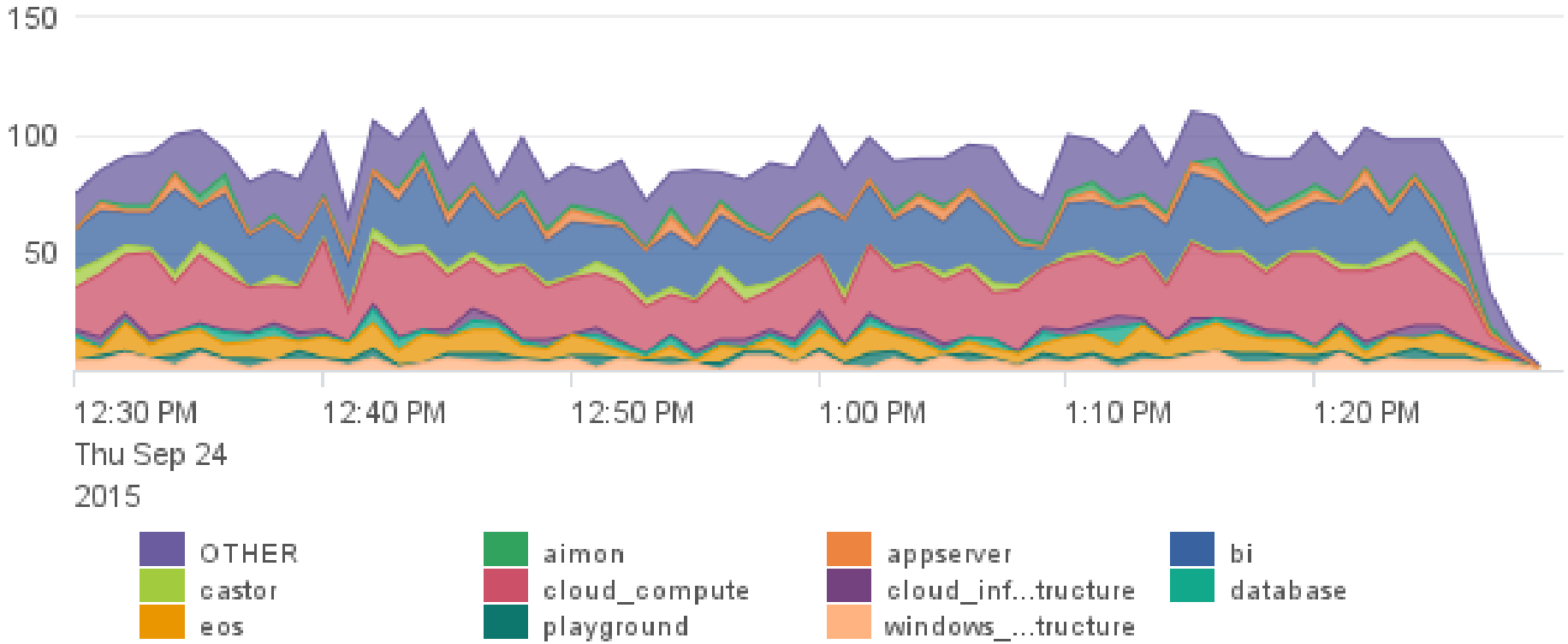
- Continue coping with the growth
  - Puppetserver
  - Puppet4 and next PuppetDB
  - Explore new ways to distribute Puppet code
  - Explore new monitoring possibilities
- *Puppetise* containers
- Add even more automation to the QA process

Configuration Management at CERN

Nacho Barrientos <nacho.barrientos@cern.ch>
on behalf of <ai-config-team@cern.ch>

Backup slides

Catalog requests per top-level hostgroup



Config Release Management / CRM-1362

Add cern_networks4 and cern_networks6 arrays of CIDR cern networks.

Comment | Assign | More | Export

Details

Type: Configuration Change

Status: CLOSED (View Workflow)

Resolution: Fixed

Security Level: Internal Data (Only authenticated CERN users can see this issue)

Labels: common

Change Type: New feature

Change scope: Manifest change

Feature Branch: NONE

Changelog: Simply adds two hiera variables to common.yaml

cern_networks4 and **cern_networks6** are each an array of cern networks as defined by

https://network.cern.ch/sc/fcgi/sc.fcgi?Action=GetFile&file=ip_networks.html

there is zero automatic updating of this list. Please advise if you notice it is wrong.

```
diff --git a/data/common.yaml b/data/common.yaml
+# Copied by hand from
+# https://network.cern.ch/sc/fcgi/sc.fcgi?Action=GetFile&file=ip_
+
+cern_networks4:
+ - 10.0.0.0/8
+ - 100.64.0.0/10
+ - 128.141.0.0/16
+ - 128.142.0.0/16
+ - 137.138.0.0/16
+ - 172.16.0.0/12
+ - 188.184.0.0/15
+ - 192.16.155.0/24
+ - 192.16.165.0/24
+ - 192.91.242.0/24
+ - 192.168.0.0/16
+ - 194.12.128.0/18
+
+cern_networks6:
+ - 2001:1458::/32
```

People

Assignee: Steve Traylen

Assign to me

Reporter: Steve Traylen

Votes: 0 Vote for this issue

Watchers: 2 Start watching this issue

Dates

Created: 09/Sep/15 2:22 PM

Updated: 1 week ago

Resolved: 1 week ago

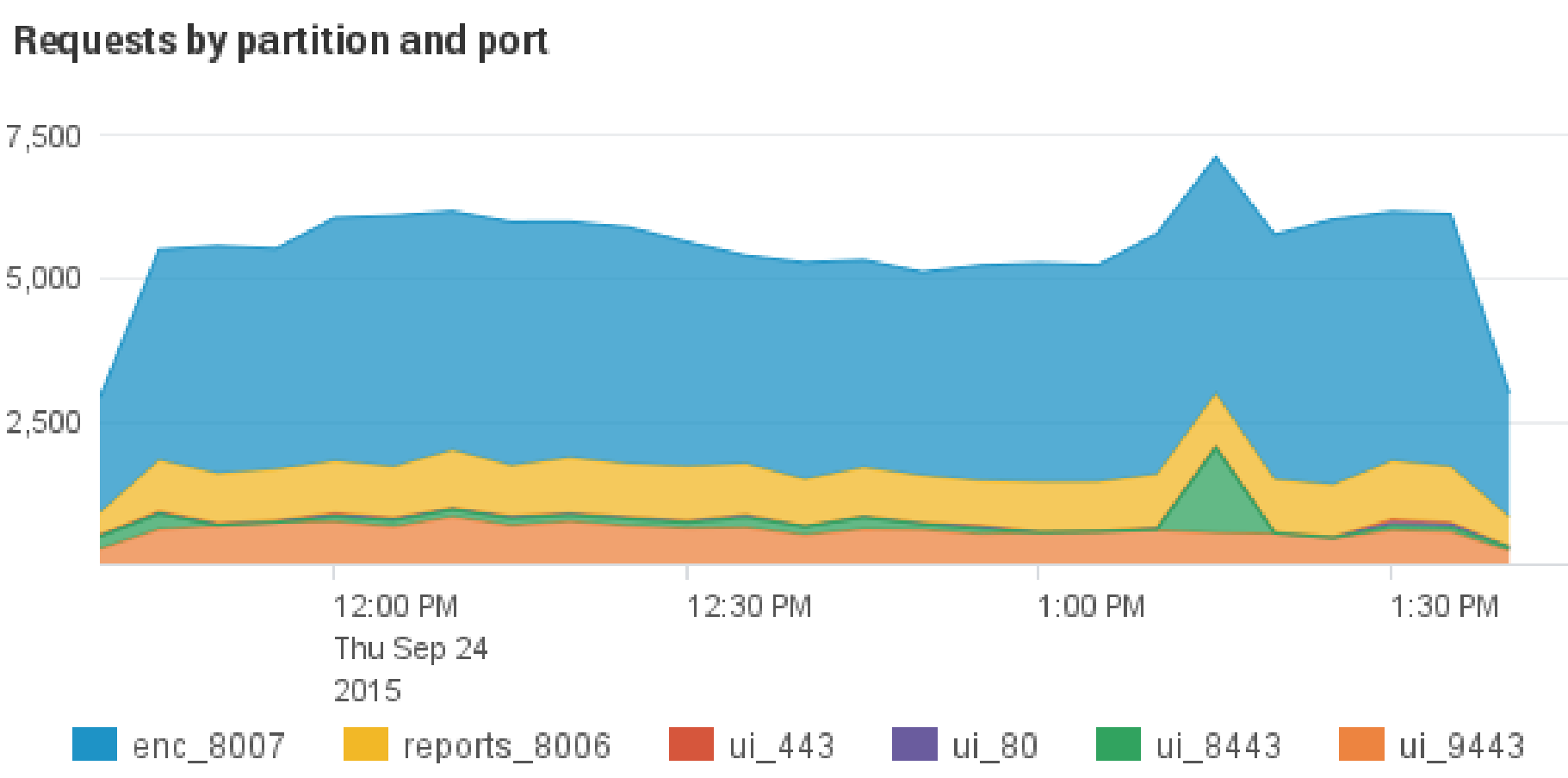
Proposed date for Production: 16/Sep/15

Agile

View on Board

HipChat discussions

Confirm access to your HipChat account for more information.


Requests by partition and port
7,500
5,000
2,500
12:00 PM
Thu Sep 24
2015
12:30 PM
1:00 PM
1:30 PM
enc_8007
reports_8006
ui_443
ui_80
ui_8443
ui_9443

FOREMAN

Nacho Barrientos Arias

Monitor | Hosts | Configure | Infrastructure | Administer

px502.cern.ch

Reports from the last 7 days - 95 reports found

Edit | Build | Delete

Details

Audits | Facts | Reports | YAML

Properties | Metrics | Templates

Properties	
Domain	cern.ch
Monitoring	Dashboards
Realm	
IP Address	188.184.64.90
MAC Address	02:16:3e:01:08:1d
Puppet Environment	production
Host Architecture	x86_64
Operating System	CentOS 7.1
Host group	myproxy/app/live
Owner	myproxy-3rd