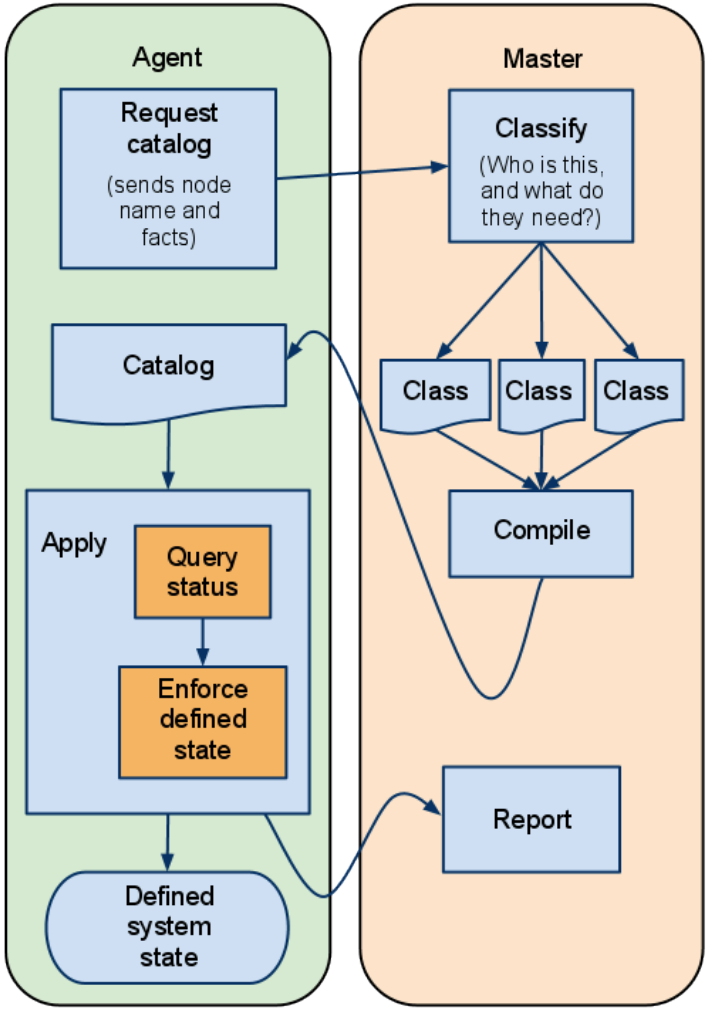
Puppet au CCIN2P3

9èmes Journées Informatiques de l'IN2P3-IRFU

Christelle Eloto, Fabien Wernli
christelle.eloto@cc.in2p3.fr, wernli@in2p3.fr

PUPPET : PRÉSENTATION

- Gestionnaire automatique de configuration
  - OS Unixlike et Windows
  - créé par Luke Kanies en 2005
  - puppetlabs : http://puppetlabs.com
    - version gratuite et commerciale
- Mode master/agent (pull)
  - classes : code Puppet => manifestes
  - catalogue :
    - état désiré des ressources
    - généré à partir des manifestes
  - RQ : un mode standalone existe



http://docs.puppetlabs.com/learning/agent_master_basic.html

PUPPET : CODE & DONNÉES (1)

- Description de la configuration
  - déclaration de ressources (fichier, paquet, service...)
  - classe
    - ensemble de ressources
    - peut être appelée dans le reste du code
    - paramétrable

- Facts
  - FQDN, version d'OS, adresses IP/MAC...
  - issus du client, de l'ENC (External Node Classifiers), d'extra built-in variables

```
class yum::repositories (
  $user,
  $group,
){
  file { '/etc/yum.conf':
    owner  => $user,
    group  => $group,
    mode   => '0644',
    source => [
      "puppet:///modules/yum/yum.conf.${::operatingsystem}",
      'puppet:///modules/yum/yum.conf',
    ],
  }

  file { '/etc/yum.repos.d/sl.repo': ensure => absent, }
  package { 'sl-release': ensure => latest, }

  Package['sl-release'] ~> File['/etc/yum.repos.d/sl.repo']
}
```

exemple de code Puppet

PUPPET : CODE & DONNÉES (2)

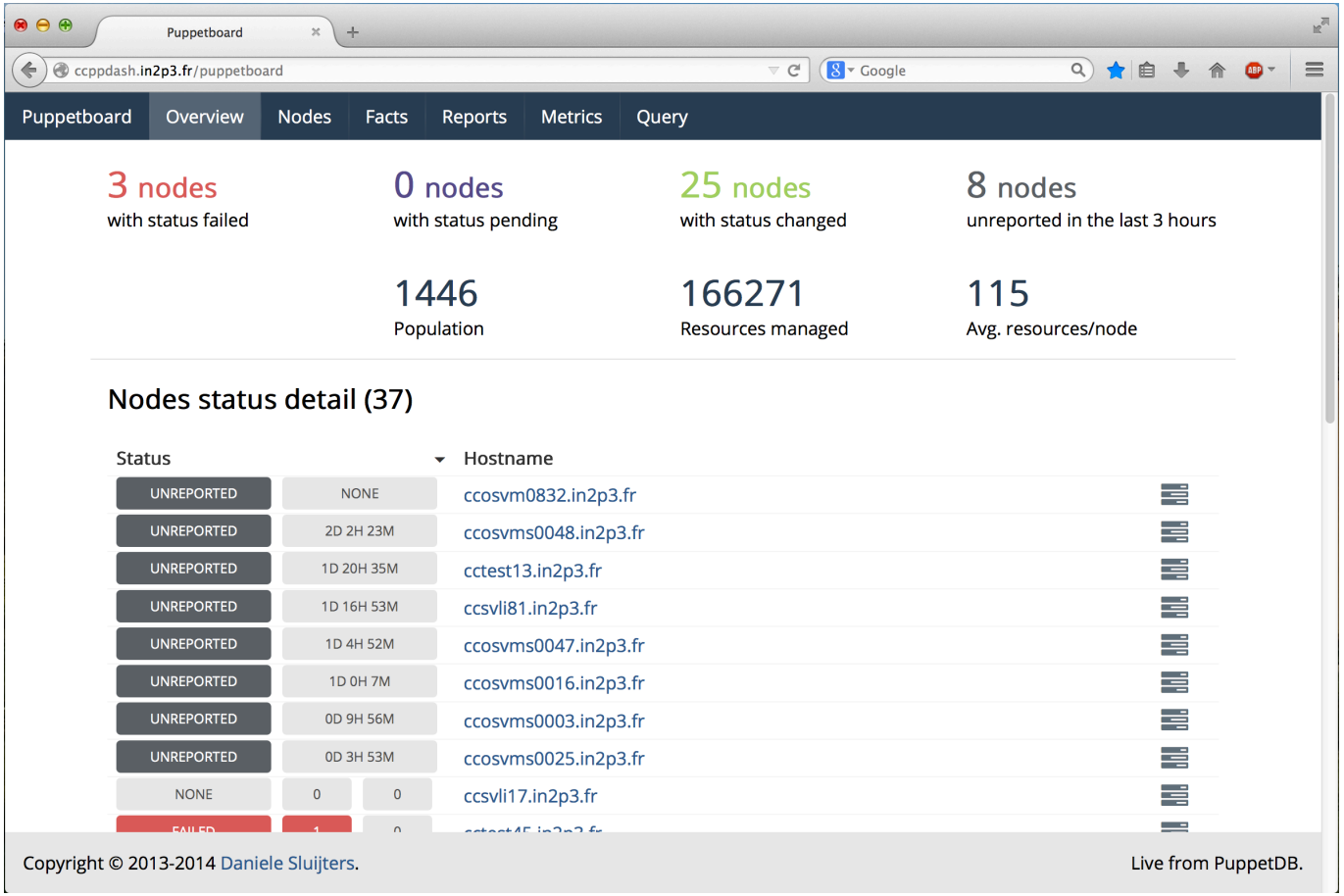
- Module
  - ensemble du code Puppet
    - pour configurer un composant : NTP, Apache...
    - pour implémenter de nouvelles fonctionnalités – ex : stdlib (upcase...)
  - partage de code
    - nombreux modules dans la Forge Puppet et GitHub :

    https://forge.puppetlabs.com/
    https://github.com/search?q=module+puppet&ref=cmdform

- Hiera
  - séparation du code et des données
    - fixer les valeurs des variables des classes, selon une hiérarchie définie
  - inclusion des classes
  - cryptage des variables secrètes

PUPPET AU CC : INFRASTRUCTURE

- depuis 2009
- 3 serveurs Puppet
  - nginx/Unicorn
- PuppetDB
- + 1400 clients
- 150 cnx http/s



PuppetDB du CC

PUPPET AU CC : CODE & DONNÉES DE CONFIGURATION

- ~ 100 ressources/nœud
- Modules
  - gestion via r10k
  - actuellement
    - 17 externes
    - 18 internes
    - 2 partagés : patterndb[1] & remctl[2]
- Hiera
  - merge récursif
  - cryptage : hiera-eyaml-gpg, clé partagée par les serveurs Puppet
- Migration de SVN à Git
  - modules dans GitLab
  - Hiera et environnements dans Gitolite avec **délégation** de privilèges
    => l'utilisateur peut modifier uniquement ses machines
  - $\neq^{ts}$ environnements $\Leftrightarrow$ $\neq^{tes}$ branches git => **tests** avant mise en production

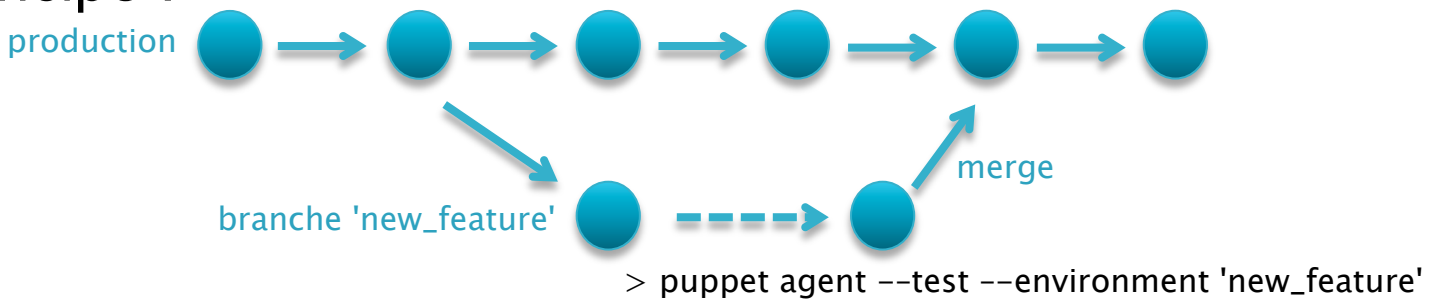
```
> hiera.yaml

:hierarchy:
  - "usages/%{::cfg_usage}/%{::clientcert}"
  - "usages/%{::cfg_usage}/default"
  - "modules/%{calling_module}/default"
  - "%{::operatingsystem}_%{::lsbdistrelease}"
  - "%{::operatingsystem}_%{::lsbmajdistrelease}"
  - "%{::operatingsystem}"
  - "%{::osfamily}"
  - "%{::kernel}"
  - "%{::virtual}"
  - "%{::productname}"
  - default
```

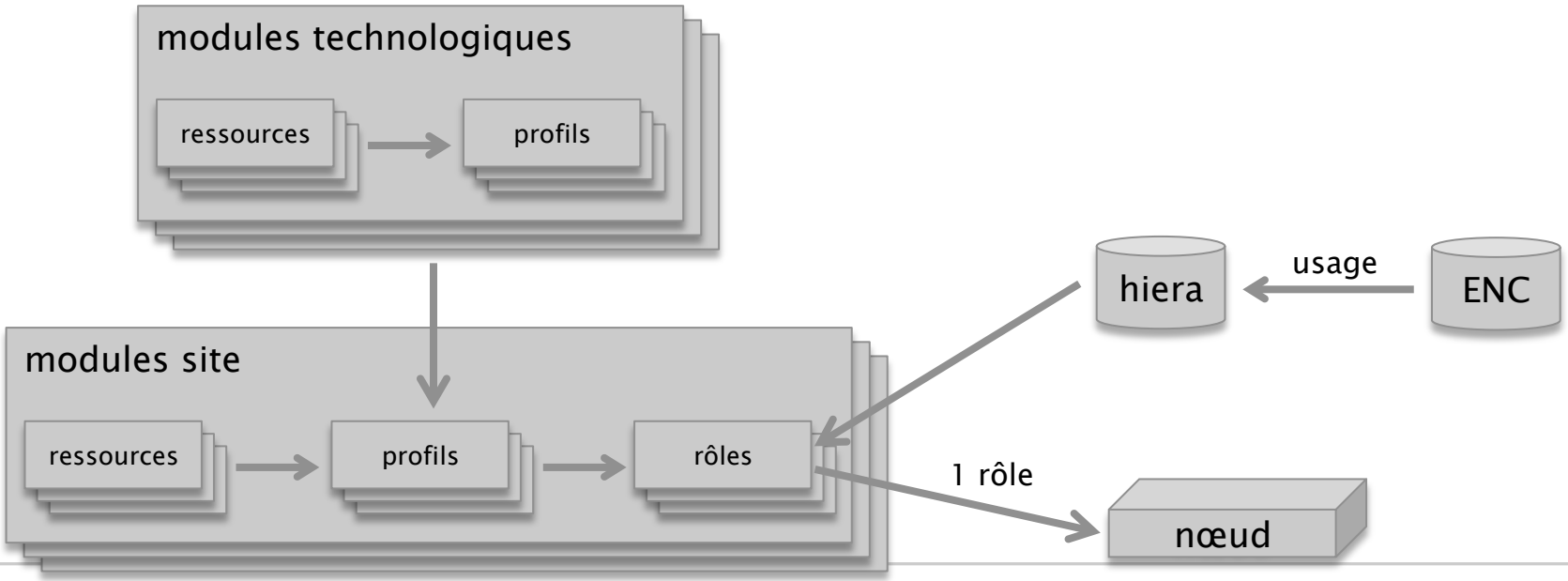
pyramide Hiera du CC

1 - https://forge.puppetlabs.com/ccin2p3/patterndb
2 - https://forge.puppetlabs.com/ccin2p3/remctl

- Environnements & code Puppet
  - hook Git : propagation automatique des modifications sur les serveurs
  - principe :



- Configuration des machines



- Ressources exportées et facts des nœuds
  - utilisables par d'autres services (CMDB...)
  - accessibles aux autres nœuds

ex : configuration automatique des hôtes et services Nagios

```
clients Nagios : exportent les ressources nagios_host & nagios_service
@@nagios_host { $fqdn:
  ensure  => present,
  alias   => $hostname,
  address => $ipaddress,
  use     => "generic-host",
}

@@nagios_service { "check_ping_${hostname}":
  check_command       => "check_ping!100.0,20%!500.0,60%",
  use                 => "generic-service",
  host_name           => "$fqdn",
  notification_period => "24x7",
  service_description => "${hostname}_check_ping",
}

serveur Nagios : collecte les ressources nagios_host et nagios_service des
clients => nagios_*.cfg
Nagios_host <<||>>
Nagios_service <<||>>
```

https://docs.puppetlabs.com/guides/exported_resources.html

DOCUMENTATION

- Code
  - https://docs.puppetlabs.com/learning/introduction.html
  - https://docs.puppetlabs.com/puppet/latest/reference/
  - https://docs.puppetlabs.com/references/latest/type.html
  - https://docs.puppetlabs.com/references/latest/function.html
- Module
  - https://docs.puppetlabs.com/puppet/latest/reference/modules_fundamentals.html
  - https://docs.puppetlabs.com/guides/style_guide.html
- Hiera
  - https://docs.puppetlabs.com/hiera/latest/index.html
- PupetDB
  - https://docs.puppetlabs.com/puppetdb/latest/

QUESTIONS...


감사합니다
Natick
Grazie
Danke
Ευχαριστίες
Dalu
Obrigado
Thank You
Köszönöm
Tack
Спасибо
Dank
Gracias
谢谢
Merci
Seé
ありがとう

ANNEXE : PUPPETDB

```
> curl -X GET http://ccosvms0025.in2p3.fr:8080/v3/resources/Package --data-urlencode
'query=["=", "certname", "cccreamceli09.in2p3.fr"]'
[ {
  "tags" : [ "package", "select_config_sl", "class", "puppet", "default", "node" ],
  "file" : "/etc/puppet/tmp_env/production/manifests/classes/sl/puppet.pp",
  "type" : "Package",
  "title" : "puppet",
  "line" : 6,
  "resource" : "efcf97958ac3a4aa34ce4943708ed80001207e08",
  "certname" : "cccreamceli09.in2p3.fr",
  "parameters" : {
    "allow_virtual" : false,
    "before" : "File[puppet_conf]",
    "ensure" : "present",
    "provider" : "yum"
  },
  "exported" : false
},
...
} ]

> curl -X GET http://ccosvms0025.in2p3.fr:8080/v3/facts/operatingsystem --data-
urlencode 'query=["=", "certname", "cccreamceli09.in2p3.fr"]'
[ {
  "certname" : "cccreamceli09.in2p3.fr",
  "name" : "operatingsystem",
  "value" : "Scientific"
} ]
```

ANNEXE : HIERA & VARIABLES SECRÈTES

```
> gpg --list-keys
~/.gnupg/pubring.gpg
------------------------------
pub   2048D/092C6C46 2014-07-04
uid                  cle_puppet (for puppet secret variables) <christelle.eloto@cc.in2p3.fr>
sub   2048g/2B62EEB9 2014-07-04

pub   2048D/1D877874 2014-07-04
uid                  cle_perso (for puppet secret variables) <christelle.eloto@cc.in2p3.fr>
sub   2048g/D400EC76 2014-07-04


> cat ~/.gnupg/hiera-eyaml-gpg.recipients
cle_puppet
cle_perso


> eyaml encrypt -n gpg --gpg-always-trust -s 'mot de passe secret' --gpg-recipients-file ~/.gnupg/hiera-eyaml-gpg.recipients
string: ENC[GPG,hQIOA3fxw9YrYu65EAf+I20ICQ0jdxyyXcavoaosWcusTc53kCviKJMNqLs/Kq9CTqEQwhC4ABye/...
...
QMv+EqQSDDOpC28SAtYPTqT5SgvDNYle7FeZclqonWcDr+xFTAjxvJK8/Y+DJUF9kmTrWREKHu6kG3QY1Zyg==]

OR

block: >
    ENC[GPG,hQIOA3fxw9YrYu65EAf+I20ICQ0jdxyyXcavoaosWcusTc53kCviKJMNqLs/
    ...
    TrWREKHu6kG3QY1Zyg==]


> vi hieradata/usages/ce/cccreamceli09.in2p3.fr.yaml
mon_module::ma_classe::mdp: >
 ENC[GPG,hQIOA3fxw9YrYu65EAf+I20ICQ0jdxyyXcavoaosWcusTc53kCviKJMNqLs/
 ...
 TrWREKHu6kG3QY1Zyg==]

> hiera mon_module::ma_classe::mdp ::cfg_usage=ce ::clientcert=cccreamceli09.in2p3.fr
mot de passe secret
```

ANNEXE : INFRASTRUCTURE DU CC EN DETAILS

- Installation
  - RPM : puppet (client 3.6.2-1), puppet-server-3.6.2-1, nginx (1.0.15-5), hiera (1.3.3-1), puppetdb (2.2.0-1)
  - Gems : unicorn (4.8.3), hiera-eyaml (2.0.2/2.0.3), hiera-eyaml-gpg (0.4), deep_merge (1.0.1), r10k (1.3.2)

- nginx
  - serveur web et reverse proxy

- Unicorn
  - serveur HTTP pour applications Rack
  - pour les clients rapides