Puppet / Marionette Collective

d’une altitude de 40 000 pieds et à mach 0.8

Romain Tartière <romain@opus-codium.fr>

1er Mars 2017

puppet

Objectifs

1. Présenter transversalement l'écosystème pour que vous choisissiez vos briques ;
2. Donner quelques pointeurs : par où commencer ;
3. Mettre en avant des points de vigilance ;
4. Ça n'est pas un how-to !

puppet

Sommaire

puppet

Gestion de configuration

Objectif : maintenir la configuration d'un parc de machines dans un état donné.

Exemples :

- Gérer les logiciels sur des ensembles de machines
  - Machines étudiants :
    - Authentification LDAP des utilisateurs ;
    - Environnement de bureau ;
    - Logiciels spécifiques aux enseignements.
  - Serveurs :
    - Authentification SSH par clés publiques uniquement ;
    - Clés SSH des administrateurs.
- Faire évoluer le parc de manière **ordonnée**.

puppet

Orchestration

Objectif : déclencher une action sur un ensemble de machines de manière **coordonnée**.

Exemples :

- Appliquer un correctif de sécurité sur un parc de machines ;
- Coordonner la mise à jour d'une application distribuée.

puppet

Synthèse

Gestion de configuration

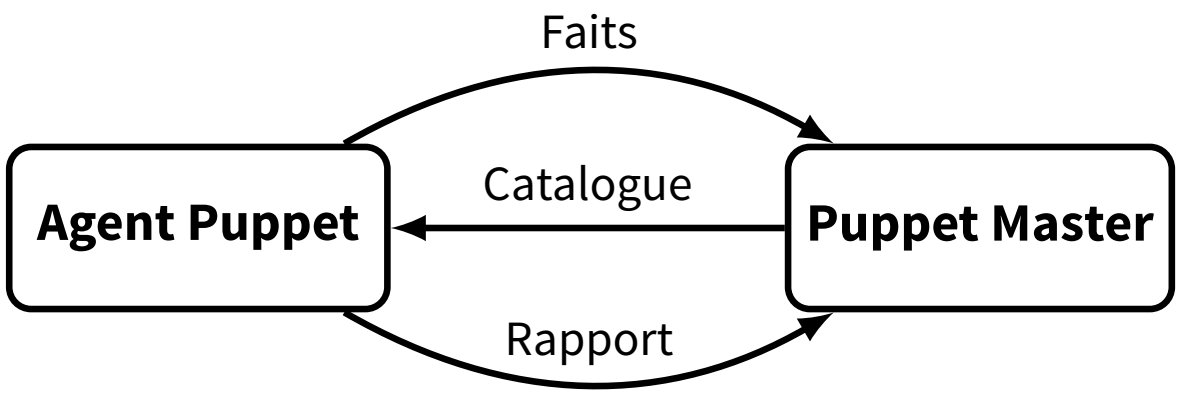
- tirée par les noeuds ;
- de manière indépendante.

Orchestration

- poussée vers les noeuds ;
- par salves.

puppet

Architecture



puppet

Écosystème

- Facter
- External Node Classifier
- Hiera
- PuppetDB
- Déploiement
  - r10k
  - jens
- Tests / QA
  - puppet-lint
  - rspec-puppet
  - beaker
- Visualisation
  - puppetboard
  - puppet-dashboard
  - puppetexplorer

puppet

Quelle saveur installer ?

- Puppet Entreprise 2016.5.1
- Puppet (PE and Open Source) 4.8.2
- Puppet Server (PE and Open Source) 2.7.2
- Puppet Agent 1.8.3

puppet

Quelle version installer ?

- Puppet 3 n’est plus supporté ;
- Le langage de Puppet 4 fait un bond en avant :
  - Data types ;
  - Itérations / boucles ;
  - Heredocs ;
  - Lambda ;
  - Templates EPP ;
  - etc.

puppet

Comment installer ?

```
# apt-get install puppet
```

Puppet 3.7.2 💔

Comment installer ?

```
# cat /etc/apt/sources.list.d/puppetlabs.list
deb http://apt.puppetlabs.com jessie main PC1
# apt-get install puppet-agent
```

Puppet 4.8.2 ❤️💔

Disponible uniquement pour i386 / amd64 (x86 / x86_64)

puppet

Comment installer ?

```
# cat /etc/apt/sources.list.d/puppetlabs.list
deb http://apt.puppetlabs.com stable main
# apt-get install puppet
```

Puppet 3.8.1 💔

Comment installer ?

Backports Debian

Puppet 3.8.5 💔

puppet

Comment installer ?

```
# gem install puppet
```

Puppet 4.8.2 ❤️

Un peu de glue pour lancer le service

puppet

Manifests (DSL, RAL)

```
$zsh_path = $::osfamilly ? {
  'freebsd' => '/usr/local/bin/zsh',
  default   => '/bin/zsh',
}

user { 'romain':
  ensure  => present,
  comment => 'Romain Tartière',
  home    => '/home/romain',
  shell   => $zsh_path,
}
```

« *Infrastructure as code* »

puppet

Types et providers

Types

- cron
- exec
- file
- group
- package
- service
- ssh_authorized_key
- **user**
- …

Providers du type « user »

- aix
- directoryservice
- hpuxuseradd
- ldap
- openbsd
- pw
- user_role_add
- useradd
- windows_adsi

puppet

Modules

Entités réutilisables

- package
- configuration
- service

Fournissent :

- manifests ;
- fichiers / templates ;
- faits ;
- fonctions ;
- types ;
- providers.

puppet

Modules : exemple

- puppetlabs
  - stdlib
  - apache
  - postgresql

…des dizaines d’autres sur la forge…

…et en dehors !

puppet

Modules : usage

```
% puppet module install puppetlabs-apache
‘-> puppetlabs-apache (v1.11.0)
  |-> puppetlabs-concat (v2.2.0)
  ‘-> puppetlabs-stdlib (v4.15.0)
```

```
class { ’::apache’:
  keepalive  => ’On’,
  mpm_module => ’event’,
}
```

```
include ::apache
```

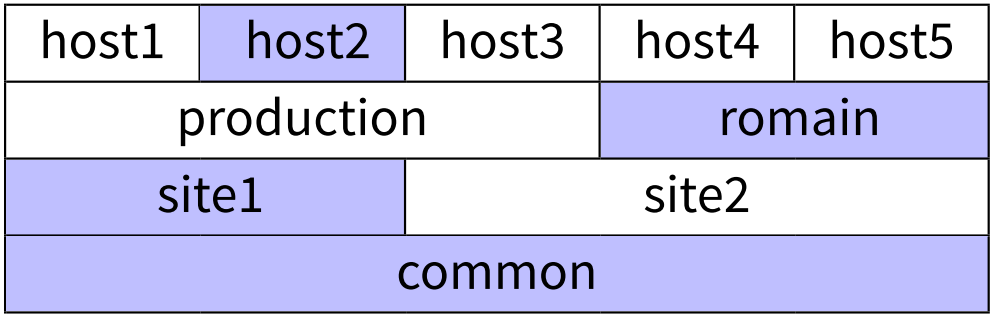
```
::apache::vhost { ’example.com’:
  port    => 80,
  docroot => ’/var/www/example.com’,
}
```

Hiera

Les **données externes** sont de la **configuration pour votre code**

Hiera : stockage clé / valeur avec « *default and override* » :

```
$::trusted.clientcert
$::environnement
$::site
```



Hiera : exemple

hieradata/common.yaml

```
---
apache::keepalive: 'On'
apache::mpm_module: 'event'
mcollective::host: 'activemq.example.com'
mcollective::port: 61614
```

hieradata/nodes/node2.example.com.yaml

```
---
mcollective::port: 143
```

PuppetDB

Collecte :

- faits ;
- catalogues ;
- rapports.

Interrogeable via une API

- Visualisation avec un dashboard ;
- Export / réalisation de ressources.

puppet-lint

Détecte les problèmes de style dans les manifests :

```
% puppet-lint manifests/foo.pp
ERROR: trailing whitespace found on line 57
ERROR: two-space soft tabs not used on line 57
WARNING: top-scope variable being used without an explicit namespace on line 1
WARNING: double quoted string containing no variables on line 28
```

puppet

rspec-puppet

```
describe 'openvpn::config' do
  let(:title) { 'test' }
  let(:facts) do
    {
      osfamily: osfamily
    }
  end

  context 'on Debian' do
    let(:osfamily) { 'Debian' }

    it { is_expected.to contain_concat('/etc/openvpn/test.conf') }
    it { is_expected.to contain_openvpn__service('test') }
  end

  context 'on FreeBSD' do
    let(:osfamily) { 'FreeBSD' }

    it { is_expected.to contain_concat('/usr/local/etc/openvpn/test.conf') }
    it { is_expected.to contain_openvpn__service('test') }
  end
end
```

puppet

beaker

```
describe 'access_point' do
  context 'create a new access point' do
    before(:all) do
      pp = <<-EOT
        access_point { 'AP3':
          ensure  => present,
          psk     => 'another-secret',
          ssid    => 'Access Point 3',
        }
      EOT

      apply_manifest(pp, catch_failures: true)
    end

    describe file('/etc/rbm/wifi/AP3.yaml') do
      it { should exist }

      its(:content_as_yaml) { should include('psk' => 'another-secret') }
      its(:content_as_yaml) { should include('ssid' => 'Access Point 3') }
    end
  end
end
```

Module qui fait tout

Chaque module devrait pouvoir être redistribué

Limiter les dépendances entre modules

Déplacer la logique dans un profil

puppet

Nommer ses nœuds

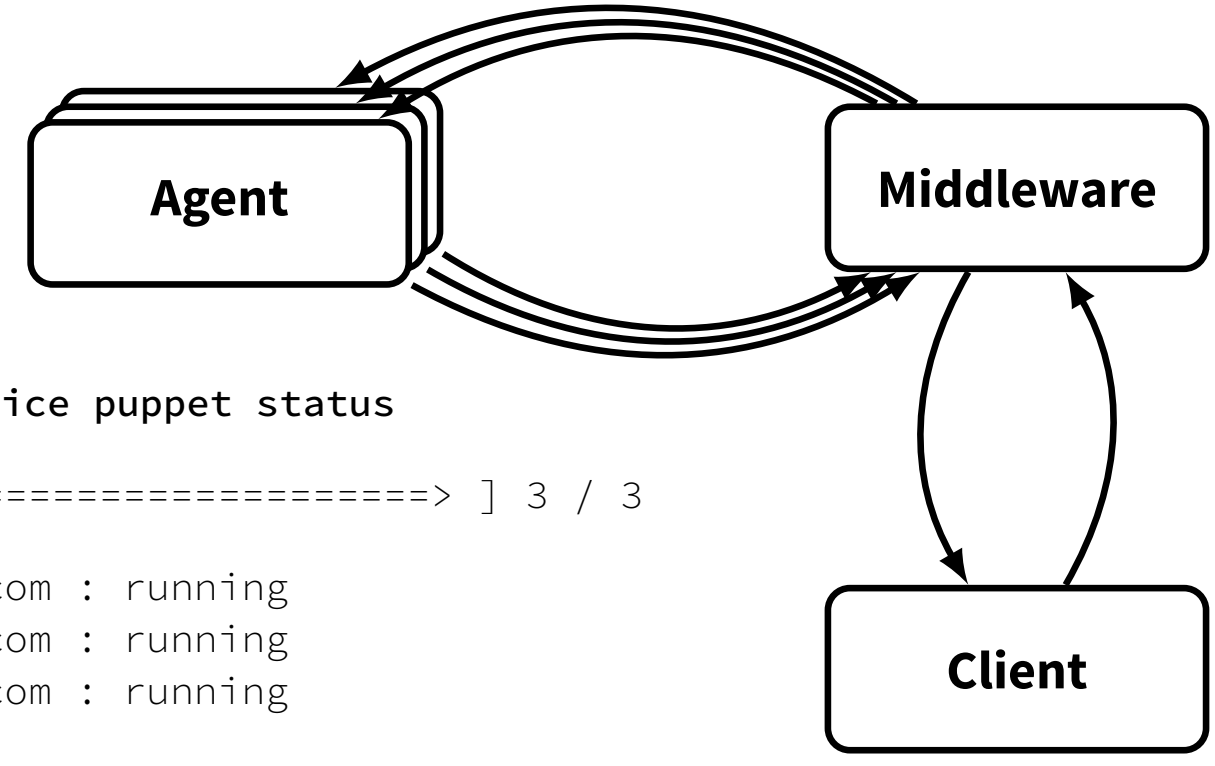
Ne pas utiliser les méta-données des nœuds dans les noms d'hôtes :

- wiki.example.com
- pccomptawin7.example.com

The Practice of System and Network Administration, Thomas A. Limoncelli
Chapitre 8, *Namespaces*

puppet

Architecture




```
client% mco service puppet status

* [ ============================> ] 3 / 3

agent1.example.com : running
agent2.example.com : running
agent3.example.com : running

Summary of Service Status :

   running = 3

Finished processing 3 / 3 hosts in 763.47 ms
```

puppet

Commandes

- facts
- find
- inventory
- ping

- package
- puppet
- service
- shell

puppet

Filtrer selon des faits

```
% mco ping -F osfamily=Debian
```

puppet

Filtrer selon une classe

```
% mco find -C apache
```

puppet

Filtrer selon un agent

```
% mco ping -A puppet
```

puppet

Filtrer selon une identité

```
% mco ping -I www3.example.com

% mco ping -I '/^www\d+\./'
```

puppet

Installation

L'installation est **pénible** !

- 6 étapes dans le déploiement standard ;
- Plusieurs options à chaque étape ;
- Chaque choix a des conséquences sur la sécurité.

Une alternative : Choria

Aller plus loin

- Documentation et Internet :
  - PKI ;
  - Control-Repo ❤️ ;
  - r10k ❤️ ;
  - Rôles et Profils ❤️ ;
  - External Node Classifier ;
  - Faits personalisés ;
  - Types personalisés ;
  - Providers personalisés.
- PuppetConf :
  - https://puppet.com/puppetconf
- Formation / Accompagnement :
  - hello@opus-codium.fr