Configuration Management

For future infrastructure

Gareth Rushgrove
Puppet Labs


@garethr

Weekly Devops Email News

www.devopsweekly.com

Archive

DEVOPS WEEKLY

A weekly slice of devops news

13,142 subscribers
powered by MailChimp

Kindly sponsored by Brightbox

garethr@garethr: mutt — mutt — 99×18

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.    r:Reply  j:Next ?:Help
Date: Sun, 21 Nov 2010 08:22:54 -0500
From: Devops Weekly <gareth@morethanseven.net>
To: gareth@morethanseven.net
Subject: Devops Weekly #0
X-Mailer: MailChimp Mailer - **CID1556f6f0e7**

DEVOPS WEEKLY
ISSUE #0 - 21st November 2010

Welcome to the first issue of Devops Weekly.

I've been finding Ruby Weekly (http://rubyweekly.com/), a weekly email newsletter from Peter
+Cooper, increasingly useful. Something about finding a small amount of high quality content once a
+week easier to digest than the usual fire hose of RSS and Twitter. So I'm trying the format out
+for devops related content. Please email me with anything you think is worth featuring.
-  F- 1/22: Devops Weekly          Devops Weekly #0                                    -- (20%)
```

Subscribe

Please provide your email address


puppet
labs®

What is configuration management?

Any input to your infrastructure is configuration

Configuration management is about managing all of those inputs over time

Configuration management is about managing all of those inputs **over time**

This talk

A little history

Emerging patterns

Immutable infrastructure

Infrastructure APIs

Autonomous systems

Simpler hosts

Immutable infrastructure

Infrastructure APIs

Autonomous systems

Simpler hosts

Immutable infrastructure

Infrastructure APIs

Autonomous systems

Simpler hosts

Immutable infrastructure

Infrastructure APIs

Autonomous systems

Simpler hosts

Future infrastructure as code

A little history

1950s research, 1960s 480 series, 1991 MIL-HDBK-61, 1998 ANSI-EIA-649

Military Handbook Configuration Management Guidance MIL-HDBK-61B

Identification
Control
Status accounting
Verification and audit

National Consensus Standard for Configuration Management EIA-649

Configuration management verifies that a system is identified and documented in sufficient detail

Configuration management verifies that a system performs as intended

Service management, ITIL, ISO 20000

Infrastructure as code

```
file { '/etc/ssh/ssh_config':
  ensure => file,
  owner  => 'root',
  mode   => '0600',
  source => 'puppet:///modules/ssh/sshd_config',
}
```

Immutable infrastructure

Build once, run many times

Amazon Machine Images

End-to-end automation to avoid the golden image problem

NETFLIX

Containers


docker

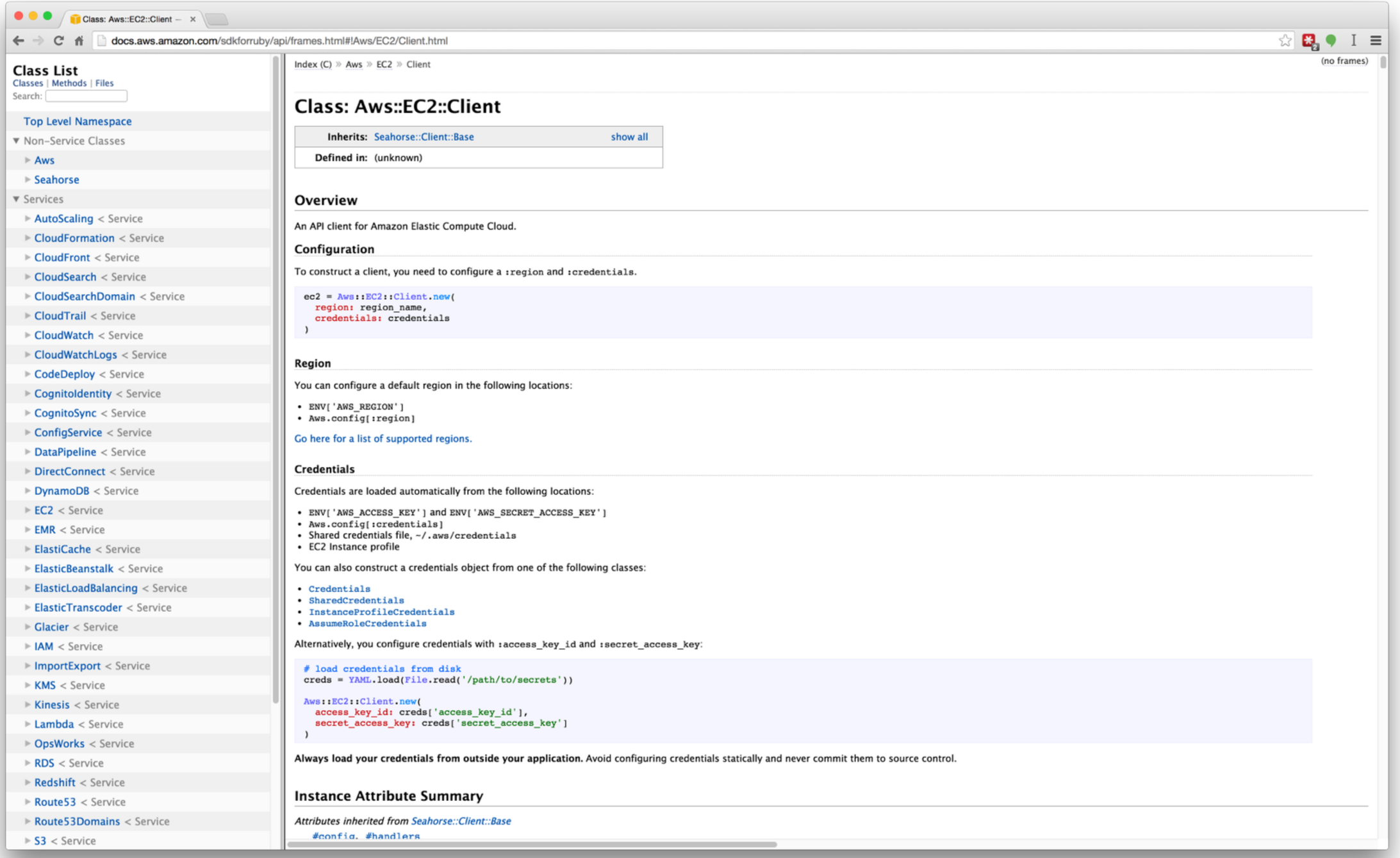
Docker as the user interface

How immutable are your docker containers?

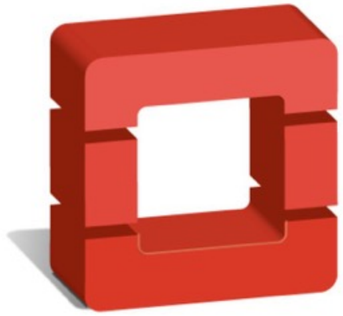
Infrastructure with APIs

Infrastructure as a service


amazon
web services™


Class: Aws::EC2::Client
docs.aws.amazon.com/sdkforruby/api/frames.html#!Aws/EC2/Client.html
Class List
Classes | Methods | Files
Search:
Top Level Namespace
Non-Service Classes
Aws
Seahorse
Services
AutoScaling < Service
CloudFormation < Service
CloudFront < Service
CloudSearch < Service
CloudSearchDomain < Service
CloudTrail < Service
CloudWatch < Service
CloudWatchLogs < Service
CodeDeploy < Service
CognitoIdentity < Service
CognitoSync < Service
ConfigService < Service
DataPipeline < Service
DirectConnect < Service
DynamoDB < Service
EC2 < Service
EMR < Service
ElastiCache < Service
ElasticBeanstalk < Service
ElasticLoadBalancing < Service
ElasticTranscoder < Service
Glacier < Service
IAM < Service
ImportExport < Service
KMS < Service
Kinesis < Service
Lambda < Service
OpsWorks < Service
RDS < Service
Redshift < Service
Route53 < Service
Route53Domains < Service
S3 < Service
Index (C) » Aws » EC2 » Client
(no frames)
Class: Aws::EC2::Client
Inherits: Seahorse::Client::Base show all
Defined in: (unknown)
Overview
An API client for Amazon Elastic Compute Cloud.
Configuration
To construct a client, you need to configure a :region and :credentials.
ec2 = Aws::EC2::Client.new(
region: region_name,
credentials: credentials
)
Region
You can configure a default region in the following locations:
ENV['AWS_REGION']
Aws.config[:region]
Go here for a list of supported regions.
Credentials
Credentials are loaded automatically from the following locations:
ENV['AWS_ACCESS_KEY'] and ENV['AWS_SECRET_ACCESS_KEY']
Aws.config[:credentials]
Shared credentials file, ~/.aws/credentials
EC2 Instance profile
You can also construct a credentials object from one of the following classes:
Credentials
SharedCredentials
InstanceProfileCredentials
AssumeRoleCredentials
Alternatively, you configure credentials with :access_key_id and :secret_access_key:
# load credentials from disk
creds = YAML.load(File.read('/path/to/secrets'))
Aws::EC2::Client.new(
access_key_id: creds['access_key_id'],
secret_access_key: creds['secret_access_key']
)
Always load your credentials from outside your application. Avoid configuring credentials statically and never commit them to source control.
Instance Attribute Summary
Attributes inherited from Seahorse::Client::Base
#config, #handlers


amazon
web services™


openstack™


DigitalOcean


Google Cloud Platform


Windows Azure


vmware®

Platform as a service

CLOUD FOUNDRY™

Environment Variable Groups API

Updating the contents of the running environment variable group

PUT /v2/config/environment_variable_groups/running

Updates the set of environment variables which will be made available to all running apps

Fields

Name	Description	Default	Valid Values	Example Values

Request

Headers

```
Authorization: bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidWFhLWlkLTU1IiwiZW1haWwiOiJlbWFpbC01NUBzb21lZG9tYWluLmNvbSIsInNjb3BlIjpbImNsb3VkX2NvbnRyb2xsZXIuYWRtaW4iXSwiYXVkIjpbImNsb3VkX2NvbnRyb2xsZXIiXSwiZXhwIjoxNDE2ODcyMzE2fQ.ibNacKU1_3B3mHgvuhHGDV-pympHSf8ru5AySE1_bDc
Host: example.org
Content-Type: application/x-www-form-urlencoded
Cookie:
```

Route

```
PUT /v2/config/environment_variable_groups/running
```

Body

```
{
  "abc": 123,
  "do-re-me": "far-so-la-tee"
}
```

cURL

```
curl "https://api.[your-domain.com]/v2/config/environment_variable_groups/running" -d '{
  "abc": 123,
  "do-re-me": "far-so-la-tee"
}' -X PUT \
        -H "Authorization: bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoidWFhLWlkLTU1IiwiZW1haWwiOiJlbWFpbC01NUBzb21lZG9tYWluLmNvbSIsInNjb3BlIjpbImNsb3VkX2NvbnRyb2xsZXIuYWRtaW4iXSwiYXVkIjpbImNsb3VkX2NvbnRyb2xsZXIiXSwiZXhwIjoxNDE2ODcyMzE2fQ.ibNacKU1_3B3mHgvuhHGDV-pympHSf8ru5AySE1_bDc" \
        -H "Host: example.org" \
        -H "Content-Type: application/x-www-form-urlencoded" \
        -H "Cookie: "
```

Response

Headers

```
Content-Type: application/json;charset=utf-8
X-VCAP-Request-ID: a0008121-6c7a-4c29-80ea-4f6f67f40b44
Content-Length: 47
```

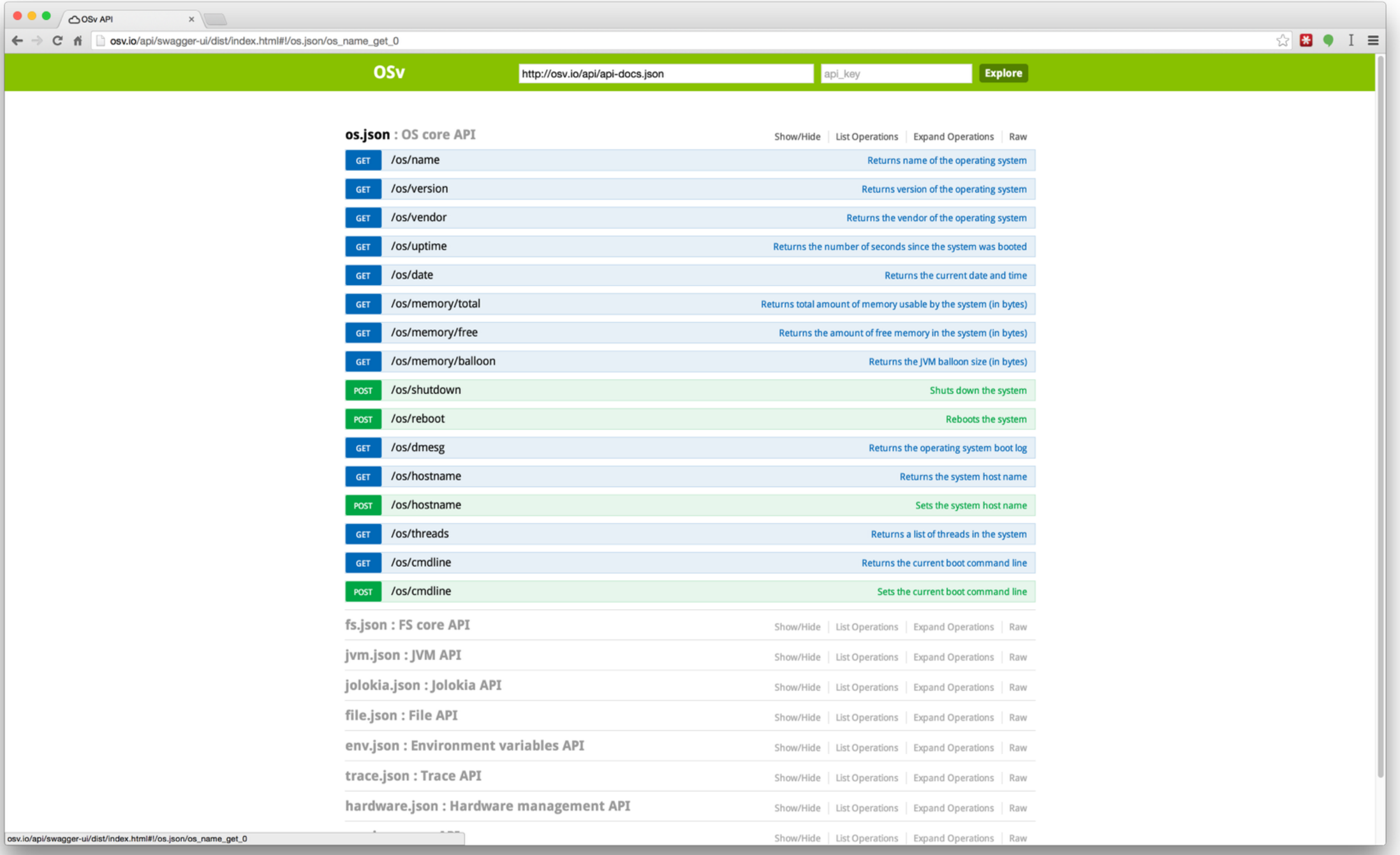


CLOUD
FOUNDRY™


OPENSHIFT


heroku

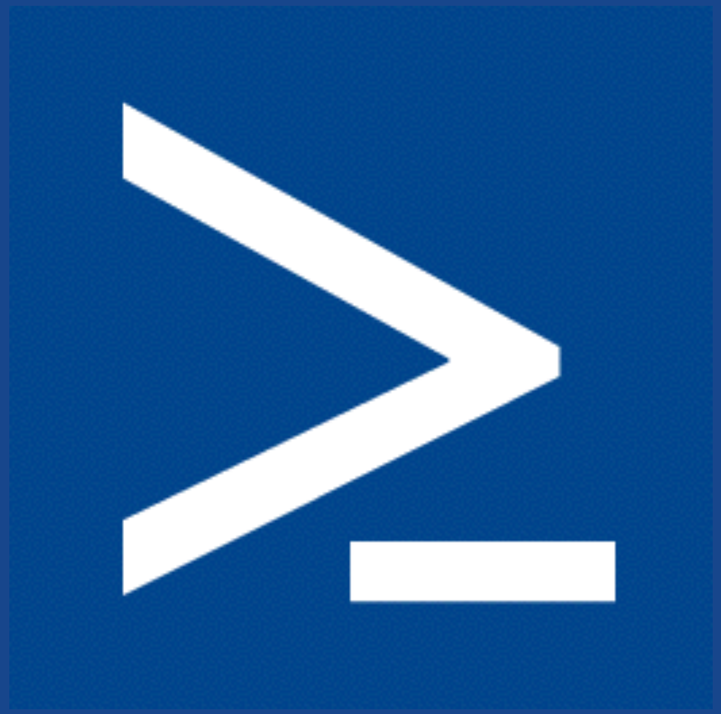
OSv


OSv API
osv.io/api/swagger-ui/dist/index.html#!/os.json/os_name_get_0
OSv
http://osv.io/api/api-docs.json
api_key
Explore
os.json : OS core API
Show/Hide | List Operations | Expand Operations | Raw
GET /os/name Returns name of the operating system
GET /os/version Returns version of the operating system
GET /os/vendor Returns the vendor of the operating system
GET /os/uptime Returns the number of seconds since the system was booted
GET /os/date Returns the current date and time
GET /os/memory/total Returns total amount of memory usable by the system (in bytes)
GET /os/memory/free Returns the amount of free memory in the system (in bytes)
GET /os/memory/balloon Returns the JVM balloon size (in bytes)
POST /os/shutdown Shuts down the system
POST /os/reboot Reboots the system
GET /os/dmesg Returns the operating system boot log
GET /os/hostname Returns the system host name
POST /os/hostname Sets the system host name
GET /os/threads Returns a list of threads in the system
GET /os/cmdline Returns the current boot command line
POST /os/cmdline Sets the current boot command line
fs.json : FS core API
jvm.json : JVM API
jolokia.json : Jolokia API
file.json : File API
env.json : Environment variables API
trace.json : Trace API
hardware.json : Hardware management API
osv.io/api/swagger-ui/dist/index.html#!/os.json/os_name_get_0

Not just compute, but network and storage too


cumulus networks

Not just *nix



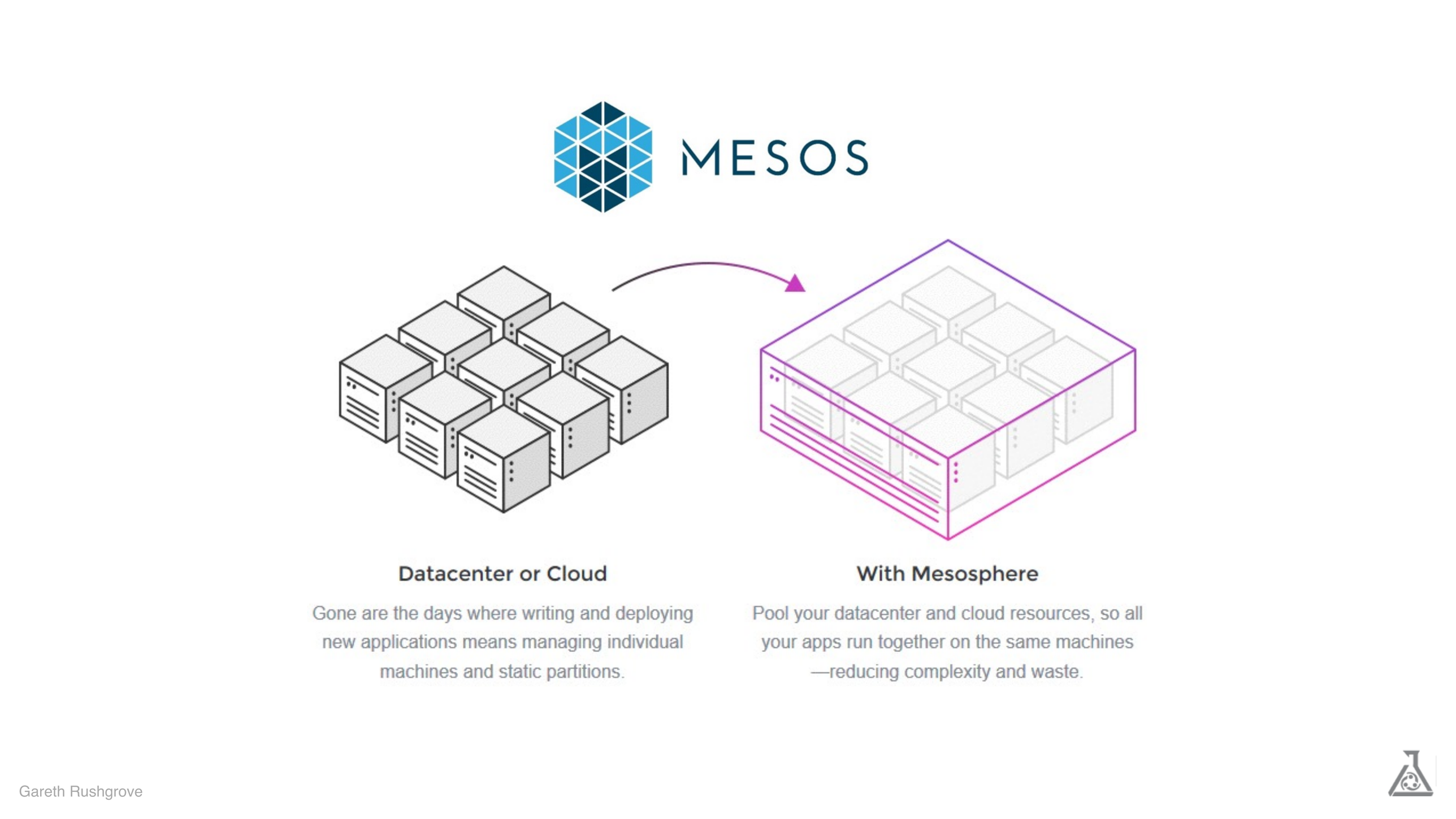
Configuration at a distance

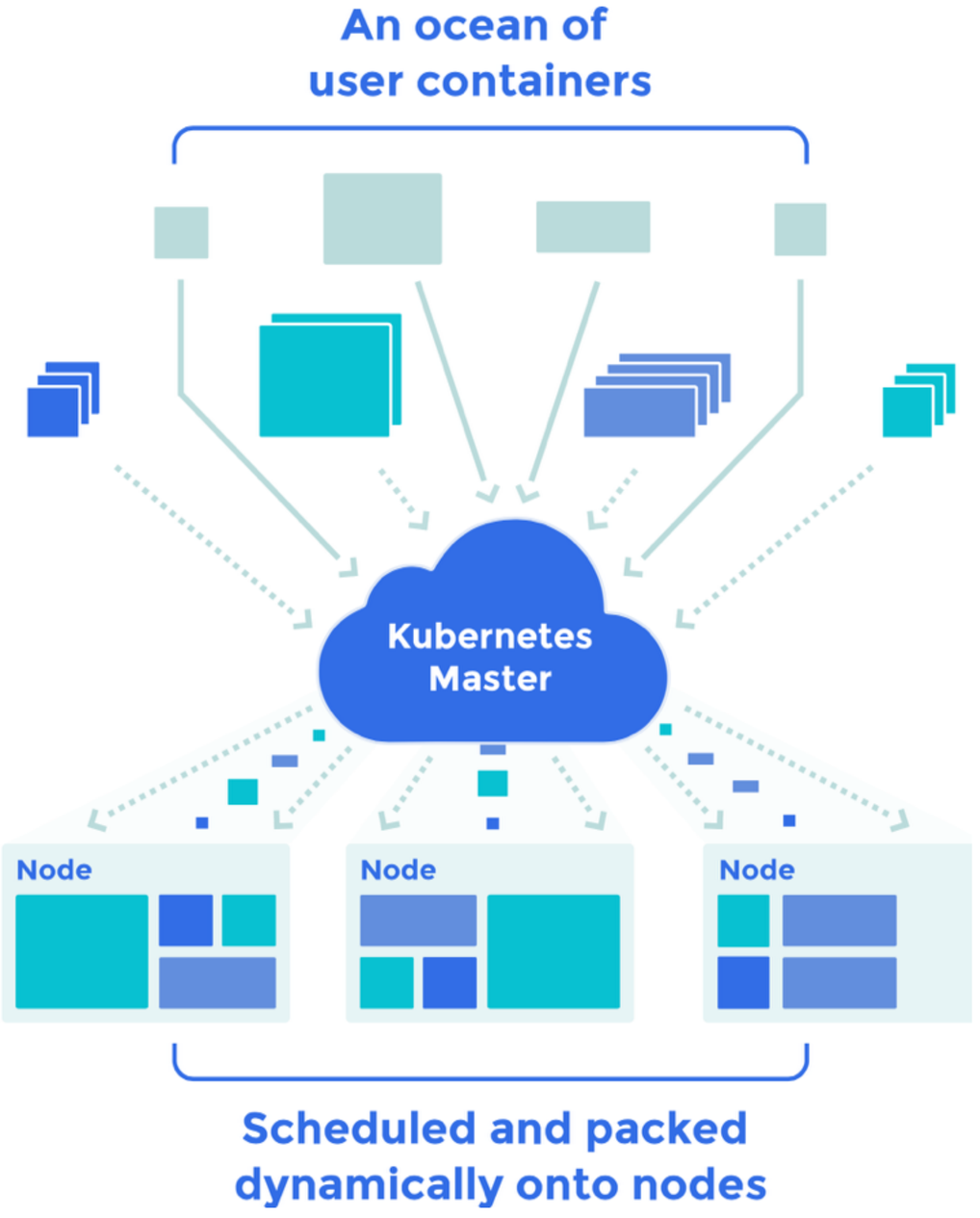
Configuring autonomous systems

We’re increasingly managing higher level systems

If servers are cattle not pets, we need to talk about fields and farms

Autoscaling groups


MESOS
Datacenter or Cloud
Gone are the days where writing and deploying new applications means managing individual machines and static partitions.
With Mesosphere
Pool your datacenter and cloud resources, so all your apps run together on the same machines —reducing complexity and waste.

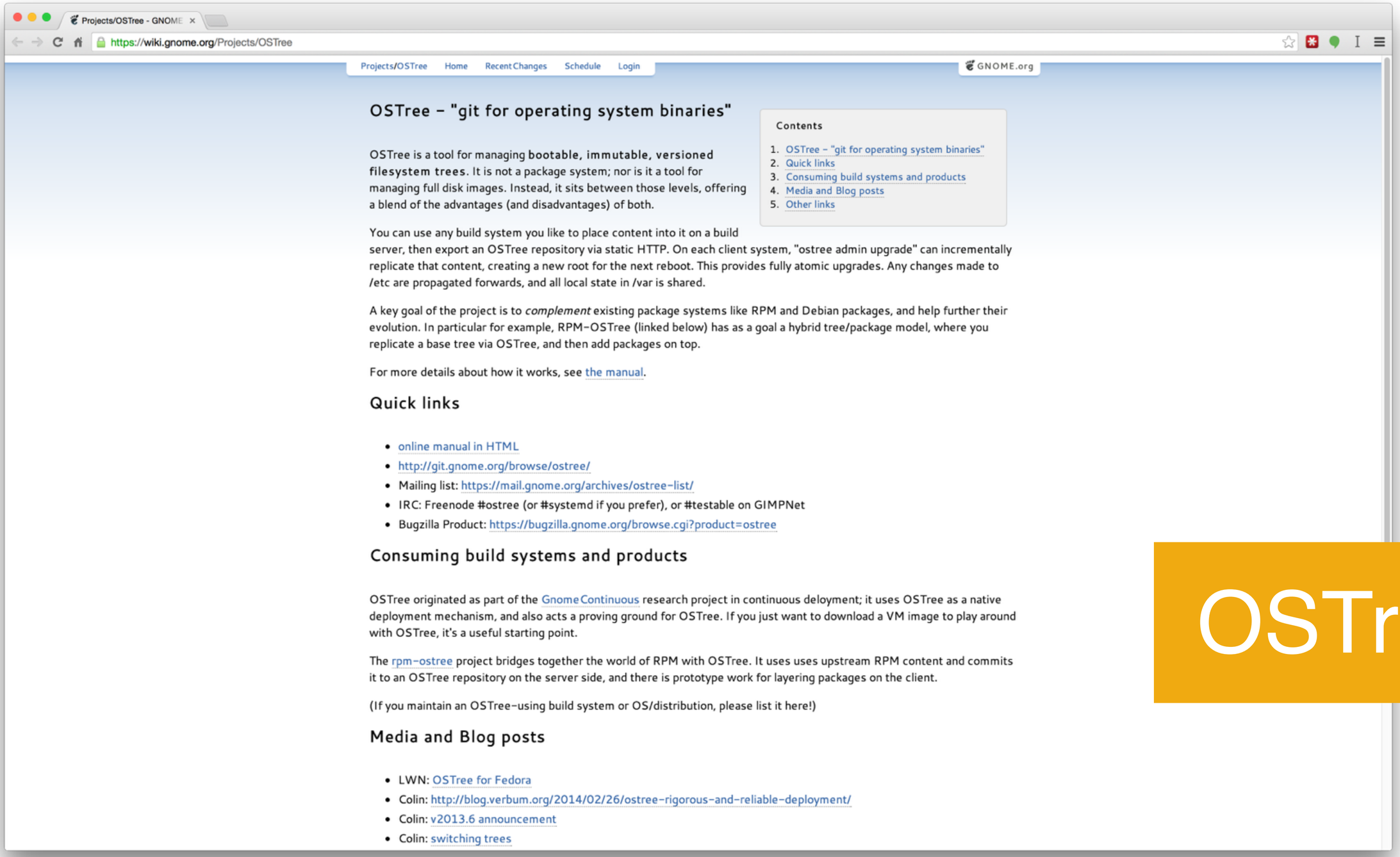

An ocean of
user containers
Kubernetes
Master
Node
Node
Node
Scheduled and packed
dynamically onto nodes

Simpler hosts

Combinatorial package explosion

PROJECT ATOMIC

Gareth Rushgrove

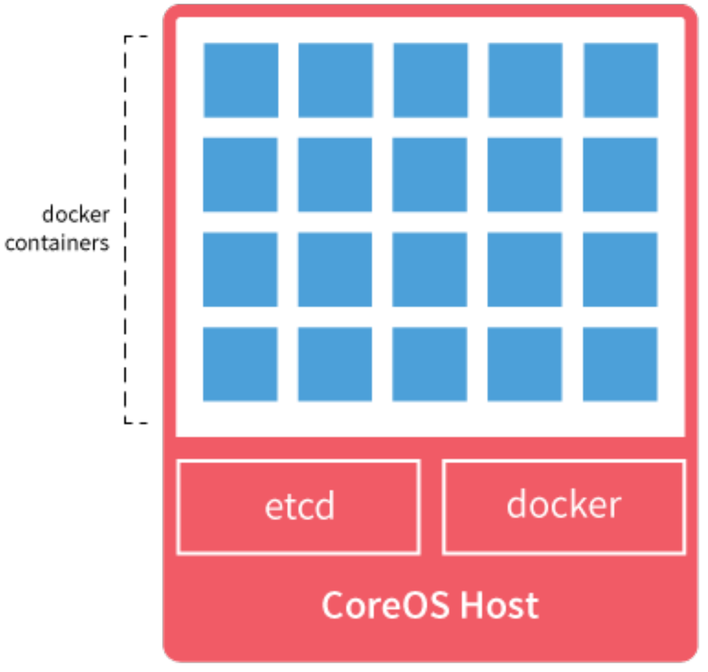

Projects/OSTree - GNOME
https://wiki.gnome.org/Projects/OSTree
Projects/OSTree Home Recent Changes Schedule Login
GNOME.org
OSTree – "git for operating system binaries"
Contents
1. OSTree – "git for operating system binaries"
2. Quick links
3. Consuming build systems and products
4. Media and Blog posts
5. Other links
OSTree is a tool for managing bootable, immutable, versioned filesystem trees. It is not a package system; nor is it a tool for managing full disk images. Instead, it sits between those levels, offering a blend of the advantages (and disadvantages) of both.
You can use any build system you like to place content into it on a build server, then export an OSTree repository via static HTTP. On each client system, "ostree admin upgrade" can incrementally replicate that content, creating a new root for the next reboot. This provides fully atomic upgrades. Any changes made to /etc are propagated forwards, and all local state in /var is shared.
A key goal of the project is to complement existing package systems like RPM and Debian packages, and help further their evolution. In particular for example, RPM-OSTree (linked below) has as a goal a hybrid tree/package model, where you replicate a base tree via OSTree, and then add packages on top.
For more details about how it works, see the manual.
Quick links
online manual in HTML
http://git.gnome.org/browse/ostree/
Mailing list: https://mail.gnome.org/archives/ostree-list/
IRC: Freenode #ostree (or #systemd if you prefer), or #testable on GIMPNet
Bugzilla Product: https://bugzilla.gnome.org/browse.cgi?product=ostree
Consuming build systems and products
OSTree originated as part of the GnomeContinuous research project in continuous deloyment; it uses OSTree as a native deployment mechanism, and also acts a proving ground for OSTree. If you just want to download a VM image to play around with OSTree, it's a useful starting point.
The rpm-ostree project bridges together the world of RPM with OSTree. It uses uses upstream RPM content and commits it to an OSTree repository on the server side, and there is prototype work for layering packages on the client.
(If you maintain an OSTree-using build system or OS/distribution, please list it here!)
Media and Blog posts
LWN: OSTree for Fedora
Colin: http://blog.verbum.org/2014/02/26/ostree-rigorous-and-reliable-deployment/
Colin: v2013.6 announcement
Colin: switching trees

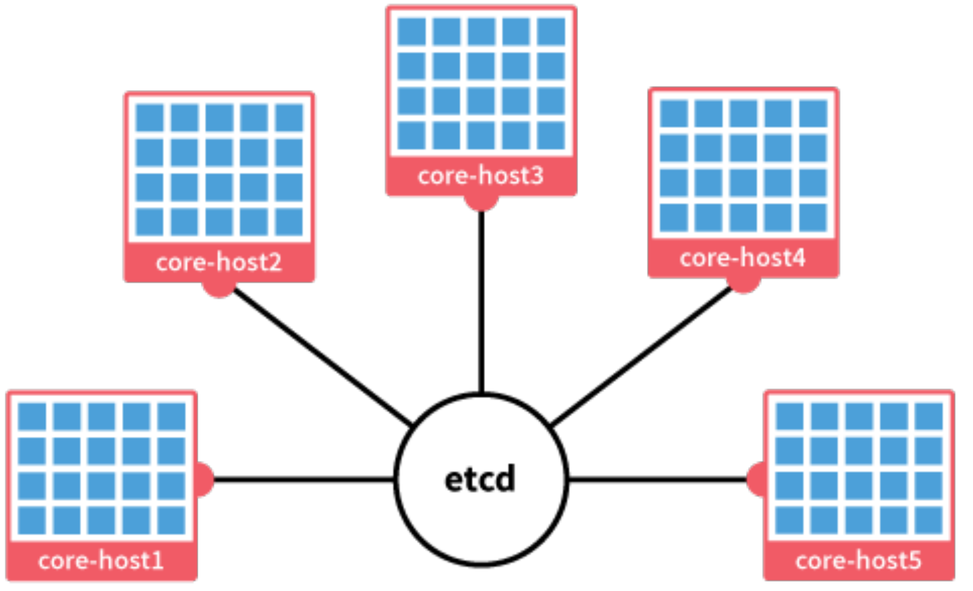
OSTree

```
» cat /ostree/repo/config
[core]
repo_version=1
mode=bare

[remote "fedora-atomic"]
url=http://dl.fedoraproject.org/pub/alt/fedora-atomic/repo
gpg-verify=false
```

CoreOS


docker
containers
etcd
docker
CoreOS Host


core-host2
core-host3
core-host4
core-host1
etcd
core-host5

CoreOS is a firmware for running containers

John Vincent - http://blog.lusis.org/blog/2014/11/21/a-few-things/

Moving configuration from hosts to the network



Etcd, Consul, Zookeeper

Future infrastructure as code

From:

Host centric

Localised

Executable for integration

To:

Cluster centric

Distributed

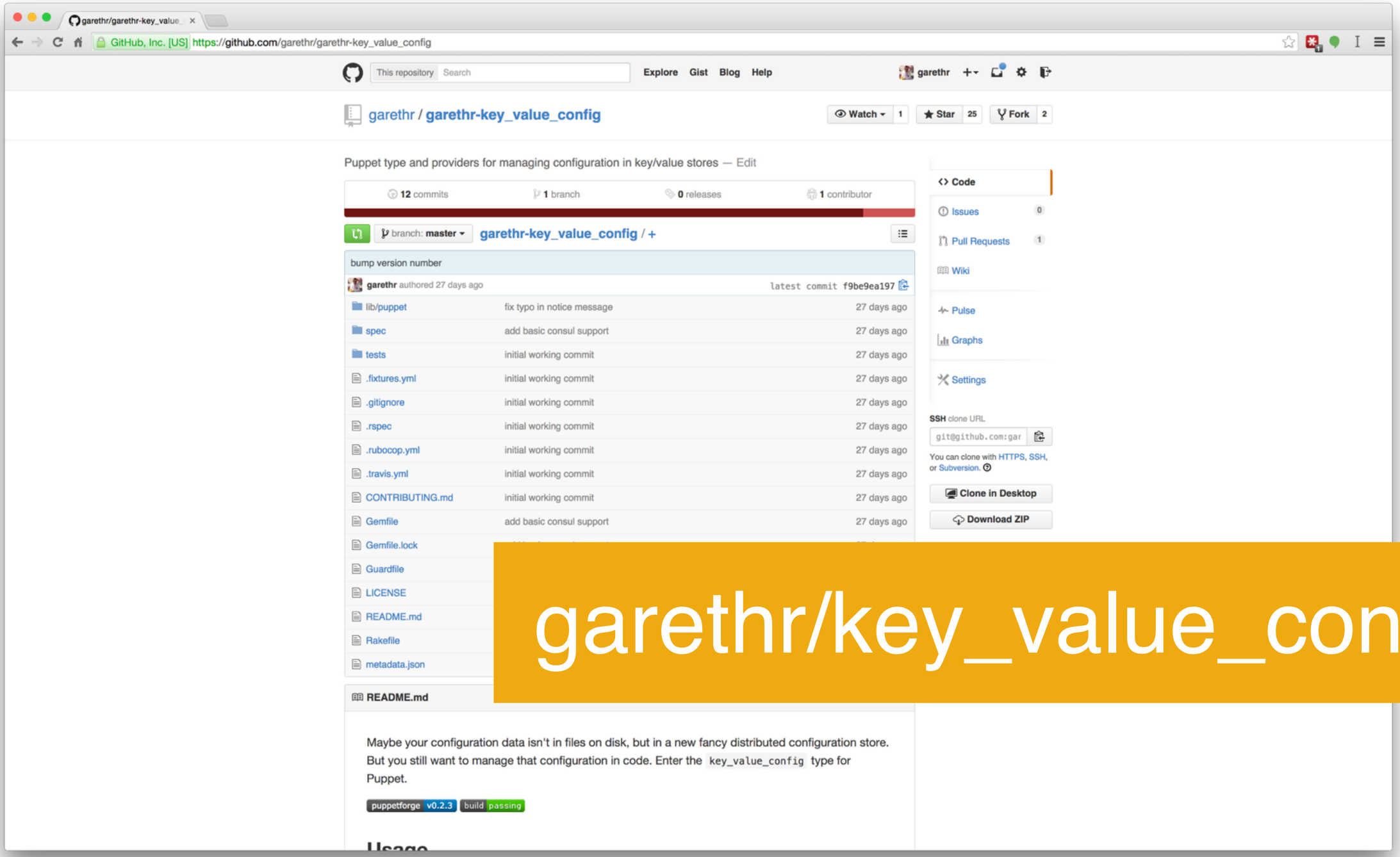
HTTP for integration

Going from Puppet to etcd

```
key_value_config { '/foo':
  ensure   => present,
  provider => etcd,
  value    => 'bar',
}
```

Where similar interfaces exist we can provide abstractions

```
key_value_config { '/foo':
  ensure   => present,
  provider => consul,
  value    => 'bar',
}
```

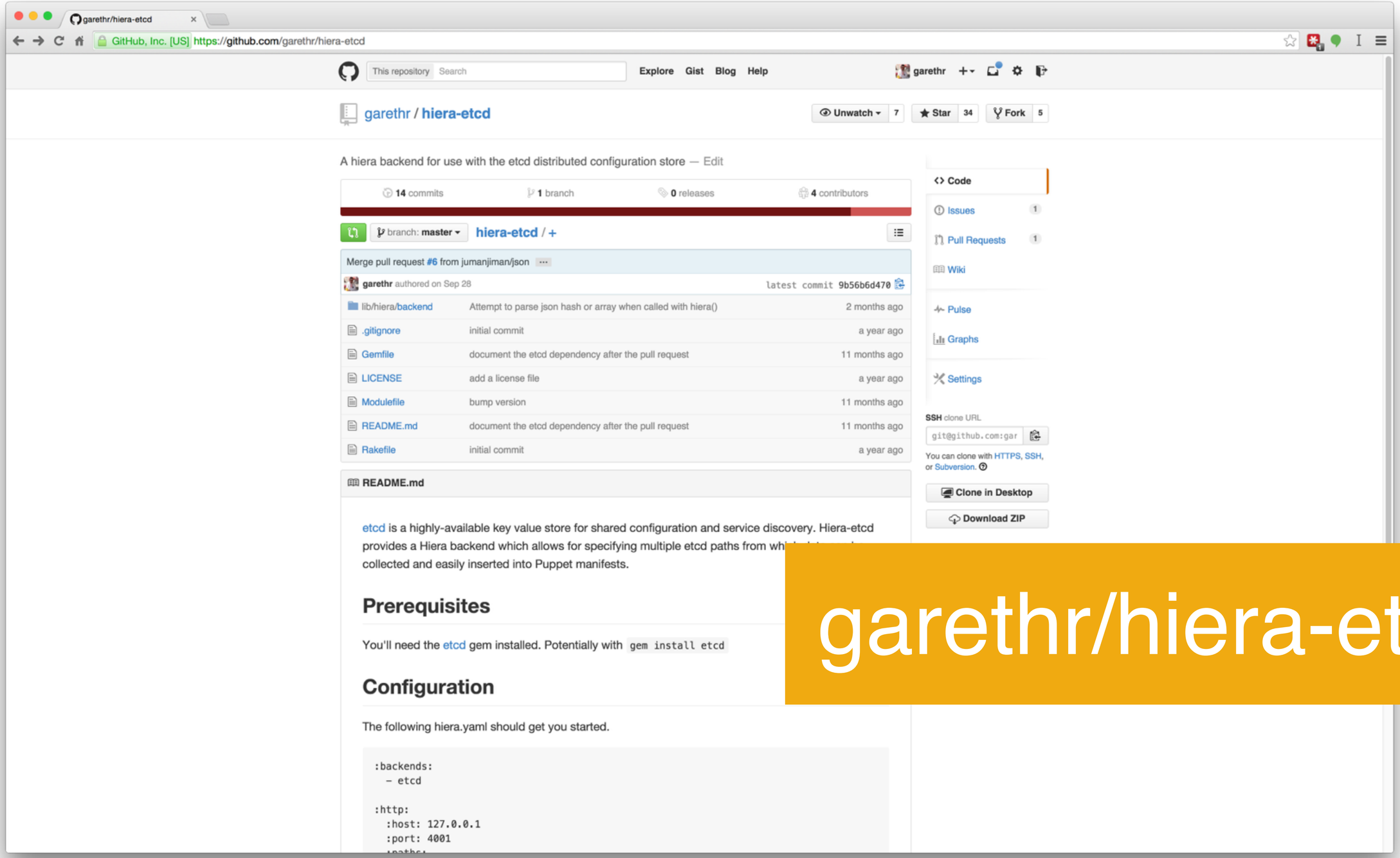

garethr/garethr-key_value
GitHub, Inc. [US] https://github.com/garethr/garethr-key_value_config
This repository Search
Explore Gist Blog Help
garethr
garethr / garethr-key_value_config
Watch 1
Star 25
Fork 2
Puppet type and providers for managing configuration in key/value stores — Edit
12 commits
1 branch
0 releases
1 contributor
branch: master
garethr-key_value_config / +
bump version number
garethr authored 27 days ago
latest commit f9be9ea197
lib/puppet fix typo in notice message 27 days ago
spec add basic consul support 27 days ago
tests initial working commit 27 days ago
.fixtures.yml initial working commit 27 days ago
.gitignore initial working commit 27 days ago
.rspec initial working commit 27 days ago
.rubocop.yml initial working commit 27 days ago
.travis.yml initial working commit 27 days ago
CONTRIBUTING.md initial working commit 27 days ago
Gemfile add basic consul support 27 days ago
Gemfile.lock
Guardfile
LICENSE
README.md
Rakefile
metadata.json
Code
Issues 0
Pull Requests 1
Wiki
Pulse
Graphs
Settings
SSH clone URL
git@github.com:gar
You can clone with HTTPS, SSH, or Subversion.
Clone in Desktop
Download ZIP
README.md
Maybe your configuration data isn't in files on disk, but in a new fancy distributed configuration store. But you still want to manage that configuration in code. Enter the key_value_config type for Puppet.
puppetforge v0.2.3
build passing
Usage
garethr/key_value_config

Going from etcd to Puppet with Hiera

Gareth Rushgrove

```
:backends:
  - etcd

:http:
  :host: 127.0.0.1
  :port: 4001
  :paths:
    - /configuration/%{fqdn}
    - /configuration/common
```



garethr/hiera-etcd

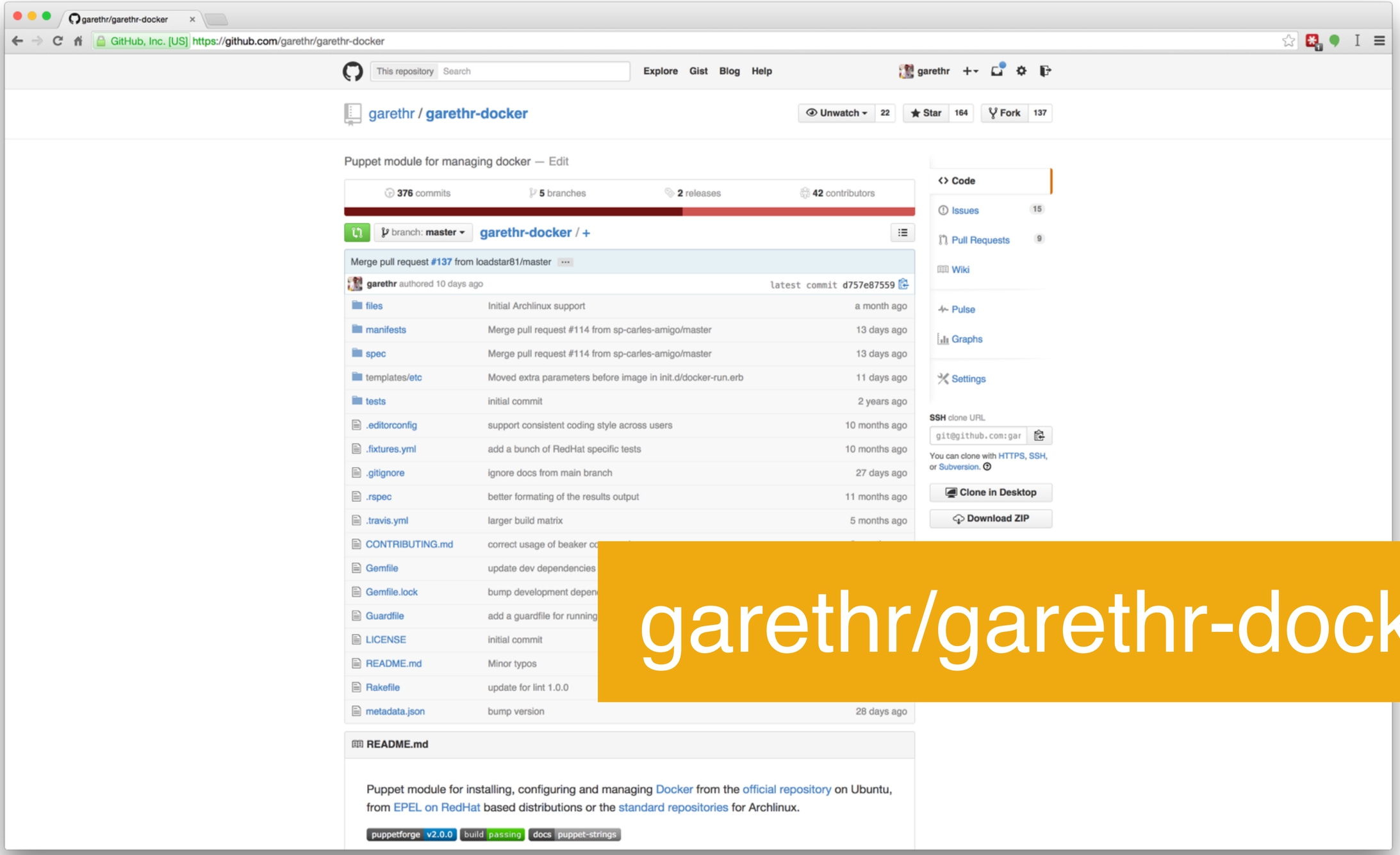
Installing systems


```
class { 'docker':
  version => 'latest',
}
docker::image { 'ubuntu':
  image_tag => 'precise'
}
```


```
class { 'mesos::master':
  zookeeper => 'zk://192.168.1.1:2181,192.168.1.2:2181,192.168.1.3:2181/mesos',
  work_dir  => '/var/lib/mesos',
  options   => {
    quorum => 2
  }
}
```

More interestingly, using systems via APIs


```
docker::run { 'helloworld':
  image   => 'base',
  command => '/bin/sh -c "while true; do echo hello world; sleep 1; done"',
}
```

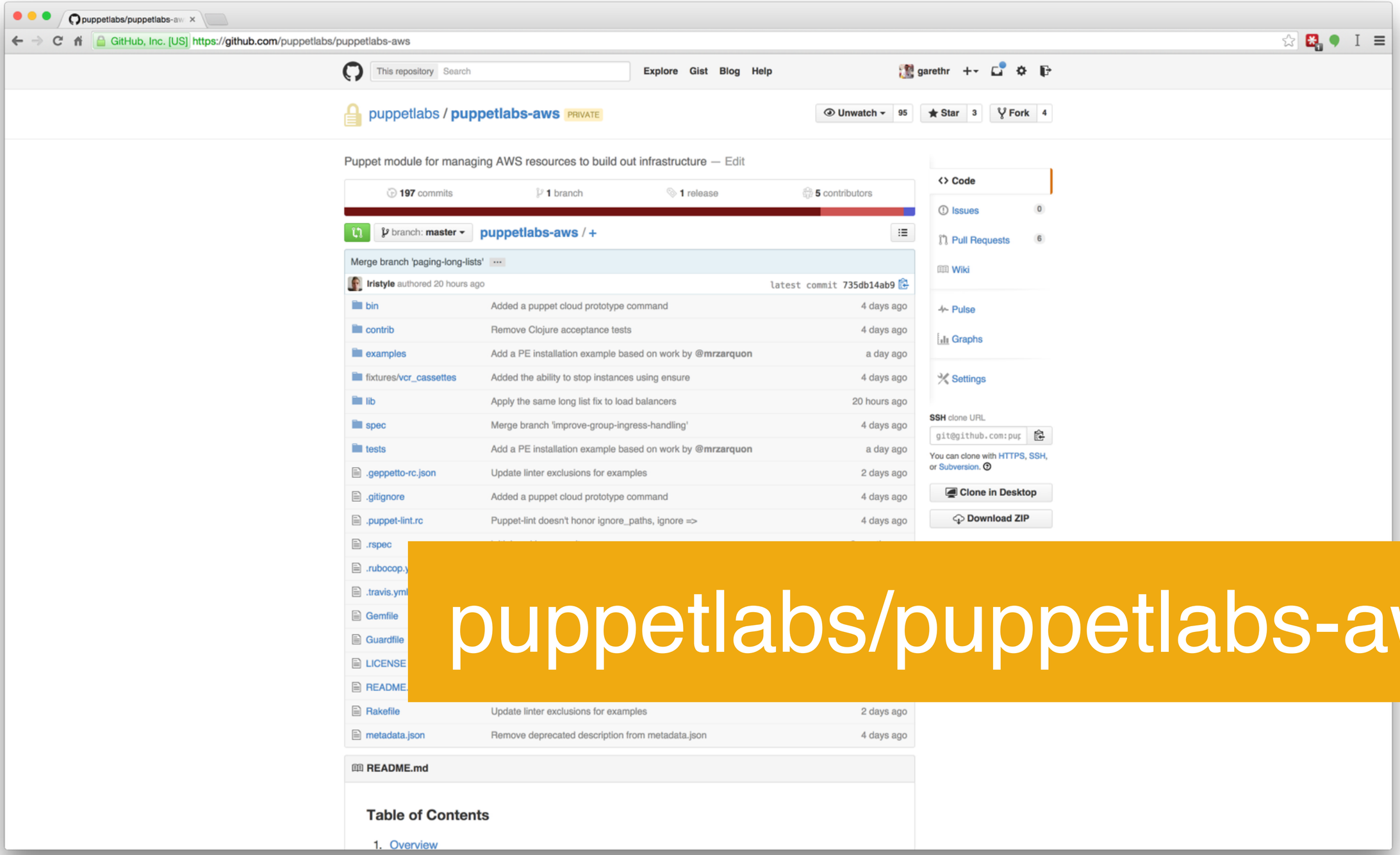


garethr/garethr-docker

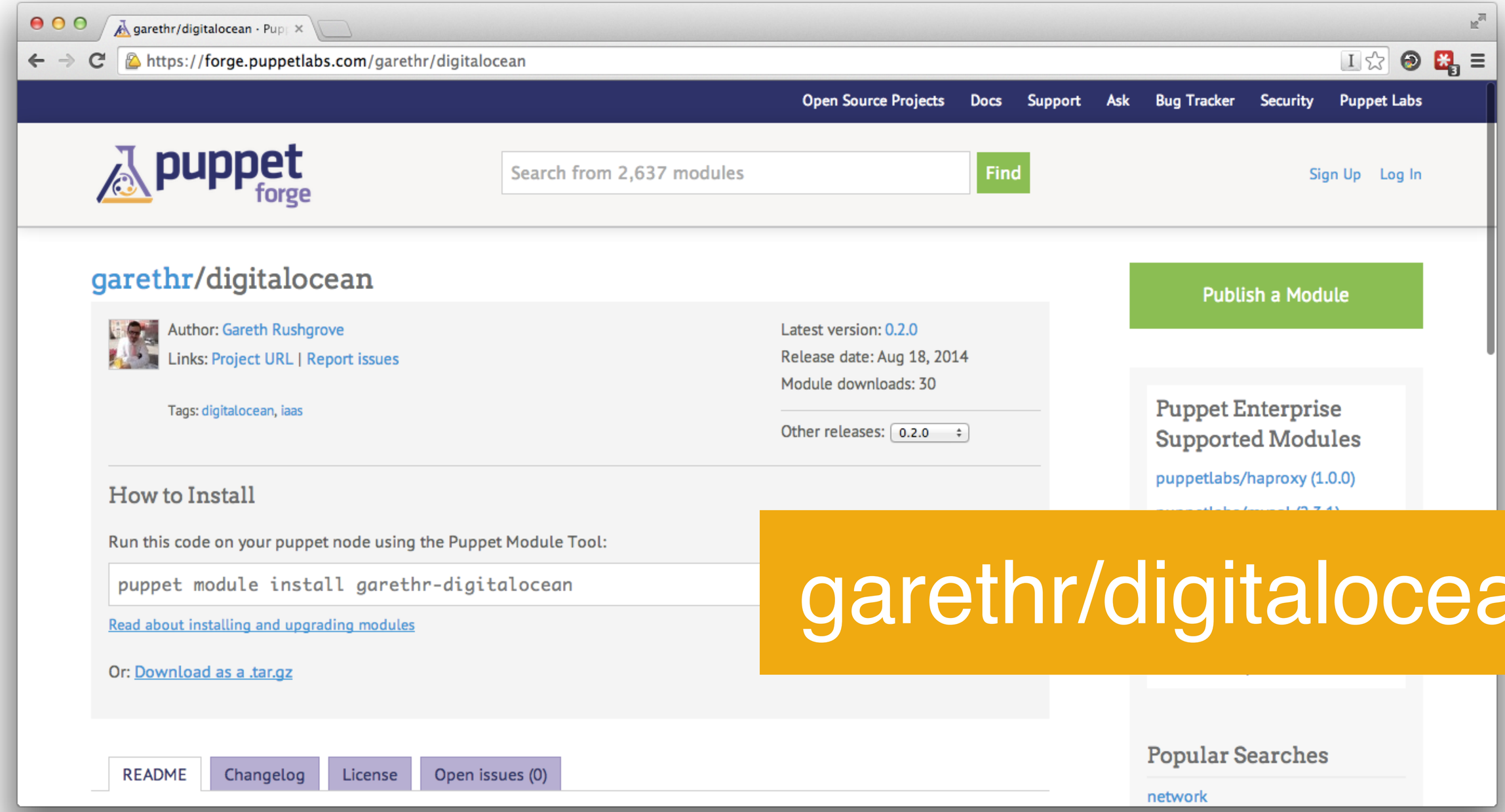

```
ec2_instance { 'name-of-instance':
  ensure            => present,
  region            => 'us-east-1',
  availability_zone => 'us-east-1a',
  image_id          => 'ami-123456',
  instance_type     => 't1.micro',
  monitoring        => true,
  key_name          => 'name-of-existing-key',
  security_groups   => ['name-of-security-group'],
  user_data         => template('module/file-path.sh.erb'),
  tags              => {
    tag_name => 'value',
  },
}
```


```
ec2_securitygroup { 'sample-group':
  ensure      => present,
  region      => 'us-east-1',
  description => 'Group used for testing Puppet AWS module',
}

ec2_loadbalancer { 'sample-load-balancer':
  ensure             => present,
  region             => 'us-west-1',
  availability_zones => ['us-west-1a', 'us-west-1b'],
  instances          => ['sample-instance', 'another-instance'],
  security_groups    => ['sample-group'],
  listeners          => [{
    protocol => 'tcp',
    port     => 80,
  }],
 }
```


puppetlabs/puppetlabs-aws
GitHub, Inc. [US] https://github.com/puppetlabs/puppetlabs-aws
This repository Search
Explore Gist Blog Help
garethr
puppetlabs / puppetlabs-aws PRIVATE
Unwatch 95 Star 3 Fork 4
Puppet module for managing AWS resources to build out infrastructure — Edit
197 commits 1 branch 1 release 5 contributors
branch: master puppetlabs-aws / +
Merge branch 'paging-long-lists'
lristyle authored 20 hours ago
latest commit 735db14ab9
bin Added a puppet cloud prototype command 4 days ago
contrib Remove Clojure acceptance tests 4 days ago
examples Add a PE installation example based on work by @mrzarquon a day ago
fixtures/vcr_cassettes Added the ability to stop instances using ensure 4 days ago
lib Apply the same long list fix to load balancers 20 hours ago
spec Merge branch 'improve-group-ingress-handling' 4 days ago
tests Add a PE installation example based on work by @mrzarquon a day ago
.geppetto-rc.json Update linter exclusions for examples 2 days ago
.gitignore Added a puppet cloud prototype command 4 days ago
.puppet-lint.rc Puppet-lint doesn't honor ignore_paths, ignore => 4 days ago
.rspec
Gemfile
Guardfile
LICENSE
Rakefile Update linter exclusions for examples 2 days ago
metadata.json Remove deprecated description from metadata.json 4 days ago
README.md
Table of Contents
1. Overview
Code
Issues 0
Pull Requests 6
Wiki
Pulse
Graphs
Settings
SSH clone URL
You can clone with HTTPS, SSH, or Subversion.
Clone in Desktop
Download ZIP
puppetlabs/puppetlabs-aws


```
droplet { ['test-digitalocean', 'test-digitalocean-1']:
  ensure             => present,
  region             => 'lon1',
  size               => '512mb',
  image              => 5141286,
  ssh_keys           => [12345], # note this is an array
  backups            => false,
  ipv6               => false,
  private_networking => false,
}
```



garethr/digitalocean

CoreOS

```
$discovery_id = '1e0904db2d660d48c534ace1325a892a'

droplet { ['coreos-1', 'coreos-2', 'coreos-3']:
  ensure             => present,
  region             => 'lon1',
  size               => '512mb',
  user_data          => template('./templates/cloud-config'),
  image              => 'coreos-stable',
  private_networking => true,
}
```

I want a pony

Managing an autoscaling CoreOS/Atomic cluster in AWS…

…with configuration in etcd/consul…

…with the network in VPC /Weave…

…with docker containers arranged by Kubernetes…

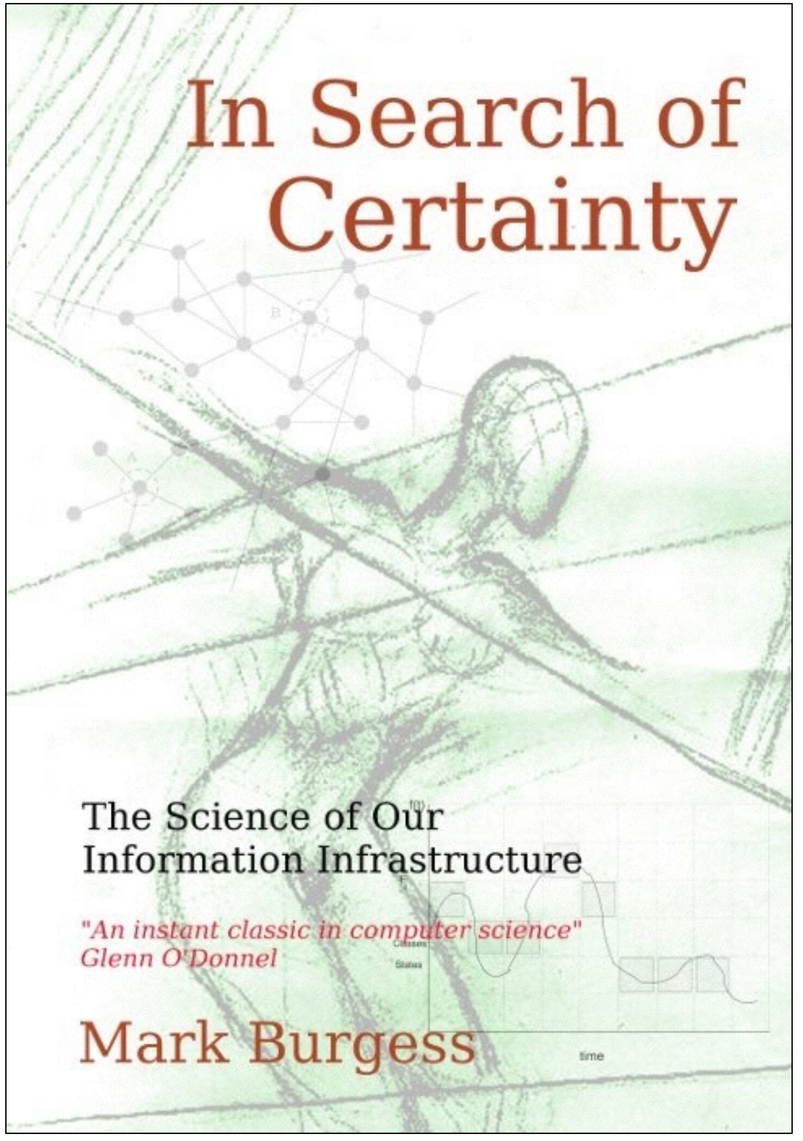
All from the Puppet DSL

Conclusions

The future is already here — it's just not very evenly distributed.

William Gibson

Manage. Not just provision


In Search of Certainty
The Science of Our Information Infrastructure
"An instant classic in computer science"
Glenn O'Donnel
Mark Burgess
time

Questions?

And thanks for listening