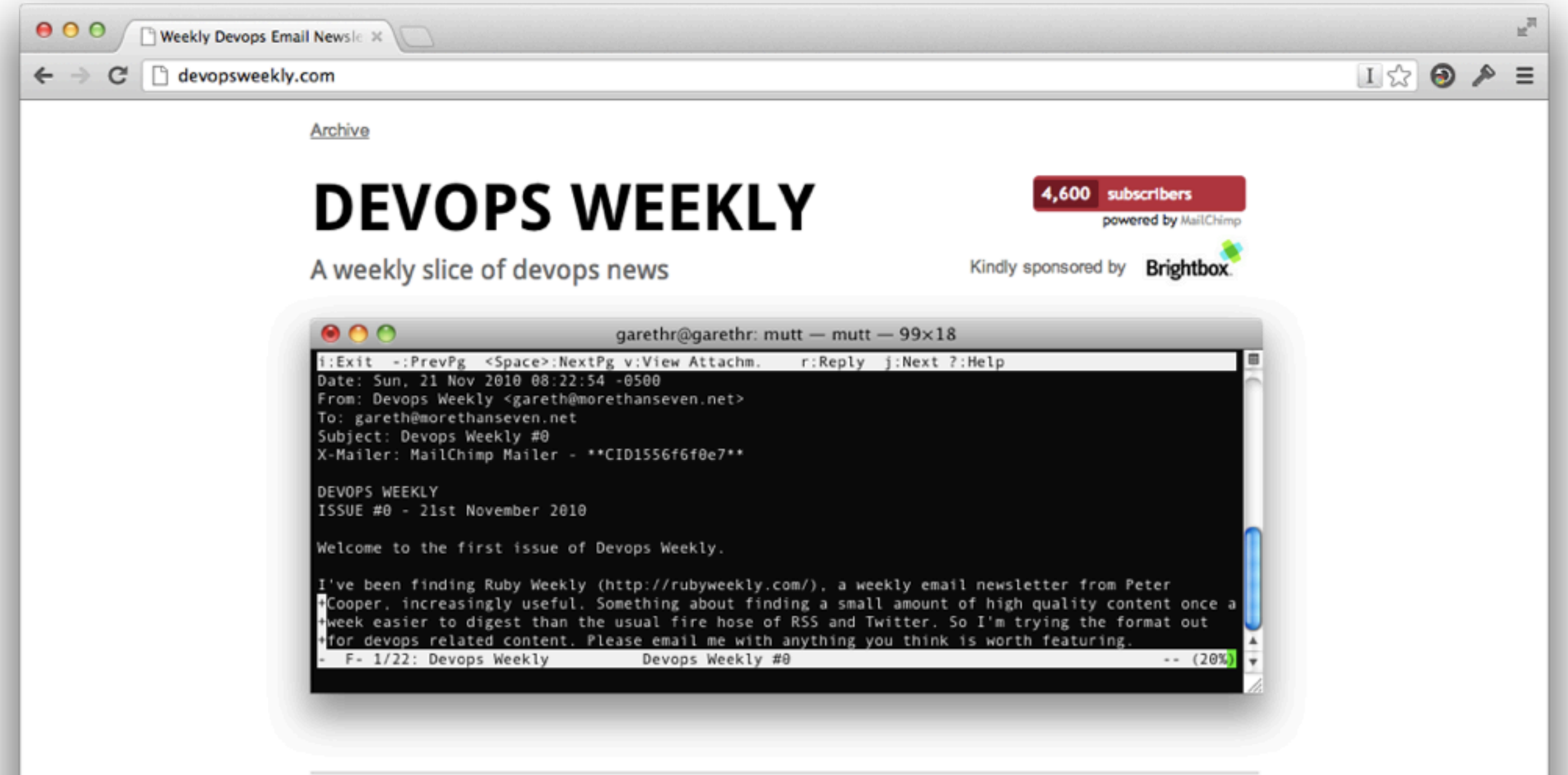
Clouds in Government
Perils of Portability

QCon 6th February 2013

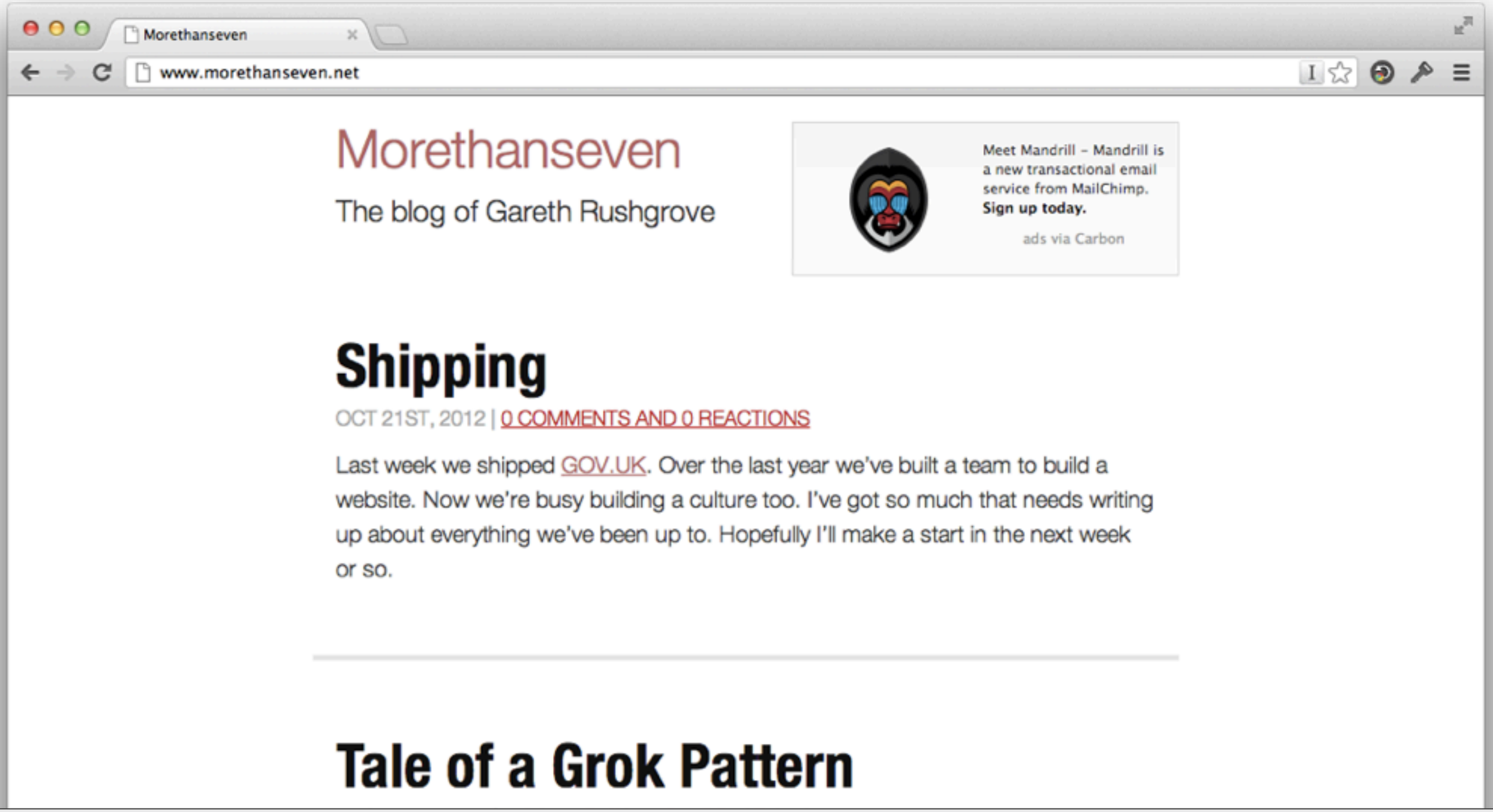
gareth rushgrove | morethanseven.net

Me

Gareth Rushgrove @garethr



Curate devopsweekly.com



Blog at morethanseven.net

Work at UK Government Digital Service

gareth rushgrove | morethanseven.net

I am a Civil Servant

http://www.flickr.com/photos/benterrett/6852348725/

Perils

Clouds and portability

per·il

/ˈperəl/

Noun

1. Serious and immediate danger.
2. The dangers or difficulties that arise from a particular situation or activity.

The 2nd definition

Peril 1

Caring about Image formats

AMI, VMDK, OVF, VHD, VDI, etc.

gareth rushgrove | morethanseven.net

But I have many machines

http://www.flickr.com/photos/uk_parliament/2700311119/

And my infrastructure is more than just machines

http://www.flickr.com/photos/uk_parliament/2700327415

Peril 2

API proliferation

AssignPrivateIpAddresses

docs.aws.amazon.com/AWSEC2/latest/APIReference/ApiReference-query-AssignPrivateIpAddresses.html

aws documentation

Amazon Elastic Compute Cloud

API Reference (API Version 2012-12-01)

Search: Documentation

- Welcome
- List of Actions by Function
- Actions
  - AllocateAddress
  - **AssignPrivateIpAddresses**
  - AssociateAddress
  - AssociateDhcpOptions
  - AssociateRouteTable
  - AttachInternetGateway
  - AttachNetworkInterface
  - AttachVolume
  - AttachVpnGateway
  - AuthorizeSecurityGroupEgress
  - AuthorizeSecurityGroupIngress
  - BundleInstance
  - CancelBundleTask
  - CancelConversionTask
  - CancelExportTask
  - CancelReservedInstancesListing
  - CreateImage

AWS Documentation » Amazon EC2 » API Reference » Actions » AssignPrivateIpAddresses

« Previous Next »

View PDF | Go to the forums

Did this page help you? Yes | No | Tell us about it...

AssignPrivateIpAddresses

Description

Assigns one or more secondary private IP addresses to the specified network interface. You can specify one or more specific secondary IP addresses, or you can specify the number of secondary IP addresses to be automatically assigned within the subnet's CIDR block range. The number of secondary IP addresses that you can assign to an instance varies by instance type. For information about instance types, see Available Instance Types in the *Amazon Elastic Compute Cloud User Guide*. For more information about Elastic IP addresses, see Elastic IP Addresses in the *Amazon Elastic Compute Cloud User Guide*.

This action is available only in VPC.

Request Parameters

Name	Description	Required
NetworkInterfaceId	The network interface to which the IP address is assigned. Type: String Default: None	Yes
PrivateIpAddress.n	The IP address to be assigned as a secondary private IP address to the network interface.	Conditional

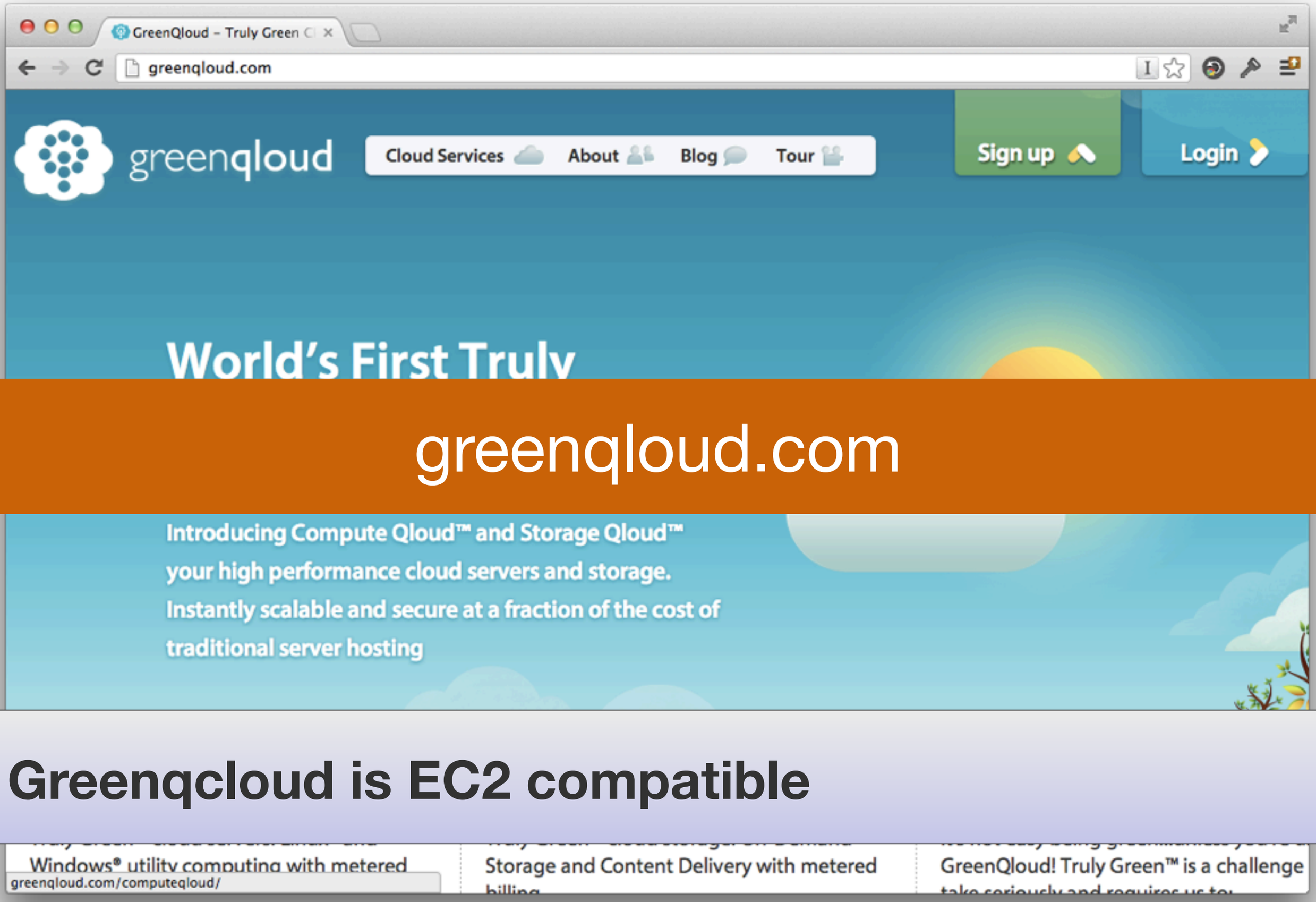
Amazon EC2

160+ actions

Big API (Just EC2)

Lots more APIs

API compatibility and de facto standards



greenqloud.com

Greenqcloud is EC2 compatible

www.eucalyptus.com

Eucalyptus

EUCALYPtUS

Funny story

Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems

Eucalyptus is an acronym

gareth rushgrove | morethanseven.net

Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems

Ta da

gareth rushgrove | morethanseven.net

It’s not all about the APIs

http://www.flickr.com/photos/uk_parliament/2757120644

Peril 3

Cloud primitives

- Instance
- Images
- Elastic Compute Cloud (EC2)
- Elastic IP (EIP)
- Elastic Network Interfaces (EIN)
- Elastic Block Store (EBS)
- Simple Storage Service (S3)
- Elastic Load Balancers (ELB)

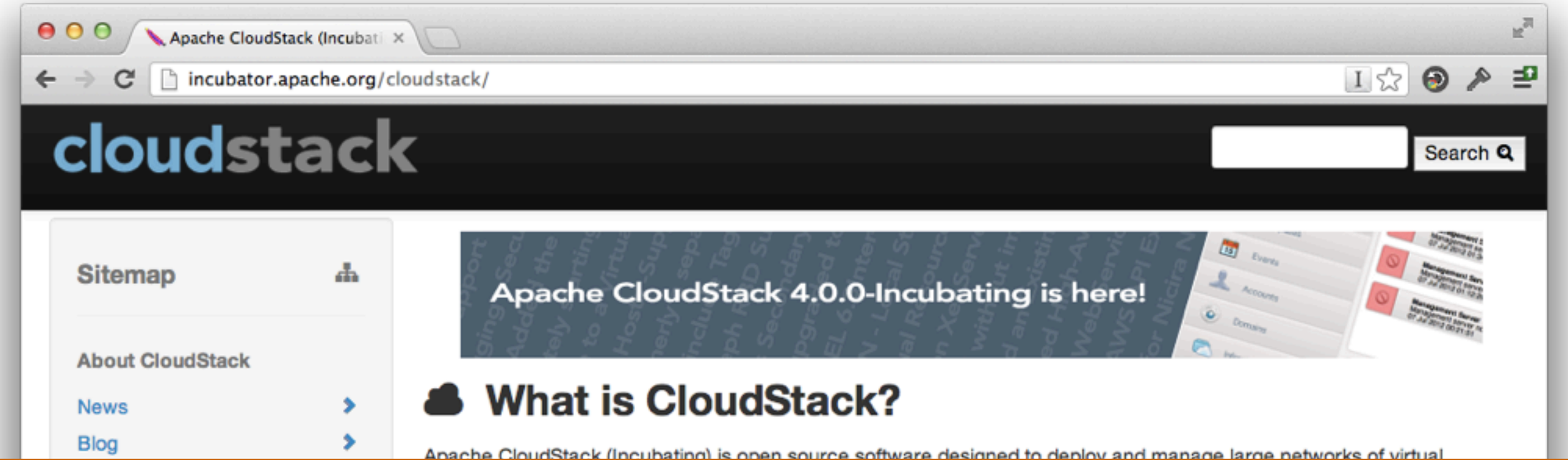
AWS - All the acronyms!

www.openstack.org

OpenStack

- Compute
- Storage
- Networking
- Instance
- Security group
- Object store
- Block store

OpenStack



incubator.apache.org/cloudstack/

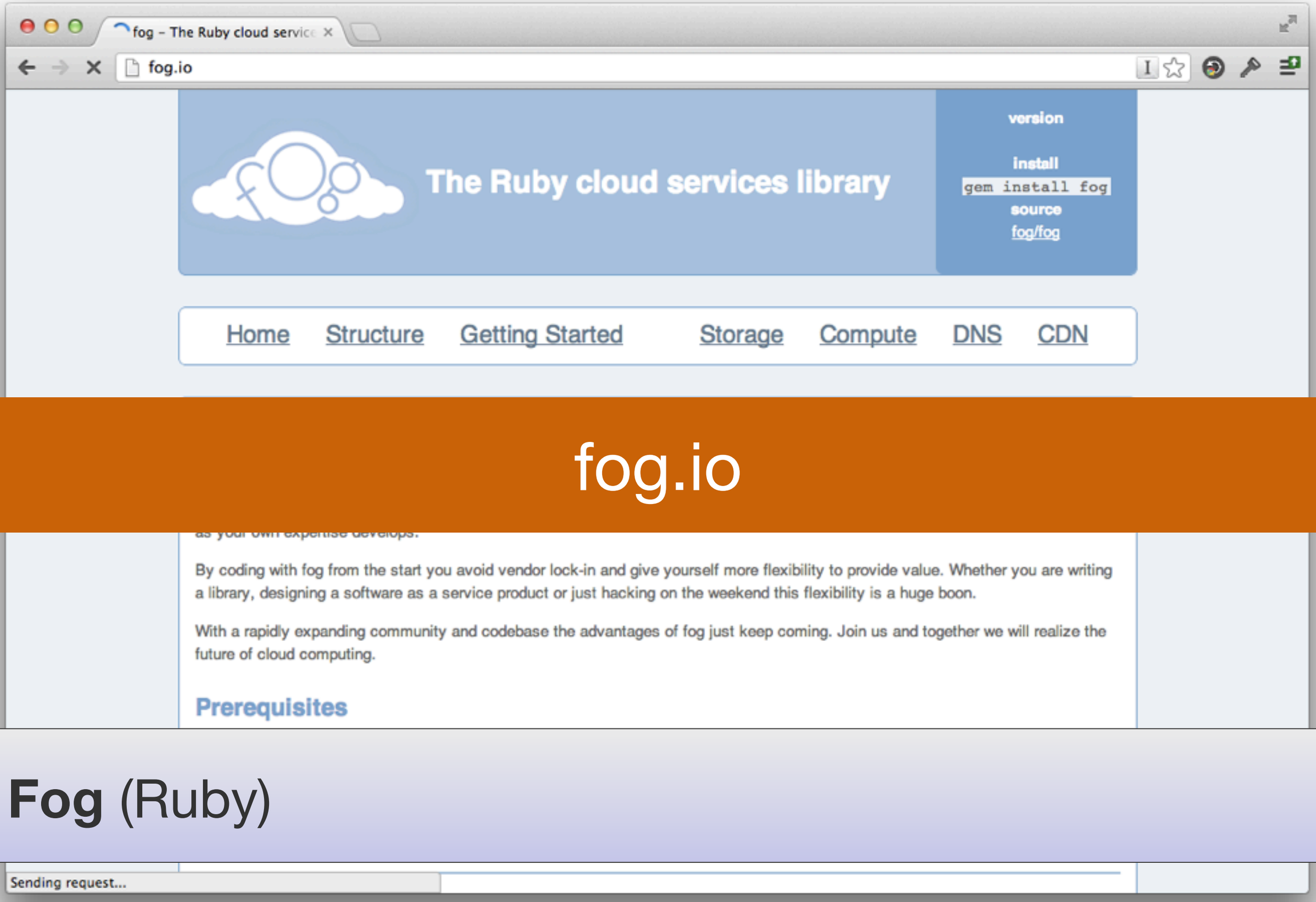
CloudStack

- Network
- VPC
- Virtual machine
- VPN
- Load balancer
- Router
- ISO
- Volume
- Template
- Security group
- User
- Snapshot
- NAT
- VM group
- Resource tag
- Address
- Zone
- Disk offering
- Project
- Network
- Firewall
- Account
- Hypervisor
- Guest OS

CloudStack

Abstractions to the rescue?

http://www.flickr.com/photos/uk_parliament/2701192648/



fog.io

Fog (Ruby)

- Compute
- Storage
- CDN
- DNS

Fog primitives

libcloud.apache.org

Apache Libcloud a unified interface to the cloud

Apache Libcloud is a standard Python library that abstracts away differences among multiple cloud provider APIs

"libcloud represents a fundamental change in the way clouds are managed, breaking the barriers of proprietary, closed clouds. We at Linode believe this is of the utmost importance and fully

"Libcloud will make life easier for our customers. We appreciate and support this standardization tool."
- Matt Tanase, Slicehost, Founder

"I'm excited to see the development of projects, like libcloud, that help make the lives of the cloud computing community easier by offering a standardized way to communicate with

"We believe in an open cloud and are thrilled to see libcloud push the movement forward."
- Paul Lancaster, GoGrid, Business Development Manager

news
about
getting started
documentation
who's using libcloud?

Apache Libcloud is a standard Python library that abstracts away differences among multiple cloud provider APIs.

The current version allows users to manage four different cloud resources:

- Cloud Servers - services such as Amazon EC2 and Rackspace CloudServers (**libcloud.compute.***)

contributing

www.slicehost.com

BLUE BOX GROUP, LLC
Flexible servers in the cloud

libcloud (Python)

- Compute
- Storage
- Load balancers
- DNS

libcloud primitives

www.jclouds.org

jclouds (Java)

- Computeservice
- Blob store

jclouds primitives

> “There are only two hard things in Computer Science: cache invalidation and naming things.”

Phil Karlton

Naming things is hard

Peril 4

Slipperly slope of
Platform as a Service

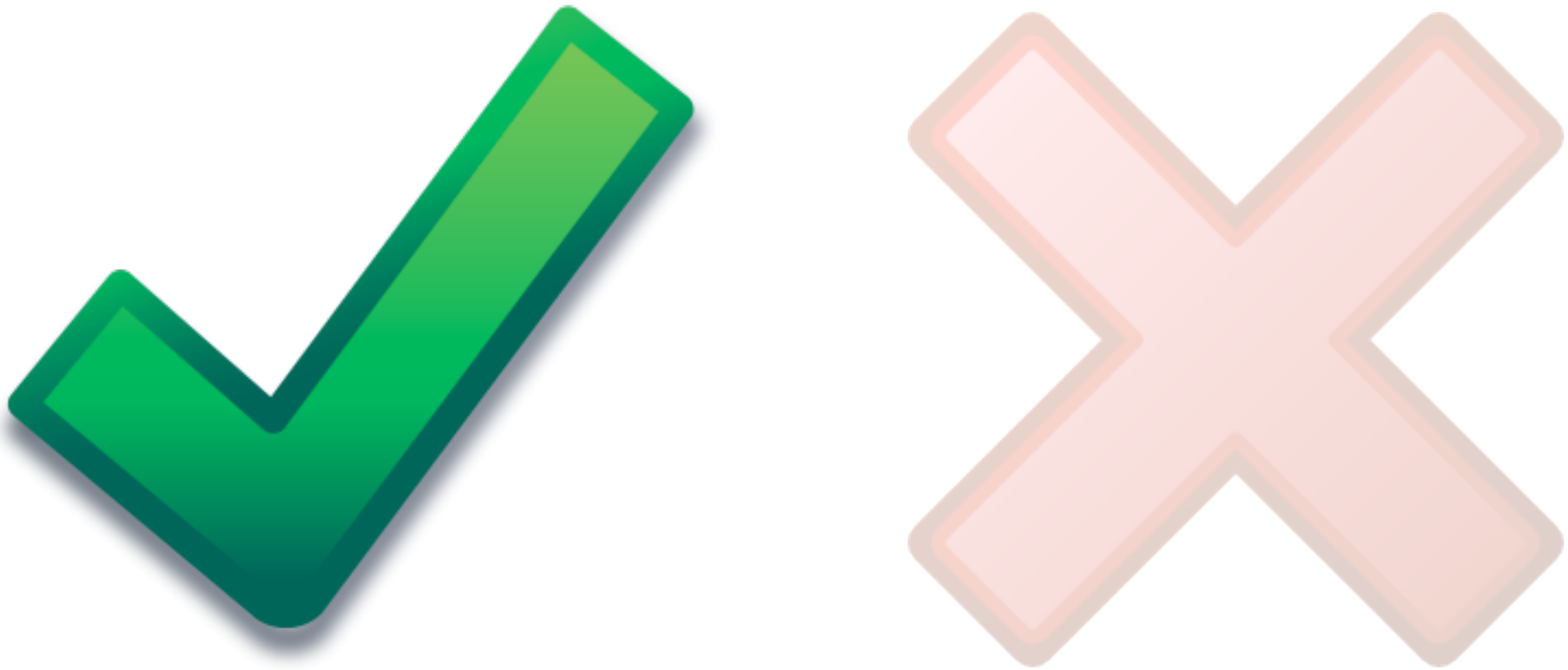
PaaS

...does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage...

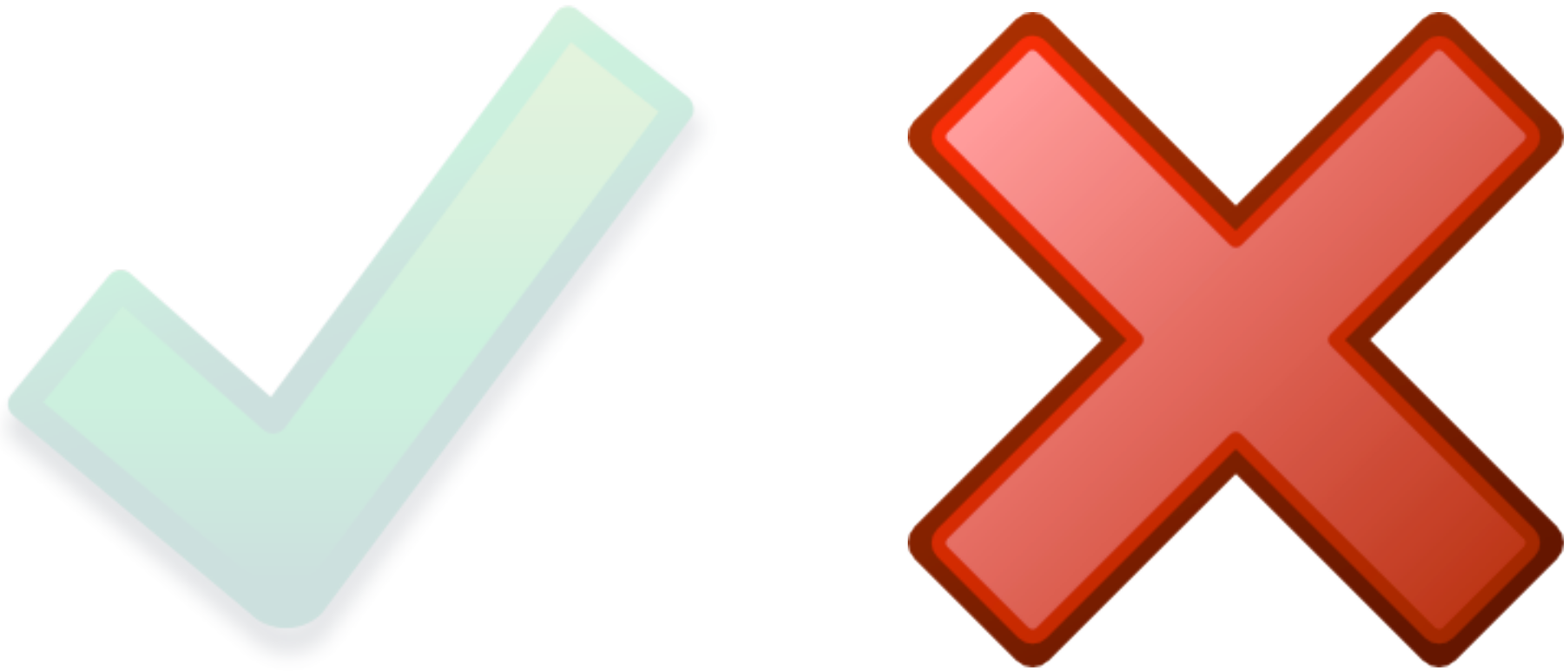
IaaS

...does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components...

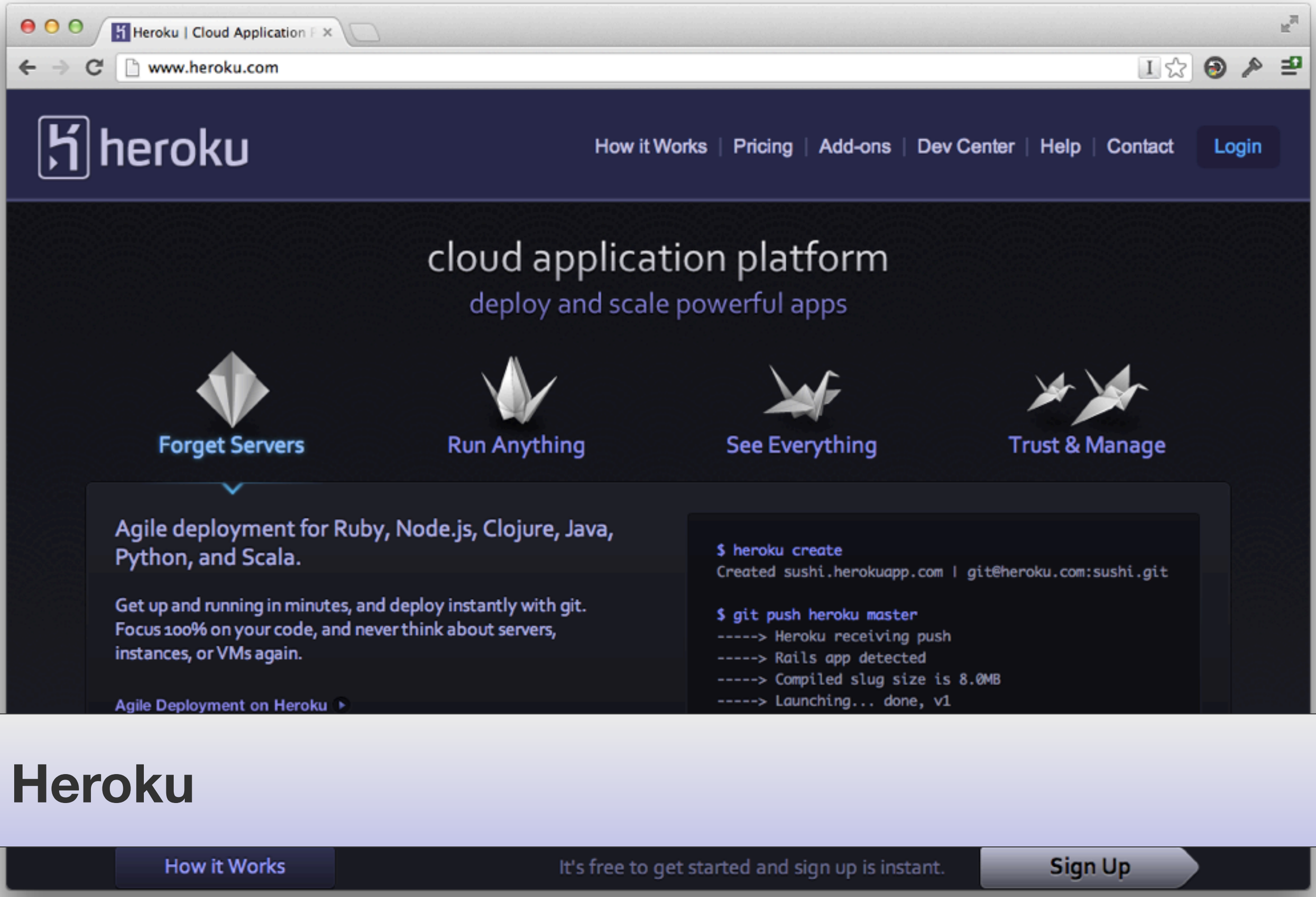
Definitions



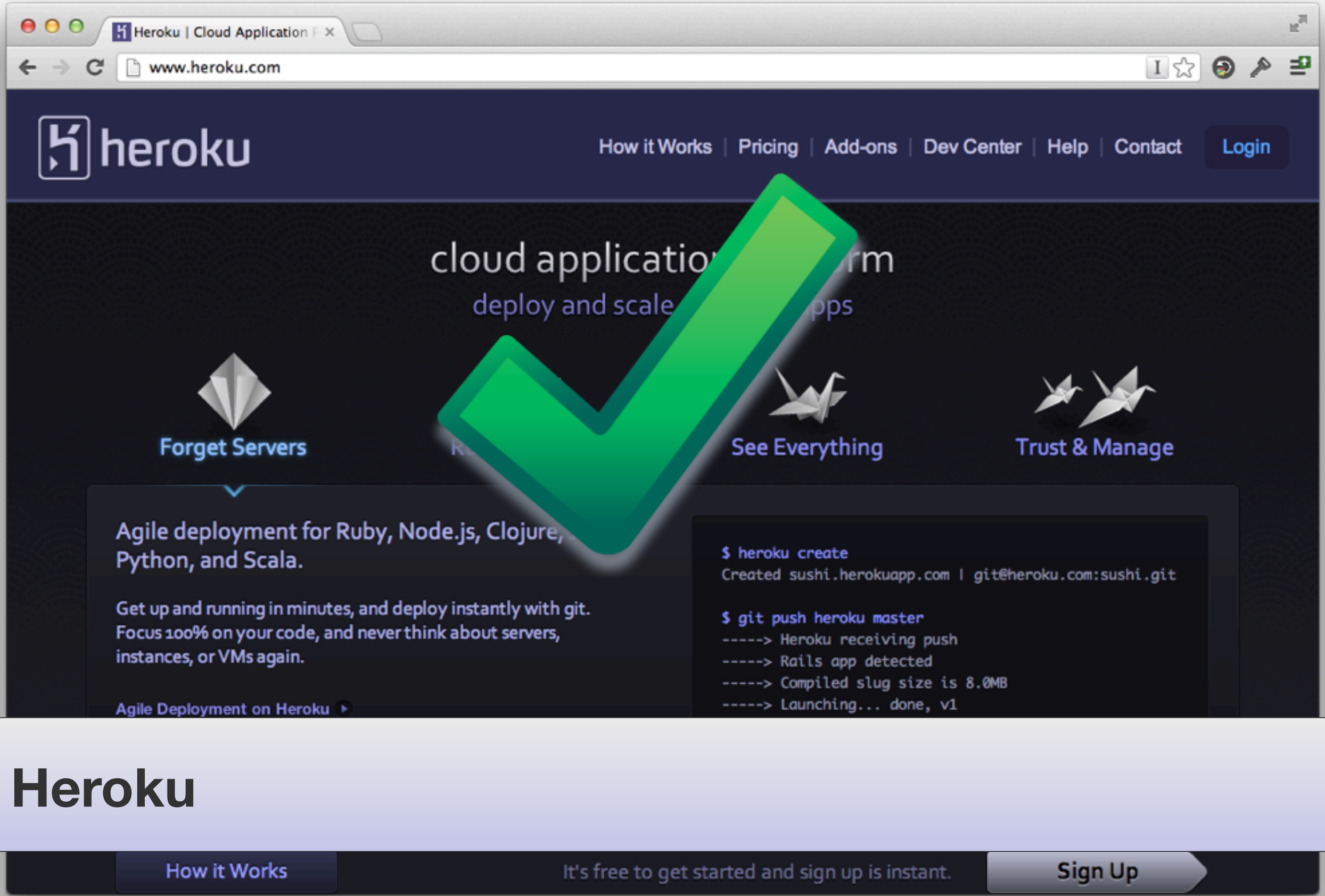
Platform as a Service



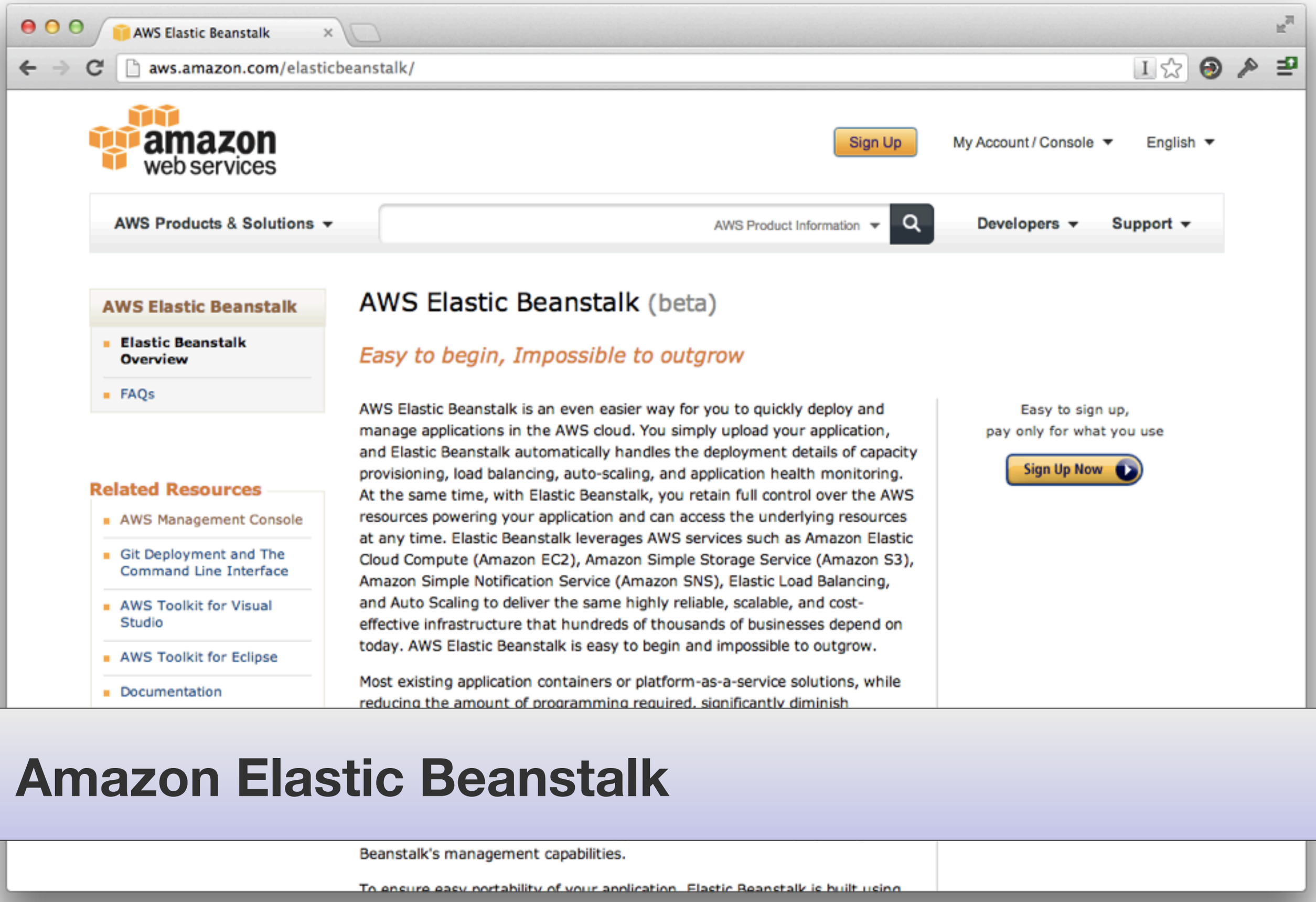
Not PaaS


Heroku | Cloud Application
www.heroku.com
heroku
How it Works | Pricing | Add-ons | Dev Center | Help | Contact
Login
cloud application platform
deploy and scale powerful apps
Forget Servers
Run Anything
See Everything
Trust & Manage
Agile deployment for Ruby, Node.js, Clojure, Java, Python, and Scala.
Get up and running in minutes, and deploy instantly with git. Focus 100% on your code, and never think about servers, instances, or VMs again.
Agile Deployment on Heroku
$ heroku create
Created sushi.herokuapp.com | git@heroku.com:sushi.git
$ git push heroku master
-----> Heroku receiving push
-----> Rails app detected
-----> Compiled slug size is 8.0MB
-----> Launching... done, v1
How it Works
It's free to get started and sign up is instant.
Sign Up

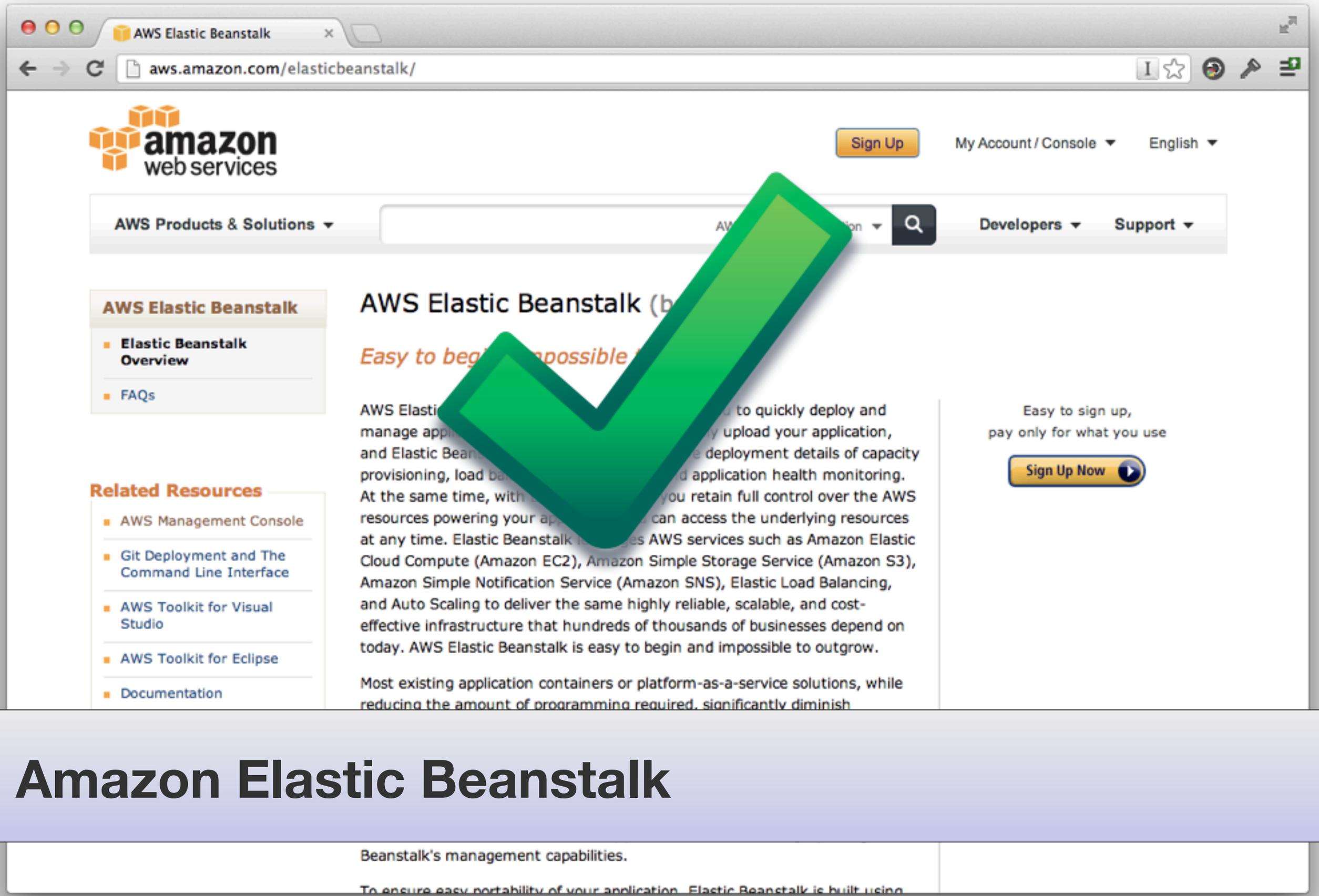
Heroku


Heroku | Cloud Application
www.heroku.com
heroku
How it Works | Pricing | Add-ons | Dev Center | Help | Contact
Login
cloud applicatio rm
deploy and scale pps
Forget Servers
See Everything
Trust & Manage
Agile deployment for Ruby, Node.js, Clojure, Python, and Scala.
Get up and running in minutes, and deploy instantly with git. Focus 100% on your code, and never think about servers, instances, or VMs again.
Agile Deployment on Heroku
$ heroku create
Created sushi.herokuapp.com | git@heroku.com:sushi.git
$ git push heroku master
-----> Heroku receiving push
-----> Rails app detected
-----> Compiled slug size is 8.0MB
-----> Launching... done, v1
How it Works
It's free to get started and sign up is instant.
Sign Up

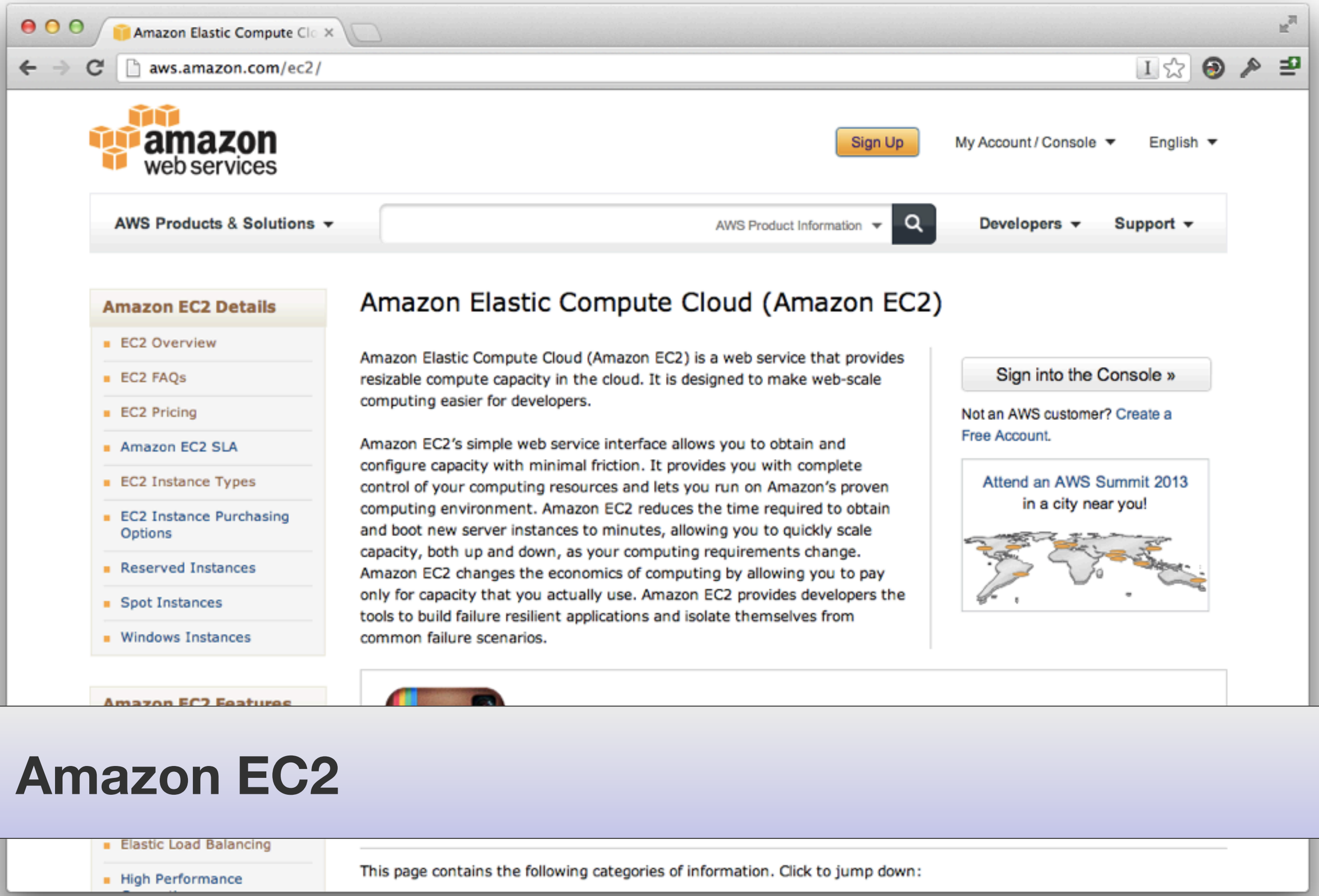
Heroku



Amazon Elastic Beanstalk



Amazon Elastic Beanstalk


Amazon Elastic Compute Cl
aws.amazon.com/ec2/
amazon web services
Sign Up
My Account / Console
English
AWS Products & Solutions
AWS Product Information
Developers
Support
Amazon EC2 Details
EC2 Overview
EC2 FAQs
EC2 Pricing
Amazon EC2 SLA
EC2 Instance Types
EC2 Instance Purchasing Options
Reserved Instances
Spot Instances
Windows Instances
Amazon EC2 Features
Elastic Load Balancing
High Performance
Amazon Elastic Compute Cloud (Amazon EC2)
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.
Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.
Sign into the Console »
Not an AWS customer? Create a Free Account.
Attend an AWS Summit 2013 in a city near you!
This page contains the following categories of information. Click to jump down:

Amazon EC2


Amazon Elastic Compute Cl
aws.amazon.com/ec2/
amazon web services
Sign Up
My Account / Console
English
AWS Products & Solutions
Developers
Support
Amazon EC2 Details
EC2 Overview
EC2 FAQs
EC2 Pricing
Amazon EC2 SLA
EC2 Instance Types
EC2 Instance Purchasing Options
Reserved Instances
Spot Instances
Windows Instances
Amazon Elasti (Amazon EC2)
Amazon Elastic Compute C service that provides resizable compute capac make web-scale computing easier for
Amazon EC2's erface a d configure cap ction. It prov te control of your urces and lets you s proven computing environ azon EC2 reduces the ti ed to obtain and boot new server ances to minutes, allowing you quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.
Sign into the Console »
Not an AWS customer? Create a Free Account.
Attend an AWS Summit 2013 in a city near you!
Amazon EC2 Features
Elastic Load Balancing
High Performance
This page contains the following categories of information. Click to jump down:

Amazon EC2

VMware vCloud Director: Se

https://www.vmware.com/products/vcloud-director/overview.html

United States [change] Search

vmware

Community | Forums | Technical Resources | Virtual Appliances | Store | My VMware

Cloud Computing | Virtualization | Solutions | Products | Services | Support & Downloads | Partners | Company

Home > Products > Datacenter Products > VMware vCloud Director

VMware vCloud™ Director

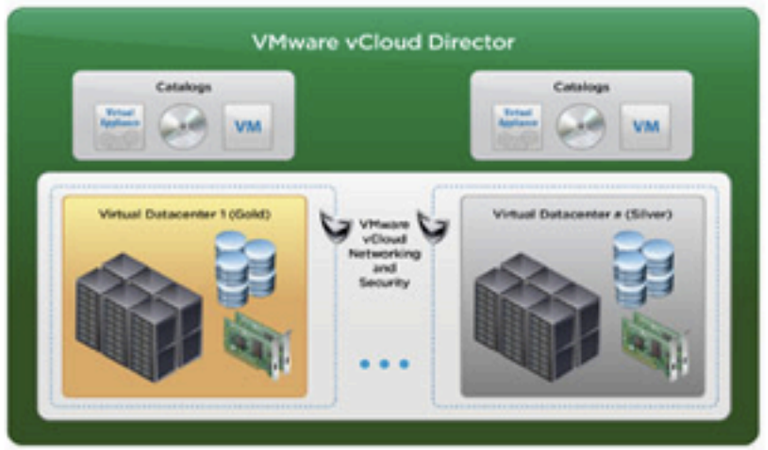
COMPLETE SOFTWARE-DEFINED DATACENTER SERVICES IN MINUTES

Questions? 1-877-486-9273

Email Us

Deliver Complete Virtual Datacenters for Consumption in Minutes

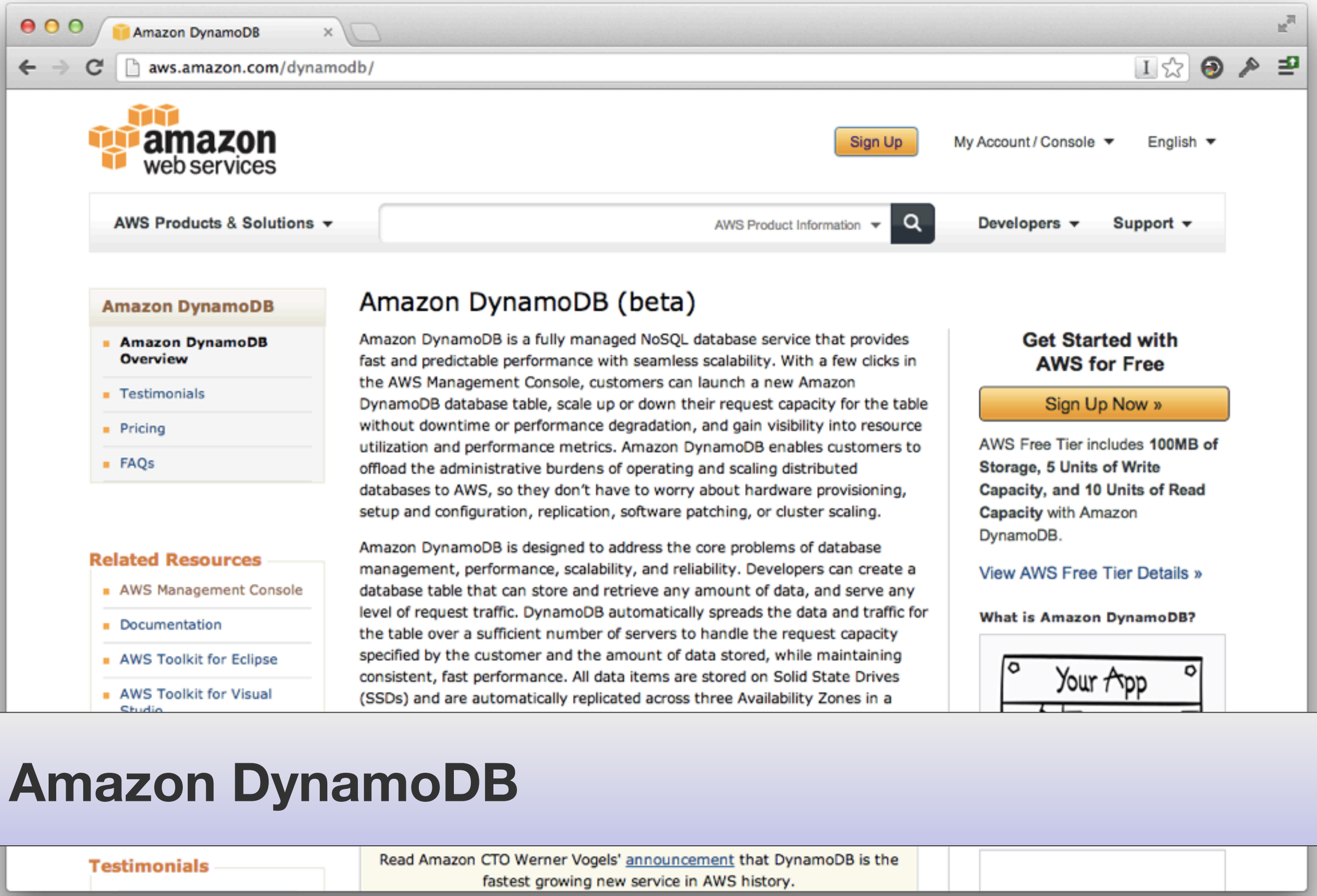
Orchestrate the provisioning of software-defined datacenter services as complete virtual datacenters that are ready for consumption in a matter of minutes. Virtual datacenters provide virtualized compute, networking, storage, and security. Administrators can provision the complete set of services necessary to make workloads operational in minutes. Software-defined datacenter service and the virtual datacenters fundamentally simplify infrastructure provisioning, and enable IT to move at the speed of business.



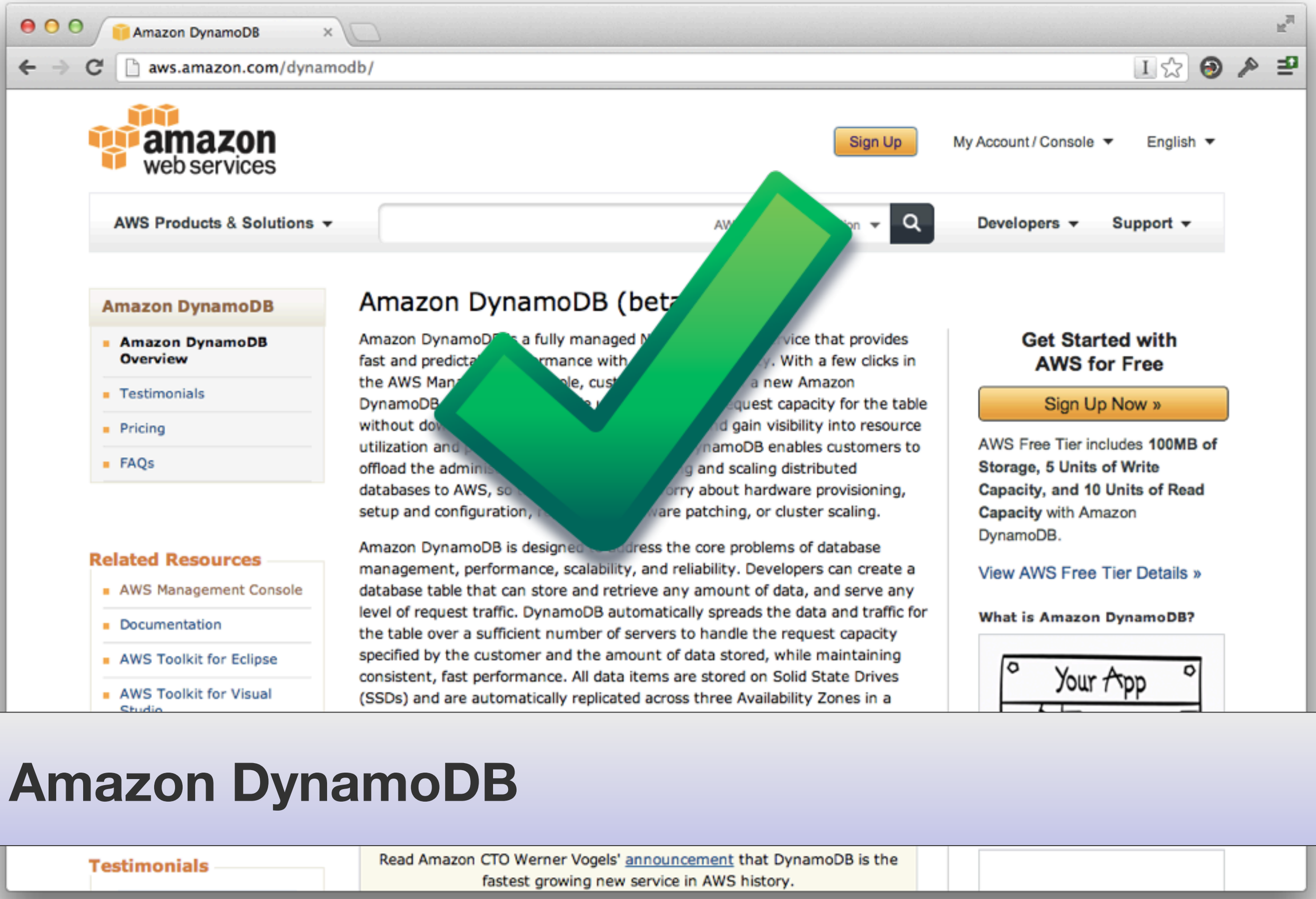
Download Free Trial | Contact Sales | Find A Partner

vCloud Director

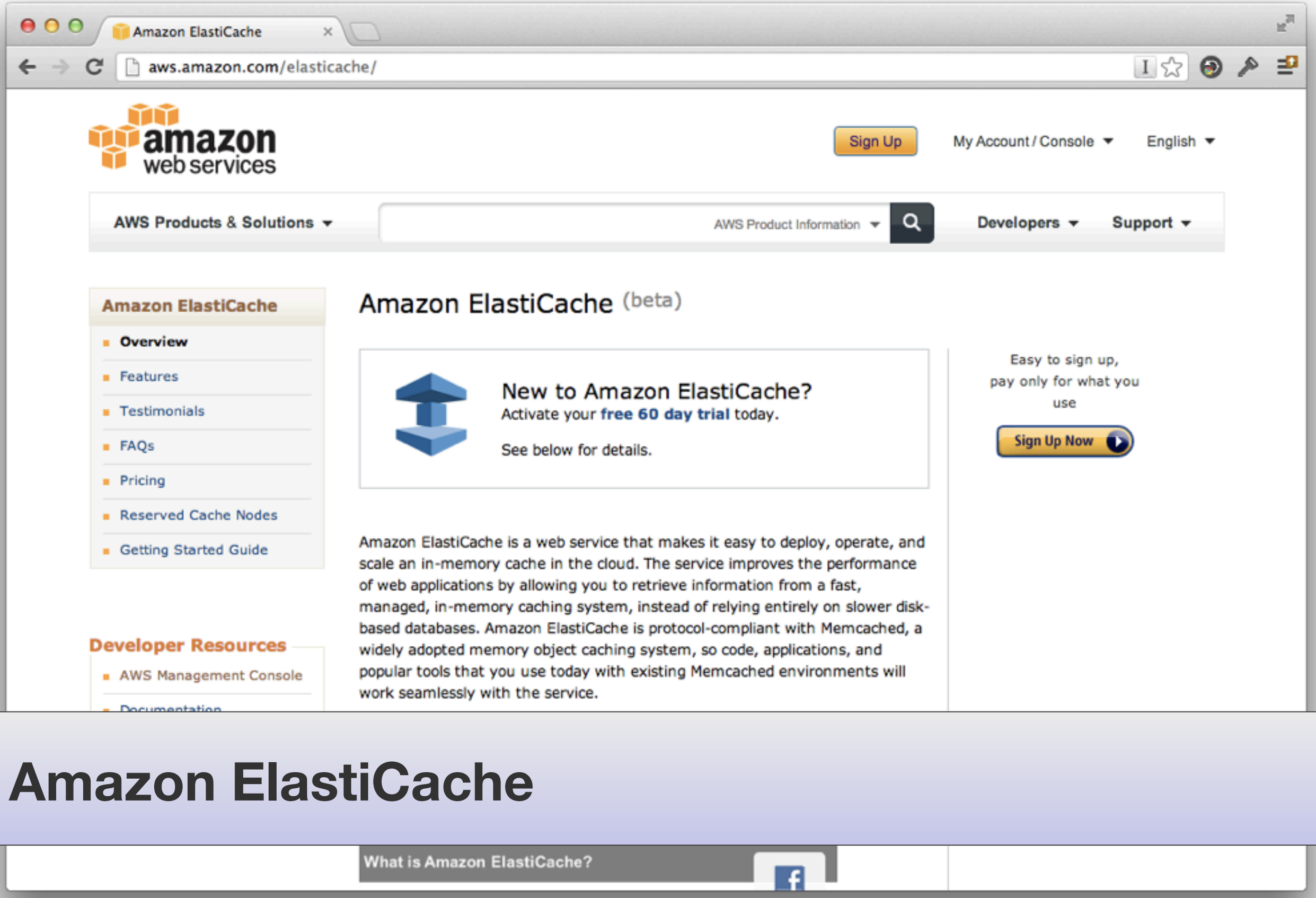
vCloud Director



Amazon DynamoDB



Amazon DynamoDB

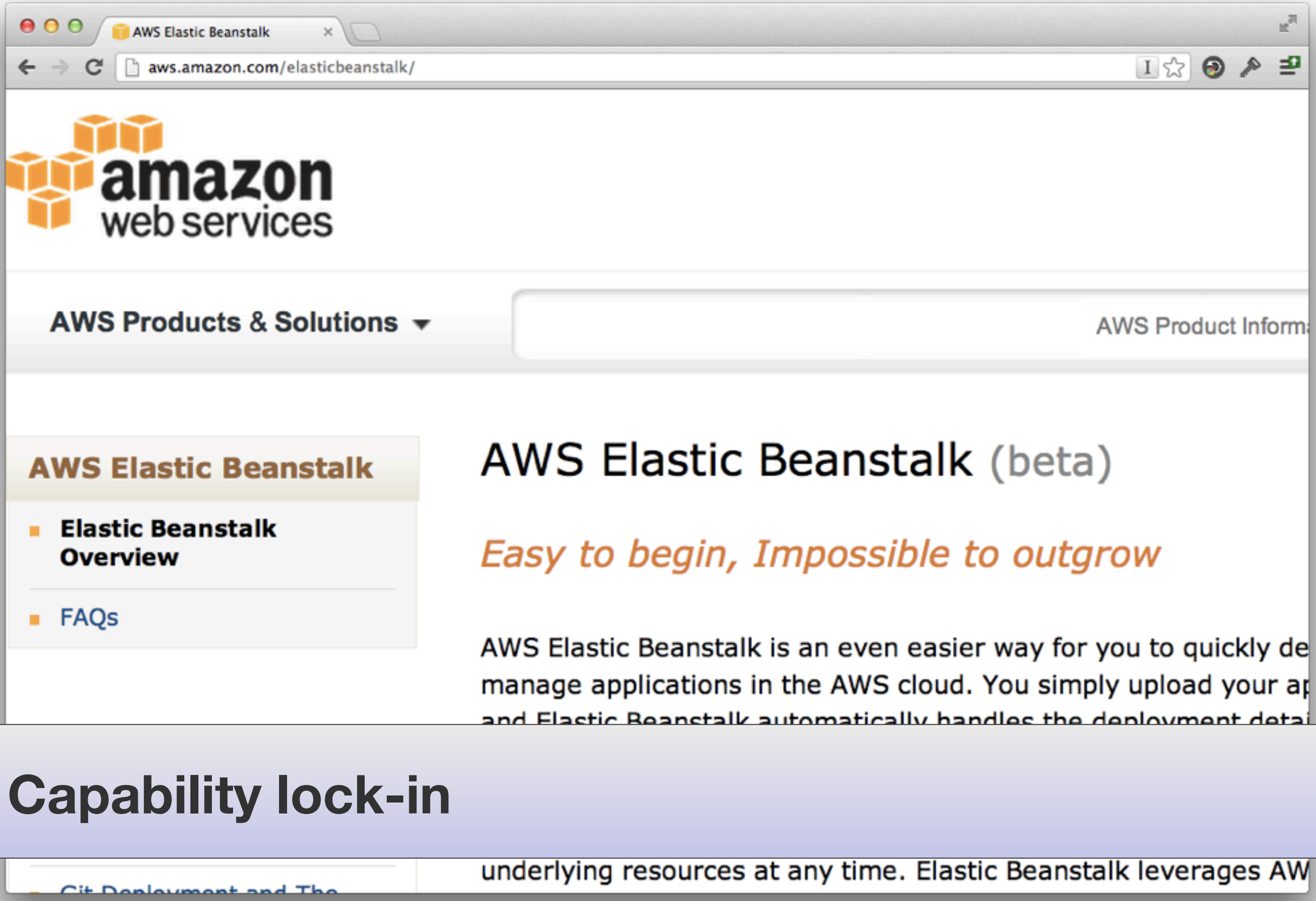


Amazon ElastiCache

Amazon ElastiCache

Peril 5

Vendor lock-in



Capability lock-in

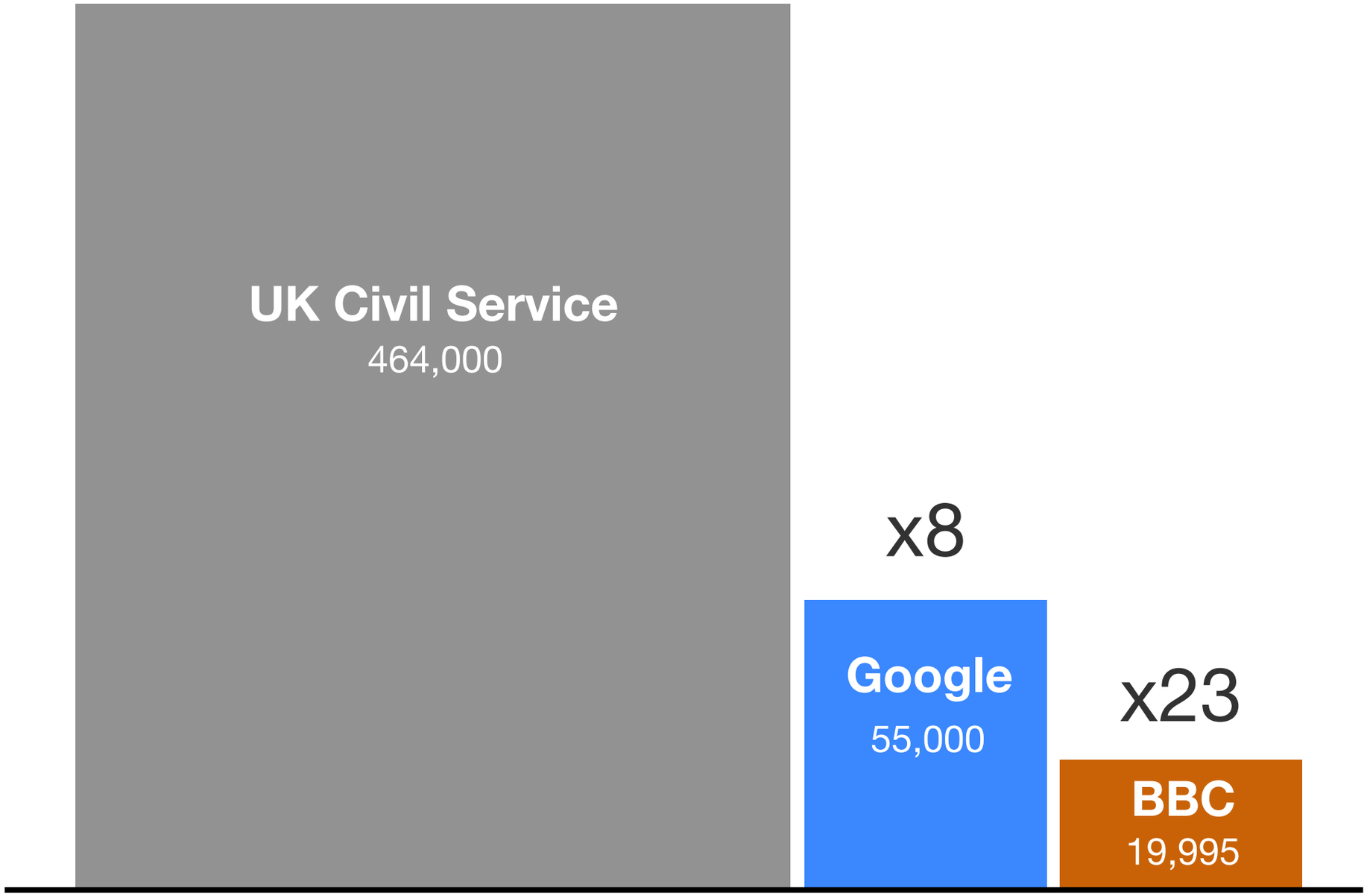
Capacity lock-in

Ecosystem lock-in

http://www.flickr.com/photos/uk_parliament/2700549757/

Interlude

The story of GOV.UK



Government is Big

www.cabinetoffice.gov.uk/sites/default/files/resources/Martha%20Lane%20Fox's%20letter%20to%20Francis%20Maude%2014th%20...

Race Online 2012

www.raceonline2012.org

14th October 2010

Dear Francis Maude,

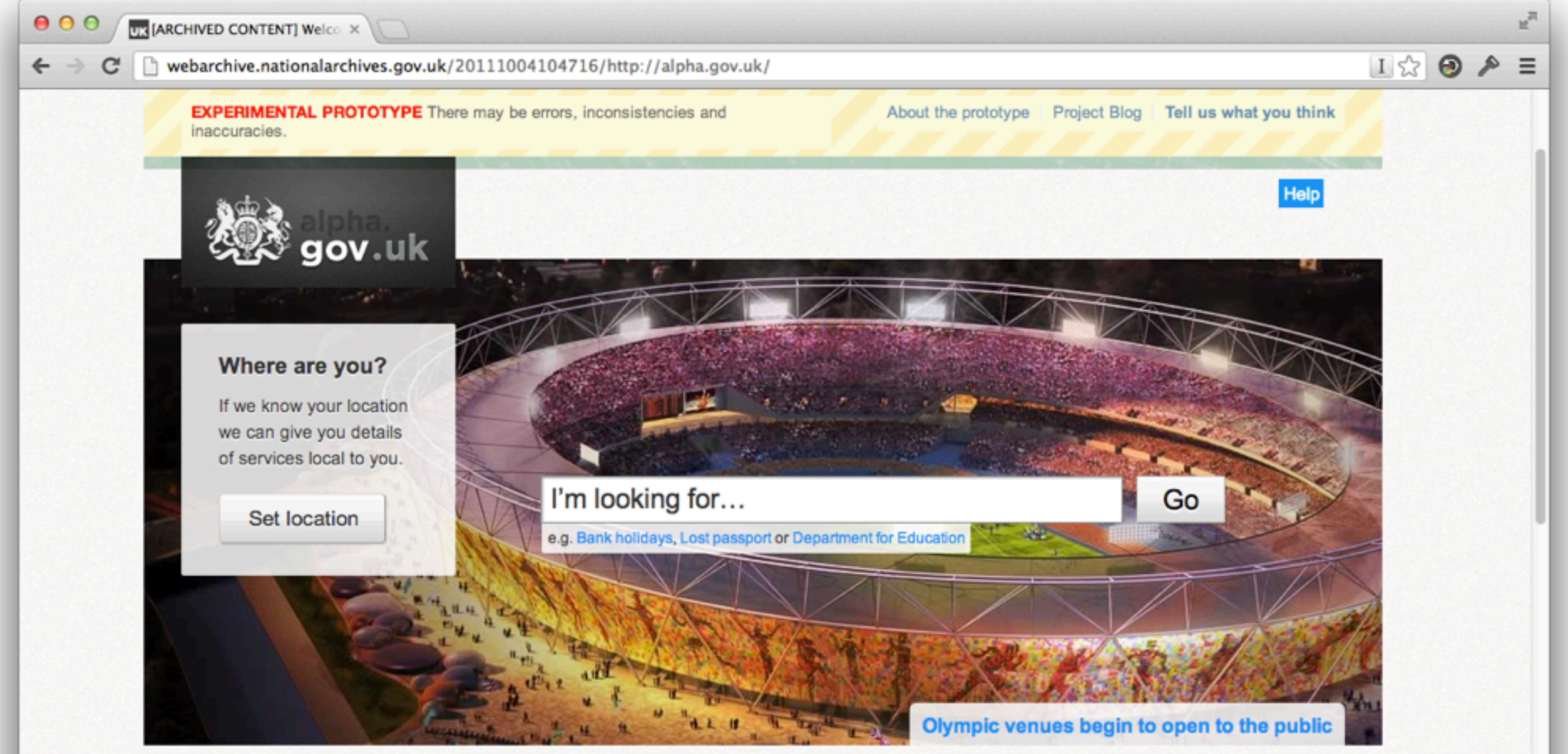
DIRECTGOV 2010 AND BEYOND: REVOLUTION NOT EVOLUTION

You asked me to oversee a strategic review of Directgov and to report to you by the end of September. I have undertaken this review in the context of my wider remit as UK Digital Champion which includes offering advice on "how efficiencies can best be realised through the online delivery of public services." This means that I have not reviewed Directgov in isolation but as part of how the government can use the Internet both to communicate and interact better with citizens and to deliver significant efficiency savings from channel shift. This letter sets out my findings and key recommendations.

Directgov as an organisation does two different things. It **provides access to**

government news, campaigns, and engagement. For me, the acid test for Directgov is whether it can **empower, and make life simpler for, citizens** and at the same time allow government to **turn other things off.** A focus on vastly increasing the range, usage and quality of online transactions will deliver the

Martha Lane-Fox Report - October 2010



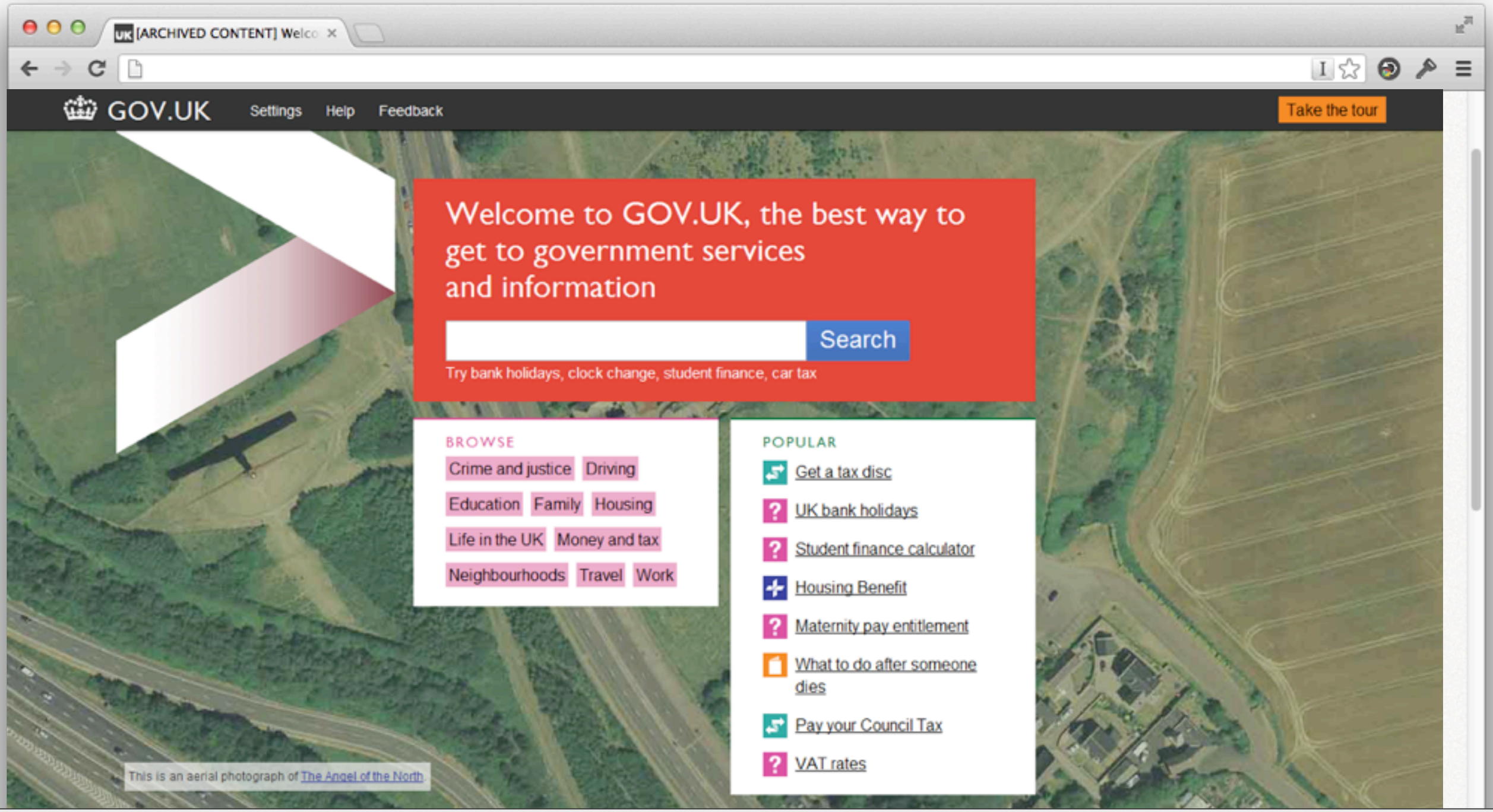
Alpha - June 2011

Me - September 2011

GDS

Government Digital Service - December 2011

gareth rushgrove | morethanseven.net



Beta - January 2012

GDS design principles

https://www.gov.uk/designprinciples

GOV.UK

Search

ALPHA Last updated 2 July 2012

Government Digital Service

Design Principles

Listed below are our design principles and examples of how we've used them so far. These build on, and add to, our original 7 digital principles.

1. **Start with needs***
2. **Do less**
3. **Design with data**
4. **Do the hard work to make it simple**
5. **Iterate. Then iterate again.**

10. **Make things open: it makes things better**

Design Principles - April 2012

digital.cabinetoffice.gov.uk/2012/09/25/why-iaas/

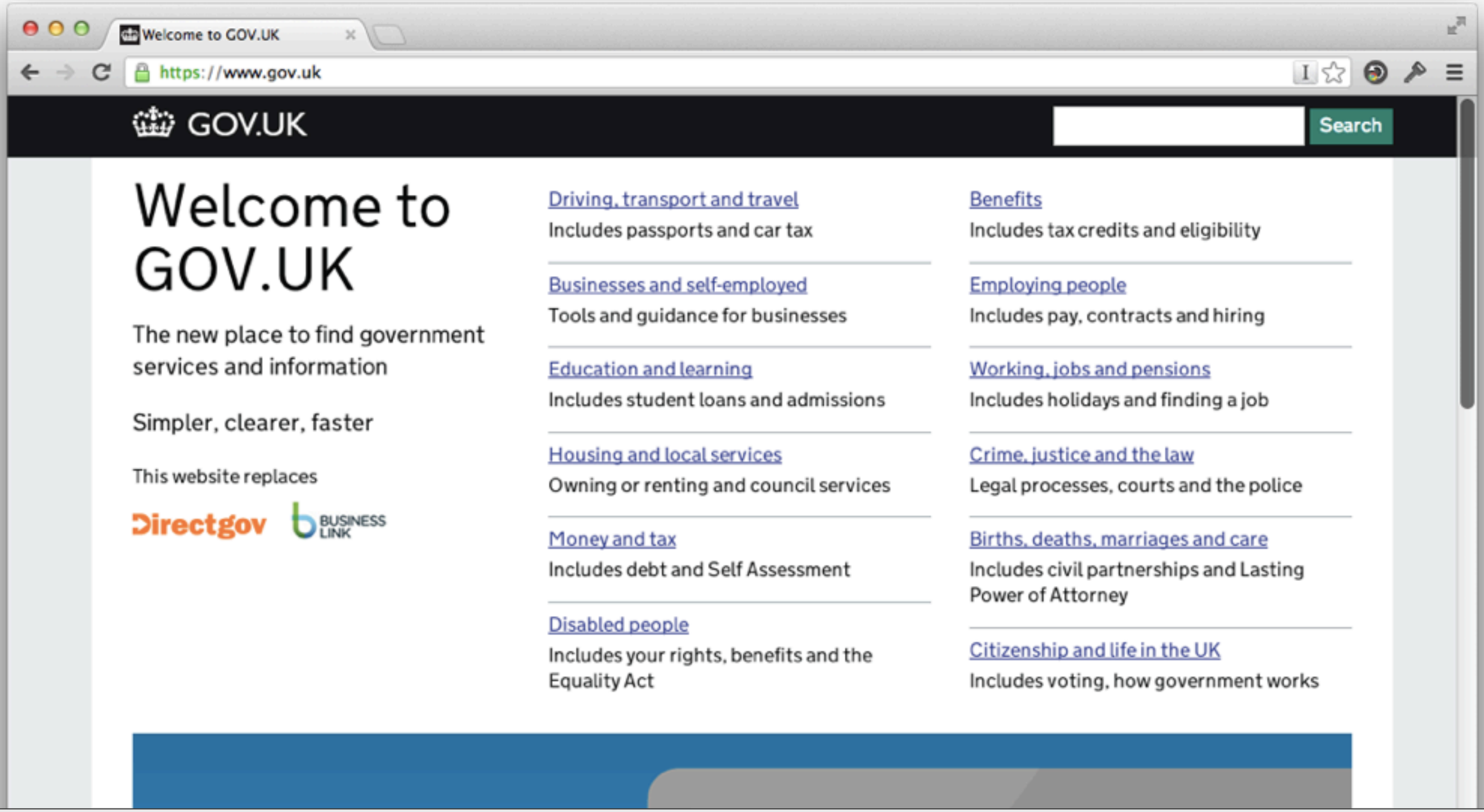
Why Infrastructure as a Service?

gcloud.civilservice.gov.uk

G-Cloud Procurement Framework

EC2 to VMWare

http://www.flickr.com/photos/uk_parliament/2701203048/



GOV.UK - October 2012

Government Digital Strategy

publications.cabinetoffice.gov.uk/digital/

Cabinet Office Government Digital Strategy Cookies

Digital services so good that people prefer to use them

publications.cabinetoffice.gov.uk/digital/

The Government Digital Strategy sets out how government will redesign its digital services to make them so straightforward and convenient that all those who can use them prefer to do so. This strategy:

- follows the March 2012 Budget commitment to digital services being the default

With a foreword by

- is supported by a cross-government approach to assisted digital provision

The strategy also describes how delivering services digitally will result in savings of £1.7 to £1.8

Government Digital Strategy - November 2012

Inside Government – GOV.UK

https://www.gov.uk/government

GOV.UK

Search

GOV.UK uses cookies to make the site simpler. Find out more about cookies

Inside Government | How government works | Departments | Topics | Content by type

13 of 24 ministerial departments have moved their corporate websites to GOV.UK.

Inside Government

By 2014, websites of all government departments and many other public bodies will be merged into the Inside Government section of www.gov.uk. Some have already moved, and more will be joining soon.

13 of 24 Departments - So far

13 of 24

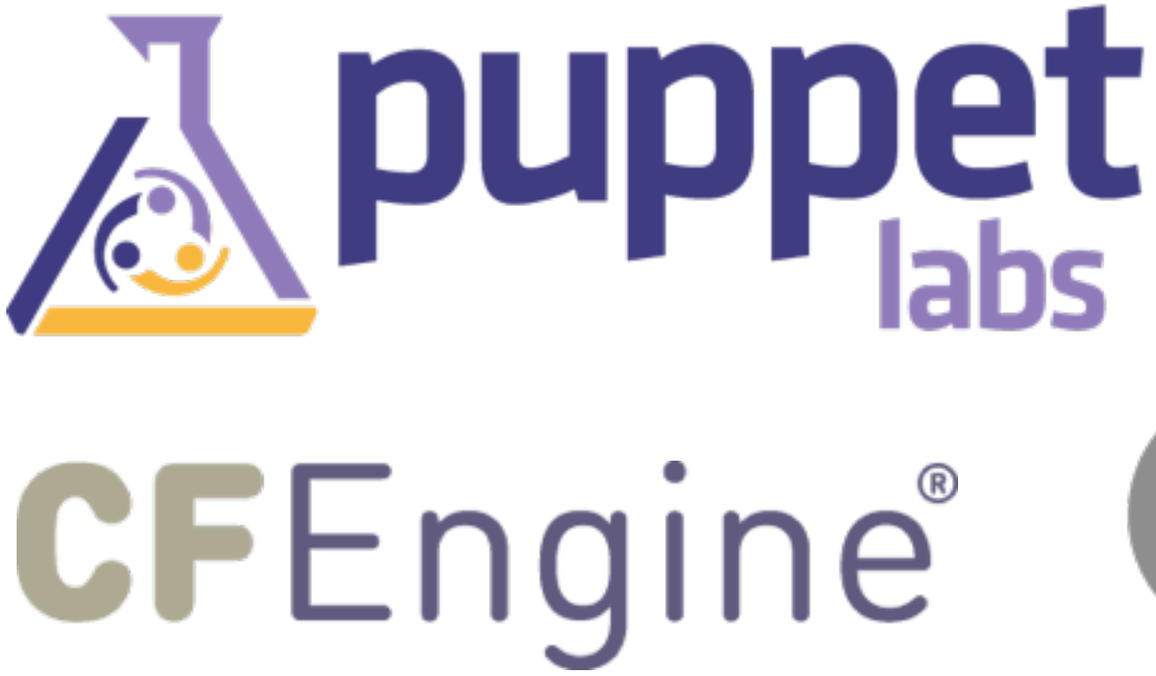
16 of 300+

Solutions?

What can we do

Solution 1

Infrastructure as code



Configuration Management

gareth rushgrove | morethanseven.net

Chef

Chef opscode.com

gareth rushgrove | morethanseven.net

```
cookbook_file "#{home_dir}/.ssh/authorized_keys" do
  source "authorized_keys"
  mode "0600"
  owner username
  group username
end

group "sysadmin" do
  members ["garethr"]
end
```

Chef code example

CFEngine cfengine.com

gareth rushgrove | morethanseven.net

```
bundle agent test
{
 packages:
  redhat::
   "wget"
     package_policy => "addupdate",
     package_method => yum,
     package_select => ">=",
     package_version => "1.11.4-2.el5_4.1",
     package_architectures => { "x86_64" };
}
```

CFEngine code example

Puppet puppetlabs.com

gareth rushgrove | morethanseven.net

```
package { 'apache2':
  ensure   => latest,
}

service { 'apache2':
  ensure   => running,
  provider => upstart,
  require  => Package['apache2']
}
```

Resources

```
class govuk::apps::calendars( $port = 3011 ) {
  govuk::app { 'calendars':
    app_type           => 'rack',
    port               => $port,
    health_check_path => ‘/bank-holidays’,
  }
}
```

Applications

```
class govuk::node::s_frontend inherits govuk::n
  include govuk::node::s_ruby_app_server

  include govuk::apps::businesssupportfinder
  include govuk::apps::calendars
  include govuk::apps::canary_frontend
  include govuk::apps::datainsight_frontend
  include govuk::apps::designprinciples
  include govuk::apps::feedback
  include govuk::apps::frontend
  include govuk::apps::smartanswers
  include govuk::apps::static
  include govuk::apps::tariff
```

Node types

```
class govuk::node::s_frontend inherits govuk::
  include govuk::node::s_ruby_app_server

  include govuk::apps::businesssupportfinder
  include govuk::apps::calendars
  include govuk::apps::canary_frontend
  include govuk::apps::datainsight_frontend
  include govuk::apps::designprinciples
  include govuk::apps::feedback
  include govuk::apps::frontend
  include govuk::apps::smartanswers
  include govuk::apps::static
  include govuk::apps::tariff
```

Include software on nodes

```
class govuk::node::s_frontend inherits govuk::
  include govuk::node::s_ruby_app_server

  include govuk::apps::businesssupportfinder
  include govuk::apps::calendars
  include govuk::apps::canary_frontend
  include govuk::apps::datainsight_frontend
  include govuk::apps::designprinciples
  include govuk::apps::feedback
  include govuk::apps::frontend
  include govuk::apps::smartanswers
  include govuk::apps::static
  include govuk::apps::tariff
```

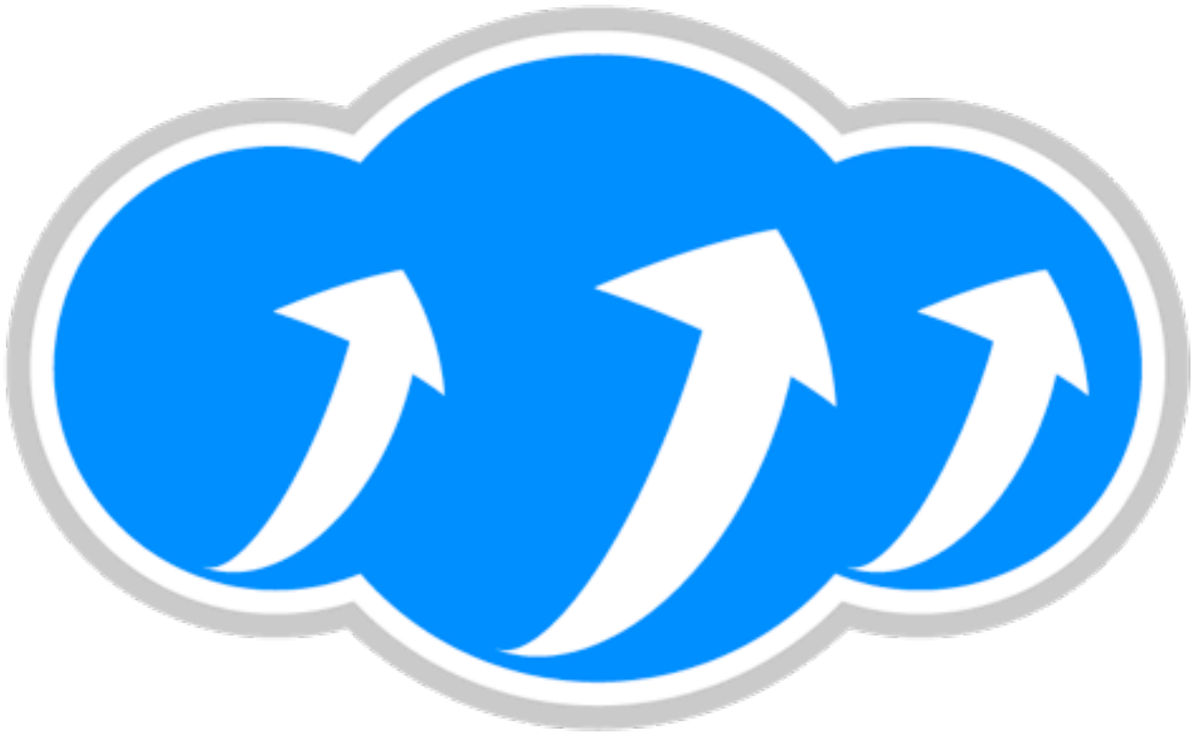
Include out applications on nodes

speakerdeck.com/garethr

More on Infrastructure as Code

Solution 2

API abstractions



libcloud

libcloud

gareth rushgrove | morethanseven.net

```
from libcloud.compute.types import Provider
from libcloud.compute.providers import get_driver

OpenStack = get_driver(Provider.OPENSTACK)

driver = OpenStack('username', 'password',
    ex_force_auth_url='https://nova-api.trystack.org:5
    ex_force_auth_version='2.0_password')

nodes = driver.list_nodes()

images = driver.list_images()
```

libcloud OpenStack example

```
from libcloud.compute.types import Provider
from libcloud.compute.providers import get_driver

vcloud = get_driver(Provider.VCLOUD)

driver = vcloud('username', 'password',
    host='vcloud.local', api_version='1.5')

nodes = driver.list_nodes()

images = driver.list_images()
```

libcloud VCloud example

```
images = driver.list_images()
sizes = driver.list_sizes()
size = [s for s in sizes if s.ram == 512][0]
image = [i for i in images if i.name == 'natty-amd64'][0]

node = driver.create_node(name='test node',
    image=image, size=size)
```

But abstractions leak

```
images = driver.list_images()
sizes = driver.list_sizes()
size = [s for s in sizes if s.ram == 512][0]
image = [i for i in images if i.name == 'natty-amd64'][0]

node = driver.create_node(name='test node',
    image=image, size=size)
```

But abstractions leak

```
vcloud = get_driver(Provider.VCLOUD)

driver = vcloud('username', 'password',
    host='vcloud.local', api_version='1.5')

node = driver.create_node(name='test node 4',
    image=image,
    ex_vm_network='your vm net name',
    ex_network='your org net name',
    ex_vm_fence='bridged',
    ex_vm_ipmode='DHCP')
```

But abstractions leak take two

```
vcloud = get_driver(Provider.VCLOUD)

driver = vcloud('username', 'password',
    host='vcloud.local', api_version='1.5')

node = driver.create_node(name='test node 4',
    image=image,
    ex_vm_network='your vm net name',
    ex_network='your org net name',
    ex_vm_fence='bridged',
    ex_vm_ipmode='DHCP')
```

More capabilities, more leaks

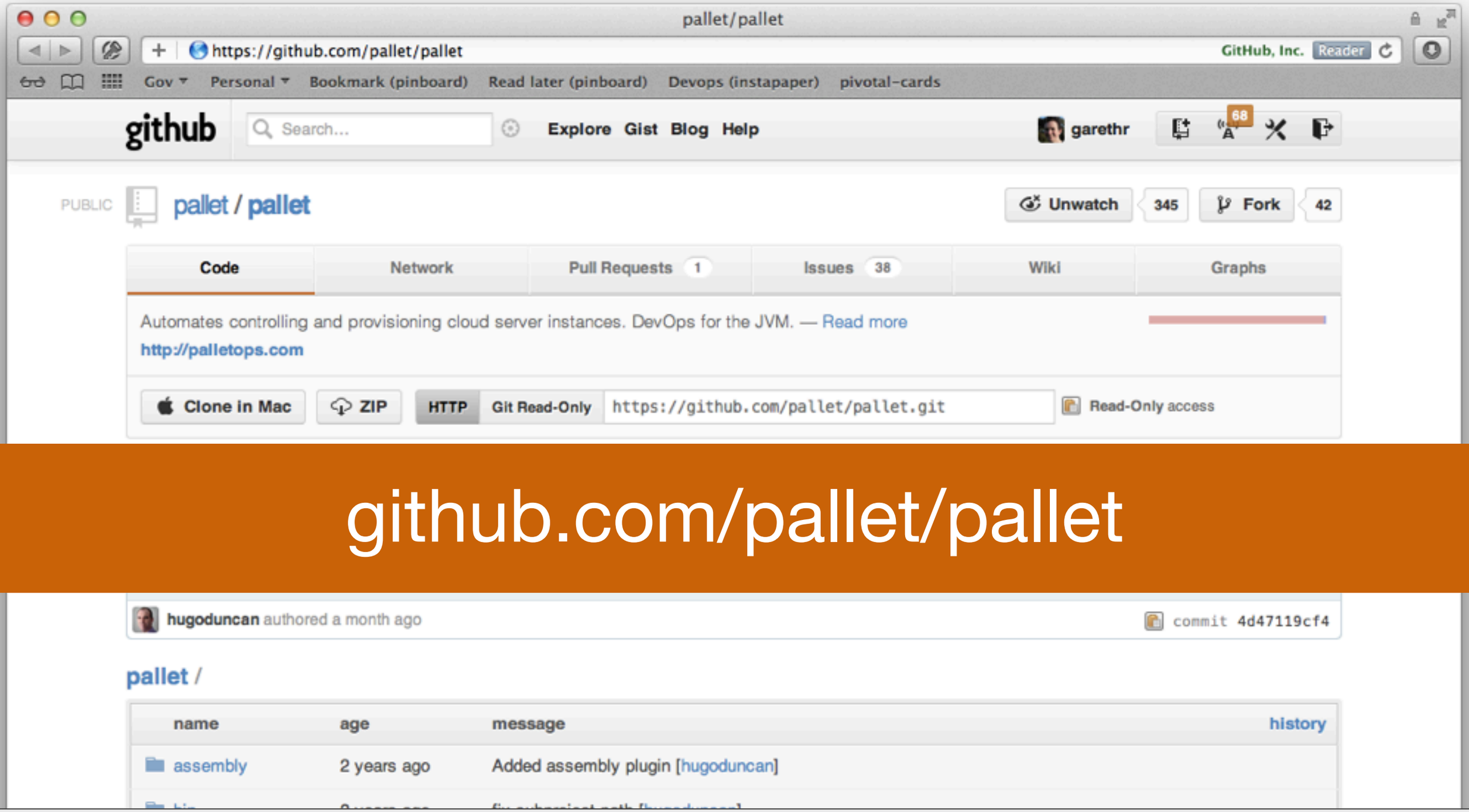
Fog

jclouds

gareth rushgrove | morethanseven.net

Solution 3

Config managent plus APIs



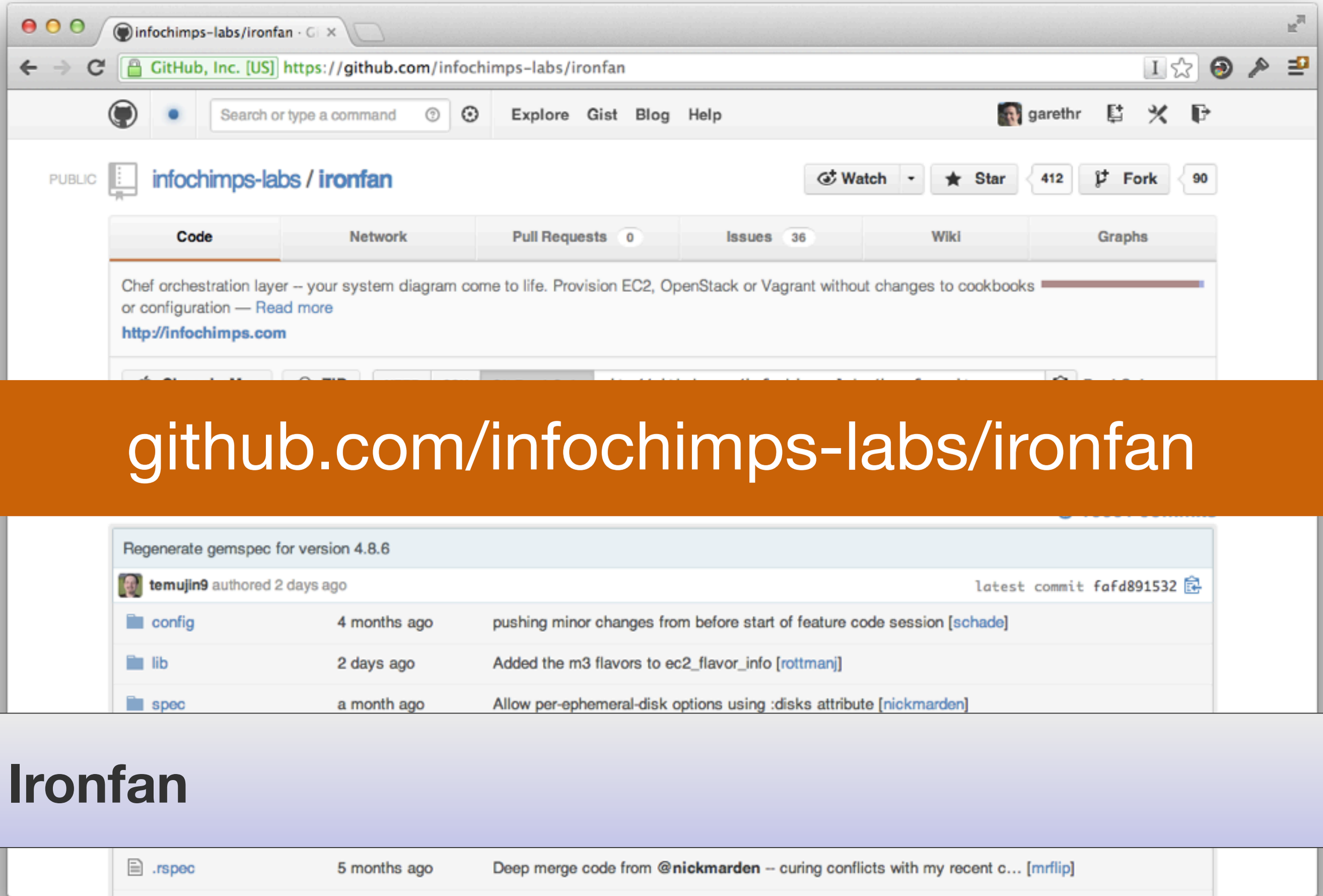
github.com/pallet/pallet

Pallet

```
(use 'pallet.crate.java)
(defnode webserver
  {}
  :configure (phase (java :openjdk)))

(converge {webserver 10} :compute service)
```

Pallet code example



github.com/infochimps-labs/ironfan

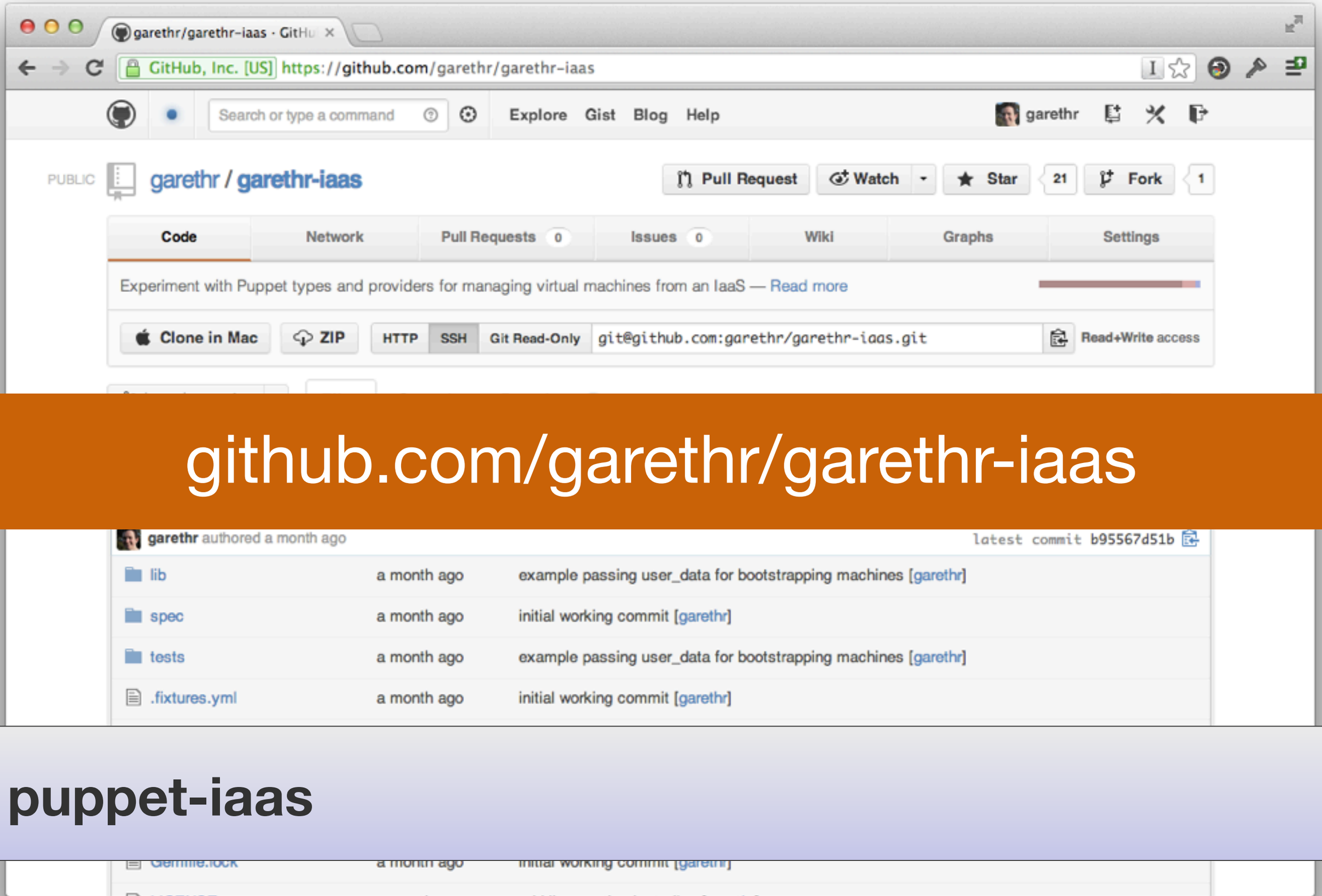
Ironfan

```
Ironfan.cluster 'web_demo' do
  cloud(:ec2) do
    flavor 't1.micro'
  end

  role :base_role

  facet :dbnode do
    instances 2
    role      :mysql_server
  end
end
```

Ironfan example



github.com/garethr/garethr-iaas

puppet-iaas

```
server { 'web-server':
  ensure   => present,
  count    => 5,
  provider => brightbox,
  image    => 'img-q6gc8', # ubuntu 12.04
}
```

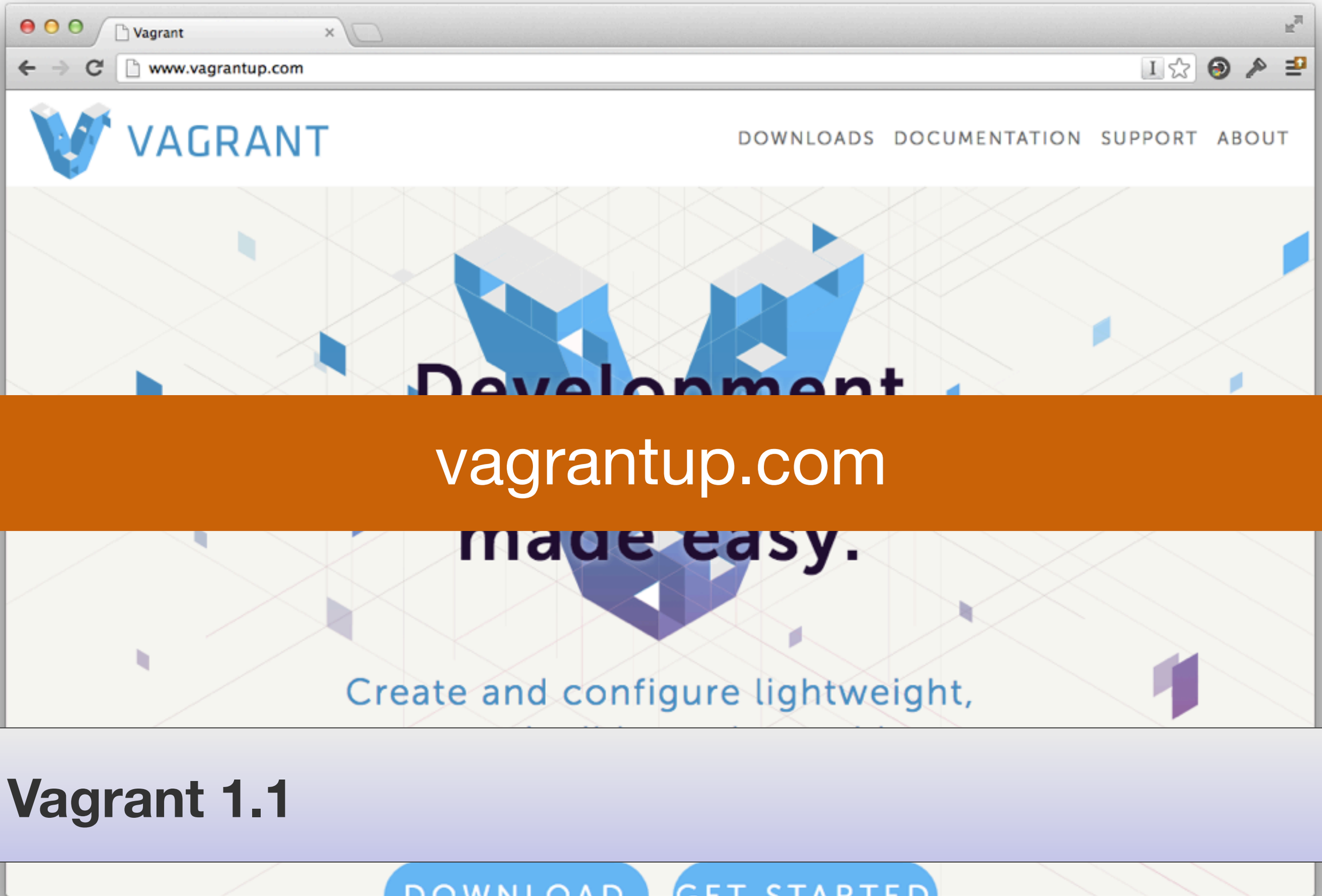
Cloud instances as resources

```
server { 'web-server':
  ensure   => present,
  count    => 5,
  provider => rackspace,
  image    => 'img-q6gc8', # ubuntu 12.04
}
```

Switch the provider

```
server { 'web-server':
  ensure   => present,
  count    => 5,
  provider => rackspace,
  image    => '5cebb13a-f783-4f8c-8058 c4182c7
  flavor   => 2, # 512 MB
}
```

Leaky interface



vagrantup.com

Vagrant 1.1

```
Vagrant::Config.run do |config|
  config.vm.box = "precise64"

  config.vm.forward_port 5555, 5555
  config.vm.forward_port 5556, 5556
  config.vm.forward_port 4567, 4567

  config.vm.provision :puppet do |puppet|
    puppet.manifests_path = "manifests"
    puppet.module_path    = "modules"
    puppet.manifest_file  = "site.pp"
  end
end
```

Define our instance

```
Vagrant.configure("2") do |config|
  config.vm.box = "precise64"

  config.vm.provider :vmware_fusion do |v|
    v.vmx["memsize"] = "1024"
  end

  config.vm.provider :aws do |aws|
    aws.instance_type = "m1.small"
  end
end
```

Configure different providers

```
$ vagrant up --provider=virtualbox
```

Choose your own provider

```
$ vagrant up --provider=ec2
```

Switch your provider

Solution 4

Software defined networks

```
require 'rubygems'
require 'nat'

nat do
  snat :interface => "Client Data",
       :original => { :ip => "10.0.0.0/xx" },
       :translated => { :ip => "xx.xx.xx.xx" },
       :desc => "Outbound internet traffic"
  dnat :interface => "Client Data",
       :original => { :ip => "xx.xx.xx.xx", :port => 22 },
       :translated => { :ip => "10.0.0.xx", :port => 22 },
       :desc => "jumpbox-1 SSH"
  dnat :interface => "Client Data",
       :original => { :ip => "xx.xx.xx.xx", :port => 80 },,
       :translated => { :ip => "10.0.0.xx", :port => 80 },
       :desc => "jenkins, logging, monitoring HTTP"
```

Ruby DSL

```
require 'rubygems'
require 'firewall'

firewall do
  # internal rules
  rule "ssh access to jumpbox1" do
     source      :ip => "Any"
     destination :ip => "xx.xx.xx.xx", :port => 22
  end

  rule "http to backend applications" do
     source      :ip => "Any"
     destination :ip => "xx.xx.xx.xx", :port => 80
  end

  rule "https to backend applications" do
```

Including Firewall and Loadbalancer

Conclusions

if all you remember is

Solve the problem for the complex case

http://www.flickr.com/photos/kevharb/5314268567

Focus on capabilities over APIs

http://www.flickr.com/photos/sprengben/5136170057

The End

Thanks for the photos

Questions?

http://flickr.com/photos/psd/102332391/

4172

QCon session code

gareth rushgrove | morethanseven.net