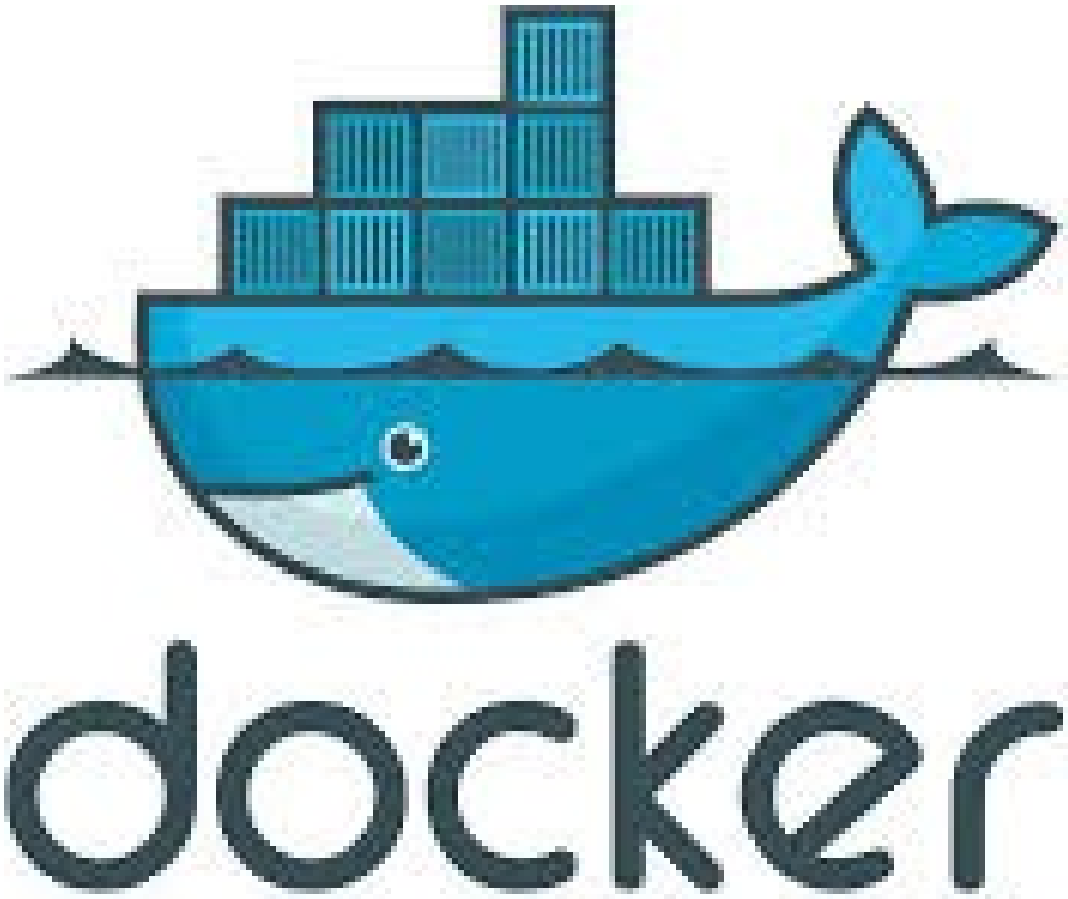
Beyond Golden Containers

Complementing Docker with Puppet

David Lutterkort
@lutterkort
lutter@puppetlabs.com

puppet
labs


docker

What's that container doing ?

```
FROM fedora:20
MAINTAINER scollier <scollier@redhat.com>

RUN  yum -y update && yum clean all
RUN  yum -y install couchdb && yum clean all

RUN  sed \
     -e 's/^bind_address = .*$/bind_address = 0.0.0.0/' \
     -i /etc/couchdb/default.ini
ADD  local.ini /etc/couchdb/local.ini

EXPOSE  5984

CMD ["/bin/sh", "-e", "/usr/bin/couchdb",
                "-a", "/etc/couchdb/default.ini",
                "-a", "/etc/couchdb/local.ini",
                "-b", "-r", "5", "-R"]
```

http://www.partialhospitalization.com/2010/08/363/

What's that machine doing ?

```
lang en_US.UTF-8
keyboard us
…
rootpw --iscrypted $1$uw6MV$m6VtUWPed4SqgoW6fKfTZ/
part / --size 1024 --fstype ext4 --ondisk sda

repo --name=fedora –mirrorlist=…
repo --name=updates –mirrorlist=…

%packages
@core
%end

%post
curl http://example.com/the-script.pl | /usr/bin/perl
```

puppet labs

http://www.gcksa.com/en/

puppet labs

msc
GL
MEDU 128486 1
2261
M. G. W.
TARE
NET
CU.CAP.
MEDITERRANEAN SHIPPING CO.
160

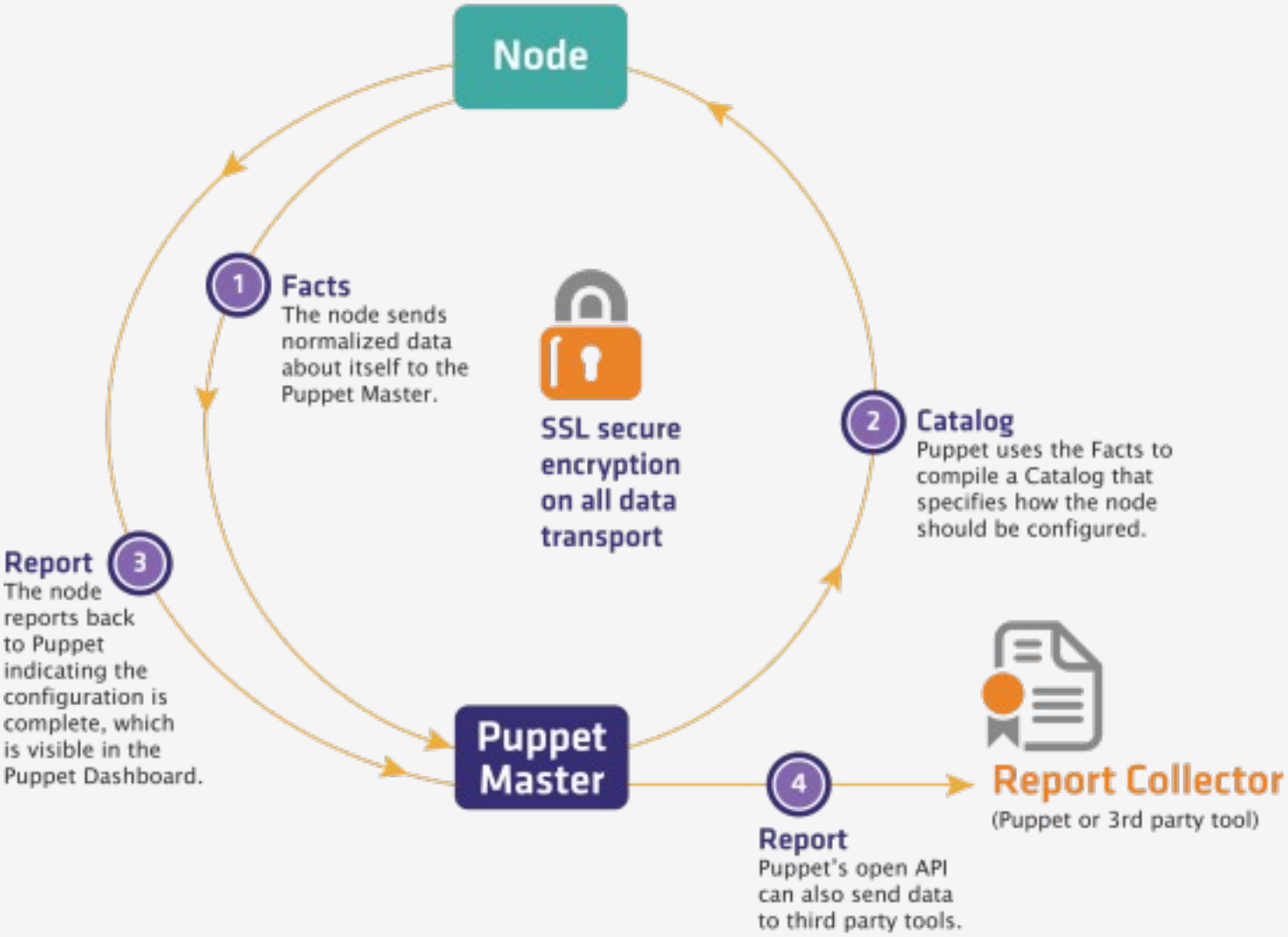
ITAL FLORIDA
TRIESTE
IMO 9308039
22.06.2007

GOTTWALD
CMA CGM
CHINA SHIPPING
GOTTWALD
GOTTWALD
GOTTWALD
GOTTWALD
tex
2008 2 21
www.cargolaw.com

Overview

- *Puppet from 10,000 feet*
- Managing the host
- Building images
  - without a master (`puppet apply`)
  - with a master (`puppet agent`)
- Runtime configuration

Dataflow in Puppet



puppet labs

A basic manifest

```
class webserver {

  package { 'httpd':
    ensure => latest
  } ->

  file { '/etc/httpd/conf.d/local.conf':
    ensure => file,
    mode   => 644,
    source => 'puppet:///modules/httpd/local.conf',
  } ->

  service { 'httpd':
    ensure      => running,
    enable      => true,
    subscribe   => File['/etc/httpd/conf.d/local.conf'],
  }
}
```

puppet labs

Override via inheritance

```
class webserver2 inherits webserver {

  File['/etc/httpd/conf.d/local.conf'] {
    source => 'puppet:///modules/httpd/other-local.conf',
  }

}
```

puppet labs

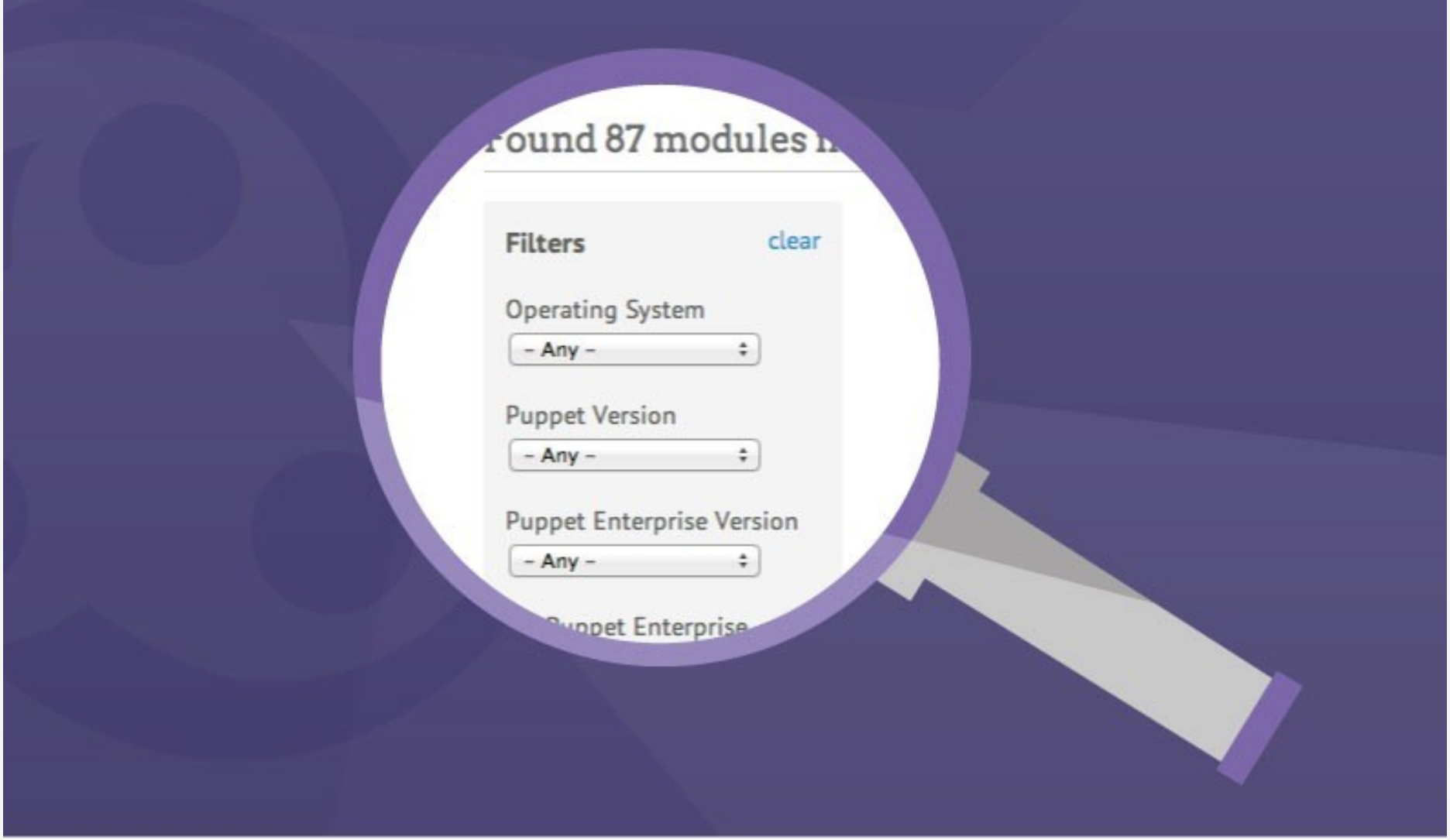
The site-wide manifest

```
node host1.example.com {
  class { 'webserver': }
}


node host2.example.com {
  class { 'webserver2': }
}


node host3.example.com {
  class {'mongodb::server':
    port    => 27018
  }
}
```

puppet labs



puppet forge

Overview

- Puppet from 10,000 feet
- *Managing the host*
- Building images
  - without a master (`puppet apply`)
  - with a master (`puppet agent`)
- Runtime configuration

Managing the host

Gareth Rushgrove's module:

https://forge.puppetlabs.com/garethr/docker

- Install docker
- Manage images
- Run containers
- Version 2.0.0 just released

Setting up Docker

```
class { 'docker':
  tcp_bind    => 'tcp://127.0.0.1:4243',
  socket_bind => 'unix:///var/run/docker.sock',
}
```

puppet labs

Pulling down images

```
docker::image { 'ubuntu':
  image_tag => 'precise'
}
```

puppet labs

Running containers

```
docker::run { 'appserver2':
  image            => 'fedora:20',
  command          => '/usr/sbin/init',
  ports            => ['80', '443'],
  links            => ['mysql:db'],
  use_name         => true,
  volumes          => ['/var/lib/couchdb', '/var/log'],
  volumes_from     => 'appserver1',
  memory_limit     => 10485760, # bytes
  username         => 'appy',
  hostname         => 'app2.example.com',
  env              => ['FOO=BAR', 'FOO2=BAR2'],
  dns              => ['8.8.8.8', '8.8.4.4']
}
```

puppet labs

Overview

- Puppet from 10,000 feet
- Managing the host
- *Building images*
  - *without a master (`puppet apply`)*
  - with a master (`puppet agent`)
- Runtime configuration

Dockerfile for puppet apply

```
FROM fedora:20
MAINTAINER James Turnbull <james@lovedthanlost.net>

ADD modules /tmp/modules
RUN yum -y install puppet; \
    puppet apply --modulepath=/tmp/modules \
      -e "class { 'nginx': service_ensure => disable }"; \
    rm -rf /tmp/modules

EXPOSE 80
CMD ["nginx"]
```

puppet labs

Dockerfile for puppet agent

```
FROM fedora:20
MAINTAINER David Lutterkort <lutter@watzmann.net>

ADD puppet /tmp/puppet-docker

RUN yum -y install puppet; \
    /tmp/puppet-docker/bin/puppet-docker
```

puppet labs

Support files

```
> tree puppet

puppet/
├── bin
│   └── puppet-docker
├── config.yaml
└── ssl
    ├── agent-cert.pem
    ├── agent-private.pem
    ├── agent-public.pem
    └── ca.pem
```

puppet labs

Configure agent run

```
> cat puppet/config.yaml

---
certname: docker.example.com
server: puppet-master.example.com
facts:
  container: docker
  build: true
```

puppet labs

Dockerfile for puppet agent

```
FROM fedora:20
MAINTAINER David Lutterkort <lutter@watzmann.net>

ADD puppet /tmp/puppet-docker

RUN yum -y install puppet; \
    /tmp/puppet-docker/bin/puppet-docker
```

puppet labs

Overview

- Puppet from 10,000 feet
- Managing the host
- Building images
  - without a master (`puppet apply`)
  - with a master (`puppet agent`)
- *Runtime configuration*

Runtime configuration

- Oneshot at container launch
- Install an init system (systemd)
  - run cron or puppetd
  - run target service(s)
- Possibly move to one agent per host

Summary

- Manage container hosts with

  https://forge.puppetlabs.com/garethr/docker

- Sample materials for `puppet agent` etc. at

  https://github.com/lutter/puppet-docker

Questions ?