

The seal of the University of Murcia is a circular emblem. It features a central figure, likely a saint or a personification of knowledge, holding a book and a staff. The figure is surrounded by three pointed arches. The outer ring of the seal contains the Latin text "UNIVERSITAS • STUDIORVM • MVRCIA" at the top and "ANNO • MCCLXXII" at the bottom.

Gestión de la configuración con puppet

Angel L. Mateo - amateo@um.es

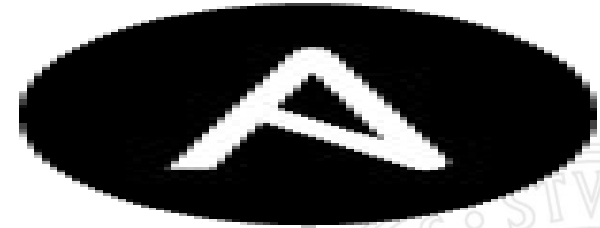
UNIVERSIDAD DE
MURCIA

Configuration Management

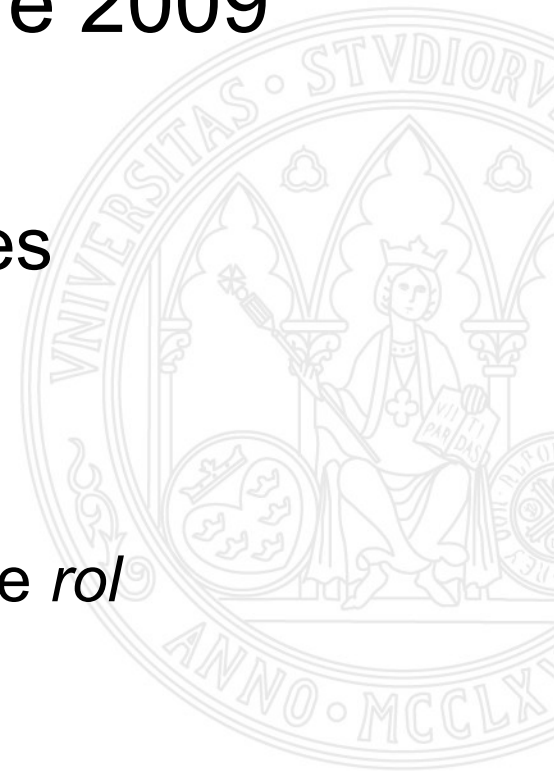


Configuration management (CM) is a systems engineering process for establishing and maintaining **consistency** of a product's performance, **functional** and physical attributes with its requirements, design and operational information **throughout its life**

Software de CM



- Cfengine 2: desde octubre 2005
- Puppet: 0.25.4 desde noviembre 2009
 - \approx 130 servidores
 - \approx 98 módulos de componentes
 - \approx 40 módulos de *rol*
 - \approx 32000 líneas de código
 - \approx 14000 líneas de código de *rol*



Puppet: Características

- Software libre (licencia apache 2.0)
- Programado en ruby
- Multiplataforma
- Fácil de extender
- Gran comunidad detrás
 - <https://forge.puppetlabs.com/>
- Arquitectura cliente/servidor



- Elementos de configuración
 - file

```
file { $config:  
  ensure => file,  
  owner  => 0,  
  group  => 0,  
  mode   => '0644',  
  content => template($config_template),  
}
```



- Elementos de configuración
 - package

```
package { 'ntp':  
  ensure => $package_ensure,  
  name   => $package_name,  
}
```



- Elementos de configuración
 - service

```
service { 'ntp':  
  ensure      => $service_ensure,  
  enable      => $service_enable,  
  name        => $service_name,  
  hasstatus   => true,  
  hasrestart  => true,  
}
```



- Elementos de configuración
 - user

```
user { 'www-data':  
  ensure => present,  
  gid    => $group,  
  require => Package['httpd'],  
}
```



- Elementos de configuración
 - cron
 - group
 - sshkey
 - exec
 - ...



Puppet: facter

- Recoge información básica sobre el nodo:
 - Hostname, direcciones IP, información sobre el hardware..
- Extensible

```
~$ facter operatingsystem
Ubuntu
~$ facter lsbdistcodename
precise
```

```
~$ facter processors
{"count"=>4, "models"=>["Intel (R)
Xeon(R) CPU          E5640  @
2.67GHz", "Intel(R) Xeon(R) CPU
E5640  @ 2.67GHz", "Intel(R) Xeon(R)
CPU          E5640  @ 2.67GHz",
"Intel(R) Xeon(R) CPU          E5640
@ 2.67GHz"], "physicalcount"=>2}
```

```
~$ facter is_virtual
True
```

```
~$ facter virtual
vmware
```

Gestión de versiones

- git, svn
 - Mantener control sobre el código
 - Histórico de cambios
 - Trazabilidad
- No editar código directamente
- Definir flujo de trabajo
- Gestor de integraciones?



Environments

- Agrupar nodos
- Diferentes manifiestos y módulos para cada grupo
- Entornos de desarrollo y producción



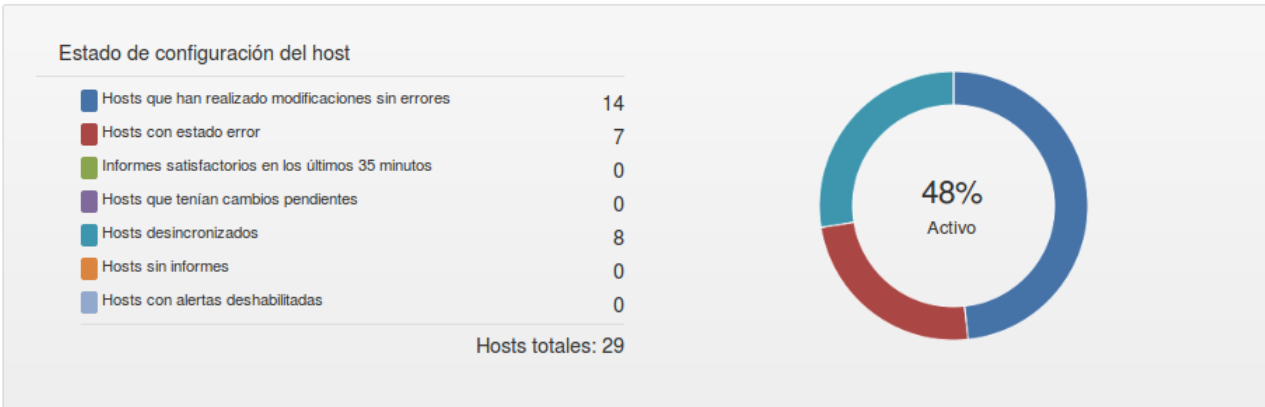
- Descubrimiento y provisión
- Gestión de configuración: puppet/chef
- Monitorización
- *Cloud ready*: VMware, OpenStack, Google Cloud Engine...
- Inventario
- ...



Visión de conjunto

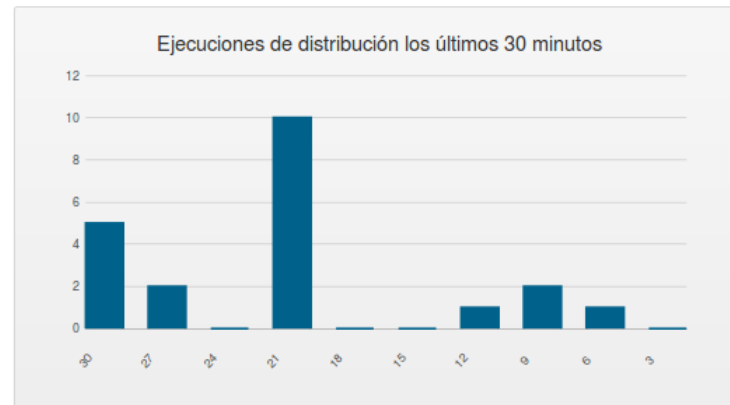
Filtro ... Buscar

Generado a las 18 Nov 08:57



Últimos Eventos

Equipo	A	R	F	RF	O	P
atlas2.um.es	4	0	2	0	0	0
pituf010.um.es	1	0	0	0	0	0
clutv02.um.es	4	0	2	0	0	0
clutv00.um.es	4	0	2	0	0	0
nyctalus21...	2	0	0	0	0	0
galemys-ubu...	2	0	0	0	0	0



plm.um.es

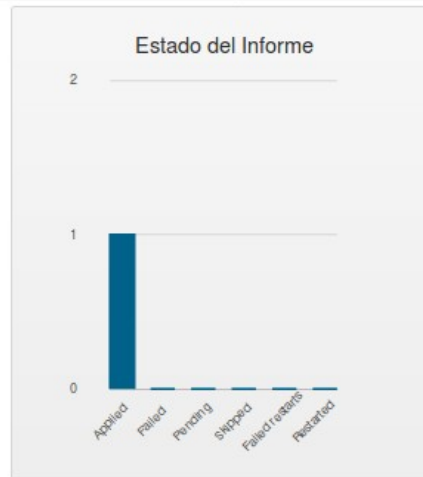
Mostrar registro de mensajes:

Todos los mensajes

Atrás **Borrar** Detalles del Equipo Otros informes de este equipo

Reportado en Tue Nov 18 08:51:31 +0100 2014

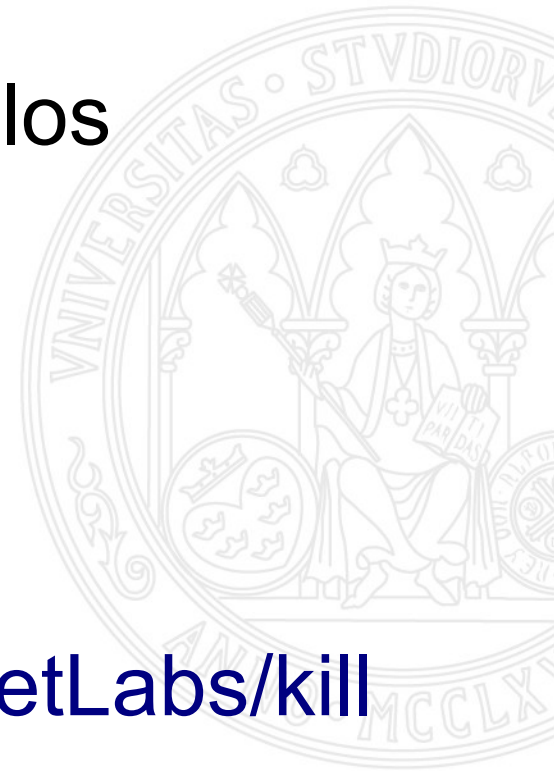
Nivel	Recurso	mensaje
notice	/Stage[main]/Mcollective::Server::Config::Factsource::Yaml/File[etc/mcollective/facts.yaml]/content	content changed '[md5]2d8013ecfb861c708c23109a3cf8b11f' to '[md5]e7a11a507f95a338aa587f73d62e5cb1'



anchor	0.0067
augeas	0.0669
concat_build	0.003
config_retrieval	23.6255
cron	0.0019
datacat_collector	0.0086
datacat_fragment	0.006
exec	0.9163
file	0.413
host	0.0027
package	0.3214
service	0.9528
ssh_authorized_key	0.0035
sshkey	0.0217
user	0.0158
Total	26.3688



- Un repositorio por cada módulo
 - Un repositorio para r10k
- Automatizar mantenimiento de los environment
 - Creación
 - Actualización
 - Borrado
- <http://www.slideshare.net/PuppetLabs/killer-r10k-39571913>



Puppetfile

```
forge "http://forge.puppetlabs.com"

mod 'puppetlabs/stdlib', '4.2.1'
mod 'theforeman/puppet'
mod 'theforeman/foreman', '2.1.3'
mod 'theforeman/git'
mod 'theforeman/concat_native'
mod 'puppetlabs/apache'

mod 'role',
  :git => 'gitolite@XXX.um.es:puppet/modules/role',
  :ref => '0.0.35'

mod 'profile',
  :git => 'gitolite@XXX.um.es:puppet/modules/profile',
  :ref => '0.0.233'
```

›Puppetfile en su propio repositorio

›Inventario de módulos

production

```
mod 'role',
  :git => 'gitolite@mus21.um.es:puppet/modules/role',
  :ref => '0.0.35'

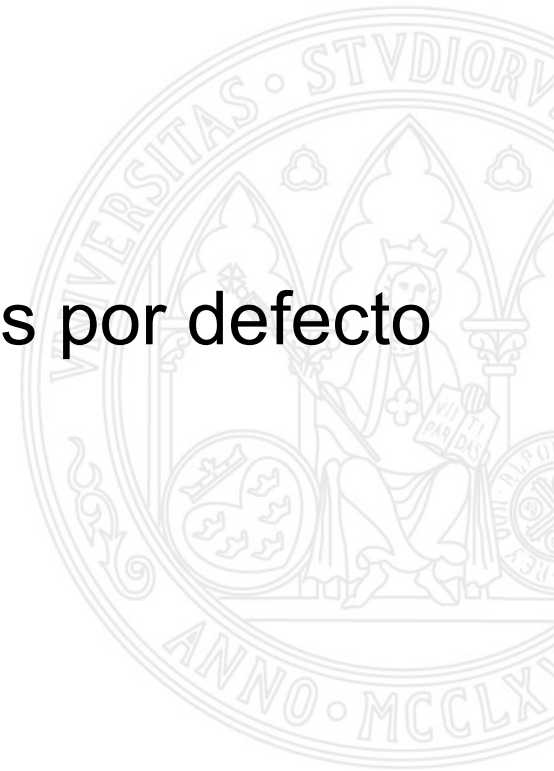
mod 'profile',
  :git =>
'gitolite@mus21.um.es:puppet/modules/profile',
  :ref => '0.0.233'
```

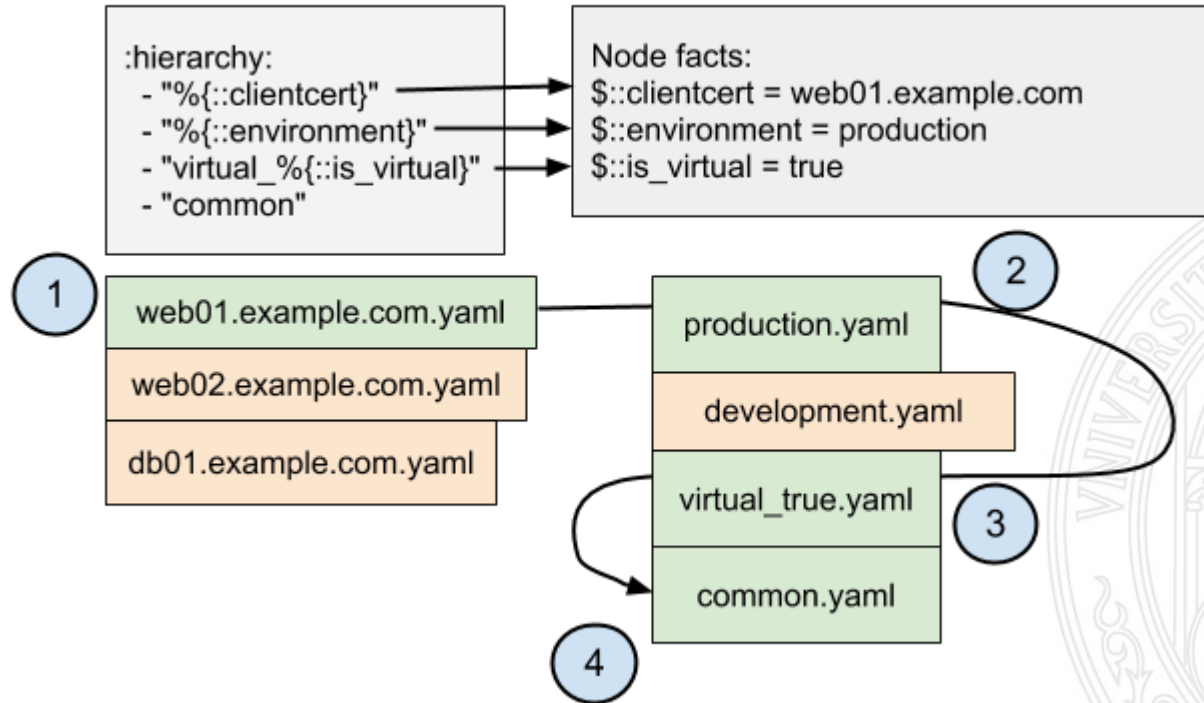
feature_tlm_846

```
mod 'role',
  :git => 'gitolite@mus21.um.es:puppet/modules/role',
  :ref => '0.0.31'

mod 'profile',
  :git =>
'gitolite@mus21.um.es:puppet/modules/profile',
  :ref => 'feature/TLM-846'
```

- Quitar información específica propia de los módulos
 - Mejorar reusabilidad
 - Compartición
 - Más fácil sobrescribir valores por defecto
 - Eliminar repeticiones
- Jerarquía configurable
 - Fuentes estáticos
 - Fuentes dinámicos





hiera.yaml

```
---  
:backends:  
  - yaml  
:hierarchy:  
  - "%{::fqdn}"  
  - "cluster_%{::hostgroup}"  
  - "%{::location}"  
  - common
```

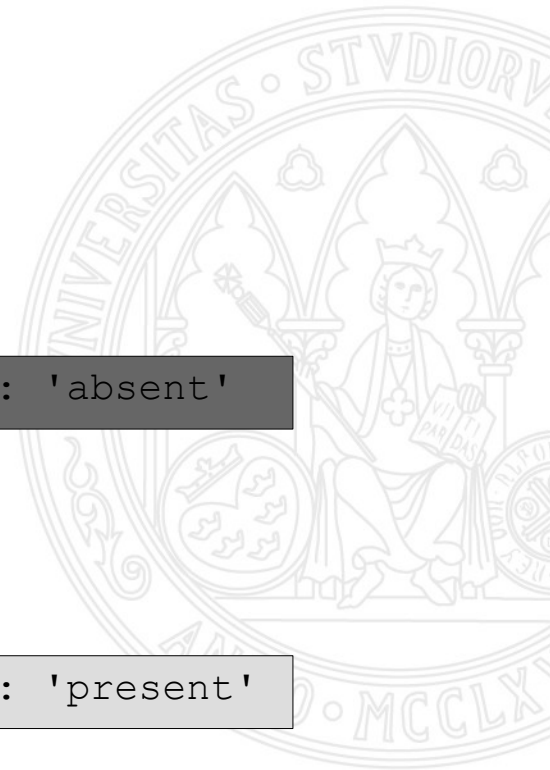
xxx10.um.es.yaml

profile::nagios::ensure: 'absent'

cluster_xxx.yaml

common.yaml

profile::nagios::ensure: 'present'



Hiera como ENC

site.pp

```
node smtp.um.es {
  include ::role::smtp_um_es
}

node www.um.es {
  include ::role::www_um_es
}
...
```

site.pp

```
node default {
  hiera_include('role')
}
```

cluster_xxx.yaml

```
---

# El role asignado
role: role::smtp_um_es
```

common.yaml

```
---

# Por defecto, un role básico
role: role::base
```

- Recoge información generada por puppet
 - Los *facts* más recientes de cada nodo
 - El último *catálogo* de cada nodo
 - Últimos informes de cada nodo
 - **Exported resources**



Puppetdb: Exported resources

node1

```
@sshkey { "${::fqdn}_dsa":  
  host_aliases => $host_aliases,  
  type         => dsa,  
  key          => $::sshdsa_key,  
}
```

1



PuppetDB

2

node2

```
Sshkey <<| |>> {  
  ensure => present,  
}
```

/etc/ssh/ssh_known_hosts

```
node1.um.es_dsa,node1.um.es,node1,1.2.  
3.4,10.14.3.23 ssh-dss AAAAB3NzaC1...
```

Puppetdb: monitorización

Type Reference

- o augeas
- o computer
- o cron
- o exec
- o file
- o filebucket
- o group
- o host
- o interface
- o k5login
- o macauthorization
- o mailalias
- o maillist
- o mcx
- o mount
- o nagios_command
- o nagios_contact
- o nagios_contactgroup
- o nagios_host
- o nagios_hostdependency
- o nagios_hostescalation
- o nagios_hostextinfo
- o nagios_hostgroup
- o nagios_service
- o nagios_servicedependency
- o nagios_serviceescalation
- o nagios_serviceextinfo
- o nagios_servicegroup
- o nagios_timeperiod
- o notify
- o package
- o resources
- o router
- o schedule
- o scheduled_task
- o selboolean
- o selmodule
- o service
- o ssh_authorized_key
- o sshkey
- o stage
- o tidy
- o user
- o vlan
- o yumrepo
- o zfs
- o zone
- o zpool



- Problema
 - La configuración se aplica en el propio host
- Solución

```
@nagios_host { "${::hostname}":  
  ensure      =>  
  hiera('profile::nagios::ensure', 'present'),  
  host_name   => $::nagios_hostname,  
  alias       => $::hostname,  
  address     => $::ipaddress,  
  tag         => 'telematica',  
}
```

```
Nagios_host <<| tag == 'telematica' |>> {  
}
```

Monitorización: automatización Roles&Profiles



```
node smtp.um.es {  
  include ::role::smtp_um_es  
}
```


```
class role::smtp_um_es inherits role::base {  
  include ::profile::postfix  
  ...  
}
```

```
class profile::postfix {  
  include ::postfix  
  ...  
}
```



Puppetdb + Monitorización: Poniéndolo todo junto

```
class profile::postfix {
  include ::postfix
  ...
  @@nagios_service { "${::nagios_hostname}_smtp":
    ensure           => 'present',
    host_name        => $::nagios_hostname,
    service_description => 'SMTP',
    check_command    => 'check_smtp',
    use              => 'Servicio_Generico_Telematica_Grafica',
    tag              => 'omd-nagios-telematica',
  }
  ...
}
```



Puppetdb + Monitorización: Poniéndolo todo junto

The screenshot shows the Thruk web interface. On the left is a navigation sidebar with sections: General (Home, Documentation, Panorama View), Current Status (Tactical Overview, Map, Hosts, Services, Host Groups, Service Groups, Problems), and Reports (Availability, Trends, Alerts). The main content area is titled 'Service Status Details' and shows a table of service status for SMTP services. A 'Display Filters' panel is open, showing filters for Host Status Types (All), Host Properties (Any), Service Status Types (All), and Service Properties (Any). A search filter is set to 'Service = SMTP'. Below the table, there are instructions: 'Select hosts / services with leftclick to send multiple commands. Select multiple with shift + mouse.' and 'select all (hosts) - unselect all - all problems - all with downtime'. The table has columns: Host, Service, Status, Last Check, Duration, Attempt, and a final column for the service name and status.

Host ▲▼	Service ▲▼	Status ▲▼	Last Check ▲▼	Duration ▲▼	Attempt ▲▼	
t1m_xenon32	SMTP	OK	13:35:22	34d 5h 22m 20s	1/3	SMTP OK
t1m_xenon31	SMTP	OK	13:33:47	35d 2h 33m 43s	1/3	SMTP OK
t1m_xenon24	SMTP	OK	13:35:53	61d 1h 30m 19s	1/3	SMTP OK
t1m_xenon23	SMTP	OK	13:33:01	61d 1h 32m 50s	1/3	SMTP OK
t1m_xenon22	SMTP	OK	13:35:14	61d 1h 30m 20s	1/3	SMTP OK
t1m_xenon21	SMTP	OK	13:37:14	28d 6h 40m 2s	1/3	SMTP OK

- Server orchestration
- Ejecución de tareas en paralelo
- Integrada con puppet
- Arquitectura cliente-servidor

```
~$ mco find -C role::smtp_um_es  
xenon20  
xenon24  
xenon23  
xenon22  
xenon21
```



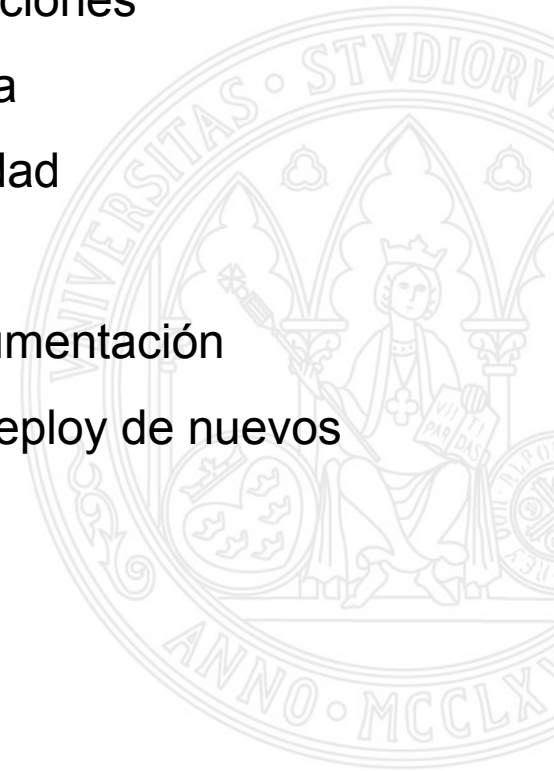
Conclusiones

- Contras

- Barrera de entrada
- Sensación de
 - ▶ pérdida de control
 - ▶ pérdida de agilidad

- Pros

- Coherencia en las configuraciones
- Confianza
- Trazabilidad
- Auditoría
- Autodocumentación
- Facilita deploy de nuevos sistemas




```
~$ mco shellcmd 'hostname' -C rol_pop_um_es_v2
=====
HOST:myotis42.um.es EXITCODE:0 STDOUT:
=====
myotis42
=====
HOST:myotis50.um.es EXITCODE:0 STDOUT:
=====
myotis50
=====
...
~$ mco service snmpd status -C role::smtp_um_es
* [ =====> ] 5 / 5

  xenon24: running
  xenon21: running
  xenon20: running
  xenon22: running
  xenon23: running

Summary of Service Status:

  running = 5

Finished processing 5 / 5 hosts in 166.99 ms
```



Conclusiones

"No longer shall we hand-configure servers! No longer shall we go without service monitoring! Now and forevermore we shall Puppetize!"

<http://nrvale0.github.io/posts/2014/10/deploy-to-noop/>



```
file { '/etc/issue':  
  content => 'Muchas gracias.  
  ¿Preguntas?',  
}
```

