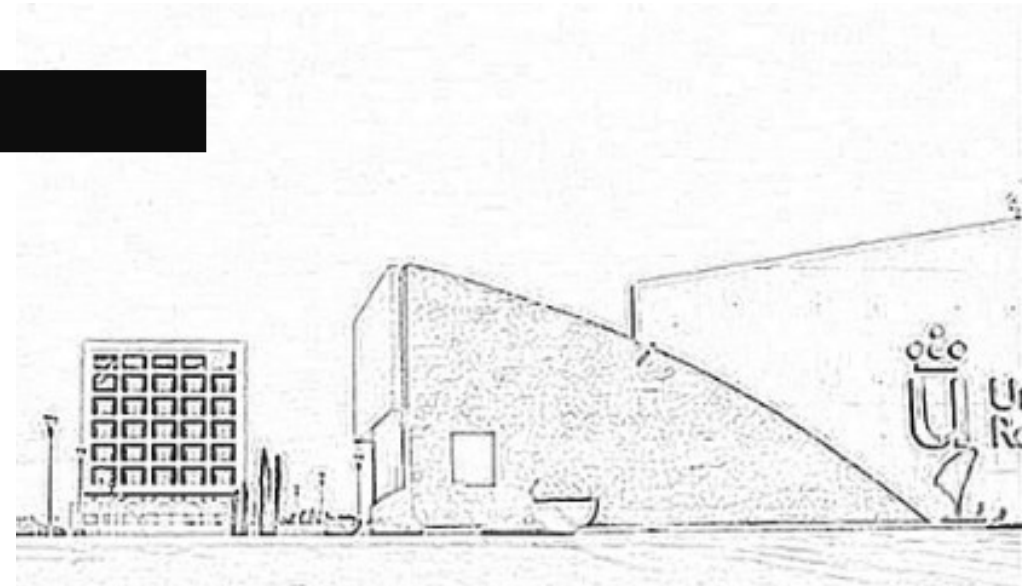


# Laboratorios Docentes GNU/Linux de la ETSIT

Cómo administrar y no morir en el intento

Antonio Gutiérrez Mayoral [antonio.gutierrez@urjc.es](mailto:antonio.gutierrez@urjc.es)

Servicio Técnicos Laboratorio ETSIT



# Resumen

- ✓ Presentación
- ✓ Historia de los Laboratorios GNU/Linux en la URJC
- ✓ Entorno actual
- ✓ Cómo administrar sin morir en el intento
- ✓ Trabajo futuro (propuestas)

# @About

- ✓ Licenciado en Ingeniería Informática por la URJC
- ✓ De 2006-2011 administré los Laboratorios Docentes de Linux (ETSII-ETSIT)
- ✓ De 2011-2013 en la empresa privada (Sociedad de valores de bolsa)
- ✓ A partir de 2015 en la URJC de nuevo.
  - ✓ Desde 2017 coordino el Servicio de Laboratorios Docentes de la ETSIT

# Historia de los Laboratorios de GNU/Linux en la URJC

- ✓ Existieron desde que yo llegué a la Universidad a estudiar (Año 2000-2001)
  - ✓ Debian 2.2 Potato con Gnome 1.0
- ✓ Administrados por profesores de manera *altruista*, hasta que fue imposible
- ✓ En 2006 comienzo a administrarlos guiado por la ayuda de Jose Centeno
- ✓ Se introducen los primeros cambios y se empieza a construir un entorno más estable
  - ✓ Cuentas de usuario basadas en LDAP
  - ✓ La distribución pasa a ser Ubuntu (que cobra fuerza en aquellos años)
  - ✓ Sistema de instalación basado en preseeds (ficheros de semilla)
- ✓ (2008) Comienza a impartirse docencia en la ESTIT, con dos Laboratorios GNU/Linux
  - ✓ Administrador itinerante

# Historia de los Laboratorios de GNU/Linux en la URJC

Laboratorios Móstoles (ETSII)



Laboratorio II, 109



Laboratorio II, 108

# Historia de los Laboratorios de GNU/Linux en la URJC

Laboratorios Fuenlabrada (ETSII)



Laboratorio II, 003



Laboratorio II, 004

# Historia

El "CPD" (Año ~2009)



Servidor de HOMES y LDAP

# Historia

## El "CPD" (Actualidad)



CPD Actual. Fuenlabrada



Servidores en RACK



- ✓ **En el Campus de Fuenlabrada**
  - ✓ 9 Laboratorios de GNU/Linux con capacidades diversas (50,56,70,20)
  - ✓ Unos 427 puestos en el Campus de Fuenlabrada
- ✓ **En el Campus de Alcorcón**
  - ✓ Dos Laboratorios de 51 puestos (102 puestos en total)
- ✓ **527 puestos en total (Sólo Laboratorios GNU/Linux)**
- ✓ Unas 1200 horas de clase al año solo en estos Laboratorios
- ✓ Unas 1200 cuentas de usuario (~800 activas)
- ✓ Unos 60 profesores imparten clase en estos Laboratorios
- ✓ Unas 75 asignaturas diferentes imparten sus prácticas en estos Laboratorios

# Entorno Actual

## Laboratorios Docentes Fuenlabrada: Infraestructura

- ✓ **Infraestructura**

- ✓ Servidores Físicos **solo si es necesario**

- Servidor de HOMES por NFS (Disco) uno por cada campus + backup

- ✓ Máquinas Virtuales con ProXmox 6.0 (Administración Web)

- ✓ **Máquinas Virtualizadas**

- ✓ **Servidor de DHCP**

- ✓ **Servidor GitLab**

- ✓ **Servidores de LDAP (Cuentas en red)**

# Entorno Actual

## Laboratorios Docentes Fuenlabrada: Infraestructura

The screenshot displays the Proxmox VE 5.0-30 interface. The left sidebar shows a tree view of the Datacenter with two main nodes: proxmox1 and proxmox2. The main panel shows a summary table of all nodes in the Datacenter, including their type, description, disk usage, memory usage, CPU usage, and uptime.

Type	Description	Disk usage...	Memory us...	CPU usage	Uptime
node	proxmox1	54.2 %	34.1 %	7.5% of 32...	4 days 18:00...
node	proxmox2	7.2 %	42.7 %	2.8% of 24...	4 days 17:59...
node	proxmox3	11.8 %	4.7 %	0.2% of 8C...	01:12:07
node	proxmox5	3.7 %	4.8 %	0.6% of 8C...	01:18:34
qemu	100 (ldap1.aulas.gsync.urjc.es)		51.3 %	4.2% of 2C...	4 days 17:54...
qemu	101 (ldap1.aulas.etsit.urjc.es)				-
qemu	102 (win7)				-
qemu	103 (labs.etsit.urjc.es)		52.7 %	15.9% of 4...	4 days 17:54...
qemu	104 (zabbix.etsit.urjc.es)				-
qemu	105 (testvm)				-
qemu	107 (puppet.aulas.etsit.urjc.es)		88.0 %	17.2% of 8...	4 days 17:54...
qemu	108 (puppet2.aulas.etsit.urjc....)				-
qemu	110 (dockerserver.aulas.gsy...)		14.4 %	2.4% of 2C...	4 days 17:54...
qemu	150 (f-l-vm01.aulas.etsit.urjc....)		82.2 %	1.1% of 4C...	4 days 17:59...
qemu	160 (scruffy.etsit.urjc.es)				-
qemu	180 (mysql.aulas.etsit.urjc.es)		22.9 %	1.2% of 4C...	4 days 17:54...
qemu	190 (dhcp1.aulas.etsit.urjc.es)		21.2 %	3.7% of 4C...	4 days 17:54...
qemu	195 (dhcp-gsync-2)				-
qemu	202 (ldap4.aulas.etsit.urjc.es)				-
qemu	125 (debian10-template)				-

# Entorno Actual

## Dotación humana

- ✓ 5 personas a tiempo completo formando parte del PAS para
  - ✓ Laboratorios Docentes ETSIT (Todos los Laboratorios)
- ✓ Para los Laboratorios GNU/Linux
  - ✓ 2 personas
- ✓ Antes (2017-), solamente una persona (Yo :-)
- ✓ Ahora, 1,5 personas
- ✓ **¿Cómo se puede administrar todo este entorno con 1,5 personas?**

# Entorno Actual

Nosotros



# Los retos del día a día

- ✓ **Con esta dotación de personal es necesario**
  - ✓ Automatizar todo lo posible
  - ✓ No perder tiempo en las tareas repetitivas
  - ✓ Intentar siempre usar un control de versiones, por si alguien mete la zarpa
    - ✓ GIT, GitLab
  - ✓ Programar, programar, programar
- ✓ **2 retos que pueden hacer que perdamos los nervios:**
  - ✓ Instalación anual (o en un momento dado) de TODOS los puestos
  - ✓ Administración de la configuración del entorno

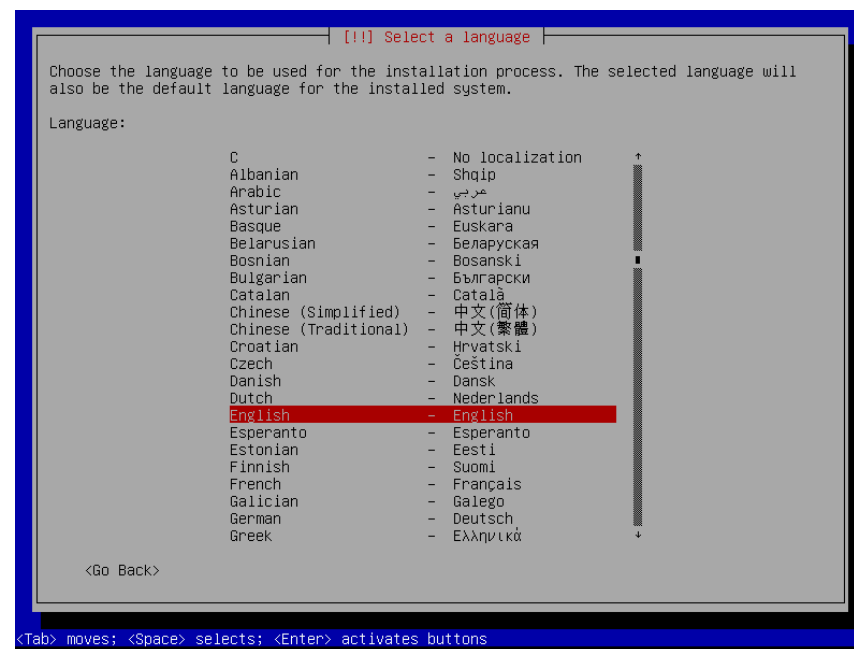
# Instalación anual

- ✓ **Necesario reinstalar 500 PCs en demanda, mínimo una vez al año.**
  - ✓ Cada PC con sus peculiaridades
    - ✓ Diferente disco, memoria, tarjetas de red, gráficas, etc.
  - ✓ Al menos lo vamos a tener que hacer una vez al año
- ✓ **Soluciones**
  - ✓ ¿Clonación? **Clonezilla**, Ghost, Acronis
  - ✓ Punto ideal: requerir la menor intervención humana.

# Instalación automática *desatentida*

Instalación mediante ficheros *preseeds*

- ✓ **Método inicialmente incluido en Debian y en distribuciones derivadas (Ubuntu).**
- ✓ Las respuestas al proceso de instalación están incluidas en un fichero de texto
- ✓ Si conseguimos prefijar todas las preguntas, el proceso no nos preguntará.
- ✓ Mucha prueba-error.
  - ✓ Pero merece la pena



```
languagechooser/language-name=English  
countrychooser/shortlist=US  
console-keymaps-at/keymap=us
```



# Instalación automática *desatentida*

## Instalación mediante ficheros *preseeds*

- ✓ La sintaxis del fichero es sencilla (excepto la sección de particionado)
- ✓ Se puede consultar un fichero base en la guía de Ubuntu/Debian:
  - <https://help.ubuntu.com/lts/installation-guide/i386/apbs04.html>
- ✓ Se debe incluir el fichero en el medio (ISO) o accesible por red
- ✓ En nuestro caso, lo “colgamos” de un servidor tftp y el propio instalador lo descarga:
  - **preseed/url**=tftp://10.110.32.21/boot/ubuntu/18.04.3/preseed/l3202/preseed-1819-configlab.cfg  
**preseed/url/checksum**=e98ae5c63dd62ef8e6366eaf75107d4b

# Instalación automática *desatentida*

## Instalación mediante ficheros *preseeds*

```
d-i debian-installer/locale string en_US
d-i console-setup/ask_detect boolean false
d-i keyboard-configuration/xkb-keymap select us
d-i netcfg/choose_interface select auto
d-i netcfg/get_hostname string unassigned-hostname
d-i netcfg/get_domain string unassigned-domain
d-i passwd/root-password-crypted password [crypt(3) hash]
d-i user-setup/encrypt-home boolean false
d-i time/zone string US/Eastern
[...]
[...]
d-i preseed/late_command string wget http://puppet.aulas.etsit.urjc.es:8080/1819/finaliza.php?
environment=configlab --output-document=/tmp/finaliza.sh; chmod 755 /tmp/finaliza.sh;
/tmp/./finaliza.sh
```

# Instalación automática *desatentida*

## Instalación mediante ficheros *preseeds*

- ✓ Con esto tendríamos un medio de instalación automático
- ✓ Falta un poco de “pegamento”
  - WakeOnLan
  - PXE
  - Configuración de BIOS
- ✓ Combinando todo esto, podemos conseguir que los Pcs hagan lo que queremos en un momento dado
  - Arranque de la primera unidad de disco
  - Instalación

# Instalación automática *desatentida*

Inicio: Vamos a Instalar

- ✓ Cambiar **BootDefault** a “Instalar”
- ✓ Enviar wake-on-lan a todos los Pcs
- ✓ Todos los Pcs arrancan y se instalan
- ✓ Bajar al Bar



# Instalación automática *desatentida*

Mientras tanto...



# Instalación automática *desatentida*

Fin: Laboratorio Instalado

- ✓ Todo el aula se ha instalado
  - ✓ Sin hacer prácticamente nada.
  - ✓ Epic win
- 
- ✓ Método escalable
  - ✓ Limitado únicamente por la red
  - ✓ Se adapta al HW
  - ✓ Instalación Limpia



¡Entorno Instalado!

¿Ahora qué?

# Administración diaria del Entorno

Comienza la Fiesta

▶ Miguel Ortuño



[Tecnicos-lab] apt install recode

- ✓ Instalar un paquete en 500 máquinas.
  - Cambiar un fichero
  - Quitar un paquete
  - Colocar un directorio
  - Cambiar el FW (iptables)
- ✓ ¿Cómo lo hacemos? ¿Aproximaciones?



# Administración diaria del Entorno

## Aplicar cambios en el entorno (I)

- ✓ **Primera aproximación:**

- ✓ `ssh -l root alpha01.aulas.etsit.urjc.es "apt-get install recode"`

```
agutierr@gsync:~$ ssh root@f-l-vm01.aulas.etsit.urjc.es
The authenticity of host 'f-l-vm01.aulas.etsit.urjc.es (212.128.254.16)' can't be established.
ECDSA key fingerprint is SHA256:ewRGMFMGaBGfVxDaHQIe99JNjn4uZUwCkRoX3VzPk+Y.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'f-l-vm01.aulas.etsit.urjc.es,212.128.254.16' (ECDSA) to the list of known hosts.
root@f-l-vm01.aulas.etsit.urjc.es's password:
```

- ✓ **¿Tengo que poner la clave de *root* 500 veces?**

# Administración diaria del Entorno

## Aplicar cambios en el entorno (II)

- ✓ **Segunda aproximación:**

- ✓ Genero una clave pública/privada y uso el fichero **authorized\_keys** en destino

```
agutierr@gsys:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/agutierr/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/agutierr/.ssh/id_rsa.
Your public key has been saved in /home/agutierr/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:h9UWuOf8+4VX5h/0EY1VL+JVavmWh+zirg05BWFzkWk agutierr@gsys
The key's randomart image is:
+----[RSA 2048]-----+
|
|  +.++  =|
|  ..=E. *o|
|  oo+ B.o|
|  o.+.= +o|
|  S .+o o+*|
|  . oo..==|
|  + ..O.=|
|  = ...+|
|  .o+ .oo|
+----[SHA256]-----+
agutierr@gsys:~$ ls -l .ssh/id_rsa.pub
-rw-r--r-- 1 agutierr agutierr 395 dic 10 11:52 .ssh/id_rsa.pub
agutierr@gsys:~$
```

- ✓ **Fichero id\_rsa.pub**

- ✓ En destino, \$HOME/authorized\_keys
- ✓ Ya puedo hacer ssh root@destino
- ✓ Sin contraseña

# Administración diaria del Entorno

## Aplicar cambios en el entorno (III)

- ✓ Por lo tanto ya puedo hacer
  - `ssh -l root destino 'apt-get install screen'`
- ✓ ¿Cómo lo hago en todas las máquinas?
  - Me apoyo en scripts de bash: `scripts ssh-a-todos`

```
#!/bin/bash
comando=$1
for lab in `echo lab1 lab2 lab3 lab4`; do
  for pc in `seq -w 01 50`; do
    ssh root@$lab$pc $comando
  done
done
```

`./sshatodos-lab1 reboot`



# Administración diaria del Entorno

## Gestión del Cambio (IV)

- ✓ Esta solución, (a pesar de que fue la que usé durante mucho tiempo) tiene muchos problemas
  - Máquinas apagadas
  - Máquinas estropeadas
  - Requiere intervención humana
  - Cambios *no trackeados*
  - En definitiva...

# ¡ LA GESTIÓN DEL CAMBIO !

# Administración diaria del Entorno

## Gestión del Cambio (I)

- ✓ La gestión del cambio (o de los cambios) es un problema crucial para un SysAdmin
- ✓ A día de hoy existen diferentes soluciones para gestionar esto
  - Puppet
  - Chef
  - Ansible

# Administración diaria del Entorno

## Gestión del Cambio (I)

- ✓ La gestión del cambio (o de los cambios) es un problema crucial para un SysAdmin
- ✓ A día de hoy existen diferentes soluciones para gestionar esto
  - Puppet
  - Chef
  - Ansible
- ✓ Todas estas soluciones persiguen el mismo problema:
  - Gestionar los cambios de manera eficiente
  - Todas las máquinas en un único estado identificable

# Administración diaria del Entorno

## Gestión del Cambio (II)

- ✓ Las más usadas: Puppet y Ansible
  - Guerra de religión: Linux vs Windows, Android vs Apple, Tortilla con cebolla/ sin cebolla.
- ✓ **Puppet**
  - **Modelo cliente-servidor**
  - Más antiguo que Ansible. Más comunidad de usuarios (puppet forge)
  - Requiere un cliente instalado en cada máquina
- ✓ Ansible
  - Más usado en entornos empresariales
  - No requiere cliente (funciona con SSH)
  - **Requiere que al volcar la configuración la máquina esté disponible (encendida)**
  - (Dicen) Más fácil de aprender



# Administración diaria del Entorno

## Puppet (I)

### ✓ **Puppet**

- Herramienta de gestión de la configuración basada en código abierto
- Permite la gestión del cambio de una manera eficiente
- El estado del Sistema/configuración se describe en unos ficheros llamados manifiestos
- Clientes solicitan la configuración cada cierto tiempo y aplican los cambios necesarios
- Sistema *idempotente*
- Lenguaje declarativo, multiplataforma
- Módulos desarrollados por la Comunidad (forja)

# Administración diaria del Entorno

## Puppet (II)

- ✓ Cada aspecto de la máquina se describe mediante un objeto.
- ✓ Existen objetos predefinidos y se pueden construir más (módulos)
  - file
  - package
  - cron
  - user
  - group
  - exec

# Administración diaria del Entorno

## Puppet (III)

► Miguel Ortuño



[Tecnicos-lab] apt install bsdgames

fichero aptget.pp :

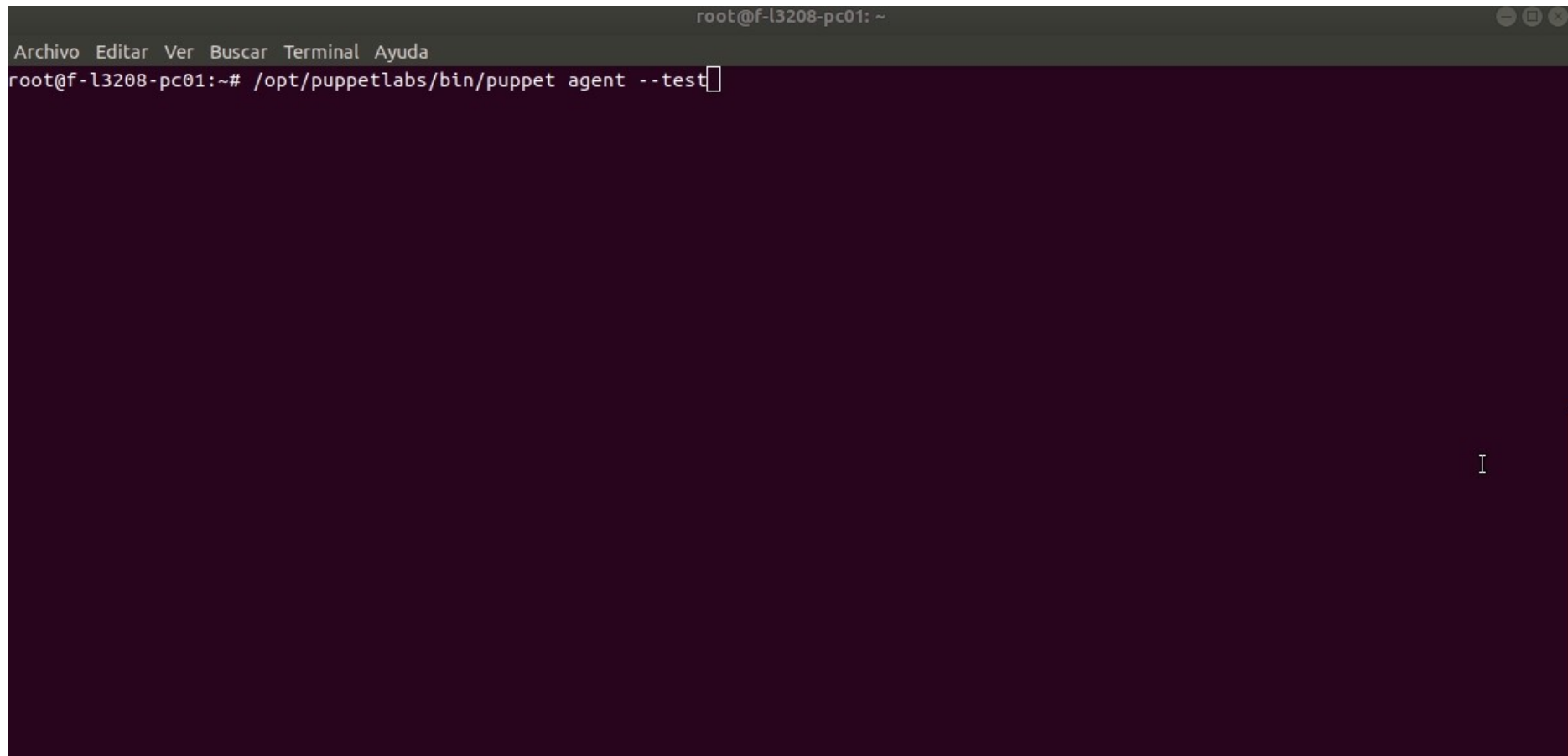
```
package {'bsdgames' =>  
  ensure => latest  
}
```

\$ git commit -m "Instalación de paquete bsdgames" aptget.pp

\$ git push

# Administración diaria del Entorno

## Puppet (IV)



```
root@f-l3208-pc01: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@f-l3208-pc01:~# /opt/puppetlabs/bin/puppet agent --test
```

# Administración diaria del Entorno

## Puppet (V)

- ✓ Ejemplo: sincronización de directorio en todas las máquinas

```
file {'/opt/ayedd/':  
  path => '/opt/ayedd/',  
  ensure => directory,  
  owner => root,  
  group => root,  
  mode => '0755',  
  source => 'puppet:///modules/software/ayedd/',  
  recurse => true,  
}
```

# Administración diaria del Entorno

## Puppet (VI)

- ✓ Ejemplo: creación de tarea programada (cron)

```
cron {  
  'apagado-automagico':  
    command => '/sbin/shutdown -h now',  
    user => 'root',  
    hour => '22',  
    minute => '10',  
    weekday => '*',  
}
```

- ✓ **La configuración del Laboratorio:**

```
agutierr@puppet:/etc/puppetlabs/code/environments/configlab/mymodules/configbase/manifests$ ls  
aptconfig.pp      crontab.pp        ldaplabs.pp       nfssystemdmounts.pp  other.pp          rsyslog.pp       sshserver.pp      usrlocalbin.pp  
aptsources.pp    gdm.pp            lightdm.pp        nntp.conf            polkit.pp         services.pp       sudo.pp  
basepackages.pp  gnomeconfig.pp    motd.pp           novnc.pp             puppetagent.pp   sshkeys.pp       udev.pp  
basicpam.pp      init.pp           networkmanager.pp nvidia.pp            rotatelog.pp     sshrootkeys.pp   unityconfig.pp  
agutierr@puppet:/etc/puppetlabs/code/environments/configlab/mymodules/configbase/manifests$
```

# Administración diaria del Entorno

## Puppet (VII)

- ✓ Ejemplo: fijar políticas de firewall (iptables)

```
firewall { '007 Aceptar tcp,udp red laboratorios 212.128.254.0/23':  
  chain => 'INPUT',  
  proto  => 'all',  
  iniface => $iface,  
  source  => '212.128.254.0/23',  
  action  => 'accept',  
  state  => ['NEW', 'RELATED', 'ESTABLISHED'],  
}  
firewall { '008 Aceptar tcp,udp red departamentos 193.147.79.0/24':  
  chain => 'INPUT',  
  proto  => 'all',  
  iniface => $iface,  
  source  => '193.147.79.0/24',  
  action  => 'accept',  
  state  => ['NEW', 'RELATED', 'ESTABLISHED'],  
}
```

# Administración diaria del Entorno

## Puppet (VIII)

### Con esta herramienta...

- La configuración está **escrita**, se puede leer
- Es *mantenible*
- Los cambios se aplican, secuencialmente uno por uno ante cualquier problema (máquina apagada, etc)
- El Técnico/Administrador solamente se preocupa de ir añadiendo los cambios en el manifiesto en el servidor
- Además de esto, ponemos por encima git para versionar los cambios (ante catástrofes)
- TODO: Implementar un ciclo CI/CD para **provocar** el cambio
  - Usando Vagrant, Docker
  - Usaría dos ramas en el mismo repositorio
    - {prod, test}
    - Probaría en test. Si la integración ha ido bien, haría un merge en prod
    - TFG!!!

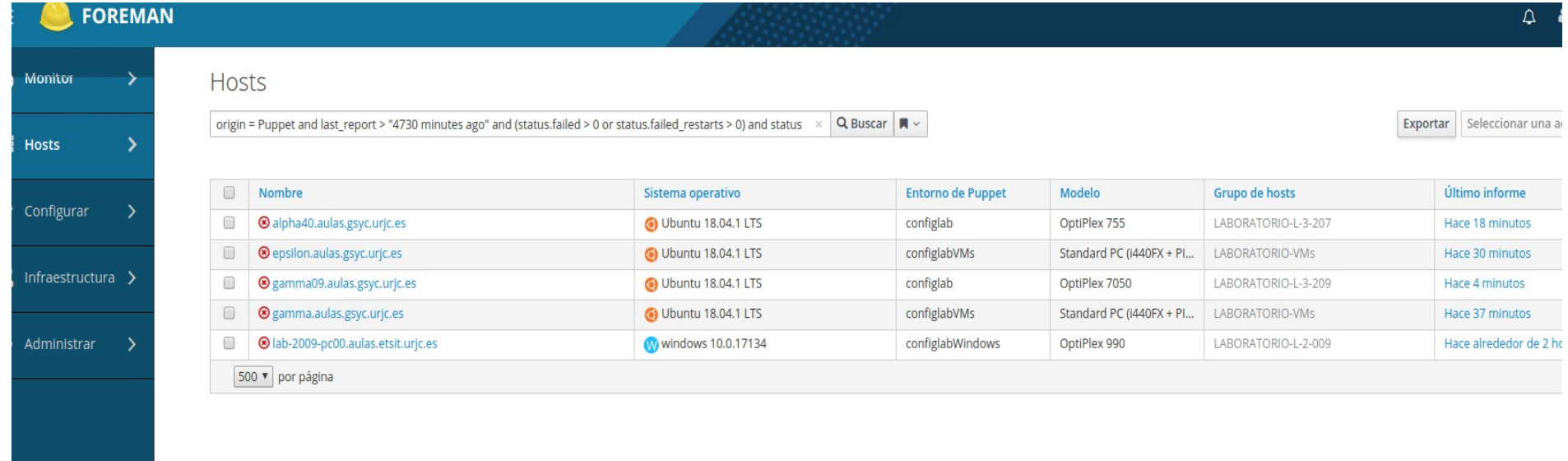


# Administración diaria del Entorno

## Puppet (IX)

### Puppet + Foreman

- Los agentes de Puppet que ejecutan en las máquinas vuelcan un informe
- Este informe es difícil de procesar/gestionar
- Mediante un panel web tenemos una visión completa del estado de todos los hosts gestionados
- Podemos gestionar alertas, ver el estado de la ejecución de los manifiestos, y más cosas



The screenshot shows the Foreman web interface. The top navigation bar includes the 'FOREMAN' logo and a search bar. The left sidebar contains navigation options: Monitor, Hosts, Configurar, Infraestructura, and Administrar. The main content area is titled 'Hosts' and displays a table of managed hosts. A search filter is applied: 'origin = Puppet and last\_report > "4730 minutes ago" and (status.failed > 0 or status.failed\_restarts > 0) and status'. The table has columns for Nombre, Sistema operativo, Entorno de Puppet, Modelo, Grupo de hosts, and Último informe. Below the table, there is a pagination control showing '500 por página'.

Nombre	Sistema operativo	Entorno de Puppet	Modelo	Grupo de hosts	Último informe
alpha40.aulas.gsync.urjc.es	Ubuntu 18.04.1 LTS	configlab	OptiPlex 755	LABORATORIO-L-3-207	Hace 18 minutos
epsilon.aulas.gsync.urjc.es	Ubuntu 18.04.1 LTS	configlabVMs	Standard PC (i440FX + PI...	LABORATORIO-VMs	Hace 30 minutos
gamma09.aulas.gsync.urjc.es	Ubuntu 18.04.1 LTS	configlab	OptiPlex 7050	LABORATORIO-L-3-209	Hace 4 minutos
gamma.aulas.gsync.urjc.es	Ubuntu 18.04.1 LTS	configlabVMs	Standard PC (i440FX + PI...	LABORATORIO-VMs	Hace 37 minutos
lab-2009-pc00.aulas.etsit.urjc.es	windows 10.0.17134	configlabWindows	OptiPlex 990	LABORATORIO-L-2-009	Hace alrededor de 2 hc

# Trabajo Futuro

## Ideas Futuras para TFGs

- ✓ **Todavía hay mucho trabajo por hacer. Algunas ideas:**
  - ✓ Interfaz web para activar/desactivar el modo examen
    - ✓ Ahora mismo este proceso requiere intervención humana
    - ✓ En la UCM tienen algo similar. El profesor puede seleccionar el modo de funcionamiento del aula (normal, sin acceso a internet, etc)
  - ✓ Integración de un proceso CI-CD en la gestión de la configuración
    - ✓ Que existan diferentes ramas test y producción
    - ✓ Cada cambio se realice mediante feature-request en test
    - ✓ Los cambios en la configuración se testeen antes de ser integrados
      - ✓ Mediante vagrant, hooks de Gitlab, etc.



**¡GRACIAS!**