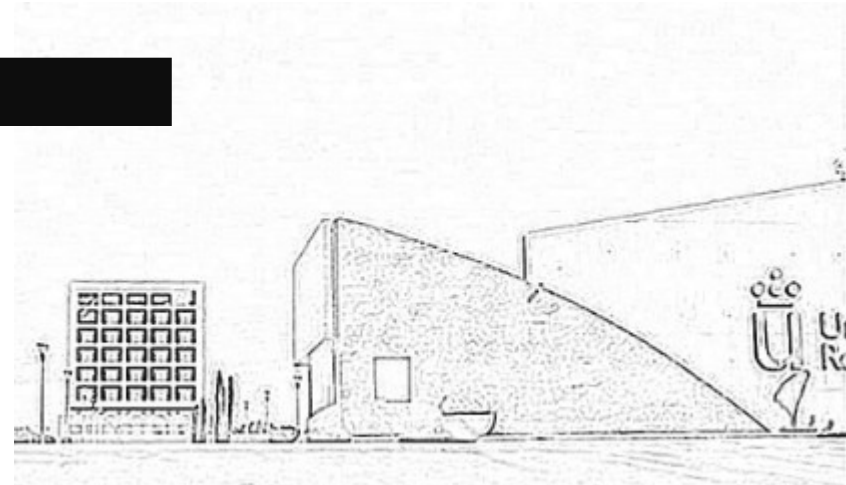


Laboratorios Docentes GNU/Linux de la ETSIT

PASADO, PRESENTE Y FUTURO

Antonio Gutiérrez Mayoral
<antonio.gutierrez@urjc.es>



Universidad
Rey Juan Carlos

Escuela Técnica Superior de Ingeniería de Telecomunicación

Resumen

- Acerca de
- Historia y evolución
- Entorno actual
- Infraestructura core
- Futuro

Acerca De

A. Gutiérrez Mayoral

Mi perfil

- Ingeniero en Informática de Sistemas (URJC) (2005)
- Ingeniero en Informática (URJC) (2010)
- 2006 – 2011 : Administrador de Sistemas, PDI, Departamento GsyC (ETSII)
- 2011 – 2015 : Administrador de Sistemas en CM Capital Markets
- 2015 - ? : Técnico Laboratorio ETSIT, URJC, PAS URJC

¿ Cómo empecé en todo esto?



Diciembre de 2006, aterrizo como puedas

- 4 Laboratorios de 40 puestos en Móstoles
- 2 Laboratorios en Fuenlabrada de 40 puestos
- En total, unos 240 equipos (más servidores)
- La infraestructura “core” se basaba en principalmente,
 - Un sistema de cuentas NIS (más antiguo que...)
 - Un servidor NFS para las cuentas de alumno
 - Un servidor NFS que replicaba el directorio /usr
 - Esto para cada Campus
- No se administraba la red
- No había modo examen
- No teníamos cuarto de servidores, ni HW especializado
- El soporte iba y venía por la M-506 cuando se necesitaba...

Historia

Laboratorios Fuenlabrada



Historia

Laboratorios Móstoles



Historia

El “CPD”



Historia

El “CPD” (Año ~2009)



Problemas cuando llegué...

- Un sistema de cuentas arcaico y poco integrable (NIS)
 - Ningún control sobre las cuentas de usuario
 - Todo el mundo “metía la mano”
- Un sistema de instalación muy antiguo y poco manejable
- Distribución Debian GNU/Linux: muy estable pero poco flexible
- Cero copias de seguridad
- Ningún control en la configuración del software ni en la distribución
- Escasa (por no decir nula) monitorización de servicios

Historia

Primera Evolución

Primeros cambios

- Pasamos de Debian a Ubuntu
- Se implementó un sistema de cuentas basado en OpenLDAP
 - El cual no estuvo exento de polémica los primeros meses :)
- Se eliminó la distribución de software a través de un NFS por /usr
- Se implementó una serie de servicios que nunca habían existido
 - Copias de seguridad basadas en rsync
 - Monitorización de los servicios a través de Nagios
 - Creación de un portal basado en PHP y HTML para dar de alta cuentas/ cambiar contraseñas
 - Etc
- El programa de instalación se modificó completamente
 - Pasamos a un sistema basado en ficheros de semilla preseed

Instalación desatendida basada en preseeds

- Situación:
 - (2006) Instalar 240 equipos en un plazo razonable de tiempo
 - (2018) Instalar 500 equipos en un plazo razonable de tiempo
- Por aquél entonces, el sistema de instalación era muy tosco y poco *mantenible*. Pero era muy rápido
- Decidimos pasar a un sistema más lento pero más *mantenible* y “legible”
- El sistema se basa en un fichero de semilla llamado preseed, que contiene todas las preguntas a la instalación, en un fichero de texto.
- Para que la automatización sea completa, el sistema se complementa con
 - Un servidor DHCP para la configuración de la red
 - Un arranque basado en 1º) tarjeta de red 2º) disco duro
 - Un menú PXE que decide que se hace en cada momento:
 - “bootar” del disco duro, o,
 - Instalar el puesto

Historia

Fichero preseed

Fuente:

<https://help.ubuntu.com/lts/installation-guide/s390x/apbs02.html>

```
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
[...]
```

Historia

Resultado



Entorno Actual Laboratorios Docentes GNU/Linux

De un vistazo...

Ahora mismo, lo que tenemos es,

- 6 aulas dedicadas puramente a Telemática, 275 equipos físicos (+virt)
- 2 aulas dedicadas principalmente a Ing. Biomedica (~ 104 equipos)
- Un aula en otro campus, dedicada a Ing. Biomédica (~ 50 equipos)
- Esto solamente, puestos de usuario puramente Linux. (Tot- ~ 410 equipos)

Además,

- Entorno de servidores para dar servicio a toda la Infraestructura
 - Unos 4 servidores físicos core y unos 15 virtuales
- Administración del CPD
- Administración de la red (Nivel alto)

Entorno Actual Laboratorios Docentes GNU/Linux

De un vistazo...

Unos números rápidos,

- 1171 cuentas de alumnos (~700 activas)
- ~ 40 cuentas de PDI (Personal Docente Investigador)
- soporte ~ 60 asignaturas alrededor del año



Entorno actual “Core”

Otros servicios

Otros servicios de “valor añadido”

- Conexión remota a puestos de Laboratorio
 - SSH
 - VNC (*tunelizado*)
 - ¡2018! VNC-web
- GitLab para Comunidad ETSIT
- ¡2018! Servicio de Bases de Datos MySQL
- Dar un servicio nuevo no es trivial
 - Documentación
 - Copias de seguridad
 - Gestión del propio servicio
 - ...

Entorno Actual

El “CPD” (Año 2018)



Entorno Actual

El “CPD” (Año 2018)



Entorno actual “Core”

Instalación desatendida

Instalación desatendida basada en preseeds

- Este sistema lo seguimos usando en la actualidad,
- Permite la instalación de un aula totalmente desatendida en unas dos-tres horas
- En el peor caso, un aula se puede usar de un día para otro (catástrofe)
- La interacción por parte del Técnico/Administrador, es nula
- Combinamos otras herramientas como
 - Wakeonlan
 - Mirror local de paquetes, para “ahorrar tráfico” (apt-mirror)
 - Scripts que personalizan el puesto (late_command en preseed)
 - **Puppet** para configuración temprana (hablaremos después)
- Cuando la máquina termina de instalarse, es perfectamente usable.
- Reinstalar un puesto es trivial. Se tarda menos en reinstalar que en analizar qué ha ocurrido (denuncia seguridad).

Entorno actual “Core”

Cuentas de Usuario

Sistema de Cuentas de usuario basado en LDAP

- No usamos el sistema de cuentas corporativo
- Solución basada en OpenLDAP
 - Integración con otras aplicaciones (Gitlab, horarios, etc)
- Antes,
 - No había control sobre quién se hacía una cuenta
 - Alumnos con varias cuentas
 - Cuentas “eternas”
- Ahora,
 - Automatismos para la creación, renovación de cuenta, cambio de pass
 - Los Técnicos no hacemos nada, sólo si hay problemas

Entorno actual “Core”

Servidor de ficheros NFS

Servidor de Ficheros NFS para cuentas en red

- Es necesario un servidor que facilite la abstracción de “directorio en red”
- Servidor Físico en CPD con mucho disco y muy rápido
 - Ojo con los raids
 - Ojo con las copias de seguridad
 - Ojo con la conexión a la red
 - Escalabilidad, tolerancia a fallos, disponibilidad
- Cada Campus tiene su propio servidor NFS (no como el resto de servicios)
 - La interacción suele ser nula, sólo si hay problemas

Entorno actual “Core”

Infr. de Virtualización

Hoy en día, el servidor físico está prácticamente en desuso

- A no ser que sea algo muy específico
- Es necesario implementar/usar un servidor de virtualización
 - Que permita flexibilizar
 - Compartir los recursos de red, disco, etc
 - Que permita administrar de manera sencilla
 - Escalabilidad, tolerancia a fallos, disponibilidad
- A día de hoy la solución que estamos usando es Proxmox 5.0, 4 hosts
 - Es gratis
 - Licencia de código abierto
 - Basado en Debian GNU/Linux
 - Características de HA
 - Modelo de virtualización KVM y contenedores de Linux (LXC)
 - Administración Web: <https://192.168.125.11:8006/#v1:0:18:4::::::>

Entorno actual “Core”

Infr. de Virtualización

Cuando uno administra un entorno de virtualización...

- Separar bien el tráfico de las Vms
- Cada máquina/conjunto de máquinas → un interfaz virtual
- Cada interfaz virtual → uno o más interfaces físicos
- Para acceder al host (servidor de virtualización) uso un interfaz totalmente independiente, que no se comparte con ninguna máquina
- Características de HA, medio de almacenamiento compartido, gestión de las Vlanes, etc.
- Copias de seguridad de las Vms

Entorno actual “Core”

Gestión de la configuración

El día a día

► Miguel Ortuño



[Tecnicos-lab] apt install recode

- Instalar un paquete. O varios
 - Cambiar un fichero
 - Desinstalar un paquete
 - Cambiar las reglas de **iptables** en cada máquina para permitir un puerto nuevo
 - **Pero cada item, en 500 equipos,**
 - Gestión del cambio
 - Todos los equipos tienen que estar siempre igual (mismo estado)

Entorno actual “Core”

Gestión de la configuración

Antes (2006-2011)

- Las tareas más básicas de instalación de software y configuración del entorno las hacíamos con los scripts ssh-a-todos
 - `./sshatodos-delta “apt-get install -assume-yes ssss”`
 - `./scpatodos-delta /tmp/hosts/ /etc/hosts`
 - `for i in `seq -w 00 $sup`; do ssh delta$i “$1”; done`
- La gestión del cambio era muy complicada (a pesar de que el servicio era muy bueno :-)
- Hoy en día seguimos usando esos scripts, pero solo en emergencias

Entorno actual “Core”

Gestión de la configuración

Ahora (2016-?)

- Gestión de la configuración basada en **Puppet**
 - Herramienta de gestión de la configuración basada en código abierto
 - Permite la gestión del cambio de una manera eficiente
 - El estado del sistema se describe en unos ficheros llamados **manifiestos**
 - Los clientes ejecutan el manifiesto acorde a su configuración y aplican los cambios necesarios para cumplimentarlo.
 - Basado en una arquitectura cliente servidor
 - Los clientes solicitan su configuración cada X segundos, y aplican los cambios que sean necesarios para estar “conformes” con su manifiesto
 - Lenguaje declarativo, multiplataforma, módulos desarrollados por la comunidad

Entorno actual “Core”

Gestión de la configuración

Ejemplo: la configuración básica de una máquina del lab:

```
agutierr@puppet: /etc/puppetlabs/code/environments/configlab/mymodules/configbase/manifests$ ls
aptconfig.pp      crontab.pp        ldaplabos.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$
```

Ejemplo: tarea de cron

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

Entorno actual “Core”

Gestión de la configuración

Ejemplo: cuando la máquina solicita la configuración...

```
root@alpha00:~# pat
Info: Using configured environment 'configlab'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Retrieving locales
Info: Loading facts
Info: Caching catalog for alpha00.aulas.gsync.urjc.es
Info: Applying configuration version '1544449146'
Notice: /Stage[main]/Configbase::Crontab/Exec[/usr/bin/crontab -r]/returns: executed successfully
Notice: /Stage[main]/Configbase::Crontab/Cron[avisa-apagado1]/ensure: created
Notice: /Stage[main]/Configbase::Crontab/Cron[avisa-apagado2]/ensure: created
Notice: /Stage[main]/Configbase::Crontab/Cron[avisa-apagado-final]/ensure: created
Notice: /Stage[main]/Configbase::Crontab/Cron[apagado-automagico]/ensure: created
Notice: /Stage[main]/Configbase::Crontab/Cron[apagado-automagico-2]/ensure: created
Notice: /Stage[main]/Configbase::Crontab/Cron[apagado-automagico-3]/ensure: created
Notice: /Stage[main]/Configbase::Crontab/Cron[clean-var-tmp-task-cron]/ensure: created
Notice: Applied catalog in 25.70 seconds
root@alpha00:~# █
```


Entorno actual “Core”

Gestión de la configuración

Lenguaje declarativo de puppet

- Nos facilita abstracciones para los recursos de configuración más básicos
 - File
 - Cron
 - Package
 -

Entorno actual “Core”

Gestión de la configuración

Lenguaje declarativo de puppet: instalación de un paquete

- Mediante el recurso *package*:

```
# a petición de Gregorio Robles 27.10.2018
package {'python3-pydocstyle':
  ensure => latest,
}

package {'pydocstyle':
  ensure => hold,
}
```

Entorno actual “Core”

Gestión de la configuración

Lenguaje declarativo de puppet: configuración de iptables

- Mediante el recurso *firewall* del módulo *puppetlabs-firewall*:

```
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'],  
}
```

Entorno actual “Core”

Gestión de la configuración

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

Entorno actual “Core”

Gestión de la configuración


Puppet + Foreman

- Los agentes de Puppet que ejecutan en las máquinas vuelcan un informe
- Este informe es difícil de procesar/gestionar
 - Foreman
- 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

Entorno actual “Core”

Gestión de la configuración

Puppet + Foreman



FOREMAN

Monitor >

Hosts >

Configurar >

Infraestructura >

Administrar >

Visión general

Filtro ... 🔍 Buscar 📄

Estado de configuración del host para Puppet

Hosts que han realizado modificaciones sin errores	432
Hosts con estado error	5
Informes satisfactorios en los últimos 3 días	1
Hosts que tenían cambios pendientes	0
Hosts desincronizados	0
Hosts sin informes	0
Hosts con alertas inhabilitadas	0

Hosts en total: 438

Entorno actual “Core”

Gestión de la configuración

Puppet + Foreman

FOREMAN

Monitor >

Hosts >

Configurar >

Infraestructura >

Administrar >

Hosts

origin = Puppet and last_report > "4730 minutes ago" and (status.failed > 0 or status.failed_restarts > 0) and status × 🔍 Buscar 📄

Exportar Seleccionar una acción

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

500 ▼ por página

El Futuro

El Futuro

A futuro...

- Integración LDAP ↔ LDAP URJC
- Integración de Laboratorios Windows
- Pasar de virtualización de servidores a contenedores
- Mejorar el sistema de copias de seguridad
- Pasar a un ciclo de integración continua en la configuración
- ¿?



¡ GRACIAS !

