S(TIC)

# Solución Libre IPAM Basada en OpenNetAdmin

Daniel Martín Brito< dmartinb@ull.edu.es>
Jonás Regueira Rodríguez <jregueir@ull.edu.es>

ULL | Universidad de La Laguna

# Motivación

Situación Previa:

- 4 Nodos Infoblox.
- Caro, renovación de licencias anual
- Nuevas versiones era necesario migrar a nuevos equipos (appliance o MV)


Entonces… ya que hay que migrar …

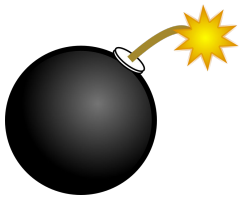
¿Alternativas que nos ahorren costes de mantenimiento?

Muchas

Elegimos: OpenNetAdmin

# Anécdota: ¡El CAOS!

13/06/2014



¡Y de repente murió Infoblox!

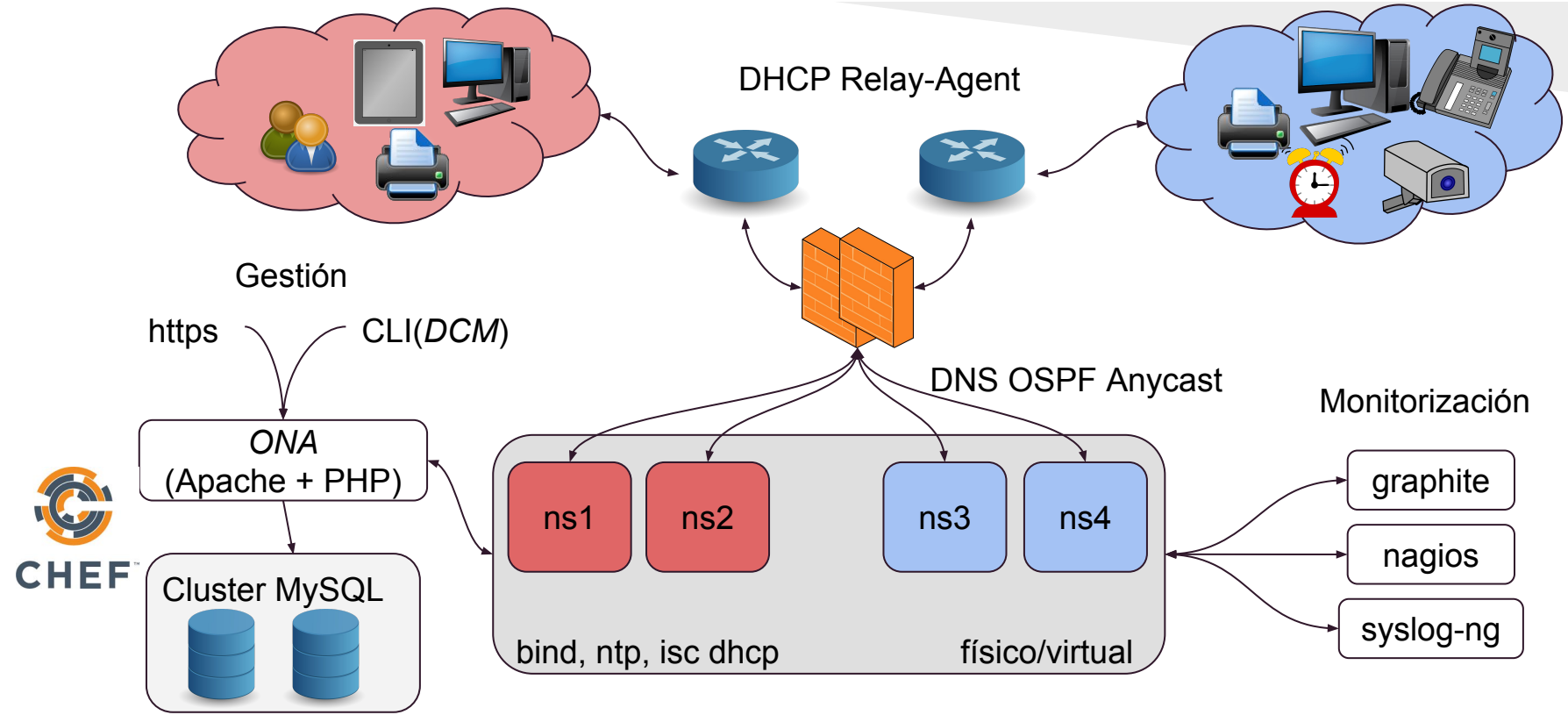
6-7 Horas sin servicio de DHCP y DNS

# Anécdota: ¡El Héroe!

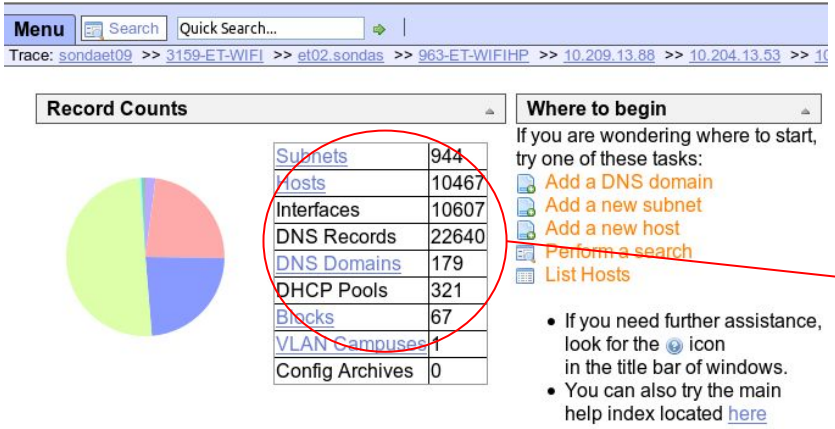
OpenNetAdmin de maqueta a Producción

Desde el 13/06/2014 dando servicios de DHCP y DNS sin problemas

# Arquitectura IPAM ULL
# Proyecto OpenNetAdmin + Personalizaciones

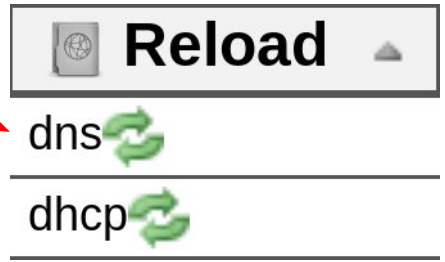


# Interfaz Web I
# ONA (PHP + AJAX + MySQL)

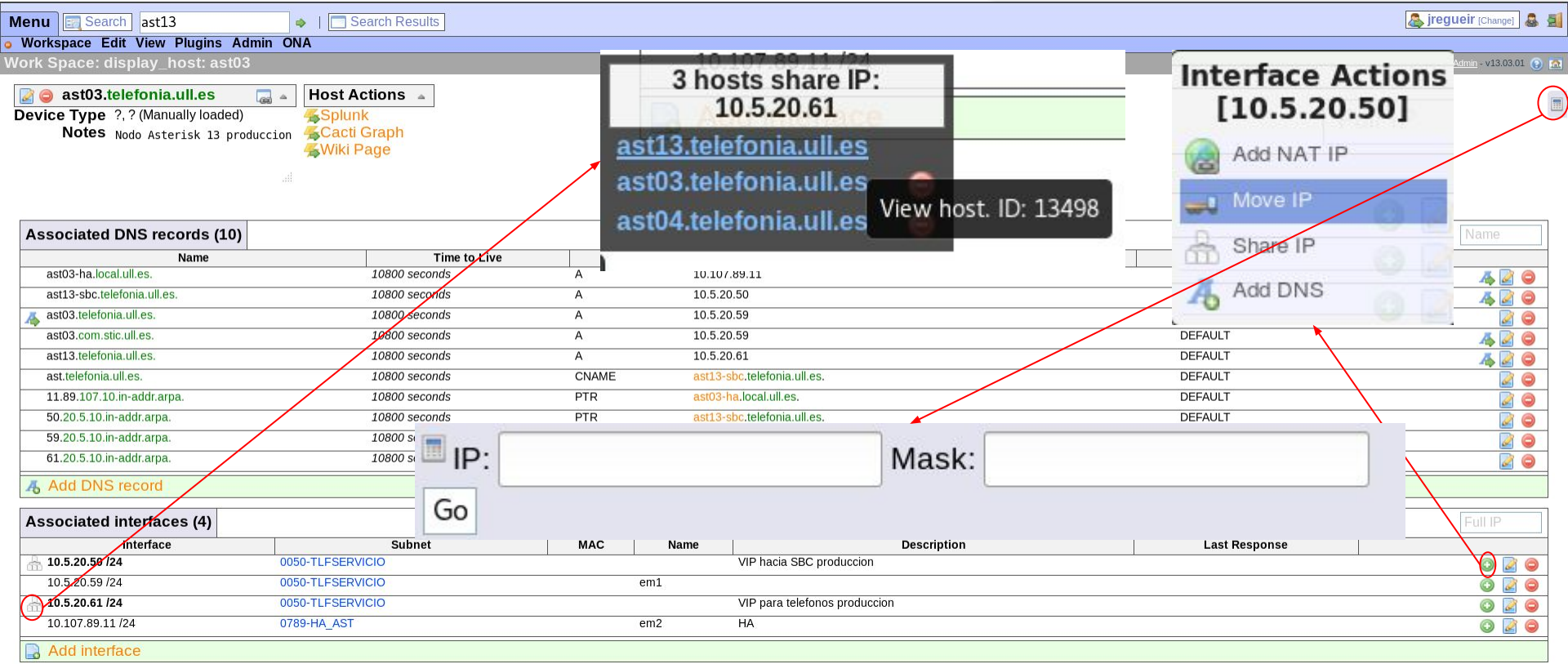



| | |
|---|---|
| Subnets | 944 |
| Hosts | 10494 |
| Interfaces | 10635 |
| DNS Records | 22694 |
| DNS Domains | 179 |
| DHCP Pools | 321 |
| Blocks | 67 |


Plugin STIC




# Interfaz Web II
# Ejemplo Host

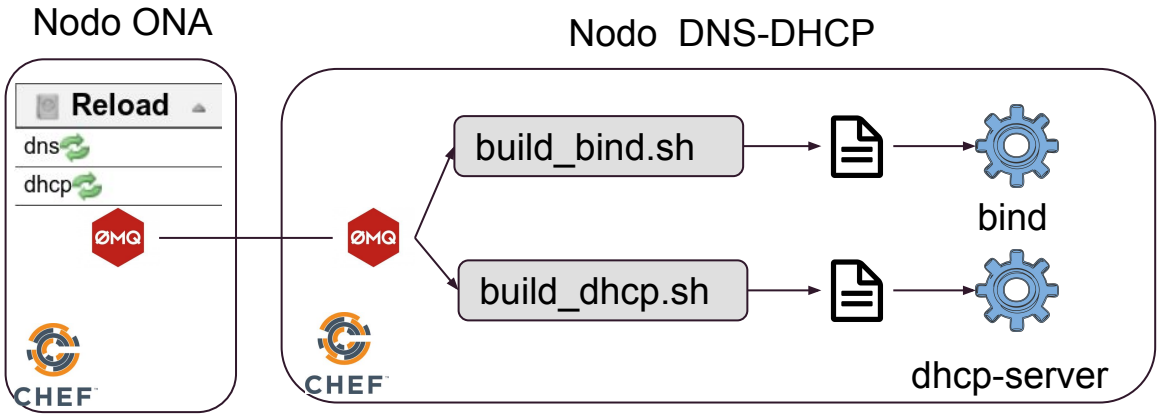


# OpenNetAdmin CLI: Módulo DCM

```
>dcm.pl -r dns_record_add name=test.ull.es
type=A ip=10.0.0.1 view=PUBLIC addptr
```

- Script perl que permite desde línea de comandos hacer lo mismo que desde la interfaz Web.
- Como norma, no modificar la BBDD directamente.
- Ejemplo usos:
  - Carga datos masivos: Migración Infoblox a ONA (API Infoblox -> API ONA) y activación DHCP FAILOVER
  - APP gestión TOIP ULL
  - APP gestión impresoras ULL

# Generación ficheros configuración
# Módulos build_bind y build _isc_dhcp



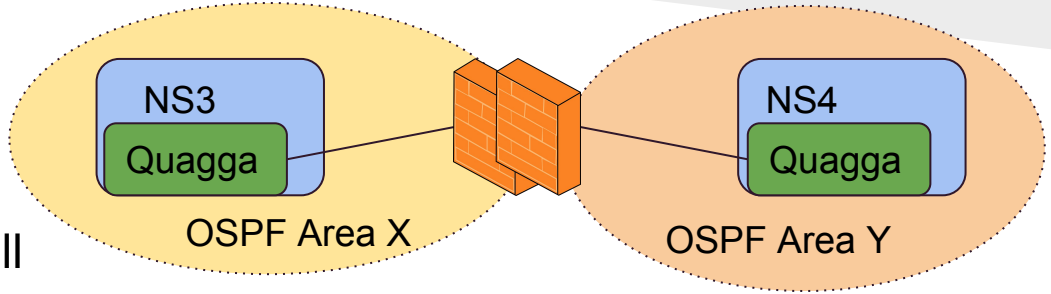

Personalizaciones:

- Gestión ficheros: configuración base, header y footer con CHEF
- Chequeos de sintaxis antes de un reload.
- Soporte vistas con ACLs
- Regeneración ficheros configuración a través del "sistema reload ULL": *Plugin Reload + Librería zeromq + retardo aleatorio*

# HA DNS: OSPF ANYCAST

DNS: anycast - OSPF DNS

- Ventajas:
  - Nodo más cercano
  - Failover - electrónica de red
- Faltaría balanceo: ECMP en firewall



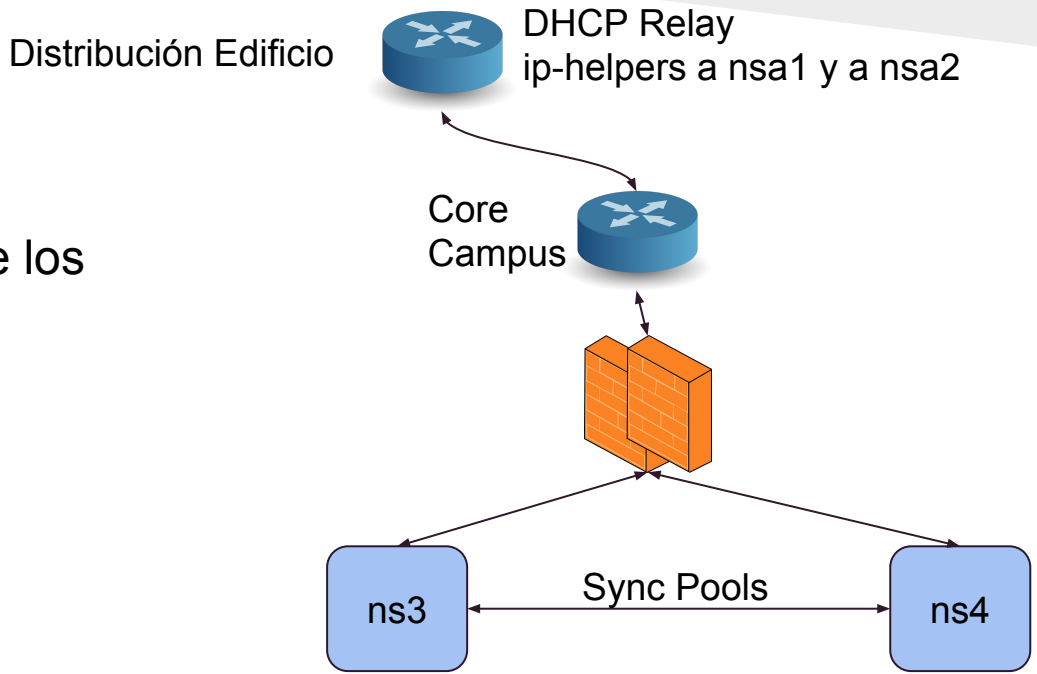

Script Cron

*/1 * * * * root /opt/ona/bin/dnscheck.sh. Si detecta problemas con el bind detiene el *quagga* y el *bind* => resuelve las peticiones DNS el otro nodo

# HA DHCP: DHCP-FAILOVER

OMAPI:

- Monitorización estado de los servidores: check_dhcp_failover.py ( librería *pypureomapi)*.
- Poner en Partner-Down



# Monitorización
# Scripting + Nagios

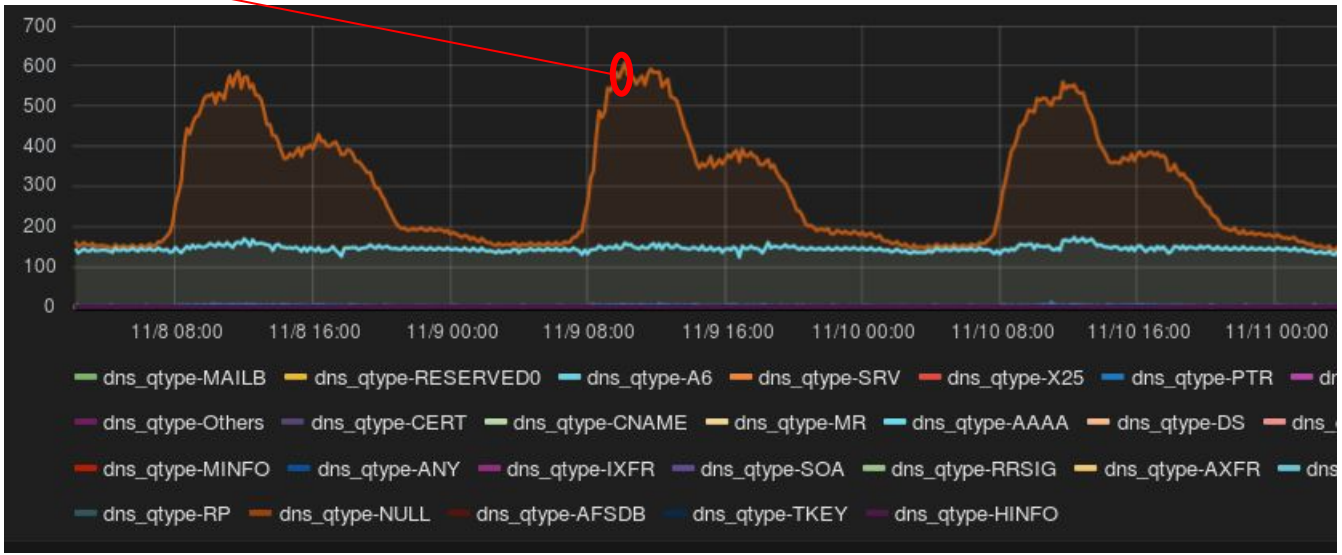
| Host | Service | Status |
|---|---|---|
| nsr1.ull.es | DHCPD PROC | OK |
| | DISK USG | OK |
| | DNS | OK |
| | DNS_ULL | OK |
| | LOAD | OK |
| | MEM USG | OK |
| | NTPD | OK |
| | OSPFD PROC | OK |
| | UPSMON | OK |
| | copia dns dhcp PASV | OK |
| | dhcpd-pools PASV | OK |

# Monitorización
# Scripting + Grafana


Actualización Kernel vulnerabilidad “Dirty Cow”
Sin Pérdida de Servicio DHCP

# Monitorización
# Scripting + Grafana

| | |
|---|---|
| dns_qtype-AFSDB: | 0 |
| dns_qtype-A: | 635 |
| dns_qtype-MX: | 0 |
| dns_qtype-SPF: | 0 |
| dns_qtype-SOA: | 1 |
| dns_qtype-CERT: | 0 |
| dns_qtype-CNAME: | 0 |
| dns_qtype-MR: | 0 |
| dns_qtype-AAAA: | 164 |
| dns_qtype-X25: | 0 |
| dns_qtype-NAPTR: | 0 |
| dns_qtype-SSHFP: | 0 |
| dns_qtype-WKS: | 0 |
| dns_qtype-RESERVED0: | 0 |
| dns_qtype-TYPE52: | 0 |
| dns_qtype-RP: | 0 |
| dns_qtype-MG: | 0 |
| dns_qtype-DNAME: | 0 |
| dns_qtype-NSEC: | 0 |
| dns_qtype-MINFO: | 0 |
| dns_qtype-ANY: | 0 |
| dns_qtype-IXFR: | 0 |
| dns_qtype-RRSIG: | 0 |
| dns_qtype-AXFR: | 0 |
| dns_qtype-NSAP: | 0 |
| dns_qtype-NS: | 0 |
| dns_qtype-LOC: | 0 |
| dns_qtype-NSEC3PARAM: | 0 |
| dns_qtype-DNSKEY: | 0 |
| dns_qtype-Others: | 0 |
| dns_qtype-NULL: | 0 |
| dns_qtype-NSEC3: | 0 |
| dns_qtype-EID: | 0 |



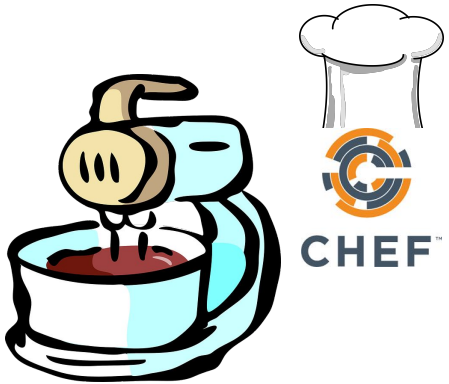
# Trabajo Futuro. Mejoras, detalles

- Sin auditorías: ¿cambios recientes?
- (probar ona_recent_additions), ¿quién hizo un cambio?.
- Optimizar la generación de la configuración DNS
- IPV6
- DNSSEC
- Delegar zonas. De momento no interesados.
- Alimentar ONA con CHEF
- Publicar personalizaciones
- Reload desde CLI

# Conclusión: OpenNetAdmin + Personalizaciones

Ingredientes:

- BD: mysql
- Interfaz web: PHP-AJAX
- Interfaz CLI (scripting)
- Autenticación vía LDAP, autorización en aplicación
- Servicios: BIND, ISC DHCP, NTP
- Quagga
- ZeroMQ



# Conclusión: OpenNetAdmin + Personalizaciones

Obtenemos:

- Inventario de redes
- Los nodos no necesitan gestión para dar servicio
- Alta disponibilidad y tolerancia a fallos
- Actualizaciones sin corte
- Ahorro en costes de mantenimiento
- Mayor control de la solución
- Fácilmente escalable apoyado en CHEF, MV y/o hardware genérico
- Entorno de preproducción
- Potenciar la economía local

# Bibliografía

- Listado de alternativas, de soluciones IPAM: Wikipedia IPAM
- Página principal proyecto OpenNetAdmin
- ONA, interfaz Web de OpenNetAdmin:
  - Código: https://github.com/opennetadmin/ona
  - Documentación: https://github.com/opennetadmin/ona/wiki
- CLI: https://github.com/opennetadmin/dcm
- Generación de ficheros de configuración:
  - Plugin build_bind: https://github.com/opennetadmin/build_bind
  - Plugin build_isc_dhcp: https://github.com/opennetadmin/build_isc_dhcp

# y todo esto ….

Para y por la ULL - 100% disponibilidad

Daniel Martín Brito< dmartinb@ull.edu.es>
Jonás Regueira Rodríguez <jregueir@ull.edu.es>

ULL | Universidad de La Laguna