

Solución Libre IPAM Basada en OpenNetAdmin

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



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 ...

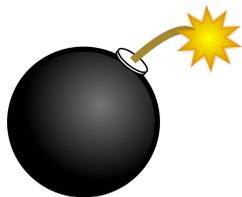
¿Alternativas que nos ahorren costes de mantenimiento?

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!

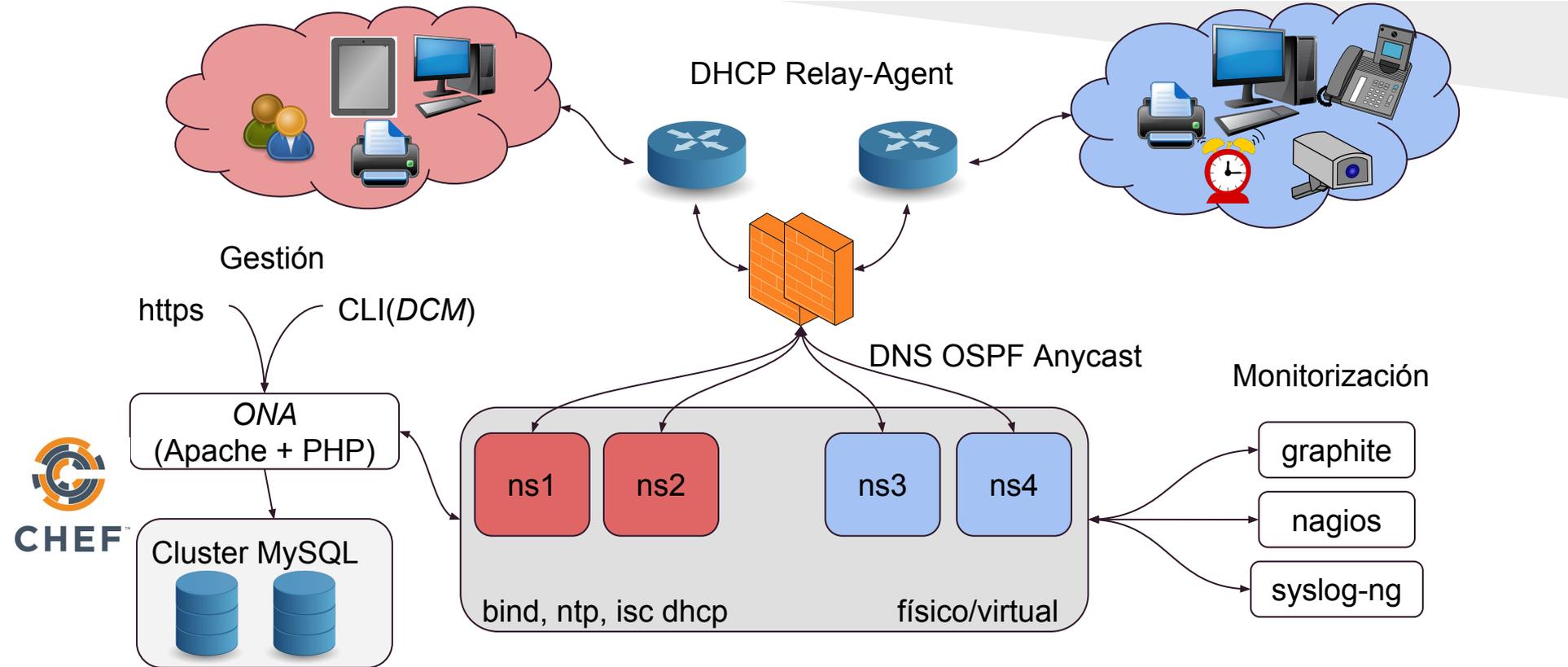


OpenNetAdmin de maqueta a
Producción

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

Arquitectura IPAM ULL

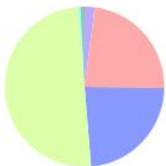
Proyecto OpenNetAdmin + Personalizaciones



Interfaz Web I ONA (PHP + AJAX + MySQL)

Menu Search Quick Search...
Trace: sondaet09 >> 3159-ET-WIFI >> et02.sondas >> 963-ET-WIFIHP >> 10.209.13.88 >> 10.204.13.53 >> 10

Record Counts



Subnets	944
Hosts	10467
Interfaces	10607
DNS Records	22640
DNS Domains	179
DHCP Pools	321
Blocks	67
VLAN Campuses	1
Config Archives	0

Where to begin

If you are wondering where to start, try one of these tasks:

-  [Add a DNS domain](#)
-  [Add a new subnet](#)
-  [Add a new host](#)
-  [Perform a search](#)
-  [List Hosts](#)

- If you need further assistance, look for the  icon in the title bar of windows.
- You can also try the main help index located [here](#)

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

Reload

dns 

dhcp 

Plugin STIC

 **Reload**

dns 

dhcp 



Interfaz Web II Ejemplo Host



Menu Search ast13 Search Results jreguir [Change]

Workspace Edit View Plugins Admin ONA
Work Space: display_host: ast03

ast03.telefonia.ull.es Host Actions
Device Type ? (Manually loaded)
Notes Nodo Asterisk 13 produccion

- Splunk
- Cacti Graph
- Wiki Page

**3 hosts share IP:
10.5.20.61**
ast13.telefonia.ull.es
ast03.telefonia.ull.es
ast04.telefonia.ull.es View host. ID: 13498

Interface Actions [10.5.20.50]

- Add NAT IP
- Move IP
- Share IP
- Add DNS

Associated DNS records (10)

Name	Time to Live			
ast03-ha.local.ull.es.	10800 seconds	A	10.107.89.11	
ast13-sbc.telefonia.ull.es.	10800 seconds	A	10.5.20.50	
ast03.telefonia.ull.es.	10800 seconds	A	10.5.20.59	
ast03.com.stic.ull.es.	10800 seconds	A	10.5.20.59	
ast13.telefonia.ull.es.	10800 seconds	A	10.5.20.61	
ast.telefonia.ull.es.	10800 seconds	CNAME	ast13-sbc.telefonia.ull.es.	
11.89.107.10.in-addr.arpa.	10800 seconds	PTR	ast03-ha.local.ull.es.	
50.20.5.10.in-addr.arpa.	10800 seconds	PTR	ast13-sbc.telefonia.ull.es.	
59.20.5.10.in-addr.arpa.	10800 seconds			
61.20.5.10.in-addr.arpa.	10800 seconds			

IP: Mask:

Go

Associated interfaces (4)

Interface	Subnet	MAC	Name	Description	Last Response
10.5.20.59 /24	0050-TLFSERVICIO			VIP hacia SBC produccion	
10.5.20.59 /24	0050-TLFSERVICIO		em1		
10.5.20.61 /24	0050-TLFSERVICIO			VIP para telefonos produccion	
10.107.89.11 /24	0789-HA_AST		em2	HA	

Add DNS record

Add interface

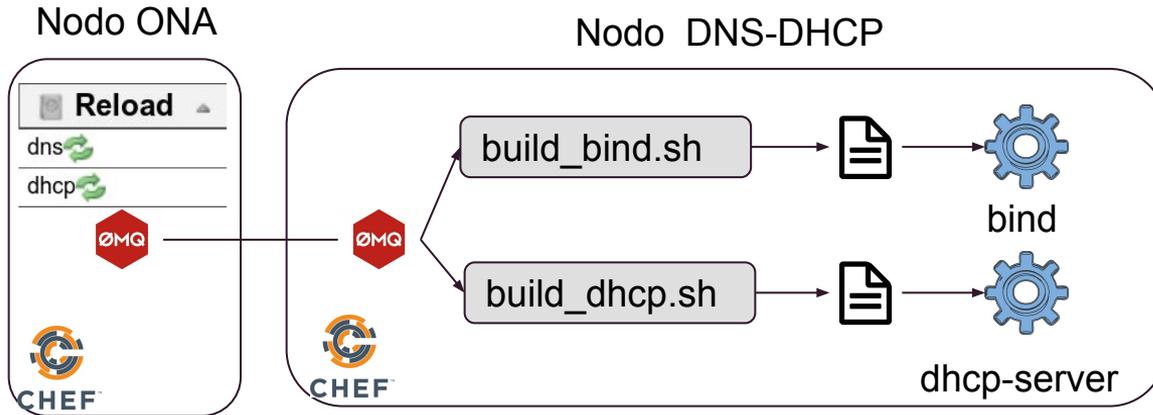
```
>dcm.pl -r dns_record_add name=test.ull.es  
type=A ip=10.0.0.1 view=PUBLIC addptr
```

- 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:

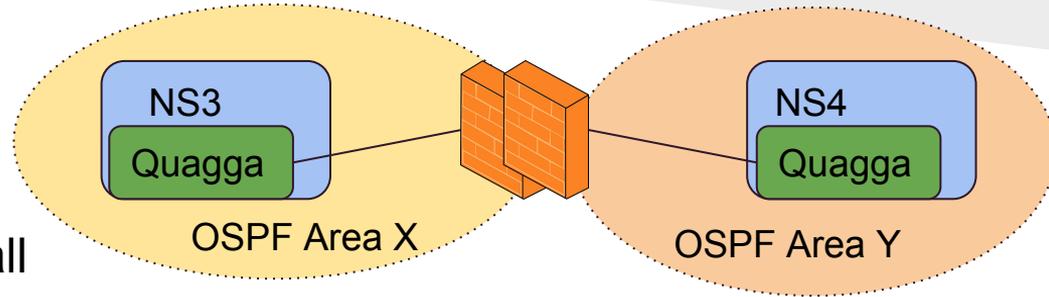


- Gestión ficheros: configuración base, header y footer con CHEF
- Chequeos de sintaxis antes de un reload.
- Soporte vistas con ACLs
- Regeneración ficheros configuración a través del “sistema reload ULL”: *Plugin Reload + Librería zeromq + retardo aleatorio*

HA DNS: OSPF ANYCAST

DNS: anycast - OSPF DNS

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



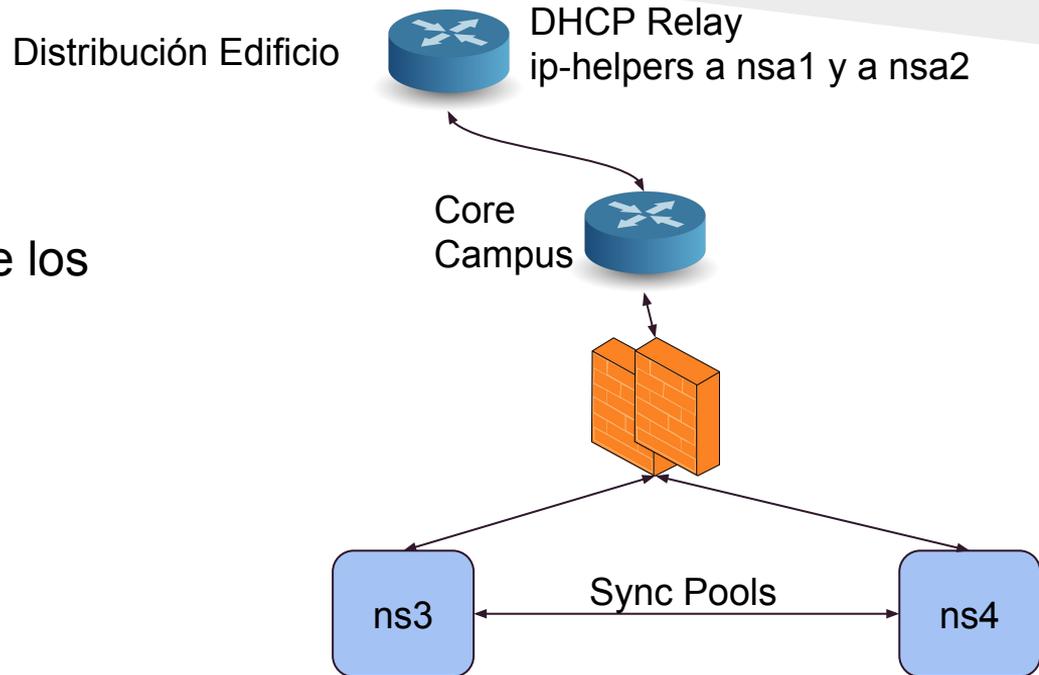
Script Cron

```
*/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		OK
	dhcpd-pools		OK

Monitorización Scripting + Grafana

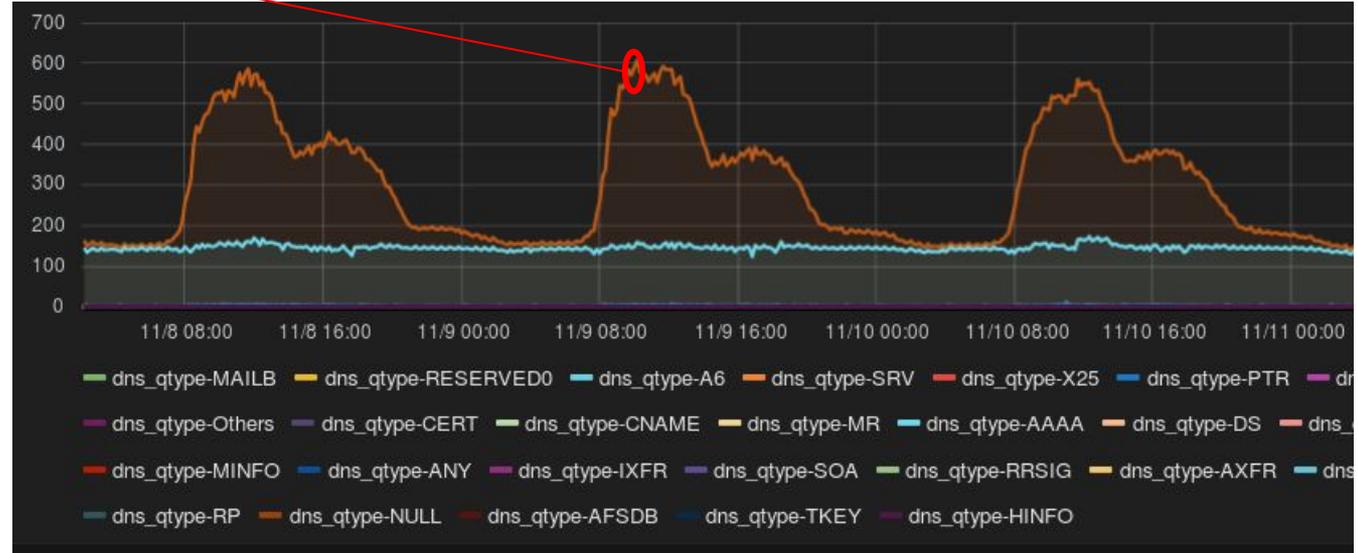


Actualización Kernel vulnerabilidad “Dirty Cow”
Sin Pérdida de Servicio DHCP

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-FID:	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

- 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

