Actualidad de DNS

48º GGTT RedIRIS

Valladolid, 28 de noviembre de 2019

Juan Carlos Rodríguez

Jcarlos.rodriguez@rediris.es

RedIRIS

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

Servicios DNS

- Delegacion DNS
  - Delegar resoluciones inversas del direccionamiento IP que provee RedIRIS
  - Aceptamos registros DS (DNSSEC)

- Secundario DNS
  - Publicar zonas como secundarios
  - Dos nubes Anycast DNS

- Hosting DNS
  - Gestionar y publicar zonas de instituciones
  - Gestión desde aplicación IRISDNS
  - Firmado DNSSEC
  - Publicación en las nubes Anycast

Servicios DNS

- Lista IRIS-DNS
  - Coordinación de servicio, novedades, incidencias, etc.
  - Cada administrador de DNS de la institución debería estar suscrito
    - Enviadnos los contactos para el servicio DNS (iris-nic@rediris.es)

- Herramienta IRISDNS https://irisdns.rediris.es
  - Gestión de los servicios Delegacion DNS, Secundario DNS y Hosting DNS
  - Monitorización de la configuración

- Formación
  - Cursos de formación DNS

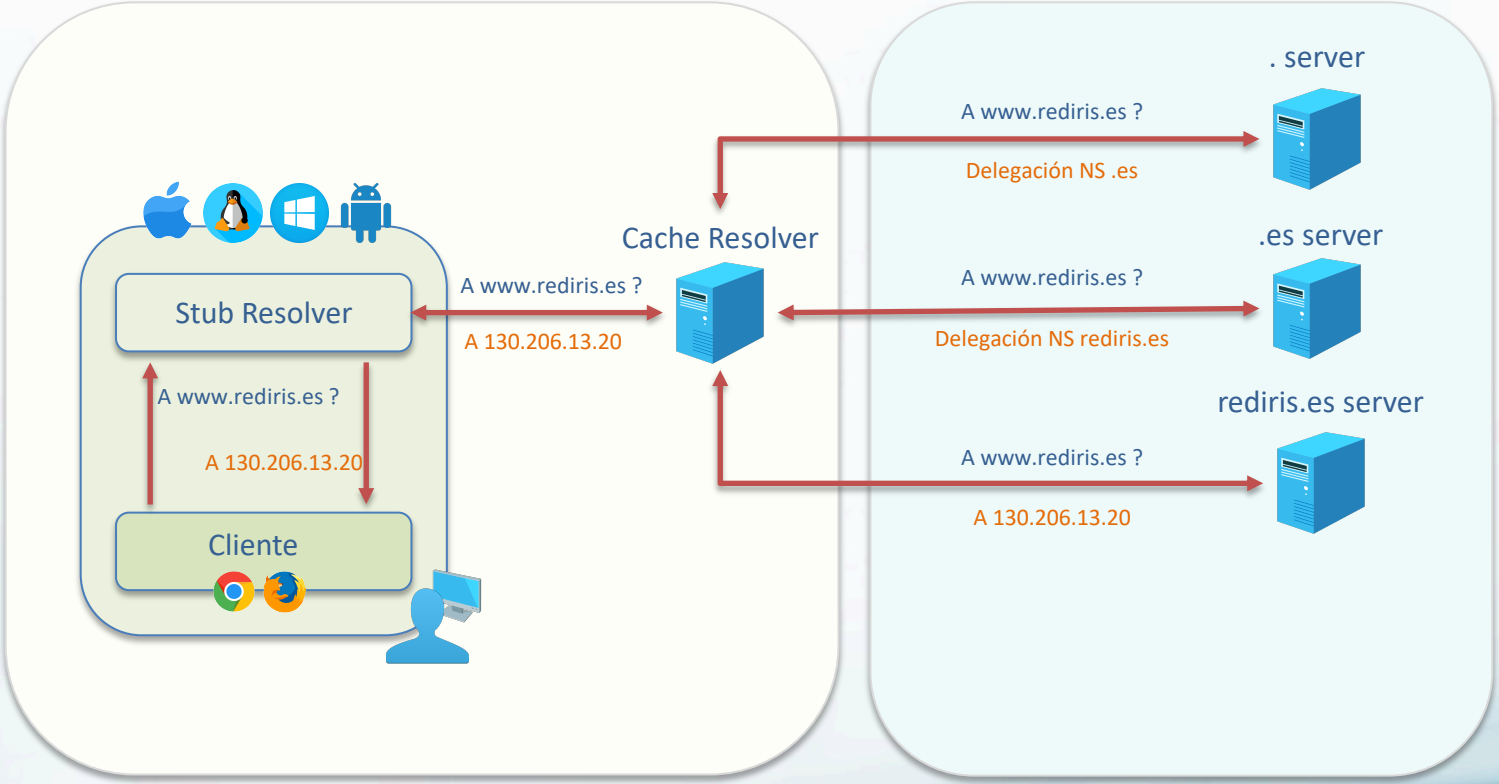
- http://www.rediris.es/servicios/conectividad/dns/

DNSSEC ¿qué es?

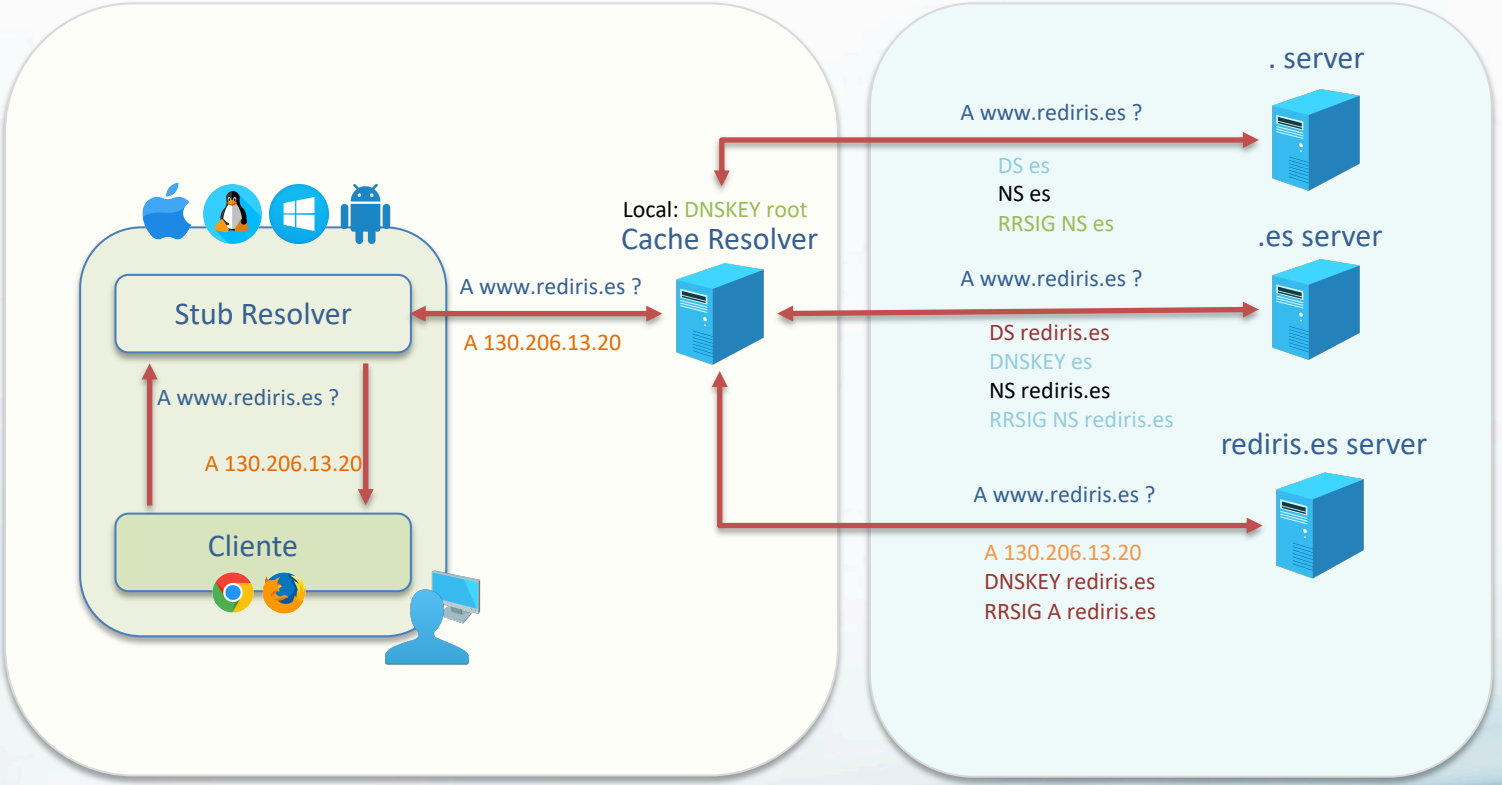
- DNSSEC verifica la autenticidad e integridad de la respuesta
  - Firmado criptográfico mediante clave pública/privada
  - Se garantiza la cadena de confianza mediante delegaciones firmadas por el dominio superior
  - Protege contra ataques man-in-the-middle y de envenenamiento de caché
    - Redirecciones a servidores comprometidos
  - Nuevas funcionalidades: DANE

- DNSSEC no cifra el mensaje
  - No añade privacidad ni confidencialidad
- DNSSEC todavía en etapa de adopción

Funcionamiento DNS



Funcionamiento DNSSEC



DANE: DNS-based Authentication of Named Entities

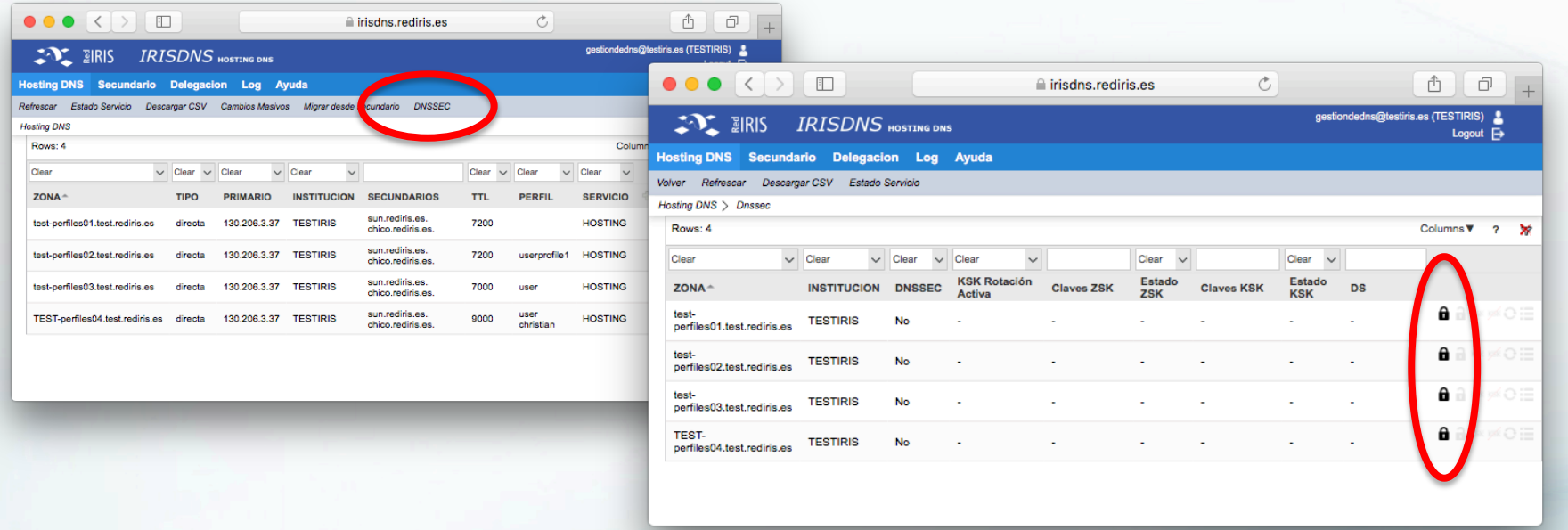
- Permite asociar certificados de tipo X.509 a dominios
  - Permite validar certificados creados por una CA o autofirmados
- Es un paso extra de seguridad y requiere DNSSEC
- Define un nuevo registro tipo TLSA:
  - *_25._tcp.mx09.puc.rediris.es. IN TLSA 3 1 2*
    6f4d03121ce3a83ab3c7b8dab9df0024ee53fc791e09d146169e0ff01ab7a1e15ac
    b0144353840fa176a35aec73956f51ba0bda16e1b27a3a5a99d4c8fd54d1d
  - *_443._tcp.redirisnova.es. IN TLSA 3 1 1*
    d011d8cfea96ba7afcf914e2f9d60aaac172f93bd6a3dd109aae2c58633f6c81
- Correo electrónico como caso de uso (RFC 7929)
  - Permite el SMTP cifrado y verificado
  - La existencia de un registro TLSA exige el uso de TLS

DNSSEC actividades 2019

- Firmados todos los dominios de RedIRIS desde Junio
- Disponible firmado de zonas en servicio "Hosting DNS”
- Disponible despliegue de delegaciones inversas firmadas (registros DS)

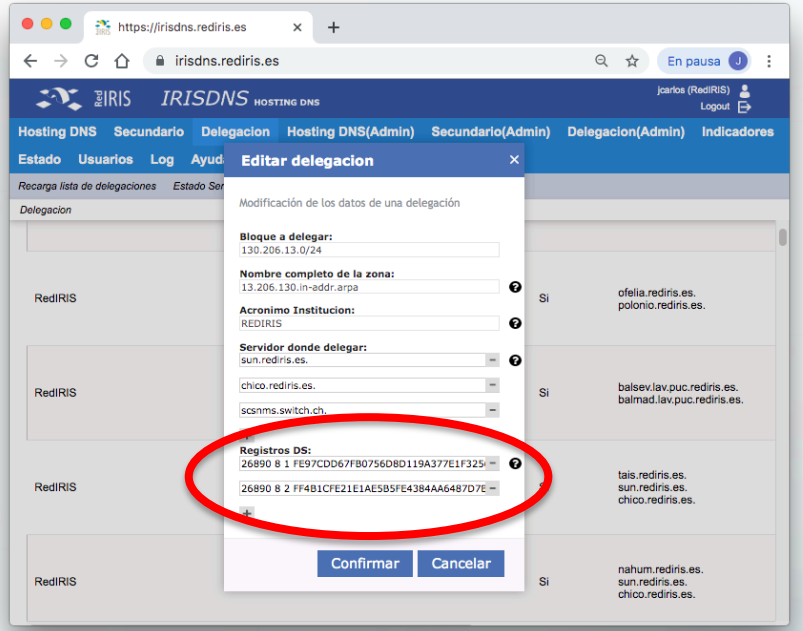
DNSSEC actividades 2019

Disponible firmado de zonas en servicio "Hosting DNS”



DNSSEC actividades 2019

Disponible despliegue de delegaciones inversas firmadas (registros DS)



ANYCAST ¿qué es?

- Servicio Unicast: una localización
  - Problemas si hay una caída o un ataque DDoS

- Servicio Anycast: múltiples localizaciones compartiendo dirección IP
  - El cliente es redirigido mediante routing al nodo más cercano
  - Si un nodo cae, el routing redirige el cliente al siguiente nodo más próximo
  - Si hay un ataque DDoS
    - Cada elemento del ataque sólo ataca al nodo más cercano
      - Contra más nodos, más difícil es saturar cualquiera de ellos
    - Aunque un nodo se saturase, sólo afectaría parcialmente a los clientes

ANYCAST actividades 2019

- Sustitución de los servidores unicast de RedIRIS por nubes Anycast
  - sun.rediris.es
    - 130.206.1.2 -> 199.184.182.1
    - 2001:720:418:CAF1::2 -> 2620:171:808::1

- Los antiguos unicast quedan como intermediarios para las transferencias de zona
  - sun.rediris.es -> sunrelay.rediris.es (130.206.1.2 // 2001:720:418:CAF1::2)

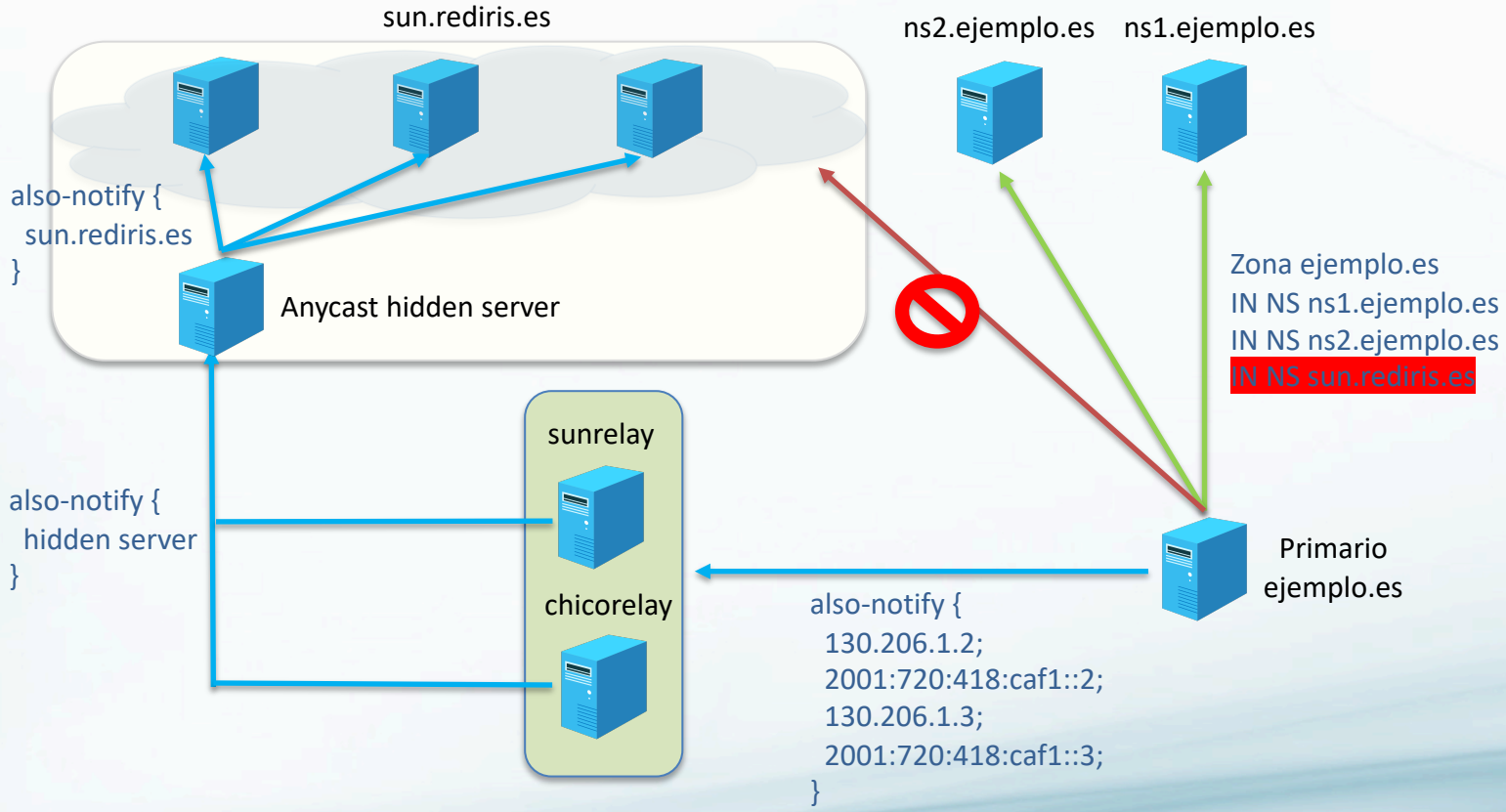
- Licitación y despliegue de dos nubes Anycast de diferentes proveedores comerciales
  - PCH (Packet Clearing House): licitado, desplegado y migrado
  - CIRA (Canadian Internet Registry Autorithy): adjudicado

ANYCAST cambios de configuración

¡Se requiere configuración adicional!

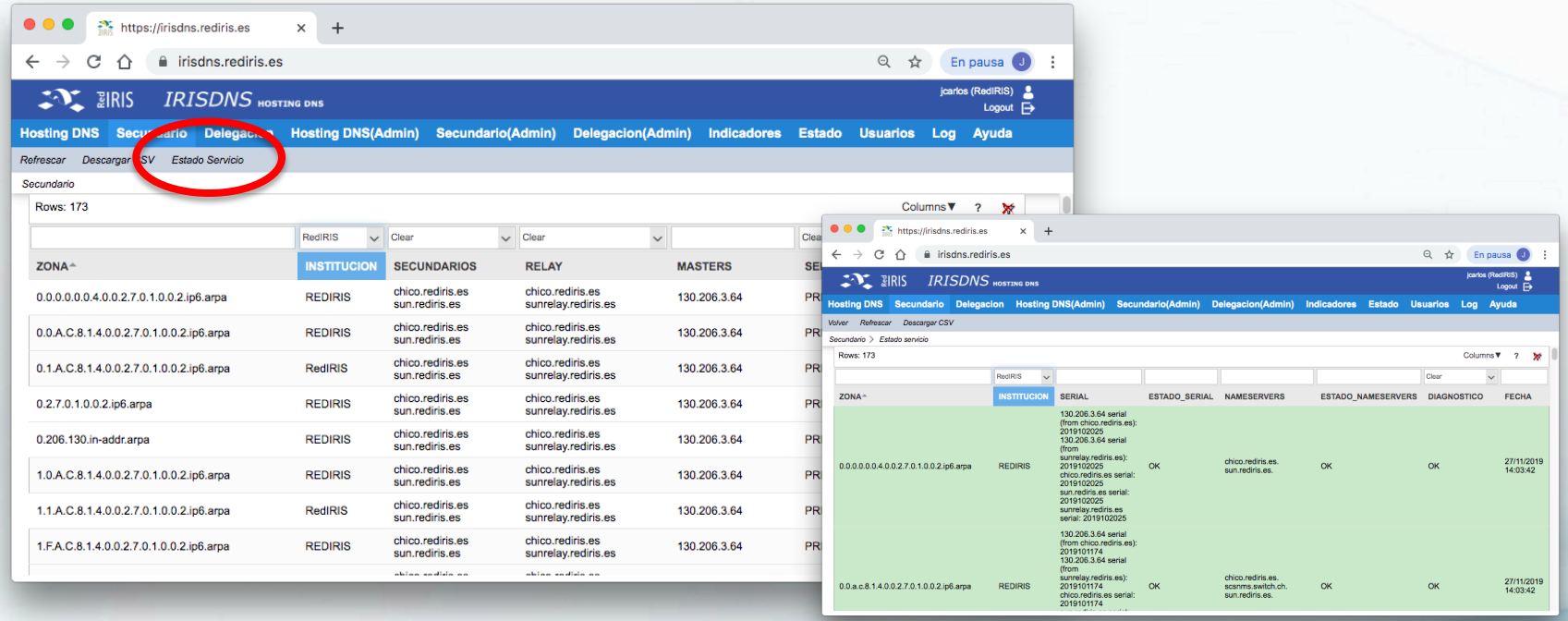
```
zone ”rediris.es" {
        type master;
        file ”rediris.es.db";
        also-notify {
                130.206.1.2;
                130.206.1.3;
                2001:720:418:caf1::2;
                2001:720:418:caf1::3;
        };
        allow-transfer {
                130.206.1.2;
                130.206.1.3;
                2001:720:418:caf1::2;
                2001:720:418:caf1::3;
};
```

ANYCAST transferencias de zona



ANYCAST comprobación de configuración

A través de IRISDNS podéis ver el estado de vuestra configuración



ANYCAST tamaños de las zonas

- Algunas zonas del servicio Secundario DNS son MUY grandes (decenas y centenares de miles de registros)
  - Contienen registros en desuso…
  - Contienen direccionamiento privado…
  - No están debidamente jerarquizadas…

- Es conveniente sanear las zonas
  - Son más difíciles de gestionar
  - Aumentan los costes
  - Publican vistas privadas de la infraestructura

Resumen de mejoras en el servicio durante 2019 (inicio 2020)

- Hosting DNS
  - Nueva funcionalidad de firmado DNSSEC
  - Desplegado servidores de publicación Anycast
- Secundario DNS
  - Servidores Anycast
- Delegación
  - Aceptamos registros DS
  - Zonas de RedIRIS firmadas
    - cadena de validación DNSSEC completa
- Organizado curso presencial de DNS

Evolución y próximas mejoras

- Terminar despliegue Anycast migrando chico.rediris.es (principios 2020)
- TSIG disponible en IRISDNS para servicio Secundario DNS (principios 2020)
- Estudio de interés/viabilidad de nuevo servicio DNS firewall (2020)
- Formación (2020)
  - Cursos
  - Videosesiones

¡Muchas gracias!

Más de 25 años al servicio de la investigación