OK, DNSSEC instalado. Y ahora, qué..?

Juan P. Cerezo

Internet Kahuna, BT ES LABS

Kahuna *(ka-hoo-nah), .n: Hombre-medicina hawaiano. En entornos técnicos, “aquel que hace funcionar las cosas”.*

jpc@lab.bt.es

Contenido

- DNS.. qué?
- Instalación
- En marcha…
- Herramientas

DNS: un gran poder conlleva una gran responsabilidad

DNSSEC: cuestión de autoridad. Y de autenticidad.

DNSSEC es complicado*, y difícil de instalar y mantener. Pero funciona, y resuelve algunos problemas graves del DNS global

(*) - Solo para el nivel al que hemos permitido que se degrade la “calidad” de la operación de Internet, especialmente de los sistemas de red. Probablemente no es para tanto…

DNSSEC… y ahora, qué?

Hay material disponible suficiente para tomar contacto, si se quiere:
http://www.slideshare.net/search/slideshow?searchfrom=header&q=DNSSEC

Lo importante es empezar a probar, adquirir experiencia y comenzar a operar (aunque sea parcialmente) en el proceso global.

El proposito de la charla es compartir la experiencia del despliegue, y ayudar a que otros puedan comenzar a probar.

DNSSEC… y ahora, qué?

Experiencias de ccTLDs, gTLDs, DNS providers, herramientas de testing, de configuración, grupos de trabajo,... todo el material está disponible.

La coordinación y la colaboración facilita el proceso.

Es posible, funciona, y es útil (si, incluso aunque .ES no esté firmado)

DNSSEC… y ahora, qué?

Trasfondo: experiencia básica en configuración y operación de DNS (BIND9), posibilidad de experimentar con dominios reales, y mucho mucho mucho interés.

Origen: charla práctica de Joao Damas/JPC en GORE-11.

Proceso: basado fundamentalmente en el “best seller” de ISC: “Deploying DNSSEC in 6 minutes”, con algunas sugerencias del “guru” residente (Joao).

Instalación

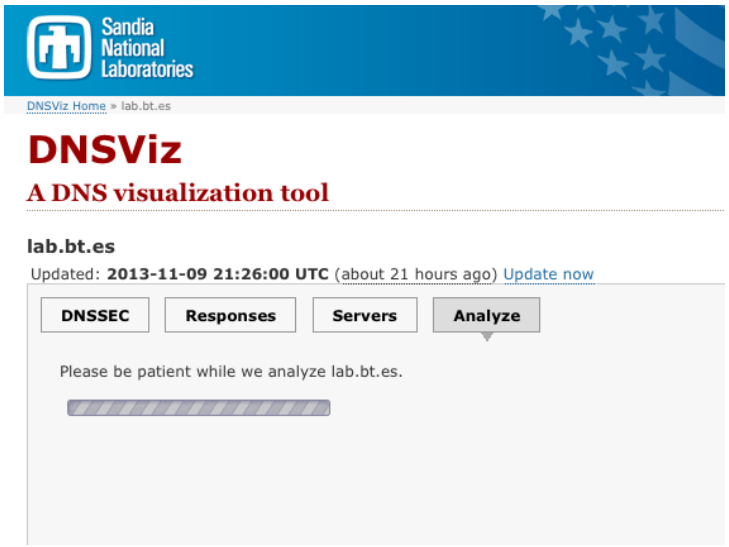
Duró algo más de “6 minutes”, pero en una mañana estaba todo hecho, incluyendo el registro en el DLV de ISC: https://dlv.isc.org/

Zona lab.bt.es DNSSEC activa el 26-mayo de 2013, usando las herramientas básicas proporcionadas por BIND.

Como no estaba muy seguro, lo mejor era verificarlo, por ejemplo en http://dnsviz.net/d/lab.bt.es/dnssec/*

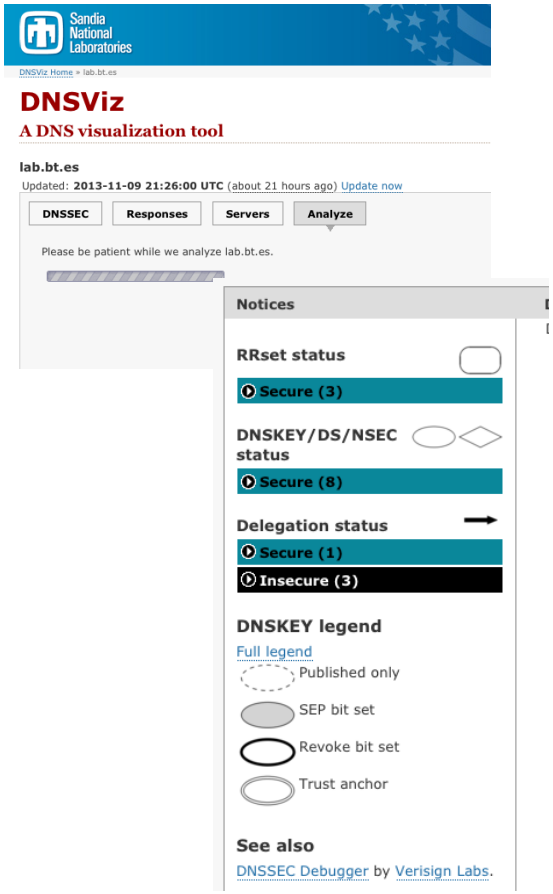
(*) - Básicamente porque los gráficos molan...

Instalación

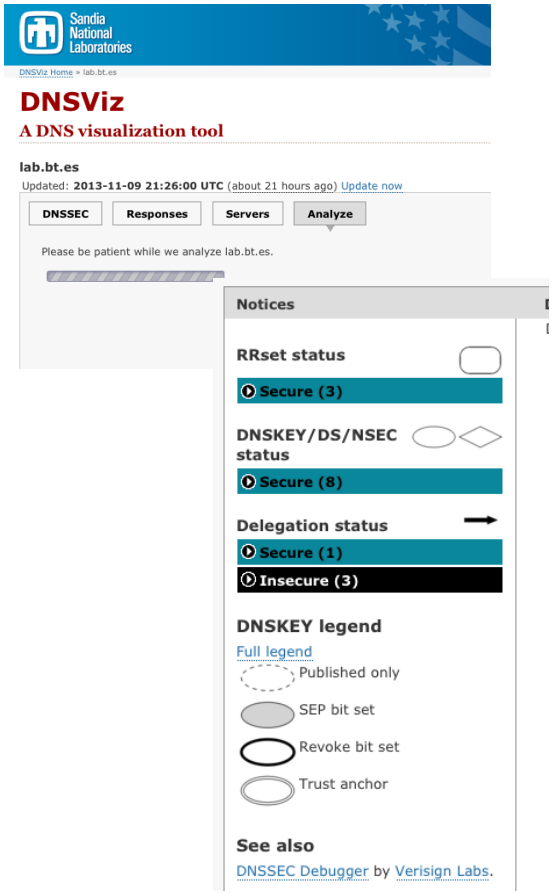


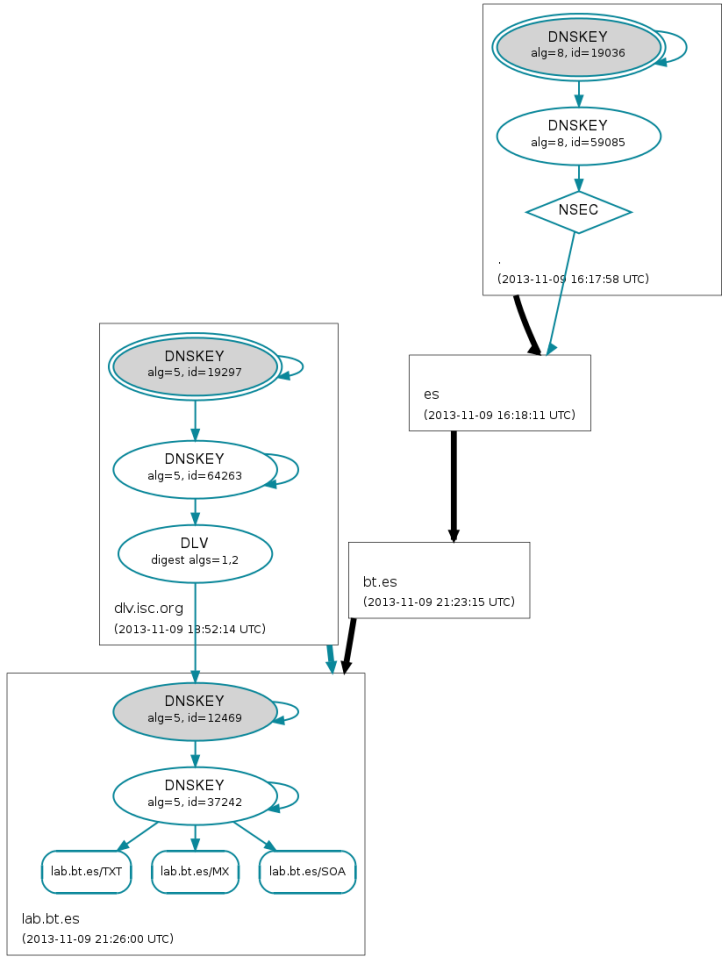
Instalación

Instalación

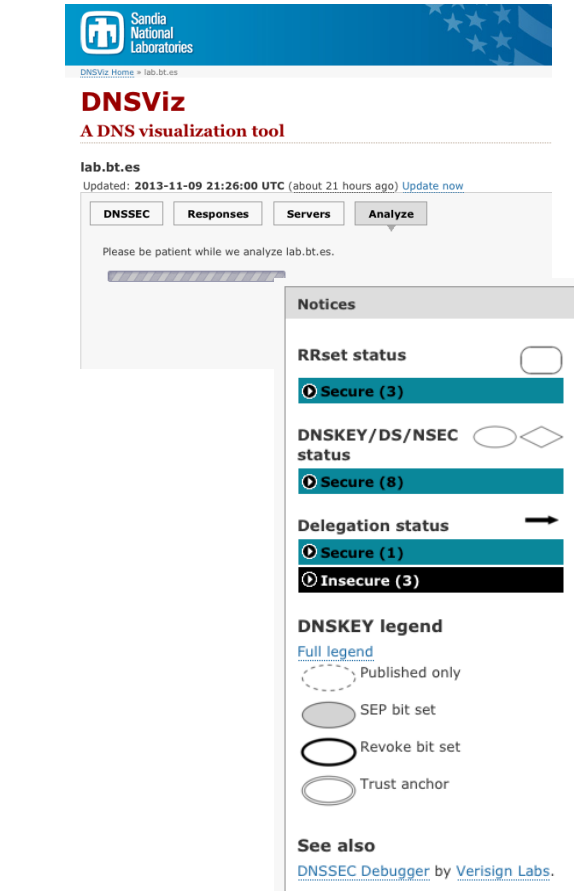


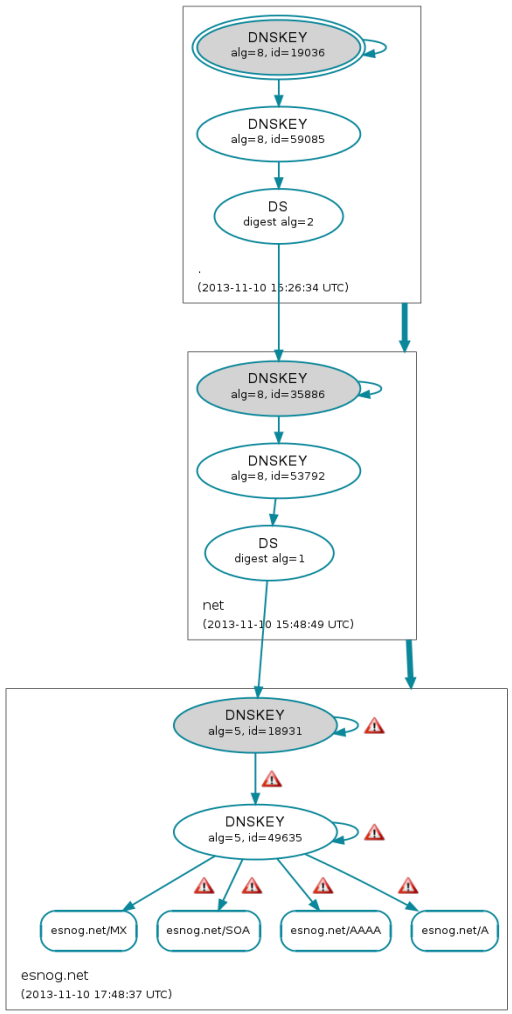
Instalación

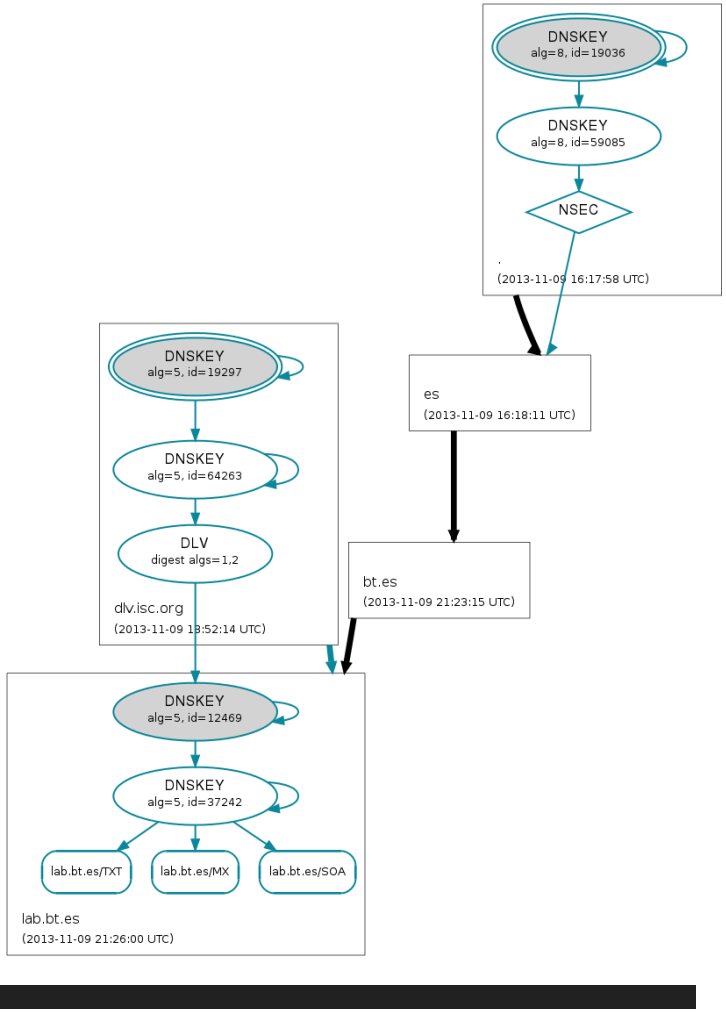




Instalación







Instalación

Instalación

Todo aparentemente OK.

Sin prestar atención especial durante los meses posteriores...

En marcha...

Todo aparentemente OK.

Sin prestar atención especial durante los meses posteriores...

...hasta que expiró la ZSK !!!

(en pleno Agosto, asi que pasó algún tiempo antes de arreglarlo…)

DS actualizada en DLV.ISC.ORG al 1 de Octubre

En marcha...

Sin pre

...hasta

(en ple

DS act

ISC DNSSEC Look-aside Validation Registry

Home | Manage Zones | Change password | Log out | Help

Name	lab.bt.es (delete)
Status	✓ No problems were detected.
DNSKEY Records	1 (add)
Created	2013-05-26 10:32:17 UTC
Last Update	2013-05-26 10:32:17 UTC

DNSKEY Records

(add record)

More	Status	Published	Key Tag	Flags	Type	Key (partial)
(details) (show log)	✓ Good	Yes	12469	257 (KSK)	RSASHA1	AwEAA...Up3X3GDZVt0jLGL

En marcha...

Desde entonces, más pendiente del estado de la zona, y su integración en el despliegue de DNSSEC.

Osea, mirando más en detalle lo propio y lo que hacen a tu alrededor...

Gracias a Marcos Sanz (DENIC) y a Iñigo Ortiz (RIPE NCC) por la información aportada para esta sección…

En marcha...

Para geeks (mayormente, basadas en cli):

- DIG (opción **`+dnssec`** básicamente, aunque permite ver otras cosas, como las **`root.keys, traverse keys,`** etc.)
- DRILL (ahora **`ldns`**), de http://www.nlnetlabs.nl/projects/drill/
- Por favor, que NADIE vuelva a mencionar **`nslookup`**...

Herramientas

Para geeks (continuación):

- http://www.dnssec-tools.org/, incluyendo wiki, tutoriales y herramientas on-line

- DNSSEC trigger, de http://www.nlnetlabs.nl/projects/dnssec-trigger/ permite instalarte tu propio DNSSEC validator, junto con una instancia de **`unbound`** como “local resolver”

  (versiones para Windows, Mac OS X y fuentes para compilar en Linux/*BSD/etc)

Herramientas

Para la gestión de las zonas/claves/etc:

- Ya no hace falta picarse los scripts uno mismo: http://www.opendnssec.org/

Para hacer la verificación de zonas:

- Sandia Labs: http://dnsviz.net/
- Verisign Labs: http://dnssec-debugger.verisignlabs.com/
- .SE DNS check: http://dnscheck.iis.se/
- AFNIC Zonecheck: http://www.zonecheck.fr/

Herramientas

Comprobar la validación DNSSEC del DNS que usa tu browser:

- DNSSEC Validation: http://bit.ly/1hu4GcP (tutorial de Men&Mice)
- Univ. Düsseldorf: http://dnssec.vs.uni-due.de/, tipo tortuga KAME. También apunta a un dominio “falsificado” de Comcast para hacer comprobaciones: *http://www.dnssec-failed.org/*
- La portada de http://www.dnssec-tools.org/ también verifica la validación

Herramientas

Comprobar la validación DNSSEC del DNS que usa tu browser:

- Validator de SIDN: http://dnssectest.sidn.nl/ (estricto y detallado)
- U. Berkeley ICSI Netalyzr: un super-completo test de conectividad desde el cliente, que incluye verificaciones de DNSSEC: http://netalyzr.icsi.berkeley.edu/index.html (aviso: usa JAVA…)

Herramientas

Comprobar rápidamente si accedes a dominios DNSSECizados:

- Mozilla/Chrome* validator plug-in de CZ.NIC: http://www.dnssec-validator.cz/ (El premio a tu trabajo: un )

- Otro plug-in para Mozilla, con parte del código compartido con el anterior: https://os3sec.org/

Muy visuales (para enseñar a tu jefe), pero no permiten depurar. Además, tu DNS debe poder validar DNSSEC...o usar el validator del plugin, que no siempre funciona

(*) – La versión de Chrome no instala en Windows 8 ?

Herramientas

Estado del despliegue (para ayudar a convencer a tu jefe):

- CentralNIC: https://manage.centralnic.com/support/dnssec
- http://www.dnssec-deployment.org/
- ISOC: http://www.internetsociety.org/deploy360/dnssec/statistics/
- Verisign Labs: http://secspider.cs.ucla.edu/ (incluye un zone checker)

Herramientas

DNSSEC es complicado, pero es posible.

Hay necesidad.

Hay herramientas, hay (empieza a haber) experiencia, y hay gente dispuesta a ayudar, dentro de la comunidad ESNOG/GORE.

¿Preguntas?

jpc@lab.bt.es ()

Conclusión