

# 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](mailto: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 minutos”, 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



Sandia  
National  
Laboratories

[DNSViz Home](#) » [lab.bt.es](#)

## DNSViz

A DNS visualization tool

**lab.bt.es**

Updated: **2013-11-09 21:26:00 UTC** (about 21 hours ago) [Update now](#)

DNSSEC

Responses

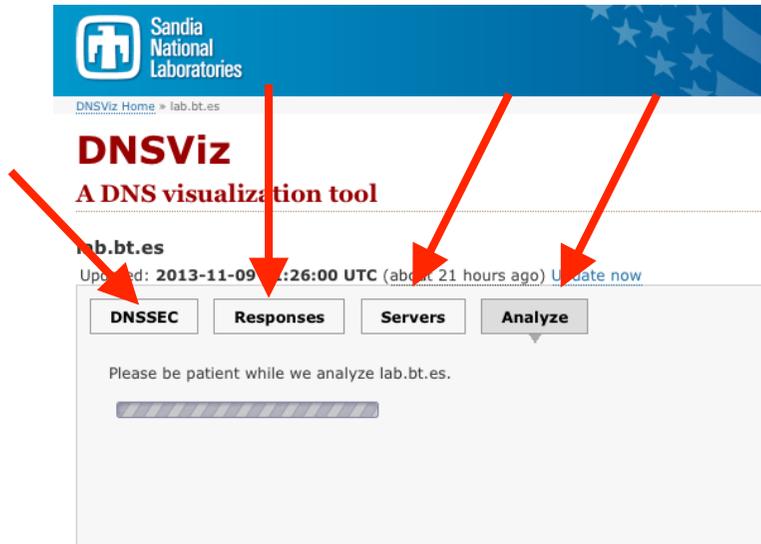
Servers

Analyze

Please be patient while we analyze lab.bt.es.



# Instalación



Instalación



DNSViz Home » lab.bt.es

## DNSViz

A DNS visualization tool

lab.bt.es

Updated: 2013-11-09 21:26:00 UTC (about 21 hours ago) [Update now](#)

[DNSSEC](#) [Responses](#) [Servers](#) [Analyze](#)

Please be patient while we analyze lab.bt.es.



### Notices

**RRset status**

**Secure (3)**

**DNSKEY/DS/NSEC status**

**Secure (8)**

**Delegation status**

**Secure (1)**

**Insecure (3)**

**DNSKEY legend**

[Full legend](#)

- Published only
- SEP bit set
- Revoke bit set
- Trust anchor

**See also**

[DNSSEC Debugger](#) by [Verisign Labs](#).

# Instalación



DNSViz Home » lab.bt.es

## DNSViz

A DNS visualization tool

lab.bt.es

Updated: 2013-11-09 21:26:00 UTC (about 21 hours ago) [Update now](#)

**DNSSEC** Responses Servers Analyze

Please be patient while we analyze lab.bt.es.

### Notices

#### RRset status

Secure (3)

#### DNSKEY/DS/NSEC status

Secure (8)

#### Delegation status

Secure (1)

Insecure (3)

#### DNSKEY legend

[Full legend](#)

Published only

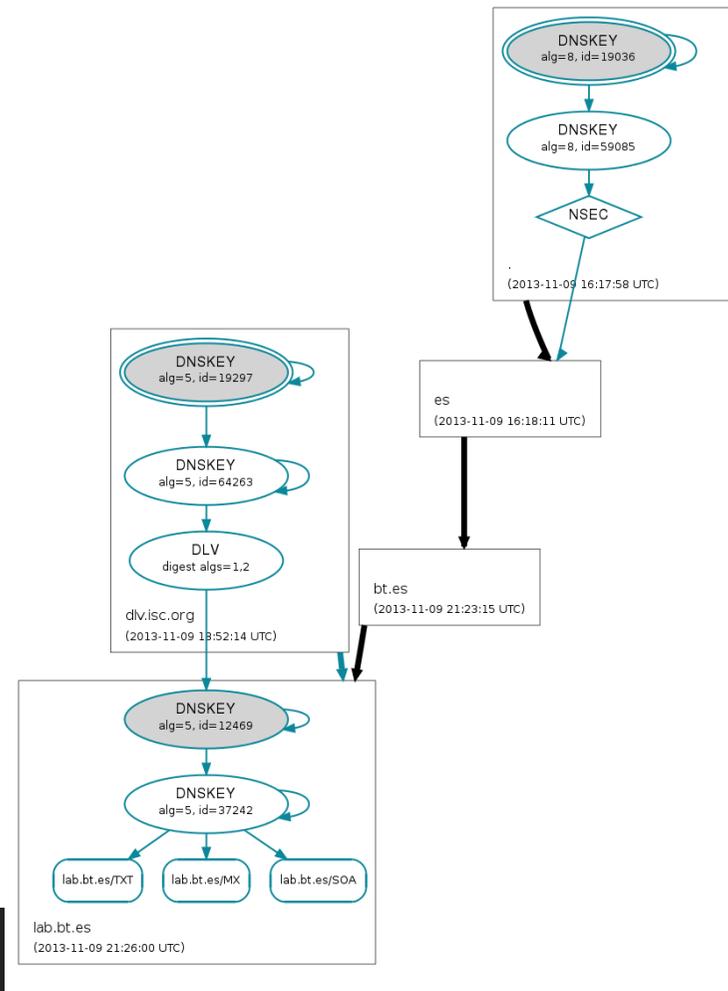
SEP bit set

Revoke bit set

Trust anchor

#### See also

[DNSSEC Debugger](#) by [Verisign Labs](#).



# Instalación

Sandia National Laboratories  
DNSViz Home » lab.bt.es

## DNSViz

A DNS visualization tool

lab.bt.es  
Updated: 2013-11-09 21:26:00 UTC (about 21 hours ago) [Update now](#)

DNSSEC Responses Servers Analyze

Please be patient while we analyze lab.bt.es.

**Notices**

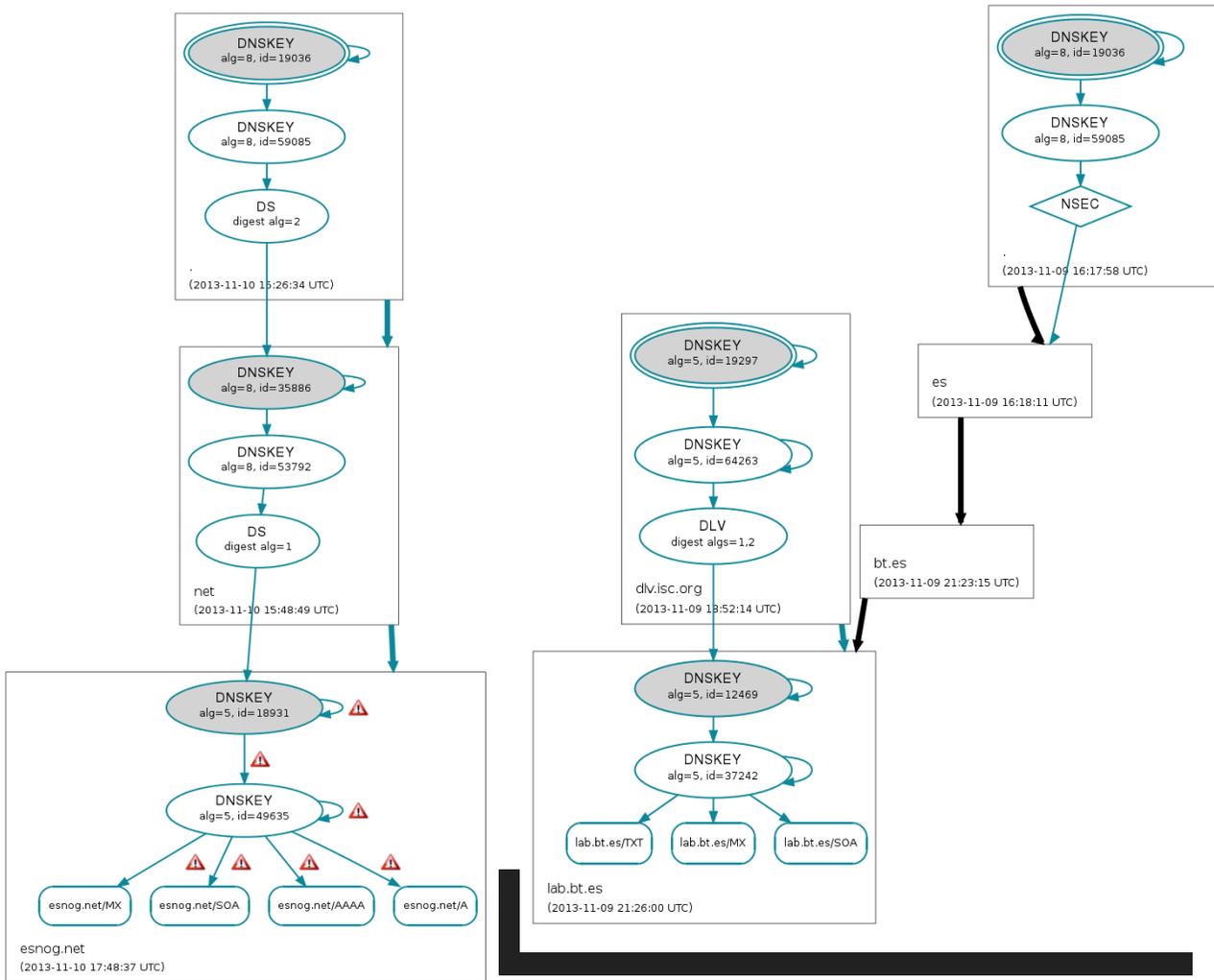
**RRset status**  
Secure (3)

**DNSKEY/DS/NSEC status**  
Secure (8)

**Delegation status**  
Secure (1)  
Insecure (3)

**DNSKEY legend**  
[Full legend](#)  
Published only  
SEP bit set  
Revoke bit set  
Trust anchor

**See also**  
[DNSSEC Debugger](#) by Verisign Labs.



# Instalación

# DNSViz

A DNS visualization tool

lab.bt.es  
Updated: 2013-11-09 21:26:00 UTC (about 21 hours ago) Update now

DNSSEC Responses Servers Analyze

Please be patient while we analyze lab.bt.es.

**Notices**

**RRset status**  
 Secure (3)  
 Insecure (0)

**DNSKEY/DS/NSEC status**  
 Secure (8)  
 Insecure (0)

**Delegation status**  
 Secure (1)  
 Insecure (3)

**DNSKEY legend**  
[Full legend](#)  
  Published only  
  SEP bit set  
  Revoke bit set  
  Trust anchor

**See also**  
[DNSSEC Debugger](#) by Verisign Labs.

# Instalación

lab.bt.es  
Updated: 2013-11-09 21:26:00 UTC (about 21 hours ago) Update now

DNSSEC Responses Servers Analyze

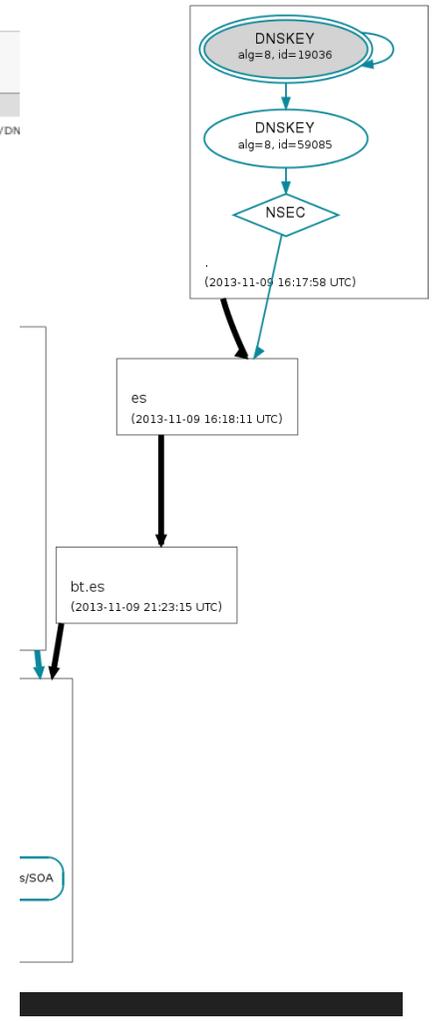
**DNS Server Status**  
 Notice: The features on this page are not yet fully developed but it has been deployed in its infant form to further aid with DNS/DN

**Delegation Information**

Name	Exists?	Parent zone		Child zone	Exists?	Authoritative IPs	
		Glue/additional records					
nadja.lab.bt.es	yes	A	212.49.129.203	yes	A	212.49.129.203	
		AAAA	2001:ac0::a00:20ff:fee6:ce32			AAAA	2001:ac0::a00:20ff:fee6:ce32
ns.lab.bt.es	yes	A	212.49.128.132	yes	A	212.49.128.132	
		AAAA	2001:ac0::20e:cff:fe77:8eac			AAAA	2001:ac0::20e:cff:fe77:8eac
nsjpc.lab.bt.es	yes	A	195.5.95.121	yes	A	195.5.95.121	
		AAAA	2001:ac0:0:ff::bebe:cafe			AAAA	2001:ac0:0:ff::bebe:cafe

**Server information**

	nadja.lab.bt.es. (212.49.129.203)	nadja.lab.bt.es. (2001:ac0:a00:20ff:fee6:ce32)	ns.lab.bt.es. (212.49.128.132)	nsjpc.lab.bt.es. (195.5.95.121)	nsjpc.lab.bt.es. (2001:ac0:0:ff::bebe:cafe)
Responsive over UDP	ERR	OK	OK	ERR	OK
Responsive over TCP	OK	OK	OK	OK	OK
Answers authoritatively (AA bit)	OK	OK	OK	OK	OK
SOA serial consistent	OK	OK	OK	OK	OK
SOA authority correct (NXDOMAIN)	OK	OK	OK	OK	OK
SOA consistent (NXDOMAIN)	OK	OK	OK	OK	OK
SOA authority correct (Empty Answer)	OK	OK	OK	OK	OK
SOA consistent (Empty Answer)	OK	OK	OK	OK	OK
EDNS capable	OK	OK	OK	OK	OK
PMTU sufficient	OK	OK	OK	OK	OK
Returns DNSKEY	OK	OK	OK	OK	OK
Returns RRSIG	OK	OK	OK	OK	OK
Returns NSEC/NSEC3 (NXDOMAIN)	OK	OK	OK	OK	OK
Returns RRSIG covering NSEC/NSEC3 (NXDOMAIN)	OK	OK	OK	OK	OK
Returns NSEC/NSEC3 (Empty Answer)	OK	OK	OK	OK	OK
Returns RRSIG covering NSEC/NSEC3 (Empty Answer)	OK	OK	OK	OK	OK



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, así 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 acti



## DNSSEC Look-aside Validation Registry

[Home](#) [Manage Zones](#) [Change password](#) [Log out](#) [Help](#)

<b>Name</b>	lab.bt.es ( <a href="#">delete</a> )
<b>Status</b>	✓ No problems were detected.
<b>DNSKEY Records</b>	1 ( <a href="#">add</a> )
<b>Created</b>	2013-05-26 10:32:17 UTC
<b>Last Update</b>	2013-05-26 10:32:17 UTC

### DNSKEY Records

[\(add record\)](#)

More	Status	Published	Key Tag	Flags	Type	Key (partial)
<a href="#">(details)</a> <a href="#">(show log)</a>	✓ 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 `1dns`), 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](mailto:jpc@lab.bt.es)



**Conclusión**