

Tema: DNS Externo y su optima configuración

Descripción: Principales Registros que debe tener todo DNS externo para una empresa con delegación de zona

Autor: Armando Felipe Fuentes Denis email: armandof at armandof.com; armandofelipe1992 at gmail.com

Bibliografía: [Manual de Hugo en GUTL](#), Documentación de Internet

La mayoría de los administradores de red familiarizados con GNU/Linux usan BIND como la aplicación por excelencia para implementar un servicio de nombres de dominio para su red. No obstante, de hace algunos existen varias alternativas en desarrollo, una de ellas es NSD, sobre la que hablaremos un poco en este manual.

NSD es un servidor de DNS de alto rendimiento implementado desde cero por NLnetLabs. Es razonablemente compatible con BIND, es decir, pudiera tenerse un servidor maestro con BIND y un esclavo con NSD o viceversa. Además, consume considerablemente menos memoria que BIND, y al estar concebido solo como servidor autoritario puede resultar potencialmente más seguro.

NSD utiliza una base de datos para almacenar los registros, lo cual permite un inicio rápido del servicio y facilita la detección de errores sintácticos y estructurales en los archivos de zonas, antes que se proporcionen al servicio. Actualmente algunos [rootservers](#) están utilizando NSD en lugar de BIND, lo cual ya dice bastante sobre la eficiencia, seguridad y robustez de esta aplicación.

Preparativos para la configuración del NSD

A los efectos de este tutorial, supongamos que nuestro proveedor de servicios es [ETECSA](#) y que nos ha delegado la zona **dominio.co.cu** y asignado el bloque de direcciones ipv4 200.55.111.5/29, que pretendemos distribuir de la siguiente manera para proporcionar servicios a una WAN:

Dirección IP	Funcionalidad	Hostname
200.55.111.5	Dirección de la red	N/A
200.55.111.6	Router	N/A
200.55.111.7	Servidor DNS maestro	ns1
200.55.111.8	Servidor DNS esclavo	ns2
200.55.111.9	Servidor de correo	mail
200.55.111.10	Servidor de web	www

De modo que vamos a realizar una instalación de NSD en modo maestro y esclavo para que se mantengan sincrónicos.

Instalación

Para instalar este servicio digamos en Debian o derivadas, podemos utilizar el siguiente comando:

```
sudo apt-get install nsd3
```

Adicionalmente, si deseamos podemos crear directorios personalizados para la ubicación de la base de datos y los archivos de zona:

```
cd /etc/nsd3 && sudo mkdir -p db zones
```

Como todos sabemos no en todas las empresas cubanas podemos contar con el equipamiento necesario para montar disimiles servidores, algo que podemos hacer es coger y tener el **BIND** escuchando para nuestra red interna y el **NSD** que no debemos tocar mucho escuchando por la externa. Lo anteriormente lo logramos especificándole al **BIND** que escuche por nuestra IP Interno imaginemos que sea 192.168.0.1, eso lo logramos editando el archivo `/etc/bind/named.conf.options`

```
listen-on {192.168.0.1; 127.0.0.1};
```

Configuración del maestro

Ahora si ya ahora podemos configurar nuestro NSD para que cumpla la función de DNS para la red externa.

Primeramente, editemos el archivo de configuración (por defecto, `/etc/nsd3/nsd.conf`) y coloquemos en su interior algo como esto:

```
server:
  debug-mode: no
  ip4-only: yes
  hide-version: yes
  database: "/etc/nsd3/db/nsd.db"
  logfile: "/var/log/nsd.log"
  difffile: "/etc/nsd3/db/ixfr.db"
  xfrdfile: "/etc/nsd3/db/xfrd.state"
  pidfile: "/var/run/nsd.pid"
  statistics: 3600
  #username: "bind"
  zonesdir: "/etc/nsd3/zones"
  verbosity: 0
  ip-address: 200.55.111.7

zone:
  name: "dominio.co.cu"
  zonefile: "dominio.co.cu.zone"
  provide-xfr: 200.55.111.5/29 NOKEY
  notify: 200.55.111.8 NOKEY
```

```
zone:
  name: "111.55.200.in-addr.arpa"
  zonefile: "dominio.co.cu.reverse1.zone"
  provide-xfr: 200.55.111.5/29 NOKEY
  notify: 200.55.111.8 NOKEY
```

```
zone:
  name: "5/29.111.55.200.in-addr.arpa"
  zonefile: "dominio.co.cu.reverse2.zone"
  provide-xfr: 200.55.111.5/29 NOKEY
  notify: 200.55.111.8 NOKEY
```

Observarán que se ha anclado el servicio a la interfaces de red externa y dejando el **BIND** para la local y la interna. De no incluirse la línea ip-address, el servicio escucha en todas las interfaces. Un detalle importante a tomar en consideración aquí es que cuando tenemos un bloque de direcciones con máscara 29 la cual es la que **ETECSA** nos pone en el contrato, tenemos que utilizar un tipo de delegación llamada "sin clases" que tiene una sintaxis ligeramente más compleja, para esto hemos declarado en la configuración dos zonas inversas. El motivo lo explicaremos más adelante. La opción **notify** pudiera repetirse múltiples veces para notificar sobre cambios en las zonas a más de un esclavo, de haber varios en la misma subred.

Configuración de los archivos de zonas

Zona principal o directa

Editamos ahora el archivo de la zona principal (/etc/nsd3/zones/dominio.co.cu.zone):

```
$ORIGIN dominio.co.cu.
$TTL 1d ; Tiempo de vida por defecto para los registros

@ 0 SOA ns1.dominio.co.cu. hostmaster.dominio.co.cu. (
  2015042501 ; Número de serie (YYYYMMDDNN)
  6h ; Tiempo de refrescar la informacion por parte del esclavo
  1h ; Tiempo de reintento por parte del esclavo en caso de problemas
  4w ; Tiempo de expiracion de la información por parte del esclavo
  3h ; Tiempo que deben permanecer cacheadas las respuestas negativas
)

NS ns1.dominio.co.cu.
NS ns2.dominio.co.cu.
MX 10 mail.dominio.co.cu.
TXT "v=spf1 ip4:200.55.111.9/32 a mx ptr mx:mail.dominio.co.cu include:dominio.co.cu -all"
SPF "v=spf1 ip4:200.55.111.9/32 a mx ptr mx:mail.dominio.co.cu include:dominio.co.cu -all"
TXT "Empresa ....."
TXT "E-Mail: hostmaster at dominio.co.cu"
TXT "Voice: +53-(*)*****"

_jabber._tcp.dominio.co.cu. IN SRV 5 0 5269 web.dominio.co.cu.
_xmpp-server._tcp.dominio.co.cu. IN SRV 5 0 5269 web.dominio.co.cu.
_conferencia._tcp.dominio.co.cu. IN SRV 5 0 5269 web.dominio.co.cu.
_xmpp-client._tcp.dominio.co.cu. IN SRV 5 0 5222 web.dominio.co.cu.

_domainkey.dominio.co.cu. IN TXT "o=~; r=hostmaster@dominio.co.cu"
mail._domainkey.dominio.co.cu. IN TXT "v=DKIM1; k=rsa: *****"
_dmarc.dominio.co.cu. IN TXT "v=DMARC1; p=none; rua=mailto: hostmaster@dominio.co.cu; ruf=mailto: hostmaster@dominio.co.cu; adkim=r; aspf=r"

router A 200.55.111.6
ns1 A 200.55.111.7
ns2 A 200.55.111.8
ns CNAME ns1
mail A 200.55.111.9
www A 200.55.111.10
webmail CNAME mail
* CNAME www
```

IMPORTANTE: Se recomienda que el FQDN del Server del Correo de la empresa se mantenga el que **ETECSA** configuro cuando se hizo el contrato pues algunos servidores de correo tienen una seguridad pues tienen que coincidir siempre el FQDN, el MX y la inversa del IP y el hostname que tenga configurado en el server de Correo, también es recomendando que a la cuenta del administrador de la red se le cree los alias "hostmaster@dominio.co.cu", "postmaster@dominio.co.cu", "abuse@dominio.co.cu" estas son cuentas de correo predeterminada en algunos sistemas de comprobación y de seguridad en todo el mundo. Como notarán, se ha incluido un registro para habilitar la protección SPF, DomainKEY, DMARC en nuestro servicio de correo donde se configura poniendo el FQDN del servidor de correo y el dominio (ver el documento [RFC4408](#)). También se crearon registros TXT para dar a conocer algunas informaciones de contacto de la Empresa, se crearon los registros SRV para el jabber de modo que el mismo correo de los usuarios será el del jabber, se ha creado un registro de tipo CNAME para el nombre **ns** (algunas veces las consultas buscan este *nameserver* en particular), y al final se ha colocado otro CNAME con un comodín, lo cual simplemente significa que cualquier petición a un subdominio inexistente, apuntará en su lugar hacia el sitio web. Para más información sobre la configuración de un DNS, consultar los documentos [RFC1033](#), [RFC1034](#) y [RFC1035](#). Adicionalmente, resulta conveniente consultar el documento [RFC1912](#) para evitar errores que suelen cometerse.

Los valores de tiempo pueden establecerse en segundos (la norma) o mediante abreviaturas que pueden combinarse (por ejemplo, 2h30m) y se permiten tanto en minúsculas como mayúsculas:

Abreviatura	Significado	Equivalente en segundos
m	minuto	60
h	hora	3600
d	día	86400
w	semana	604800

Nota Importante: Un detalle que conviene aclarar: el tiempo de vida por defecto para los registros (establecido en la variable TTL que aparece al principio del archivo de zona) es uno de los valores más importantes a tener en cuenta, pues define el tiempo tras el cual los clientes deben actualizar la información que tienen en su cache, y también define cuan rápidamente los cambios en nuestro dominio se propagarán a los *nameservers* padres. Si la información de nuestro dominio cambia con relativa frecuencia, puede ser conveniente un valor bajo, pero si este no es el caso y especialmente si tenemos una red con muchos equipos, puede mejorarse el rendimiento aumentando este valor hasta un día, una semana, o más (el límite máximo permisible es $2^{31} - 1$, es decir 2147483647, ¡unos 68 años!). Aumentar el valor del TTL reduce las consultas de DNS y hace que los servicios (navegación y demás) funcionen ligeramente más rápido. Un buen truco puede ser mantener el TTL por defecto en un valor relativamente alto (digamos de uno a varios días) y cuando tengamos previsto hacer cambios en el DNS, reducir el TTL unos días antes a un valor bajo (digamos entre unos minutos y una hora), de esta manera cuando se realicen los cambios en el DNS, todos los clientes y *nameservers* padres se actualizarán rápidamente, luego podrá aumentarse nuevamente el TTL a su valor para "producción". Por cierto, si bien según el documento [RFC1035](#) el registro SOA debe tener un TTL de valor cero para evitar que se cachee, posteriormente el documento [RFC2181](#) clarificó que esto no es un requerimiento.

Otra cosa a tener presente es que el último valor del registro SOA originalmente se conocía como Default TTL o Minimum TTL, pero su efecto ha cambiado con el paso del tiempo y actualmente (de acuerdo al documento [RFC2308](#)) se utiliza para definir el tiempo que deben almacenarse en la cache las respuestas negativas (se recomienda un valor entre 1 y 3 horas), de modo que ya no debería utilizarse este campo para establecer el valor predeterminado o mínimo de los registros.

Obviamente, cualquier cambio en los archivos de zonas requiere actualizar también el número de serie, para que el *nameserver* esclavo se sincronice debidamente. Y a propósito del esclavo, conviene tener en el registro SOA un valor de expiración alto, de esta manera si el servidor primario falla, el esclavo tendrá una copia en la cache que durará por el tiempo que se haya definido en el valor de expiración. Mantener *nameservers* secundarios con un valor de expiración bajo contradice el propósito de estos.

Zonas inversas

Pasemos ahora a la delegación de la zona inversa. Algo importante a tomar en consideración aquí es que la delegación de zonas inversas usualmente se realiza para las redes con máscaras 8, 16 ó 24. Sin embargo, como vimos anteriormente **ETECSA** normalmente nos asignado un bloque de direcciones ipv4 con máscara 29 (8 direcciones con 6 utilizables, de ellas una para el router). ¿Qué hacer entonces? Bueno, pues para las máscaras 25 o superiores, debe implementarse algo conocido como delegación sin clases (para más detalles, ver el documento [RFC2317](#)). No todas las implementaciones de DNS permiten este tipo de delegación, pero afortunadamente, NSD sí las permite.

Sin más, declaremos entonces nuestra primera zona inversa (/etc/nsd3/zones/dominio.co.cu.reverse1.zone):

```
$ORIGIN 111.55.200.in-addr.arpa.
$TTL 1d ; Tiempo de vida por defecto para los registros

@ 0 SOA ns1.dominio.co.cu. hostmaster.dominio.co.cu. (
2015042501 ; Número de serie (YYYYMMDDNN)
6h ; Tiempo de refrescar la información por parte del esclavo
1h ; Tiempo de reintento por parte del esclavo en caso de problemas
4w ; Tiempo de expiración de la información por parte del esclavo
3h ; Tiempo que deben permanecer cacheadas las respuestas negativas
)

NS ns1.dominio.co.cu.
NS ns2.dominio.co.cu.

6 CNAME 6.111/29
7 CNAME 7.111/29
8 CNAME 8.111/29
9 CNAME 9.111/29
10 CNAME 10.111/29
```

Como podemos apreciar, hemos colocado registros de tipo CNAME a las verdaderas direcciones inversas que nos han asignado (no es imprescindible colocar la dirección completa, ya que el sistema es capaz de hacer el completamiento automáticamente gracias a la variable ORIGIN definida al inicio de la zona). El único propósito de esta zona es replicar la delegación sin clases que usualmente hace el proveedor (en este caso, **Etecsa**) para que en caso de hacerse una consulta a la zona inversa desde una PC en la misma subred de direcciones que nos han asignado, la respuesta apunte hacia las direcciones correctas, de lo contrario podríamos encontrar problemas con las búsquedas inversas.

En el segundo archivo de zona inversa (/etc/nsd3/zones/dominio.co.cu.reverse2.zone), colocaremos los verdaderos registros para resolver las direcciones ip a sus nombres de dominio.

```
$ORIGIN 111/29.255.55.200.in-addr.arpa.
$TTL 1d ; Tiempo de vida por defecto para los registros

@ 0 SOA ns1.dominio.co.cu. hostmaster.dominio.co.cu. (
2015042501 ; Número de serie (YYYYMMDDNN)
6h ; Tiempo de refrescar la información por parte del esclavo
1h ; Tiempo de reintento por parte del esclavo en caso de problemas
4w ; Tiempo de expiración de la información por parte del esclavo
3h ; Tiempo que deben permanecer cacheadas las respuestas negativas
)

NS ns1.dominio.co.cu.
NS ns2.dominio.co.cu.

6 PTR router.dominio.co.cu.
7 PTR ns1.dominio.co.cu.
8 PTR ns2.dominio.co.cu.
9 PTR mail.dominio.co.cu.
10 PTR www.dominio.co.cu.
```

Inicialización del servicio

Con lo anterior, el servicio debería quedar configurado. Ahora, generemos la base de datos:

```
sudo nsdc rebuild
```

Este comando en realidad lo que hace es llamar al comando zonec, que también podemos invocar directamente con parámetros:

```
sudo zonec -vv
```

La ventaja de disponer de estos comandos es que antes de iniciar el servicio, se realiza una validación básica de la configuración y las zonas.³⁾ Una vez generada la base de datos con los registros de nuestras zonas, iniciamos el servicio:

```
sudo nsdc start
```

Podríamos comprobar si el servicio se está ejecutando con el siguiente comando:

```
ps ax | grep -v grep | grep nsd
```

Deberían aparecer uno o más procesos, lo cual significa que el servicio está ejecutándose. Otra variante que también podría utilizarse:

```
sudo nsdc running
```

Si el servicio se está ejecutando, el comando anterior no devuelve nada, en caso contrario devuelve un mensaje indicando que el servicio está detenido.

Configuración del esclavo

La instalación y configuración del equipo esclavo es muy parecida a la del maestro, excepto que no es necesario llenar las zonas, sino solamente ajustar el archivo de configuración:

```
server:
  debug-mode: no
  ip4-only: yes
  hide-version: yes
  database: "/etc/nsd3/db/nsd.db"
  logfile: "/var/log/nsd.log"
  difffile: "/etc/nsd3/db/ixfr.db"
  xfrdfile: "/etc/nsd3/db/xfrd.state"
  pidfile: "/var/run/nsd.pid"
  statistics: 3600
  #username: "bind"
  zonesdir: "/etc/nsd3/zones"
  verbosity: 0
  ip-address: 200.55.111.8

zone:
  name: "dominio.co.cu"
  zonefile: "dominio.co.cu.zone"
  allow-notify: 200.55.111.7 NOKEY
  request-xfr: AXFR 200.55.111.7 NOKEY

zone:
  name: "111.55.200.in-addr.arpa"
  zonefile: "dominio.co.cu.reverse1.zone"
  allow-notify: 200.55.111.7 NOKEY
  request-xfr: AXFR 200.55.111.7 NOKEY

zone:
  name: "5/29.111.55.200.in-addr.arpa"
  zonefile: "dominio.co.cu.reverse2.zone"
  allow-notify: 200.55.111.7 NOKEY
  request-xfr: AXFR 200.55.111.7 NOKEY
```

Como podemos apreciar, las cláusulas "zone:" en lugar de tener las opciones **provide-xfr** y **notify** como en el maestro, tienen como contraparte las opciones **allow-notify** y **request-xfr**, para especificar respectivamente qué equipos pueden enviar notificaciones y a cuáles consultar para buscar actualizaciones en las zonas.

Configuración con un solo servidor

Las configuraciones antes mostradas es como debería ser pero como todos sabemos en Cuba no siempre podemos contar con el equipamiento que quisiéramos ahora comporto con ustedes que cambios habría que haber en caso que nada mas contemos con un servidor.

Imaginemos que solo tenemos solamente el servidor de correo es decir el server **mail.dominio.co.cu** con el IP **200.55.111.9**

En las configuraciones cambiara lo siguiente:

1- Primeramente, editemos el archivo de configuración (por defecto, `/etc/nsd3/nsd.conf`) y coloquemos en su interior algo como esto:

```
server:
  debug-mode: no
  ip4-only: yes
  hide-version: yes
  database: "/etc/nsd3/db/nsd.db"
  logfile: "/var/log/nsd.log"
  difffile: "/etc/nsd3/db/ixfr.db"
  xfrdfile: "/etc/nsd3/db/xfrd.state"
  pidfile: "/var/run/nsd.pid"
  statistics: 3600
  #username: "bind"
  zonesdir: "/etc/nsd3/zones"
  verbosity: 0
  ip-address: 200.55.111.9
```

```

zone:
  name: "dominio.co.cu"
  zonefile: "dominio.co.cu.zone"
  provide-xfr: 200.55.111.5/29 NOKEY

zone:
  name: "111.55.200.in-addr.arpa"
  zonefile: "dominio.co.cu.reverse1.zone"
  provide-xfr: 200.55.111.5/29 NOKEY

zone:
  name: "5/29.111.55.200.in-addr.arpa"
  zonefile: "dominio.co.cu.reverse2.zone"
  provide-xfr: 200.55.111.5/29 NOKEY

```

2- Editemos ahora el archivo de la zona principal (/etc/nsd3/zones/dominio.co.cu.zone):

```

$ORIGIN dominio.co.cu.
$TTL 1d ; Tiempo de vida por defecto para los registros

@ 0 SOA mail.dominio.co.cu. hostmaster.dominio.co.cu. (
  2015042501 ; Número de serie (YYYYMMDDNN)
  6h ; Tiempo de refrescar la información por parte del esclavo
  1h ; Tiempo de reintento por parte del esclavo en caso de problemas
  4w ; Tiempo de expiración de la información por parte del esclavo
  3h ; Tiempo que deben permanecer cacheadas las respuestas negativas
)

NS mail.dominio.co.cu.
MX 10 mail.dominio.co.cu.
TXT "v=spf1 ip4:200.55.111.9/32 a mx ptr mx:mail.dominio.co.cu include:dominio.co.cu -all"
SPF "v=spf1 ip4: 200.55.111.9/32 a mx ptr mx:mail.dominio.co.cu include:dominio.co.cu -all"
TXT "Empresa ....."
TXT "E-Mail: hostmaster at dominio.co.cu"
TXT "Voice: +53-(*)*****"

_jabber._tcp.dominio.co.cu. IN SRV 5 0 5269 mail.dominio.co.cu.
_xmpp-server._tcp.dominio.co.cu. IN SRV 5 0 5269 mail.dominio.co.cu.
_conferencia._tcp.dominio.co.cu. IN SRV 5 0 5269 mail.dominio.co.cu.
_xmpp-client._tcp.dominio.co.cu. IN SRV 5 0 5222 mail.dominio.co.cu.

_domainkey.dominio.co.cu. IN TXT "o=~; r=hostmaster@dominio.co.cu"
mail._domainkey.dominio.co.cu. IN TXT "v=DKIM1; k=rsa; *****"
_dmarc.dominio.co.cu. IN TXT "v=DMARC1; p=none; rua=mailto: hostmaster@dominio.co.cu; ruf=mailto: hostmaster@dominio.co.cu; adkim=r; aspf=r"

router A 200.55.111.6
mail A 200.55.111.9
ns CNAME mail
webmail CNAME mail
www CNAME mail
* CNAME mail

```

3- Sin más, declaremos entonces nuestra primera zona inversa (/etc/nsd3/zones/dominio.co.cu.reverse1.zone):

```

$ORIGIN 111.55.200.in-addr.arpa.
$TTL 1d ; Tiempo de vida por defecto para los registros

@ 0 SOA mail.dominio.co.cu. hostmaster.dominio.co.cu. (
  2015042501 ; Número de serie (YYYYMMDDNN)
  6h ; Tiempo de refrescar la información por parte del esclavo
  1h ; Tiempo de reintento por parte del esclavo en caso de problemas
  4w ; Tiempo de expiración de la información por parte del esclavo
  3h ; Tiempo que deben permanecer cacheadas las respuestas negativas
)

NS mail.dominio.co.cu.

6 CNAME 6.111/29
9 CNAME 9.111/29

```

4-En el segundo archivo de zona inversa (/etc/nsd3/zones/dominio.co.cu.reverse2.zone), colocaremos los verdaderos registros para resolver las direcciones ip a sus nombres de dominio.

```

$ORIGIN 111/29.255.55.200.in-addr.arpa.
$TTL 1d ; Tiempo de vida por defecto para los registros

@ 0 SOA mail.dominio.co.cu. hostmaster.dominio.co.cu. (
  2015042501 ; Número de serie (YYYYMMDDNN)
  6h ; Tiempo de refrescar la información por parte del esclavo
  1h ; Tiempo de reintento por parte del esclavo en caso de problemas
  4w ; Tiempo de expiración de la información por parte del esclavo
  3h ; Tiempo que deben permanecer cacheadas las respuestas negativas
)

NS mail.dominio.co.cu.

6 PTR router.dominio.co.cu.
9 PTR mail.dominio.co.cu.

```

Comprobación

Ahora podríamos realizar algunas comprobaciones del servicio DNS con comandos como dig, host o nslookup. Por ejemplo:

```
dig @200.55.111.7 dominio.co.cu. any +norecurse +multiline
host -t any dominio.co.cu 200.55.111.7
nslookup -q=any dominio.co.cu 200.55.111.7
nslookup 200.55.111.7 200.55.111.7
drill dominio.co.cu. @200.55.111.7 any
```

Incluso, NLnetLabs ha desarrollado una librería independiente llamada [ldns](#) que proporciona entre otras cosas el comando drill, una alternativa para hacer consultas que no depende de las librerías de BIND (a diferencia de dig), ni tampoco está anclado a NSD. Para instalar la librería, podemos ejecutar el siguiente comando:

```
sudo apt-get install ldnsutils
```

Utilizar entonces el comando drill es sencillo:

```
drill dominio.co.cu. @200.55.111.7 any
```

Notas

Este tutorial pudiera ampliarse con la utilización de IXFR y DNSSEC, la ejecución de NSD de forma *chrooted*, el uso de direcciones ipv6, la interacción de NSD con BIND, etc.