Configuración de un servidor DNS autorizado

Operaciones y Seguridad
de DNS Avanzado

Repaso

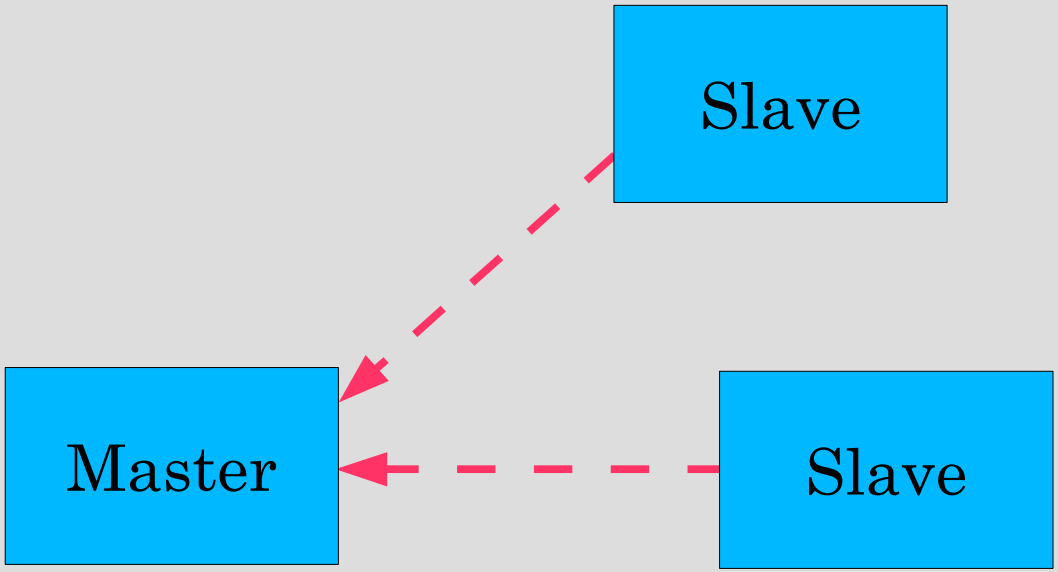
- DNS = Base de datos distribuída
- El *resolver* le pregunta al servidor *recursivo*
- El recursivo atraviesa el árbol de delegación para encontrar el servidor autorizado para entregar la información en cuestión
- La mala configuración de los servidores autorizados puede causar que los dominios no estén disponibles

Replicación en DNS

- Para cada dominio, necesitamos más de un servidor autorizado para ofrecer la misma información (RFC 2182)
- Los datos se introducen en un servidor (maestro) y se replican en otros (esclavos)
- El mundo exterior no puede ver quién es el maestro y cuáles son los esclavos
  - Los récords NS se entregan ordenados al azar para distribuir la carga
- Se solía hablar de “primarios” y “secundarios”

Los esclavos se conectan al maestro para copiar la información

- El maestro no “empuja” los datos a los esclavos



Cuándo se hacen las copias?

- Los esclavos interrogan al maestro periódicamente – ésto es el "Intervalo de actualización (refresh interval)" – para obtener actualizaciones
  - Originalmente éste era el único mecanismo
- El maestro también puede notificar a los esclavos cuando hay cambios
  - Las actualizaciones se sincronizan más rápido
- La notificación no es confiable (la red puede perder un paquete) así que aún es necesario interrogar periódicamente

Números de serie

- Toda zona tiene un número de serie
- El esclavo sólo iniciará la copia cuando este número *AUMENTA*
  - Petición periódica sobre UDP
  - Si hay un número mayor, iniciar transferencia sobre TCP
- Es su responsabilidad incrementar el número de serie con cada cambio. De lo contrario habrá inconsistencia con los datos en los esclavos

Números de serie

- Toda zona tiene un número de serie
- El esclavo sólo iniciará la copia cuando este número *AUMENTA*
  - Petición periódica sobre UDP
  - Si hay un número mayor, iniciar transferencia sobre TCP
- Es su responsabilidad incrementar el número de serie con cada cambio. De lo contrario habrá inconsistencia con los datos en los esclavos

Formato recomendado: YYYYMMDDNN

- YYYY = año
- MM = mes (01-12)
- DD = día (01-31)
- NN = Número de cambio en el día (00-99)
  - e.g. Si cambia el fichero el 5 de marzo de 2004, el número de serie será 2004030500. Si lo hace de nuevo el mismo día, será 2004030501.

Número de serie: Peligro #1

- Si por error usted *decrementa* el número, los esclavos *nunca actualizarán* hasta que el número sea mayor que el valor anterior
- En el RFC1912, sección 3.1 se explica un método para resolver este problema
- En el peor de los casos, puede contactar a los administradores de los esclavos y pedirles que borren la copia de la zona

Número de serie: Peligro #2

- # Serie es un entero de 32 bits sin signo
- Rango: 0 a 4,294,967,295
- Cualquier valor mayor que éste será truncado en silencio
- ej. 20040305000 (fíjese en el dígito extra)
  = 4AA7EC968 (hex)
  = AA7EC968 (32 bits)
  = 2860435816
- Si comete este error, y luego lo corrige, el número de serie habrá decrementado

Configuración del maestro

- */etc/namedb/named.conf* apunta al fichero de zona (creado manualmente)
- Elija un nombre y lugar apropiado
  - ej. /etc/namedb/master/tiscali.co.uk
  - o /etc/namedb/master/uk.co.tiscali

```
zone "example.com" {
        type master;
        file "master/example.com";
        allow-transfer { 192.188.58.126;
                         192.188.58.2; };
};
```

Configuración del esclavo

- *named.conf* hace referencia a la IP del maestro y el lugar donde se guardará la copia de la zona
- Las zonas esclavas se copian automáticamente

```
zone "example.com" {
        type slave;
        masters { 192.188.58.126; };
        file "slave/example.com";
        allow-transfer { none; };
};
```

Maestro y Esclavo

- Es perfectamente válido que un servidor sea maestro para algunas zonas y esclavo para otras
- Por ello es buena idea mantener las zonas en directorios separados
  - /etc/namedb/master/
  - /etc/namedb/slave/
    - (este directorio slave debe tener permisos adecuados para que el demonio pueda guardar la zona)

allow-transfer { ... }

- Una máquina externa puede solicitar la transferencia de una zona completa
- Usted puede controlar qué sistemas pueden obtener (transfer) una copia de la zona.
- Por defecto, sólo los servidores listados en la zona (NS) pueden
- Puede configurar un valor global por defecto, y especificar valores por zona si quiere

```
options {
    allow-transfer { 127.0.0.1; };
};
```

Estructura de un fichero de zona

- Opciones globales
  - $TTL 1d
  - Configura el TTL por defecto para todos los récords
- Record SOA
  - "Start Of Authority" – Inicio de Autoridad
  - Información pertinente a la zona completa
- Records NS
  - Lista de todos los servidores de la zona, maestros y esclavos
- Otros Records
  - Los datos que usted quiere publicar

Formato de un record

www	3600	IN	A	212.74.112.80
Domain	*TTL*	*Class*	*Type*	*Data*

- Uno por línea (excepto el SOA, que puede extenderse a varias líneas)
- Si omite el nombre de dominio, es el mismo de la línea anterior
- Abreviaciones de TTL: ej. 60s, 30m, 4h, 1w2d
- Si omite el TTL, se usará el valor por defecto $TTL
- Si omite la clase, se usa IN
- El tipo de record y el valor no se pueden omitir
- Comentarios con PUNTO-Y-COMA (;)

Atajos

- Si el nombre de dominio no termina en *punto*, se añade el dominio de la zona misma ("origin")
- El nombre "@" significa el nombre del dominio mismo
- ej. en el fichero para example.com:
  - `@` significa `example.com.`
  - `www` significa `www.example.com.`

Si escribe esto...

```
$TTL 1d
@                                   SOA ( ... )
                                    NS  ns0
                                    NS  ns0.as9105.net.

; Main webserver
www                                 A   212.74.112.80
                                    MX  10 mail
```

... se convierte en

```
example.com.        86400   IN  SOA ( ... )
example.com.        86400   IN  NS  ns0.example.com.
example.com.        86400   IN  NS  ns0.as9105.net.
www.example.com.    86400   IN  A   212.74.112.80
www.example.com.    86400   IN  MX  10 mail.example.com.
```

Formato del record SOA

```
$TTL 1d

@  1h  IN  SOA  ns1.example.net. hervey@nsrc.org. (
              2004030300      ; Serial
              8h              ; Refresh
              1h              ; Retry
              4w              ; Expire
              1h )            ; Negative

       IN  NS  ns1.example.net.
       IN  NS  ns2.example.net.
       IN  NS  ns1.othernetwork.com.
```

Formato del record SOA

- `ns1.example.net.`
  - Nombre del servidor maestro
- `hervey@nsrc.org.`
  - E-mail de la persona responsable, terminado en punto.
  - En versiones antiguas "@" se cambiaba por “.”
- Número de serie
- Intervalo de actualización (refresh)
  - Con qué frecuencia el esclavo debe revisar el número de serie del maestro
- Intervalo de reintento (retry)
  - Con qué frecuencia reintentar si el servidor maestro no responde

Formato del record SOA

- Tiempo de caducidad (expiry)
  - Si el esclavo no puede comunicarse con el maestro durante este intervalo, debe borrar su copia de la zona
- Negativo / Mínimo
  - Versiones antiguas interpretaban éste como el valor mínimo del TTL
  - Ahora se usa para la memoria de respuestas negativas: por cuanto tiempo puede recordarse la no-existencia de un récord
- RIPE-203 tiene varlores recomendados
  - http://www.ripe.net/ripe/docs/dns-soa.html

Formato de los récords NS

- Lista de todos los servidores de la zona - maestro y esclavo(s)
- Debe ser un NOMBRE, no una IP

```
$TTL 1d

@  1h  IN  SOA  ns1.example.net. brian.nsrc.org. (
              2004030300      ; Serial
              8h              ; Refresh
              1h              ; Retry
              4w              ; Expire
              1h )            ; Negative

       IN  NS  ns1.example.net.
       IN  NS  ns2.example.net.
       IN  NS  ns1.othernetwork.com.
```

Formato de otros récords

- `IN  A  1.2.3.4`
- `IN  MX  10 mailhost.example.com.`
  - Este número es un "valor de preferencia". El correo se enviará al servidor con menor valor MX
  - Debe usarse NOMBRE y no IP
- `IN  CNAME  host.example.com.`
- `IN  PTR  host.example.com.`
- `IN  TXT  "cualquier cosa"`

Cuando agregue o cambie una zona:

- Recuerde incrementar el número de serie!
- `named-checkzone example.com \ /etc/namedb/master/example.com`
  - Disponible en BIND 9
  - Detecta errores de sintaxis; corríjalos!
- `named-checkconf`
  - Detecta errores en named.conf
- `rndc reload`
  - o: `rndc reload example.com`
- `tail /var/log/messages`

Estas comprobaciones son ESENCIALES

- Si tiene un error en named.conf o en un fichero de zona, named quizá continuará su ejecución pero no será autorizado para la(s) zona(s)
- Se convertirá en un “lame” para la zona sin saberlo
- Los esclavos no serán capaces de comunicarse con el maestro
- En algún momento (ej. 4 semanas después) la zona caducará en los esclavos
- Su dominio dejará de ser visible

Otras comprobaciones

- `dig +norec @x.x.x.x example.com. soa`
  - Compruebe el bit AA
  - Repita para el maestro y todos los esclavos
  - Revise que todos los números de serie corresponden
- `dig @x.x.x.x example.com. axfr`
  - "Authority Transfer"
  - Solicitar una copia completa de la zona sobre TCP, igual que hacen los esclavos
  - Sólo funcionará si su dirección IP está en la sección *allow-transfer {...}*

Ahora tiene servidores autorizados en operación!

- Pero nada de esto tendrá utilidad hasta que tenga la delegación del dominio superior
- O sea, ellos colocan los récords NS en su dominio, apuntando a los servidores de usted
- Usted también ha colocado los récords NS en su zona
- Estos dos conjuntos deberían concordar

Preguntas?

?

Los diez errores más comunes

- Todos los administradores de servidores autorizados deberían leer el RFC 1912
  - Common DNS Operational and Configuration Errors
- Y también el RFC 2182
  - Selection and Operation of Secondary DNS servers

1. Errores de número de serie

- Olvidó incrementar el número de serie
- Incrementó el número de serie, y luego lo decrementó
- Usó un número mayor que 2^{32}
- Impacto:
  - Los esclavos no actualizan la copia
  - Maestros y esclavos terminan con datos incongruentes
  - Las cachés a veces obtendrán los datos válidos y a veces no – problemas intermitentes

2. Comentarios con '#' en lugar de ';'

- Error de sintaxis
- El maestro ya no es autorizado para la zona
- Los esclavos no pueden comprobar el SOA
- Los esclavos en algún momento caducan la zona, y ésta desaparece
- Use "named-checkzone"
- Use "tail /var/log/messages"

3. Otros errores de sintaxis en ficheros de zona

- Ej. Omitir el valor de preferencia en los records MX
- Mismo impacto

4. Olvidar el punto al final

```
; zone example.com.
@  IN  MX 10  mailhost.example.com

Se convierte en

@  IN  MX 10  mailhost.example.com.example.com.
```

```
; zone 2.0.192.in-addr.arpa.
1  IN  PTR    host.example.com

Se convierte en

1  IN  PTR    host.example.com.2.0.192.in-addr.arpa.
```

5. NS o MX con direcciones IP en lugar de nombres

- Deben usar nombres, no IP
- Desafortunadamente, algunos servidores de correo *sí* aceptan direcciones IP en records MX, así que el problema será inconsistente dependiendo del sitio

6. El esclavo no puede recibir la transferencia de zona

- Acceso restringido por allow-transfer {...} y el esclavo no está en la lista
- O existen filtros de paquetes IP erróneos
- El escavo será “lame” (no-autorizado)

7. Delegación “lame” (coja, incorrecta)

- No puede simplemente poner cualquier lista de servidores NS para su dominio
- Debe establecer un acuerdo con el operador del servidor, y ellos tienen que configurarlo como un esclavo para su zona
- En el mejor de los casos: resolución más lenta y no fiable
- En el peor de los casos: fallos intermitentes al resolver su dominio

8. Sin delegación

- Usted configura "example.com" en sus servidores pero el resto del mundo no le enviará solicitudes porque no tiene una delegación
- El problema no será obvio si su servidor está actuando a la vez como autorizado y como recursivo para su dominio
- Sus propios clientes pueden resolver *www.example.com*, pero el resto del mundo no podrá

9. Récords “glue” obsoletos

- Veremos esto más tarde

10. No manejar el TTL correctamente durante los cambios

- ej. Si su TTL es de 24 horas, y usted cambia *www.example.com* para apuntar a un nuevo servidor, habrá un largo período en el cual algunos usuarios recibirán una IP y otros la otra
- Siga el procedimiento:
  - Reduzca el TTL a 10 minutos
  - Espere al menos 24 horas
  - Haga el cambio
  - Restaure el TTL a 24 horas

Práctica

- Cree un nuevo dominio
- Configure servicios maestro y esclavo
- Obtenga la delegación del dominio superior
- Haga pruebas

Parte II – delegación avanzada

Resumen: Cómo se delega un sub-dominio?

- En principio es simple: ponga los récords NS del subdominio, apuntando a los servidores de otros
- Si tiene cuidado, debería primero *comprobar* que dichos servidores son autorizados para el dominio
  - Usando "dig +norec" con cada uno
- Si el subdominio no está bien gestionado, se refleja negativamente en usted!
  - Y usted no quiere lidiar con problemas que no son suyos

Fichero de zona para "example.com"

```
$TTL 1d
@  1h  IN  SOA  ns1.example.net. hervey@nsrc.org. (
              2007112601     ; Serial
              8h             ; Refresh
              1h             ; Retry
              4w             ; Expire
              1h )           ; Negative

       IN  NS  ns1.example.net.
       IN  NS  ns2.example.net.
       IN  NS  ns1.othernetwork.com.

; My own zone data
       IN  MX  10  mailhost.example.net.
www    IN  A   212.74.112.80

; A delegated subdomain
subdom IN  NS  ns1.othernet.net.
       IN  NS  ns2.othernet.net.
```

Aquí hay un problema:

- Los récords NS apuntan a nombres, no IPs
- Qué pasa si la zona "example.com" se delega a "ns.example.com"?
- Quien trate de resolver, digamos, *www.example.com* primero tiene que resolver *ns.example.com*
- Pero para resolver *ns.example.com* primero tienen que resolver *ns.example.com* !

En este caso, necesita un "glue" (pegamento)

- Un "glue record" es un record tipo A para el servidor, ubicado más arriba en la jerarquía
- Ejemplo: Considere los servidores para .com y la delegación para example.com

```
; this is the com. zone

example             NS   ns.example.com.
                    NS   ns.othernet.net.

ns.example.com.     A    192.0.2.1      ; GLUE RECORD
```

No ponga récords “glue” donde no haga falta

- En el ejemplo anterior, *ns.othernet.net* no es un subdominio de *example.com*.
  - Así que el pegamento no hace falta.
- Los records “glue” obsoletos crean problemas
  - ej. al cambiar la dirección del servidor
  - El resultado son problemas intermitentes, difíciles de depurar.

Ejemplo donde el “glue” es necesario

```
; My own zone data
            IN  MX  10  mailhost.example.net.
www         IN  A   212.74.112.80

; A delegated subdomain
subdom      IN  NS  ns1.subdom          ; éste sí
            IN  NS  ns2.othernet.net.   ; éste no
ns1.subdom  IN  A   192.0.2.4
```

Comprobar los records “glue”

- dig +norec ... *y repítalo varias veces*
- Busque los récords tipo A en la sección "Additional" cuyo TTL no decrementa

```
$ dig +norec @a.gtld-servers.net. www.as9105.net. a
 ...
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; QUERY SECTION:
;;      www.as9105.net, type = A, class = IN

;; AUTHORITY SECTION:
as9105.net.          172800  IN    NS         ns0.as9105.com.
as9105.net.          172800  IN    NS         ns0.tiscali.co.uk.

;; ADDITIONAL SECTION:
ns0.as9105.com.      172800  IN    A          212.139.129.130
```

Práctica

- Delegar un subdominio

DNS: Resumen

- Base de datos distribuida de records
  - e.g. A, MX, PTR, ...
- Tres roles: resolver, caché, autorizado
- El resolver se configura estáticamente con los cachés más cercanos
  - e.g. /etc/resolv.conf
- Los cachés tienen un fichero con la lista de los servidores raíz
  - Zona tipo "hint", /etc/namedb/named.root
- Los servidores autorizados contienen los récords para ciertas zonas (como parte del árbol DNS)
  - Con copias para balanceo de carga y fiabilidad

DNS: Resumen

Los servidores raíz contienen delegaciones (records NS) para los gTLD o ccTLD (com, uk etc)

- Estos contienen a su vez más delegaciones
- El recursivo finalmente localiza a un servidor autorizado que contiene los récords buscados
- Los errores en la configuración de los autorizados o en la delegación resulta en que el dominio no es visible, o en errores intermintentes

Referencias

- "DNS and BIND" (O'Reilly)
- Manual de Referencia del Administrador de BIND 9
  - /usr/share/doc/bind9/arm/Bv9ARM.html
- http://www.isc.org/sw/bind/
  - Incluye FAQ, avisos de seguridad
- RFC 1912, RFC 2182
  - http://www.rfc-editor.org/