Operación de DNS

Operación y Seguridad
de DNS

Metas

- Ir más allá de la administración de DNS, enfocarse en estabilidad
- Identificar problemas de operación comunes que afectan a los administradores de servidores autorizados
- Identificar errores comunes al actualizar los archivos de zona
- Definir arquitecturas apropiadas
- Incrementar la disponibilidad y reducir la probabilidad de fallos al utilizar monitorización activa

Visión General

- Herramientas
  - Usar *dig* e interpretar sus resultados
  - doc, dnstop
- Problemas y errores comunes
  - RFC1912, 2182, 2870
  - Delegación y ”glue”, mantenimiento
  - Delegaciones con inconsistencias entre padre/hijo
  - Efectos de la caché
  - Políticas de TTL

Visión General

- Operaciones
  - Bitácoras usando canales de BIND
  - Monitorización de servicios
  - Chequeos activos de delegación
  - Automatización

Herramientas – dig

- dig - *domain information groper*.
- dig se utiliza para interrogar a los servidores DNS, generalmente para depuración de errores.
- dig es mucho más poderoso que otras herramientas como nslookup o host
- La salida de dig puede ser confusa la primera vez que se usa

Herramientas – dig

```
$ dig ns nsrc.org.

; <<>> DiG 9.4.1-P1 <<>> ns nsrc.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40659
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;nsrc.org.          IN   NS

;; ANSWER SECTION:
nsrc.org.      132391    IN   NS   ARIZONA.EDU.
nsrc.org.      132391    IN   NS   RIP.PSG.COM.

;; ADDITIONAL SECTION:
ARIZONA.EDU.        104458    IN   A    128.196.128.233
RIP.PSG.COM.        89057     IN   A    147.28.0.39

;; Query time: 60 msec
;; SERVER: 212.38.128.2#53(212.38.128.2)
;; WHEN: Tue Nov 27 02:58:37 2007
;; MSG SIZE  rcvd: 108
```

Herramientas – dig

- Preste particular atención a las ”flags” y a la sección de la respuesta
- Verifique con dig las zonas padre e hija para comprobar que la delegación es correcta
  Concuerdan los parámetros?
- Ejemplo con cctld.eu.org
  Identificar los servidores para EU.org

  dig ns eu.org.

Herramientas – dig

```
;; ANSWER SECTION:
eu.org.          23772   IN  NS  ns0.pasteur.fr.
eu.org.          23772   IN  NS  ns.eu.org.
eu.org.          23772   IN  NS  ns-slave.free.org.
eu.org.          23772   IN  NS  dns3.gandi.net.
eu.org.          23772   IN  NS  auth1.dns.elm.net.
eu.org.          23772   IN  NS  relay-1.ftel.co.uk.
eu.org.          23772   IN  NS  ns1.pasteur.fr.
```

- Consulte a uno de los servidores los records NS de cctld.eu.org

  dig @ns.eu.org NS cctld.eu.org.

Herramientas – dig

```
;; AUTHORITY SECTION:
cctld.eu.org.          259200   IN   NS   NS1.CATPIPE.NET.
cctld.eu.org.          259200   IN   NS   NS2.CATPIPE.NET.
cctld.eu.org.          259200   IN   NS   NS1.cctld.eu.org.
```

- Fíjese en las *flags*, y la forma en que se presentan las respuestas
- Compruebe que los servidores de cctld.eu.org devuelven la misma información:

  dig @ns1.cctld.eu.org NS cctld.eu.org.
  dig @x0.dk NS cctld.eu.org.

- Se da cuenta de algo?

Herramientas – doc

- Verificar las delegaciones manualmente es tedioso y es propenso a causar errores
- Existe una herramienta que lo hace automáticamente: doc
- Doc se puede instalar como un port o paquete en FreeBSD
- Utilización:

```
doc [-p] domain.name
```

Herramientas – doc

- Pruebe a usar doc – debería estar instalado en el laboratorio

```
doc -p cctld.eu.org
```

Problemas comunes

- La bitácora (log) es la herramienta más útil para depurar problemas en un servidor DNS
- Revise los RFC 1912, 2182 and 2870
- Las delegaciones inconsistentes y los problemas de récords ”glue” se pueden pasar por alto si se utilizan las herramientas inadecuadas
- Las caché complican aún más – los problemas pueden aparecer después.
- Elija una política de TTL razonable

Problemas comunes: cachés

- Efectos de la caché
  Los cambios pueden tardar en propagarse – planifique tomando esto en cuenta
- Política de TTL y SOA
  RIPE tiene un documento con parámetros del SOA recomendados: ftp://ftp.ripe.net/ripe/docs/ripe-203.pdf

```
example.com.  3600  SOA  dns.example.com. admin.example.com. (
                         1999022301   ; serial YYYYMMDDnn
                         86400        ; refresh (  24 hours)
                         7200         ; retry   (   2 hours)
                         3600000      ; expire  (1000 hours)
                         3600 )       ; neg ttl (   1 hour )
```

Problemas comunes: cachés

- Es común malinterpretar/olvidar el valor ”negative TTL” del récord SOA
- ”negative” significa ”Por cuánto tiempo recordar que el récord para esta petición *NO* existe”

Bitácora

- Utilizar *canales* de BIND, categorías y severidades
  Definir canales (file, syslog, ...) y luego asignar categorías a estos canales:

```
logging {
   channel transfers {
      file ”log/transfers” versions 5 size 100M;
      print-time yes;
   };
   category xfer-out {
      transfers;
   };
   category default {
      default_syslog;
      default_debug;
   };
};
```

Bitácora

- Categorías de interés:
  - default
    - Valores por defecto – enviar a syslog
  - lame-servers
    - Delegaciones incorrectas
  - load
    - Eventos de carga de zonas
  - notify
    - Notificaciones de cambios de zona
  - queries
    - Peticiones – Puede ser demasiado!
  - response-checks
    - Respuestas mal formadas, información adicional, ...
  - xfer-in / xfer-out
    - Eventos acerca de las transferencias de zonas

Bitácora

- Configure /etc/namedb/named.conf, y reinicie named

  # rndc reconfig

- Haga una transferencia de zona:

  # dig @ns.of.neighbor axfr zone.name

- Mire en /etc/namedb/log/transfers

  # more /etc/namedb/log/transfers

Monitorización - Servicios

- Monitorizar servicios – por qué?
  Asegúrese de que su servidor está respondiendo con datos correctos, y a tiempo
  Monitorizar los secundarios
  Monitorizar la infraestructura (network, servers, ...)
- Herramientas útiles:
  echoping – Retardo y disponibilidad
  SmokePing – Graficar los tiempos de respuesta
  Nagios – monitorizar los servidores y servicios
  ... etc

Monitorización – exportación de zonas

- Por qué ?
  Evite publicar información incorrecta
  O información incompleta (zona truncada)
  Evite la desaparición de su zona! (errores sin detectar + caducidad de zona)
- Chequeos
  Controles de cambio de zona antes y después de publicación
  - named-checkzone

  Usar marcadores EOD (Datos que su script añade a la zona al final de la exportación

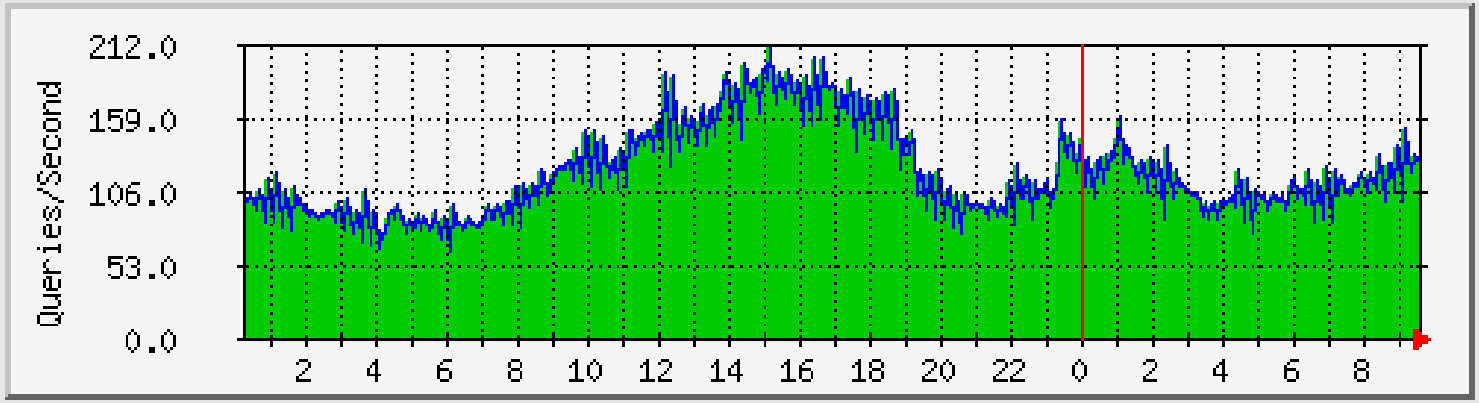
  - zonevalid TXT ”exported at 20071126 09:54”

Monitorización – exportación de zonas

- Errores sin detectar
  - La zona no se carga (sintaxis inválida on inconsistente – *CNAME and other data* por ejemplo)
  - Nadie se da cuenta
  - 2-4 semanas más tarde, la zona caduca en los secundarios
  - La zona desaparece
  - Difícil correlacionar el problema con la causa exacta (a menos que tenga logs)
- Fíjese que si usa ”rndc reload”, BIND mantendrá la zona actual en memoria si la nueva no pasa la validación

Monitorización – marco de referencia

- Familiarícese con su sistema
- Usando herramientas como dnstop, tcpdump, MRTG, establezca un marco de referencia para su plataforma cuando está operando normalmente
- Identifique
  - Peticiones por segundo promedio
  - Utilización de memoria de named



Monitorización – marco de referencia

- Util para planificar capacidad para el crecimiento futuro, y para lidiar con ataques

Chequeos de delegación

- Una decisión de políticas
- Proactiva o reactiva ?
  Chequear regularmente cada delegación
  o chequear cuando la delegación cambia
- Pero hay ventajas
  Evite lidiar con reportes de problemas que no son Su Problema (”dominio XYZ no funciona!”)
- Algunos TLDs tienen un procedimiento de ”Registro de servidor de dominio”.

Consideraciones Secundarias

- Si no lo está haciendo ya, asegúrese de que su servidor SOA es un máster escondido (hidden master), no accessible al resto del mundo
- Ninguno de sus servidores públicos debería servir datos únicos/no-reemplazables.
- Normalmente, todos los servidores públicos son esclavos (pero hay otros métodos, como *secure copy*)

Scripts y automatización

- Debería tratar de aprender al menos un lenguaje de programación de scripts (Shell, Perl, Python, ...)
- Automatizar lo más posible
- Usar herramientas como doc, dig para controlar las delegaciones de zonas críticas

Preguntas ?

?