Эксплуатация DNS

DNS. Эксплуатация
и защита данных.
Продвинутый курс.

Задачи

- Продвинуться дальше основ DNS администрирования, сосредоточение на стабильности сервиса
- Определить общие эксплуатационные проблемы, беспокоящие администраторов авторитетных серверов
- Определить ошибки и ситуации, которых нужно избегать при изменении зон
- Определить надлежащую архитектуру
- Используя активный мониторинг, улучшить доступность и уменьшить шансы поломки сервиса

Обзор

- Инструментарий
  - использование dig и интерпретация результатов
  - doc, dnstop
- Подводные камни и часто встречающиеся проблемы отладки
  - RFC1912, 2182, 2870
  - Делегирование и связки, поддержание их актуальности
  - Противоречивые делегирования (между зоной и зоной более высокого уровня)
  - Эффекты кэширования
  - Правила работы с TTL

Обзор

- Эксплуатация
  - Логирование при помощи каналов BIND
  - Мониторинг сервисов и экспорта зоны
  - Активные проверки делегирования
  - Соображения по поводу распределенного хостинга
  - Автоматизация и скрипты

Инструментарий – использование dig

- dig означает *domain information groper*.
- dig используется для создания запросов к DNS серверам, обычно в отладочных целях.
- dig дает вам такую информацию, и осуществляет такие запросы, которые не могут быть сделаны другими часто используемыми инструментами (nslookup, host)
- Вывод команды dig может на первых порах приводить в замешательство...

Инструментарий – использование 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
```

Инструментарий – использование dig

- Обращайте особое внимание на флаги и на раздел "answer"
- Для проверки правильности делегирования используйте dig на авторитетных серверах родительской и дочерней зон
- Совпадает ли информация?
- Пример для cctld.eu.org
  - Определите серверы для EU.org

```
dig ns eu.org.
```

Инструментарий – использование 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.
```

- Спросите один из этих серверов о записях NS для cctld.eu.org

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

Инструментарий – использование 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.
```

- Обратите внимание на флаги запроса, а также на то, как отображаются ответы
- Убедитесь, что серверы для cctld.eu.org возвращают ту же информацию:

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

- На что вы обратили внимание?

Инструментарий – doc

- Проверка делегирования вручную утомительно и может привести к ошибкам
- Существует инструмент, автоматизирующий эту конкретную проверку: doc
- Doc может быть установлен как порт или пакет
- Использование:

```
doc [-p] имя.домена
```

Инструментарий – doc

- Попробуйте запустить doc – он должен быть установлен.

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

Подводные камни и часто встречающиеся проблемы отладки

- Логгирование – самый полезный инструмент для отладки работающего DNS-сервера – дальше мы увидим, как его настроить
- Посмотрите RFC1912, 2182 и 2870
- Неправильное делегирование и проблемы со связками легко не заметить при пользовании неподходящим инструментарием
- Кэширование усложняет картину – проблемы могут не проявиться сразу.
- Выберите разумные правила работы с TTL

Подводные камни: кэширование

- Эффекты кэширования
  - Распространение изменений может быть достаточно длительным – учитывайте это
- Правила работы с TTL и SOA
  - RIPE создал документ с рекомендованными значениями SOA: 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 часа)
                         7200         ; retry   (   2 часа)
                         3600000      ; expire  (1000 часов)
                         172800 )     ; neg ttl (   2 дня)
```

Подводные камни: кэширование

- Значение отрицательного кэширования в SOA часто недопонимают/забывают
- ”отрицательное” означает ”как долго кэш может помнить, что запись по данному запросу НЕ существует”

Эксплуатация

- Не забудьте отключить рекурсию!
- Логирование
- Мониторинг сервиса (доступность и валидность данных)
- Активные проверки делегирования
- Хостинг и архитектурные соображения

Логирование

- Использование каналов BIND, категорий, и уровней (глава 7.5 книги DNS & Bind)
  - Идея в том, чтобы определить *каналы* (файл, syslog, ...) и назначить *категории* этим каналам:

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

Логирование

- Категории, заслуживающие внимания:
  - default
    - Хороший набор настроек по умолчанию – направьте эту категорию в системный лог (syslog)
  - lame-servers
    - Поломанное делегирование
  - load
    - События загрузки зон
  - notify
    - Уведомления об измененных зонах
  - queries
    - Логирование запросов – может быть много информации
  - response-checks
    - Некорректный вид ответов, дополнительной информации и т.д.
  - xfer-in / xfer-out
    - Скачивания / запросы на скачивание зоны

Логирование

- Добавьте логирование в /etc/namedb/named.conf, и перезапустите named
  ```
  # rndc reconfig
  ```
- Скачайте зону с соседнего сервера:
  ```
  # dig @ns.of.neighbor axfr zone.name
  ```
- Проверьте /etc/namedb/log/transfers
  ```
  # more /etc/namedb/log/transfers
  ```

Мониторинг сервисов

- Мониторинг сервисов – для чего ?
  - Быть уверенным, что ваш сервер выдает правильные ответы, причем вовремя
  - Мониторинг вторичных серверов
  - Мониторинг инфраструктуры DNS-сервиса – сеть, серверы, ...
- Инструментарий для мониторинга:
  - echoping – проверяет доступность и время отклика
  - SmokePing – создает график времени отклика
  - Nagios – мониторинг сервисов и серверов
  - ... и многие другие

Мониторинг экспорта зон

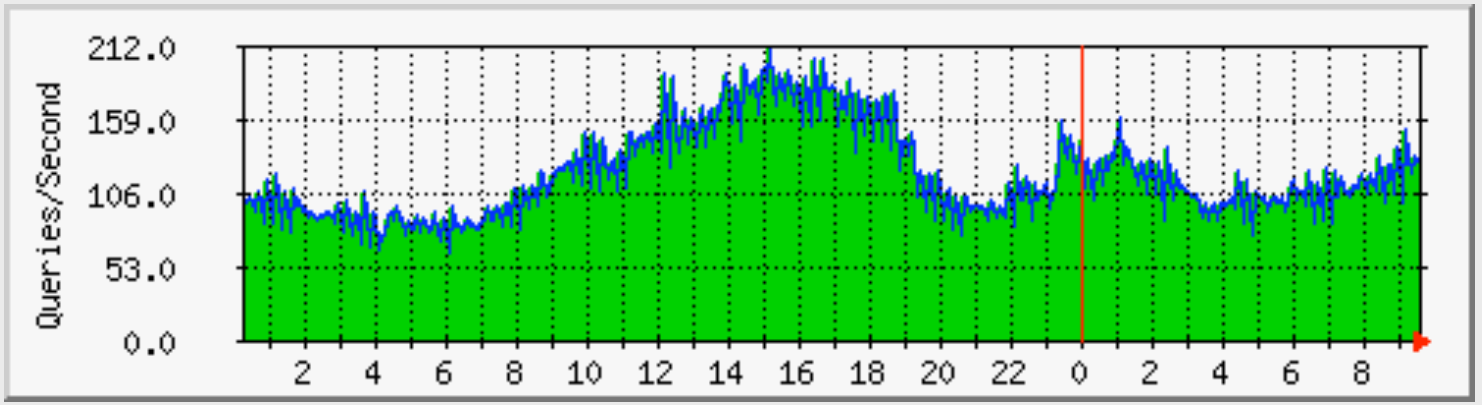
- Мониторинг экспорта зон – для чего?
  - Чтобы не публиковать неправильную информацию
  - Чтобы не публиковать неполную информацию (урезанные зоны)
  - Чтобы не допустить пропадания зоны (необнаруженные ошибки + достижение предельного времени потери контакта)
- Проверки
  - Проверка изменение до И после публикации новой версии зоны
    - named-checkzone
  - Использование маркеров ”конец данных” (данные, который ваш экспортирующий скрипт добавляет в зону в самом конце свое работы
    - zonevalid TXT ”exported at 20071126 09:54”

Мониторинг экспорта зон

- Необнаруженные ошибки
  - Зона не может быть заргужена (неверный синтаксис либо несовместимые записи – например, ”CNAME and other data”)
  - Никто не заметил этого
  - Через 2-4 недели, зона удаляется на слейвах
  - Зона исчезает
  - Тяжело найти, какая именно ошибка привела к проблеме – если у вас нет логов
- Обратите внимание: если используется ”rndc reload”, BIND сохранит копию старой зоны в памяти, если новая не проходит проверку

Мониторинг – базовый уровень

- Знайте особенности вашей системы
- Используя такие инструменты как dnstop, tcpdump, MRTG, определите базовый уровень для вашей платформы когда она функционирует в обычном режиме
- Определите
  - Среднее количество запросов в секунду
  - Сколько памяти использует named



Мониторинг – базовый уровень

- Полезно для планирования ресурсов для будущего роста, и для реагирования на сетевые атаки

Проверка делегирования

- Главным образом стратегическое решение
- Проактивность или реактивность?
  - Регулярная проверка каждого делегирования
  - Либо проверка только при изменениях
- Но есть и преимущества
  - Вы не будете получать сообщения об ошибках, за которые вы не отвечаете (”домен XYZ не работает!”)
- Некоторые домены высшего уровня (TLD) определяют процедуру регистрации DNS-серверов.

Дальнейшие соображения

- Если вы пока еще этого не делаете, убедитесь, что ваш SOA-сервер является "спрятанным мастером", который недоступен для остальной сети
- Ваши публично-доступные серверы не должны предоставлять никакую уникальную либо незаменимую информацию.
- Обычно, все публичные серверы являются слейвами (но есть и другие методы, включая безопасное копирование)

Скрипты и автоматизация

- Вам следует иметь представление хотя бы об одном языке написания скриптов (Shell, Perl, Python, ...)
- Автоматизируйте как можно большее количнство задач
- Для проверки делегирования важных зон используйте такие программы как doc и dig

Вопросы?