Конфигурация авторитетных DNS-серверов

DNS. Эксплуатация
и защита данных.
Продвинутый курс.

Резюме

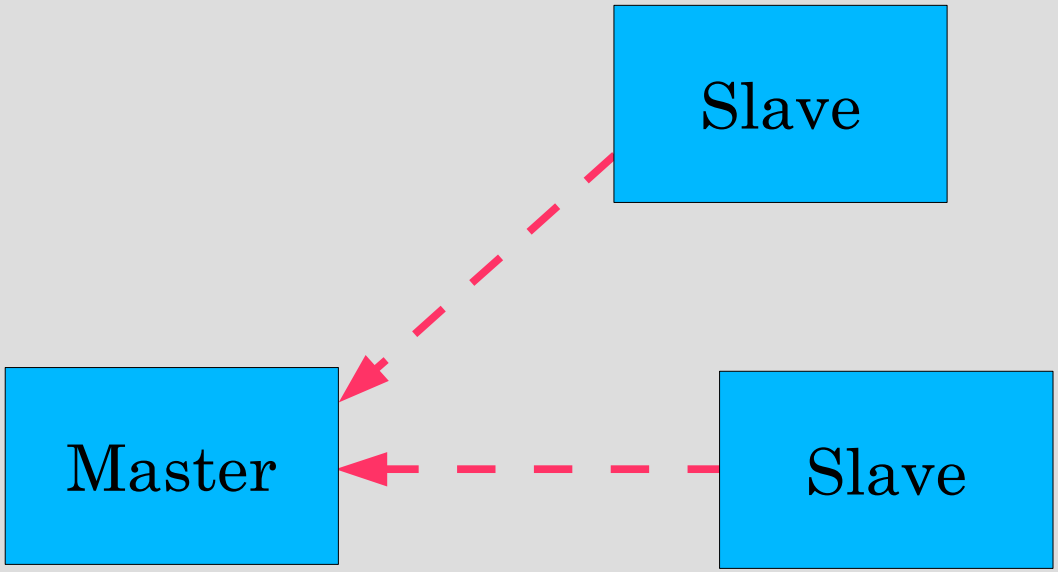
- DNS – распределенная база данных
- Система разрешения имен запрашивает кэширующий сервер
- Кэширующий сервер спускается по дереву DNS делегирования, чтобы найти авторитетный сервер, обладающий запрошенной информацией
- Неправильная конфигурация авторитетных серверов может привести к неработоспособности домена

Репликация DNS

- Для каждого домена требуется более одного авторитетного сервера с одной и той же информацией (RFC 2182)
- Данные вводятся на одном мастер-сервере, и реплицируются на других, подчиненных серверах (“слейвы”)
- Остальной мир не знает разницы между мастером и слейвом
  - записи NS возвращаются в случайном порядке для распределения нагрузки
- Раньше говорили "первичный" и "вторичный"

Слейв запрашивают копию зоны у мастера

- Копирование инициируется слейвом а не мастером



Когда происходи репликация?

- Слейвы периодически (“интервал обновления”) опрашивают мастера чтобы проверить, есть ли новые данные
  - Исходно это был единственный метод
- Мастер также может дать знать слейвам когда данные меняются
  - Это приводит к более быстрому обновлению
- Такое уведомление ненадежно из-за потерь в сети, поэтому слейвам все равно нужно опрашивать мастера с интервалом обновления

Серийные номера

- Каждый файл зоны содержит серийный номер
- Слейв копирует данные только когда этот номер УВЕЛИЧИВАЕТСЯ
  - Периодический UDP-запрос с целью проверки серийного номера
  - Если увеличился, TCP-передача данных зоны
- Увеличивать серийный номер после каждого изменения – ваша ответственность, иначе слейвы не будут синхронизированы с мастером

Рекомендованый формат серийного номера: YYYYMMDDNN

- YYYY = год
- MM = месяц (01-12)
- DD = день (01-31)
- NN = число изменений сегодня (00-99)
  - Например, если вы изменяете файл 5-го марта 2004 года, серийный номер будет 2004030500. Если вы измените файл еще раз в тот же день, серийный номер станет 2004030501.

Серийные номера: опасность 1

- *Если вы когда-либо уменьшите* серийный номер, слейвы *не обновятся* до тех пор пока серийный номер не станет больше предыдущего значения
- RFC1912 раздел 3.1 объясняет, как исправить эту проблему
- В худшем случае вам придется связаться с вашими слейвами и удалить их копию данных зоны

Серийные номера: опасность 2

- Серийный номер – 32-битное неотрицательное число
- Интервал: от 0 да 4,294,967,295
- Любое большее значение будет молча обрезано
- например 20040305000 (лишний 0)
  = 4AA7EC968 (hex)
  = AA7EC968 (32 bits)
  = 2860435816
- Если вы так ошибетесь а потом исправите ошибку, серийный номер уменьшится

Конфигурация мастера

- В /etc/namedb/named.conf прописан файл зоны (созданный вручную), содержащий ваши записи
- Выбирайте логичное место их хранения
  - например /etc/namedb/master/tiscali.co.uk
  - или /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; };
};
```

Конфигурация слейва

- В named.conf прописан IP-адрес мастера и местоположение копии файла зоны
- Файлы зон создаются автоматически
- Не редактируйте их!

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

Мастер и слейв

- Совершенно нормально, когда один и тот же сервер работает мастером для каких-то зон и слейвом для других зон
- Поэтому лучше хранить их в разных каталогах на диске
  - /etc/namedb/master/
  - /etc/namedb/slave/
    - (также, слейв-каталог должен иметь подходящие права для того, чтобы сервер-демон мог создавать в нем файлы)

allow-transfer { ... }

- Удаленные машины могут запрашивать скачивание зоны целиком
- Вы можете определять, кому разрешено скачивать копию зоны.
- По умолчанию, только DNS-серверы, прописанные в самой зоне, могут это делать
- Вы также можете определить значение по умолчанию, и переопределить это значение для каждой зоны, если нужно

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

Структура файла зоны

- Общие параметры
  - $TTL 1d
  - Устанавливает TTL по умолчанию для всех записей
- Запись (RR) SOA
  - "Начало Авторитетности"
  - Служебная информация о зоне
- Записи NS
  - Список всех DNS-серверов для зоны, мастера и всех слейвов
- Прочие записи
  - Реальные данные вы хотите обнародовать

Формат ресурсной записи

www	**3600**	**IN**	**A**	**212.74.112.80**
Домен	*TTL*	Класс	Тип	Данные

- Одна строка – одна запись (кроме SOA, которая может занимать несколько строк)
- Если Домен не указан, он такой-же, как в предыдущей строке
- TTL скоращения, например 60s, 30m, 4h, 1w2d
- Без TTL используется значение по умолчанию, $TTL
- Без Класса, значение по умолчанию “IN”
- Тип и Данные не могут быть опущены
- Комментарии начинаются с “;”

Сокращения

- Если Домен не заканчивается точкой, присоединяется собственный домен зоны “источник”, или “origin”
- Домен "@" означает источник сам по себе
- Например, в файле зоны example.com:
  - `@` означает `example.com.`
  - `www` означает `www.example.com.`

Если вы пишете...

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

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

... то получается

```
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.
```

Формат записи 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.
```

Формат записи SOA

- `ns1.example.net.`
  - имя мастер-сервера
- `hervey@nsrc.org.`
  - E-mail-адрес ответственного лица, с точкой в конце
  - В старых версиях меняли "@" на точку
- Серийный номер
- Интервал обновления
  - Как часто слейв проверяет серийный номер на мастере
- Интервал повтора
  - Как часто слейв проверяет серийный номер, если мастер не отвечает

Формат записи SOA (прод.)

- Предельное время потери контакта
  - Если слейв не может достучаться до мастера в течение этого времени, он удалит свою копию зоны
- Отрицательное кэширование / Минимум
  - Старые версии использовали это как минимальное значение TTL
  - Сейчас это значение говорит, как долго кэш может помнить факт отсутствия записи
- RIPE-203 описывает рекомендованные значения
  - http://www.ripe.net/ripe/docs/dns-soa.html

Формат записей NS

- Список всех авторитетных серверов для зоны – мастер и слейвы
- Должен указывать на ИМЯ ХОСТА, а не на IP адрес

```
$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.
```

Формат прочих записей

- `IN  A  1.2.3.4`
- `IN  MX  10 mailhost.example.com.`
  - Число - “значение предпочтения”. Почта сперва доставляется на MX с наименьшим значением
  - Должно указывать на ИМЯ ХОСТА а не на IP адрес
- `IN  CNAME  host.example.com.`
- `IN  PTR  host.example.com.`
- `IN  TXT  "any text you like"`

Когда вы добавили либо изменили файл зоны:

- Не забудьте увеличить серийный номер!
- `named-checkzone example.com \`
  `/etc/namedb/master/example.com`
  - в bind версии 9
  - Сообщает о синтаксических ошибках в файле зоны; исправьте их!
- `named-checkconf`
  - Сообщает об ошибках в named.conf
- `rndc reload`
  - или: `rndc reload example.com`
- `tail /var/log/messages`

Эти проверки НЕОБХОДИМЫ

- При ошибке в named.conf либо в файле зоны named может продолжать выполнение, но не будет авторитетным для неправильной зоны
- Зона будет отсутствовать, а вы можете об этом и не подозревать
- Слейвы не смогут контактировать с мастером
- В конечно итого (например через 4 недели) слейвы удалят зону
- И ваш домен перестанет работать

Другие возможные проверки

- `dig +norec @x.x.x.x example.com. soa`
  - Проверьте флаг AA
  - Повторите для мастера и для всех слейвов
  - Убедитесь что серийные номера совпадают
- `dig @x.x.x.x example.com. axfr`
  - "Авторитетное Скачивание"
  - Запрашивает полную копию зоны используя TCP, точно так как делают слейвы
  - Это будет работать только с IP-адресов, указанных в разделе allow-transfer {...}

Теперь у вас есть работающие авторитетные серверы!

- Но ничего из этого не будет работать пока у вас нет делегирования от домена более высокого уровня
- То есть, пока они не создадут записи NS для вашего домена, указывающие на ваши сервера
- Вам также следует создать записи NS внутри файла зоны
- Они должны совпадать друг с другом

Вопросы?

?

ГЛАВНЫЕ 19 ОШИБОК при работе с авторитетными серверами

- Всем администраторам авторитетных серверов следует прочитать 1912
  - Основные ошибки эксплуатации и конфигурации DNS
- А также RFC 2182
  - Выбор и эксплуатация вторичных серверов DNS

1. Ошибки в серийных номерах

- Забыли увеличить серийный номер
- Увеличили серийный номер, затем уменьшили его
- Использовали серийный номер больше чем 2^{32}
- Последствия:
  - Слейвы не скачивают зону с мастера
  - Мастер и слейвы не синхронизированы
  - Кэши иногда будут получать новые данные, а иногда – старые

2. Комментарии в файлах зоны начинаются с '#', а не с ';'

- Синтаксическая ошибка в файле зоны
- Мастер более не авторитетен для зоны
- Слейвы не могут проверить SOA
- Слейвы в конечном итоге удалят зону, и домен перестанет работать
- Пользуйтесь "named-checkzone"
- Пользуйтесь "tail /var/log/messages"

3. Другие синтаксические ошибки в файлах зон

- Например, опущено значение предпочтение в записи MX
- Те же последствия

4. Недостающая точка в конце

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

становится

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

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

становится

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

5. NS или MX указывают на IP-адрес

- Они должны указывать на имя хоста, а не на IP адрес
- К сожаление, некоторые почтовые сервера понимают IP-адреса в записях MX, поэтому проблема может не проявляться при работе с некоторыми удаленными серверами

6. Слейв не может скачать зону с мастера

- Доступ ограничен при помощи allow-transfer {...} и слейв не указан
- Или IP-фильтры (брандмауэры) неправильно сконфигурированы
- Слейв не будет иметь копии зоны (не будет авторитетным сервером)

7. Неправильное делегирование

- Вы не может указать произвольные серверы в записях NS для вашего домена
- Вы должны договориться с администраторами слейвов, и они должны сконфигурировать вашу зону как слейв
- В лучшем случае: медленное разрешение имен и отсутствие устойчивости к ошибкам
- В худшем случае: разрешение имен в вашем домене осуществляется с перебоями

8. Отсутствие делегирования

- Вы можете сконфигурировать "example.com" на ваших DNS серверах, но остальной мир не будет их запрашивать до тех пор пока у вас нет делегирования
- Проблема невидима (для вас), если ваши DNS серверы работают и как кэш и как авторитетный сервер
- Ваши собственные клиенты видят www.example.com, в отличие от всех остальных

9. Устаревшие записи-связки

- См. дальше

10. Отсутствие правильного управления TTL во время изменений changes

- Например если TTL равен 24 часам, и в меняете www.example.com, чтобы он указывал на новый сервер, в течение большого времени некоторые пользователи будут запрашивать старую машину, а другие - новую
- Следуйте процедуре:
  - Уменьшите TTL до 10 минут
  - Подождите 24 часа
  - Сделайте изменение
  - Увеличьте TTL опять до 24 часов

Практика

- Создайте новый домен
- Настройте мастера и слейва
- Получите делегирование от домена вышестоящего уровня
- Осуществите тестирование

Часть II – продвинутое делегирование

DNS. Эксплуатация
и защита данных.
Продвинутый курс.

Вкратце: Как вы делегируете поддомен?

- В принципе просто: добавьте записи NS для поддомена, указывающие на чьи-то сервера
- Если вы аккуратны, вначале *проверьте,* что эти сервера авторитетны для поддомена
  - используя "dig +norec" для каждого сервера
- Если поддомен плохо сконфигурирован, это отразится и на вашей репутации!
  - и вы не хотите отвечать на сообщения о чужих ошибках

Файл зоны "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.

; Данные нашей зоны
         IN   MX   10   mailhost.example.net.
www      IN   A    212.74.112.80

; Делегированный поддомен
subdom   IN   NS   ns1.othernet.net.
         IN   NS   ns2.othernet.net.
```

Тут есть одна проблема:

- Записи NS указывают на имена, не IP-адреса
- Что если зона "example.com" делегирована на "ns.example.com"?
- Тот, кто пытается ращрешить имя (например) www.example.com должен вначале разрешить имя ns.example.com
- Но для нахождения ns.example.com ему потребуется найти ns.example.com !

В таком случае нужна запись-”связка”

- "Запись-связка" это запись типа A для DNS-сервера, которая находится в дереве выше
- Пример: рассмотрим сервер для .com, и делегирование для example.com

```
; это зона com.

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

ns.example.com.     A    192.0.2.1      ; запись-связка
```

Не создавайте записи-связки если они не нужны

- В предыдущем примере, "ns.othernet.net" не является поддоменом "example.com".
  - Поэтому связка не нужна
- Устаревшие записи-связки – источник серьезных проблем
  - Например, если сервер DNS меняет IP-адрес
  - Проблема то есть, то ее нет – тяжело отлаживать

Пример, где запись-связка НУЖНА

```
; Данные нашей собственной зоны
            IN  MX  10  mailhost.example.net.
www         IN  A   212.74.112.80

; Делегированный поддомен
subdom      IN  NS  ns1.subdom          ; связка нужна
            IN  NS  ns2.othernet.net.   ; не нужна
ns1.subdom  IN  A   192.0.2.4
```

Проверка записей-связок

- dig +norec *... и повторите несколько раз*
- Ищите записи A в разделе "Additional", такие что их TTL не уменьшается

```
$ 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
```

Практика

- Делегирование поддомена

DNS: сводка

- Распределенная база данных ресурсных записей
  - например A, MX, PTR, ...
- Три роли: система разрешения имен, кэш, авторитетный сервер
- Система разрешения имен сконфигурирована статически, указывает на ближайшие кэши
  - например /etc/resolv.conf
- Кэши хранят список корневых серверов
  - Тип зоны "hint", /etc/namedb/named.root
- Авторитетные сервера содержат ресурсные записи для некоторіх зон (частей дерева DNS)
  - Несколько копий для надежности и распределения нагрузки

DNS: сводка (прод.)

- Корневые серверы содержат делегированые записи NS на gTLD или серверы уровня страны (com, uk etc)
- Те, в свою очередь, содержат делегирования для поддоменов
- Кэш в конечном итоге находит авторитетный сервер, содержащий запрошенные ресурсные записи
- Ошибки в делегировании или в конфигурации авторитетных серверов приводят к отсутствию ответа либо к противоречивым ответам

Дальнейшее чтение

- "DNS and BIND" (O'Reilly)
- BIND 9 Administrator Reference Manual
  - /usr/share/doc/bind9/arm/Bv9ARM.html
- http://www.isc.org/sw/bind/
  - Включает в себя FAQ, security alerts
- RFC 1912, RFC 2182
  - http://www.rfc-editor.org/