Н.Н. Диваков

УО «Гомельский государственный университет
имени Франциска Скорины», Гомель, Беларусь

КОНФИГУРАЦИЯ СЕРВЕРА DNS ДЛЯ IPV6

Введение

DNS обычно реализуется с использованием одного или нескольких централизованных серверов, которые являются авторитетными для определенных доменов. Когда клиент хост запрашивает информацию от сервера имен, как правило, подключается к порту 53. Затем сервер имен пытается разрешить имя запрошенного. Если он не имеет авторитетный ответ, или еще не имеет ответа на вызов закэшированное из ранее запроса, он запрашивает другие серверы имен, называемых корневых серверов имен, чтобы определить, какие серверы имен являются авторитетными имя в вопросе, а затем запрашивает их, чтобы получить запрашиваемое имя.

В DNS-сервере, таким как BIND (Berkeley Internet Name Domain), вся информация хранится в базовых элементах данных, называемые *записи ресурсов* (RR). Запись ресурса, как правило, *полное доменное имя* (FQDN) хоста, и разбита на несколько секций, организованных в виде древовидной иерархии. Эта иерархия состоит из основного ствола, первичных ветвей, вторичных ветвей, и так далее (рисунок 1).

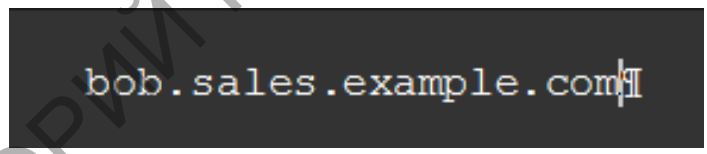

Рисунок 1 – Полное доменное имя

Зоны определяются на полномочных серверов за счет использования файлов зон, которые содержат определения ресурсных записей в каждой зоне. Файлы зон хранятся на первичных серверов имен (также называемый мастер NameServers), где вносятся изменения в файлы, а также вторичных серверов имен (также называемые ведомые NameServers), которые получают определения зоны с первичного сервера имен. И первичные и вторичные серверы имен являются авторитетными для зоны и выглядят одинаково для клиентов. В зависимости от конфигурации, любой сервер имен может также служить в качестве первичного или вторичного сервера для нескольких зон одновременно.

1.Конфигурация сервера

Есть два типа конфигурации сервера имен:

– авторитетные неймсерверов ответ на записи ресурсов, которые являются частью только их зон. Эта категория включает в себя как первичный (основной) и вторичные (Slave) сервера имен;

– рекурсивные неймсерверов предлагают услуги по разрешению, но они не являются авторитетными для любой зоны. Ответы на все резолюции кэшируются в памяти в течение фиксированного периода времени, который определен извлеченной записи ресурса.

Несмотря на то, сервер имен может быть как авторитетный и рекурсивный в то же время, рекомендуется не совмещать типы конфигурации. Для того, чтобы быть в состоянии выполнять свою работу, авторитетные серверы должны быть доступны всем клиентам все время. С другой стороны, так как рекурсивный поиск занимает гораздо больше времени, чем авторитетные ответы, рекурсивные серверы должны быть доступны для ограниченного числа только для клиентов, в противном случае они склонны к распределенный отказ в обслуживании (DDoS) атак.

Файл конфигурации состоит из набора утверждений с вложенными вариантов окруженный путем открытия и закрытия фигурные скобки. Обратите внимание, что при редактировании файла, вы должны быть осторожны, чтобы не делать какие-либо синтаксические ошибки, в противном случае с именемслужбы не запустится. Типичный /etc/named.conf файл организован следующим образом:

```
statement-1 ["statement-1-name"] [statement-1-class] {
  option-1;
  option-2;
  option-N;
};
statement-2 ["statement-2-name"] [statement-2-class] {
  option-1;
  option-2;
  option-N;
};
statement-N ["statement-N-name"] [statement-N-class] {
  option-1;
  option-2;
  option-N;
};
```

Если вы установили связывания-CHROOT пакет, служба BIND будет работать в /var/named/chrootenvironment среды. В этом случае сценарий инициализации будет монтировать вышеуказанные файлы конфигурации, используя the mount --bind команду, так что вы можете управлять конфигурацией вне этой среды. Там нет необходимости копировать что-либо

в /var/named/chroot каталога, так как он установлен автоматически. Это упрощает техническое обслуживание, так как вам не нужно предпринимать каких-либо особой заботы о BIND файлах конфигурации, если он выполняется в CHROOT среде. Вы можете организовать все так, как вы бы с BIND не работает в CHROOT среде.

Следующие каталоги автоматически монтируются в /var/named/chroot, если они пусты в /var/named/chroot каталога. Они должны быть пустым, если вы хотите, чтобы они были установлены в /var/named/chroot:

```
/var/named
/etc/pki/dnssec-keys
/etc/named
/usr/lib64/bind or /usr/lib/bind (architecture dependent).
```

Следующие файлы также установлены , если целевой файл не существует в `/var/named/chroot`.

```
/etc/named.conf
/etc/rndc.conf
/etc/rndc.key
/etc/named.rfc1912.zones
/etc/named.dnssec.keys
/etc/named.iscdlv.key
/etc/named.root.key
```

2.Настройка ACL

Следующие типы заявлений обычно используются в /etc/named.conf:

ACL (Список контроля доступа) оператор позволяет определять группы хостов, так что они могут быть разрешены или запрещен доступ к серверу имен. Он принимает следующий вид:

```
acl acl-name {
  match-element;
  ...
};
```

Имя-ACL имя оператора это имя списка управления доступом, а также матч-элемент вариант, как правило, индивидуальный IP-адрес (например, 10.0.1.1) или CIDR (бесклассовое Inter-Domain Routing) сети обозначения (например, 10.0.1.0/24). ACL утверждение может быть особенно полезно в сочетании с другими операторами, такими как варианты. «Использование ACL в сочетании с опциями" определяет два списка управления доступом, черных шляпах и красных цилиндрах, и добавляет черные цилиндрах на черном списке некоторое время предоставление красно-шляпы нормальный доступ.

```
acl black-hats {
  10.0.2.0/24;
  192.168.0.0/24;
  1234:5678::9abc/24;
};
acl red-hats {
  10.0.1.0/24;
```

```
};
options {
  blackhole { black-hats; };
  allow-query { red-hats; };
  allow-query-cache { red-hats; };
};
```

Включают в себя утверждение позволяет включать файлы в /etc/named.conf , так что потенциально конфиденциальные данные могут быть размещены в отдельном файле с ограниченными разрешениями. Он принимает следующий вид:

```
include "file-name"
```

Имя-файла имя оператора абсолютный путь к файлу.

```
include "/etc/named.rfc1912.zones";
```

Параметры личных данных позволяет определить глобальные параметры конфигурации сервера, а также установить значения по умолчанию для других утверждений. Он может быть использован для определения местоположения с именем рабочего каталога, типы запросов разрешено, и многое другое. Он принимает следующий вид:

```
options {
  option;
  ...
};
```

Чтобы предотвратить распределенный отказ в обслуживании (DDoS) атак, рекомендуется использовать allow-query-cacheопцию, чтобы ограничить рекурсивных услуги DNS для конкретного подмножества только для клиентов.

```
options {
  allow-query       { localhost; };
  listen-on port    53 { 127.0.0.1; };
  listen-on-v6 port 53 { ::1; };
  max-cache-size    256M;
  directory         "/var/named";
  statistics-file   "/var/named/data/named_stats.txt";

  recursion         yes;
  dnssec-enable     yes;
  dnssec-validation yes;
};
```

Вид личных данных позволяет создавать специальные взгляды в зависимости от какой сети хост запрашивая сервер имен включен. Это позволяет некоторые хосты получить один ответ относительно зоны, в то время как другие хосты получают совершенно другую информацию. В качестве альтернативы, некоторые зоны могут быть доступны только для отдельных доверенных хостов, в то время как ненадежный хосты могут только делать запросы для других зон.

Заключение

Как видно ниже, любые имена, используемые в записях ресурсов, которые не заканчиваются в период завершающего добавляются с example.com .
`$ORIGIN example.com.`

$ TTL директива позволяет установить по умолчанию время жить значение (TTL) для зоны, то есть, как долго это запись зона действует. Каждая запись ресурса может содержать свое собственное значение TTL, которое перекрывает эту директиву.

Увеличение этого значения позволяет удаленным неймсерверам кэшировать информацию о зоне в течение более длительного периода времени, уменьшая количество запросов для зоны и удлиняя количество времени, необходимого для распространения изменений записи ресурса.

Следующие записи ресурсов обычно используются в файлах зон: «A». Адрес записи указывает IP-адрес, который будет назначен на имя. Он принимает следующий вид:
hostname IN A *IP-address*

Большинство реализаций BIND использовать только с именем службы для предоставления услуг разрешения имен или выступать в качестве органа для конкретного домена. Тем не менее, BIND версии 9 имеет ряд дополнительных функций, которые позволяют более безопасной и эффективной службы DNS.

Система доменных имен расширений безопасности (DNSSEC) обеспечивает проверку подлинности происхождения данных DNS, подтверждаемое отрицание существования и целостность данных. Когда конкретный домен помечен как безопасный, то SERFVAIL ответ возвращается для каждой записи ресурса, который терпит неудачу проверки.

Если серийный номер не увеличивается, первичный сервер имен будет иметь правильную, новую информацию, но вторичные серверы имен никогда не будут уведомлены об изменениях, и не будет пытаться обновить свои данные этой зоны.

Литература

1. Google Developers [Электронный ресурс]. Discussion Groups and Issue Reporting-Маунтин-Вью, 2004. – Режим доступа: https://developers.google.com /speed/publicdns/docs/using#configure_your_network_settings_to_use_google_public_dns. – Дата доступа: 16.03.2016.

2. Диваков, Н.Н. Настройка DNS / Н.Н. Диваков, П.Л. Чечет // XIX Республиканская Научная конференция студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях». – 2016. – С. 34.

3. Диваков, Н.Н. Переходные механизмы между IPv4 и IPv6 / Н.Н. Диваков, П.Л. Чечет // XIX Республиканская Научная конференция студентов и аспирантов «V Республиканская научная конференция «Актуальные вопросы физики и техники»». – 2016. – С. 75–76.

С.С. Дик, Н.И. Цырельчук, С.М. Боровиков

УО «Белорусский государственный университет
информатики и радиоэлектроники», Минск, Беларусь

МОДЕЛИРОВАНИЕ КАК СПОСОБ ИССЛЕДОВАНИЯ НАДЁЖНОСТИ И ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННЫХ СИСТЕМ

Введение

Одной из важнейших учебных дисциплин профессиональной подготовки по специальности «Электронные системы безопасности» является дисциплина «Надёжность технических систем» (НТС). Для обеспечения указанных в типовой программе требований, предъявляемых к практической подготовке, служат лабораторные занятия, которые в значительной степени позволяют обеспечить требования программы учебной дисциплины в части реализации рубрики «обучающийся должен уметь…».

Возникает вопрос, что должен представлять собою лабораторный практикум по дисциплине «Надёжность технических систем»?

Классический подход к постановке и проведению лабораторных работ здесь не приемлем из-за того, что надёжность электронных устройств и систем является таким свойством, которое проявляется с течением длительного времени работы (наработки): тысячи и даже десятки тысяч часов. Какой же выход из положения?

Анализ показывает, что выходом из положения является математическое моделирование наработки электронных устройств и систем с использованием достижений информационных технологий. Лабораторный практикум должен представлять собой виртуальные лабораторные работы. Причём, слово «виртуальные» подчёркивает то, что исследуемые элементы, устройства, системы и их функционирование (длительная наработка и возникновение отказов) будут моделироваться в памяти ЭВМ. Итоговые показатели надёжности можно будет определить, выполняя обработку результатов моделирования.