ЛАБОРАТОРНА РОБОТА № 9

Тема: Налаштування й супровід сервера DNS BIND.

Мета: Конфігурування служби доменних імен на базі сервера BIND 9. Одержання практичних навичок налаштування й супроводу DNS.

Час виконання: 2 год.

За замовчуванням в Linux використовується одна з версій програми BIND (Berkeley Internet Name Domain), що є найбільш поширеною реалізацією протоколу DNS для UNIX-систем. На сьогодні найпоширенішою версією є BIND 9, що надає розширені настроювання безпеки, нову схему розташування файлів конфігурації й автоматичних настроювань для chroot. Документацію й програмне забезпечення BIND також можна завантажити з web-вузла www.isc.org. Новини й інструментальні засоби DNS доступні на вузлі DNS Resource Directory за адресою http://104.207.142.209/Links/17/3/www.dns.net/dnsrd/.

Програмне забезпечення сервера BIND складається з демона сервера імен, декількох зразків файлів конфігурації й бібліотек програми перетворення імен. Демон сервера імен BIND називається named. Щоб ваш комп'ютер працював як сервер імен, потрібно просто запустити цей демон у відповідній конфігурації. Демон буде очікувати надходження запитів на перетворення імен і повідомляти відповідну IP-адресу для запитуваного імені хоста. За допомогою утиліти rndc, що поставляється разом з BIND, можна запускати, зупиняти, перезапускати й перевіряти стан сервера під час його настроювання. Команда *stop* утиліти rndc зупиняє демон named, а команда *start* знову запускає його, при цьому зчитується файл конфігурації *named.conf*. Під час виклику утиліти *rndc* з опцією *help* виводиться список усіх доступних команд.

Сервери імен звичайно використовуються у двох видах: авторитетний сервер імен і кешуючий сервер імен. Авторитетний сервер імен потрібний, коли:

- потрібно надавати інформацію про DNS іншому середовищі, відповідаючи на запити авторизовано;
- зареєстрований домен, такий, як example.org і в цьому домені потрібно поставити імена машин у відповідність із їхніми адресами IP;
- блоку адрес IP потрібні зворотні записи DNS (перетворення IP-адрес в імена хостів);
- резервний (slave) сервер імен повинен відповідати на запити.

Кешуючий сервер імен потрібний, коли локальний сервер DNS може кешувати інформацію й відповідати на запити швидше, ніж це відбувається при прямому опитуванні зовнішнього серверу імен.

Наприклад, коли будь-хто запитує інформацію про www.lnu.edu.ua, то звичайно резолвер звертається до сервера імен вашого провайдера, надсилає

запит і очікує відповіді. З локальним кешуючим сервером DNS-запит у зовнішнє середовище буде виконаний всього один раз. Кожний додатковий запит не буде посилатися за межі локальної мережі, тому що інформація вже є в кеші.

Настроювання BIND

Настроювання сервера BIND вимагає наявності декількох файлів, посилання на які вказуються у файлі конфігурації *named.conf*. Повний набір файлів виглядає таким чином:

Файл настроювання (конфігураційний файл)

Визначає загальні аспекти роботи *named* і вказує джерела бази даних DNS, які використовує цей сервер. Джерелами можуть слугувати локальні файли або віддалені сервери. Файл настроювання зазвичай називається *named.conf*.

Структура команд настроювання файлу *named.conf* схожа на структуру програм мови С. Оператор закінчується крапкою з комою (;), константи беруться у лапки (" "), а споріднені елементи групуються за допомогою фігурних дужок ({ }). Коментар може обмежуватися парами символів /* і */, //, або #.

Основні команди настроювання *named.conf* наведені в табл. 1.

Таблиця 1. Команди настроювання *named.conf*

Команда	Призначення
Acl	Визначає список керування доступом, що складається з IP-адрес
Include	Включає вміст зовнішнього файлу у файл настроювання
Key	Визначає ключі перевірки дійсності
Logging	Визначає склад журналу повідомлень
Options	Визначає глобальні параметри настроювання
Server	Визначає властивості вилученого серверу
Zone	Визначає зону

Вміст файлу named.conf визначає роль серверу: основний сервер зони, підлеглий сервер зони або спеціальний кешируючий сервер.

Файл кореневих покажчиків

Вказує на сервери кореневих зон. Файл кореневих зон може мати назву *named.ca*, *db.cache*, *named.root* або *root.ca*. У розглянутій реалізації BIND використовується ім'я *named.root*. У процесі настроювання сервера імен цей файл НЕ РЕДАГУЮТЬ!

Кільцевий файл

Використається для локального розв’язання кільцевої адреси.

Називається *localhost.rev*.

Файл зони прямого перетворення

Файл зони, що містить відображення імен вузлів в IP-адреси. Саме цей файл містить основний масив інформації про зону.

Файл зони зворотного перетворення

Файл зони, що містить відображення IP-адрес в імена вузлів.

Файли прямої й зворотної зон зазвичай мають наочні імена, що дозволяють зрозуміти дані якої зони зберігаються у файлі.

На файлах зон зупинимося більш докладно. Ці файли мають схожу будову й складаються із однотипних записів, а саме стандартних записів ресурсів, відомих як RR-записи.

RR-запис має наступний формат:

```
[ім'я]      [ttl] IN    <тип> <дані>
```

ім'я

Ім’я доменного об’єкта, з яким зв’язаний запис. Це може бути окремий вузол або цілий домен. Рядок у поле імені інтерпретується відносно поточного домену, за винятком імені, що закінчується крапкою.

ttl

Час існування (time-to-live) визначає тривалість зберігання запису в кеші вилученої системи. Як правило, це поле залишають пустим, і в такому випадку використовується час існування за замовчуванням, установлене для всієї зони в цілому.

IN

Вказує, що RR-запис має клас Internet (теоретично можуть існувати й інші мережі).

<тип>

Вказує тип RR-запису. Основні типи записів наведені в табл. 2.

Таблиця 2. Типи записів ресурсів

Тип запису	**Назва запису**	**Призначення**
SOA	Початок компетенції	Відзначає початок даних зони й визначає параметри, що впливають на зону в цілому
NS	Сервер імен	Указує сервер імен домена
A	Адреса	Забезпечує перетворення імені вузла на адресу
PTR	Покажчик	Забезпечує перетворення адреси вузла в ім’я

MX	Поштовий ретранслятор	Вказує, куди слід доставляти пошту, призначену певному доменному імені
CNAME	Канонічне ім’я	Визначає псевдонім для імені вузла
TXT	Текст	Зберігає довільні текстові рядки

<дані>

Інформація, що властива даному типу RR-запису. Наприклад, у випадку адресної (A) запису поле даних містить IP-адресу.

Також у BIND існує чотири директиви, що спрощують створення файла зон або визначальних параметрів RR-записів.

Директива $TTL задає значення часу існування за замовчуванням для RR-записів, що не містять наявної вказівки параметра ttl.

Директива $ORIGIN установлює поточну зону, тобто доменне ім’я, яким доповнюються всі відносні доменні імена. Відносним вважається будь-яке доменне ім’я, що не закінчується крапкою. За замовчуванням $ORIGIN приймає значення доменного імені, зазначеного в операторі *zone*.

Директива $INCLUDE включає вміст зовнішнього файла як фрагмент файла зони.

Директива $GENERATE використається для створення серій RR-записів.

Утиліта nslookup

Nslookup – це інструмент налагодження, що входить до складу пакета BIND. Програма дозволяє користувачу прямо звертатися до сервера імен з запитами й одержувати будь-яку інформацію, збережену в розподіленій базі даних DNS. Команда *nslookup* допомагає визначити факт працездатності сервера й коректність його налаштування, а також запитати інформацію, яку мають віддалені сервери.

У наступному лістингу показано, як nslookup використовують для визначення IP-адреси певного вузла:

```
#nslookup comp1.sirius.edu
   Server:      ns.sirius.edu
   Address:     192.168.1.25

   Name:        comp1.sirius.edu
   Address:     192.168.1.188
```

Приклад налаштування сервера імен

У даному прикладі ми налаштовуватимемо уявний домен *example.org* для того, щоб можна було побачити, як усі компоненти сервера DNS працюють разом.

Спочатку переконайтеся, що сервер BIND встановлено на вашому комп’ютері. У дистрибутиві OpenSUSE Linux це можна перевірити, запустивши з правами адміністратора команду

```
# zypper search named
```

(в інших дистрибутивах це може бути *yum*, *apt-get* тощо). Якщо виявиться, що програму не встановлено, то її слід встановити командою

```
# zypper install named
```

Файли конфігурації демона *named* у дистрибутиві OpenSUSE Linux розташовані в каталозі /var/lib/namedb і лише у випадку, коли вам потрібний не просто резолвер, вимагають модифікації. Для створення основної зони для локального хоста перейдіть у каталог /var/lib/namedb. У каталозі повинен бути файл localhost.zone для локальної адресної зони. Посилання на нього вже втримуються у файлі конфігурації named.conf. Варіант вмісту файлу *localhost.zone* наведено нижче:

```
$TTL 1W
@               IN SOA  @   root (
                                42              ; serial (d. adams)
                                2D              ; refresh
                                4H              ; retry
                                6W              ; expiry
                                1W )            ; minimum

                IN    NS           @
                IN    A            127.0.0.1
                IN    AAAA         ::1
```

Після цього можемо перейти до створення файлів зон. Розглянемо вміст файла зони прямого перетворення *example.org.zone*.

```
@86400      IN    SOA ns.example.org. root.example.org. (

                  2013040501
                  28800
                  7200
                  604800
                  86400)

            IN    NS    10.100.1.101

localhost   IN    A     127.0.0.1
ns          IN    A     10.100.1.101
test        IN    A     10.100.1.101
comp2       IN    A     10.100.1.102
comp3       IN    A     10.100.1.103
comp4       IN    A     10.100.1.104
comp5       IN    A     10.100.1.105
comp6       IN    A     10.100.1.106
comp7       IN    A     10.100.1.107
comp8       IN    A     10.100.1.108
comp9       IN    A     10.100.1.109
```

root.example.org – електронна адреса сервера DNS.
2003040501 – порядковий номер (як правило, формується із дати зміни файла);
28800 – періодичність відновлень (с);
7200 – повторення спроби розв’язання (с);

604800 – старіння (с);
86400 – TTL кеша (с).
IN NS 10.100.1.101 – вказівка на IP-адресу сервера імен.
comp2 IN A 10.100.1.102 – запис ресурсів, використовуваний для перетворення імені хоста в IP-адресу.

Розглянемо вміст файла зони зворотного перетворення *1.100.10.zone*.

```
$TTL            86400
@ 86400     IN  SOA ns.example.org. root.example.org. (
                2003090501
                28800
                7200
                604800
                86400)

            IN  NS    ns.example.org.
101         IN  PTR   ns.example.org.
101         IN  PTR   test.example.org.
102         IN  PTR   comp2.example.org.
103         IN  PTR   comp3.example.org.
104         IN  PTR   comp4.example.org.
105         IN  PTR   comp5.example.org.
106         IN  PTR   comp6.example.org.
107         IN  PTR   comp7.example.org.
108         IN  PTR   comp8.example.org.
109         IN  PTR   comp9.example.org.
```

Структури файлів зон мають багато спільного між собою. Основною відмінністю є використання покажчика PTR для зворотного дозволу IP-адреси комп'ютера в його символічне ім'я. Зверніть увагу, що у файлі зони зворотного перетворення вказується лише останній октет IP-адреси, який однозначно ідентифікує хост. Так, запис

```
103   IN    PTR   comp3.example.org.
```

позначає, що імені comp3.example.org зіставляється адреса 10.100.1.103.

Тепер пропишемо шляхи до файлів бази даних DNS у конфігураційному файлі *named.conf*:

```
# Copyright (c) 2001-2004 SuSE Linux AG, Nuernberg, Germany.
# All rights reserved.
#
# Author: Frank Bodammer, Lars Mueller <lmuelle@suse.de>
#
# /etc/named.conf
#
# This is a sample configuration file for the name server BIND 9.  It works as
# a caching only name server without modification.
#
# A sample configuration for setting up your own domain can be found in
# /usr/share/doc/packages/bind/sample-config.
#
# A description of all available options can be found in
# /usr/share/doc/packages/bind/misc/options.

options {
```

```
        # The directory statement defines the name server's working directory

        directory "/var/lib/named";
        managed-keys-directory "/var/lib/named/dyn/";

        # Write dump and statistics file to the log subdirectory.  The
        # pathenames are relative to the chroot jail.

        dump-file "/var/log/named_dump.db";
        statistics-file "/var/log/named.stats";

        # The forwarders record contains a list of servers to which queries
        # should be forwarded.  Enable this line and modify the IP address to
        # your provider's name server.  Up to three servers may be listed.

        #forwarders { 192.0.2.1; 192.0.2.2; };

        # Enable the next entry to prefer usage of the name server declared in
        # the forwarders section.

        #forward first;

        # The listen-on record contains a list of local network interfaces to
        # listen on.  Optionally the port can be specified.  Default is to
        # listen on all interfaces found on your system.  The default port is
        # 53.

        #listen-on port 53 { 127.0.0.1; };

        # The listen-on-v6 record enables or disables listening on IPv6
        # interfaces.  Allowed values are 'any' and 'none' or a list of
        # addresses.

        listen-on-v6 { any; };

        # The next three statements may be needed if a firewall stands between
        # the local server and the internet.

        #query-source address * port 53;
        #transfer-source * port 53;
        #notify-source * port 53;

        # The allow-query record contains a list of networks or IP addresses
        # to accept and deny queries from. The default is to allow queries
        # from all hosts.

        #allow-query { 127.0.0.1; };

        # If notify is set to yes (default), notify messages are sent to other
        # name servers when the the zone data is changed.  Instead of setting
        # a global 'notify' statement in the 'options' section, a separate
        # 'notify' can be added to each zone definition.

        notify no;

    disable-empty-zone
"1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA";
};

# To configure named's logging remove the leading '#' characters of the
# following examples.
#logging {
#       # Log queries to a file limited to a size of 100 MB.
```

```
#       channel query_logging {
#               file "/var/log/named_querylog"
#                       versions 3 size 100M;
#               print-time yes;                 // timestamp log entries
#       };
#       category queries {
#               query_logging;
#       };
#
#       # Or log this kind alternatively to syslog.
#       channel syslog_queries {
#               syslog user;
#               severity info;
#       };
#       category queries { syslog_queries; };
#
#       # Log general name server errors to syslog.
#       channel syslog_errors {
#               syslog user;
#               severity error;
#       };
#       category default { syslog_errors;  };
#
#       # Don't log lame server messages.
#       category lame-servers { null; };
#};

# The following zone definitions don't need any modification.  The first one
# is the definition of the root name servers.  The second one defines
# localhost while the third defines the reverse lookup for localhost.

zone "." in {
        type hint;
        file "root.hint";
};

zone "localhost" in {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone  "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa"
in {
    type master;
    file "127.0.0.zone";
};


# Include the meta include file generated by createNamedConfInclude.  This
# includes all files as configured in NAMED_CONF_INCLUDE_FILES from
# /etc/sysconfig/named

include "/etc/named.conf.include";

# You can insert further zone records for your own domains below or create
# single files in /etc/named.d/ and add the file names to
# NAMED_CONF_INCLUDE_FILES.
# See /usr/share/doc/packages/bind/README.SUSE for more details.
```

```
zone "example.org" in {
        type master;
        file "example.org.zone";
};

zone "1.100.10.in-addr.arpa" in {
        type master;
        file "10.100.1.zone";
};
logging {
        category default { log_syslog; };
        channel log_syslog { syslog; };
};
```

Аналіз вмісту *named.conf* показує, що всі файли, які забезпечують роботу DNS, зберігаються в каталозі */var/lib/named*. Файли дампа зберігаються в */var/log/named_dump.db*.

Форвардер не налаштовано. Також слід згадати файл кореневих покажчиків named.hint, який ми в процесі настроювання DNS залишили без змін.

Тепер ми можемо запустити сервер імен. Для одноразового запуску демона в цій конфігурації використайте команду

```
# server named start
```

або

```
# systemctl start named
```

Щоб демон named запускався під час завантаження, скористайтеся командою

```
# systemctl enable named
```

Працездатність сервера імен можна перевірити утилітою *nslookup*.

Хід роботи

1. Настроювання сервера імен виробляється для домену *прізвищестудента.org*.
2. Перевірте наявність файлів зони для локального хоста і за необхідності створіть їх.
3. Визначте адреси комп’ютерів у лабораторії для внесення їх у файли зон.
4. Керуючись поданим прикладом, напишіть свій файл для прямої зони, після чого з відповідним ім'ям скопіюйте його в каталог */var/lib/named/*.
5. Керуючись поданим прикладом, напишіть свій файл для зворотної зони, після чого з відповідним ім'ям скопіюйте його в каталог */var/lib/named/*.
6. Пропишіть посилання на відповідні файли в *named.conf*. Також відредагуйте інші необхідні параметри для функціонування сервера імен. Як форвардер прийміть машину з IP-адресою 192.168.224.12.
7. Запустіть сервер BIND.
8. За допомогою nslookup переконайтеся в працездатності сервера.

Контрольні запитання

1. Поясніть призначення служби доменних імен.
2. З яких компонентів складається сервер BIND?
3. Поясніть відмінність основного сервера імен (master) від кешуючого.
4. Які файли необхідні для настроювання авторитетного серверу імен?
5. Перелічіть використовувані директиви для файлів зон. Пояснить їхнє призначення.
6. Перелічіть основні типи RR-записів, поясніть кожен з них.
7. Яким чином стартувати демон *named* під час завантаження системи?