DNS-сервер BIND9

Данная статья применима к:

- ОС ОН Орёл 2.12;
- ОС СН Смоленск 1.6;
- ОС СН Ленинград 8.1.

Установка пакета

Пакет `bind9` входит в стандартный дистрибутив ОС ОН Орёл 2.12 и доступен через репозиторий ОС ОН Орёл.
Установку службы DNS BIND9 можно выполнить из графического менеджера пакетов, или из командной строки:

```
sudo apt install bind9
```

При установке пакета `bind9` будет автоматически уставновлен пакет инструментов командной строки `bind9utils`. Из этих инструментов следует отметить:

- named-checkconf — инструмент проверки синтаксиса файлов конфигурации;
- named-checkzone — инструмент проверки файлов зон DNS;
- rndc — инструмент управления службой DNS.

В дополнение к пакетам `bind9` и `bind9utils`, рекомендуем сразу установить пакет инструментов командной строки `dnsutils`, предназначенных для работы с DNS:

```
sudo apt install dnsutils
```

В составе пакета `dnsutils` будут установлены следующие инструменты:

- dig - инструмент для опроса DNS-серверов и проверки их реакции
- nslookup - инструмент для проверки преобразования имен в IP-адреса
  (далее в тексте используется термин "разрешение имён")
- nsupdate - инструмент для динамического обновления записей DNS

Многие устаревшие материалы в сети Интернет рекомендуют для работы bind создать учётную запись и группу named.
Этого делать не следует, так как при установке пакета будут автоматически созданы учётная запись пользователя и группа, причем не named, как написано в устаревших метериалах, а учетная запись bind и группа bind.
Соответственно, сервис будет работать от имени bind:bind, а не от имени named:named, о чем следует помнить при работе с устаревшими примерами из сети Интернет.

Настройка службы

После настройки службы DNS не забудьте перенастроить службу DHCP,
чтобы клиентам автоматически выдавались правильные адреса серверов DNS.

Конфигурационные файлы BIND9находятся в каталоге /etc/bind.
При установке BIND9 автоматически создаются следующие конфигурационные файлы:

/etc/bind/named.conf	Основной файл конфигурации. Этот файл изменять не следует, так как он содержит в себе только ссылки на остальные конфигурационные файлы (см. ниже)
/etc/bind/named.conf.options	Файл для глобальных настроек службы
/etc/bind/named.conf.local	Файл для настроек зоны DNS

/etc/bind/named.conf.default-zones	Файл конфигурации зон "по умолчанию". В частности, этом файле содержатся ссылки на автоматически созданные файлы конфигурации зоны localhost /etc/bind/db.local и /etc/bind/127.db

Подробности о конфигурационных параметрах см. в руководстве man named.conf (5).

Получение списка корневых DNS-серверов

Данный пункт необязателен, и применим только для открытых сетей.

Загружаем свежий список корневых DNS-серверов в файл /etc/bind/named.root:

```
sudo wget -q -O /etc/bind/named.root http://www.internic.net/zones/named.root
```

Предоставляем доступ к файлу учётной записи bind:

```
sudo chown root:bind /etc/bind/named.root
sudo chmod 640 /etc/bind/named.root
```

Дополнительно, можно установить задачу cron для автоматического обновления файла.

В файл конфигурации добавляем ссылку на файл:

```
// Имя из одной точки (.) предатсвляет собой корень всего пространства имён DNS namespace,
// таким образомм, это определение зоны указывает, где начинать поиск любого имени в Интернет
zone "." IN {
type hint;
file "named.root";
};
```

Настройка BIND9 для работы с Samba AD

Параметры настройки BIND9 и BIND9_DLZ для использования в качестве DNS-сервера домена см. BIND9 как DNS-сервер для Samba AD

Вариант простейшей настройки "Кеширующий сервер DNS"

Если у вас уже есть настроенный и доступный DNS-сервер (собственный, или сервер провайдера), создание в локальной сети кеширующего DNS-сервера позволит без особых затрат ускорить работу с Интернет за счет ускорения разрешения имен по запросам различных сетевых служб и/или пользовательскими программами.

Для примера предположим, что у нас есть:

- сервер DNS с адресом `192.168.32.211`

Для создания кеширующего dns-сервера

- раскомментируем в файле конфигурации `/etc/bind/named.conf.options` строки

```
//  forwarders {
//      0.0.0.0;
//  };
```

- указываем адреса используемых DNS-серверов, которым нужно передавать запросы (для примера взяты адреса DNS-серверов Google)
- и, в этом примере, отключаем авторизацию dnssec (использование dnssec будет рассмотрено позже)

```
forwarders {
        8.8.8.8;
        8.8.4.4;

};

dnssec-validation False;
```

Можно , но не обязательно, ещё добавить список интерфейсов компьютера, через которые сервис DNS должен принимать запросы:

```
listen-on {
        127.0.0.1;
        192.168.1.1;
};
```

- сохраняем файл конфигурации
- проверяем правильность конфигурации командой (если команда не выдаёт никаких сообщений - значит ошибок нет)

```
sudo named-checkconf
```

- и перезапускаем сервис

```
sudo systemctl restart bind9
```

Проверить работоспособность и эффективность кеширующего DNS-сервера можно с помощью инструмента `dig`:

```
dig @localhost www.astralinux.ru | grep msec              #
;; Query time: 15 msec

dig @localhost www.astralinux.ru | grep msec           #       5
  ;; Query time: 0 msec
```

Вариант простой настройки "Локальный сервер DNS"

Это вариант настройки собственного полноценного DNS-сервера, обеслуживающего собственную локальную сеть (собственный DNS-домен).
Создание DNS-сервера в локальной сети позволяет организовать единое пространство имён для всех сетевых служб и пользователей.
В отличие от кеширующего сервера из предыдущего примера, этот сервер самостоятельно обрабатывает запросы, относящиеся к его зоне ответственности.

Для примера, предположим, что у нас есть

- домен `localnet.example.ru`
- сервер DNS в этом домене с именем `dns.localnet.example.ru` и адресом `192.168.32.211`
- компьютер host в этом домене с именем `host.localnet.example.ru` и адресом `192.168.32.96`

Настройка конфигурации bind:

- на сервере DNS файл конфигурации `/etc/bind/named.conf.options` используем из предыдущего примера:

```
forwarders {
        8.8.8.8;

        8.8.4.4;
};

listen-on {
        127.0.0.1;

        192.168.32.211;
};

dnssec-validation False;
```

- внесём информацию о домене в файл конфигурации `/etc/bind/named.conf.local`. Исходно в этом файле содержатся только комментарии. Добавляем следующие строки:

```
zone "localnet.example.ru"    {                    #
    type master;                                    #  master ,          ,
    file "/etc/bind/zones/db.localnet.example.ru"; #


};

zone "32.168.192.in-addr.arpa" {                    #   .       ,    .
    type master;                                    #  master ,  ,    ,    ,

    file "/etc/bind/zones/db.32.168.192";           #  192.168.32.0/24,
};
```

- создаём каталог для хранения файлов данных, и копируем в созданный каталог образцы файлов данных:

```
mkdir /etc/bind/zones
cp /etc/bind/db.local /etc/bind/zones/db.localnet.example.ru
cp /etc/bind/db.127 /etc/bind/zones/db.32.168.192
```

- вносим изменения в файл прямой зоны /etc/bind/zones/db.localnet.example.ru:

```
$TTL    604800
@ IN SOA localhost. root.localhost. (
@       IN      SOA     dns.localnet.example.ru. admin.localnet.example.ru. (
  2 ; Serial
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@ IN NS localhost.
; name servers - NS records -   DNS-
        IN      NS      dns.localnet.example.ru.
@ IN A 127.0.0.1
; name servers - A records -   ,  () DNS
dns.localnet.example.ru.          IN      A      192.168.32.211
@ IN AAAA ::1
; 192.168.32.0/24 - A records -     ()
host.localnet.example.ru.         IN      A      192.168.32.96
```

- вносим измения в файл /etc/bind/zones/db.32.168.192 реверсивной зоны:

```
$TTL    604800
@ IN SOA localhost. root.localhost. (
@       IN      SOA     localnet.example.ru. admin.localnet.example.ru. (
 1         ; Serial
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL ;
@ IN NS localhost. ; delete this line
; name servers
      IN      NS      dns.localnet.example.ru.
1.0.0 IN PTR localhost. ; delete this line
; PTR Records
211 IN      PTR     dns.localnet.example.ru.    ; 192.168.32.211
96  IN      PTR     host.localnet.example.ru.   ; 192.168.32.96
```

- проверяем созданную конфигурацию с помощью соответствующих инструментов :

```
named-checkconf
named-checkzone localnet.example.ru     /etc/bind/zones/db.localnet.example.
ru
named-checkzone 32.168.192.in-addr.arpa /etc/bind/zones/db.32.168.192
```

- и перезапускаем службу:

```
systemctl restart bind9
```

Проверить работу сервера можно выполнив на сервере команду:

```
dig @localhost host.localnet.example.ru
```

Добавляем резервный сервер.

Как и в примере ранее, предположим, что у нас есть

- домен `localnet.example.ru`
- сервер DNS в этом домене с именем `dns.localnet.example.ru` и адресом `192.168.32.211`
- компьютер host в этом домене с именем `host.localnet.example.ru` и адресом `192.168.32.96`
- и добавляется резервный сервер DNS `dns2.localnet.example.ru` и адресом `192.168.32.212`

Для добавления резервного сервера

- на основном сервере DNS внесём информацию о резервном сервере в файл конфигурации `/etc/bind/named.conf.local`, и перезапустим сервис. Добавляемые строки выделены:

```
zone "localnet.example.ru"    {
    type master;
    file "/etc/bind/zones/db.localnet.example.ru";

    allow-transfer { 192.168.32.212; };             #
};

zone "32.168.192.in-addr.arpa" {
    type master;

    file "/etc/bind/zones/db.32.168.192";

    allow-transfer { 192.168.32.212; };             #

};
```

- на резервном сервере DNS файл конфигурации `/etc/bind/named.conf.options` используем из предыдущего примера, но с одним отличием - резервный сервер слушает адрес 192.168.32.212:

```
forwarders {
        8.8.8.8;

        8.8.4.4;
};

listen-on {
        127.0.0.1;

        192.168.32.212; #
};
```

- вносим изменения в файл конфигурации `/etc/bind/named.conf.local`.

```
zone "localnet.example.ru" {
    type slave;
    file "slaves/db.nyc3.example.ru";
    masters { 192.168.32.211; };  #
};

zone "32.168.192.in-addr.arpa" {
    type slave;
    file "slaves/db.32.168.192";

    masters { 192.168.32.211; };  #

};
```

- проверяем корректность конфигурации и перезапускаем сервис

```
named-checkconf
systemctl restart bind9
```

Добавляем служебные записи (SRV-записи).

Служебная запись (SRV-запись) — стандарт в DNS, определяющий имя хоста и номер порта серверов для определённых служб. Определяется в RFC 2782. Могут использоваться в различных протоколах, например, в Kerberos.

SRV-записи располагаются в файлах зоны (в примере выше - это файл /etc/bind/zones/db.localnet.example.ru).

Формат записи:

```
_service._proto.name TTL class SRV priority weight port target
```

Где:

- service - символьное имя сервиса;

- proto - транспортный протокол используемый сервисом, как правило _tcp или _udp;
- name - доменное имя, для которого эта запись действует;
- TTL - стандарт DNS, время жизни;
- class- стандарт DNS, поле класса (это всегда IN);
- priority - приоритет целевого хоста, более низкое значение означает более предпочтительный;
- weight - относительный вес для записей с одинаковым приоритетом;
- port - Порт TCP или UDP, на котором работает сервис;.
- target - канонические имя машины, предоставляющей сервис.

Примеры служебных записей (Kerberos и NTP)

$ORIGIN samdom.example.ru.
$TTL 1h
@ IN SOA dns.samdom.example.ru. root.samdom.example.ru. (

```
        2 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
        IN NS dns.samdom.example.ru.
@ IN AAAA ::1
dns.samdom.example.ru. IN A 10.0.2.254
dhcp.samdom.example.ru. IN A 10.0.2.254
kdc.samdom.example.ru. IN A 10.0.2.253
ntp.samdom.example.ru. IN A 10.0.2.253
;kerberos
_kerberos TXT "SAMDOM.EXAMPLE.RU"
kerberos CNAME kdc
_kerberos._udp SRV 0 0 88 kdc
                       SRV 0 0 88 kdc
                       SRV 0 0 88 kdc
_kerberos-master._udp SRV 0 0 88 kdc
_kerberos-adm._tcp SRV 0 0 749 kdc
_kpasswd._udp SRV 0 0 464 kdc
;ntp server
_ntp._udp IN SRV 0 100 123 ntp.samdom.example.ru.
```

Включение аутентификации по ключам.

В работе

Настройка клиентов

В работе.