Bind 9.9 установка

Начиная с FreeBSD 10, в базовый состав операционной системы не входит DNS-сервер и его нужно устанавливать из портов отдельно. Этим мы и займемся.

Настройка будет серверная, а потому наш named, как и положено на защищенном сервере, будет развиваться в песочнице и отдавать только свои зоны.

Использованные версии ПО:

```
# uname -sr
FreeBSD 10.0-STABLE
# pkg info | grep bind
bind99-9.9.5_12          BIND DNS suite with updated
DNSSEC and DNS64
```

Установка

```
# cd /usr/ports/dns/bin99
# make install clean
```

Настройки:

```
[ ] DOCS          Build and/or install documentation
[ ] FILTER_AAAA  Enable filtering of AAAA records
[ ] FIXED_RRSET  Enable fixed rrset ordering
[ ] GSSAPI       GSSAPI support
[x] IDN          International Domain Names support
[x] IPV6         IPv6 protocol support
[x] LARGE_FILE   64-bit file support
[ ] LINKS        Create conf file symlinks in /usr/local
[ ] NEWSTATS     Enable alternate xml statistics channel
format
[ ] REPLACE_BASE Replace base BIND (FreeBSD 9.x and
earlier)
[ ] RPZ_NSDDNAME Enable RPZ NSDDNAME policy records
[ ] RPZ_NSIP     Enable RPZ NSIP trigger rules
[ ] RPZ_PATCH    RPZ improvements
[ ] RRL          Response Rate Limiting
[ ] SIGCHASE     dig/host/nslookup will do DNSSEC
validation
[x] SSL          Build with OpenSSL (Required for DNSSEC)
```

```

[x] THREADS          Threading support
   ?????????????????????????????????????????? Dynamically Loadable Zones
?????????????????????????????????????????
[ ] DLZ_POSTGRESQL  DLZ Postgres driver
[ ] DLZ_MYSQL       DLZ MySQL driver (no threading)
[ ] DLZ_BDB         DLZ BDB driver
[ ] DLZ_LDAP        DLZ LDAP driver
[ ] DLZ_FILESYSTEM  DLZ filesystem driver
[ ] DLZ_STUB        DLZ stub driver

```

Настройка

```

/etc/rc.conf:
named_enable="YES"
named_flags="-t /var/named"
/var/named - это и есть наша песочница, где named будет жить

```

Делаем песочницу, которая раньше делалась в FreeBSD автоматом

```

# mkdir -p /var/named/usr/local/etc/
# mkdir -p /var/named/var/dump
# mkdir -p /var/named/var/run/named
# mkdir -p /var/named/var/stats
# mv /usr/local/etc/namedb /var/named/usr/local/etc/
# cd /usr/local/etc
# ln -s /var/named/usr/local/etc/namedb
# cd /var/run
# ln -s /var/named/var/run/named

```

последнюю строчку возможно придется вбить после запуска named, если вдруг ругнется на отсутствие файла и не захочет делать ссылку.

Создаем правила для devfs. Правим /etc/devfs.conf

```

# Custom rules for the named chroot dev
[devfsrules_named_chroot=4]
add hide
add path run unhide
add path random unhide

```

Добавляем в /etc/fstab

```

devfs          /var/named/dev  devfs      rw,ruleset=4

```

0 0

Монтируем

```
mount /var/named/dev
```

Однако когда `named` уже запущен, может появиться необходимость перезапустить его по каким-либо причинам, в том числе и для того, чтобы сервер имен проверил наличие обновлений в файлах зон. Для этих целей пакет BIND включает в себя инструмент удаленного управления сервером имен (`Remote Name Daemon Control`), `rndc(8)`.

Настройка `rndc`

`rndc` взаимодействует с демоном `named(8)` через безопасное TCP-соединение, даже на локальном компьютере. Это означает, что у вас есть возможность управлять серверами имен на удаленных системах, не выполняя вход в них. Однако для создания безопасного соединения необходим ключ. Пакет BIND содержит сценарий `rndc-confgen(8)`, который генерирует ключи и выполняет рутинные задачи по настройке `rndc`. Чтобы создать конфигурационный файл для `rndc`, достаточно запустить команду `rndc-confgen`:

```
# rndc-confgen > /etc/namedb/rndc.conf
```

Полученный файл включает в себя все необходимые параметры настройки `rndc`, а также ряд параметров настройки для включения в файл `named.conf`. Раздел с настройками для `named.conf` закомментирован символами решетки (`#`) и выглядит примерно так:

Самая интересная часть – это ключ, необходимый для обеспечения возможности управления сервером имен. Ключи в `rndc.conf` и `named.conf` должны совпадать, в противном случае `rndc` не сможет подключиться к серверу. Здесь также указываются IP-адрес и порт TCP, на котором `named` ожидает управляющие соединения, далее выдается разрешение на управление с указанного IP-адреса при наличии указанного ключа. Есть возможность выдать

разрешение на управление сервером имен нескольким клиентам и каждому клиенту выдать свой собственный ключ. За подробностями обращайтесь к страницам руководства `rndc` и `rndc.conf`.

Скопируйте закомментированные строки из файла `rndc.conf` в файл `named.conf`, удалите символы решетки и перезапустите демон `named` командой `/etc/rc.d/named restart`. После этого вы сможете управлять сервером имен с помощью `rndc`.

Работа с `rndc`

Теперь, когда все препоны установки и настройки `rndc` позади, — что еще можно сказать об этой программе? Полный список ее возможностей приведен на странице руководства `rndc(8)`. Наиболее типичные задачи, решаемые с ее помощью: перезапуск сервера имен, повторная загрузка зон, обновление зон, перенастройка `named` и проверка состояния демона.

Перезагрузка сервера имен командой `rndc reload` вынуждает `named(8)` повторно прочитать и обработать конфигурационные файлы, загрузить из текстовых файлов информацию о первичных доменах и проверить наличие обновлений для вторичных доменов. Эта операция обычно выполняется при изменении конфигурационных файлов и файлов зон.

В промежутках между перезагрузками и полным перезапуском сервера имен с помощью команды `rndc reconfig` можно заставить `named` проверить наличие новых зон.

Для *повторной загрузки зоны* без перезагрузки всего сервера имен в команде `rndc reload` следует указать имя домена. Обычно такая операция выполняется в случае, когда сервер имен испытывает серьезную нагрузку и повторная перезагрузка может потребовать слишком длительного времени или вызвать неприятности в сети.

Выполнение *операции обновления зоны* вынуждает вторичный сервер немедленно проверить наличие обновлений для указанной зоны на

первичном сервере. Например, заставить вторичный сервер *absolutefreebsd.com* проверить наличие обновлений на первичном сервере можно с помощью команды `rndc refresh absolutefreebsd.com`.

Программа `rndc` не дает возможности перезапустить `named`. Для полного перезапуска демона следует применить команду `/etc/rc.d/named restart`.

С помощью команды `rndc status` можно получить разнообразную информацию о сервере имен, включая количество обслуживаемых им доменов, число клиентов, обратившихся к серверу, и т. д.

Черновик

```
/usr/local/etc/namedb/named.conf

acl localnet { 192.168.0.0/22; 127.0.0.1; };
acl all { any; };
options {
// Запрет отдавать номер версии сервера.
    version none;
// Запрет отдавать имя хоста, на котором работает BIND
    hostname none;
// запрет отдавать запросы об идентификаторе
    server-id none;
// Разрешаем по-умолчанию днс запросы только от доверенных
сетей
    allow-query { localnet; };
// Разрешать ли рекурсивные запросы, или отдавать только те
зоны, которые держит сам сервак.
    recursion yes;
// Посылка рекурсивных запросов
// разрешена только клиентам подсети
    allow-recursion { localnet; };
// Игнорировать запросы blackhole
// DNS-сервер не посылает запросы к DNS-серверам из этого
```

списка

// и не отвечает на за, получаемые от этих серверов.

```
blackhole {
```

```
0.0.0.0/8;
```

```
10.0.0.0/8;
```

```
169.254.0.0/16;
```

```
172.16.0.0/12;
```

```
192.0.2.0/24;
```

```
192.168.0.0/16;
```

```
224.0.0.0/4;
```

```
240.0.0.0/4;
```

```
};
```

```
};
```

- allow-query: указывает список хостов, которым разрешено запрашивать все зоны name-сервера или конкретную зону внутри name-сервера.
- allow-recursion: указывает список хостов, которым разрешено создавать рекурсивные запросы к name-серверу для всех зон или для конкретной зоны, обслуживаемой name-сервером.
- allow-transfer: указывает список хостов, которым разрешено инициировать запросы зонной пересылки к name-серверу для всех зон или для конкретной зоны внутри name-сервера. Данное утверждение обязательно требуется в конфигурации первичного name-сервера.
- allow-update: указывает список хостов, которым разрешено инициировать запросы динамического обновления.
- allow-update-forwarding: указывает список хостов, которым разрешено перенаправление запросов динамического обновления (независимо от того, кто является источником запроса).
- allow-notify: указывает список хостов, с которых можно принимать сообщения DNS NOTIFY, говорящих об изменениях в зонном файле. Данный список относится только к конфигурации вторичного name-сервера.

- blackhole: указывает список хостов, которые входят в черный список (запрещен доступ) для инициализации любых транзакций с данным пате-сервером.