План практики № 2 по DNS

Цель занятия

Построение своей собственной системы серверов dns. В качестве сервера будем использовать BIND, потому что его можно установить в любую операционную систему.

Ход работы

0. Разбиться по парам. Два студента настраивают один DNS сервер и поддерживают одну зону.

1. Спроектировать схему сети.

(root) – это компьютер преподавателя, записываем IP-адрес этого компьютера. IP-адреса корневых серверов должны быть известны всем участвующим в сети серверам DNS.

(ru), (com), (edu), (test) – это первый ряд парт, записываем их IP-адреса. Тот факт, что домена test в интернете нет, не играет никакой роли. В нашей сети такой домен будет.

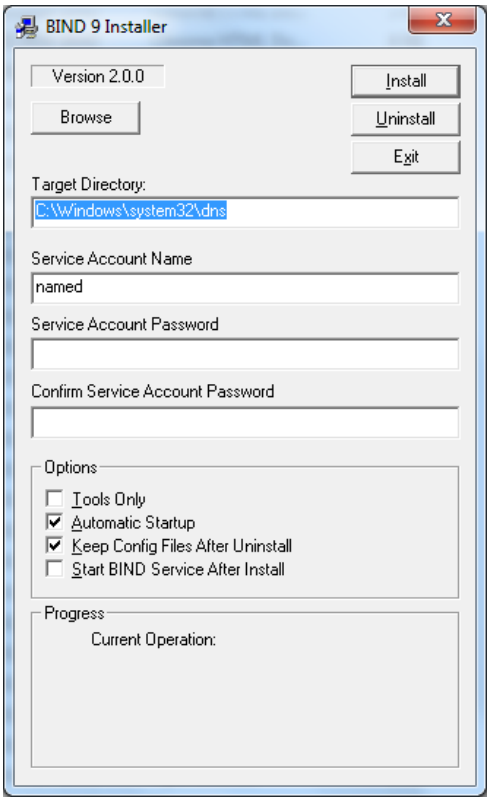
(yandex.ru), (e1.ru), (google.com), (ibm.com) – второй ряд парт,

(mit.edu), (berkeley.edu), (zeus.test), (mars.test) – третий ряд парт.

2. Установить на компьютер DNS-сервер BIND (Версия BIND 9.9.5-W1).

http://www.isc.org/downloads/ Выбрать версию 9.9.7, она имеет статус Current-Stable, ESV, Windows. Распаковать во временную папку, запускаем BINDInstall.exe.

3. При установке указать параметры Service Account Name: named – это создаваемый пользователь, от имени которого будет запущен сервис. Service Account Password задавать надо обязательно, без пароля – только локальный вход.



4. Перед запуском BIND необходимо выполнить некоторые настройки, указанные в файле readme1st.txt. Из методический соображений не будем делать этих настроек, посмотрим на ошибки, к которым приведет запуск.

Убедиться, что сервис изначально остановлен (не запущен):

```
C:\Users\Slava>sc query named

SERVICE_NAME: named
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Запустить сервис в командной строке с повышенными привилегиями:

```
C:\Windows\system32>sc start named

Имя_службы: named
        Тип                : 10  WIN32_OWN_PROCESS
        Состояние          : 2  START_PENDING
                           (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        Код_выхода_Win32   : 0  (0x0)
        Код_выхода_службы  : 0  (0x0)
        Контрольная_точка  : 0x0
        Ожидание           : 0x7d0
        ID_процесса        : 5588
        Флаги              :
```

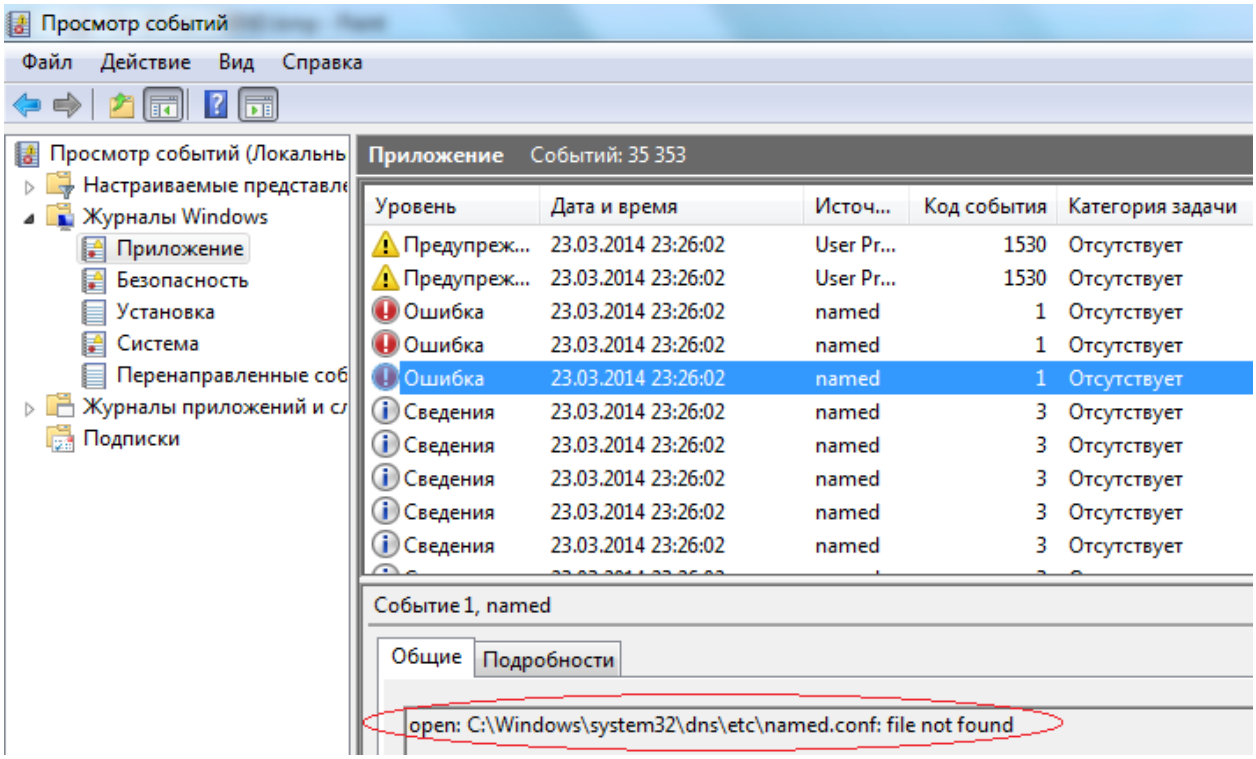
Сервис стартует и сразу завершает работу. Проверить это, сделав запрос `query`:

```
C:\Windows\system32>sc query named
```

Открываем просмотр событий:

```
C:\Windows\system32>eventvwr.exe
```

Причина ошибки, как видно, в отсутствии файла конфигурации.



5. Создать файл конфигурации named.conf и поместить его в C:\Windows\SysWOW64\dns\etc.

Открыть index.html из дистрибутива, BIND 9 Administrator Reference Manual, выбрать Chapter 3. Name Server Configuration и изучить примеры конфигурационных файлов для кэширующих DNS серверов не отвечающих ни за какую зону.

Содержимое файла named.conf:

```
options {
      // Working directory
      directory "c:\\temp\\";
      // This is the default
      allow-query { any; };
};
```

Не забываем закрывающие точки с запятой после каждой директивы и блока директив, их отсутствие – самая частая ошибка.

ВНИМАНИЕ! В 64-битной версии Windows каталог system32\dns при системных вызовах переадресуется в C:\Windows\SysWOW64\dns.

Запустить сервис в командной строке. В журнале событий найти возникшие ошибки, которые связаны с

а) отсутствием файла rndc.key (он нужен для управления сервером без его перезапуска),

б) невозможностью записи 'C:\Windows\system32\dns\etc\named.pid'.

6. Выполнить недостающие настройки для успешного запуска BIND.

Остановить сервер:

```
C:\Windows\system32>sc stop named
```

Выполнить

```
C:\Windows\system32>cacls C:\Windows\SysWOW64\dns\etc /e /g named:c
C:\Windows\SysWOW64\dns\bin>rndc-confgen.exe –a
```

Запустить сервер. Проверить содержимое папки `C:\Windows\SysWOW64\dns\etc`. Там должны появиться два файла: named.pid, содержащий число, и session.key примерно следующего содержания:

```
key "local-ddns" {
     algorithm hmac-sha256;
     secret "VeK8cSuYELI5z3kJ8CeuvCnblZFdhjRALbXN9OM7fkk=";
};
```

7. Проверить, как работает сервер.

Включить режим записи запросов:

```
C:\Windows\SysWOW64\dns\bin> rndc querylog
```

Записывать будет всё в тот же журнал событий.
Запустить nslookup для разрешения доменного имени локальным DNS (т.е. нашим) сервером:

```
C:\Windows\nslookup e1.ru. 127.0.0.1
```

Сервер «думает» (надо все промежуточные серверы опросить), а потом отвечает.

8. Создать свою собственную зону e1.ru и внести туда записи типа A для имен e1.ru и www.e1.ru. В качестве значения можно использовать адрес 194.226.146.222.

В конфигурационный файл named.conf добавить:

```
zone "e1.ru" {
     type master;
     file "e1.ru.txt";
};
```

Создать файл `e1.ru.txt` и разместить его (согласно директиве `directory`) в папке `C:\temp`

```
$TTL 86400
@     SOA  localhost. root.localhost. (
      1; Serial
      604800; Refresh
      86400; Retry
      2419200; Expire
      86400) ; Negative Cache TTL
                    NS    localhost.
@                   A     194.226.146.222
www                 A     194.226.146.222
```

Перегрузить сервер BIND. Сделать, используя утилиту nslookup, запрос к локальному серверу запрос на разрешение имени `e1.ru.` Завершающую точку в имени не забываем ставить, чтобы образовать полностью определенное имя!

9. Изучить настройки ретрансляции зоны САМОСТОЯТЕЛЬНО ☺

10. В конфигурационный файл named.conf добавить:

```
zone "." {
      type hint;
      file "root.txt";
};
```

Создать файл `root.txt`:

```
.     3600000    NS    NS.
NS.   3600000    A     172.16.0.xxx ; адрес преподавательской машины
```

11. Создать primary и secondary зоны dns для назначенных в начале пары доменов (список с адресами авторитетных серверов выписываем на доску). В каждой зоне создаем по крайней мере записи www и пустую запись (совпадающую с именем зоны) по аналогии с зоной e1.ru.

Надо разрешить в свойствах зоны её передачу "на сторону".

Завершающим этапом создать в зонах связующие записи NS и сделать так, чтобы созданная система серверов, каждый из которых отвечает за свою зону, заработала.

В процессе тестирования отрицательные ответы будут сохраняться в кеше ресолвера. Для сброса кэша надо использовать ipconfig /flushdns.

Отчетность

Продемонстрировать работающий BIND. Выслать на почту преподавателя конфигурационные файлы, файлы описания зон, результаты обращения к корневому серверу из утилиты nslookup.