

DNS. Эксплуатация и защита данных. Продвинутый курс

DNS: списки доступа в BIND



DNS ACL

- ACL (списки контроля доступа) и параметры конфигурации в BIND используются для создания более защищенных конфигураций
- Хорошие правила эксплуатации подсказывают, что ACL и параметры конфигурации следует регулярно перепроверять
- Убедитесь, что они по-прежнему уместны: проверяйте их регулярно, чтобы быть уверенным, что они точно отражают именно то, что вам нужно
- Их может быть непросто поддерживать

Элементы списков соответствия адресов

- Индивидуальные IP-адреса
- Пары адрес/маска
- Названия других ACL
- В некоторых ситуациях, названия ключей (более подробно об этом дальше)

Их назначение в BIND

- Ограничить запросы и скачивания зон
- Разрешение/ограничение динамических обновлений
- Выбор интерфейса, на котором BIND принимает запросы
- Сортировка ответов
- Списки соответствия адресов всегда обрамляются фигурными скобками

Замечания о списках соответствия адресов

- Элементы разделяются точкой с запятой ‘;’
- Список должен заканчиваться “.”
- Элементы проверяются последовательно
- Отрицание соответствия обозначается восклицательным знаком перед элементом ‘!’
- Используйте оператор 'acl' для именования списка соответствия адресов
- ACL должен быть определен перед его использованием в другом месте

Пример: список соответствия адресов

- Для сети 192.168.0.0 255.255.255.0:
{ 192.168.0.0/24; };
- Для этой сети плюс локальный интерфейс:
{ 192.168.0.0/24; 127.0.0.1; };
- Адреса плюс название ключа:
{192.168.0.0/24; 127.0.0.1; noc.ws.nsrc.org; };

Оператор ACL

- Синтаксис:

```
acl имя_acl { список_соответствия_адресов; };
```

- Пример:

```
acl internal { 127.0.0.1; 192.168.0/24; };
```

```
acl dynamic-update { key dhcp.ws.nsrc.org; };
```

Замечание об операторе ACL

- Название acl не нужно помещать в кавычки:
- Существует четыре predefined ACL:

any - любой IP-адрес

none - никакой IP-адрес

localhost - локальный IP, 127.0.0.1, ::1

localnets - все сети к которым DNS-сервер имеет
прямое подключение

Черный список

```
options {  
    blackhole { ACL-имя или список по пунктам; };  
};
```

Разрешения скачивания

```
zone "myzone.example" {  
    type master;  
    file "myzone.example";  
    allow-transfer { ACL-name or itemized list; };  
  
};
```

Разрешение запросов

```
zone "myzone.example" {  
    type master;  
    file "myzone.example";  
    allow-query { ACL-name or itemized list; };  
  
};
```

Слушать на IP

```
options {  
    listen-on port # { ACL-name or itemized list; }  
  
};
```

Вопросы

