ФГБОУ ВО “Чувашский государственный университет им. И. Н. Ульянова” Факультет: ИВТ

Кафедра: Вычислительной техники

Предмет: Сети и телекоммуникации

Лабораторная работа 12

**Доменная зона**

Выполнил: студент группы ИВТ-41-20

Галкин Дмитрий

Проверила: Путевская И.В.

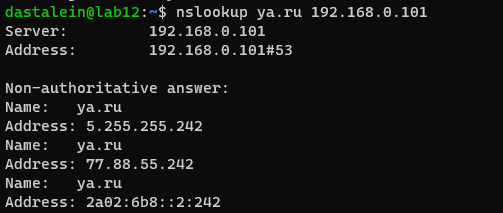
Чебоксары 2023 г.

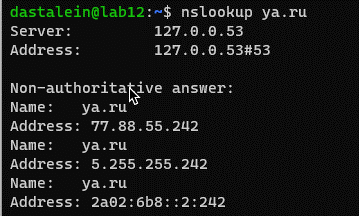
**Цель:** настроить доменную зону с именами локальных ресурсов DNS.

**Задача 1:** установить и настроить dns-сервер

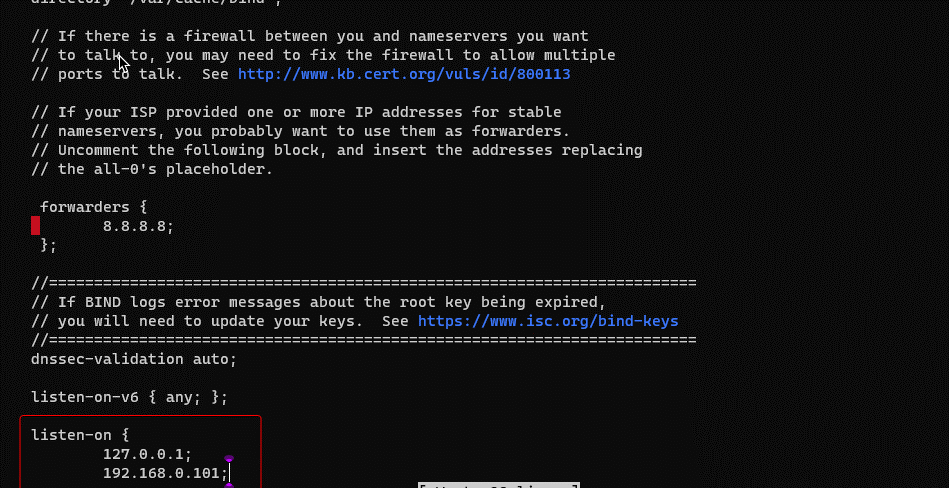
1. Установка dns-сервера



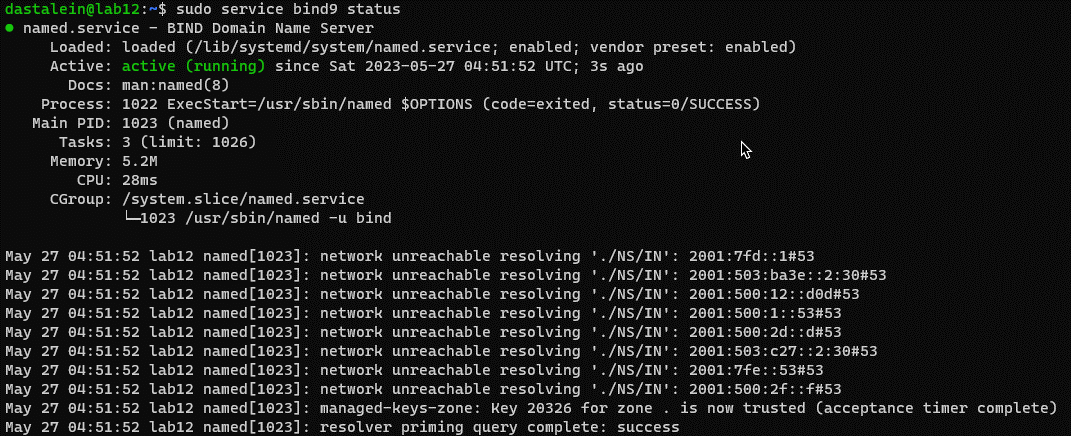




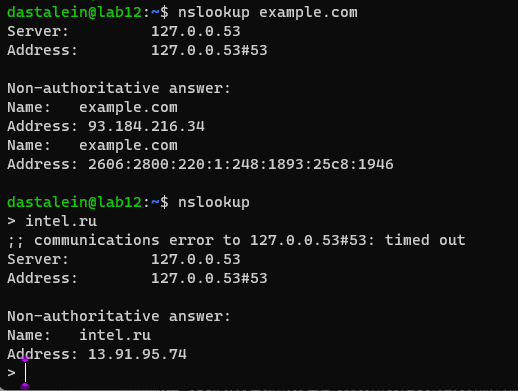
1. Настройка dns-сервера (перенаправляющий сервер)
   1. Настраиваем bind (sudo nano /etc/bind/named.conf.options)



1. Перезапускаем сервис



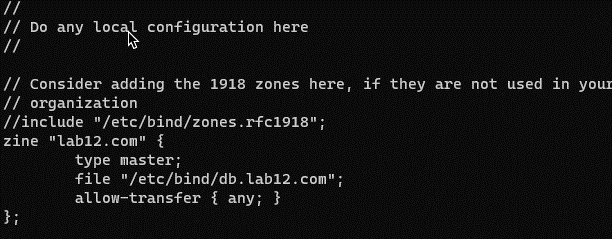
1. Проверка



1. Добавить запись о доменной сети локальной зоне
   1. Настраиваем bind (sudo nano /etc/bind/named.conf.local)

type master – основная доменная зона

file – ссылка, где будет хранится файл, который будет описывать эту доменную зону



* 1. Создаем файл /etc/bind/db.lab12.com

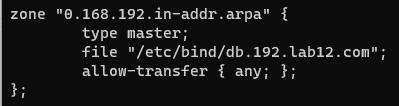


* 1. Настройка файла /etc/bind/db.lab12.com



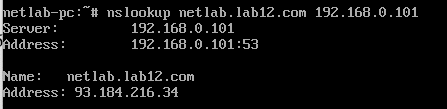
1. Настроить обратную зону
   1. Создаем файл sudo cp /etc/bind/db.lab12.com /etc/bind/db.192.lab12.com
   2. Настройка файла





1. Проверка через netlab\_pc\_11





1. Проверить работу, вывести (dig, nslookup, drill)

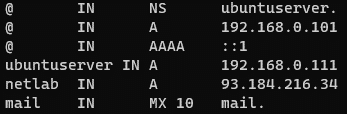
* ip-адрес по имени

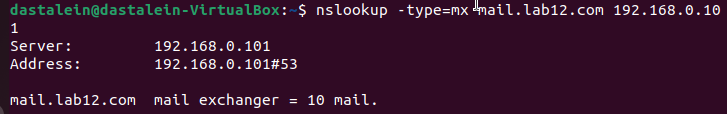


* имя по ip-адресу

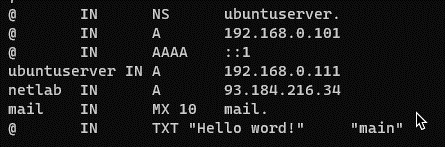


* mx записи



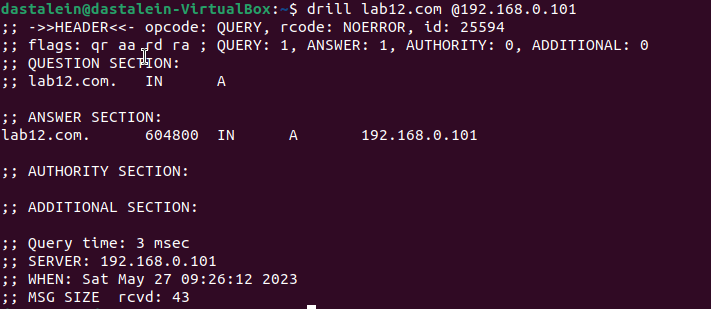


* TXT запись





* Информация о зоне



**Ответы на вопросы:**

1. Как посмотреть доступные на устройстве dns-сервера?

На Linux, система использует файл /etc/resolv.conf для определения DNS-серверов, которые она будет использовать для поиска доменных имен.

1. Какие типы записей доменной зоны существуют?

Доменные зоны содержат несколько типов записей (resource records, RR), каждый из которых отвечает за различные аспекты работы DNS. Вот некоторые из наиболее распространенных типов записей:

* **A (Address Record)**: указывает IPv4-адрес для заданного имени хоста.
* **AAAA (Address Record)**: указывает IPv6-адрес для заданного имени хоста.
* **CNAME (Canonical Name record)**: указывает, что доменное имя является алиасом для другого домена. Другой домен в этом случае называется "каноническим" именем.
* **MX (Mail Exchange record)**: указывает почтовые серверы, которые принимают почту для данного домена.
* **NS (Name Server record)**: определяет серверы имен (DNS-серверы), ответственные за эту зону.
* **PTR (Pointer Record)**: используется для обратного DNS-выяснения, указывает доменное имя, соответствующее данному IP-адресу.
* **SOA (Start Of Authority record)**: содержит информацию об авторитете этой зоны, включая основной сервер имен, а также некоторые другие параметры, такие как время жизни кэша.
* **TXT (Text Record)**: может содержать произвольный текст и часто используется для различных целей, таких как верификация владения доменом или определение политик SPF для предотвращения спама.
* **SRV (Service Record)**: определяет расположение серверов для определенных услуг, таких как SIP или XMPP.
* **CAA (Certification Authority Authorization)**: помогает контролировать, какие организации могут выпускать сертификаты SSL/TLS для вашего домена.
* **DNSKEY, RRSIG, NSEC, DS (DNSSEC Records)**: эти записи используются для обеспечения безопасности DNS через механизм DNSSEC, который помогает предотвратить некоторые виды атак, такие как DNS spoofing.

1. Зачем нужна обратная доменная зона?

Обратная доменная зона в DNS используется для обратного преобразования IP-адресов в имена хостов. Это процесс, известный как обратное DNS-выяснение (reverse DNS lookup или rDNS).

1. Какие связи и существуют между dns-серверами?

В рамках системы DNS серверы между собой могут устанавливать различные связи и взаимодействовать друг с другом. Ниже приведены основные типы связей между DNS-серверами:

* Рекурсивные и итеративные запросы: Клиенты (обычно это компьютеры пользователей) отправляют DNS-запросы на рекурсивный DNS-сервер (часто называемый DNS-резолвер), который в свою очередь может отправлять итеративные запросы на другие DNS-серверы, чтобы разрешить имя. Рекурсивный DNS-сервер будет продолжать делать запросы другим серверам, пока не найдет ответ или не выяснит, что имя не существует.
* Авторитетные серверы: Авторитетные DNS-серверы содержат информацию о конкретных доменных зонах. Они предоставляют эту информацию другим DNS-серверам в ответ на итеративные запросы. Авторитетные серверы бывают первичными (master) и вторичными (slave). Первичные серверы содержат исходные копии данных зоны, а вторичные серверы получают копии этих данных через процесс, называемый зоновой передачей (zone transfer).
* Root-серверы: Root-серверы DNS являются критически важной частью интернет-инфраструктуры. Они обслуживают корневую зону DNS и предоставляют информацию о том, какие авторитетные серверы отвечают за различные домены верхнего уровня (TLD).
* Прямые и обратные зоны: DNS-серверы могут управлять прямыми зонами (для преобразования имен хостов в IP-адреса) и обратными зонами (для преобразования IP-адресов обратно в имена хостов).
* Протокол DNSSEC: DNS-серверы могут использовать протокол DNSSEC для подписи и проверки DNS-данных, что позволяет защититься от некоторых видов атак.