Базовое Администрирование Linux

Занятие 7

Дмитрий Молчанов

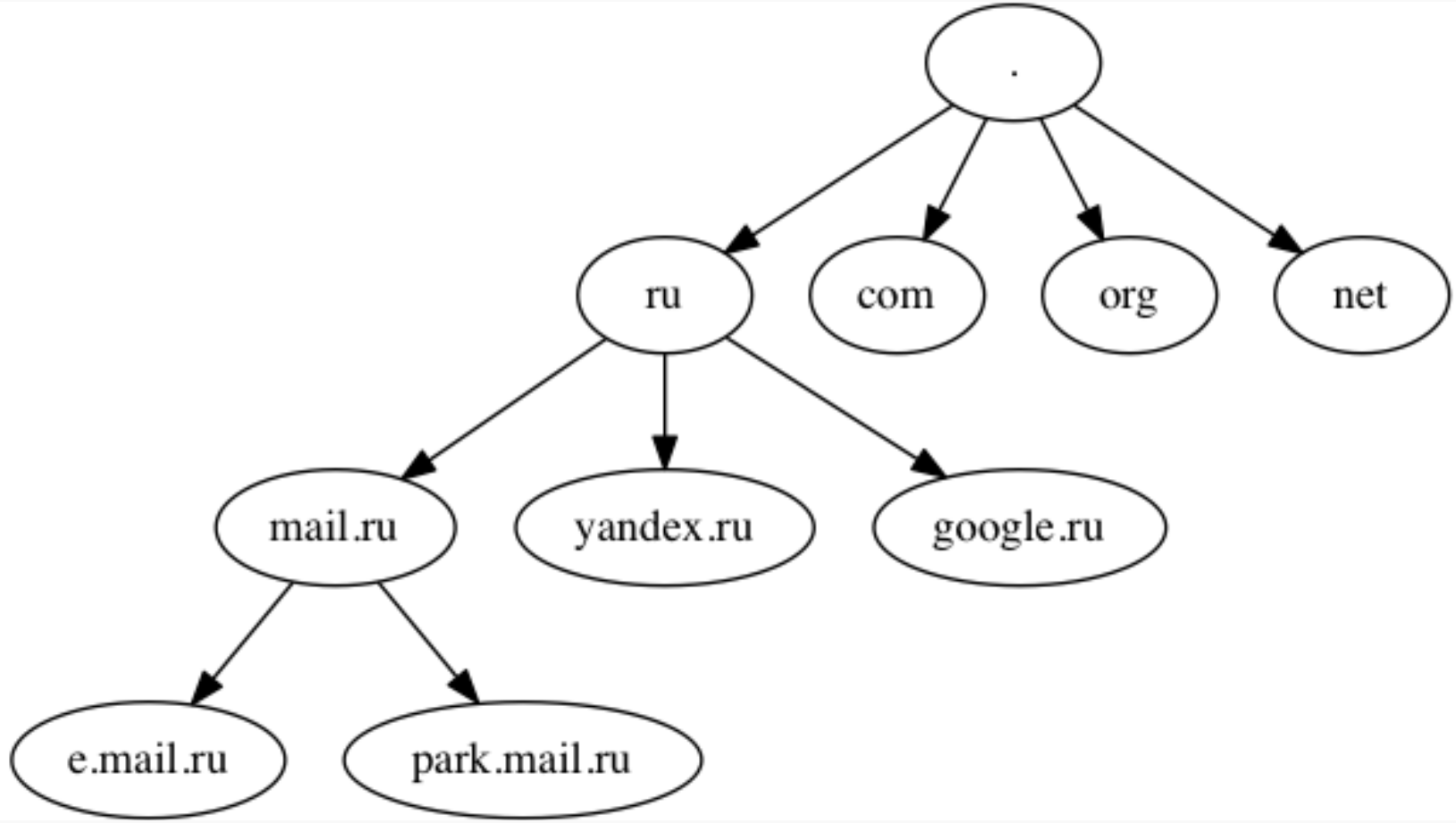
DNS

1. Обзор работы DNS
2. Настройка фильтров
3. Настройка DNS-сервера

Терминология

- dns RR – Resource record, DNS запись, единица хранения и передачи данных в DNS. Состоит из имени, типа и значения.
- dns зона – совокупность DNS-записей, домен.
- TLD – Top Level Domain, домен верхнего уровня.
- master server – сервер являющийся первичным источником данных для зоны доменных имен. Сервер где хранится и изменяется зона
- slave server – реплика master-сервера, не является первичным источником, т.е. на этом сервере не производятся изменения

Структукра DNS



FQDN

FQDN – полностью указанное доменное имя. Характерным признаком FQDN является точка на конце, что означает, что это доменное имя в дополнениях не нуждается.

Если точку не указать, то, в зависимости от ситуации и ПО, это имя может быть обработано по-разному, например туда может быть добавлен домен по-умолчанию, или текущий домен, что может привести к нежелательным последствиям.

DNS RR

Пример:

ИМЯ	TTL	FA	ТИП	ЗНАЧЕНИЕ
park.mail.ru.	600	IN	A	185.5.138.251
mail.ru.	59	IN	NS	ns1.mail.ru.
mail.ru.	600	IN	MX	10 mxs.mail.ru.
hitech.mail.ru.	600	IN	CNAME	hi-tech.mail.ru.
hi-tech.mail.ru.	169	IN	A	217.69.139.31
mail.ru.	600	IN	SOA	**ns1.mail.ru.** hostmaster.mail.ru. **2300425699** 900 900 1209600 300

Типы RR

- A – сопоставление имени конкретному ipv4 адресу
- SOA – Start Of Authority, Указание «авторитетной» информации о зоне.:
  - master-server
  - serial
- MX – Mail eXchanger, указание сервров отвечающих за обработку почты в домене
- NS – NameServer, указание серверов отвечающих за поддержку DNS домена
- CNAME – Canonical name, ссылка на другое доменное имя

Типы запросов DNS

- Рекурсивные – запросы требующие полного поиска для получения конечного ответа
- Итеративные – Запросы не требующие поиска, в ответ возвращается либо результат, либо ошибка.
- Прямые – преобразование имени в адрес
- Обратные – преобразование адреса в имя

Обратные запросы

Информация о сопоставлении адресов именам хранится в домене in-addr.arpa. Адрес разбивается на октеты и преобразуется в доменное имя в этом домене. Это доменное имя является RR типа PTR и значение этой RR – fqdn которому соответсвует адрес

Например:

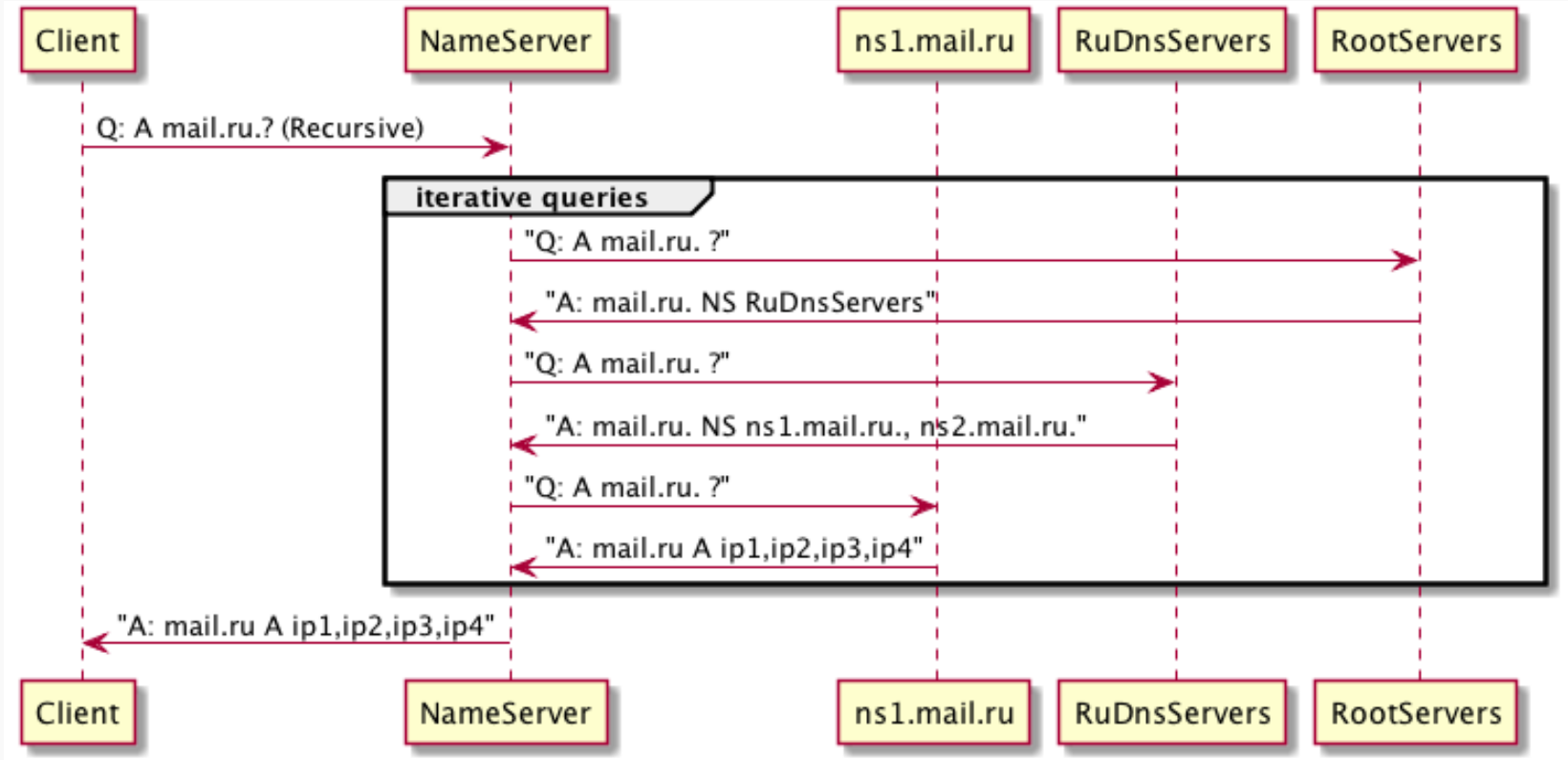
server1.domain.tld имеет адрес 192.168.10.1

server1.domain.tld. IN A 192.168.10.1

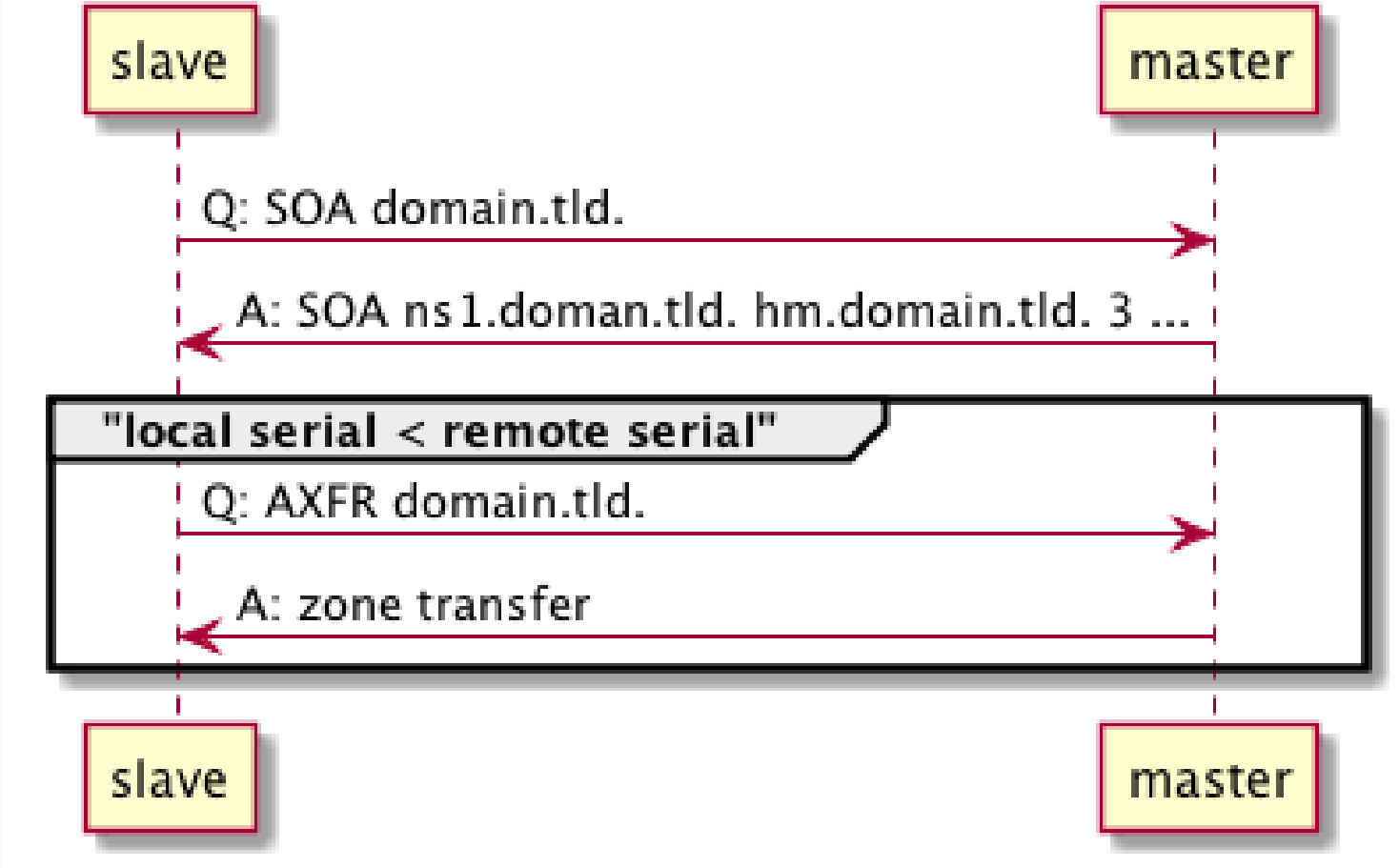
192.168.10.1 -> 1.10.168.192.in-addr.arpa

1.10.168.192.in-addr.arpa IN PTR server1.domain.tld

Схема работы DNS



Репликация


slave
master
Q: SOA domain.tld.
A: SOA ns1.doman.tld. hm.domain.tld. 3 ...
"local serial < remote serial"
Q: AXFR domain.tld.
A: zone transfer
slave
master

Порты и протоколы

DNS использует 53й порт и протоколы UDP и TCP.

Преимущественно используется UDP, TCP
Используется только для передачи зон и когда размер ответа превышает 512 байт

Настройка фильтров

Для того, чтобы на нашем сервере работал DNS-сервер нам надо открыть 53й порт udp и tcp в цепочке INPUT (входящие пакеты адресованные локальной системе).

Для того, чтобы наша машина могла выступать в роли DNS-клиента, нам необходимо разрешить входящий трафик (filter/INPUT) с порта 53 на порты 1024-65535 по протоколам tcp и udp

SplitDNS

У некоторых серверов есть возможность реализовывать разные «представления» (views) основываясь на различных факторах (адрес источника, адрес назначения, атрибуты запроса).

Таким образом можно реализовать, например, гео-балансировку – клиентам из определенного региона выдавать определенный адрес. Или для клиентов локальной сети держать отдельный набор RR который не будет доступен снаружи или будет иметь другие значения.

Настройка DNS-сервера

Ключевые моменты конфигурации:

- acl – списки адресов контроля доступа
- опции
  - listen-on – список слушающих сокетов
  - recursion – разрешение или запрет обработки рекурсивных запросов
  - forwarders – сервера которые обрабатывают рекурсивные запросы к которым наш сервер может обращаться
  - allow-query – список адресов чьи запросы наоб обрабатывать
  - allow-recursion – список адресов которым разрешена рекурсия.

Настройка DNS-сервера

- зоны
  - hint-зона “.” – адреса корневых серверов
  - обслуживаемые зоны
- view (SplitDNS)
  - match-clients – клиенты обслуживаемые данным view
  - match-destination – локальные адреса обсулживаемые данным view

Полезные ссылки

- https://ru.wikipedia.org/wiki/FQDN
- https://ru.wikipedia.org/wiki/DNS
  - https://tools.ietf.org/html/rfc1034
  - https://tools.ietf.org/html/rfc1035

Полезные команды

- dig
- host
- nslookup
- named-checkzone
- named-checkconf
- rndc