Лабораторная работа № 3.

Настройка DHCP-сервера

Диана Алексеевна Садова

Содержание

# 1 Цель работы

Приобретение практических навыков по установке и конфигурированию DHCP-сервера

# 2 Последовательность выполнения работы

## 2.1 Задание

1. Установите на виртуальной машине server DHCP-сервер.
2. Настройте виртуальную машину server в качестве DHCP-сервера для виртуальной внутренней сети.
3. Проверьте корректность работы DHCP-сервера в виртуальной внутренней сети путём запуска виртуальной машины client и применения соответствующих утилит диагностики.
4. Настройте обновление DNS-зоны при появлении в виртуальной внутренней сети новых узлов.
5. Проверьте корректность работы DHCP-сервера и обновления DNS-зоны в виртуальной внутренней сети путём запуска виртуальной машины client и применения соответствующих утилит диагностики.
6. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке DHCP-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внести изменения в Vagrantfile.

## 2.2 Последовательность выполнения работы

### 2.2.1 Установка DHCP-сервера

1. Загрузите вашу операционную систему и перейдите в рабочий каталог с проектом: cd /var/tmp/user\_name/vagrant
2. Запустите виртуальную машину server:(рис. 1).

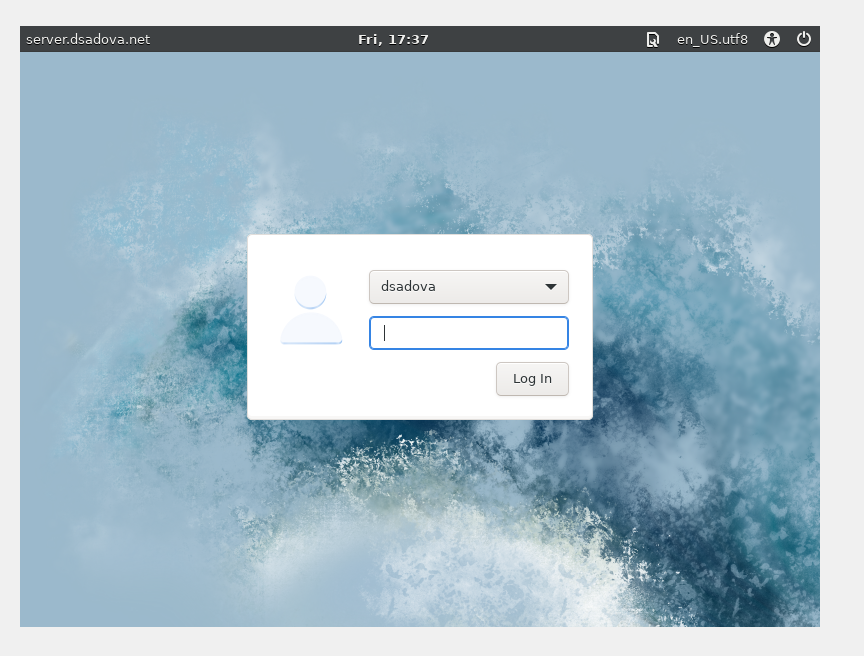


Рис. 1: Запускаем виртуальную машину

1. На виртуальной машине server войдите под вашим пользователем и откройте терминал. Перейдите в режим суперпользователя:(рис. 2).

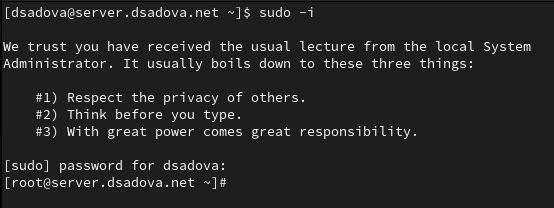


Рис. 2: Заходим в режим суперпользователя

1. Установите dhcp:(рис. 3).

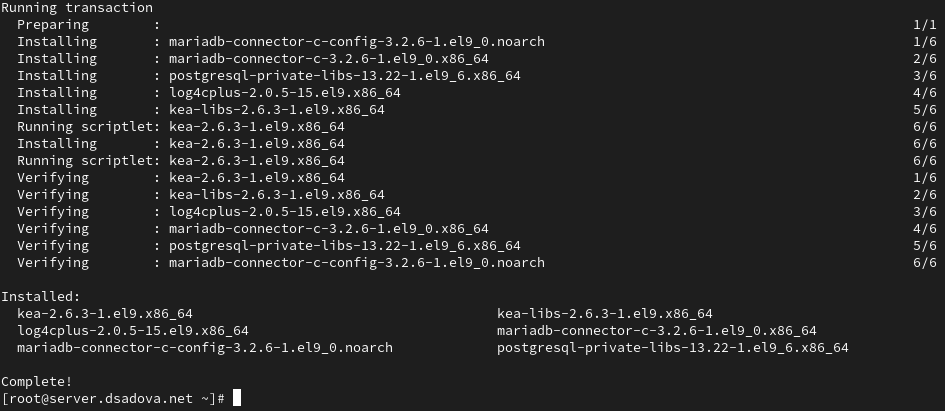


Рис. 3: Установливаем dhcp

### 2.2.2 Конфигурирование DHCP-сервера

1. Сохраните на всякий случай конфигурационный файл:(рис. 4).

Сохраняем конфигурационный файл

Рис. 4: Сохраняем конфигурационный файл

1. Откройте файл /etc/kea/kea-dhcp4.conf на редактирование. В этом файле: замените шаблон для domain-name(рис. 5),(рис. 6).



Рис. 5: Заменяем шаблон

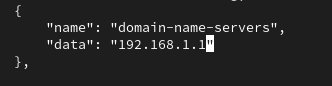


Рис. 6: Заменяем шаблон

– на базе одного из приведённых в файле примеров конфигурирования подсети задайте собственную конфигурацию dhcp-сети, задав адрес подсети, диапазон адресов для распределения клиентам, адрес маршрутизатора и broadcast-адрес:(рис. 7).

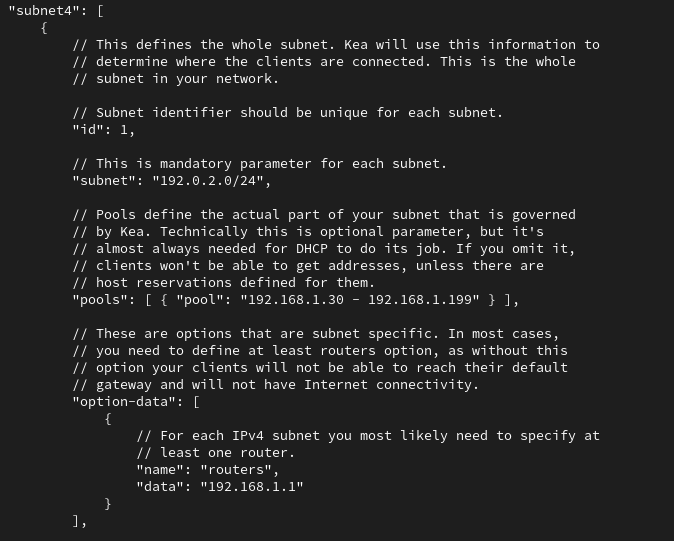


Рис. 7: Заменяем шаблон

Остальные примеры задания конфигураций подсетей удалите.

1. Настройте привязку dhcpd к интерфейсу eth1 виртуальной машины server:(рис. 8).

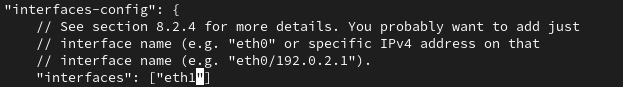


Рис. 8: Настраиваем привязку dhcpd к интерфейсу eth1

1. Проверьте правильность конфигурационного файла:(рис. 9).

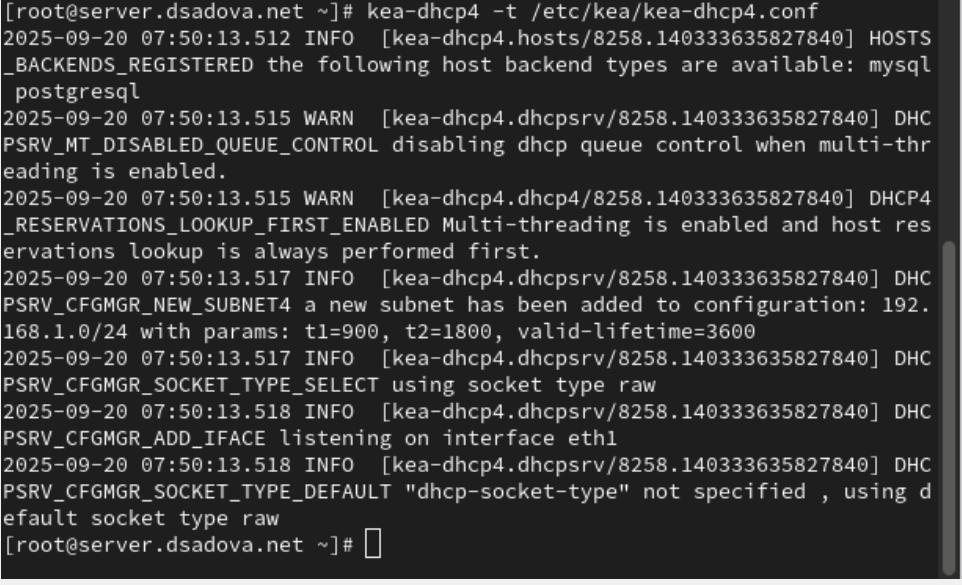


Рис. 9: Проверяем

1. Перезагрузите конфигурацию dhcpd и разрешите загрузку DHCP-сервера при запуске виртуальной машины server:(рис. 10).

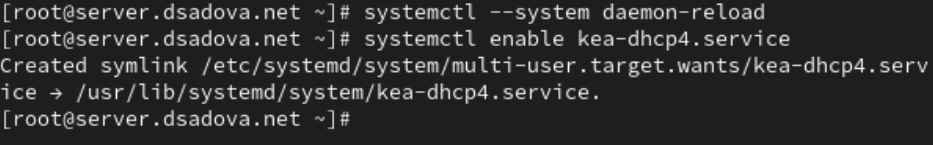


Рис. 10: Перезагружаем конфигурацию dhcpd

1. Добавьте запись для DHCP-сервера в конце файла прямой DNS-зоны /var/named/master/fz/user.net:(рис. 11).

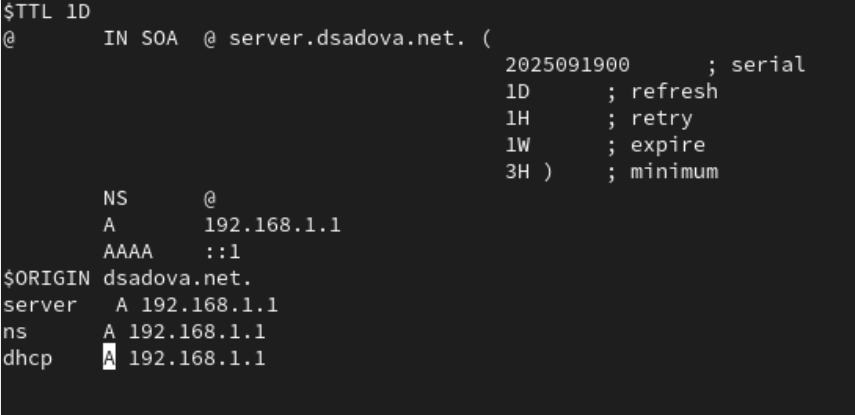


Рис. 11: Добавляем запись для DHCP-сервера

и в конце файла обратной зоны /var/named/master/rz/192.168.1:(рис. 12).



Рис. 12: Добавляем запись для DHCP-сервера

При этом не забудьте в обоих файлах изменить серийный номер файла зоны, указав текущую дату в нотации ГГГГММДДВВ.

1. Перезапустите named:(рис. 13).

Перезапускаем named

Рис. 13: Перезапускаем named

1. Проверьте, что можно обратиться к DHCP-серверу по имени:(рис. 14).

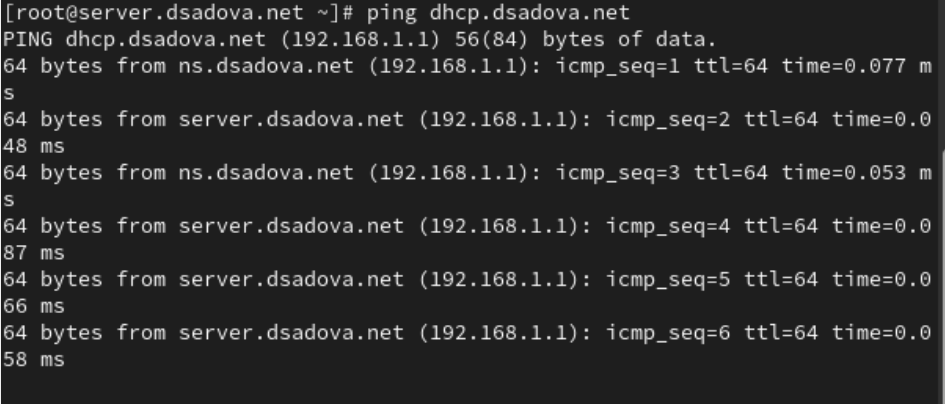


Рис. 14: Обращаемся к DHCP-серверу

1. Внесите изменения в настройки межсетевого экрана узла server, разрешив работу с DHCP:(рис. 15).

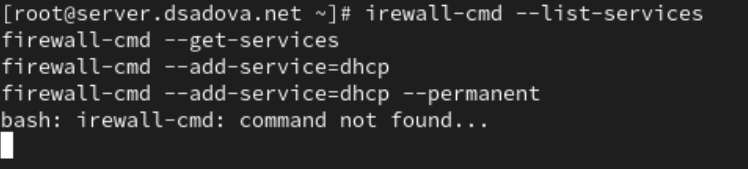


Рис. 15: Вносим изменения

1. Восстановите контекст безопасности в SELinux:(рис. 16).

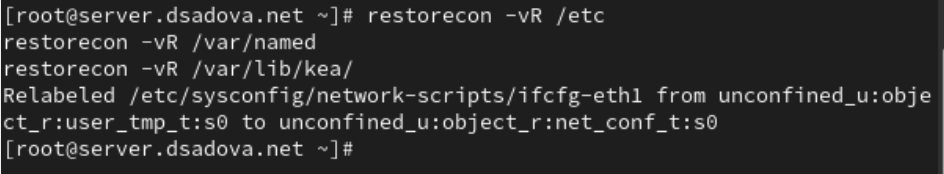


Рис. 16: Востанавливаем контекст безопасности в SELinux

1. В дополнительном терминале запустите мониторинг происходящих в системе процессов в реальном времени:(рис. 17).

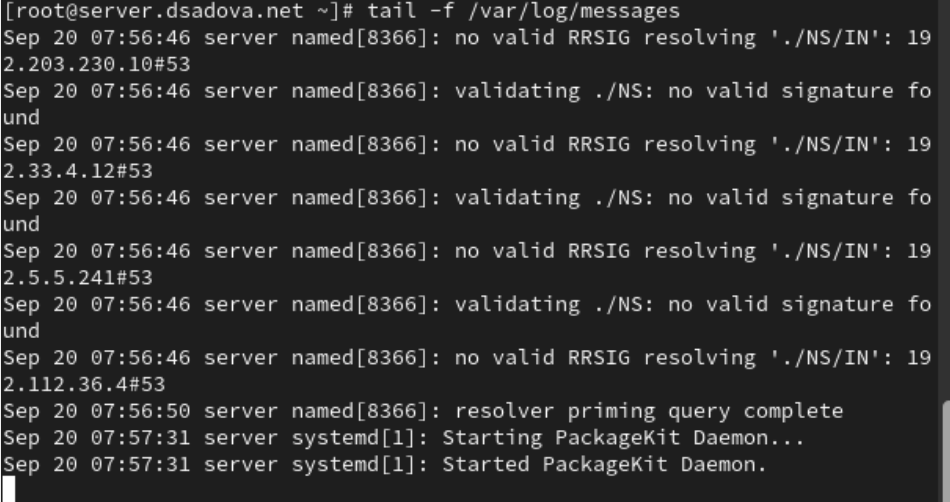


Рис. 17: Запускаем мониторинг

1. В основном рабочем терминале запустите DHCP-сервер:(рис. 18).

Запускаем DHCP-сервер

Рис. 18: Запускаем DHCP-сервер

1. Если запуск DHCP-сервера прошёл успешно, то, не выключая виртуальной машины server и не прерывая на ней мониторинга происходящих в системе процессов, приступите к анализу работы DHCP-сервера на клиенте.

Запуск произошел без ошибок. Идем дальше.

### 2.2.3 Анализ работы DHCP-сервера

1. Перед запуском виртуальной машины client в каталоге с проектом в вашей операционной системе в подкаталоге vagrant/provision/client создайте файл 01-routing.sh. Открыв его на редактирование, пропишите в нём следующий скрипт:(рис. 19).

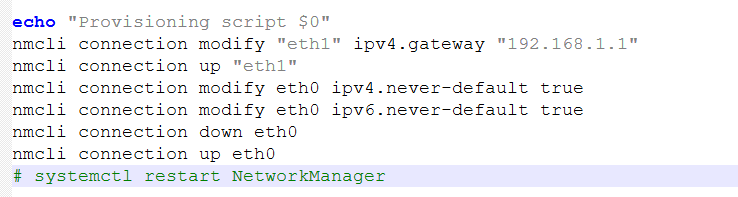


Рис. 19: Переписываем 01-routing.sh

Этот скрипт изменяет настройки NetworkManager так, чтобы весь трафик на виртуальной машине client шёл по умолчанию через интерфейс eth1.

1. В Vagrantfile подключите этот скрипт в разделе конфигурации для клиента:(рис. 20).

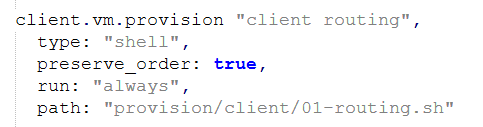


Рис. 20: Переписываем Vagrantfile

1. Зафиксируйте внесённые изменения для внутренних настроек виртуальной машины client и запустите её, введя в терминале: vagrant up client –provision.
2. После загрузки виртуальной машины client вы можете увидеть на виртуальной машине server на терминале с мониторингом происходящих в системе процессов записи о подключении к виртуальной внутренней сети узла client и выдачи ему IP-адреса из соответствующего диапазона адресов. Также информацию о работе DHCP-сервера можно наблюдать в файле /var/lib/kea/kea-leases4.csv. В отчёте прокомментируйте построчно информацию из этого файла.(рис. 21).

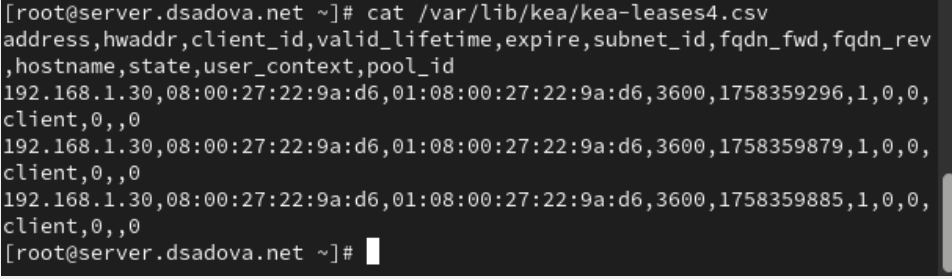


Рис. 21: Просматриваем что leases4.csv появился

Файл /var/lib/kea/kea-leases4.csv содержит историю аренды IPv4 адресов сервером Kea DHCP.

Строка 1-2: Заголовок с полями:

* address - IP-адрес
* hwaddr - MAC-адрес клиента
* client\_id - идентификатор клиента
* valid\_lifetime - время жизни аренды (секунды)
* expire - timestamp истечения аренды
* subnet\_id - ID подсети
* fqdn\_fwd, fqdn\_rev - флаги DNS-записей
* hostname - имя хоста
* state - состояние аренды
* user\_context, pool\_id - дополнительные параметры

Строка 3: 192.168.1.30,08:00:27:22:9a:d6,01:08:00:27:22:9a:d6,3600,1758359296,1,0,0,,client,0,,0

Адрес: 192.168.1.30. MAC: 08:00:27:22:9a:d6 (вероятно виртуальная машина VirtualBox). Время жизни: 3600 секунд (1 час). Истекает: 1758359296 (Unix timestamp). Подсеть: ID 1. Имя хоста: client. Состояние: 0 (активная/нормальная аренда)

Строка 4: 192.168.1.30,08:00:27:22:9a:d6,01:08:00:27:22:9a:d6,3600,1758359879,1,0,0,,client,0,,0

Обновление аренды того же клиента. Новое время истечения: 1758359879. Увеличение времени аренды

Строка 5: 192.168.1.30,08:00:27:22:9a:d6,01:08:00:27:22:9a:d6,3600,1758359885,1,0,0,,client,0,,0

1. Войдите в систему виртуальной машины client под вашим пользователем и откройте терминал. В терминале введите(рис. 22).

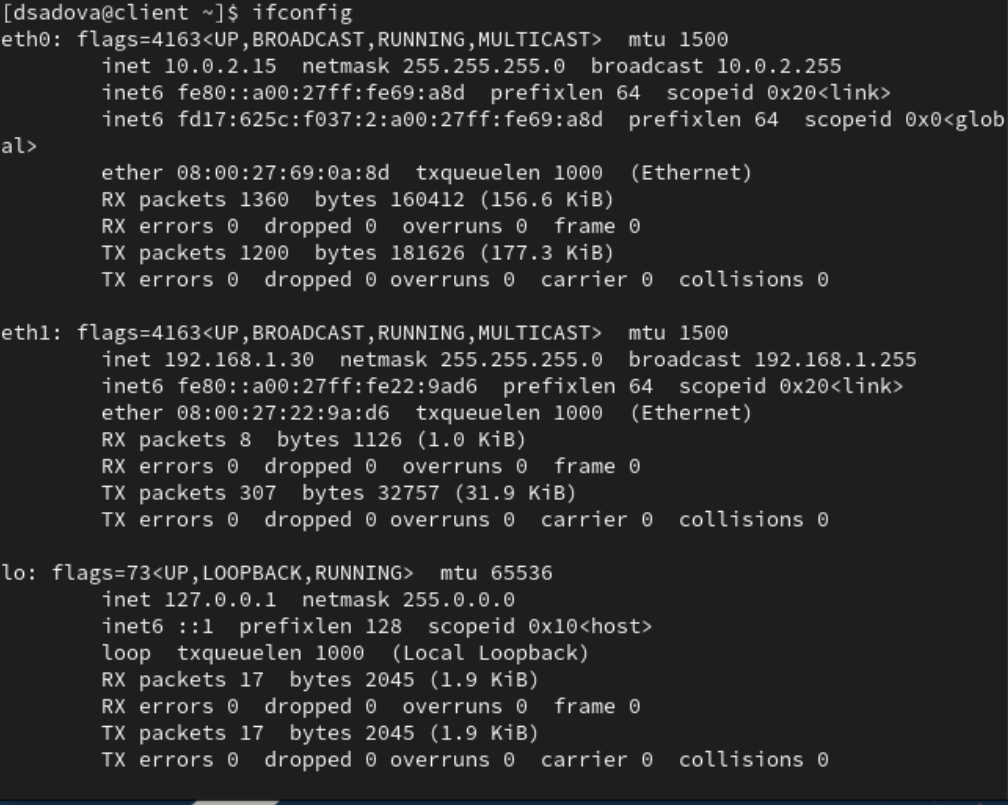


Рис. 22: Заходим в client

На экран будет выведена информация об имеющихся интерфейсах. Прокомментируйте её построчно в отчёте.

Система имеет три сетевых интерфейса - eth0, eth1 и loopback (lo). Интерфейс eth1 соответствует записям из DHCP-сервера.

Интерфейс eth0:

* flags=4163<UP,BROADCAST,RUNNING,MULTICAST> - интерфейс активен, поддерживает широковещание и multicast
* inet 10.0.2.15 - IPv4 адрес (вероятно NAT-интерфейс VirtualBox)
* netmask 255.255.255.0 - маска подсети класса C
* broadcast 10.0.2.255 - широковещательный адрес
* inet6 fe80::a00:27ff:fe69:a8d - link-local IPv6 адрес
* inet6 fdl7:625c:f037:2:a00:27ff:fe69:a8d - глобальный IPv6 адрес (с ошибкой в записи)
* ether 08:00:27:69:0a:8d - MAC-адрес интерфейса

Интерфейс eth1 (основной интерес):

* flags=4163<UP,BROADCAST,RUNNING,MULTICAST> - интерфейс активен
* inet 192.168.1.30 - IPv4 адрес, совпадает с арендой из DHCP-сервера
* netmask 255.255.255.0 - маска подсети
* broadcast 192.168.1.255 - широковещательный адрес
* inet6 fe80::a00:27ff:fe22:9ad6 - link-local IPv6 адрес
* ether 08:00:27:22:9a:d6 - MAC-адрес, полностью совпадает с записью в DHCP: 08:00:27:22:9a:d6

Интерфейс lo (loopback):

* flags=73<UP,LOOPBACK,RUNNING> - loopback интерфейс активен
* inet 127.0.0.1 - стандартный loopback адрес
* netmask 255.0.0.0 - маска класса A
* inet6 ::1 - IPv6 loopback адрес

1. На машине server посмотрите список выданных адресов:(рис. 23).

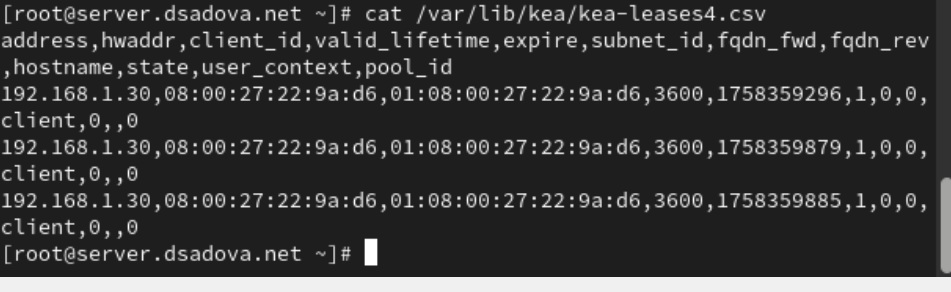


Рис. 23: Просматриваем список выданных адресов

Прокомментируйте построчно в отчёте.

Файл /var/lib/kea/kea-leases4.csv содержит историю аренды IPv4 адресов сервером Kea DHCP.

Строка 1-2: Заголовок с полями:

* address - IP-адрес
* hwaddr - MAC-адрес клиента
* client\_id - идентификатор клиента
* valid\_lifetime - время жизни аренды (секунды)
* expire - timestamp истечения аренды
* subnet\_id - ID подсети
* fqdn\_fwd, fqdn\_rev - флаги DNS-записей
* hostname - имя хоста
* state - состояние аренды
* user\_context, pool\_id - дополнительные параметры

Строка 3: 192.168.1.30,08:00:27:22:9a:d6,01:08:00:27:22:9a:d6,3600,1758359296,1,0,0,,client,0,,0

Адрес: 192.168.1.30. MAC: 08:00:27:22:9a:d6 (вероятно виртуальная машина VirtualBox). Время жизни: 3600 секунд (1 час). Истекает: 1758359296 (Unix timestamp). Подсеть: ID 1. Имя хоста: client. Состояние: 0 (активная/нормальная аренда)

Строка 4: 192.168.1.30,08:00:27:22:9a:d6,01:08:00:27:22:9a:d6,3600,1758359879,1,0,0,,client,0,,0

Обновление аренды того же клиента. Новое время истечения: 1758359879. Увеличение времени аренды

Строка 5: 192.168.1.30,08:00:27:22:9a:d6,01:08:00:27:22:9a:d6,3600,1758359885,1,0,0,,client,0,,0

Еще одно обновление аренды. Последнее записанное время истечения: 1758359885

### 2.2.4 Настройка обновления DNS-зоны

Требуется настроить обновление DNS-зоны при появлении в виртуальной внутренней сети новых узлов.

1. Создадим ключ на сервере с Bind9 (на виртуальной машине server):(рис. 24).

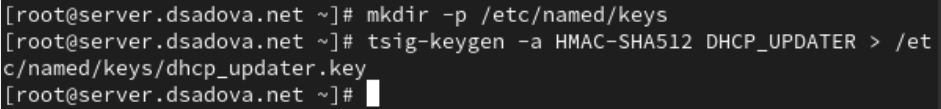


Рис. 24: Создаем ключ

1. Файл /etc/named/keys/dhcp\_updater.key будет иметь следующий вид:(рис. 25).

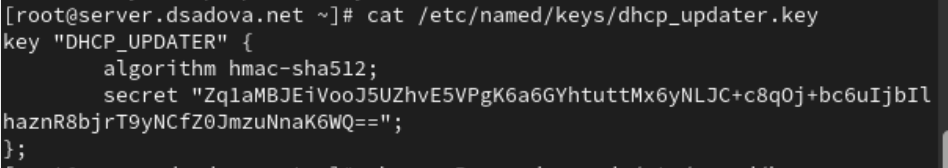


Рис. 25: Просматриваем ключ

1. Поправим права доступа:(рис. 26).

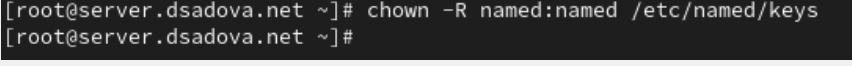


Рис. 26: Меняем права доступа

1. Подключим ключ в файле /etc/named.conf:(рис. 27).

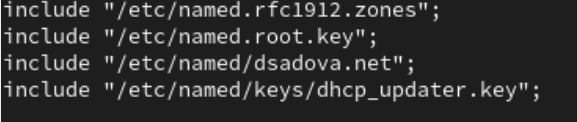


Рис. 27: Подключаем ключ

1. На виртуальной машине server под пользователем с правами суперпользователя отредактируйте файл /etc/named/user.net (вместо user укажите свой логин), разрешив обновление зоны:(рис. 28).



Рис. 28: Обнавляем зоны

1. Сделаем проверку конфигурационного файла:(рис. 29).

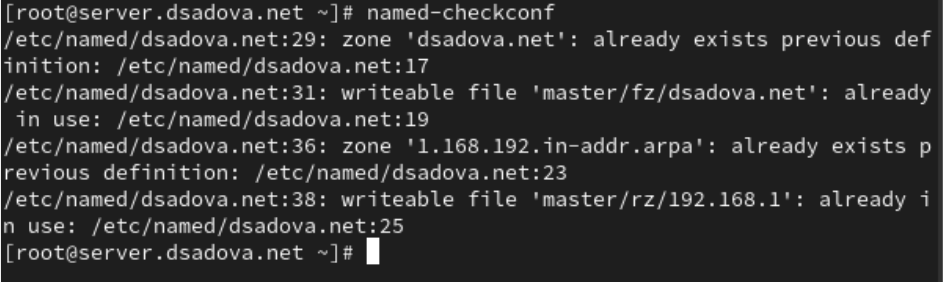


Рис. 29: Проверка конфигурационного файла

1. Перезапустите DNS-сервер:(рис. 30).

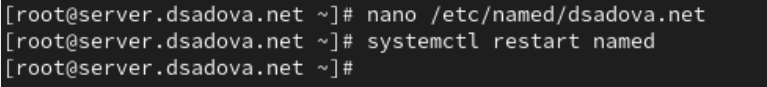


Рис. 30: Перезагружаем DNS-сервер

1. Сформируем ключ для Kea. Файл ключа назовём /etc/kea/tsig-keys.json:(рис. 31).

Формируем ключ

Рис. 31: Формируем ключ

1. Перенесём ключ на сервер Kea DHCP и перепишем его в формате json:(рис. 32).

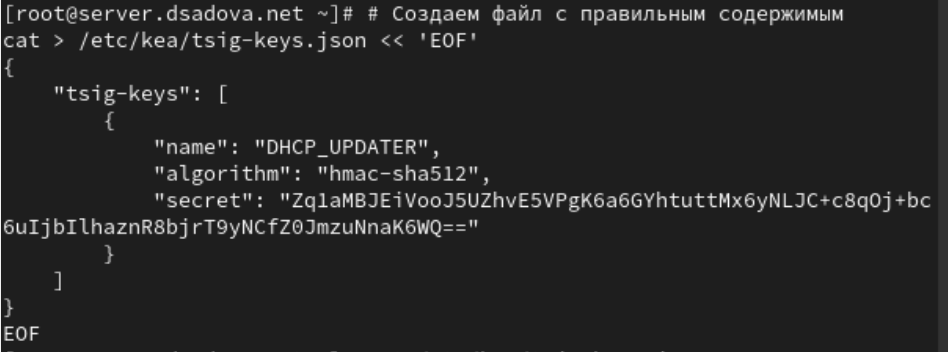


Рис. 32: Переносим ключ на сервер

1. Сменим владельца:(рис. 33).

Меняем владельца

Рис. 33: Меняем владельца

1. Поправим права доступа:(рис. 34).

Меняем права доступа

Рис. 34: Меняем права доступа

1. Настройка происходит в файле /etc/kea/kea-dhcp-ddns.conf:(рис. 35).



Рис. 35: Настраиваем

Обратите особое внимание на точку в конце имени зоны, иначе DDNS завершится сбоем и сообщит, что не удалось найти соответствующее полное доменное имя.

1. Изменим владельца файла:(рис. 36).

Меняем владельца

Рис. 36: Меняем владельца

1. Проверим файл на наличие возможных синтаксических ошибок:(рис. 37).

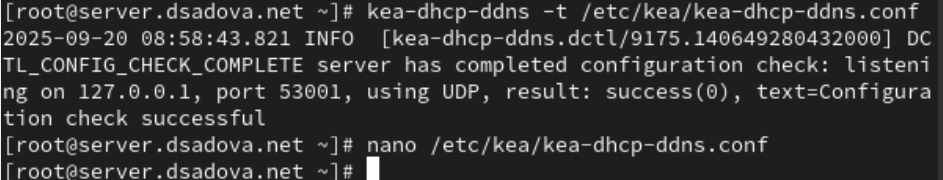


Рис. 37: Проверяем файл

1. Запустим службу ddns:(рис. 38).

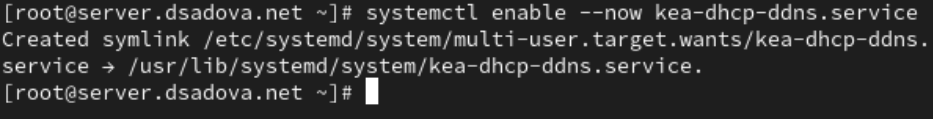


Рис. 38: Запускаем службу

1. Проверим статус работы службы:(рис. 39).

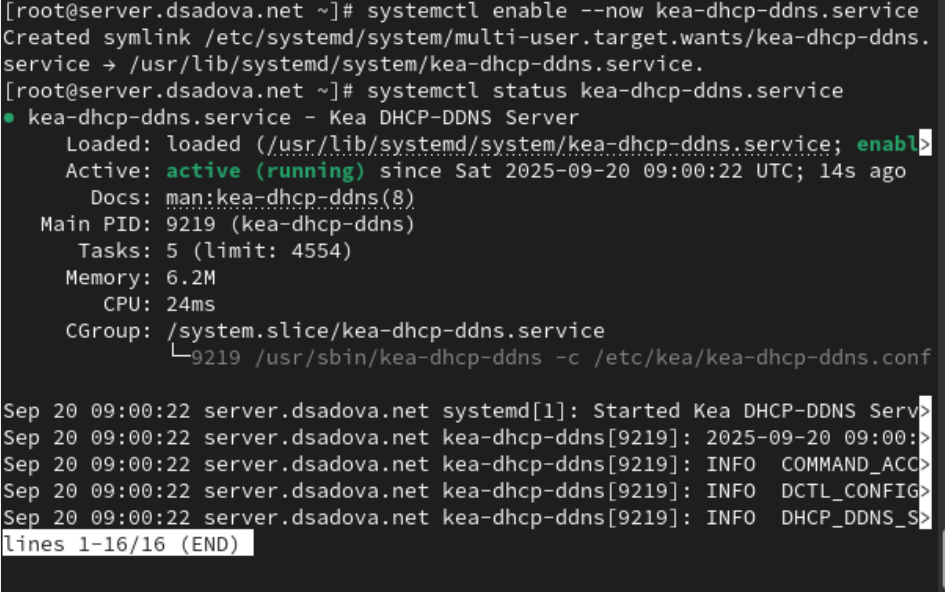


Рис. 39: Проверяем статус

1. Внесите изменения в конфигурационный файл /etc/kea/kea-dhcp4.conf, добавив в него разрешение на динамическое обновление DNS-записей с локального узла прямой и обратной зон:(рис. 40).

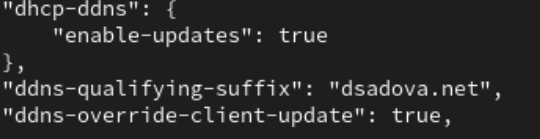


Рис. 40: Вносим изменения в файл

1. Проверим файл на наличие возможных синтаксических ошибок:(рис. 41).

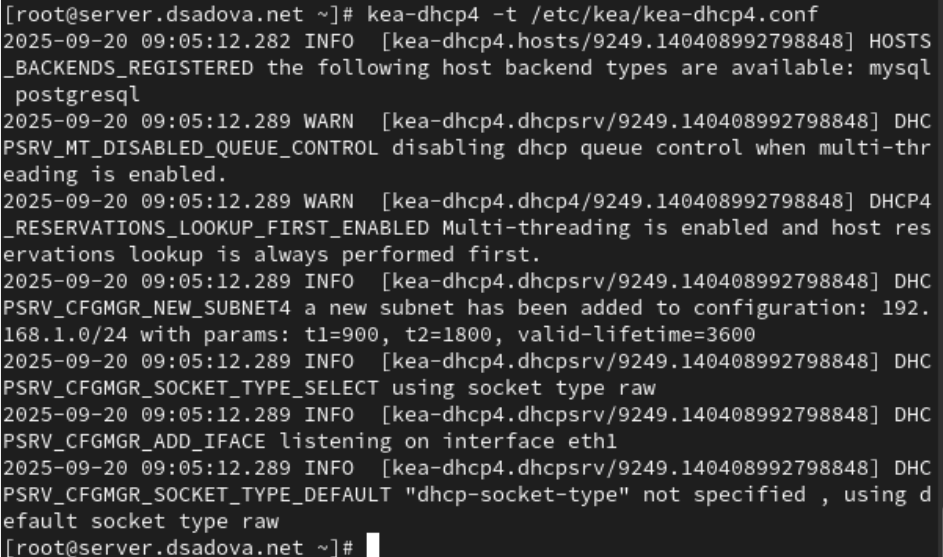


Рис. 41: Проверяем статус

1. Перезапустите DHCP-сервер:(рис. 42).

Перезапускаем сервер

Рис. 42: Перезапускаем сервер

1. Проверим статус:(рис. 43).

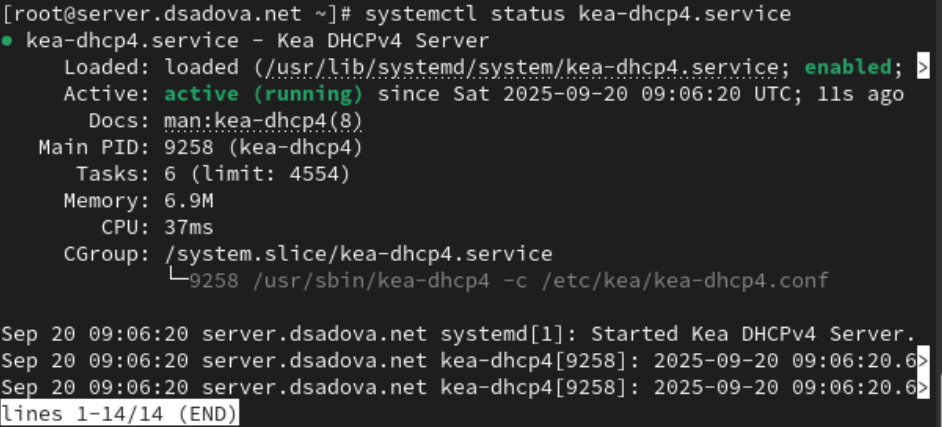


Рис. 43: Проверяем статус

1. На машине client переполучите адрес:(рис. 44).

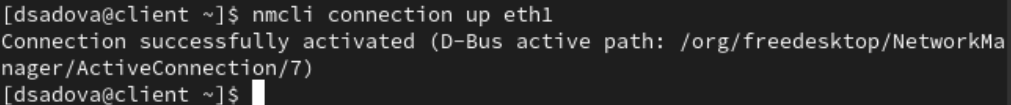


Рис. 44: На client получаем адрес

1. В каталоге прямой DNS-зоны /var/named/master/fz должен появиться файл user.net.jnl, в котором в бинарном файле автоматически вносятся изменения записей зоны.(рис. 45).



Рис. 45: Проверяем наличие файла

### 2.2.5 Анализ работы DHCP-сервера после настройки обновления DNS-зоны

На виртуальной машине client под вашим пользователем откройте терминал и с помощью утилиты dig убедитесь в наличии DNS-записи о клиенте в прямой DNS-зоне:(рис. 46).

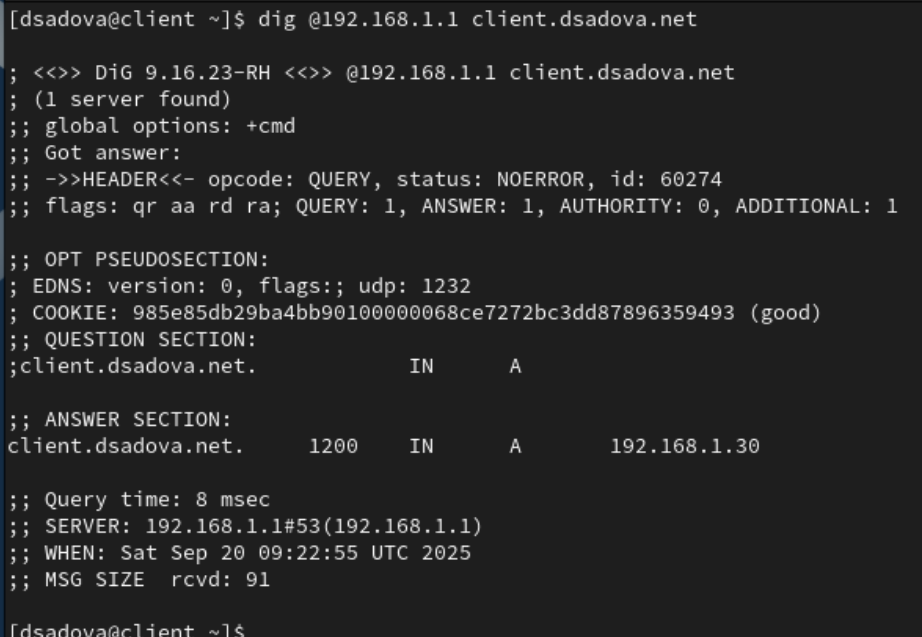


Рис. 46: Убедимся в наличии DNS-записи о клиенте в прямой DNS-зоне

В отчёте построчно прокомментируйте выведенную на экран информацию.

* opcode: QUERY - тип операции: запрос
* status: NOERROR - успешное выполнение
* id: 60274 - идентификатор запроса
* flags: qr aa rd ra - флаги: qr - это ответ (query response), aa - авторитетный ответ (authoritative answer), rd - рекурсия запрошена (recursion desired), ra - рекурсия доступна (recursion available)

Секция QUESTION:

* client.dsadova.net. IN A - запрос IPv4 адреса для client.dsadova.net

Секция ANSWER:

* client.dsadova.net. 1200 IN A 192.168.1.30 - ключевой результат!
* Время жизни записи: 1200 секунд (20 минут)
* Класс: IN (Internet)
* Тип: A (IPv4 адрес)
* Адрес: 192.168.1.30 - полностью совпадает с DHCP-арендой

### 2.2.6 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог dhcp, в который поместите в соответствующие подкаталоги конфигурационные файлы DHCP:(рис. 47).

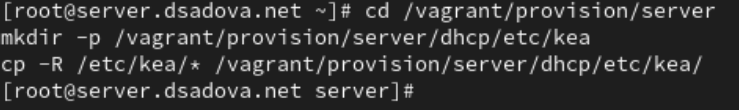


Рис. 47: Создаем каталог dhcp

1. Замените конфигурационные файлы DNS-сервера:(рис. 48).

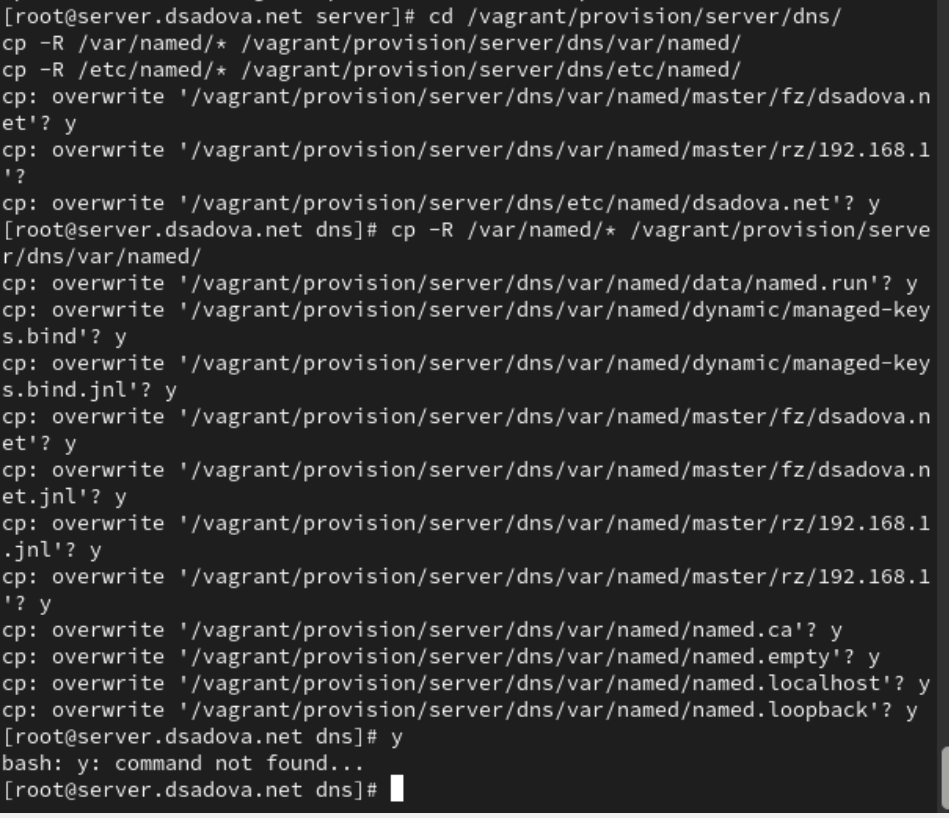


Рис. 48: Переписываем файлы DNS-сервера

1. В каталоге /vagrant/provision/server создайте исполняемый файл dhcp.sh. Открыв его на редактирование, пропишите в нём следующий скрипт: (рис. 49).

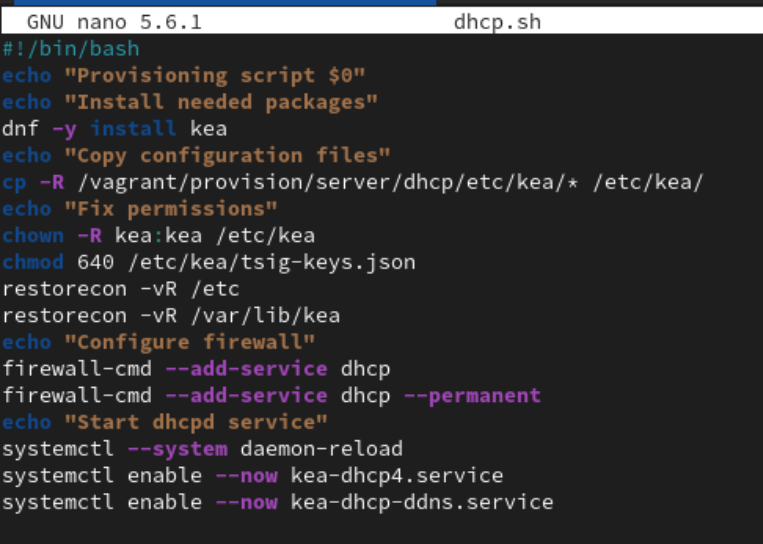


Рис. 49: Создаем исполняемый файл dhcp.sh

Этот скрипт, по сути, повторяет произведённые вами действия по установке и настройке DHCP-сервера.

1. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:(рис. 50).

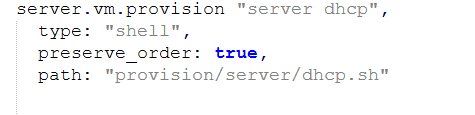


Рис. 50: Переписываем файл Vagrantfile

1. После этого виртуальные машины client и server можно выключить.

# 3 Выводы

Приобрели практические навыки по установке и конфигурированию DHCP-сервера. Решили проблемы и неисправности при настройке и конфигурированию DHCP-сервера.

# Список литературы