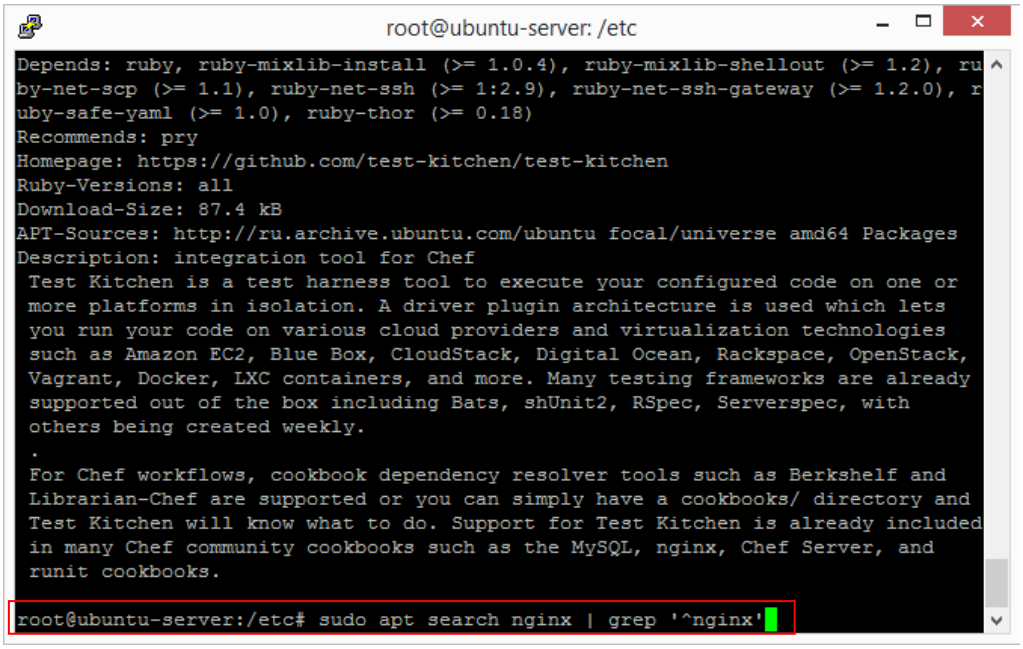
# Практическое задание по уроку №7 «Управление пакетами и репозиториями. Основы сетевой безопасности»

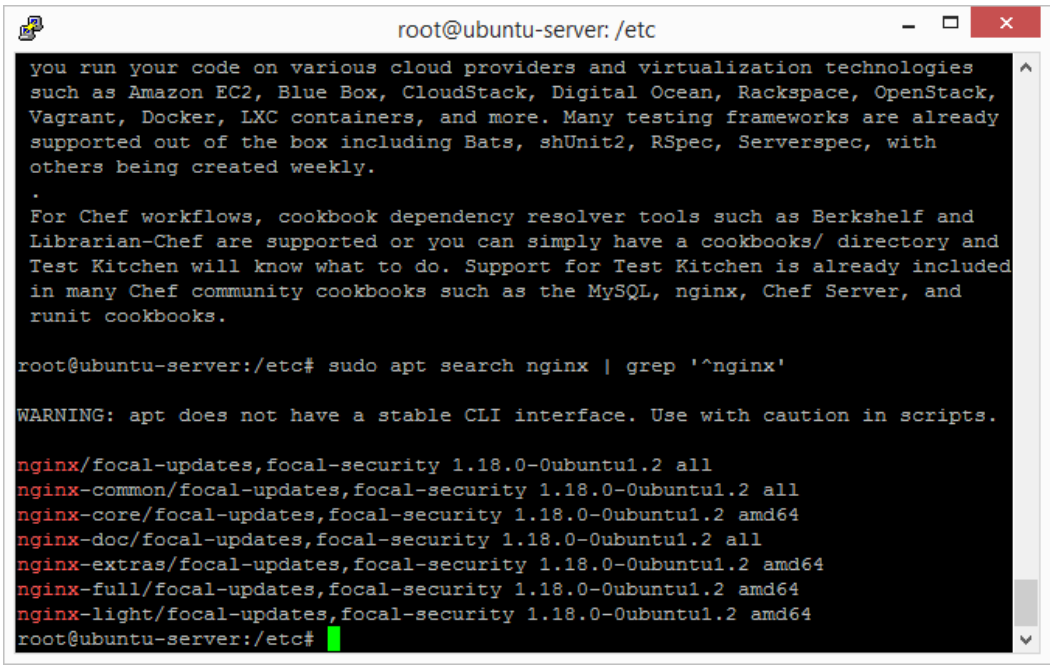
1. Подключить репозиторий с nginx любым удобным способом, установить nginx и потом удалить nginx, используя утилиту dpkg.

Решение

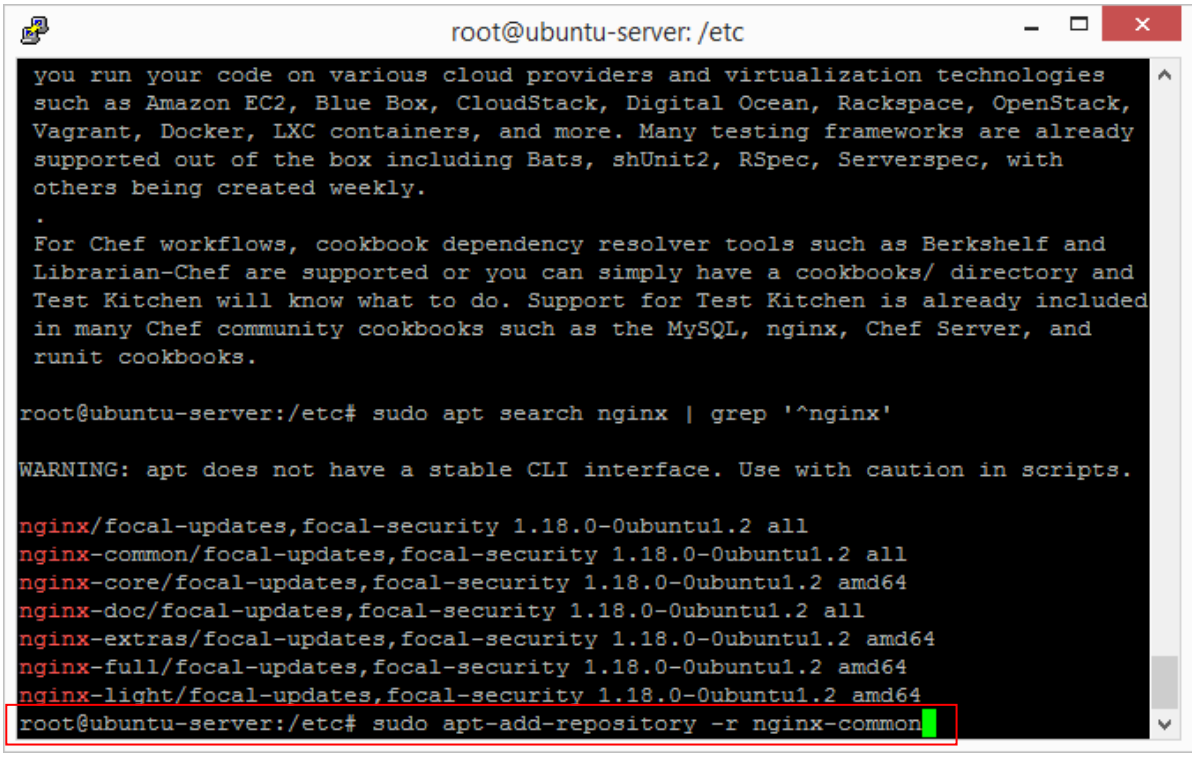
- Первоначально произведем поиск имеющихся репозиториев, включающих пакет nginx. Для этого введем команду suod apt search nginx | grep '^nginx'



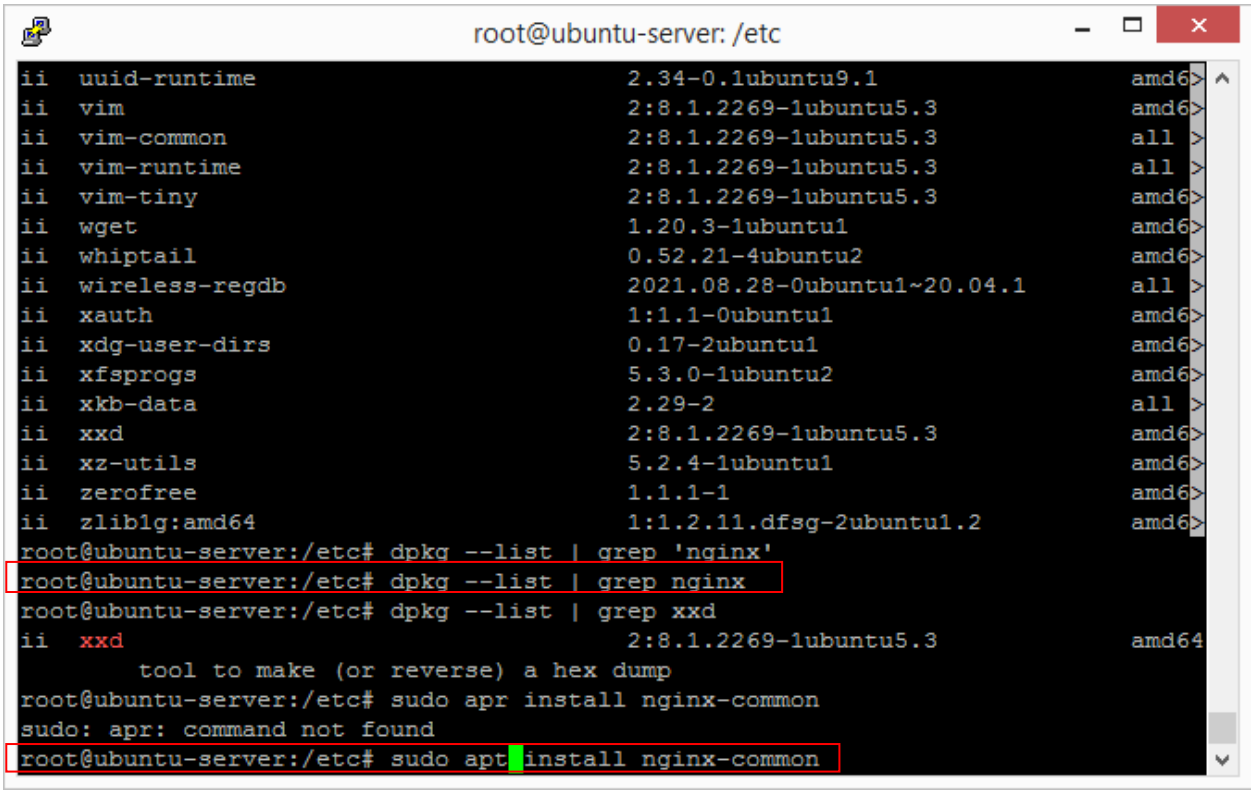

- Результаты поиска будут следующие



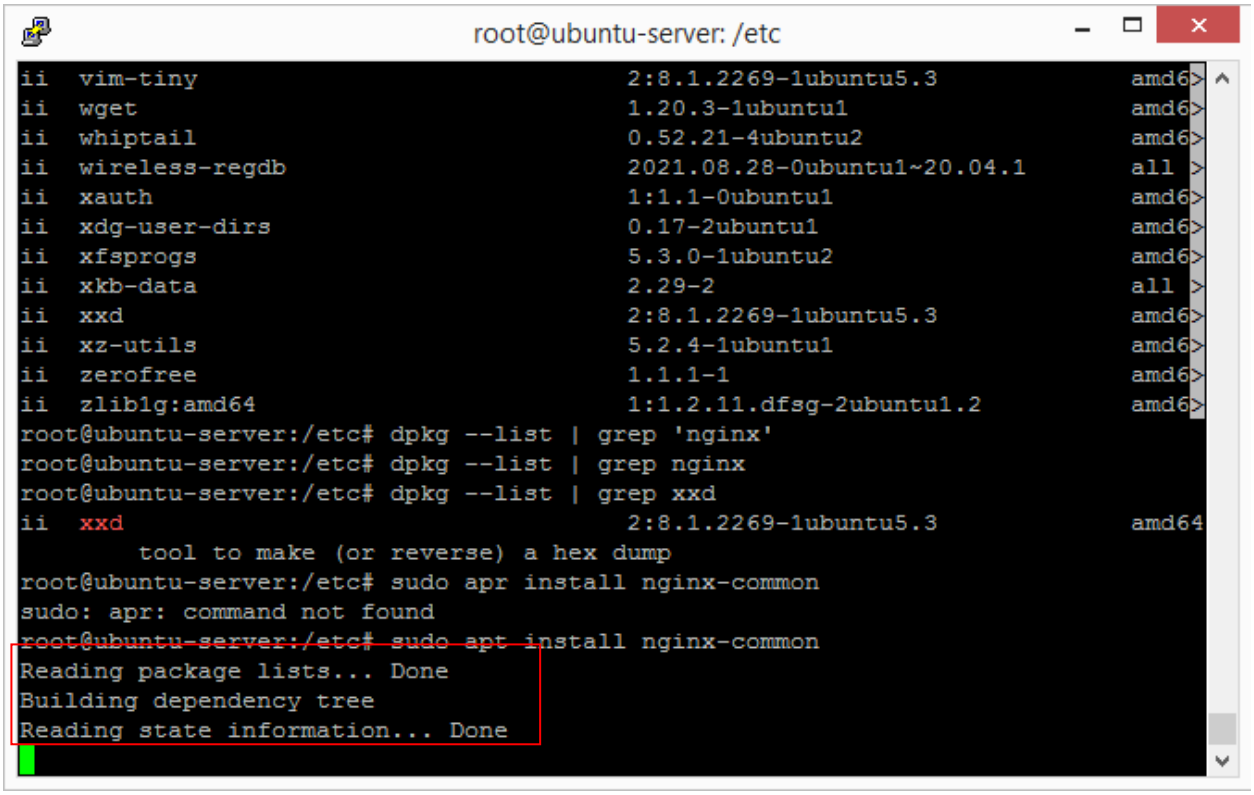
- Выбираем для установки пакет nginx-common и с помощью команды sudo apt-add-repository –r nginx-common подключаем его



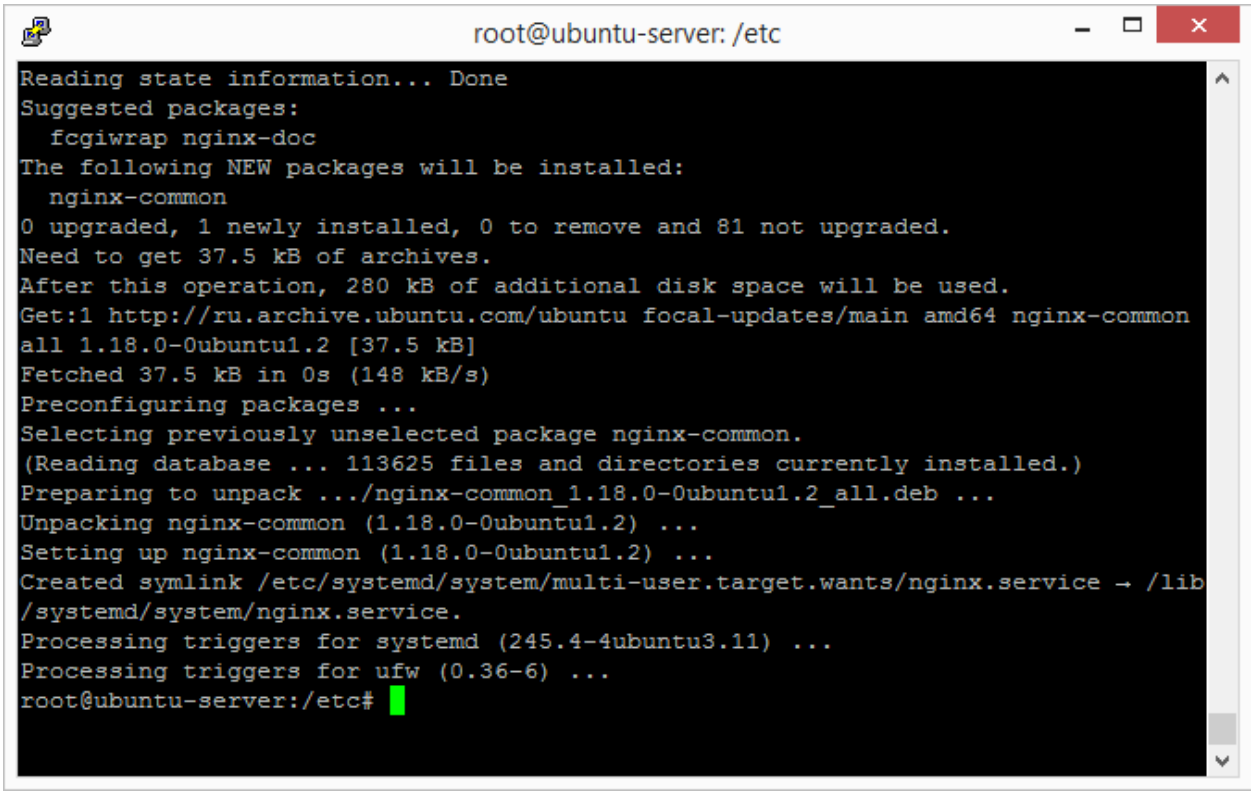

- Проверяем, что в списке установленных репозиториев нет nginx-common и с помощью команды sudo apt install nginx-common устанавливаем пакет



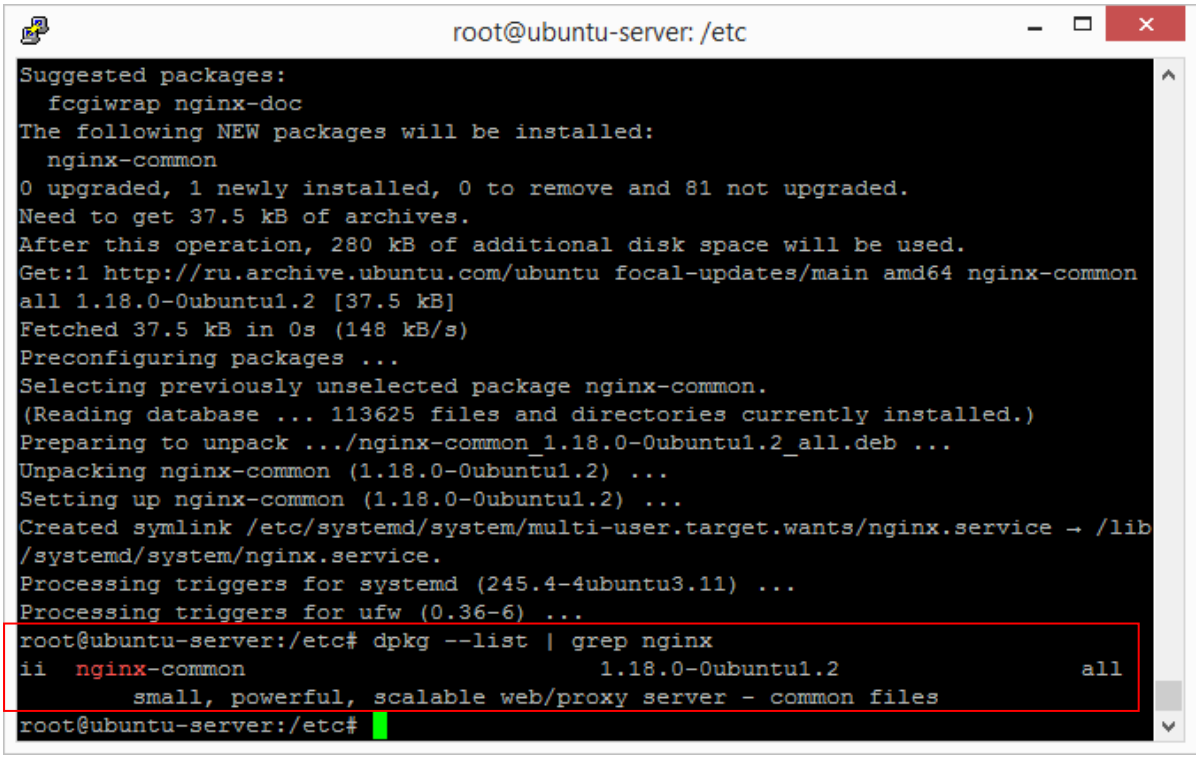
- Процесс установки начался



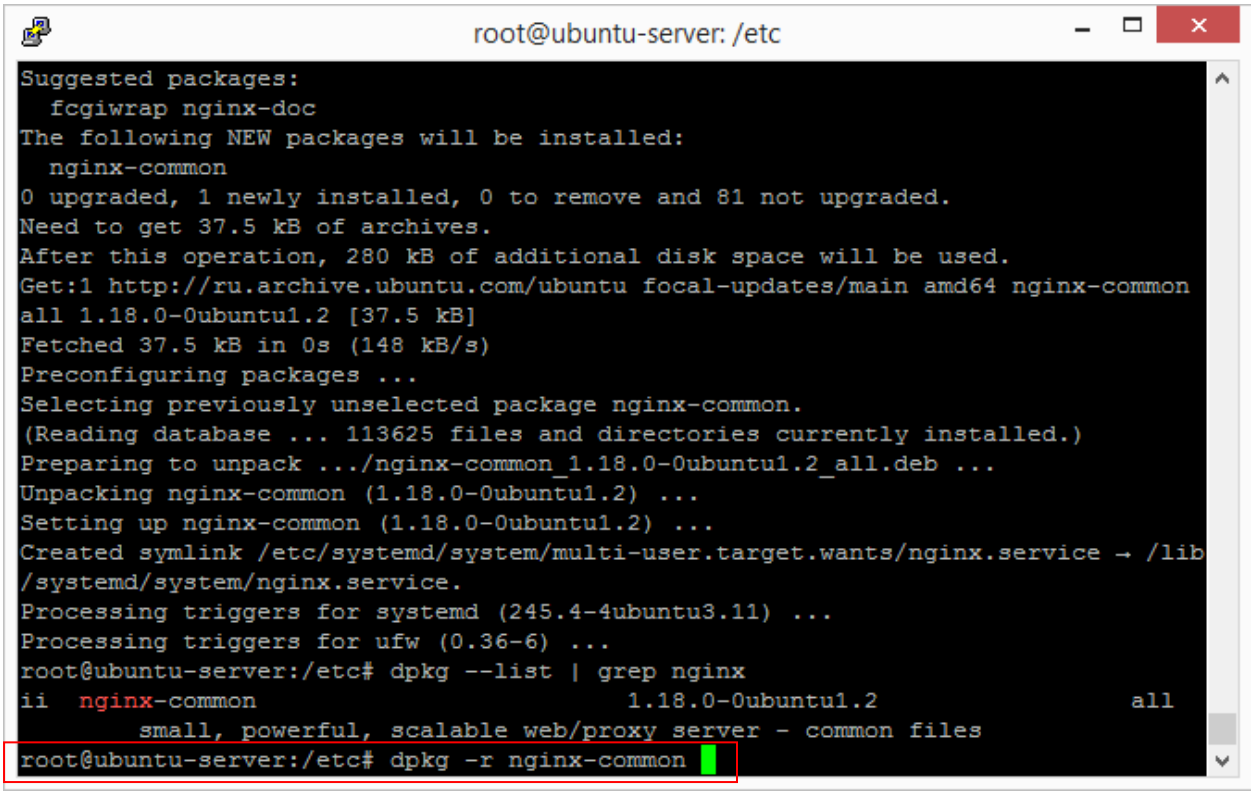

- Пакет nginx-common установлен



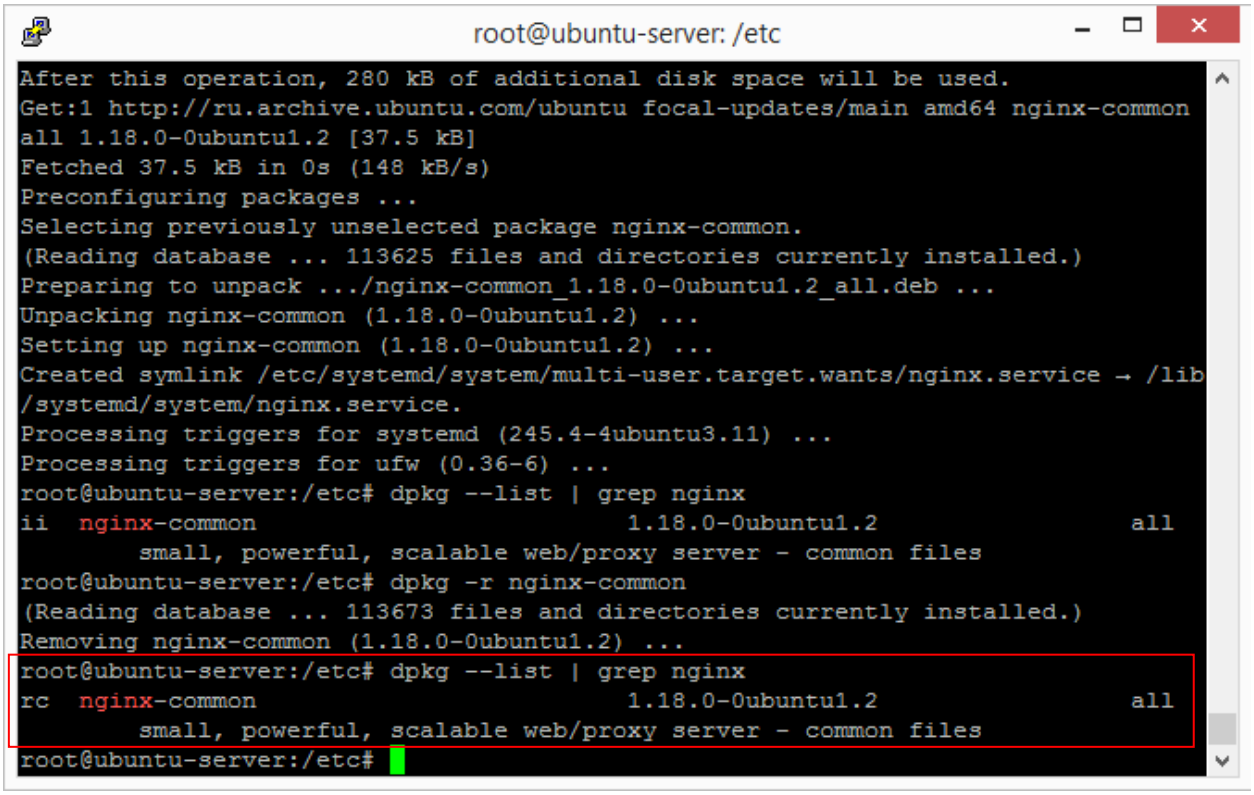
- С помощью команды dpkg --list проверяем, что пакет появился в общем списке. ii означает, что все установлено и работает




- Для удаления пакета с помощью пакетного менеджера dpkg вводим команду dpkg –r nginx-common (аргумент r – remove)

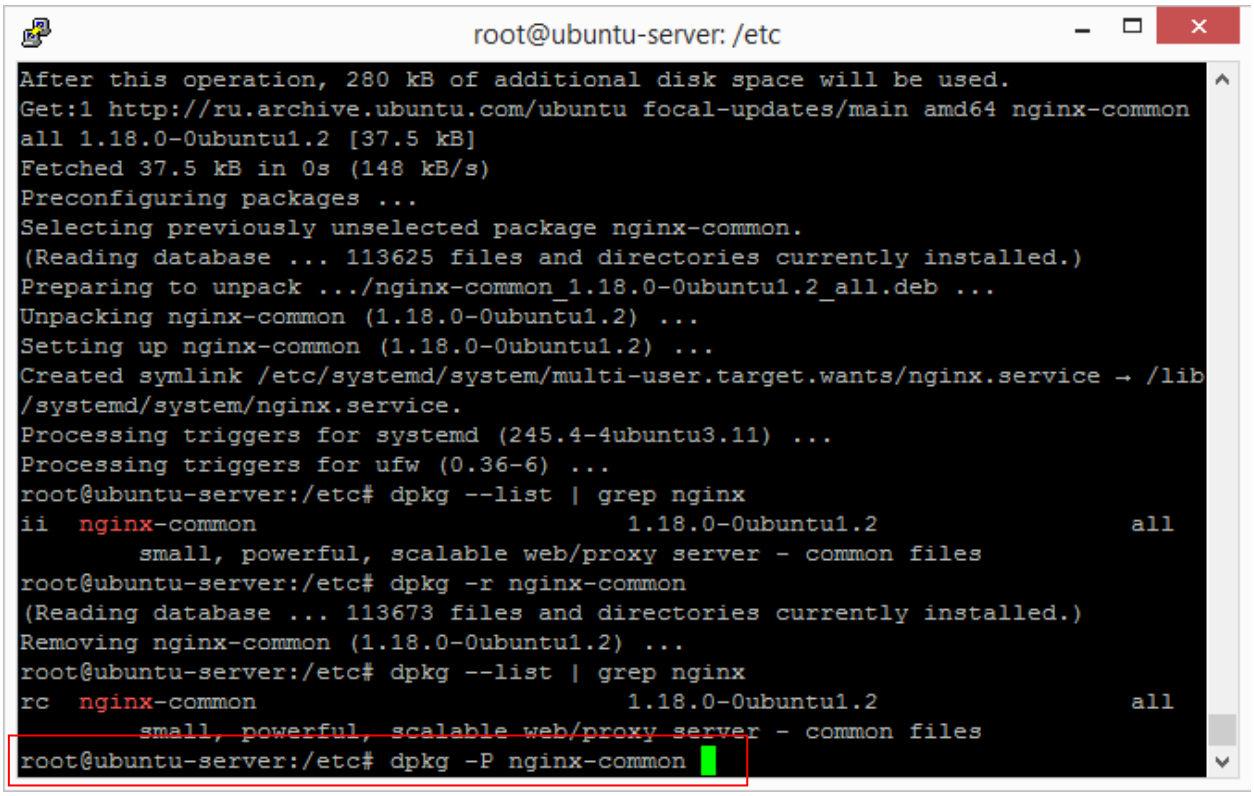


- Проверяем, остался ли пакет в общем списке

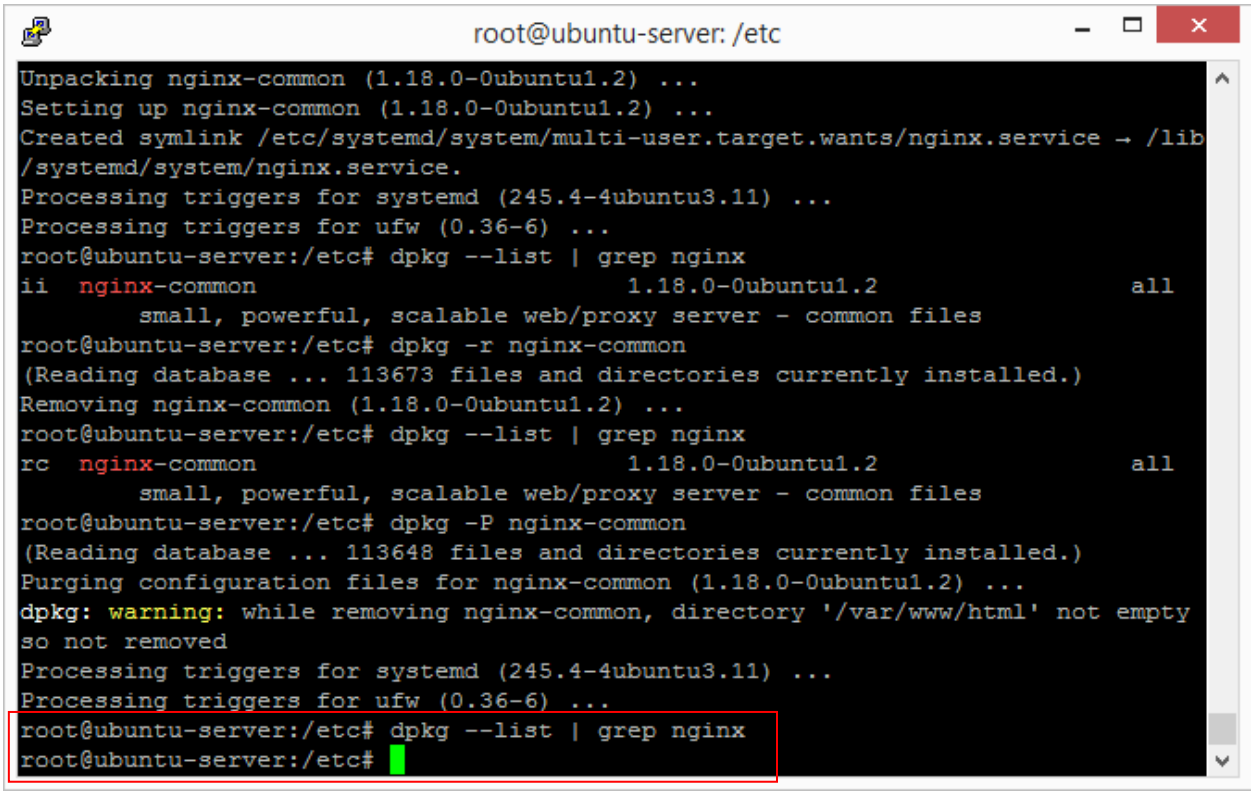



Несмотря на то, что мы его удалили, конфигурация осталась (об этом свидетельствует rc)

- Для полного удаления используем команду dpkg –P nginx-common (p – purge)



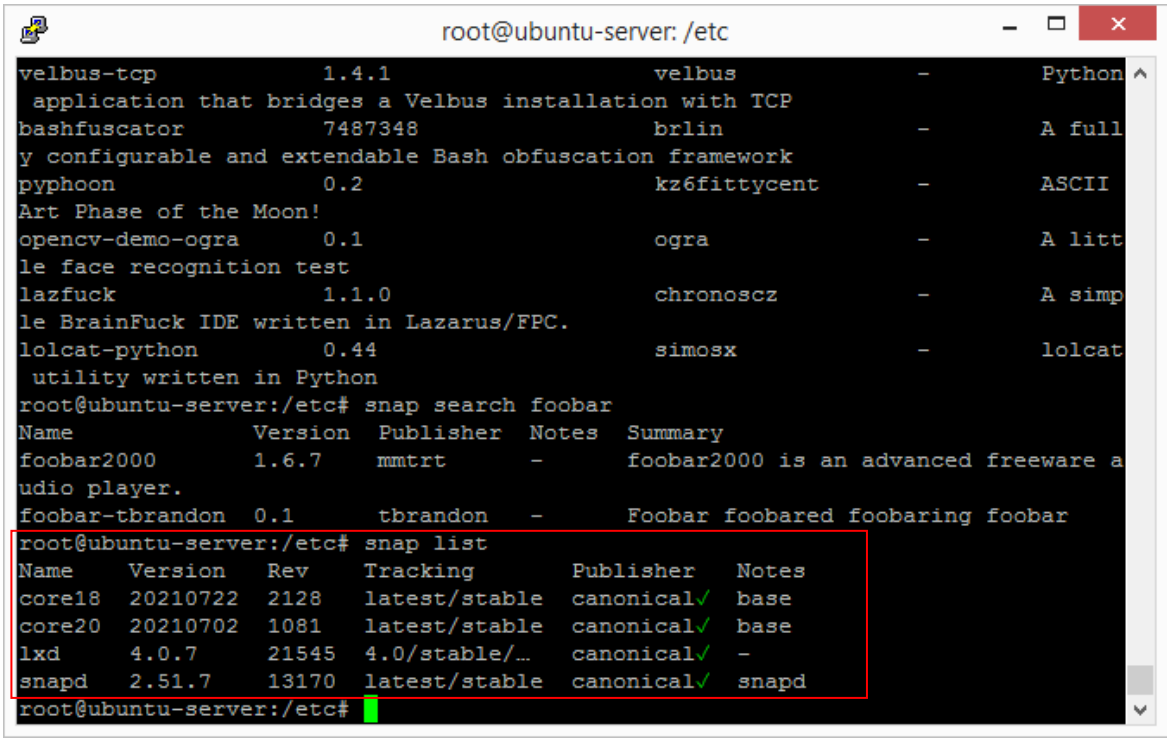
- Убеждаемся, что пакета больше нет в общем списке



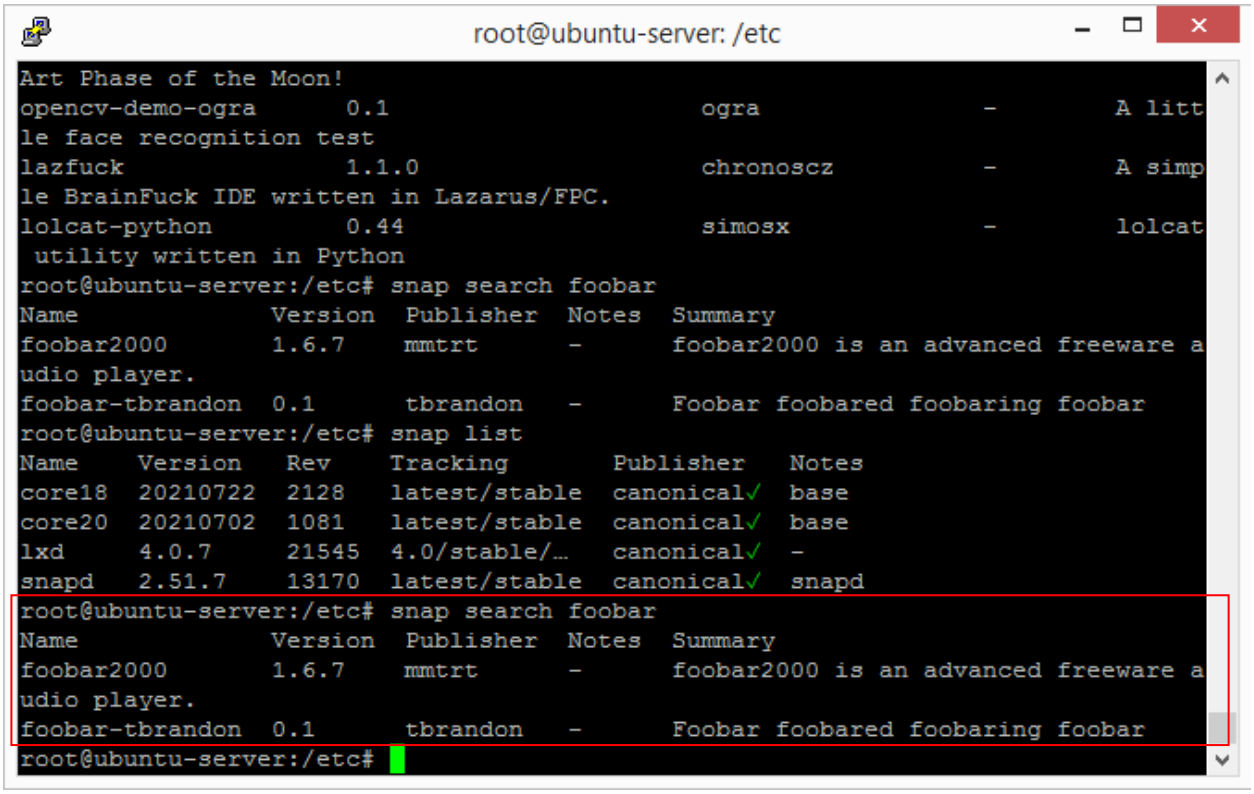
2. Установить пакет на свой выбор используя snap.

Решение

- Первоначально произведем поиск имеющихся пакетов с помощью функции snap list

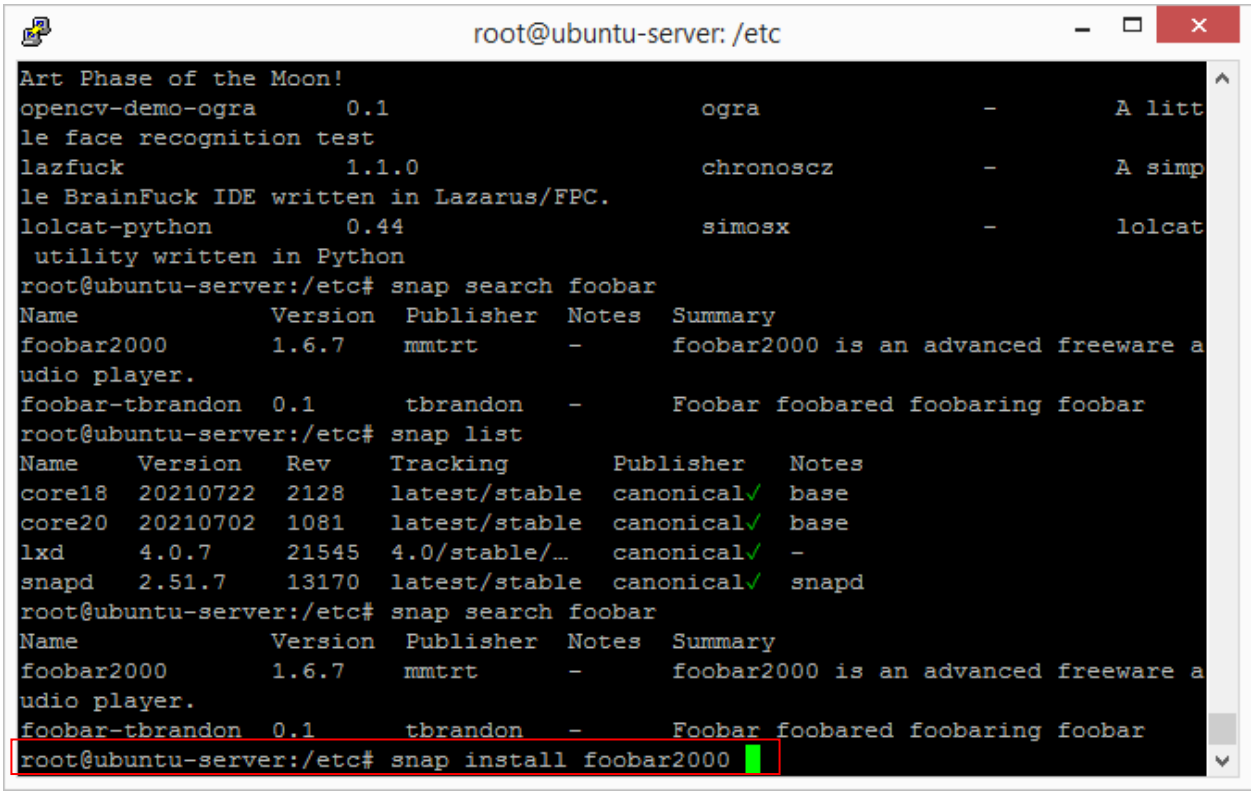



- Рассмотрим для установки пакет приложения для воспроизведения музыки foobar2000. Найдем его с помощью поиска

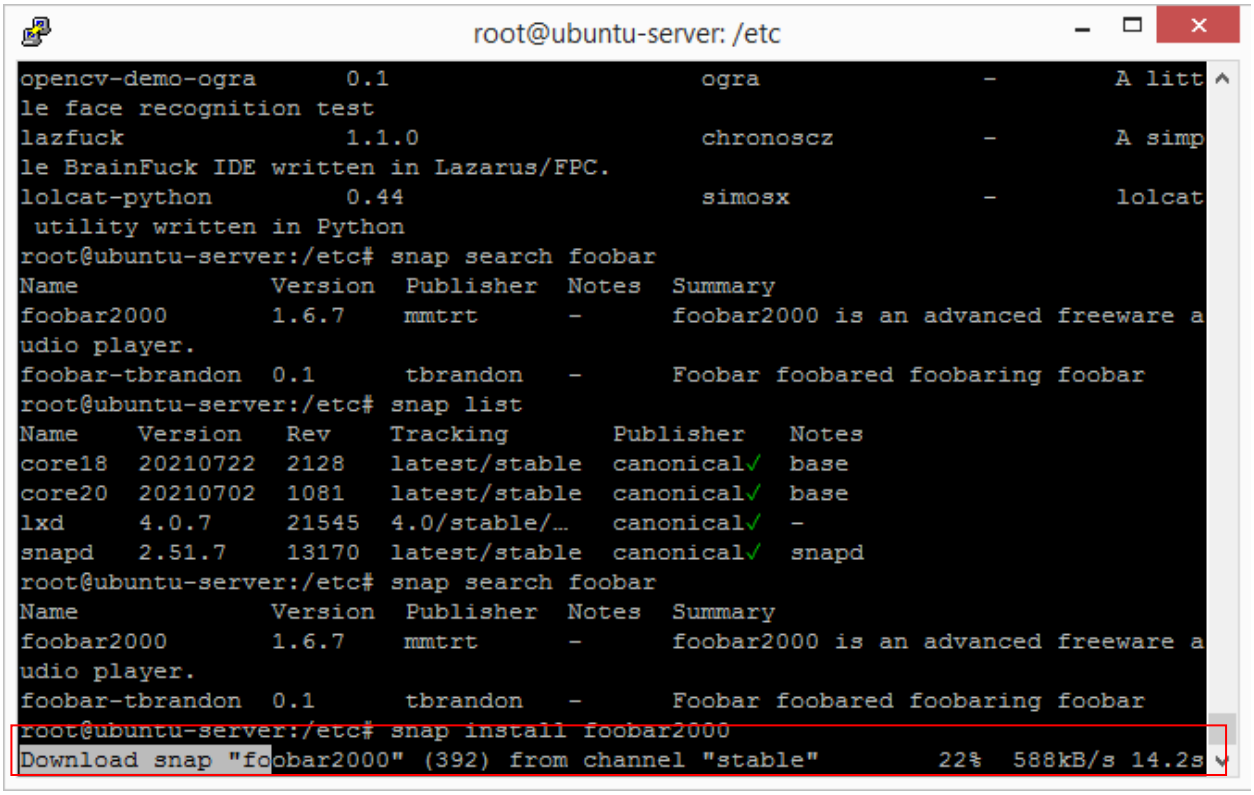



Выберем первый пакет foobar2000

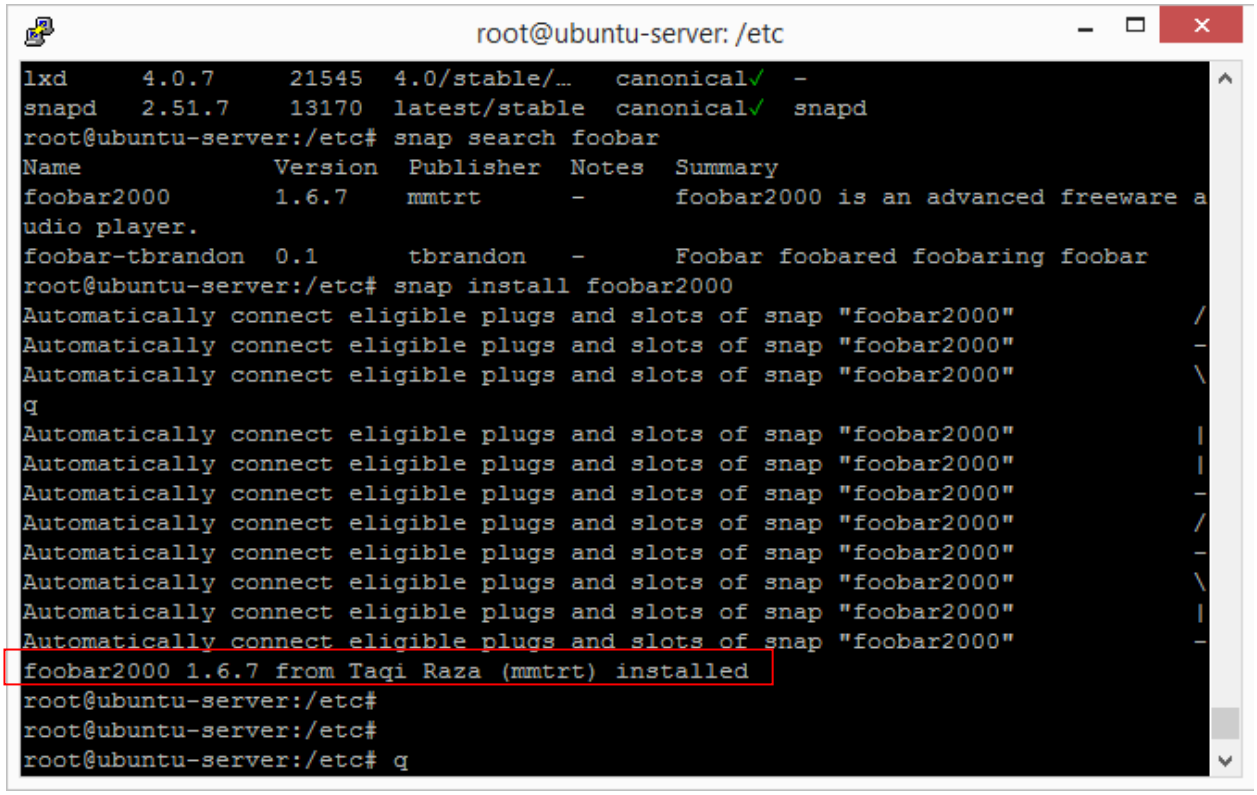
- Запустим установку данного пакета с помощью команды snap install foobar2000



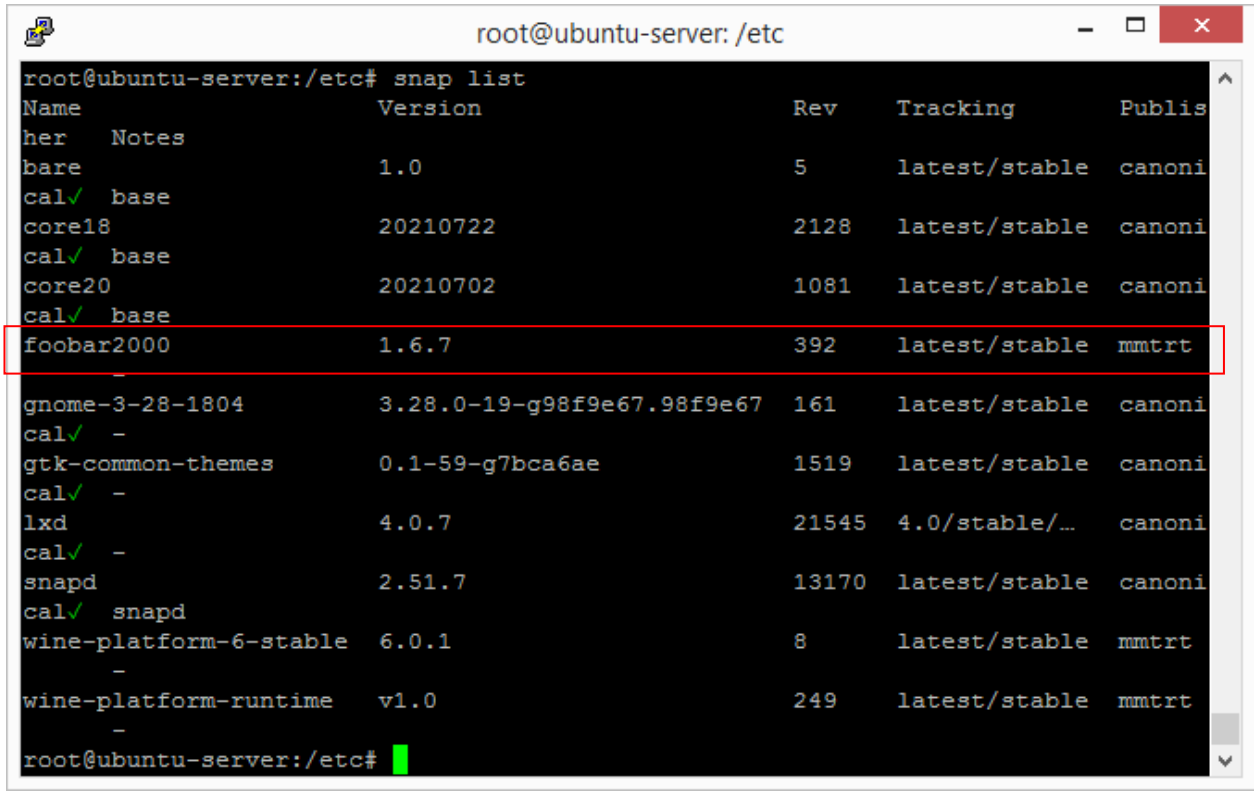

- Процесс установки пошел



- Установка завершена (потребовалось около 4 минут)



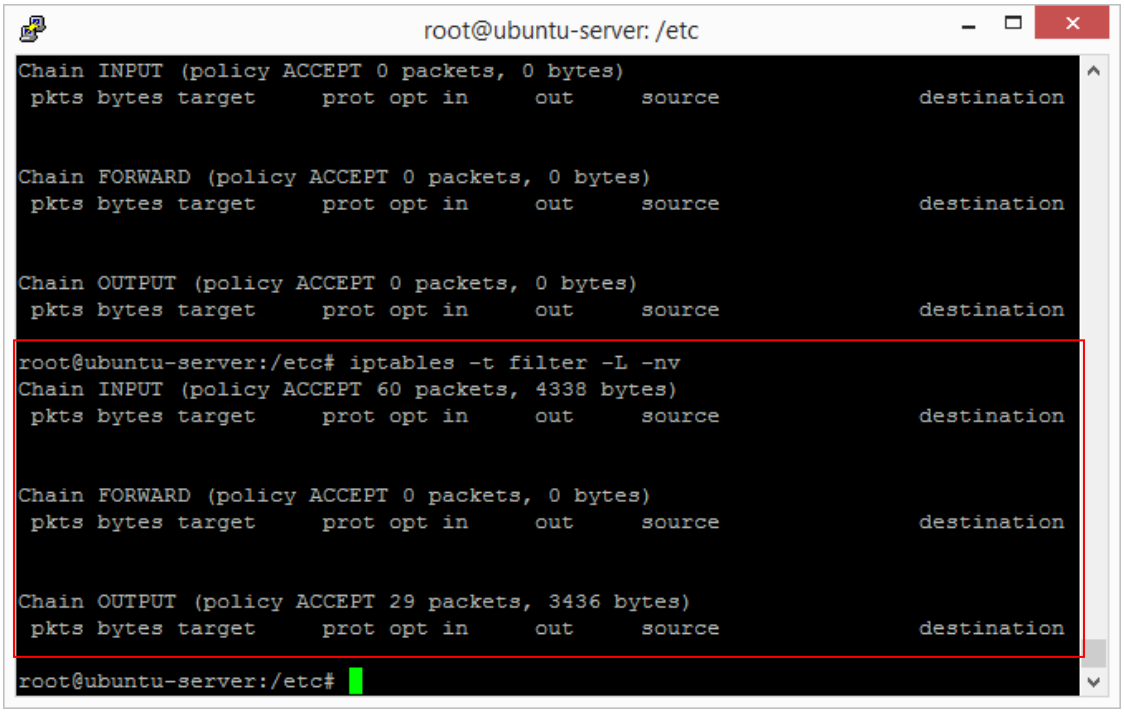

- Проверяем наличие пакета в общем списке с помощью snap list. Пакет имеется



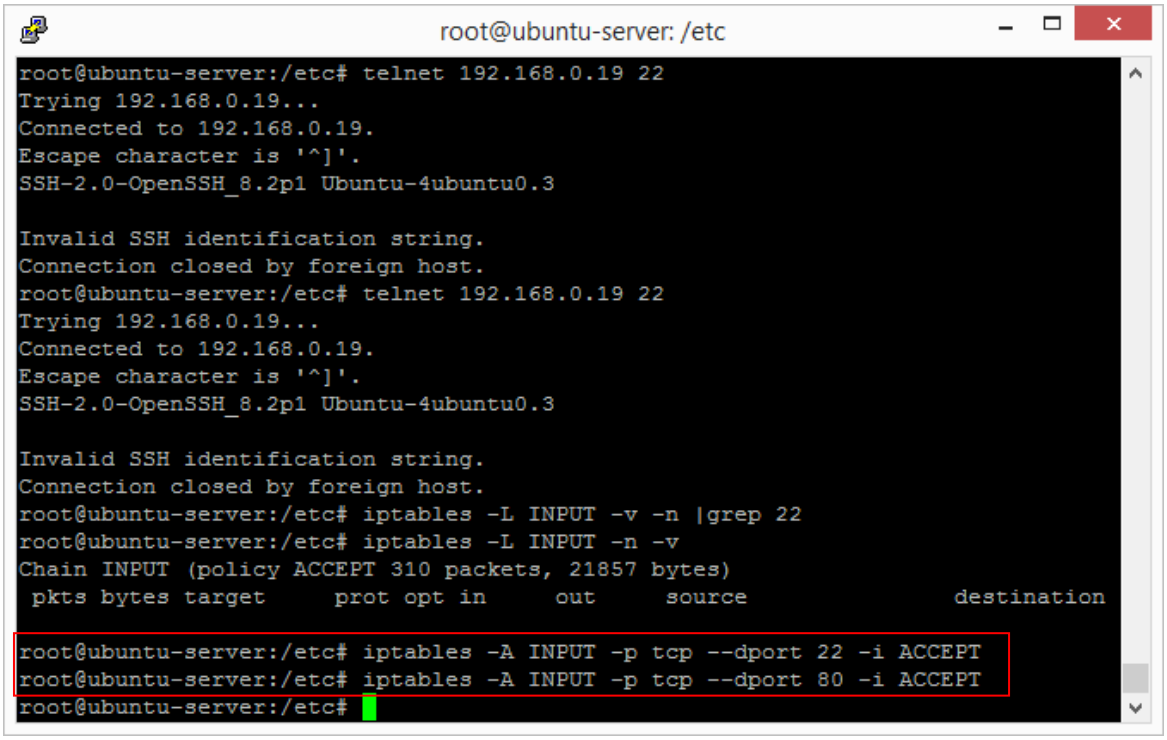
3. Настроить iptables: разрешить подключения только на 22-й и 80-й порты.

Решение

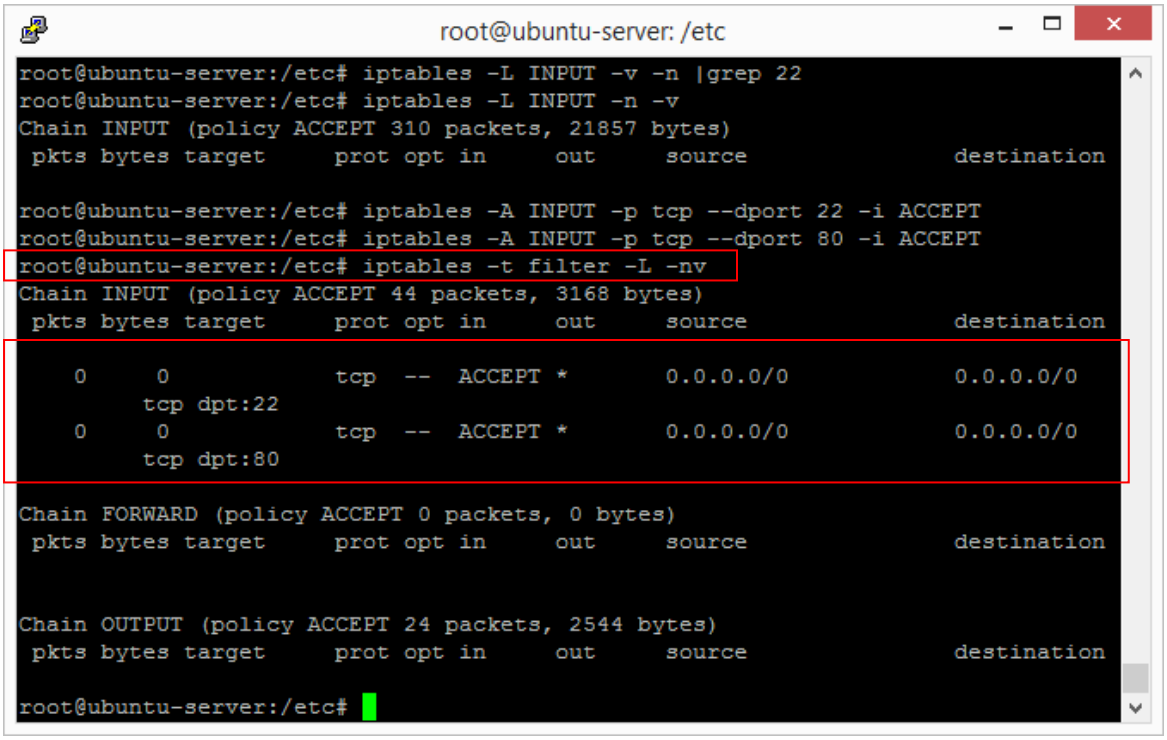
- Проверим существующие на данный момент правил с помощью команды iptables –t filter –L -nv



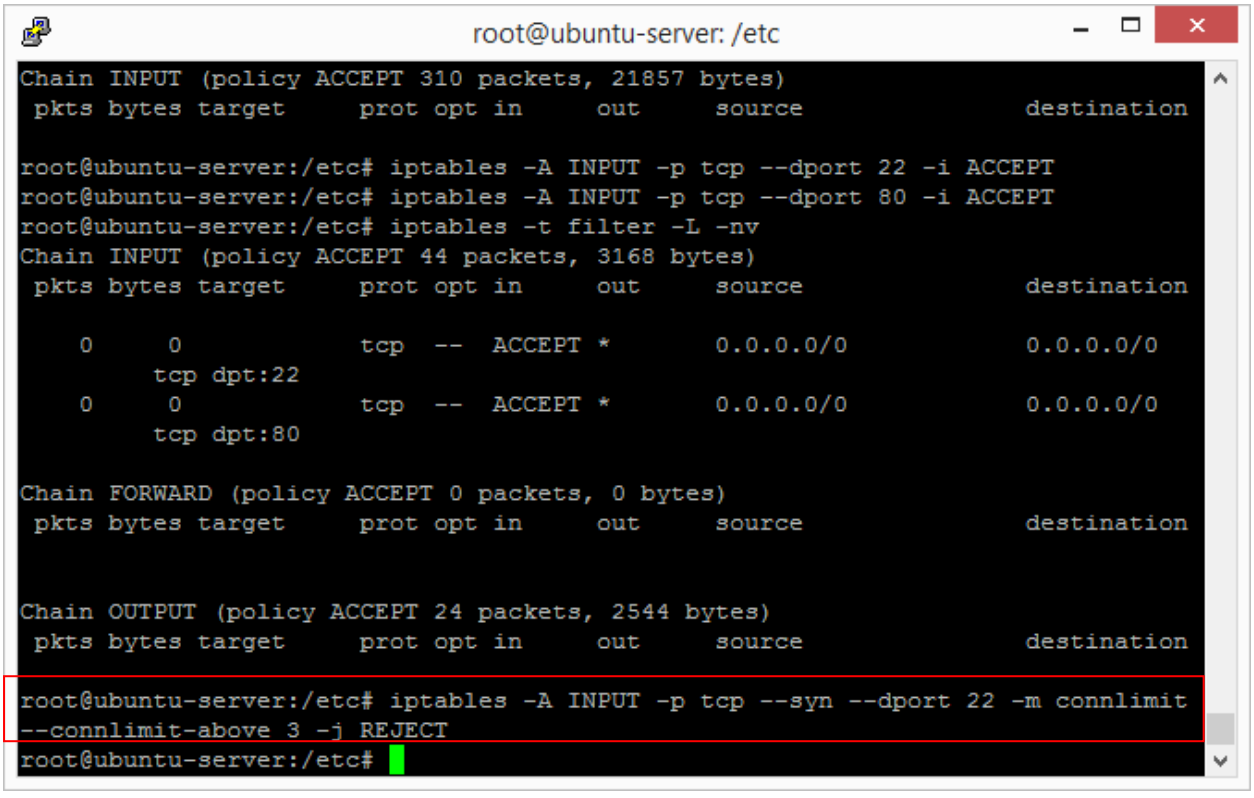

- Откроем порты 22 и 80 (разрешим подключение) с помощью команд iptables –A INPUT –p tcp –dport 22 –I ACCEPT и iptables –A INPUT –p tcp –dport 80 –I ACCEPT



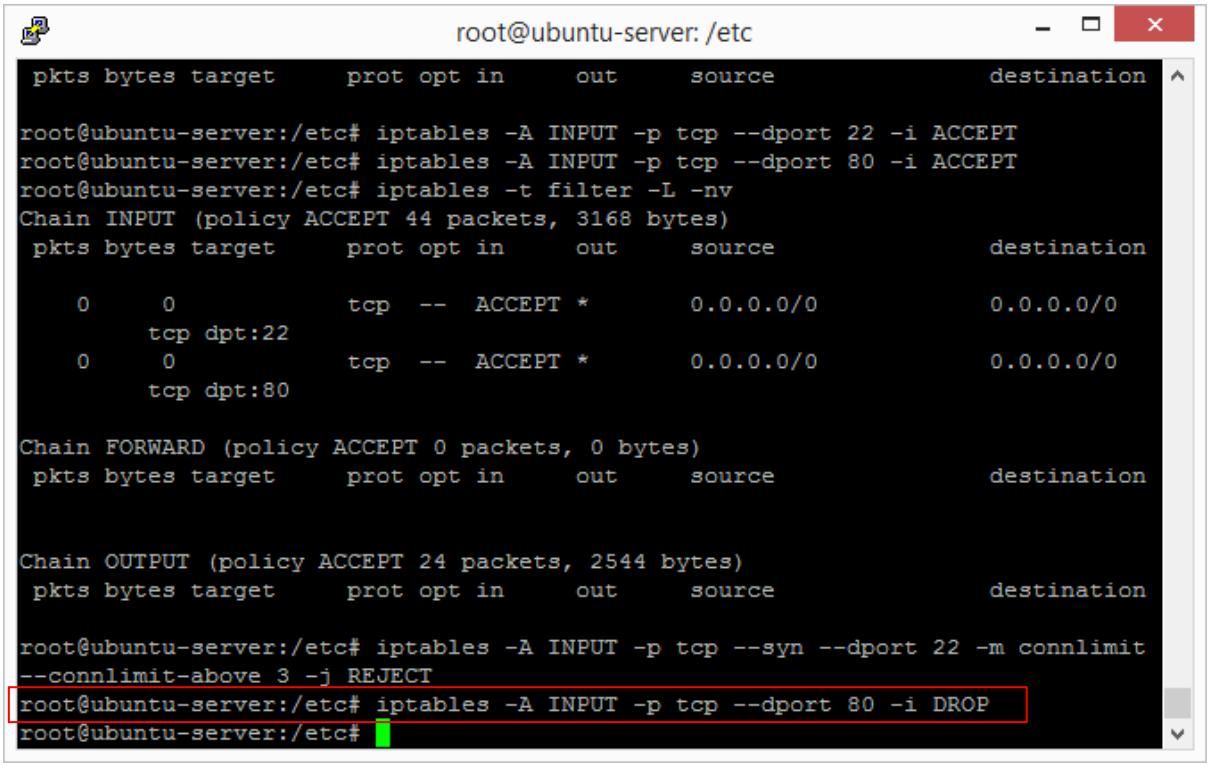
- Снова проверим правила. Указанные порты открылись



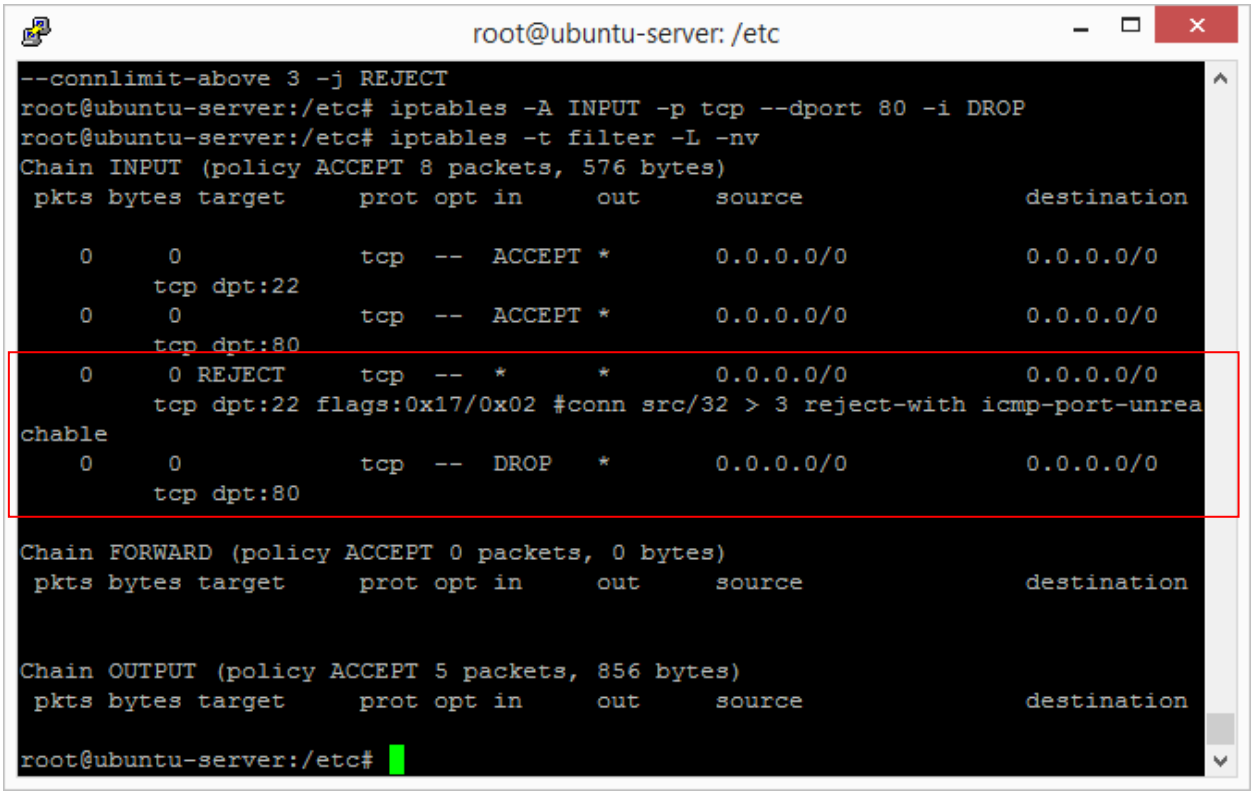

- В целях практики проведем некоторые дополнительные операции с портами. По 22 порту ограничим количество ssh-соединений на одного клиента до трех. Для этого воспользуемся командой iptables –A INPUT –p tcp –syn –dport 22 –m connlimit –connlimit-above 3 –j REJECT



- 80 порт отключим, заменив в команде, которая использовалась для подключения ACCEPT на DROP




- Вновь проверим правила. 22 порт принял изменения, 80 порт отключился

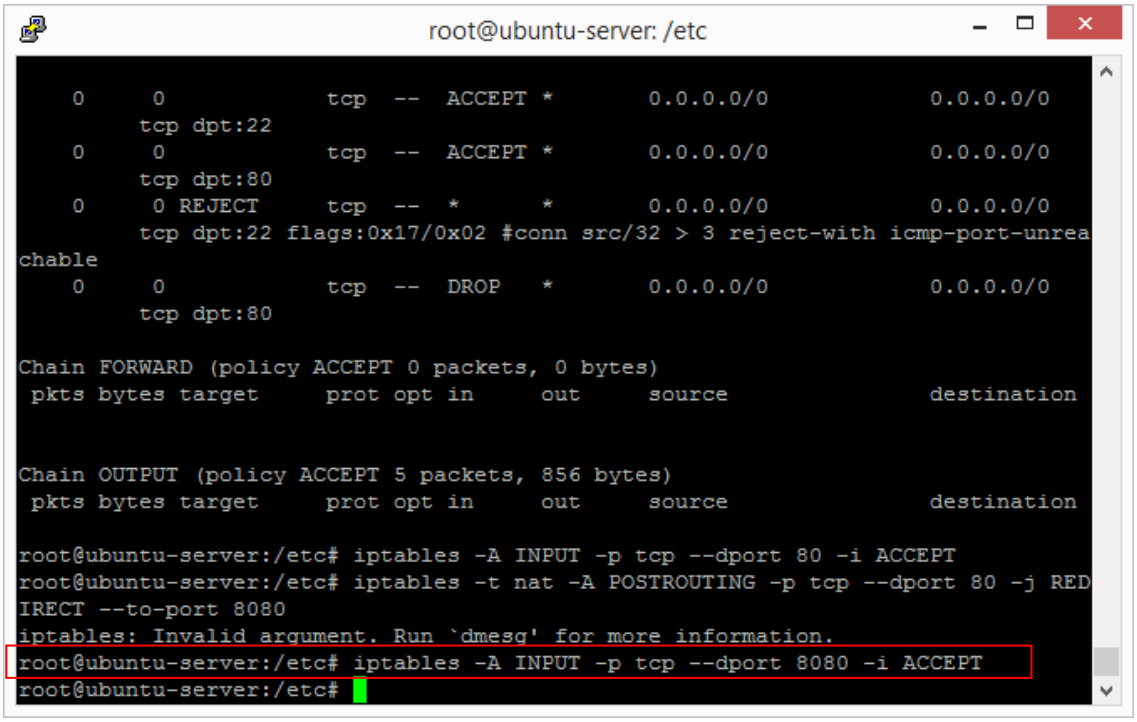


4. Настроить проброс портов локально с порта 80 на порт 8080.

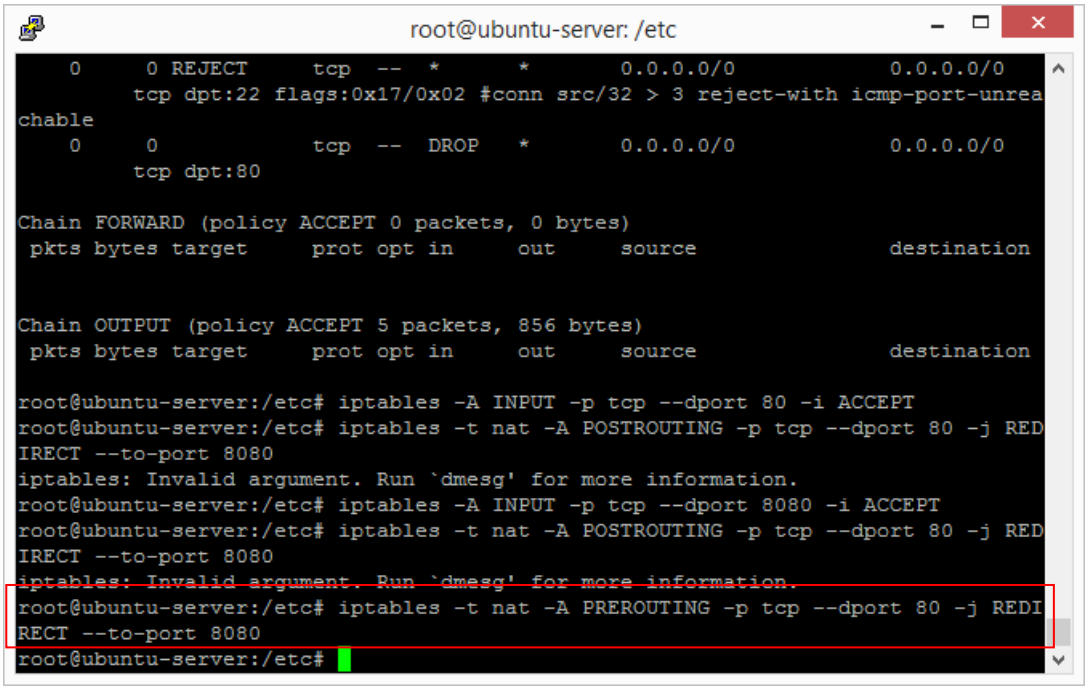
Технология NAT (network address translation) позволяет нескольким компьютерам объединяться в локальную сеть и быть доступными из внешней сети по IP адресу маршрутизатора.

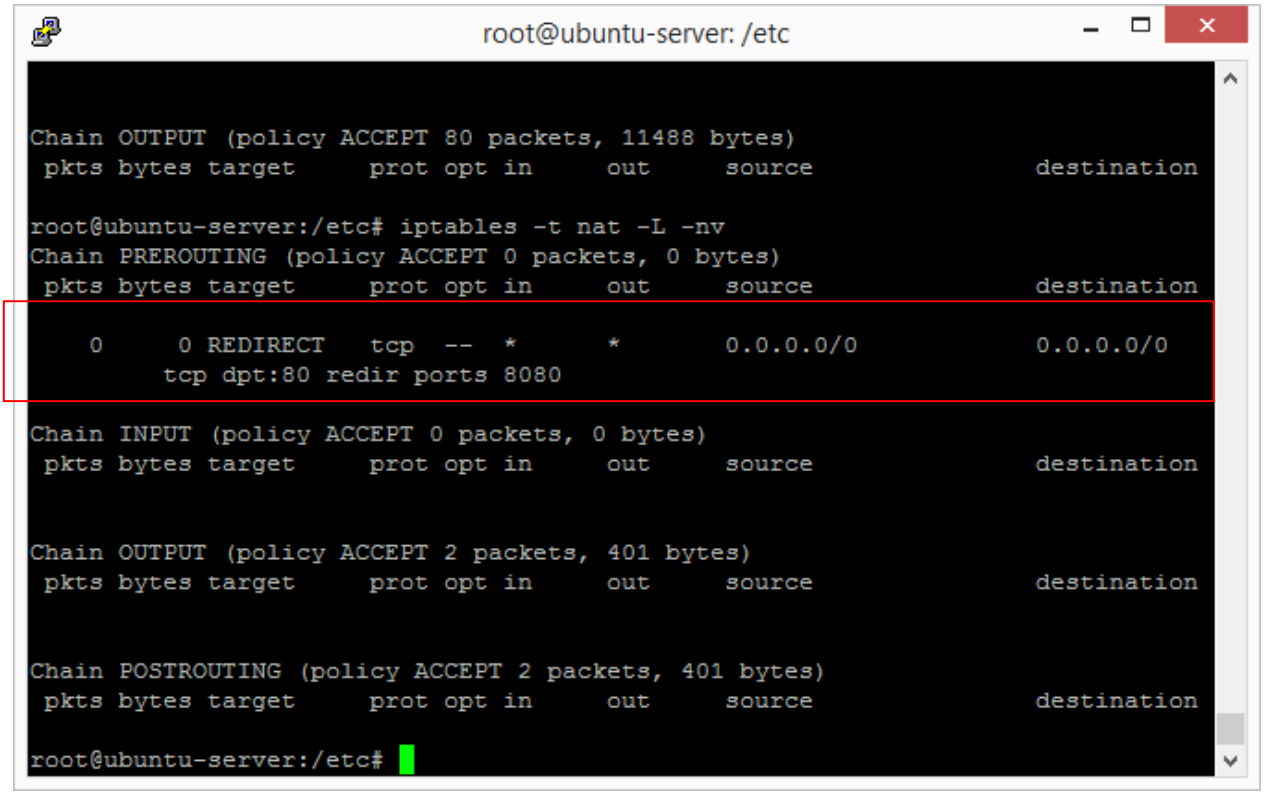
Решение

- Первоначально подключим порт 8080




- Для настройки переброса воспользуемся командой iptables –t nat –A PREROUTING –p tcp --dport 80 –j REDIRECT –to-port 8080



- Проверим правила таблиц filter (порт 8080 открыт)

- Проверим правила таблиц nat. Переброс настроен