Как установить и настроить SSH в Ubuntu 22.04

SSH – это сетевой протокол, который обеспечивает безопасное подключение клиента к серверу. Любое взаимодействие подвергается шифрованию, предотвращая хищение передаваемых по сети данных и других удаленных сетевых атак.

Например, вы заказали [облачный сервер](https://timeweb.cloud/services/cloud-servers) в Timeweb Cloud. Чтобы подключаться к серверу и администрировать его, вам потребуется установленный и настроенный SSH.

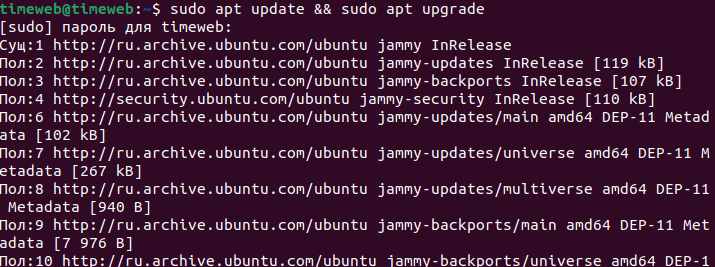
В инструкции ниже мы опишем процесс установки SSH в Ubuntu 22.04, а также последующей его настройки.

Шаг 1. Подготовка Ubuntu

Первое, что нужно сделать перед началом установки SSH в Ubuntu, это произвести синхронизацию и обновление всех пакетов apt до последних версий. Для этого воспользуемся следующей командой:

sudo apt update && sudo apt upgrade

Результат выполненной команды представлен на картинке ниже.



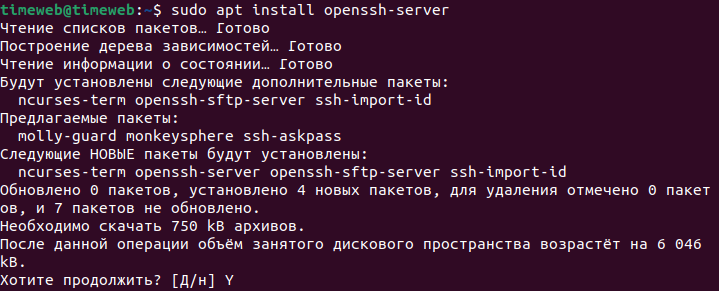
Теперь все пакеты apt обновлены и имеют последние версии. После данного шага можно переходить непосредственно к главной теме статьи – установке SSH.

Шаг 2. Установка SSH в Ubuntu

OpenSSH не предустанавливается в системе, поэтому выполним его установку вручную. Чтобы это сделать, в окне терминала вводим:

sudo apt install openssh-server

Как только команда будет выполнена, начнется установка всех необходимых компонентов в систему, как показано на картинке ниже.



На все предложения системы в момент установки отвечаем утвердительно.

Установка прошла успешно. Теперь перейдем к запуску службы.

Шаг 3. Запуск SSH

На данном этапе необходимо включить только что установленную службу. Поможет в этом команда ниже:

sudo systemctl enable --now ssh

При успешном запуске вы увидите следующее системное сообщение.

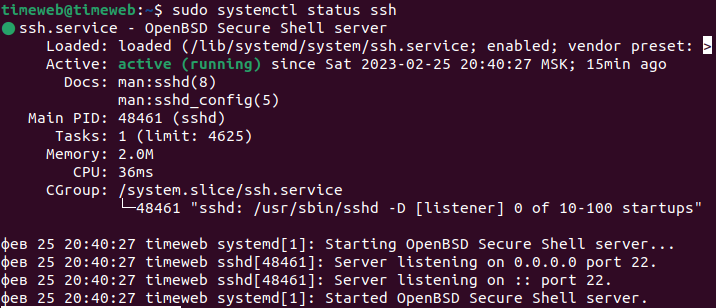
Image8

Ключ --now в команде выше отвечает за одновременный запуск программы и добавление ее в автозагрузку.

Теперь проверим, что служба включена и успешно функционирует. Для этого вводим:

sudo systemctl status ssh

В результате система выдаст следующее сообщение:



Как видно по картинке выше, установленная служба успешно функционирует. Об этом говорит строка Active: active (running).

Если необходимо выключить службу и убрать ее из автозагрузки, в окне терминала введите:

sudo systemctl disable ssh

Шаг 4. Настройка брандмауэра

Перед подключением к серверу через протокол SSH проверим состояние брандмауэра. Хотя во время установки службы и происходит настройка файрвола, повторная проверка поможет убедиться, что он настроен правильно.

VDS и VPS

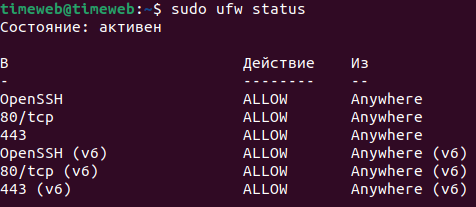
Гибкие виртуальные серверы с почасовым  
биллингом по всему миру: Россия, Азия и Европа

Создать аккаунт

В нашем случае установлен интерфейс UFW, поэтому воспользуемся следующей командой:

sudo ufw status

Результат команды представлен на картинке ниже.



Как видно по картинке, трафик по протоколу SSH разрешен. Если у вас он отсутствует в списке, то необходимо разрешить входящие SSH-соединения. В этом поможет команда:

sudo ufw allow ssh

Чтобы включить его, нужно выполнить команду **sudo ufw enable**.

Шаг 5. Подключение к серверу

После выполнения всех предыдущих шагов можно наконец переходить ко входу на сервер, используя протокол SSH.

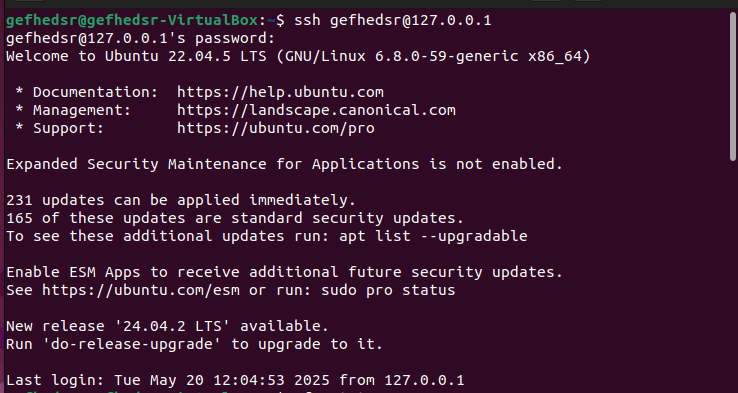
Для подключения к серверу пользователю понадобятся его IP-адрес или доменное имя.

В строку терминала вводим команду:

ssh имя\_пользователя@IP\_адрес

Или:

ssh имя\_пользователя@домен

**Проверка работы:** Для проверки работы ssh можно подключиться локально при помощи команд, которые написаны ранее. Подключаться можно к локальному адресу 127.0.0.1 или найти адрес через hostname -I

**Важно:**Для успешного подключения к удаленному серверу, на нем и на компьютере пользователя, откуда будет выполняться подключение, должен быть установлен и настроен SSH. На облачных серверах Timeweb Cloud SSH уже установлен.

Шаг 6. Настройка конфигурации SSH

Выполнив предыдущие 5 шагов, пользователь уже сможет без затруднений выполнить удалённое подключение к серверу, используя установленную службу. Однако можно дополнительно повысить безопасность выполняемого подключения, изменив стандартный порт подключения на другой или поменяв аутентификацию по паролю на аутентификацию по ключу. Для этих и других изменений необходимо отредактировать конфигурационный файл SSH.

Основные настройки OpenSSH-сервера хранятся в главном конфигурационном файле – sshd\_config (расположение: /etc/ssh). Перед тем, как приступать к редактированию, необходимо создать резервную копию данного файла:

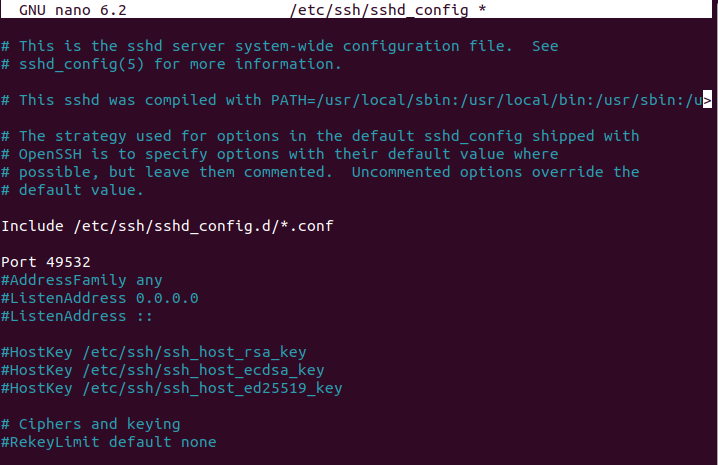
sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.initial

Теперь в случае возникновения ошибок после редактирования конфигурационного файла, пользователь без проблем сможет вернуть его к первоначальному виду.

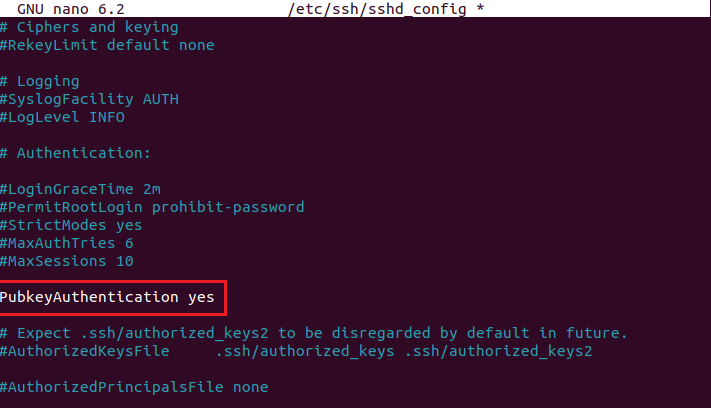
После создания резервной копии можно переходить непосредственно к редактированию конфигурационного файла. Для этого откроем его, используя терминал и редактор Nano:

 sudo nano /etc/ssh/sshd\_config

В открывшемся файле сразу изменим значение порта на более безопасное. Лучше всего устанавливать значения из динамического диапазона портов (49152 — 65535), при этом использовать набор отличных друг от друга цифр для дополнительной безопасности. Например, отредактируем значение порта на 49532. Для этого раскомментируем соответствующую строку в файле и изменим значения порта, как показано на картинке ниже.



Кроме данной настройки, необходимо изменить режим аутентификации по паролю на более безопасный по ключу. Для этого раскомментируем соответствующую строку, значение которой должно быть “Yes”, как показано на картинке ниже.



Аутентификацию по ключу разрешена. О том, как сгенерировать и использовать пару SSH-ключей, было подробно рассказано в [соответствующей статье](https://timeweb.cloud/tutorials/linux/kak-sgenerirovat-ssh-klyuch-linux).

Теперь запретим вход на сервер под суперпользователем. Для этого также изменим значение соответствующей строки, как показано на рисунке ниже.



Кроме внесенных выше изменений, перечислим ниже основные директивы конфигурационного файла, которые отвечают за безопасность сервера:

* UseDNS – отвечает за проверку соответствия имени хоста с его IP -адресом. Значение “Yes” включает этот параметр.
* PermitEmptyPasswords – данный параметр запрещает использовать пустые пароли при аутентификации, если в качестве значения указано “No”.
* MaxAuthTries – ограничение на количество неудачных попыток подключения к серверу в рамках одного сеанса связи. В качестве значения передается число.
* AllowUsers и AllowGroups – данные параметры отвечает за список пользователей и групп соответственно, которым разрешен доступ к серверу.

# AllowUsers Пользователь1, пользователь2, пользователь3

# AllowGroups Группа1, группа2, группа3

* Login GraceTime – параметр, отвечающий за время, предоставляемое для успешной авторизации. Рекомендуем уменьшить значение данного параметра в 4 раза.
* ClientAliveInterval  – ограничение на время бездействия пользователя. При выходе за указанную границу происходит отключение пользователя.

После внесения всех изменений в главный конфигурационный файл, необходимо их сохранить и закрыть редактор. После перезагружаем службу, чтобы все изменения вступили в силу:

sudo systemctl restart ssh

Если в конфигурационном файле вносились изменения порта, то выполнять подключение необходимо с указанием его нового значения:

ssh -p номер\_порта имя\_пользователя@IP\_адрес

Или:

ssh -p номер\_порта имя\_пользователя@домен

## OverTheWire

## Для подключения можно использовать сторонние открытые к подключению ssh-сервера.Платформа OverTheWire предоставляет ssh-сервер для подключения и изучения команд ssh.

## 

## Для подключения к нулевому уровню, можно использовать команду:

## ssh –p 2220 [bandit0@bandit.labs.overthewire.org](mailto:bandit0@bandit.labs.overthewire.org)

## пароль – bandit0

## Заключение

В данной статье была продемонстрирована подробная инструкция по установке и настройке SSH в Ubuntu 22.04. Также был описан процесс внесения изменений в главный файл конфигурации для повышения безопасности. Благодаря данной инструкции пользователь сможет выполнить безопасное удаленное подключение к серверу и не беспокоиться о потере или краже передаваемых данных.