

Зертханалық сабақ №13: SSH хаттамасы. Қашықтан басқару құралын қорғау

SSH протоколы компьютермен қауіпсіз қосылуды қамтамасыз ету үшін қолданылады, бұл операциялық жүйенің қабығы арқылы ғана емес, сонымен қатар шифрланған арна арқылы да қашықтан басқаруға мүмкіндік береді. Кейде Ubuntu операциялық жүйесін пайдаланушыларның кез-келген мақсатты орындау үшін компьютерге SSH серверін қою керек болады. Сондықтан біз жүктеу процедурасын ғана емес, сонымен қатар негізгі параметрлерді орнатуды зерттей отырып, осы процеспен егжей-тегжейлі танысуды ұсынамыз.

SSH компоненттерін ресми сақтау арқылы жүктеуге болады, сондықтан біз дәл осы әдісті қарастырамыз, ол ең тұрақты және сенімді, сонымен қатар жаңадан келген пайдаланушылар үшін қиындық тудырмайды.

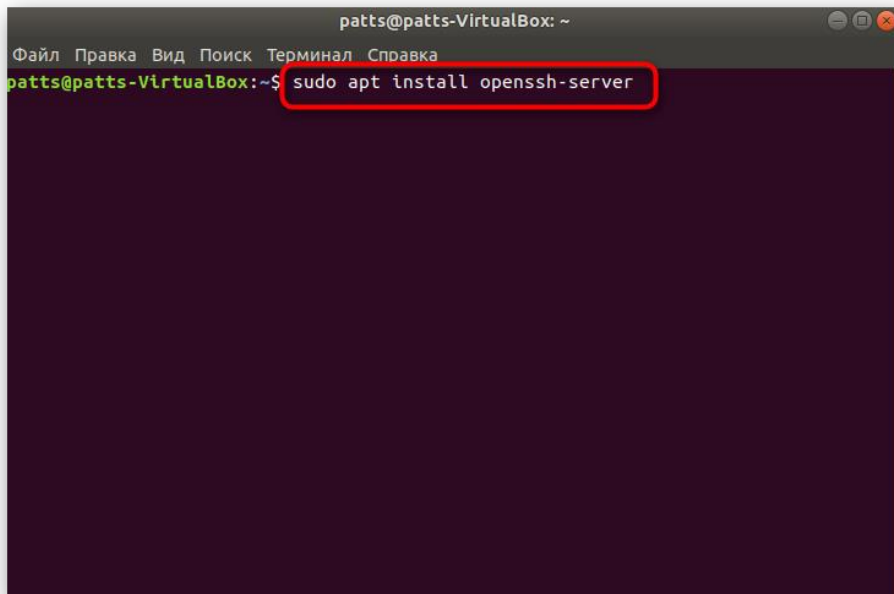
1-қадам: SSH-server жүктеу және орнату

Біз негізгі пәрмендер жиынтығын қолдана отырып, "Терминал" арқылы тапсырманы орындаймыз. Қосымша білім немесе дағды қажет емес, сіз әр әрекеттің егжей-тегжейлі сипаттамасын және барлық қажетті командаларды аласыз.

1. Консольді мәзір арқылы немесе **Ctrl + Alt + T** тіркесімін басып іске қосыңыз.

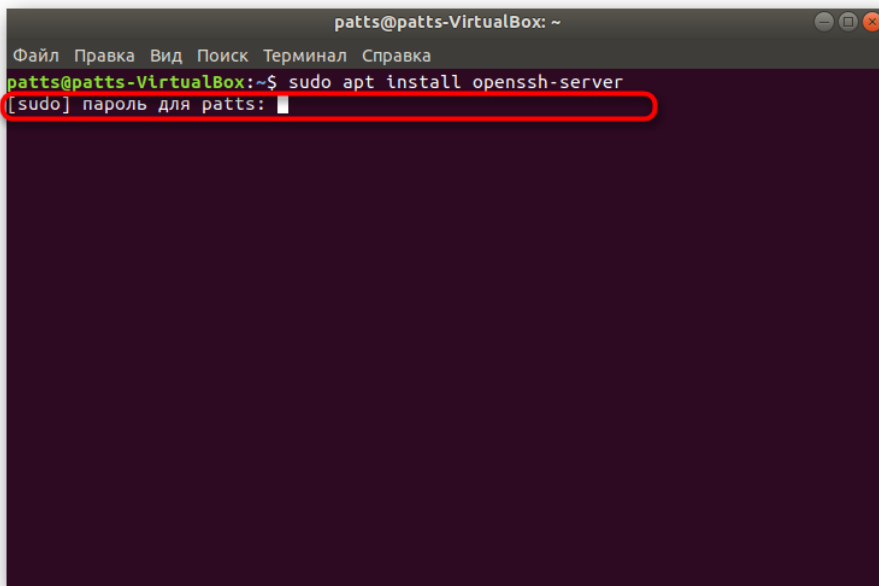


2. Дереву ресми репозиторийден сервер файлдарын жүктеуді бастаңыз. Ол үшін `sudo apt install openssh-server` енгізіп, Enter пернесін басыңыз.



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo apt install openssh-server
```

3. Біз **sudo** префиксін қолданғандықтан (әрекетті супер пайдаланушының атынан орындау), сіз өзіңіздің есептік жазбаңыздан құпия сөзді енгізуіңіз керек. Енгізу кезінде таңбалар көрсетілмейтінін ескеріңіз



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo apt install openssh-server  
[sudo] пароль для patts: █
```

4. Сізге белгілі бір мұрағат көлемін жүктеу туралы хабарланады, **Д** жеткізу опциясын таңдау арқылы әрекетті растаңыз.

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
patts@patts-VirtualBox:~$ sudo apt install openssh-server
[sudo] пароль для patts:
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
 ncurses-term openssh-sftp-server ssh-import-id
Предлагаемые пакеты:
 molly-guard monkeysphere rssh ssh-askpass
НОВЫЕ пакеты, которые будут установлены:
 ncurses-term openssh-server openssh-sftp-server ssh-import-id
Обновлено 0 пакетов, установлено 4 новых пакетов, для удаления отмечено 0 пакетов, и 184 пакетов не обновлено.
Необходимо скачать 637 кВ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 5.316 кВ.
Хотите продолжить? [Д/Н]
```

5. Әдепкі бойынша, клиент сервермен бірге орнатылады, бірақ оны қайта орнатуға тырысып, оның бар екеніне көз жеткізу артық болмайды `sudo apt-get install openssh-client`.

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
Обрабатываются триггеры для man-db (2.8.3-2) ...
Настраивается пакет ssh-import-id (5.7-0ubuntu1.1) ...
Настраивается пакет openssh-server (1:7.6p1-4ubuntu0.2) ...

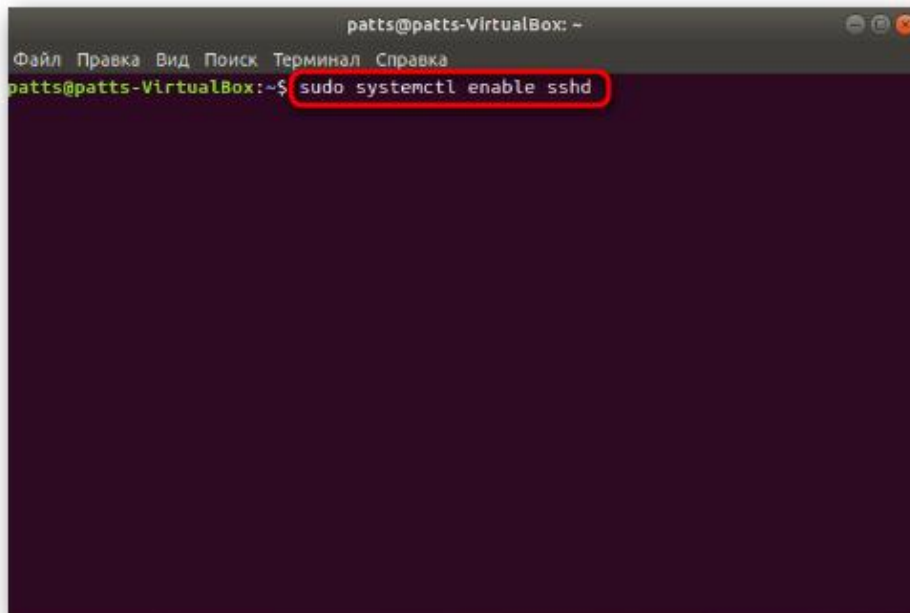
Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:looqBNgbh3jI5hLuqfMMb+USwuhUt8S5Shq+FpJ9oEU root@patts-VirtualBox (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:hjGig+ZH76x3H6j4z3Zwd/YQr4YpEwQv3eiFQ5HN5vc root@patts-VirtualBox (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:Vb0wRUEr9ruJKuovYddKJeJIKhHFEZF3NcITYDt18YU root@patts-VirtualBox (ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
Обрабатываются триггеры для systemd (237-3ubuntu10.13) ...
Обрабатываются триггеры для udev (0.100.0-20) ...
Обрабатываются триггеры для ufw (0.35-5) ...
patts@patts-VirtualBox:~$ sudo apt-get install openssh-client
```

SSH сервері операциялық жүйеге барлық файлдарды сәтті қосқаннан кейін бірден өзара әрекеттесу үшін қол жетімді болады, бірақ оны дұрыс жұмыс істеу үшін конфигурациялау керек. Келесі қадамдармен танысуға кеңес береміз.

2-қадам: серверді тексеру

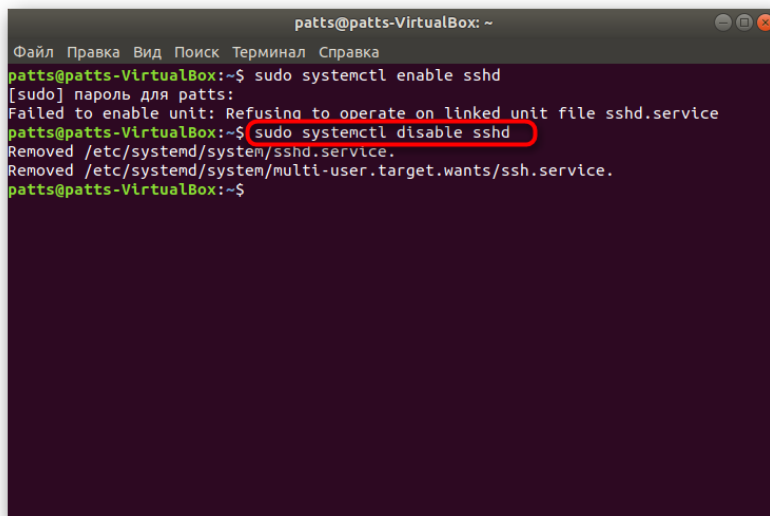
Бастау үшін стандартты параметрлер дұрыс қолданылғанына көз жеткізейік, ал SSH-server негізгі командаларға жауап береді және оларды дұрыс орындайды, сондықтан сізге қажет:

1. Консольді іске қосыңыз және егер ол орнатылғаннан кейін кенеттен автоматты түрде болмаса. Ubuntu іске қосу серверіне қосу үшін `sudo systemctl enable sshd` жазыңыз,



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo systemctl enable sshd
```

2. Егер сізге ОЖ-мен бірге бастау қажет болмаса, оны `sudo systemctl disable sshd` іске қосу арқылы автоматты түрде жойыңыз



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo systemctl enable sshd  
[sudo] пароль для patts:  
Failed to enable unit: Refusing to operate on linked unit file sshd.service  
patts@patts-VirtualBox:~$ sudo systemctl disable sshd  
Removed /etc/systemd/system/sshd.service.  
Removed /etc/systemd/system/multi-user.target.wants/ssh.service.  
patts@patts-VirtualBox:~$
```

3. Енді жергілікті компьютерге қосылуды тексеріңіз. `ssh localhost` пәрменін қолданыңыз (жергілікті компьютердің localhost мекен — жайы).

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
patts@patts-VirtualBox:~$ sudo systemctl enable sshd
[sudo] пароль для patts:
Failed to enable unit: Refusing to operate on linked unit file sshd.service
patts@patts-VirtualBox:~$ sudo systemctl disable sshd
Removed /etc/systemd/system/ssh.service.
Removed /etc/systemd/system/multi-user.target.wants/ssh.service.
patts@patts-VirtualBox:~$ ssh localhost
```

4. Yes опциясын таңдау арқылы қосылудың жалғасын растаңыз

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
patts@patts-VirtualBox:~$ sudo systemctl enable sshd
[sudo] пароль для patts:
Failed to enable unit: Refusing to operate on linked unit file sshd.service
patts@patts-VirtualBox:~$ sudo systemctl disable sshd
Removed /etc/systemd/system/ssh.service.
Removed /etc/systemd/system/multi-user.target.wants/ssh.service.
patts@patts-VirtualBox:~$ ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:hiGlo+ZH76x3H614z3Zwd/Y0r4YpEwQv3e1FQ5HN5vc.
Are you sure you want to continue connecting (yes/no)?
```

5. Жүктеу сәтті болған жағдайда, сіз келесі скриншотта көріп отырғаныңыздай, осындай ақпаратты аласыз. Басқа құрылғылар үшін әдепкі бойынша таңдалған желілік IP ретінде әрекет ететін 0.0.0.0, мекен-жайына қосылуды тексеру қажет. Ол үшін тиісті пәрменді енгізіп, **Enter** пернесін басыңыз.

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
patts@localhost's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-45-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

Могут быть обновлены 180 пакетов.
0 обновлений касаются безопасности системы.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

patts@patts-VirtualBox:~$ ssh 0.0.0.0
```

6. Әрбір жаңа қосылыста оны растау қажет болады.

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

Могут быть обновлены 180 пакетов.
0 обновлений касаются безопасности системы.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

patts@patts-VirtualBox:~$ ssh 0.0.0.0
The authenticity of host '0.0.0.0 (0.0.0.0)' can't be established.
ECDSA key fingerprint is SHA256:hiGiq+ZH76x3H6i4z3Zwd/Y0r4YpEw0v3eiFQ5HN5vc.
Are you sure you want to continue connecting (yes/no)? yes
```

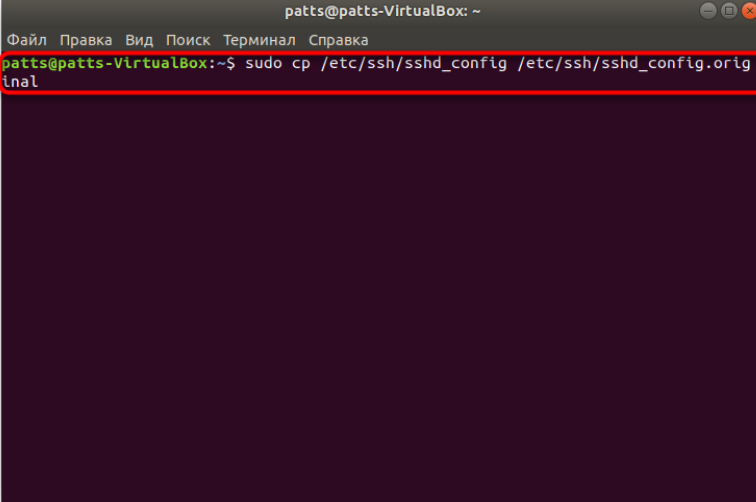
Көріп отырғаныңыздай, ssh командасы кез-келген компьютерге қосылу үшін қолданылады. Егер сіз басқа құрылғымен қосылғыңыз келсе, терминалды іске қосып, пәрменді SSH форматында `ssh имя_пользователя@ip_адрес.деп` теріңіз.

3-қадам: конфигурация файлын өңдеу

SSH протоколының барлық қосымша параметрлері жолдар мен мәндерді өзгерту арқылы арнайы конфигурация файлы арқылы жүзеге асырылады. Біз барлық тармақтарға назар аудармаймыз, сонымен қатар олардың көпшілігі әр

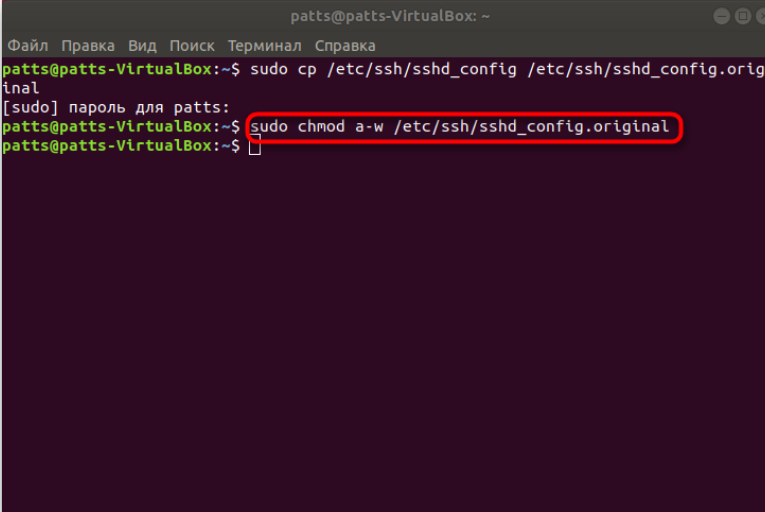
пайдаланушы үшін жеке болып табылады, біз тек негізгі әрекеттерді көрсетеміз.

1. Бірінші кезекте конфигурация файлының сақтық көшірмесін сақтаңыз, егер ол қажет болса, оған хабарласыңыз немесе SSH бастапқы күйін қалпына келтіріңіз. Консольге `sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original`. командасын қойыңыз.



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
```

2. Сосын екінші: `sudo chmod a-w /etc/ssh/sshd_config.original`.



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original  
[sudo] пароль для patts:  
patts@patts-VirtualBox:~$ sudo chmod a-w /etc/ssh/sshd_config.original  
patts@patts-VirtualBox:~$
```

3. Параметрлер файлын іске қосу `sudo vi /etc/ssh/sshd_config`. арқылы жүзеге асырылады. Кіргеннен кейін бірден ол іске қосылады және сіз оның мазмұнын төмендегі скриншотта көрсетілгендей көресіз.

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
# $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

4. Мұнда сіз пайдаланылатын портты өзгерте аласыз, ол әрқашан қосылудың қауіпсіздігін қамтамасыз ету үшін жақсы жасалады, содан кейін кіріс супер пайдаланушының атынан өшірілуі мүмкін (PermitRootLogin) және кілттің іске қосылуы (PubkeyAuthentication). Өңдеу аяқталғаннан кейін пернені басу керек : (Shift + ; латын орналасуында) және Өзгерістерді сақтау үшін w әрпін қосыңыз.

```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

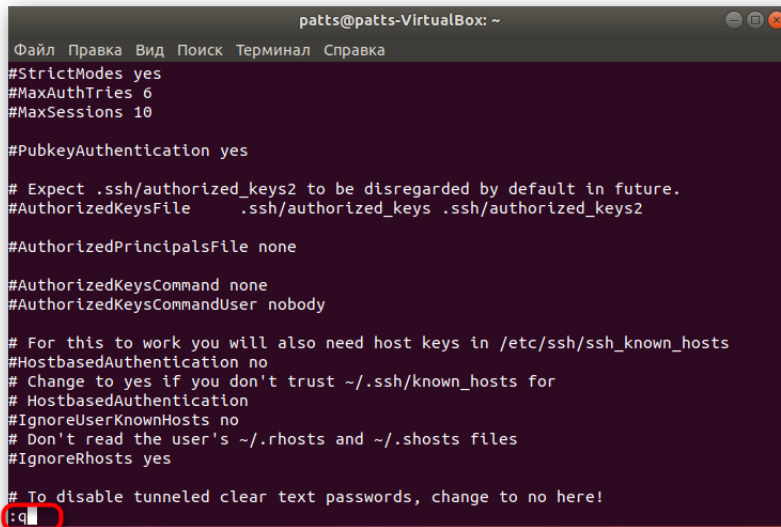
# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#   X11Forwarding no
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand cvs server
:w
```

5. Файлдан шығу дәл осылай жүзеге асырылады, тек W орнына q қолданылады.



```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

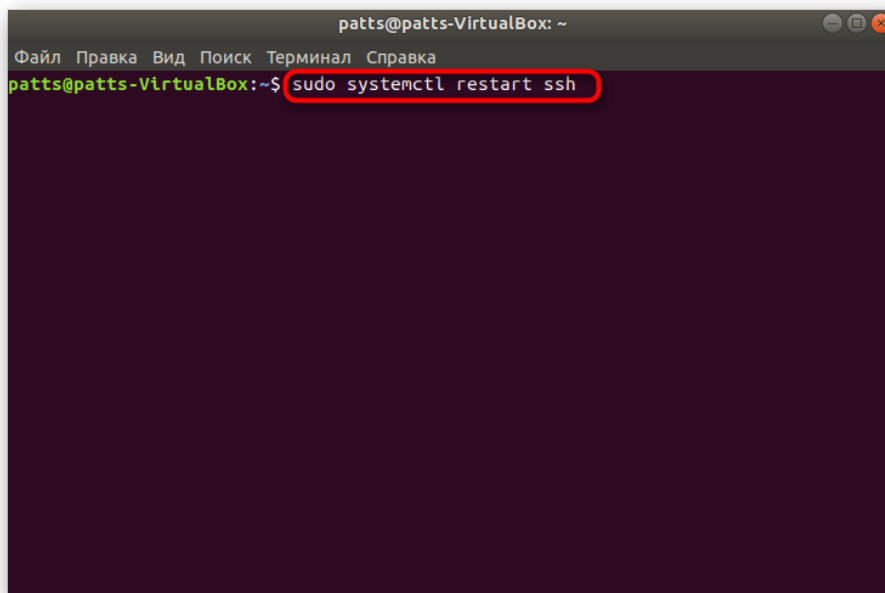
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
:q
```

6. Серверді қайта іске қосуды ұмытпаңыз `sudo systemctl restart ssh`.



```
patts@patts-VirtualBox: ~
Файл Правка Вид Поиск Терминал Справка
patts@patts-VirtualBox:~$ sudo systemctl restart ssh
```

7. Белсенді портты өзгерткеннен кейін оны клиентке бекіту керек. Бұл `ssh -p 2100 localhost` көрсету арқылы жасалады, мұнда 2100 — ауыстырылған порт нөмірі..

```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo systemctl restart ssh  
[sudo] пароль для patts:  
patts@patts-VirtualBox:~$ ssh -p 2100 localhost
```

8. . Егер сізде брандмауэр орнатылған болса, онда ауыстыру қажет: `sudo ufw allow 2100`.

```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo systemctl restart ssh  
[sudo] пароль для patts:  
patts@patts-VirtualBox:~$ ssh -p 2100 localhost  
ssh: connect to host localhost port 2100: Connection refused  
patts@patts-VirtualBox:~$ sudo ufw allow 2100
```

9. Барлық ережелер жаңарғаны жайлы ақпарат аласыз

```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ sudo systemctl restart ssh  
[sudo] пароль для patts:  
patts@patts-VirtualBox:~$ ssh -p 2100 localhost  
ssh: connect to host localhost port 2100: Connection refused  
patts@patts-VirtualBox:~$ sudo ufw allow 2100  
Правила обновлены  
Правила обновлены (v6)  
patts@patts-VirtualBox:~$
```

Басқа параметрлермен сіз ресми құжаттаманы оқып, өзіңіз танысуға құқылысыз. Сізге қандай мәндерді таңдау керектігін анықтауға көмектесетін барлық тармақтарды өзгертуге арналған кеңестер бар.

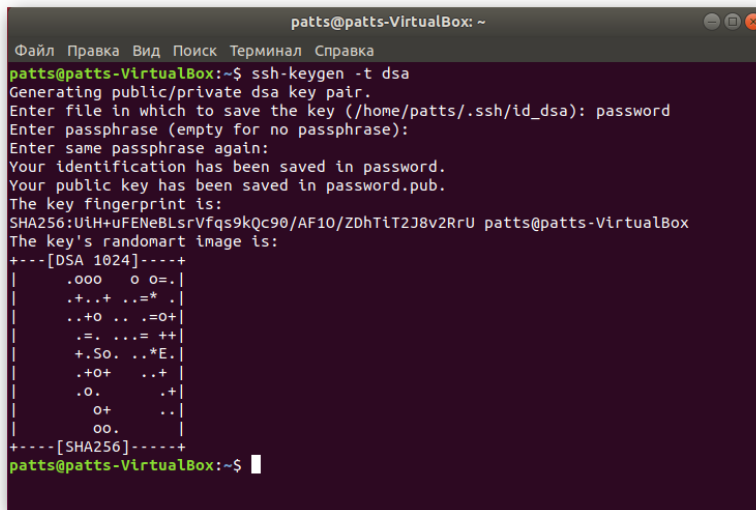
4-қадам: кілттерді қосу

SSH кілттерін қосқанда, парольді алдын-ала енгізбестен екі құрылғы арасында авторизация ашылады. Сәйкестендіру процесі құпия және ашық кілтті оқу алгоритміне қайта құрылады.

1. `ssh-keygen -t dsa` енгізу арқылы консольді ашып, жаңа клиент кілтін жасаңыз, содан кейін файлға атау беріп, кіру паролін көрсетіңіз.

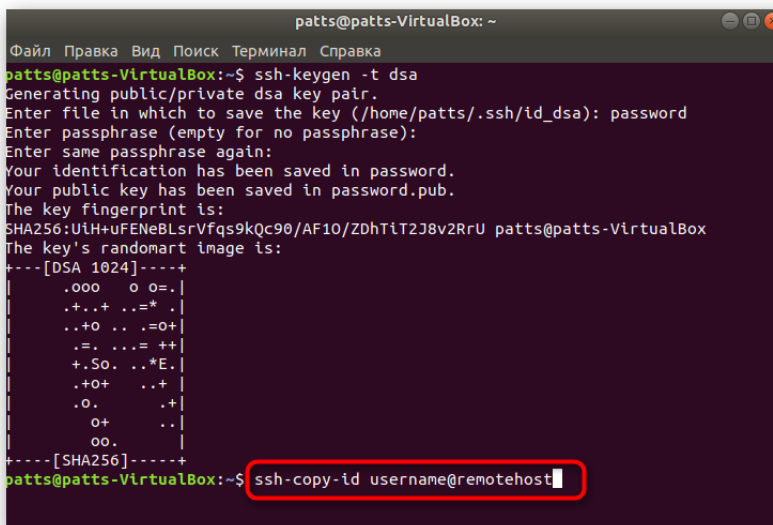
```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ ssh-keygen -t dsa  
Generating public/private dsa key pair.  
Enter file in which to save the key (/home/patts/.ssh/id_dsa):
```

2. Осыдан кейін қоғамдық кілт сақталады және құпия сурет жасалады. Экранда сіз оның көрінісін көресіз.



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ ssh-keygen -t dsa  
Generating public/private dsa key pair.  
Enter file in which to save the key (/home/patts/.ssh/id_dsa): password  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in password.  
Your public key has been saved in password.pub.  
The key fingerprint is:  
SHA256:UiH+uFENeBLSrVfqs9kQc90/AF10/ZDhTt12J8v2RrU patts@patts-VirtualBox  
The key's randomart image is:  
+----[DSA 1024]-----+  
|.000 0 0=|. |  
|.+.+. .=*|. |  
|.+.0 .. =0+|. |  
|. . . = ++|. |  
|.So. .*E|. |  
|.0+ ..+|. |  
|.O. .+|. |  
|.O+ ..|. |  
|.O|. |  
+----[SHA256]-----+  
patts@patts-VirtualBox:~$
```

3. Құпия сөз арқылы қосылымды өшіру үшін жасалған файлды екінші компьютерге көшіру ғана қалады. `ssh-copy-id username@remotehost` пәрменін пайдаланыңыз, мұнда `username@remotehost`-қашықтағы компьютердің атауы және оның IP мекенжайы.



```
patts@patts-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
patts@patts-VirtualBox:~$ ssh-keygen -t dsa  
Generating public/private dsa key pair.  
Enter file in which to save the key (/home/patts/.ssh/id_dsa): password  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in password.  
Your public key has been saved in password.pub.  
The key fingerprint is:  
SHA256:UiH+uFENeBLSrVfqs9kQc90/AF10/ZDhTt12J8v2RrU patts@patts-VirtualBox  
The key's randomart image is:  
+----[DSA 1024]-----+  
|.000 0 0=|. |  
|.+.+. .=*|. |  
|.+.0 .. =0+|. |  
|. . . = ++|. |  
|.So. .*E|. |  
|.0+ ..+|. |  
|.O. .+|. |  
|.O+ ..|. |  
|.O|. |  
+----[SHA256]-----+  
patts@patts-VirtualBox:~$ ssh-copy-id username@remotehost
```

Серверді қайта іске қосып, ашық және құпия кілт арқылы оның дұрыстығын тексеру ғана қалады.

Бұл жерде SSH серверін орнату процедурасы және оның негізгі конфигурациясы аяқталды. Егер сіз барлық командаларды дұрыс енгізсеңіз, тапсырманы орындау кезінде ешқандай қателіктер болмауы керек. Орнатудан кейін қосылымға қатысты мәселелер туындаған жағдайда, мәселені шешу үшін SSH-ны іске қосудан шығарып көріңіз (бұл туралы **2-қадамнан** оқыңыз).