

Отчёт по лабораторной работе 11

Настройка безопасного удалённого доступа по протоколу SSH

Цвелев С.А. НПИбд-02-22

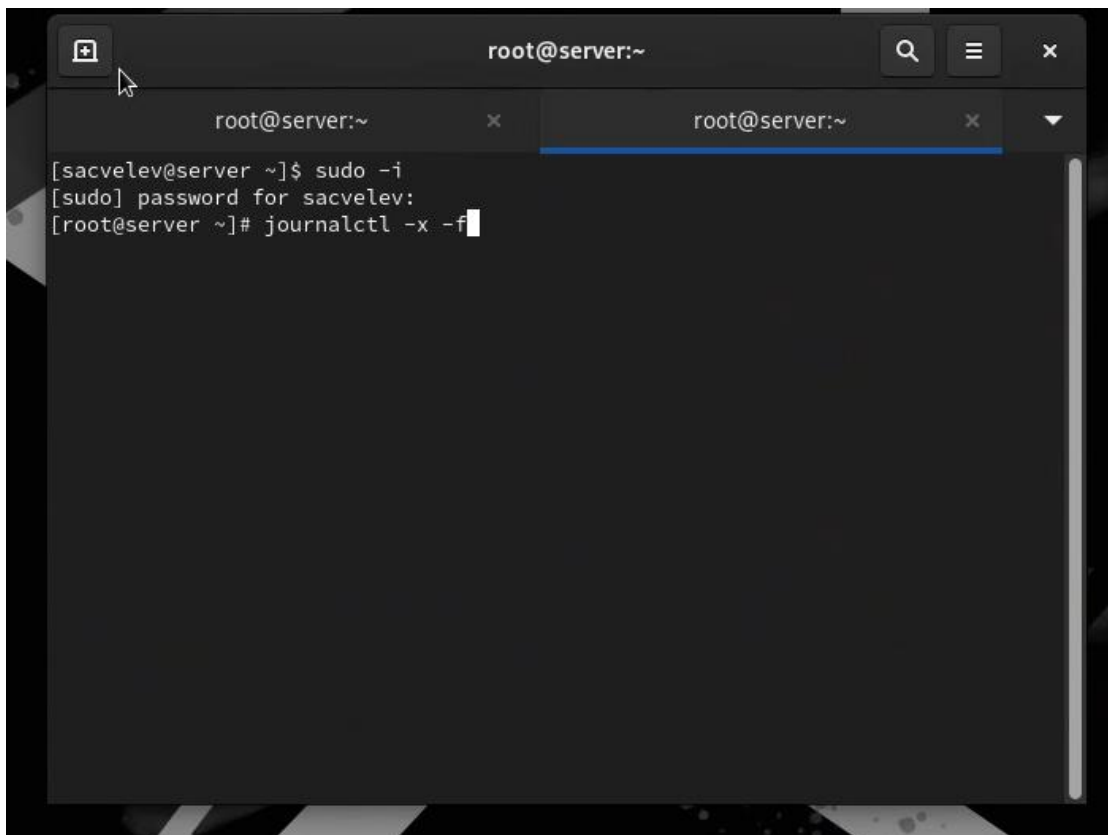
Содержание

1 Цель работы

Получение навыков по настройке удалённого доступа к серверу с помощью SSH.

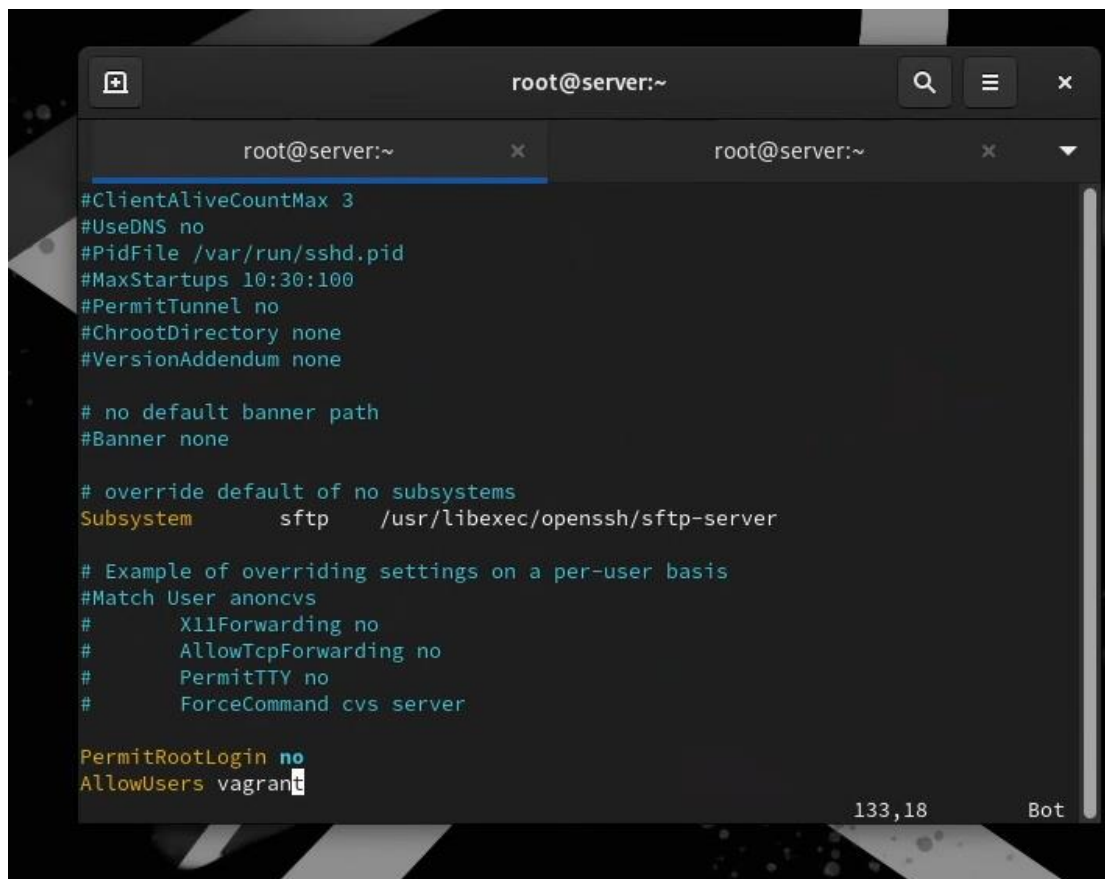
2 Ход работы

На сервере задаём пароль для root. Запускаем журнал системных событий. С клиента пытаемся получить доступ к серверу посредством SSH-соединения.

A screenshot of a terminal window with a dark background. The window title is 'root@server:~'. The terminal shows the following commands and output:

```
[sacvelev@server ~]$ sudo -i
[sudo] password for sacvelev:
[root@server ~]# journalctl -x -f
```

На сервере открываем файл `sshd_config` и запрещаем вход пользователю `root`. Перезапускаем службу. Также добавляем ещё строку про пользователя `vagrant` и `user`.

A terminal window titled 'root@server:~' with two tabs. The active tab shows the content of the /etc/ssh/sshd_config file. The configuration includes settings for ClientAliveCountMax, UseDNS, PidFile, MaxStartups, PermitTunnel, ChrootDirectory, VersionAddendum, Banner, Subsystem (sftp), Match User anoncvs, and PermitRootLogin. The user 'vagrant' is listed in the AllowUsers directive. The terminal shows a cursor at the end of the 'AllowUsers' line.

```
root@server:~  
#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  
  
# override default of no subsystems  
Subsystem      sftp      /usr/libexec/openssh/sftp-server  
  
# Example of overriding settings on a per-user basis  
#Match User anoncvs  
#      X11Forwarding no  
#      AllowTcpForwarding no  
#      PermitTTY no  
#      ForceCommand cvs server  
  
PermitRootLogin no  
AllowUsers vagrant
```

3 Вывод

Мы приобрели навыки по настройке удалённого доступа к серверу с помощью SSH.