

OpenSSH

OpenSSH (открытая безопасная оболочка) — набор программ, предоставляющих шифрование сеансов связи по компьютерным сетям с использованием протокола [SSH](#).

Настройка

Отключение доступа пользователю root по SSH

Файл `/etc/ssh/sshd_config`

В разделе Authentication нужно поставить:

```
PermitRootLogin no
```

Ускорение входа

[/etc/ssh/sshd_config](#)

```
UseDNS no
```

Автоматическое добавление ключа в known_hosts

Файл `/etc/ssh/ssh_config`

```
StrictHostKeyChecking no
```

Работа разных интерфейсов на разных портах

Файл `/etc/ssh/sshd_config`

Пример:

```
ListenAddress 1.2.3.4:2222  
ListenAddress 192.168.1.1:22
```

Перезапуск демона:

```
service ssh restart
```

Проверка:

```
sockstat |grep ssh
```

или

```
netstat -tulpn |grep ssh
```

SFTP и ограничение входа в систему

Для при использовании Restricted shell можно разрешить вход по SSH:

1)

[/etc/passwd](#)

```
user:x:1001:1001::/home/user:/bin/false
```

2)

[/etc/ssh/sshd_config](#)

```
Subsystem sftp internal-sftp
```

3)

```
service ssh restart
```

Работа OpenSSH в Windows



! Описание верно для setupssh381-20040709.zip

<http://sshwindows.sourceforge.net/>

1. Для простоты работы нужно исправить значение в файле sshd_config

```
UsePrivilegeSeparation yes
```

2. Выполнить из папки bin

```
mkgroup -l > ..\etc\group  
mkpasswd -l > ..\etc\passwd
```

3. Перезапустить сервер

```
net stop opensshd  
net start opensshd
```

Решение проблем

Ошибка fatal: no matching cipher found

Если при подключении в файле /var/log/auth.log появляется ошибка:

```
fatal: no matching cipher found: client aes256-cbc,rijndael256-cbc,rijndael-cbc@lysator.liu.se,aes192-cbc,rijndael192-cbc,aes128-cbc,rijndael128-cbc,blowfish-cbc,3des-cbc,des-cbc,des-cbc@ssh.com server aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com [preauth]
```

Нужно добавить в файл:

[/etc/ssh/sshd_config](#)

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,blowfish-cbc,aes128-cbc,3des-cbc,cast128-
```

```
cbc,arcfour,aes192-cbc,aes256-cbc
```

sshd не запускается с первого раза после перезагрузки

Нужно установить:

```
apt install haveged
```

[sshd не запускается с первого раза после перезагрузки — Admin — Форум](#)

Ссылки

<https://ru.wikipedia.org/wiki/OpenSSH>

[Getting SSH to listen to different ports on different interfaces](#)

[Памятка пользователям ssh](#)

[Fixing SSH login long delay](#)

[Steronius' Programmatically Tolerable Repository of Technical Goodies : SSH - no matching cipher found](#)

[Как ускорить вход по SSH. Что делать если медленно работает SSH](#)

<http://sysadminmosaic.ru/openssh/openssh>

2020-11-01 11:26

