

SSH

- -
 -
- -
- `ssh`
- -



:

- Astra Linux Special Edition .10015-01 .10015-10 (1.7)
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

SSH (— openssh-server — openssh-client) Astra Linux. (openssh-client).

:

- , . openssh-server;
- (. `synaptic`) :

```
sudo apt install ssh
```

ssh .

, .

, :

- Astra Linux Common Edition 2.12.12 Astra Linux Special Edition x.7 SSH ;
- SSH . :

```
sudo systemctl enable ssh
```

SSH :

```
sudo systemctl start ssh
```

ssh

:

```
systemctl status ssh
```

/etc/ssh/sshd_config. :

```
systemctl restart sshd
```



, , :

```
AllowGroups "group name@domain.name"
```

man:

man sshd_config

:

- **Port** - , (22) - ;
- **MaxAuthTries** - (6) - , , 3;
- **LoginGraceTime** - , (2m) - , 30s.

, IP-, , :

- /etc/hosts.deny :

```
i # /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.

# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example: ALL: some.host.name, .some.domain
# ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

SSHD: ALL
```

- /etc/hosts.allow :

```
i # /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example: ALL: LOCAL @some_netgroup
# ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#

SSHD: 192.168.1.1
SSHD: 192.168.0.0/16
```

, " "

/etc/ssh/ssh_config. "-".

.

(cipher) (mac) :

```
ssh -Q cipher
ssh -Q mac
```

Astra Linux ssh :

3des-cbc
 blowfish-cbc
 cast128-cbc
 arcfour
 arcfour128
 arcfour256
 aes128-cbc
 aes192-cbc
 aes256-cbc
 rijndael-cbc@lysator.liu.se
 aes128-ctr
 aes192-ctr
 aes256-ctr
 grasshopper-cbc (34.13–2015 "")
 grasshopper-ctr (34.13–2015 "")
 aes128-gcm@openssh.com
 aes256-gcm@openssh.com
 chacha20-poly1305@openssh.com

Astra Linux ssh :

hmac-sha1
 hmac-sha1-96
 hmac-sha2-256
 hmac-sha2-512
 hmac-md5
 hmac-md5-96
 hmac-ripemd160
 hmac-ripemd160@openssh.com
 umac-64@openssh.com
 umac-128@openssh.com
 hmac-sha1-etm@openssh.com
 hmac-sha1-96-etm@openssh.com
 hmac-sha2-256-etm@openssh.com
 hmac-sha2-512-etm@openssh.com
 hmac-md5-etm@openssh.com
 hmac-md5-96-etm@openssh.com
 hmac-ripemd160-etm@openssh.com
 umac-64-etm@openssh.com
 umac-128-etm@openssh.com
 hmac-gost2012-256-etm (34.11-2012)

(Ciphers) (MACs), , ():

Ciphers grasshopper-ctr,aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
 # MACs hmac-gost2012-256-etm,hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160

/etc/ssh/ssh_config, /etc/ssh/sshd_config.

, , , .

, , , /etc/ssh/ssh_config :

Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,grasshopper-ctr
 MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-gost2012-256-etm

ssh

SSHFS (Secure Shell FileSystem) - , .

SSHFS SSH File Transfer Protocol (SFTP) — , Secure Shell.

, , SSH.

Astra Linux sshfs , :

```
sudo apt install sshfs
```

(.).

:

```
sshfs -o allow_other,IdentityFile=~local_user/.ssh/id_rsa
remote_user@server:/home/remote_user /mnt
```

:

- **-o** **-o**, **-o** **/**;
- **allow_other** - **(**);
- **IdentityFile**=~local_user/.ssh/id_rsa - **(**, **-**);
- **remote_user@server:/home/remote_user** - **,**;
- **(** server remote_user /home/remote_user)
- **/mnt** -

/etc/fstab:



```
sshfs#remote_user@server:/home/remote_user/ /mnt fuse defaults,allow_other,IdentityFile=~local_user/.ssh/id_rsa 0 0
```

(.).

umount :

```
umount /mnt
```

:

```
fusermount -u /mnt
```

ssh, Astra Linux, ,
, ,
[libgost-astra](#).

:

```
/etc/ssh/sshd_config SyslogFacility LogLevel, INFO DEBUG
```



```
# Logging
SyslogFacility AUTH
LogLevel INFO
LogLevel DEBUG
```

:

```
systemctl restart ssh
```

ssh /var/log/auth.log, , , :

```
tail -f | grep cipher /var/log/auth.log
```

:

-v :

```
ssh -v ServerSSH
```

, :



debug1: kex: server->client cipher: grasshopper-ctr MAC: hmac-gost2012-256-etm compression: none
debug1: kex: client->server cipher: grasshopper-ctr MAC: hmac-gost2012-256-etm compression: none