

SSH keys

Key management

After logging in, you can see `.ssh/` directory with SSH keys and `authorized_keys` file:

```
$ cd /home/username/
$ ls -la .ssh/
total 24
drwx----- 2 username username 4096 May 13 15:12 .
drwxr-x---22 username username 4096 May 13 07:22 ..
-rw-r--r-- 1 username username  392 May 21  2014 authorized_keys
-rw----- 1 username username 1675 May 21  2014 id_rsa
-rw----- 1 username username 1460 May 21  2014 id_rsa.ppk
-rw-r--r-- 1 username username  392 May 21  2014 id_rsa.pub
```

Please note that private keys in `.ssh` directory are without passphrase and allow you to connect within the cluster.

Access privileges on `.ssh` folder

- `.ssh`
directory: 700 (`drwx---`)
- `authorized_keys`,
`known_hosts` and public key (`.pub` file):
644 (`-rw-r--r--`)
- “
Private key (`id_rsa/id_rsa.ppk`): 600 (`-rw-----`)
`cd /home/username/ chmod 700 .ssh/ chmod 644 .ssh/authorized_keys`
`chmod 644 .ssh/id_rsa.pub chmod 644 .ssh/known_hosts chmod 600`
`.ssh/id_rsa chmod 600 .ssh/id_rsa.ppk`

Private key

The path to a private key is usually `/home/username/.ssh/`

Private key file in “`id_rsa`” or “`*.ppk`” format is used to authenticate with the servers. Private key is present locally on local side and used for example in SSH

agent Pageant (for Windows users). The private key should always be kept in a safe place.

An example of private key format:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAAqbo7jokygnBpG2wYa5NB45ns6+UKTNLMLHFOB03zmRtKEE1E
aGqXfbYvWx1cuRb2d9/Y5dVpCZHV0kbY3NhtV0cE1e+1R0aiU9BESUAhMNEvgiLV
gSq14QvR04BWP1M8+WAWXDP3oeoBh8glXyuh9teb8yq98fv1r1peYGRrW3/s4V+q
01SQOXY2T7rWCYRLIP6rTMXArTI35v3WU513mn7nm1fJ7oN0QgVH5b0W9V1Kyc4l
9vILHeMXxvz+i/5jTEfLOJpiRGYZYcaYrE4dIiHP13I1bV7h1kK23Xb1US8QJr5G
ADxp1VTkhjY+mKagEfx1lhQIb42JLHhKMEGqNQIDAQABaoIBAQCkypPuxZjL+vai
UGa5dAWiRZ46P2yrwHPKpvEdpCdDPbLAc1K/CtdBkHZsUPxNHVV6eFWweW99giIY
Av+mFWC58X8asBHQ7xkmxW0cqAZRzpkRA19IBS9/fKj028Fgy/p+su0i8oWbKIgJ
3LMkX0nnT9oz1Ak0fTNC6Tv+3SE7eTj1RPcMjur4W1Cd1N3EljLszdVk4tLx1XBS
y19NzVnJJB4t01145VfFECgYEAno1WJSB/SwdZvS9GkfvmZd3r4vyV9Bmo3dn
XZA8HRW13imOnpk1DR4FRe98D9A7V3yh9h60Co4oAUd6N+0c68/qnv/809efA+M
/neI9ANYFo8F0+yFCp4Duj7zPV3aW1N/pd8TNzLqecqh10uZNMMy8rAjCxybeZjWd
DyhgYwXhAoGBAN3BCazNefYpLbpBQzwes+f2oStvwOYKDqySWsYVXeVgUI+OWTVZ
eZ26Y86E8MQ0+q0TIxpwou+TEaUgOSqCX40Q37rGS19K+rjnboJBYNcmwVp9bfy
kCLL/3g57ntSqhgHNa1xwemePvgNdn6FZteA8sXiCg5ZzaISqWAffek5AoGBAMPw
V/vwQ96C8E311cH5cUbmBCCcfXM2GLv74bb1V3SvCiAKGOrZ8gEgUiQ0+TfcbAbe
7MM20vRNQjaLTBpai/BTbmQM1Q+r1KNjq8k5bfTdAoGANGz1NM9omM10rd9WagL5
yuJcal/03p048mtB40I4Xr5ZJISHze8fK4jQ5veUT9Vu2Fy/w6QMsuRf+qWeCXR5
RPC2H0JzkS+2uZp8B0Hk1iDPqbxWXJE9I57CxBV9C/tfzo2Iht00cuJ4LY+sw+y/
ocKpJbdLTWrTLdqLHwicdn80xeWot1m0ukyK2l0UeDkY6H5pYPtHTpAZvRbD7ETL
Zs2RP3KFFvho6aIDGrY0wee740/jWotx7fbxxKwPyDRsbH3+1Wx/eX2RND40GdkH
gejJEzpk/7y/P/hCad7bSddHZw0+Z03HIRC0E8yQz+JYatrqckaRctd7cXryTmTR
FbvLJmECgYBDpfno2CzcFJCTdNBZFi34oJRiDb+HdESXepk58PcNcgK3R8PXf+au
OqDBtZiUfV9U1WAgOgzGwt/0Y9u2c8m0nXziUS6AePxy5sBHs7g9C9WeZRz/nCWK
+cHiM7X0wBEzDKz5f9eBqRGipm0skDZNK18X/5QMTT5K3Eci2n+1Tw==
-----END RSA PRIVATE KEY-----
```

Public key

Public key file in “*.pub” format is used to verify a digital signature. Public key is present on the remote side and allows access to the owner of the matching private key.

An example of public key format:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACpuju0iTKCcGkbbBhrk0HjmeZR5QpM0swscXQE7fOZG0oQSURoapd9
```

How to add your own key

First, generate a new keypair of your public and private key:

```
local $ ssh-keygen -C 'username@organization.example.com' -f additional_key
```

Please, enter **strong passphrase** for securing your private key.

You can insert additional public key into `authorized_keys` file for authentication with your own private >key. Additional records in `authorized_keys` file must be delimited by new line. Users are not advised to remove the default public key from `authorized_keys` file.

Example:

```
$ cat additional_key.pub >> ~/.ssh/authorized_keys
```

In this example, we add an additional public key, stored in file `additional_key.pub` into the `authorized_keys`. Next time we log in, we will be able to use the private `additional_key` key to log in.

How to remove your own key

Removing your key from `authorized_keys` can be done simply by deleting the corresponding public key which can be identified by a comment at the end of line (eg. `username@organization.example.com`).