FHPC - presentation and SSH 101

Ruggero Lot

October 3, 2022

Who am I?

- Technologist behind ORFEO. In practice? Development Operations.
  Software development and deployment to allow the usage of computational tools such as ORFEO (our cluster).
- I also do research in applied condensed matter.

Who am I?

- Technologist behind ORFEO.
- I also do research in applied condensed matter.
  Bridge molecular dynamics and density functional theory with machine learning approaches.

The HPC cluster

Is a collection of machines with different characteristics:

- fat nodes: 2 Intel Xeon (36 cores) and 1536GB RAM
- thin nodes: 2 Intel Xeon (24 cores) and 768GB RAM
- gpu nodes: 2 Intel Xeon (24 cores) and 256GB + 2 Nvidia V100 32GB RAM each
- epyc nodes: 2 AMD EPYC (64-Core) and 512GB RAM

The support infrastructure

Is a collection of machines with different characteristics mainly

- 2 Intel Xeon (10 cores)
- ram between 64 to 512GB

depending on their usage.

They run several services, mainly VMs and Kubernetes.
OSes: Fedora 36, Centos 7, Debian, Freebsd.

How to access all this bonanza?

1. Connect to an entry point (login node)
2. ask for the resources you need to a scheduler,
3. wait for your turn in the queue.

Today we will only discuss point 1.

What is this login node?

The login node, in this case, is a container inside a pod on the Kubernetes infrastructure running an *sshd* daemon. This container must allow you to ask for resources through the scheduler.

What is this login node?

From a practical perspective, you can see it as a machine that allows you to connect by using *ssh*, and drops you in a shell where you can run commands.

Which commands? Any that is installed, but be aware that the login node is not a place where to run your heavy code! (You will get stopped and other people on the login might get angry at you)

How do we connect to this node?

SSH

Secure SHell is a protocol that allows for secure transfer of data from a server (in our case the login node) to a client (our computer)

How to obtain it?

- On any [1] Linux distribution: shipped by default
- Apple : shipped by default
- Windows: there are software like putty, recent versions of WSL should have it.

[1] reasonable

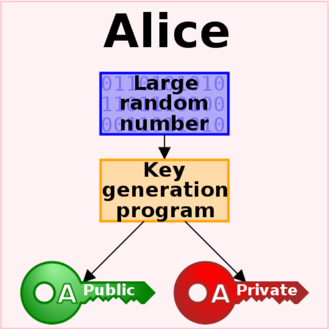
How to use it?

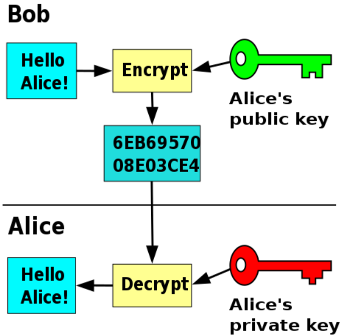
1. Fire up a terminal
2. `ssh username@(FQDN or ip)`

FQDN	ssh.wikipedia.org
ip	195.14.102.205

3. Authenticate
   Usually password, authentication is offered by we offer only key authentication.

What is key authentication?





wikipedia

What is key authentication?

The public key must be uploaded to the server. *ssh-copy-id* if the server allows other authentication methods, in our case you will have to give us the key.

The ssh handshake is much more complicated and uses approximately 10 keys, here we are limiting ourselves to the ones you need to know.

Generate the key

```
[vagrant@fedora ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key
(/home/vagrant/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/vagrant/.ssh/id_rsa
Your public key has been saved in
/home/vagrant/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:JMSeewt4t.....wrqn4bm2vc vagrant@fedora
```

id_rsa

DO NOT SHARE THIS FILE

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAA
......
PqyyyjbBXMzK3qo3kfJIKXGFj6j0GGh7+
0zcxiJivJFfEUAAAA0dmFncmFudEBmZWRvcmEBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

id_rsa.pub

SHARE THIS FILE

```
ssh-rsa AAAAB3N.........mg+h51dthN
R1hWu0VXO5zhHyNqIjQ6nNRPfTtbIa+hGp
P4L0cjeC3zdbD33+asdfasoSp0y0umoHox
08s= a_comment_here
```

and possibly fix the comment or delete it.
Once you have generated this file copy its content in `bit.ly/3fAUGUl`, and we will add it to the `authorized_keys` file in the `.ssh` folder in your home. Once this is done you will be able to connect to the cluster.

First connection, and the server key

The server has identified us but we need to identify it to avoid man-in-the-middle attacks.

```
ssh username@192.168.56.129
The authenticity of host '192.168.56.129'
can't be established.
ED25519 key fingerprint is
SHA256:3n8/5Pex0yCovbBZKHpDGFBztLIBWFiGu7L6TPrz624.
This key is not known by any other names
Are you sure you want to continue connecting
(yes/no/[fingerprint])?
```

First connection, and the server key

This information is stored in `~/.ssh/known_hosts` on your client. If something nasty happens eg. the server change keys, you no longer be able to login until you haven't deleted the old entry from the file.

other useful commands:

- `scp src dst`
- `rsync src dst`

In `~/.ssh/config`, you can define shortcuts

```
Host orfeo
   Hostname the_ip
   User username
```

then you can simply: `ssh orfeo`.

Take home messages

- to generate the key use: `ssh-keygen`
- to connect: `ssh username@ip`

Resources to install Fedora in virtualbox

- https://itsfoss.com/install-fedora-in-virtualbox/