Accessing the cluster

Step 0: Getting an account

All DIFA staff members have the right to access the OPH computing cluster. However, the access must be explicitly requested in order to obtain a valid account.

More specifically, DIFA staff members should direct an **access request email** to the computing responsible for their research sector:

applicata
: Nico Curti nico.curti2@unibo.it

astro
: Marco Baldi marco.baldi5@unibo.it

atmos
: Paolo Ruggieri paolo.ruggieri2@unibo.it

didattica
: Olivia Levrini olivia.levrini2@unibo.it

materia
: Cesare Franchini cesare.franchini2@unibo.it

nucleare
: Lorenzo Rinaldi lorenzo.rinaldi@unibo.it

teorica
: Pierbiagio Pieri pierbiagio.pieri@unibo.it

terra
: Filippo Zaniboni filippo.zaniboni@unibo.it

esterni (INFN)
: Daniele Cesini daniele.cesini3@unibo.it

For **students** the request must be submitted by their thesis supervisor. For **external users** (i.e. non-DIFA staff members) the request must be submitted by a DIFA-staff reference person.

Valid UniBo credentials are in any case necessary to obtain an account and to be able to access the cluster (for external users temporary credentials must be obtained first).

New users will be able to access the cluster after 7.00am of the day after the one they have been added to the access group. The home folder of every new user is **automatically created at the time of the first access** to the cluster.

Individual **accounts remain valid until termination of the conditions granting access rights** to the cluster (as e.g. until termination of DIFA affiliation, end of the Master/PhD thesis, end of the research collaboration for external users) and the computing responsibles of each sector have the duty to remove users from the respective access groups upon expiration of such access rights.

In any case, the home folders and all the stored data of inactive users will be automatically deleted after 6 months from their last modification time without any further notice.

Step 1: Connecting to the cluster

The cluster can be **accessed remotely through a Frontend Login node via a bastion host**, through the `ssh` secure connection protocol, using UniBo institutional credentials (i.e. username and password used for all UniBo IT services).

There are **multiple independent Frontend Login Nodes:**

- ophfe1 (137.204.165.41)
- ophfe2 (137.204.165.42)
- ophfe3 (137.204.165.43) **reserved – VM for some special tasks**

The **connection procedure** requires the use of the bastion, that allows 'mediated' ssh access to resources on the department's network, avoiding direct external exposure of services and drastically improving network security. To connect from the terminal use the following syntax:

- **STAFF MEMBERS** with e.g. UniBo email address `donald.duck7@unibo.it` can connect to the cluster with the command:

```
ssh -J donald.duck7@bastion-nav.difa.unibo.it donald.duck7@ophfe1
```

- **STUDENTS** with e.g. UniBo email address `mickey.mouse4@studio.unibo.it` can connect to the cluster with the **same command**:

```
ssh -J mickey.mouse4@bastion-nav.difa.unibo.it mickey.mouse4@ophfe1
```

followed by their UniBo institutional password (twice).

This will do a two-step connection, first to bastion-nav.difa.unibo.it (137.204.165.34) which is the **bastion host**, then to the specified cluster frontend. To avoid specifying it every time, you can simply add the following lines to `~/.ssh/config`:

```
Host bastion-nav
  Hostname bastion-nav.difa.unibo.it
  User     your.loginname

Host ophfe1 ophfe2
  User      your.loginname
  ProxyJump bastion-nav
```

After having added such lines, you can simply use `ssh ophfe1`.

For some users in PERSONALE their account does not match the mail address (so called “cambio UPN”). It's always possible to use:

```
ssh -l mail.address@unibo.it ophfe1
```

or even:

```
ssh mail.address@unibo.it@ophfe1
```

'User' line in `~/.ssh/config` also accepts the mail address.

Graphic windows require a connection with X11 forwarding, which can be established with the `ssh` options `-X` and/or `-Y` (rarely needed, **might expose your client to attacks**). In general, connecting with:

```
ssh -X albert.einstein9@ophfe1
```

is enough to use graphical tools.

If you see a message like:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:uR0mI0jPbLhSd/1HISczCCpoK9OZLOs+uqQx9b1CDjU.
```

it's probably because you connected to the old Str957-cluster (replaced by ophfe1) and server's ssh key have been changed (or you connected to the old bastion and are now connecting to bastion-nav).

CHECK that the displayed key **for bastion-nav** is one of these:

- **ECDSA**: D5hNeP9NbU/OFjPyxlp7nsryHq9Sl9WKC3ef7rUaQg4
- **ED25519**: uR0mI0jPbLhSd/1HISczCCpoK9OZLOs+uqQx9b1CDjU
- **RSA**: NUJz6tcBoz+xxOroOUeQnqQrvH99RpmS5e9io/KwYm4

then

```
ssh-keygen -R bastion-nav.difa.unibo.it
```

to remove old fingerprint from your PC.

Keys for ophfe1 and ophfe2 have not been changed and their hashes are:

- ophfe1:
  - **ECDSA**: aoqtNWk0OvSDuWAMV1y7l3E9ofdI6TKBEJxpGpPoYH4
  - **ED25519**: J7k3kS0BWspWcPNdq0Dkyuhoj3z1gnrZOCT0r+BWx2Q
  - **RSA**: bgydnQeWV3puQNHJ9hjEKo2ziLriWC/ypVWNTp1C6/k

- ophfe2:
  - **ECDSA**: aoqtNWk0OvSDuWAMV1y7l3E9ofdI6TKBEJxpGpPoYH4
  - **ED25519**: J7k3kS0BWspWcPNdq0Dkyuhoj3z1gnrZOCT0r+BWx2Q
  - **RSA**: bgydnQeWV3puQNHJ9hjEKo2ziLriWC/ypVWNTp1C6/k

Now you can retry the ssh connection: it will tell you that it can't verify server's identity and show key hash. **Verify (again)** that the key hash is from the list above, and accept it (iif it matches).