

Connection with SSH: Windows session

Olivier Mattelaer
UCLouvain
CP3 & CISM

Plan of the talk

- Cluster presentation

- how the cluster are organised
- On which machine you can connect and from where

- SSH theory

- What is a public/private key

- SSH exercise

- How to get your keys
- Use of MobaXterm
- Frequent error

Node in a cluster

- A cluster is a set of machine



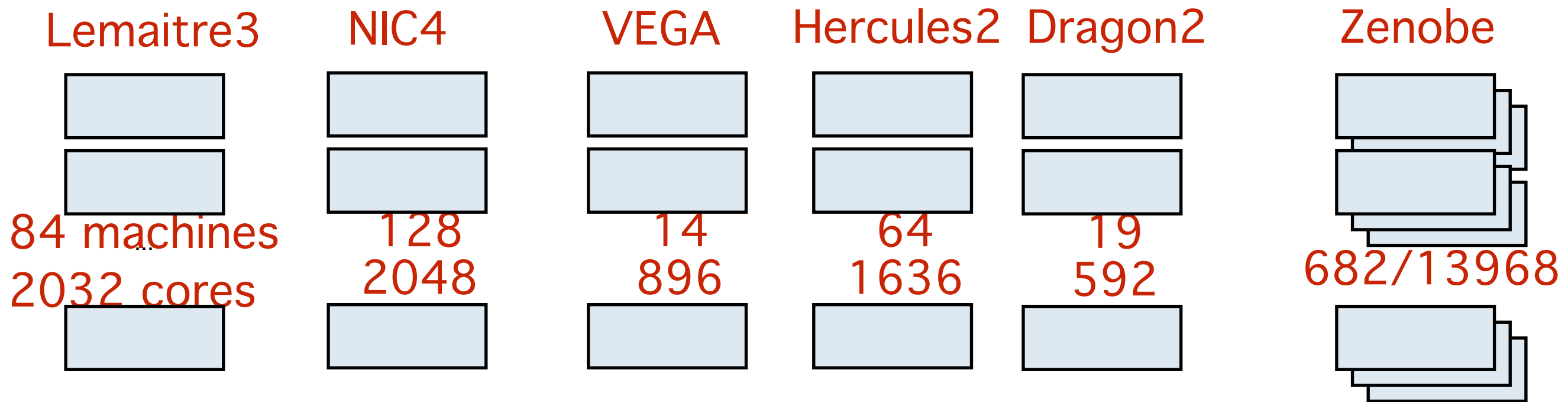
Lemaitre 3



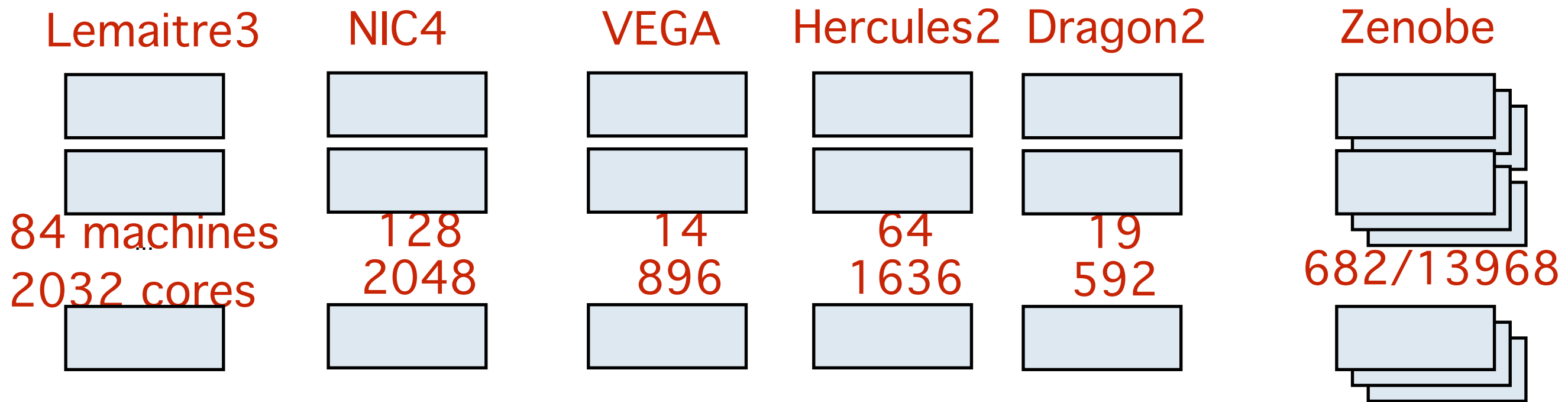
NIC4



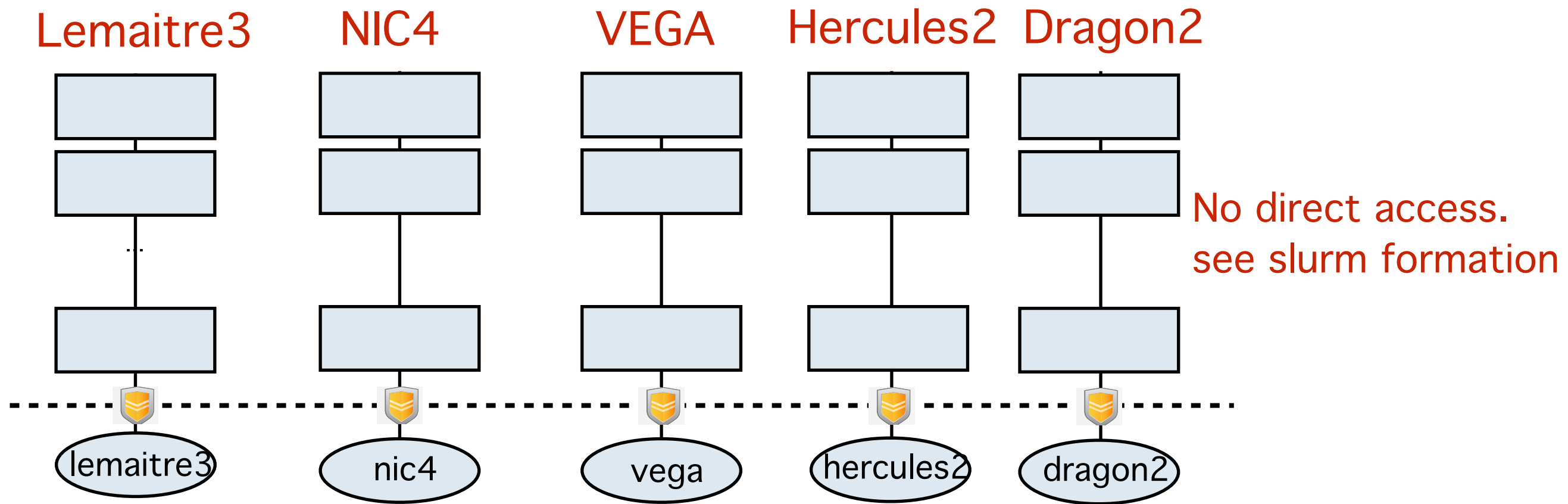
Zenobe



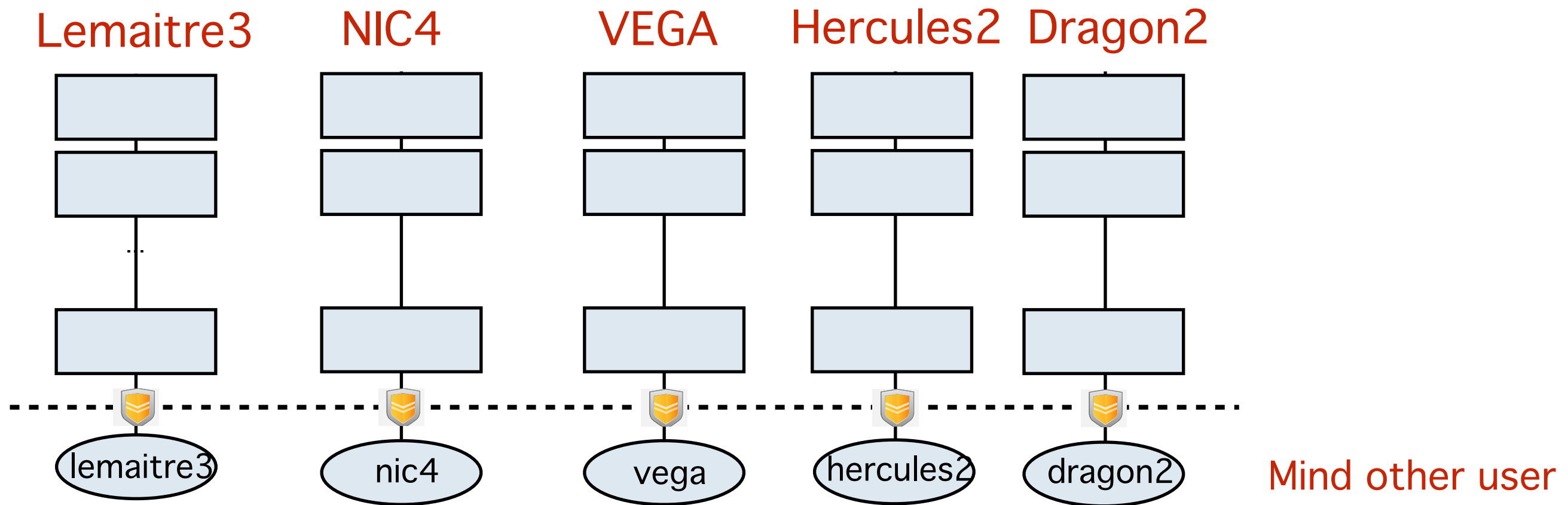
- Close to 8000 cores available through your login
 - ➔ 14k more with zenobe (require approval but same login)
 - ➔ More available at European level (Prace program)
 - ◆ European competition to receive cpu time



- You do not need/want to physically connect to all those machines to run script
 - ➔ Difficult to control fair share of the machines
 - ➔ Using a job scheduler -> SLURM
 - ➔ See slurm session for details on how to request machine for running a job



- To request machine, you connect to the **FRONTNODE** (also called user interface)
 - ◆ You can not connect to the other cpu!
 - ◆ You have to submit a job
 - ➔ **No heavy jobs** on that machine
 - ◆ You will impact everyone
 - ◆ rather use debug/fast partition



- To request machine, you connect to the **FRONTNODE** (also called user interface)
 - ◆ You can not connect to the other cpu!
 - ◆ You have to submit a job
 - ➔ **No heavy jobs** on that machine
 - ◆ You will impact everyone
 - ◆ rather use debug/fast partition

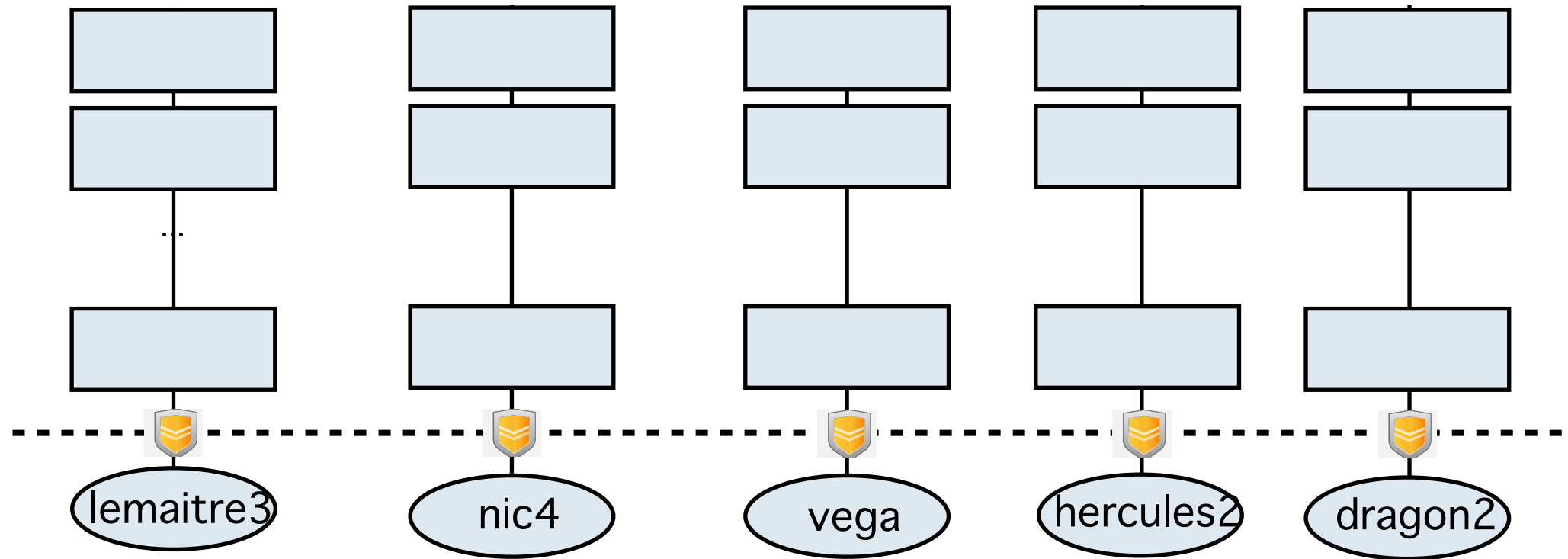
Lemaitre3

NIC4

VEGA

Hercules2

Dragon2



- Cluster address:

- ➔ lemaitre3.cism.ucl.ac.be
- ➔ login-nic4.segi.ulg.ac.be
- ➔ hercules.ptci.unamur.be
- ➔ dragon2.umons.ac.be
- ➔ vega.ulb.ac.be

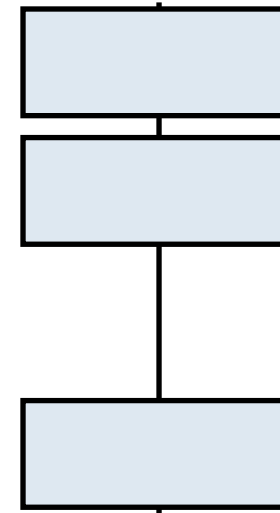
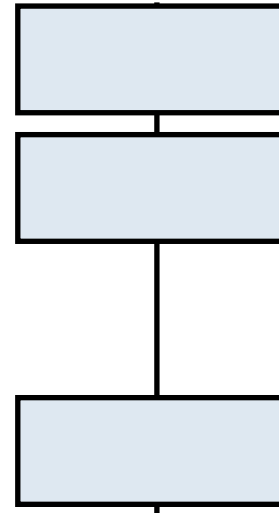
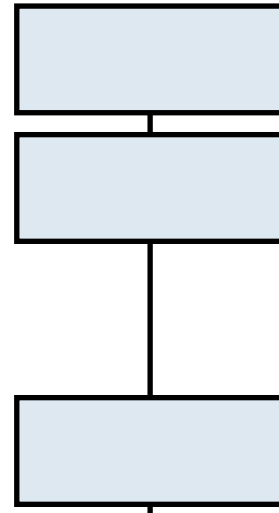
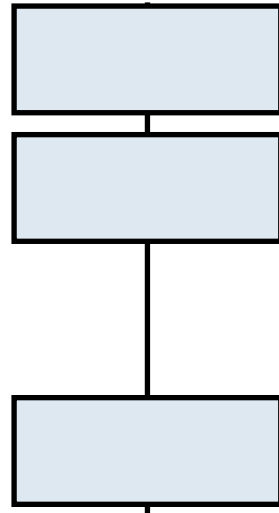
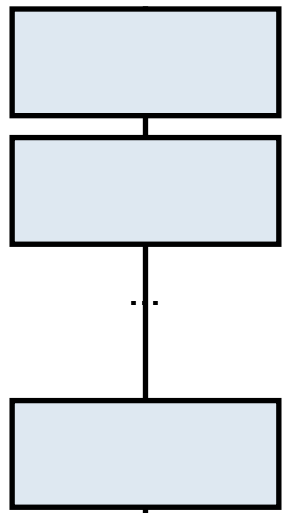
Lemaitre3

NIC4

VEGA

Hercules2

Dragon2



lemaitre3

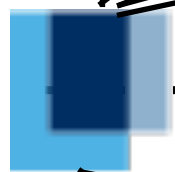
nic4

vega

hercules2

dragon2

Private network



Gateway



Home or your office





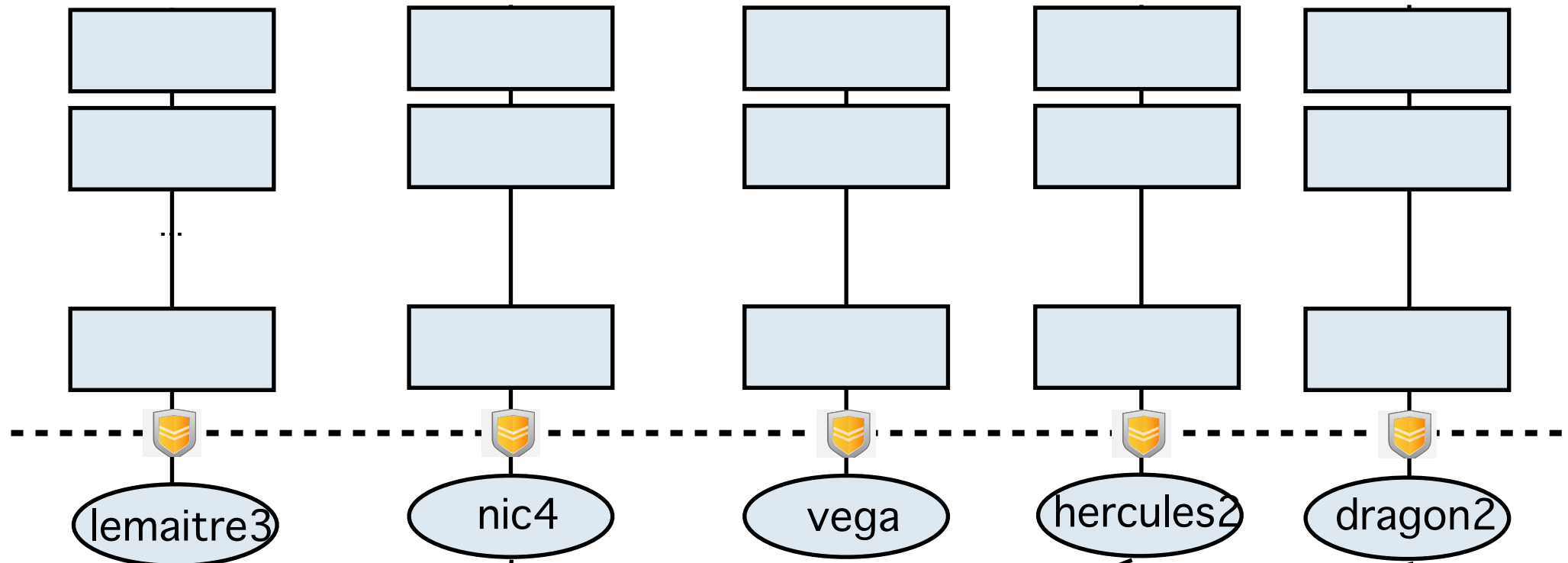
Lemaitre3

NIC4

VEGA

Hercules2

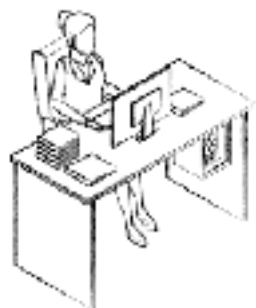
Dragon2



Private network



Gateway



ULG Network



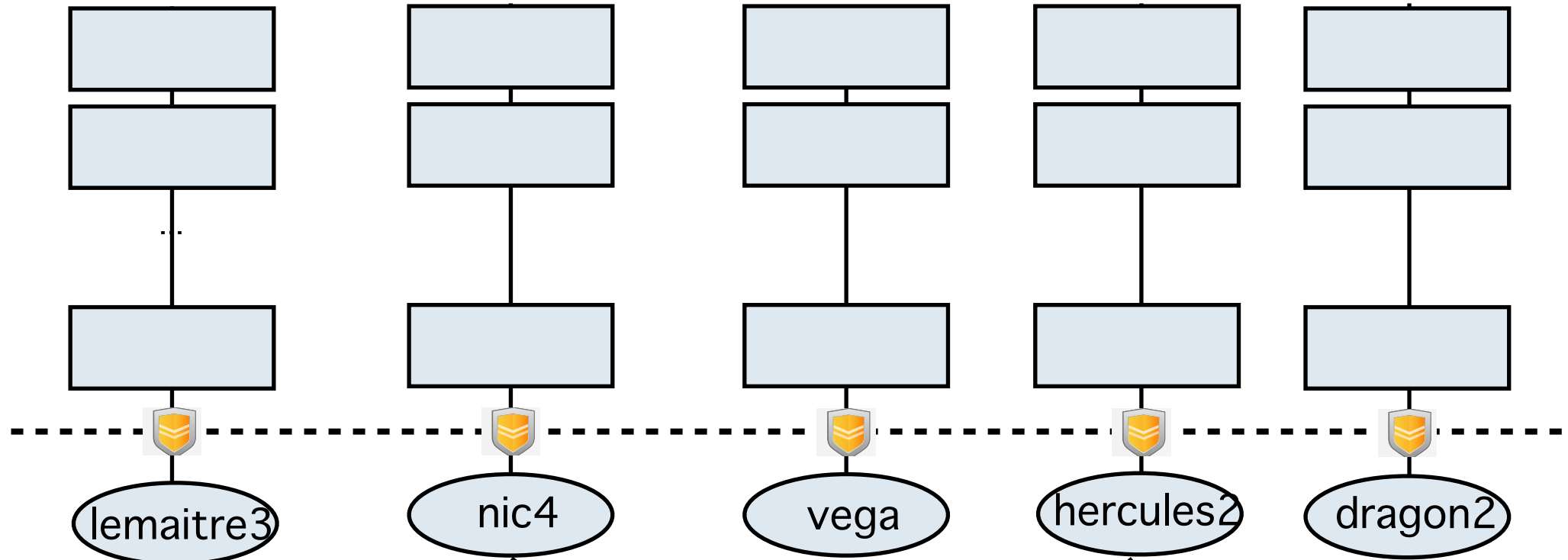
Lemaitre3

NIC4

VEGA

Hercules2

Dragon2



Private network



Gateway



Home or your office (ULB members)





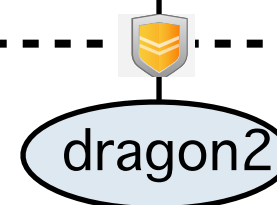
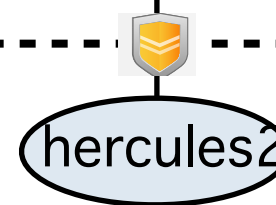
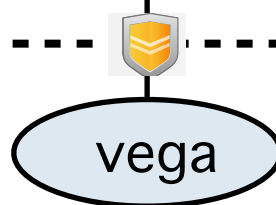
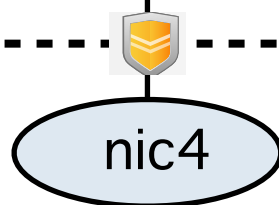
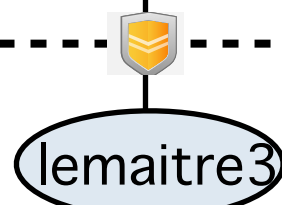
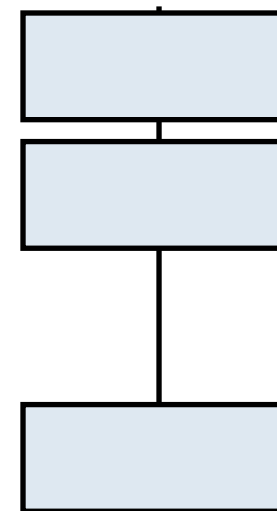
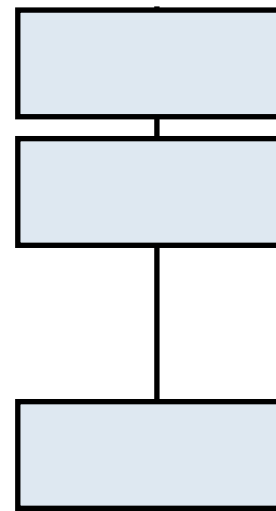
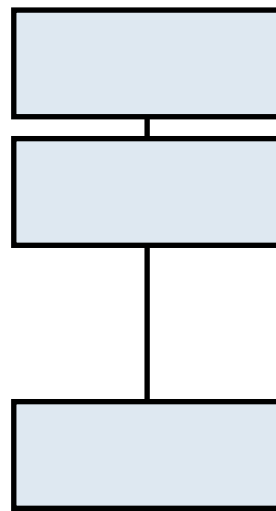
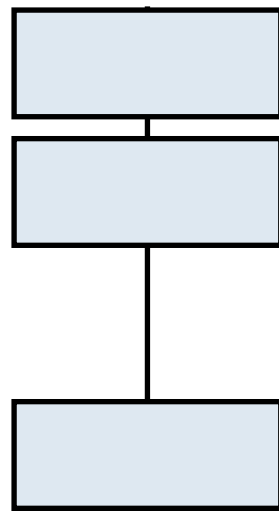
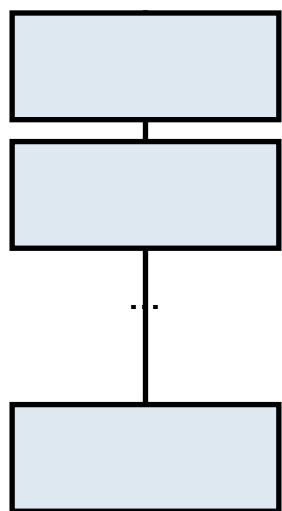
Lemaitre3

NIC4

VEGA

Hercules2

Dragon2



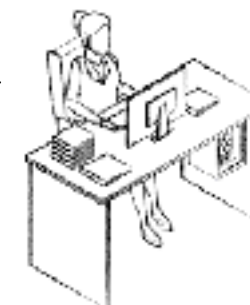
Private network



Gateway



Home or your office
Gateway login is via
university login



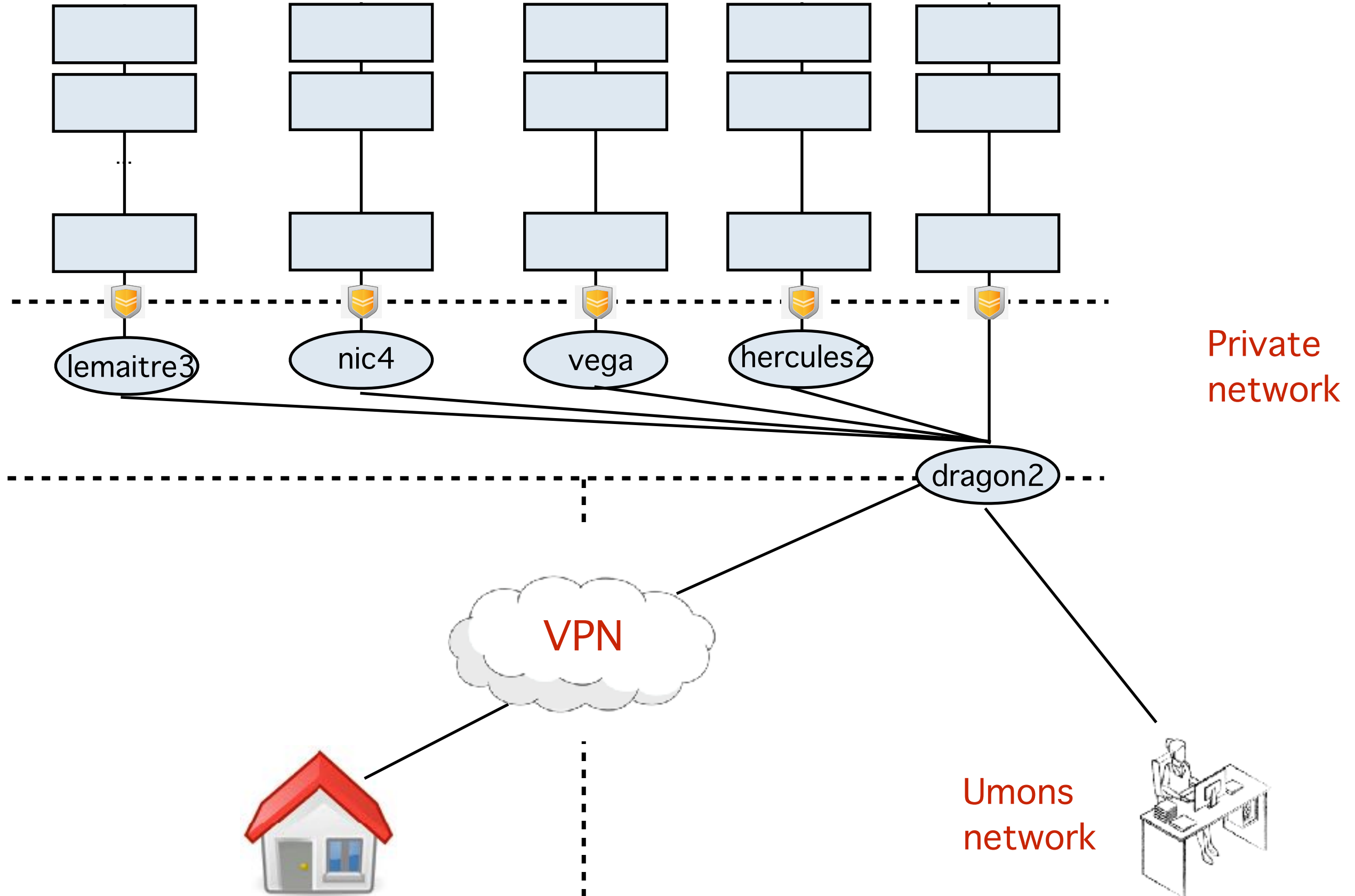
Lemaitre3

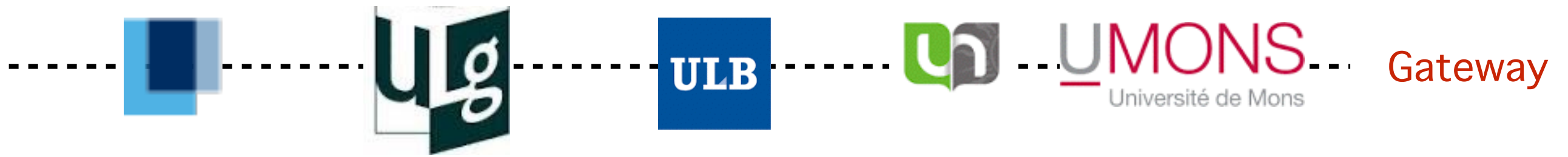
NIC4

VEGA

Hercules2

Dragon2





- Machine where you can not do anything

- ➔ But gives you access to the frontend

- Gateway address

- ➔ gwceci.cism.ucl.ac.be

- ➔ gwceci.unamur.be

- ➔ gwceci.ulb.ac.be

- ➔ dragon2.umons.ac.be

- ➔ gwceci.uliege.be

SSH concept



Each user can enter the computer via a dedicated door protected via a key hole

Key hole
=
Public key



The user has the associate key

Physical key
=
Private key



To protect the key it is store in a safe with digicode

Digi-code
=
Pass-phrase

SSH concept



Key hole
=
Public key



Physical key
=
Private key



Digi-code
=
Passphrase

- When you create/renew your CECI account
 - ➔ We generate the public key (key hole)
 - ◆ Set it up on all cluster
 - ➔ We generate the private key (crypted by your passphrase)
 - ➔ Send it to YOU by email (we do not have any copy)



● Public key

- ➔ Used to encrypt data
- ➔ Use to verify digital signature



● Private key

- ➔ Used to decrypt data
- ➔ Create digital signature

steps of a ssh connection

1. Establishing communication and Negotiate algorithm of encryption

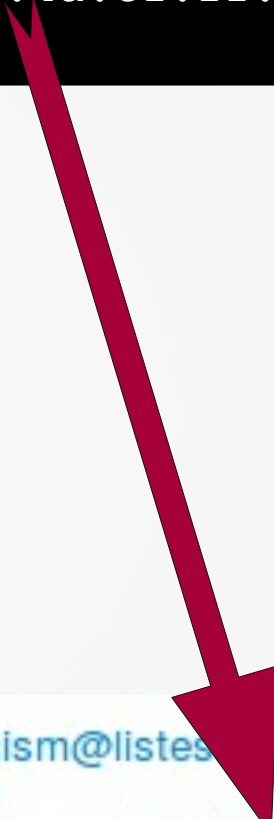
2. Host Identification

- ➔ Host send his public key + message sign with Host private key

Example

```
$ ssh -i ~/.ssh/id_rsa.ceci jcabrera@hmem.cism.ucl.ac.be
The authenticity of host 'hmem.cism.ucl.ac.be (130.104.1.220)' can't be established.
RSA key fingerprint is 06:54:39:a0:5c:b5:56:b3:29:9e:96:67:a0:4a:c1:ff.
Are you sure you want to continue connecting (yes/no)?
```

FIRST TIME you connect to a frontend host from a client,
you will be asked to accept the Public Key
Check the key fingerprint from CÉCI web site
<http://www.ceci-hpc.be/clusters.html#hmem>



SUPPORT: egs-cism@listes.uclouvain.be
Server SSH key fingerprint: (What's this?)
MD5: 06:54:39:a0:5c:b5:56:b3:29:9e:96:67:a0:4a:c1:ff
SHA256:
Xi4r0aNViNgg9KjnENiUFkEWPwnJGAjbnlX+m7Clm0

steps of a ssh connection

1. Establishing communication and Negotiate algorithm of encryption
2. Host Identification
 - ➔ Host send his public key + message sign with Host private key
3. Generation of symmetric key based on a common integer
 - ➔ from now all data are crypted with that method
4. User identification

Enough of “theory”
Let’s get practical and connect to
the machines !!



Consortium des Équipements de Calcul Intensif

6 clusters, 10k cores, 1 login, 1 home directory

I want to...

[create an account](#)

You are about to request an account on the CÉCI clusters.

The first step is to enter your email address. You will receive an email with a link to an online form which you will have to fill and submit.

Once your request has been approved, you will receive proper information on how to access the CÉCI clusters.

[renew my account](#)

[join an existing project](#)

create an account

My email address:

Send

Getting your private key (I)

- Users with email account access can ask for an account at: <https://login.ceci-hpc.be/init/>
 - ➔ Click 'Create Account'
 - ➔ Type in your email address
 - ➔ Click on the link sent to you by email.
 - ➔ Fill-in the form and hit the “Submit” button.
 - ➔ Wait ... (A sysadmin is reviewing your information). receive your private key by email.

SSH tools for windows

● Putty

- The most famous one
- Only ssh connection
- No file transfer, **bad support of key**

● MobaXterm

- Very easy
- Both connection and file transfer
- The one that you will use here

● OpenSSH on Windows (windows 10 since 2018)

- Linux like experience

Install MobaXterm



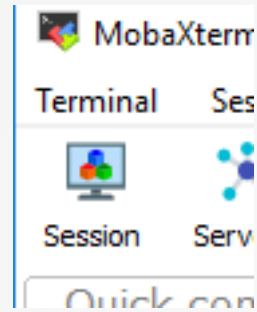
MobaXterm Home Edition v10.4
(Portable edition)

- search on your favorite web browser
- Download the free Portable edition
- Uncompress on folder
‘Documents\MobaXterm’
- Execute MobaXterm_Personal_X (where X
is version number)
- If needed allow firewall access for Private
and Domain networks

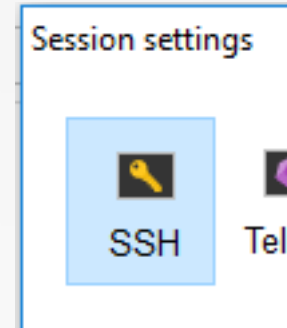
Configure mobaxterm

1) Save your id_rsa.ceci key file from your e-mail in a safe location

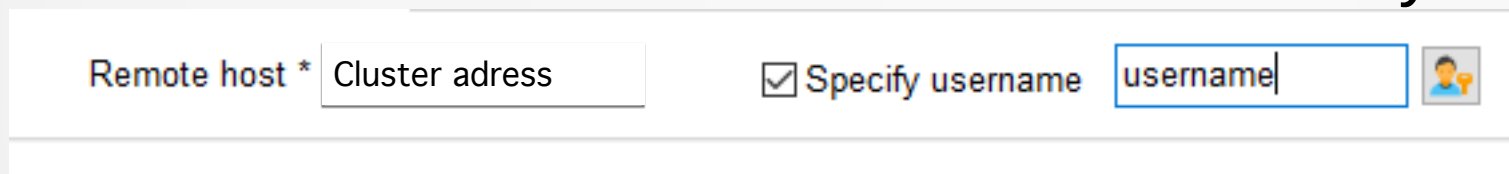
2) Click on Session



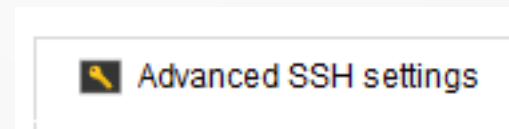
and SSH



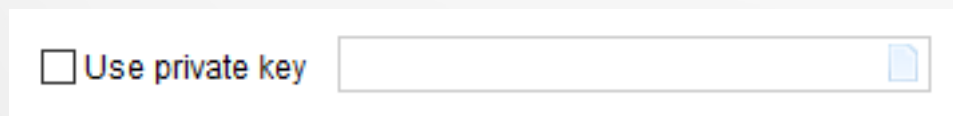
3) Add the Remote host hmem.cism.ucl.ac.be and your CÉCI user name



4) Select Advanced SSH Setting tab



5) Select use private key and browse for your id_rsa.ceci file



Depending of your version of mobaxterm/configuration it might ask you the passphrase already now

Gateway configuration

- Need to go through a gateway!
 - ➔ Network settings

Advanced SSH settings | Terminal settings | **Network settings** | Bookmark settings

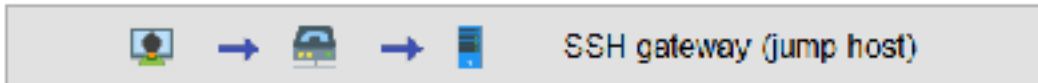
Connect through SSH gateway (jump host)

Gateway SSH server: Port: User:

Use private key

- Newer version looks like this:

Advanced SSH settings | Terminal settings | **Network settings** | Bookmark settings

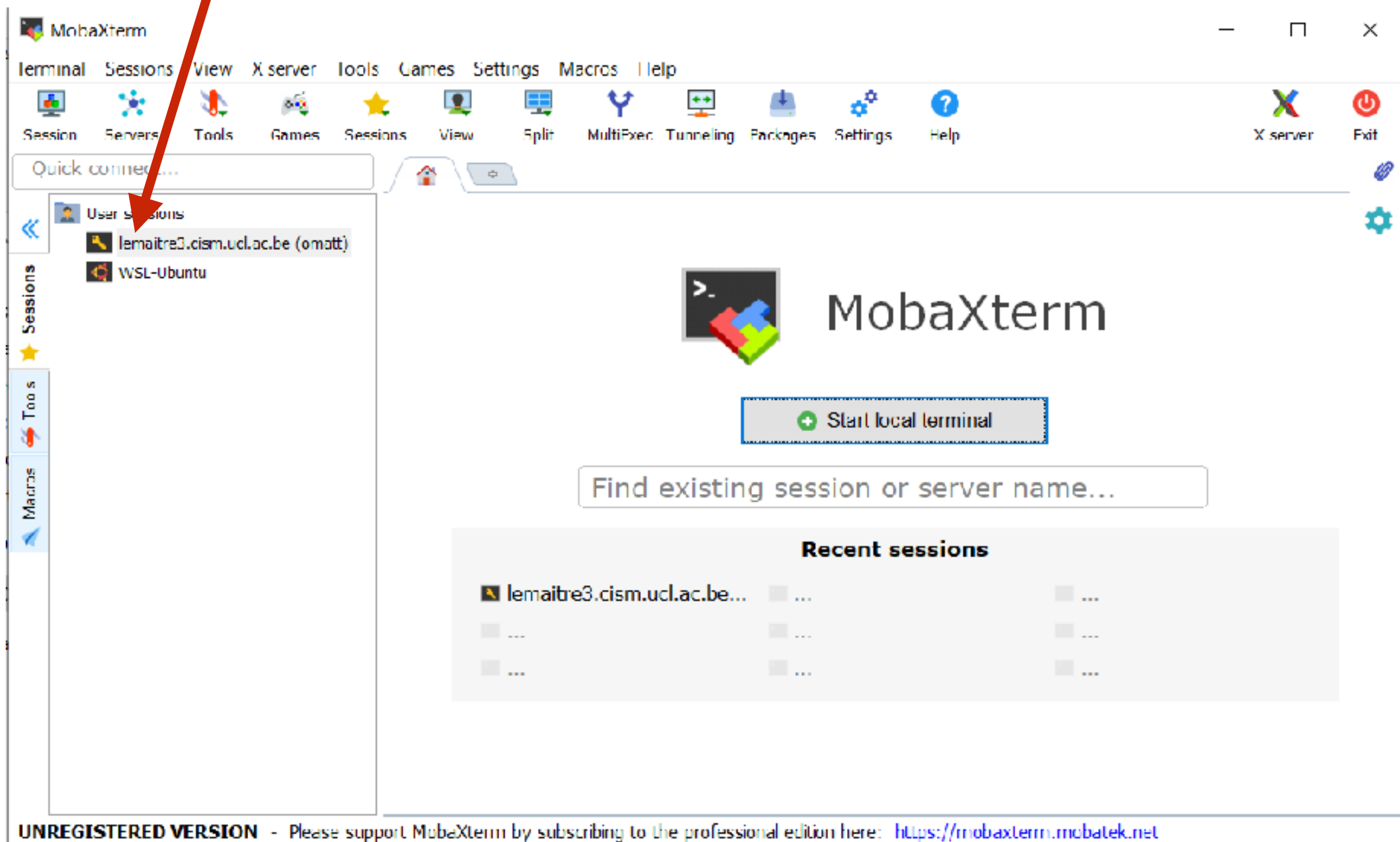
 **CLICK HERE**

Proxy settings (experimental)

Proxy type: Host: Login: Port:

You can now connect to the cluster

CLICK HERE



You are now connected

Terminal Sessions View X server Tools Games Settings Macros Help

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit

Quick connect...

4. lemaitre3.cism.ucl.ac.be (omatt)

```
Massively parallel CISM-CECI cluster

80 nodes: 2 x 12-core Intel Skylake 5118@2.3GHz, 96GB RAM
1:3-blocking OmniPath Architecture network

contact, support: cgs-cism@listes.uclouvain.be

-----
553/1984 CPUs available (load 72%) - 120 jobs running, 132 pending.

You currently have 0 job running, 0 pending.
You are using 39.1G ( out of 100G ) in $HOME.
You have 0G of data on $GLOBAL_SCRATCH.

Don't know where to start?
--> http://www.cec-hpc.be/install\_software.html
--> http://www.cec-hpc.be/slurm\_tutorial.html

[omatt@lm3-w001 ~]$
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

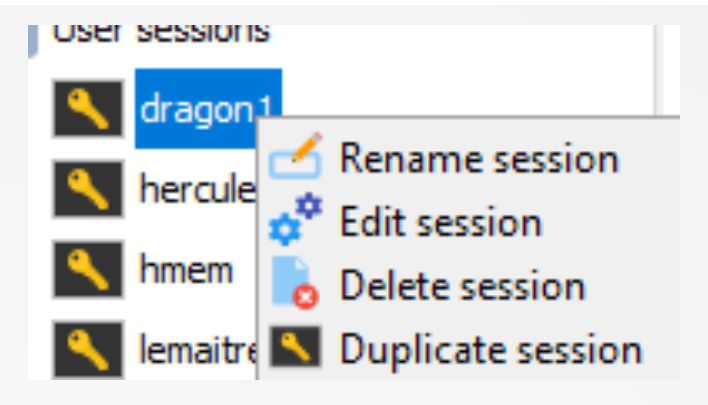
FILE ON DISK

TERMINAL

Exercise

- run `xeyes` to check that you can forward graphics through ssh
- Configure the other cluster that you need

Right click on a session to duplicate and rename it.



Frequent error

If, after running ssh, you are being asked for a password directly,

```
$ ssh hmem  
dfr@hmem.cism.ucl.ac.be's password:
```

it means that your SSH client did not try to use the SSH key.

If, after running ssh, you are being asked for a passphrase, then a password,

```
$ ssh hmem  
Enter passphrase for key '/home/dfr/.ssh/id_rsa.ceci':  
dfr@hmem.cism.ucl.ac.be's password:
```

it often means that the user name you are using is not the correct one. It could also mean that you are trying to connect with the new private key while it has not been synchronized to the cluster yet (clusters are not synchronized simultaneously.)

SSH AGENT

- Save your passphrase locally and let MobaXterm fill it for you! First, close your current ssh session

MobaXterm Configuration

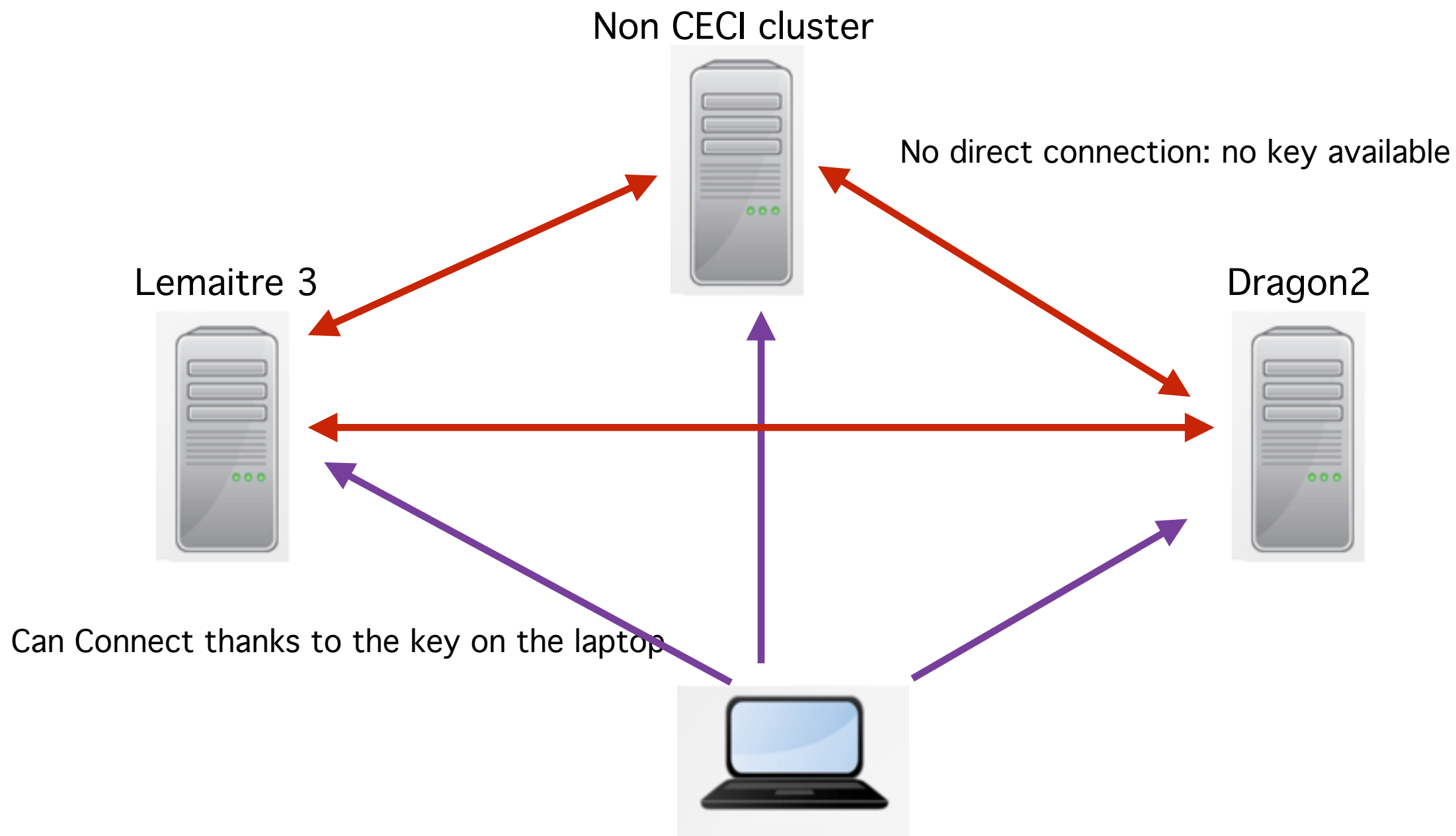
The screenshot shows the MobaXterm Configuration window with the SSH tab selected. The window has a title bar with a close button (X) and a toolbar with icons for General, Terminal, X11, SSH, Display, Toolbar, and Misc. The SSH settings are organized into three sections:

- SSH-browser settings:**
 - Enable graphical SSH-browser
 - Automatically switch to SSH-browser tab after login
 - Remote-monitoring (experimental)
 - Preserve file dates during SSH browser transfers
- SSH settings:**
 - SSH keepalive
 - Display SSH banner
 - Validate host identity at first connection
 - Default login:
 - Use 2-factor authentication for SSH gateways
 - GSSAPI Kerberos
 - Domain:
 - GSSAPI library:
 - Defaults for commandline SSH: Compression X11-Forwarding Fix connection issues
- SSH agents:**
 - Use internal SSH agent "MobAgent"
 - Use external Pageant
 - Forward SSH agents
 - Load following keys at MobAgent startup:

A tooltip is visible over the SSH-browser settings, stating: "The SSH-browser is a graphical remote file browser which is displayed in the sidebar. It allows you to browse your remote server content using the secure SSH connection." Three red arrows point to the checked checkboxes for "SSH keepalive", "Use internal SSH agent 'MobAgent'", and "Forward SSH agents".

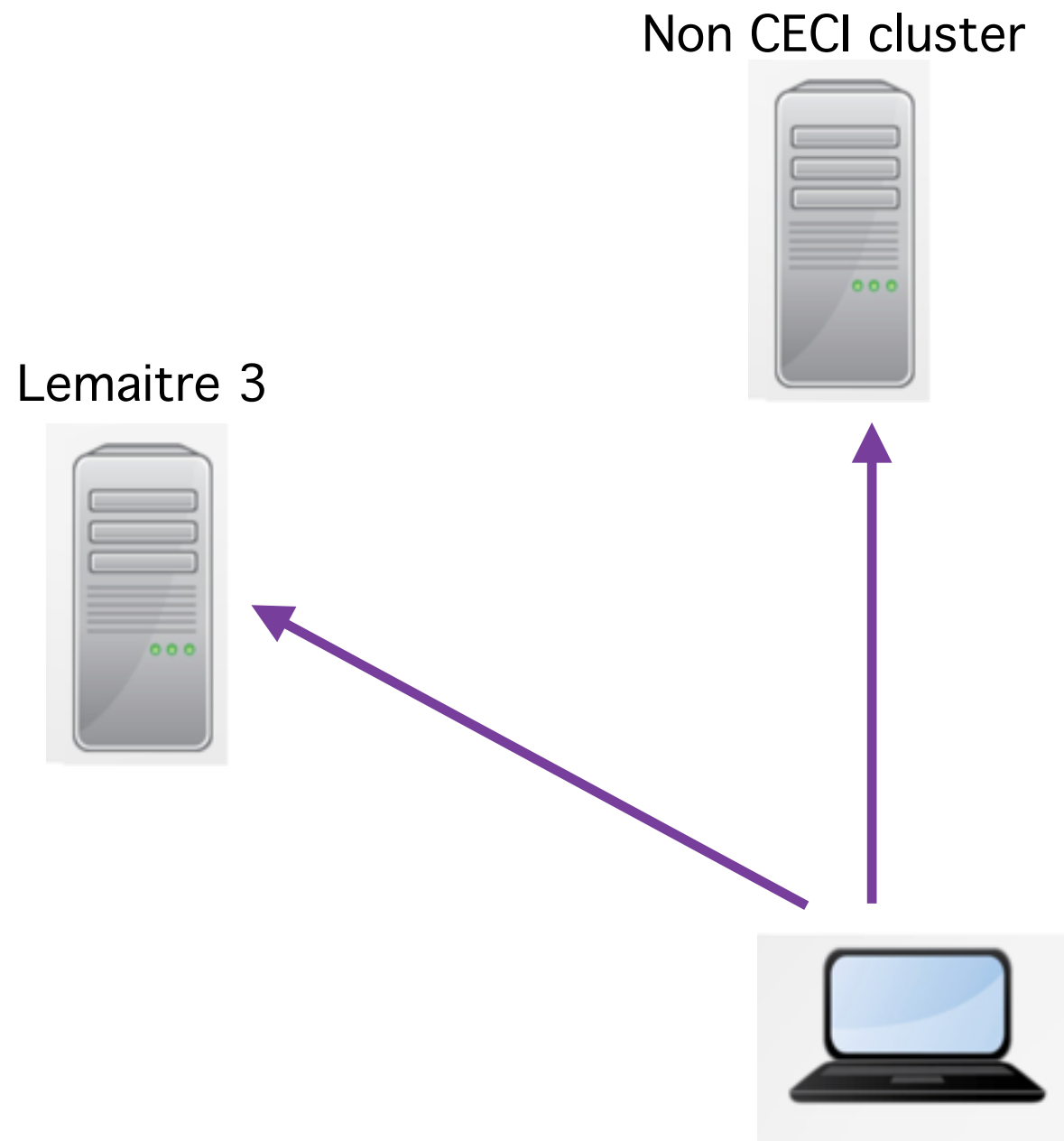
Avoid to propagate your private keys

- Less keys means more security



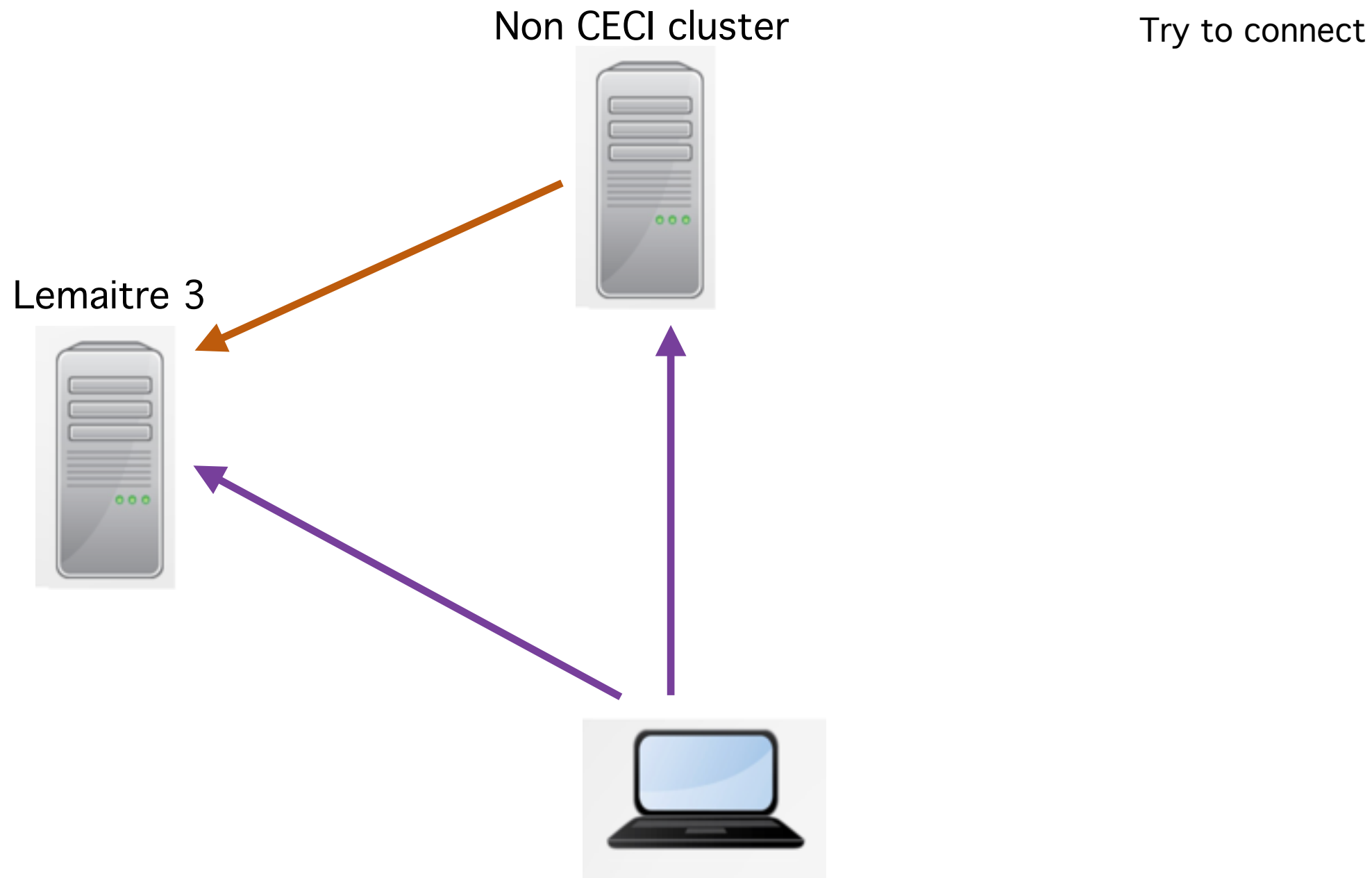
Avoid to propagate your private keys

- Forward agent send back the ssh request for a key to your laptop



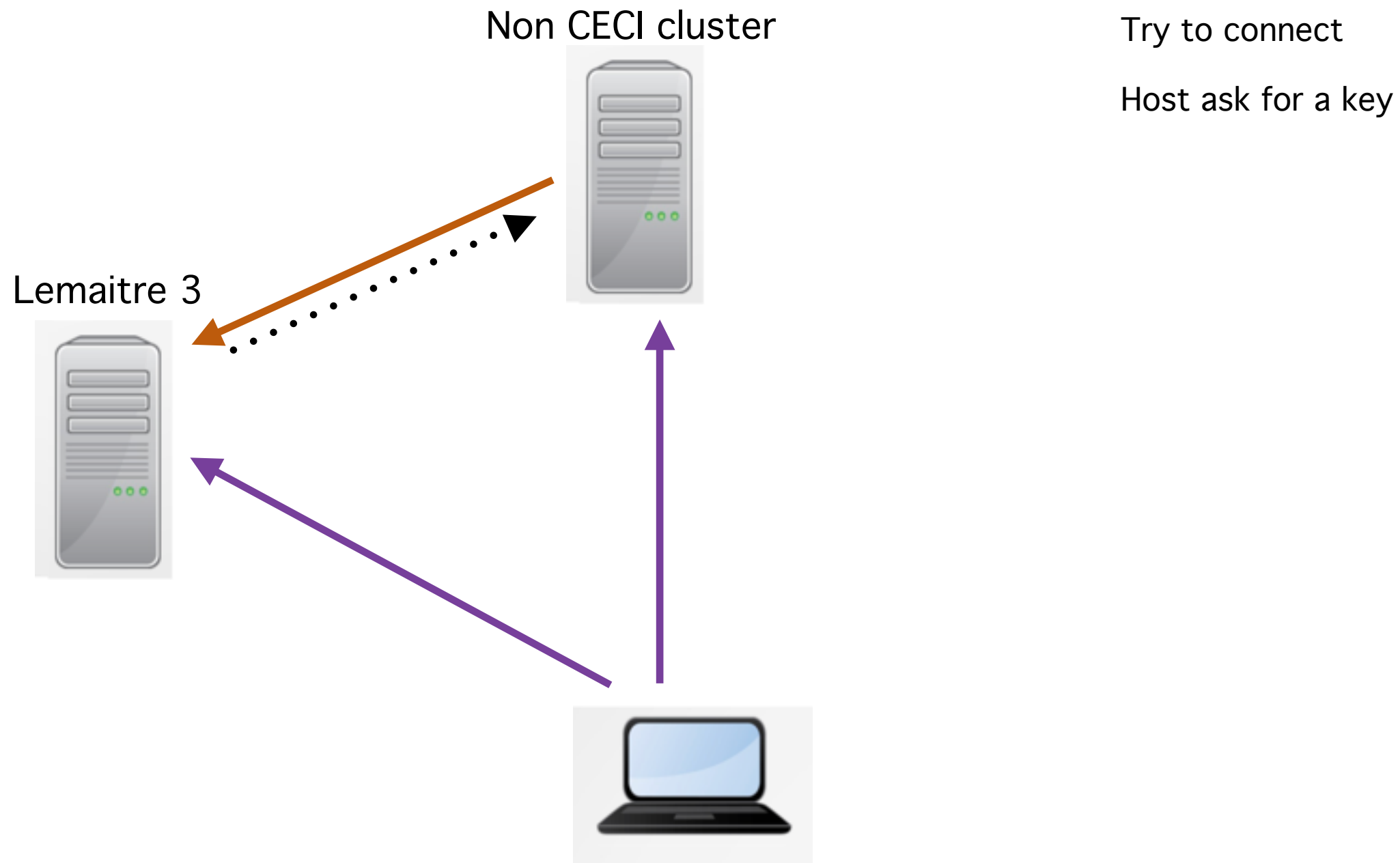
Avoid to propagate your private keys

- Forward agent send back the ssh request for a key to your laptop



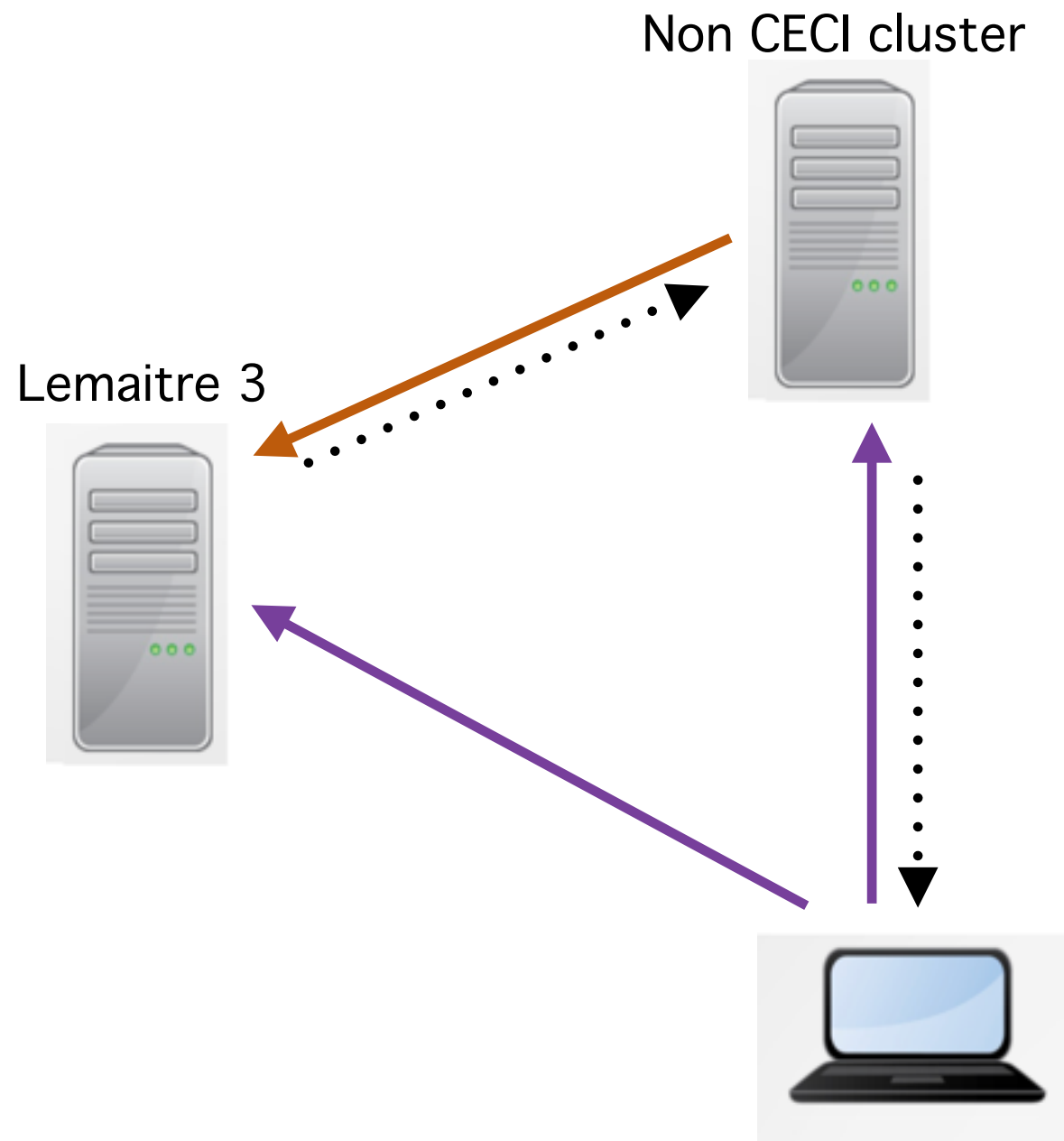
Avoid to propagate your private keys

- Forward agent send back the ssh request for a key to your laptop



Avoid to propagate your private keys

- Forward agent send back the ssh request for a key to your laptop



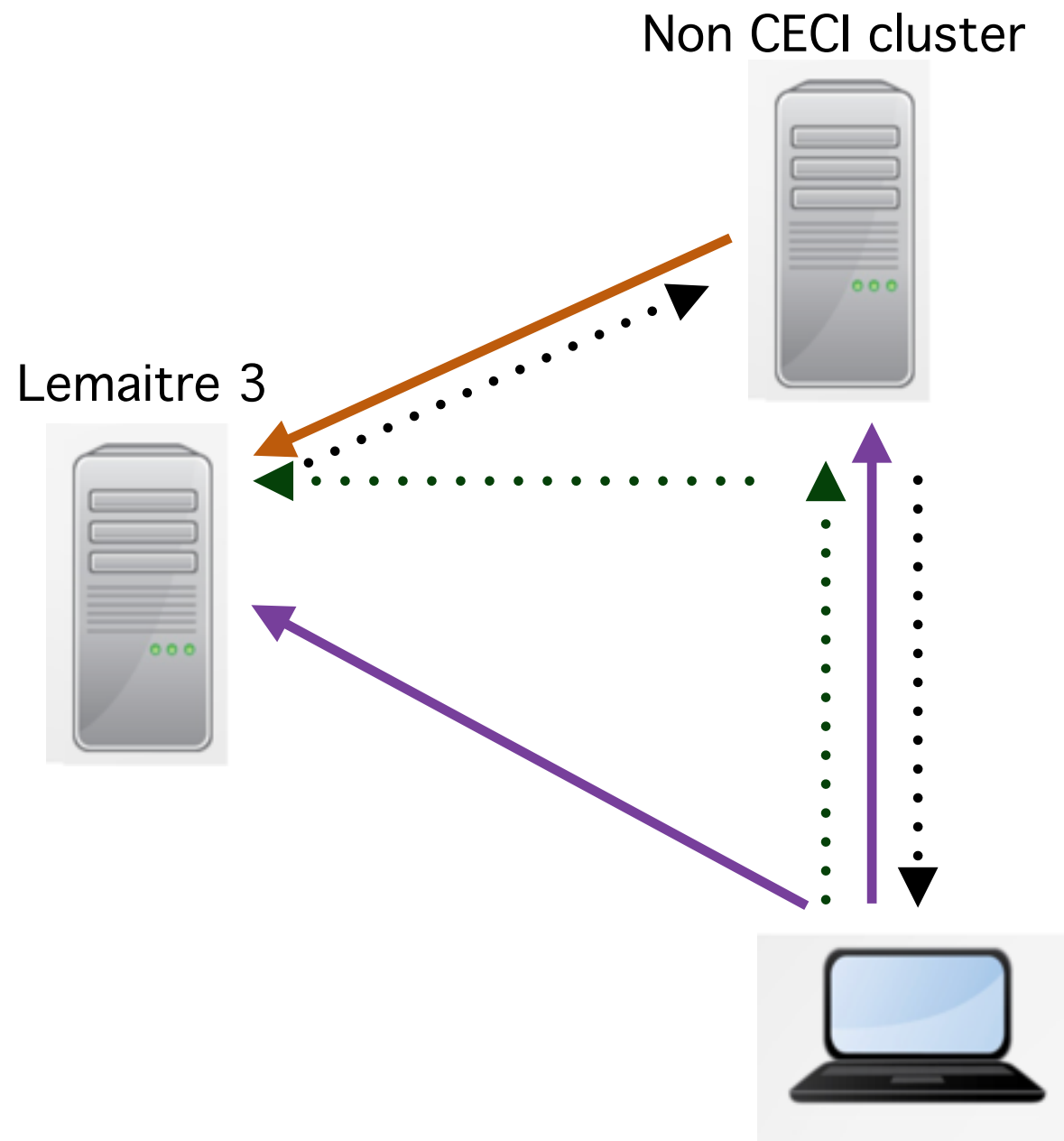
Try to connect

Host ask for a key

Message forward to laptop

Avoid to propagate your private keys

- Forward agent send back the ssh request for a key to your laptop



Try to connect

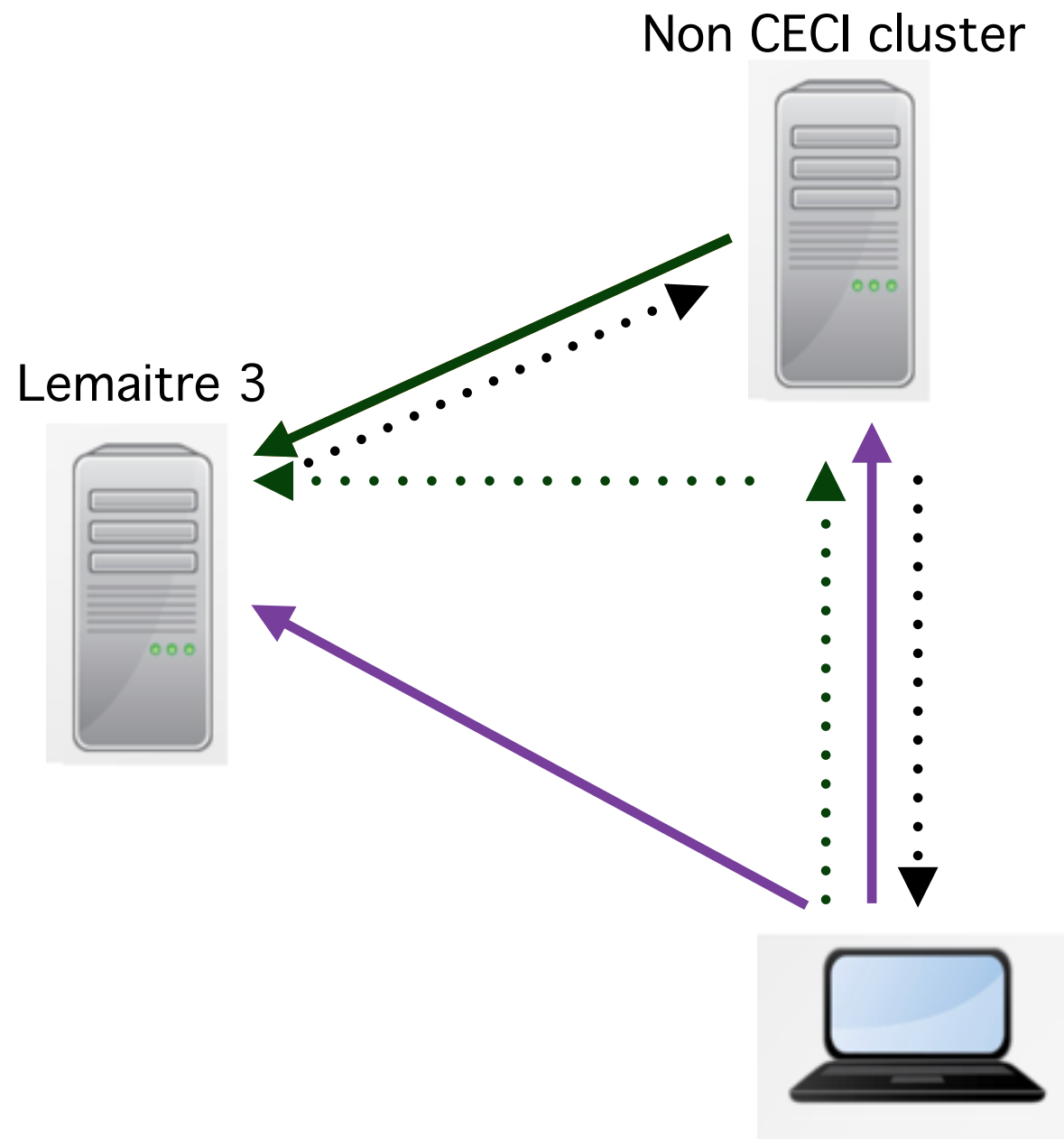
Host ask for a key

Message forward to laptop

Key provided

Avoid to propagate your private keys

- Forward agent send back the ssh request for a key to your laptop



Try to connect

Host ask for a key

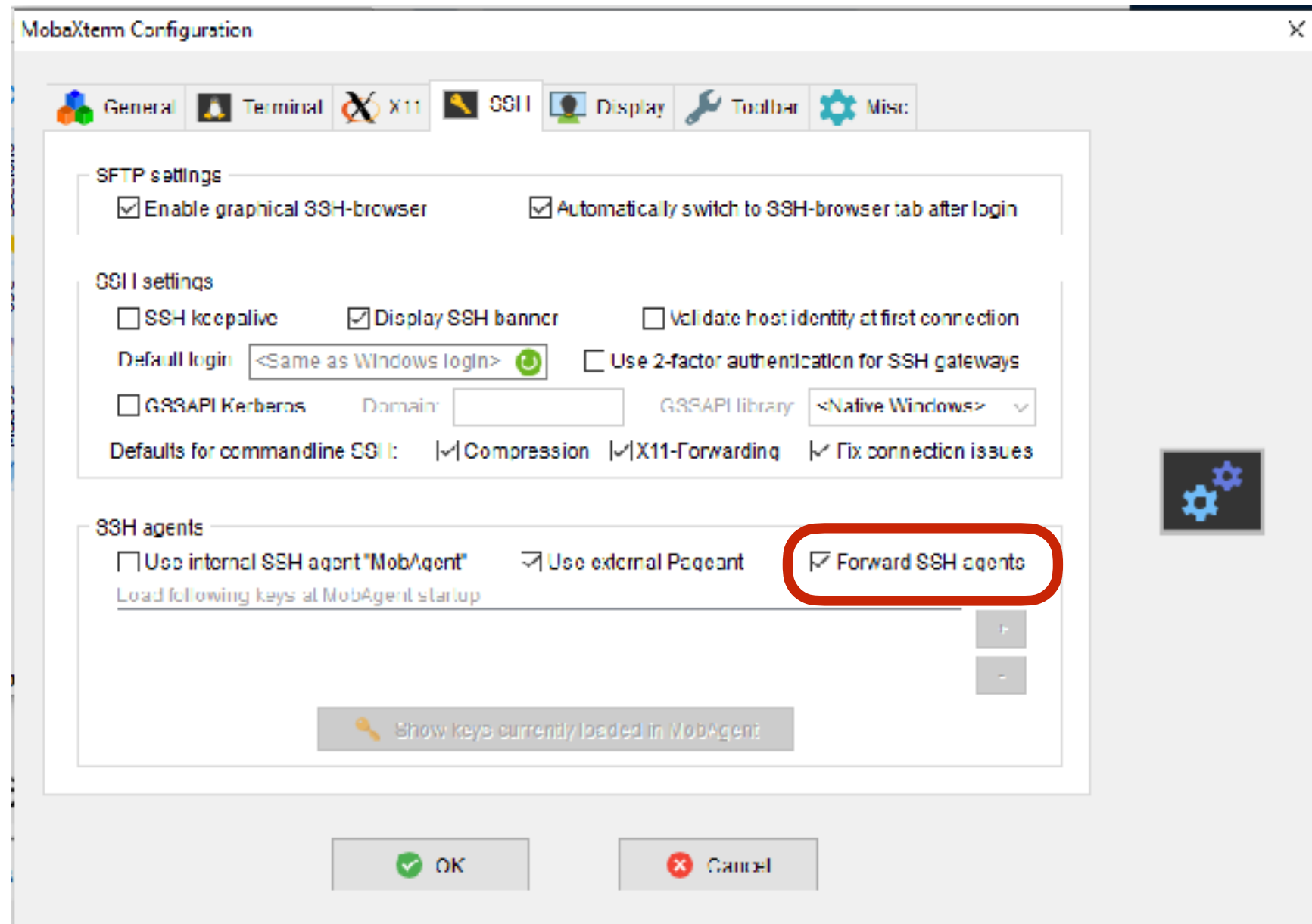
Message forward to laptop

Key provided

Connection granted

Forward Agent

- In order to connect from one machine to another (file transfer for example) Check that “forward ssh agents” is activated



- For large file use /CECI/trsf between CECI cluster