SECURE SHELL

Connecting to a lab machine

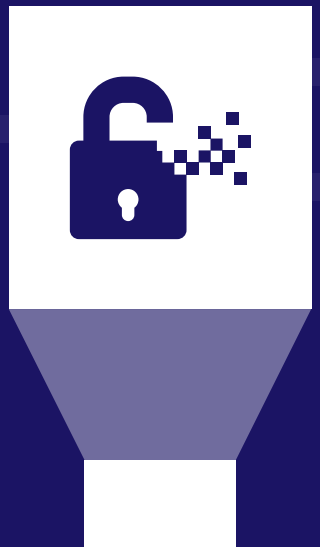
LAYERS OF CONNECTION

You

You start the connection process with SSH

Seis

Exists for security, and place to store SSH keys



Lab Machine

Load balancer allocates machine

THIS SESSION

01

Connect to lab machine

02

Set up SSH keys

03

Set up config file

04

Test connection

01

Open your terminals

Normal Connection

At each stage of logging in (Seis and lab machine), check for the '.ssh' folder with 'ls -a'. If the folder does not exist, create it with 'mkdir ~/.ssh'

usr/passwd

Connecting to lab machines using username and password

Your machine

Type ssh USERNAME@seis.bris.ac.uk

Seis

Type ssh rd-mvb-linuxlab.bristol.ac.uk

Lab Machine

Prompt should start with USERNAME@it######:~$

Exit

Type exit to return to your own machine

02

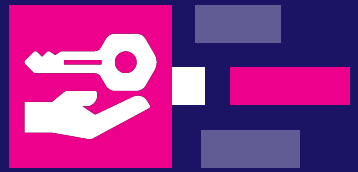
Setting up keys

THERE ARE TWO TYPES OF KEYS

Private key

In a file normally named id_CIPHER where CIPHER is the cipher in use. You need to keep this secure and only store it in places that only you have access to.

Public Key



in a file normally named id_CIPHER.pub. You can share this with the world, and you will need to store a copy of it on any machine or with any service that you want to log in to

KEYS FOR SEIS

KeyGen

ssh-keygen -t ed25519

Upload

scp <INSERT PATH TO ed25519.pub> "USERNAME@seis.bris.ac.uk:~/.ssh/"

Login

ssh USERNAME@seis.bris.ac.uk

Authorize

1. cd .ssh
2. cat id_ed25519.pub >> authorized_keys
3. chmod 600 authorized_keys

Exit

Type exit and return to your terminal

Test

ssh USERNAME@seis.bris.ac.uk
(shouldn't need password)

KEYS FOR LAB MACHINE

Seis

ssh USERNAME@seis.bris.ac.uk

Copy Key

scp ~/.ssh/id_ed25519.pub "rd-mvb-linuxlab.bristol.ac.uk:~/.ssh/"

Login

ssh rd-mvb-linuxlab.bristol.ac.uk

Authorize

1. cd .ssh
2. cat id_ed25519.pub >> authorized_keys
3. chmod 600 authorized_keys

Exit

Type exit twice and return to your terminal

Test

ssh -A -J USERNAME@seis.bris.ac.uk USERNAME@rd-mvb-linuxlab.bristol.ac.uk (shouldn't need password)

03

Configuration File

MAKING THINGS EASIER

```
ssh -A -J USERNAME@seis.bris.ac.uk USERNAME@rd-mvb-linuxlab.bristol.ac.uk
```

You now have a login command that works, but you still have to type a lot, and you need to type your username twice. We can improve this by using a configuration file.

CONFIGURATION FILE

Create File

On your machine:
cd ~/.ssh
touch config
Copy text to file
(replace USERNAME)

```
Host seis
  HostName seis.bris.ac.uk
  User USERNAME

Host lab
  HostName rd-mvb-linuxlab.bristol.ac.uk
  ProxyJump seis
  User USERNAME
```

04

Test Connection

“ssh lab”

From now on, this command will log you into the lab machines.

EXTRA DISCUSSION

- What is a **benefit** of using SSH keys?
- Other than connecting to a lab machine, where else might you **use** SSH keys?
- In what scenario would the **security** of your SSH keys be compromised?
- What is the **purpose** of the configuration file?
- What was the **name** of the encryption standard we used?

END