Land DA System Training

Connecting to an HPC Environment on Windows

By: Kristopher Booker, Gillian Petro, Edward Snyder

Introduction to SSH

- A **S**ecure **SH**ell (SSH) tunnel creates an encrypted connection between two computer systems. This allows users to:
  - Access and use a remote system via the command line on their local machine.
  - Transfer data securely between two systems.
- Many HPC platforms are accessed via SSH from a user’s computer.
  - NOAA RDHPCS
  - Academic HPCs
  - Commercial cloud platforms (e.g., AWS EC2s)

Introduction to SSH

- To use key-based authentication, you first need to generate public/private key pairs for your client. You can use **`ssh-keygen.exe`** to generate key files, and you can specify the following key-generation algorithms:
  - Digital Signature Algorithm (DSA)
  - Rivest–Shamir–Adleman (RSA)
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Ed25519
- To see the available options, run the **`ssh-keygen`** command with the **`-t`** flag
- ed25519 is the default algorithm. A strong algorithm and key length should be used, such as ECDSA.

Generate public/private key pair

- Open the PowerShell or Command Prompt application
- To generate key files using the ECDSA algorithm, run the following command in a PowerShell or Command Prompt window:

```
ssh-keygen -t ecdsa
```

- The output from the command should look like the following lines except that username is replaced with your username:

```
Generating public/private ecdsa key pair.
Enter file in which to save the key (C:\Users\username/.ssh/id_ecdsa):
```

- To accept the default file path, select **`Enter`** ; otherwise, specify a path or file name for your generated keys.

Generate public/private key pair

- Next, you will be prompted to use a passphrase to encrypt your private key files. Leave the passphrase empty by pressing **`Enter`** twice:

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
C:\Users\username/.ssh/id_ecdsa.
Your public key has been saved in
C:\Users\username/.ssh/id_ecdsa.pub.
```

Generate public/private key pair

- This should generate a public/private key pair in the directory you selected (default or other).

```
The key fingerprint is:
SHA256:OIzc1yE7joL2Bzy8!gS0j8eGK7bYaH1FmF3sDuMeSj8 username@LOCAL-HOSTNAME

The key's randomart image is:
+--[ECDSA 256]--+
|        .        |
|         o       |
|    . + + .      |
|   o B * = .     |
|   o= B S .      |
|   .=B O o       |
|  + =+% o        |
| *oo.O.E         |
|+.o+=o. .        |
+----[SHA256]-----+
```

Generate public/private key pair

- Now you have a public/private ECDSA key pair in the specified location. The **`.pub`** file is the public key, and the file without an extension is the private key:
- Use a text editor of your choice to view the public key file or view it in the command line:

```
type /Users/<username>/.ssh/id_ed25519_student(n).pub
```

- Copy-paste the public key contents to the workshop administrator via the Slack workspace channel **`#cadre-epic-data-assimilation-training`** and inform them of your student number (i.e., student 5).

Generate public/private key pair

- NOTE: Two (2) keys are generated: a public and a private key. **DO NOT SEND THE PRIVATE KEY!** A **public key** will end in `.pub` and will start something like this:

  ```
  ecdsa-sha2-nistp256 AAAAA
  ```

- And a **private key** will look like this:

  ```
  -----BEGIN OPENSSH PRIVATE KEY-----
  AAAAAAAAABAAAA
  11111111==
  -----END OPENSSH PRIVATE KEY-----
  ```

- Workshop administrators will add the public key to the authorization file on the bastion host, which will allow you to log in.

Connecting to an HPC Environment

- Ensure that the Windows SSH client (OpenSSH) is installed and configured. Information on how to perform this task can be found here:

  https://learn.microsoft.com/en-us/windows/terminal/tutorials/ssh

- Access the HPC environment using Windows Powershell or Command Prompt through the bastion host proxy by issuing the command below:

  ```
  ssh -i C:\Users\<User>/.ssh/id_ecdsa student(n)@137.75.93.46
  ```

  where `C:\Users\<User>/.ssh/` is replaced with the path to the `id_ecdsa` file on the user's system.

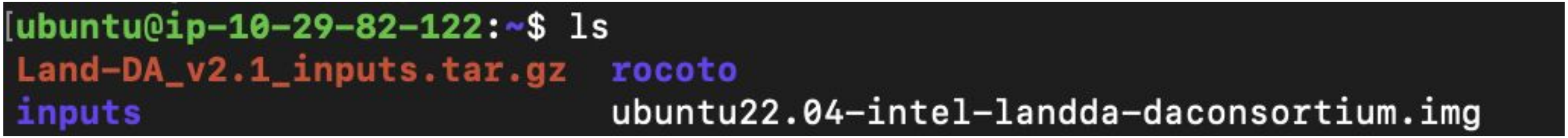
- **NOTE:** This will only work during the training when the HPC system is active for the training!

Connecting to an HPC Environment

- The user may see a message asking whether the user wants to continue connecting.
- Verify that you are connecting to the correct system and enter `yes` to continue.

Connecting to an HPC Environment

- This should automatically redirect users through the bastion proxy to the controller node of their HPC environment.
- If you run the **`ls`** command, you will see the Land DA container (**`.img`**) file, the **`inputs`** data directory, and a **`rocoto`** directory:



```
[ubuntu@ip-10-29-82-122:~$ ls
Land-DA_v2.1_inputs.tar.gz  rocoto
inputs                      ubuntu22.04-intel-landda-daconsortium.img
```