Guia del usuario cluster "Pirayu" CIMEC

Centro de Computos del CIMEC (C3)
Centro de Investigación de Métodos Computacionales
Universidad Nacional del Litoral / CONICET
Santa Fe - Argentina

2018

1. Introducción

El presente documento está dirigido para los usuarios que ya poseen una cuenta en el cluster `pirayu` e intenta ser una breve guía para el uso recomendado de aplicaciones HPC (High Performance Computting) en el mismo.
Para aquellos que aún no tengan una cuenta, dirigirse a este enlace y seguir los pasos allí descriptos.

2. Acceso

El acceso al cluster `pirayu` se realiza mediante el protocolo SSH (Secure SHell).
De ahora en adelante supondremos que el nombre de usuario otorgado por el C3 es `user`.

- Acceso desde cliente Linux:
  - Desde la red CCT Santa Fe CONICET (mediante dirección IP Privada):

    ```
    $ ssh user@172.16.254.100
    ```

  - Desde fuera de la red CCT Santa Fe CONICET (mediante dirección IP Pública):

    ```
    $ ssh -p 9015 user@200.9.237.240
    ```

- Acceso desde cliente Windows:
  Para acceder mediante máquinas Windows, debe utilizarse el programa `PuTTY` que puede descargarse de su web.
  Importante: descargar el paquete msi, como lo muestra la siguiente imagen para la versión 0.67, ya que instalará todos los programas necesarios (PuttySCP, PuttySFTP y PuttyGen).

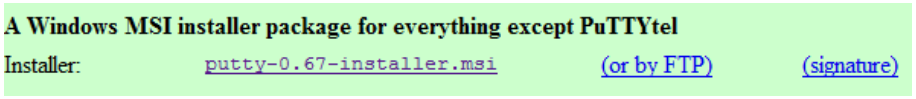
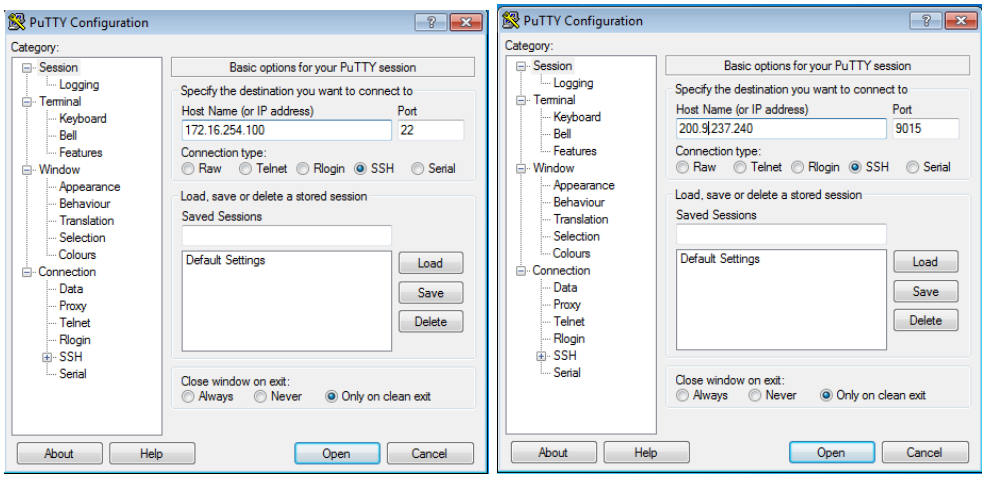


Figura 1: Link para descarga de PuTTY

- Desde la red CCT Santa Fe CONICET (mediante dirección IP Privada):
  Debe completarse el campo Host Name (or IP Address) con el valor `172.16.254.100`.
- Desde fuera de la red CCT Santa Fe CONICET (mediante dirección IP Pública):
  Deben completarse los campos Host Name (or IP Address) con el valor `200.9.237.240` y Port con el valor `9015`.

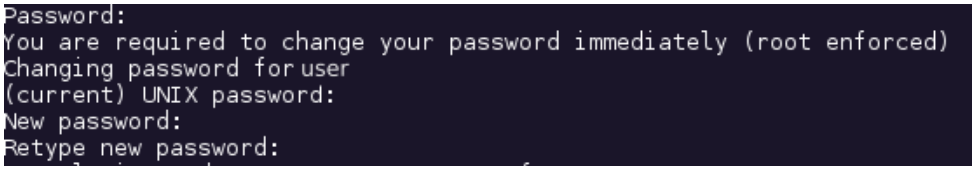
Figura 2: Configuración de PuTTY



(a) Desde la red CCT (b) Desde fuera de la red CCT

Una vez que se ha ingresado al servidor, se pedirá la contraseña brindada por los administradores de C3. Esta contraseña es válida únicamente para el primer acceso. Luego se verá obligado a cambiarla ingresando una vez la contraseña "actual" y 2 veces la contraseña "nueva" (a modo de confirmación), como lo muestra la imagen:

Figura 3: Cambio de contraseña en el primer ingreso



3. Acceso mediante clave pública

En el caso que el usuario esté utilizando un ordenador seguro (en su lugar de trabajo o en su hogar) se puede copiar la clave pública generada en ese ordenador al cluster para ingresar sin tener que tipear la contraseña.

Para ello se deben seguir los siguiente pasos:

- Cliente Linux:

  1. En su computadora personal ingrese:

```
ssh-keygen
Generating public/private rsa key pair.
```

2. A continuación el keygen requerirá un lugar donde guardar la clave (generalmente en `$HOME/.ssh`. Deje el valor por defecto y presione ENTER.

   ```
   Enter file in which to save the key (/home/user/.ssh/id_rsa):
   ```

3. Luego se pedirá una palabra clave, déjela en blanco presionando ENTER

   ```
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   ```

4. `ssh-keygen` muestra la ubicación de la clave privada (`id_rsa`) y la pública (`id_rsa.pub`)

   ```
   Your identification has been saved in /home/user/.ssh/id_rsa.
   Your public key has been saved in /home/user/.ssh/id_rsa.pub.
   The key fingerprint is:
   0e:4f:22:05:66:f0:23:9f:6a:fa:20:9a:9a:fa:40:6e user@casa
   The key's randomart image is:
   +--[ RSA 2048]----+
   |  ..+            |
   |   + .           |
   |  . o .          |
   |   o +           |
   | .  + o S        |
   |o  . . *         |
   |+Eo    o         |
   |+B               |
   |Xoo              |
   +-----------------+
   ```

5. Agregue la clave pública `id_rsa.pub` a su archivo de claves conocidas en el servidor:

   ```
   cat ~/.ssh/id_rsa.pub | ssh user@172.16.254.100 "cat >> ~/.ssh/authorized_keys"
   ```

6. Deberá ingresar la contraseña para conectarse al servidor (la IP del servidor en este ejemplo es la que se utiliza desde la red CCT):

   ```
   user@172.16.254.100's password:
   ```

7. De ahora en adelante cada vez que se ingrese al servidor mediante `ssh user@172.16.254.100` desde el ordenador donde generó la clave pública, no tendrá que ingresar contraseña.

- Para clientes Windows:

1. Lo primero será generar la clave pública mediante el programa PuTTYgen:

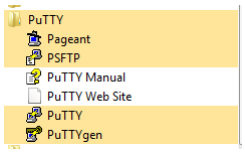


Figura 4: El programa PuTTYgen

2. Una vez en el programa, debemos generar la clave mediante el botón Generate.

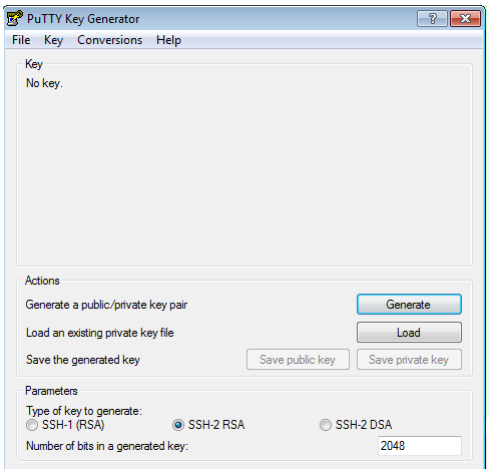


Figura 5: Generación de clave pública

3. Una vez generada la clave, se debe seleccionar y copiar al clipboard con Ctrl+C.

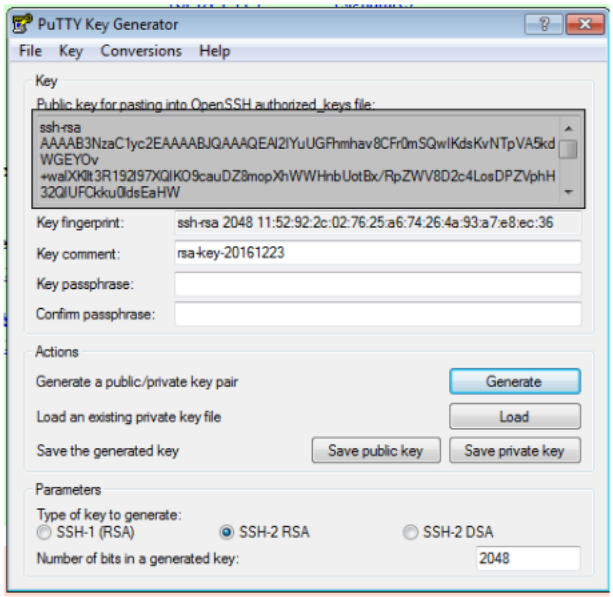


Figura 6: Clave pública generada

4. Ahora, mediante Putty (como se explicó previamente) ingresamos al servidor con nuestra cuenta e intentamos ingresar al directorio oculto .ssh y cambiamos los permisos del mismo:

```
cd ~/.ssh
chmod 0700 ~/.ssh
```

5. Si el mismo no existe, debemos crearlo:

```
mkdir ~/.ssh
```

6. Finalmente (si no existiese previamente) debemos crear el archivo `authorized_keys` y copiar allí la clave anteriormente creada.

   ```
   nano ~/.ssh/authorized_keys
   chmod 0644 ~/.ssh/authorized_keys
   ```

7. Item, una vez editado/creado el archivo `authorized_keys` lo guardamos con Ctrl+o y cerramos con Ctrl+x.
8. Si volvemos a loguearnos dentro del servidor desde el ordenador donde se creo la clave pública, entonces no se necesitará ingresar contraseña.

4. Configuración del cluster

El cluster `pirayu` posee 37 nodos de computo, configurados de la siguiente manera:

- compute-0-[0-23] : Nodos de cálculo Xeon 2650v3, 128 GB RAM, 20 cores
- compute-0-[24-28] : Nodos de cálculo Xeon 2650v3, 128 GB RAM, 20 cores + Placa GPU nVidia K40
- compute-0-[29-35] : Nodos de cálculo Xeon 2650v4, 128 GB RAM, 24 cores
- phihost : Nodo de cálculo Xeon 2650v3, 128 GB RAM + Placa Xeon Phi 7120P

Estos nodos están conectados mediante red Infiniband FDR (56 Gbps).

Para mayor información respecto del equipamiento del cluster, ver en este enlace.

5. Directorio personal

En `pirayu` el directorio personal esta ubicado en `/home/user` y cuenta con una cuota de disco de 8GB.
En el mismo directorio personal de cada usuario se encuentra el directorio `storage` que permite almacenar en el NAS mediante red Infiniband (56 Gbps) y con una cuota por usuario de 400 GB.
Si desea incrementar la cuota de disco, comunicarse con los administradores de C3 quienes analizaran la disponibilidad de recursos.

6. Instalación de aplicaciones

Todo usuario puede instalar sus aplicaciones en su directorio personal, si es que lo desea. En ese caso el usuario el personal del C3 no se hará responsable del rendimiento de la aplicación instalada.
También se puede requerir que los administradores del C3 se encarguen de realizar la configuración e instalación del código en la carpeta personal.
En el caso que el programa a instalar sea usado por más de un usuario del cluster, se debe requerir que el mismo sea instalado por el personal del C3 para que pueda ser compartido por más de un usuario.

7. Compiladores

El cluster cuenta con los siguientes compiladores y librerías instalados y preparados para el uso común en el cluster:

- GCC
- G++
- GFortran
- OpenMPI
- MVAPICH
- CUDA
- OpenBLAS

8. Modulos

Es posible cargar automáticamente el entorno de usuario para utilizar algunas librerías y/o compiladores específicos mediante la herramienta `module`.

- Para ver los módulos disponibles en el sistema:

```
[user@pirayu apps]# module avail


---------------------- /share/apps/modules ----------------------------------------------------
cuda    gcc-494 mvapich openmpi
```

- Para cargar un módulo al entorno de usuario (por ejemplo los compiladores de MVAPICH):

```
[user@pirayu apps]# module load mvapich
[user@pirayu apps]# which mpicc
/share/apps/mvapich/2.2/bin/mpicc
```

9. Ejecución de trabajos

Para enviar trabajos a los nodos de cálculo, el cluster utiliza el administrador de recursos SLURM.
SLURM permite enviar trabajos sin la necesidad de verificar si los nodos se encuentran con carga o no, encolando los trabajos de acuerdo a colas de prioridades.
Una guía completa del uso de SLURM se encuentra en el siguiente enlace.

10. Monitor Ganglia

El cluster posee un sistema de monitoreo de carga mediante el software Ganglia. Para visualizar la carga de CPU y memoria de los nodos del cluster se puede acceder mediante el siguiente enlace.

11. Copia de archivos entre cliente y servidor

Para copiar o mover los archivos desde el servidor a su ordenador personal puede utilizar varios protocolos: Para copiar archivos o directorios en clientes Linux, se pueden utilizar comandos desde la terminal o administradores de ficheros, algunos de ellos son

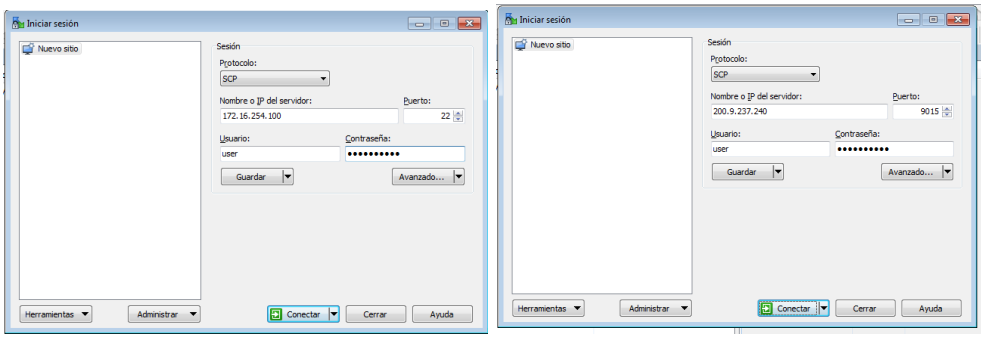
- `scp`: Secure Copy es un protocolo que permite copiar remotamente directorios y ficheros desde y hacía el servidor.
  Suponga que desea copiar el directorio `datos` ubicado en su ordenador personal a la carpeta personal de su usuario en el cluster:
  `scp -r /home/local_user/datos user@172.16.254.100:/home/user`

  Para hacer el paso inverso (desde el servidor a su ordernador personal):

  `scp -r user@172.16.254.100:/home/user/datos /home/local_user/`

- `Dolphin`: es un administrador de archivos basado en KDE, que permite una conexión segura mediante el protocolo `scp`. Si su escritorio no es KDE deberá instalarlo en su sistema operativo.
- `gnome-commander`: al igual que dolphin es un administrador de ficheros gráfico, pero basado en escritorios gnome, con lo cual debe ser instalado si el escritorio de su distribución no es gnome.
- `mc`: el Midnight Commander es una suite completa de administración y edición de archivos y ficheros que es ejecutado en una terminal sin necesidad de un entorno gráfico, lo cual lo hace muy flexible y completo.

En entornos Windows, se puede utilizar el programa WinSCP que posee un entorno gráfico para conexiones remotas en Windows. Esta aplicación es libre y gratuita:



(a) WinSCP en la red CCT (b) WinSCP desde afuera de la red CCT

Figura 7: WinSCP

12. Lista de usuarios HPC-CIMEC

Todo usuario habilitado por C3 para ingresar al cluster, automáticamente es agregado a la lista de correos HPC-CIMEC (hpc-cimec@googlegroups.com) en donde encontrará las últimas novedades sobre el uso del equipamiento: nuevos equipos, cortes programados, inconvenientes, etc.
También se puede utilizar la lista para enviar consultas grupales, compartir novedades y generar debates sobre HPC.

13. Cómo citar el cluster

Todo desarrollo científico-tecnológico generado con equipamiento del Consorcio Pirayu deberá incluir una referencia al mismo. A continuación un ejemplo de cómo citar el cluster `pirayu` en un paper o trabajo:

> *El presente trabajo utilizó recursos computacionales del cluster Pirayu, adquirido con fondos de la Agencia Santafesina de Ciencia, Tecnología e Innovación (ASACTEI), Gobierno de la Provincia de Santa Fe, mediante el Proyecto AC-00010-18, Resolución Nº 117/14. Este equipo forma parte del Sistema Nacional de Computación de Alto Desempeño del Min. Ciencia y Tecnología de la Rep. Argentina.*

14. Contacto

El cluster `pirayu` es administrado por el C3, sito en el Edificio CIMEC - Predio CONICET Santa Fe "Dr. Alberto Cassano" - Colectora Ruta Nac Nro 168, Km 0, Paraje El Pozo - (3000) Santa Fe - Argentina.

- Administración del sistema (Alejandro Dabin/Juan Pablo Dorsch): c3admin@santafe-conicet.gov.ar
- Lista usuarios de C3: hpc-cimec@googlegroups.com
- Teléfonos: +54-342-4511594/95 int 7025/7027
- Web C3: www.cimec.org.ar/c3
- Web Pirayu: www.cimec.org.ar/pirayu