Login ohne Passwort

Um die Arbeit mit dem Cluster zu erleichtern, kann es nützlich sein sich auf den Cluster ohne manuelle Passwort-Eingabe einzuloggen. Dies ist hilfreich wenn man automatisiert per SCP Dateien kopieren will oder ein Filesystem per sshfs mounten will.

Dazu muss zunächst ein SSH-Key auf ihrem lokalen Computer generiert werden und danach im Home-Verzeichnis auf dem Cluster gespeichert werden. Es wird empfohlen diese Datei mit einem Passphrase zu sichern, da sonst bei Diebstahl oder ähnlichem dem Angreifer der Zugang zum Cluster ermöglicht wird. Um diese Datei nicht immer wieder entsperren zu müssen, gibt es Tools wie ssh-agent, welche die entschlüsselte Datei sicher bereithalten bis zum nächsten Reboot.

Schritt für Schritt Anleitungen

SSH-Tools installieren

Sie müssen auf ihrem Computer die SSH-Client-Tools installieren. Dazu zählen die Tools ssh, ssh-keygen, ssh-copy-id.

Windows

Für Windows empfiehlt sich dazu das Programm PuTTY. Dort kann mit PuTTYGen ein neuer SSH-Key erstellt werden. Drücken Sie zunächst auf den Button "Generate" und danach sowohl auf "Save public key" als auch "Save private Key". Um den Key später auch unter Linux verwenden zu können, müssen Sie zusätzlich noch auf Conversions Export OpenSSH Key klicken und die Datei speichern. Zusätzlich wird ihnen eine Textbox mit dem Public-Key für OpenSSH angezeigt. Kopieren Sie diesen Text in die zwischenablage.

Linux und macOS

Unter diesen beiden Betriebssystemen sind die benötigten Tools meist schon installiert. Daher können Sie mit dem folgenden Befehl einen neuen SSH-Key erstellen:

```
ssh-keygen -t rsa -C "$USER@$HOSTNAME"
```

SSH-Key übertragen

Damit der Cluster weiß, welche SSH-Keys er akzeptieren soll, müssen diese in einer Datei eingetragen werden. Diese befindet sich in ~/.ssh /authorized_keys und beinhaltet für jeden Key eine Zeile. Löschen Sie nicht die bereits vorhandenen Keys, denn sonst können Sie keine Jobs mehr auf dem Cluster starten.

Windows

Verbinden Sie sich per SSH mit dem Cluster und öffnen Sie ein Textbearbeitungsprogramm wie nano oder vi um die Datei ~/.ssh/authorized_keys zu bearbeiten. Nun können Sie den Inhalt ihrer Zwischenablage an die Datei anhängen.

Linux und macOS

Es gibt ein kleines Hilfsprogramm namens ssh-copy-id um einen SSH-Key zu übertragen und in die Datei authorized_keys einzufügen. Bei diesem Vorgang werden Sie einmalig nach dem Passwort zu ihrer Kennung gefragt,

```
ssh-copy-id kennung@hpc.rz.uni-duesseldorf.de
```

Zugriffstest

Um zu testen ob der Login per SSH-Key nun klappt, können sie einmal versuchen sich per SSH zu verbinden. Sie sollten nun nicht mehr nach einem Passwort für ihre Kennung gefragt werden. Wenn Sie eine Passphrase für den SSH-Key angelegt haben, werden Sie gefragt ob sie den privaten Schlüssel entschlüsseln wollen.

SSH-Key nur einmal entschlüsseln

Um einen SSH-Key nur einmal pro Sitzung zu entschlüsseln gibt es das Tool ssh-agent, welches vor der ersten SSH-Verbindung gestartet wird. Dort werden die Schlüssel hineingeladen und stehen danach zur Verfügung.

Linux und macOS

Am einfachsten ist es, wenn sie folgende Zeilen in ihre .bashrc-Datei einfügen.

```
if [ -z "$SSH_AUTH_SOCK" ] ; then
  eval $(ssh-agent -s)
  ssh-add
fi
```

Danach sollten sie beim Starten einer neuen Shell nach der Passphrase gefragt werden und können danach ssh ohne weitere Fragen nach Passwörtern verwenden.