

<https://haydn2005.u-bourgogne.fr/dnum-ccub/spip.php?article978>

Connexion aux machines du centre de calcul

- Site Public -

Date de mise en ligne : jeudi 27 février 2014

Copyright © Site du Centre de Calcul de l'Université de Bourgogne - Tous
droits réservés

Sommaire

- [Connexion aux machines du centre de calcul](#)
- [1. Connexion avec SSH sous Linux et MacOS](#)
- [1.2. Modifier la clé d'hôte SSH sous Linux](#)
- [2. Connexion avec SSH sous Windows](#)
- [2.2. Modifier la clé d'hôte SSH avec Putty](#)
- [Se connecter sans taper son mot de passe](#)
- [1. Sous Linux / MacOS](#)
- [2. Sous Windows](#)

Connexion aux machines du centre de calcul

1. Connexion avec SSH sous Linux et MacOS

Pour se connecter à une machine du centre de calcul taper son nom d'utilisateur suivi de **ssh-ccub.u-bourgogne.fr**. Les connexions à ssh-ccub sont réparties sur les différentes machine interactives du cluster (les krenek).

Par exemple pour l'utilisateur *util05* :

```
ssh util05@ssh-ccub.u-bourgogne.fr
```

Un mot de passe de connexion est demandé.

Pour se déconnecter taper `exit` ou `ctrl+d`.

Remarques :

- Pour changer son mot de passe, il faut utiliser exclusivement la commande `yppasswd`. Le mot de passe sera mis à jour sur toutes les machines du *cluster* dans un délai de 30 minutes maximum.
- Sur Mac, l'application X11 (dans le dossier application) permet d'ouvrir un terminal (xterm).

Lors de la connexion les informations suivantes s'affichent dans le terminal (voir figure) :

- 1 : Connexion au centre de calcul.
- 2 : Machine sur laquelle la connexion a été effectuée.
- 3 : Le site du centre de calcul de l'université de Bourgogne.
- 4 : Rappel de sécurité et avertissement.
- 5 : Espace disque consommé sur le *cluster*, on voit bien les 3 volumes de stockage */user1*, */work* et */archive* abordés dans ["stockage et sauvegarde des données"](#), */tmp2* est un répertoire de fichiers temporaires.
- 6 : Statistiques des machines krenek01, krenek02 et krenek03
- 7 : Le temps de connexion sur la machine.

Remarque :

Le temps d'exécution des programmes est limité à 3 heures. Pour exécuter des travaux de longue durée, les systèmes de batch (voir ["Lancement des logiciels en batch"](#)) permettent d'outrepasser cette limite de temps.

```
$ ssh -X ssh -X util05@ssh-ccub.u-bourgogne.fr
util05@ssh-ccub.u-bourgogne.fr's password:
Last login: Fri Apr 10 09:01:47 2015 from huber.rp.u-bourgogne.fr
.....
DSI-Centre de Calcul uB, krenek01, CentOS Intel64 6.4
http://www.u-bourgogne.fr/DSI-CCUB
.....
L'accès à cette machine implique l'engagement de respect de la charte du
Bon Usage des Ressources Informatiques de l'Université de Bourgogne
.....
RAPPEL: le prêt de son compte ou de son mot de passe est prohibé
.....
AVERTISSEMENT
.....
Tout accès non autorisé à ce serveur vous expose à des poursuites
.....
Le vol de données, la corruption de données ou l'accès frauduleux à ce
serveur par des tentatives d'injection de codes, de scripts malveillants
ou par le biais de requêtes envoyées au serveur fera l'objet d'un dépôt
de plainte systématique par l'Université de Bourgogne et pourra aboutir
à des peines de prison de 3 à 5 ans et des amendes de 45000 à 75000 Euros.
(Art. 323.1, 323.2, 323.3 et 323.4 du Code Penal)
.....
.....
STATISTIQUES DES MACHINES INTERACTIVES
du lundi 13 avril 2015 à 08:48
.....
Machine | Utilisateur(s) | Charge en %
.....
krenek01 | 1 | 0
krenek02 | 1 | 0.25
krenek03 | 0 | 14.31
.....
Machine krenek01, temps cpu : 180 mn
mem totale : illinite
mem residente : illinite
.....
Espace disque consommés sur les différents volumes :
/user1/ccub/util05 5.7 / Inconnu Go ( 170959 / Inconnu fichiers)
/work/ccub/util05 2887.7 / 6144.00 Go ( 41918 / 1000000 fichiers)
/archive/ccub/util05 1.3 / 307.20 Go ( 11362 / 30000 fichiers)
/tmp2 0.0 / 20.00 Go ( 39 / 204800 fichiers)
.....
util05@krenek01 CentOS_Intel64_6.4 [/user1/ccub/util05]
$
```

1.2. Modifier la clé d'hôte SSH sous Linux

La clé d'hôte SSH du cluster de calcul est enregistrée par votre client SSH sur votre poste de travail. Il ne s'agit pas de la clé utilisée pour authentifier l'utilisateur. Si la clé est renouvelée côté serveur, il faudra la supprimer côté client et enregistrer la nouvelle clé.

Pour supprimer l'ancienne clé, utiliser la commande `ssh-keygen` ou éditer manuellement le fichier

`~/.ssh/known_hosts` :

```
ssh-keygen -R ssh-ccub.u-bourgogne.fr
```

Une fois la clé supprimée, il vous suffit d'établir une nouvelle connexion et répondre "oui" pour ajouter la nouvelle clé.

Le client SSH peut afficher le "fingerprint" de la nouvelle clé, voici les empreintes des différentes clés utilisées sur le cluster actuellement (juillet 2020) :

```
# format MD5
bb:ee:1b:2e:3e:48:22:a9:01:af:92:f2:13:30:72:fd ssh-ccub.u-bourgogne.fr (DSA)
ff:a2:dc:30:b9:de:b8:48:dc:4d:76:9b:87:e1:fb:7c ssh-ccub.u-bourgogne.fr (ECDSA)
26:48:16:86:6f:7d:5e:e4:00:ab:c7:12:6d:8b:0e:7c ssh-ccub.u-bourgogne.fr (ED25519)
d7:b2:ec:0a:d6:b6:2f:80:e9:86:98:0b:85:f2:c2:42 ssh-ccub.u-bourgogne.fr (RSA)

# format SHA256
E0m00qt4xuRiKagt3gylWK2oDs4yCH0/rvCTyDrukz4 ssh-ccub.u-bourgogne.fr (DSA)
IRHsB/YMpI01jDgWHj7iH0W4iFuQmxeqrphX8+Gb9Ug ssh-ccub.u-bourgogne.fr (ECDSA)
CuUTR3s0zsa4lvUEpDHjZj+n06XGzTD1mIuPWVqDaII ssh-ccub.u-bourgogne.fr (ED25519)
v3EYHPigkQktBeIBK46bJH/rk33IjjK0TjZkQbS2ZjA ssh-ccub.u-bourgogne.fr (RSA)
```

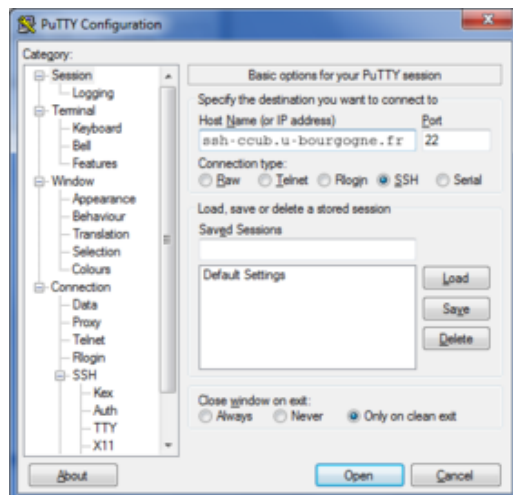
â€Œ 2. Connexion avec SSH sous Windows

► Télécharger [Putty](#).

Lancer putty :

► dans le menu **Session**

- - Host Name : **ssh-ccub.u-bourgogne.fr**
 - Port : **22**
 - Connection type : **SSH**
 - puis cliquer sur : **Open**

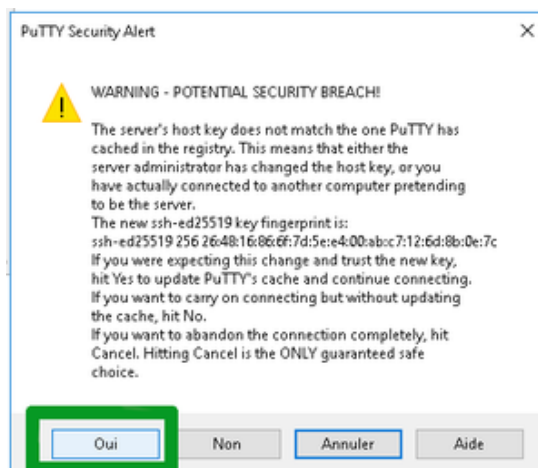


- ▶ entrez votre login
- ▶ entrez votre mot de passe

â€Œ 2.2. Modifier la clé d'hôte SSH avec Putty

La clé d'hôte SSH du cluster de calcul est enregistrée par votre client SSH sur votre poste de travail. Il ne s'agit pas de la clé utilisée pour authentifier l'utilisateur. Si la clé est renouvelée côté serveur, il faudra la supprimer côté client et enregistrer la nouvelle clé.

Si la clé d'hôte a été modifiée, Putty va vous le signaler et vous proposer de la mettre à jour lors de la connexion, il suffit de répondre "Oui" :



Le client SSH peut afficher le "fingerprint" de la nouvelle clé, voici les empreintes des différentes clés utilisées sur le cluster actuellement (juillet 2020) :

format MD5

bb:ee:1b:2e:3e:48:22:a9:01:af:92:f2:13:30:72:fd ssh-ccub.u-bourgogne.fr (DSA)

ff:a2:dc:30:b9:de:b8:48:dc:4d:76:9b:87:e1:fb:7c ssh-ccub.u-bourgogne.fr (ECDSA)

```
26:48:16:86:6f:7d:5e:e4:00:ab:c7:12:6d:8b:0e:7c ssh-ccub.u-bourgogne.fr (ED25519)
d7:b2:ec:0a:d6:b6:2f:80:e9:86:98:0b:85:f2:c2:42 ssh-ccub.u-bourgogne.fr (RSA)

# format SHA256
E0m00qt4xuRiKaqt3gyLWK2oDs4yCH0/rVCTyDrukz4 ssh-ccub.u-bourgogne.fr (DSA)
IRHSB/YMpI01jDgWHj7iH0W4iFuQmxeqrphX8+Gb9Ug ssh-ccub.u-bourgogne.fr (ECDSA)
CuUTR3s0zsa4lvUEpDHjZj+n06XGzTD1mIuPWVqDaII ssh-ccub.u-bourgogne.fr (ED25519)
v3EYHPigkQktBeIBK46bJH/rk33Ijjk0TjZkQbS2ZjA ssh-ccub.u-bourgogne.fr (RSA)
```

Se connecter sans taper son mot de passe

1. Sous Linux / MacOS

Pour se connecter à une machine du centre sans avoir à taper le mot de passe il faut :

- Générer une clé publique en tapant dans le terminal de votre ordinateur :

```
cd ~/.ssh
ssh-keygen -t rsa
```

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/nom/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nom/.ssh/id_rsa.
Your public key has been saved in /home/nom/.ssh/id_rsa.pub.
The key fingerprint is:
ab:10:6f:f5:60:f2:fe:tr:ab:3c:58:cb:32:31:fe:1e
```

deux fichiers vont être générés la clé publique `id_rsa.pub` et la clé privée `id_rsa`

- Se connecter à une machine du centre de calcul

- ▶ Ouvrir le fichier `~/.ssh/authorized_keys`

```
nedit ~/.ssh/authorized_keys
```

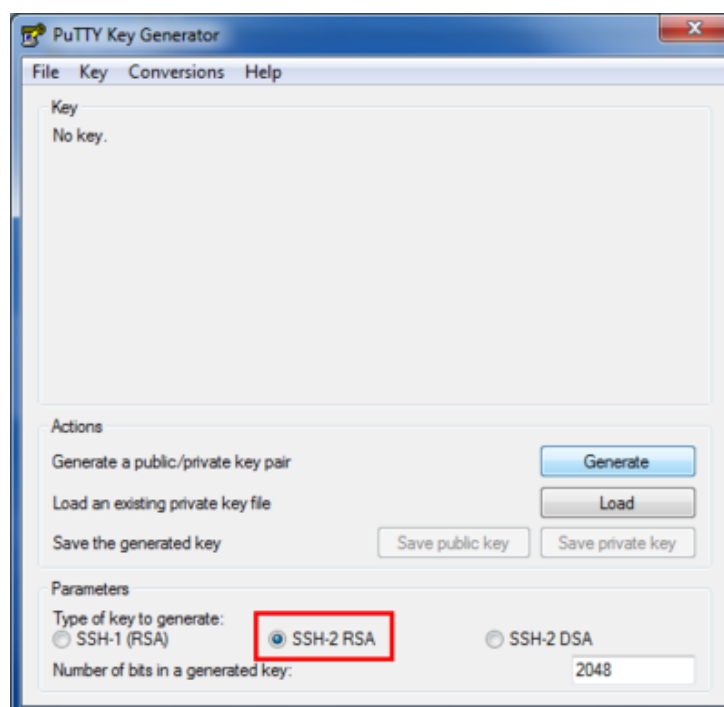
- ▶ Copier le contenu de la clé publique `id_rsa.pub` de votre ordinateur à la fin du fichier `~/.ssh/authorized_keys` de votre machine de connexion.

Vous pouvez maintenant vous connecter sans avoir à taper votre mot de passe.

â€f 2. Sous Windows

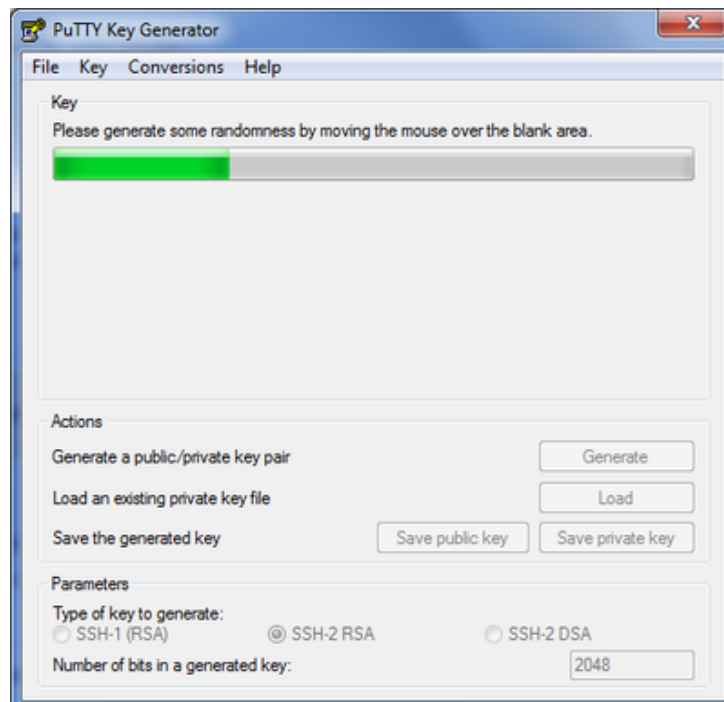
- ▶ Générer une clé publique

** Pour générer une clé publique il faut utiliser [PuttyGen](#)



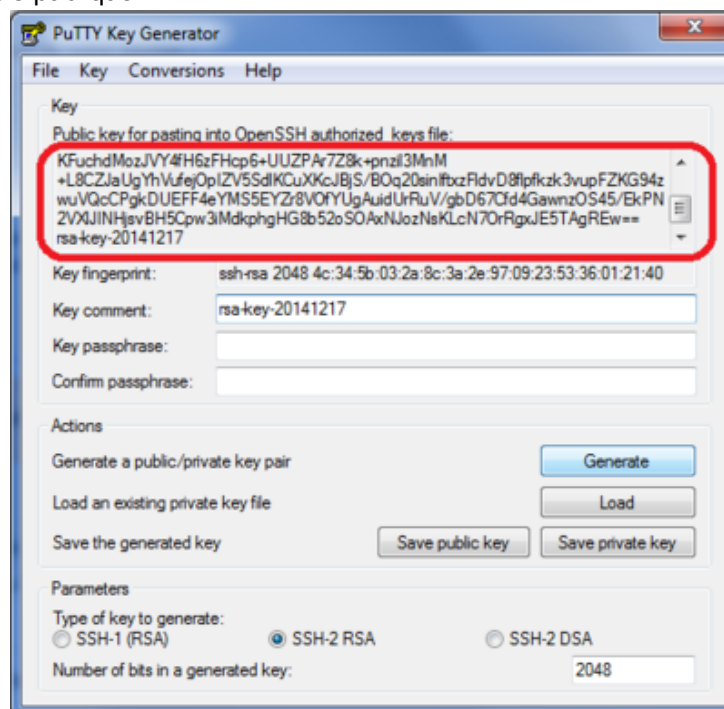
** Vérifier que SSH-2 RSA est bien coché

** Cliquer sur Generate et bouger la souris (si la souris arrête de bouger le chargement s'arrête)



** Enregistrer la clé privée sur votre ordinateur en cliquant sur "save private key"

** Copier le contenu de la clé publique



** Se connecter à une machine du centre de calcul

** Ouvrir le fichier `~/.ssh/authorized_keys` en tapant :

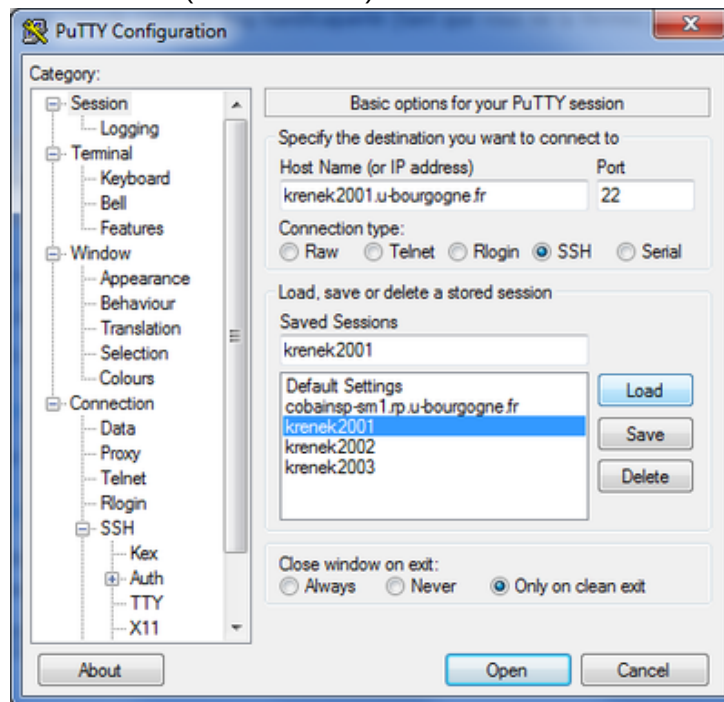
```
ncedit ~/.ssh/authorized_keys
```


coller la clé publique à la fin du fichier

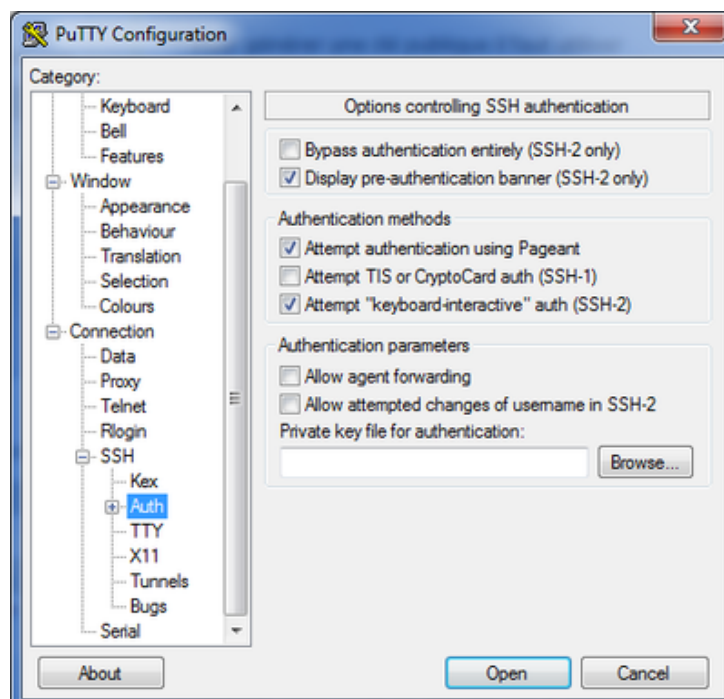
► Associer la clef privée au profil de Putty

** Ouvrir Putty

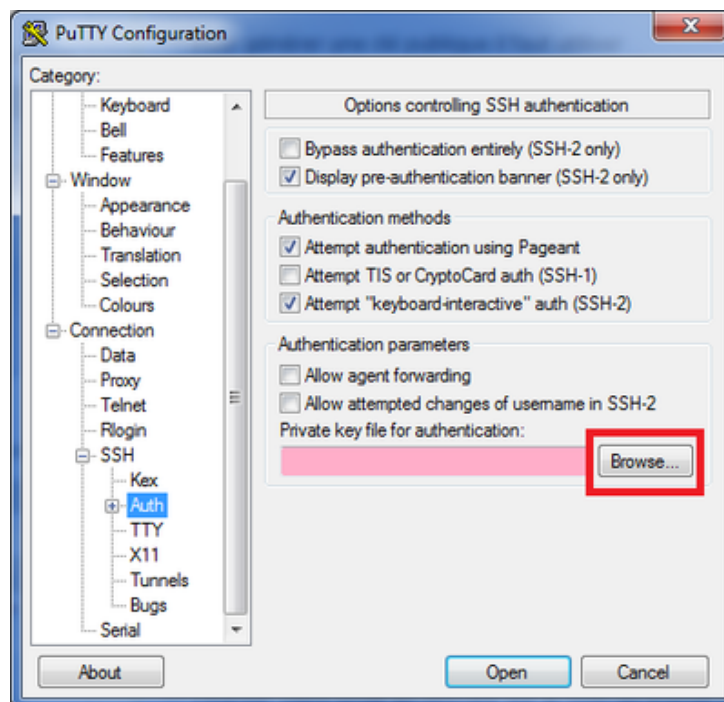
** Charger un profil en cliquant sur le nom (ici krenek2001) ensuite load



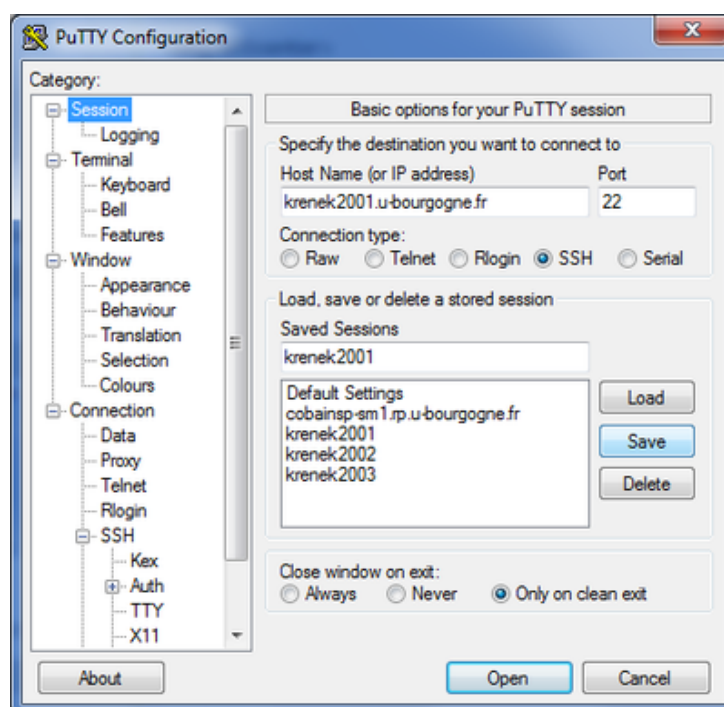
** Dans le menu de gauche, cliquer sur Auth (connexion -> SSH -> Auth)



** Charger la clé privée enregistrée sur l'ordinateur en cliquant sur "Browse..."



** Cliquer sur "Session" dans le menu de gauche puis "Save"



Vous pouvez maintenant vous connectez sans taper votre mot de passe.