Utilisation du bastion ssh

Objet et contexte:

Le but du bastion ssh est d'offrir un accès en ssh de l'extérieur de l'établissement sur une machine publique de l'université. A partir de celle-ci (le bastion), l'accès en ssh vers des serveurs internes prédéfinis est autorisé. Cette documentation s'adresse principalement aux utilisateurs ayant besoin, à partir de l'extérieur, d'un accès en ligne de commande sur un serveur de type unix/linux.

Schéma de principe :

Le principe est simple. Depuis un poste client, n'importe où dans le monde, vous vous connectez en ssh sur frontal-ssh.univ-reunion.fr sur le port ssh par défaut (22). Pour des questions de sécurité, seule l'authentification par clés est autorisée. Une fois connecté au bastion ssh, vous pouvez vous servir de cette machine comme rebond vers des serveurs internes à l'université.

Préparation de votre clé publique :

Sous linux et MacOS X :

Vous devez lancer la génération de vos clés publiques et privées. Tout se fait de manière très simple en ligne de commande. En gras apparaissent les commandes à taper, en bleu les commentaires sur ce que vous devez faire :

```
slinger:~ matt$ ssh-keygen -d
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/matt/.ssh/id_dsa):
Appuyez sur entrée pour valider le chemin proposé
Enter passphrase (empty for no passphrase):
La passphrase est l'équivalent d'un mot de passe, donc une suite de caractères dont vous devrez vous souvenir. Comme tout mot de passe, vous devez le retaper une deuxième fois pour validation. Ce mot de passe est associé à la clé et est totalement indépendant du mot de passe de votre compte sur le serveur distant.
Enter same passphrase again:
Your identification has been saved in /Users/matt/.ssh/id_dsa.
Your public key has been saved in /Users/matt/.ssh/id_dsa.pub.
The key fingerprint is:
9e:4b:28:89:23:58:31:9d:1e:a7:d3:7a:10:ae:9b:0c matt@slinger.local
```

A partir de là, votre clé publique est stockée dans le fichier ~/.ssh/id_dsa.pub. Pour afficher votre clé publique, vous pouvez faire :

```
slinger:~ matt$ cat ~/.ssh/id_dsa.pub
```

Attention, en aucun cas vous ne devez communiquer votre clé privée à qui que ce soit. Elle est aussi confidentielle que le code de votre carte bancaire.

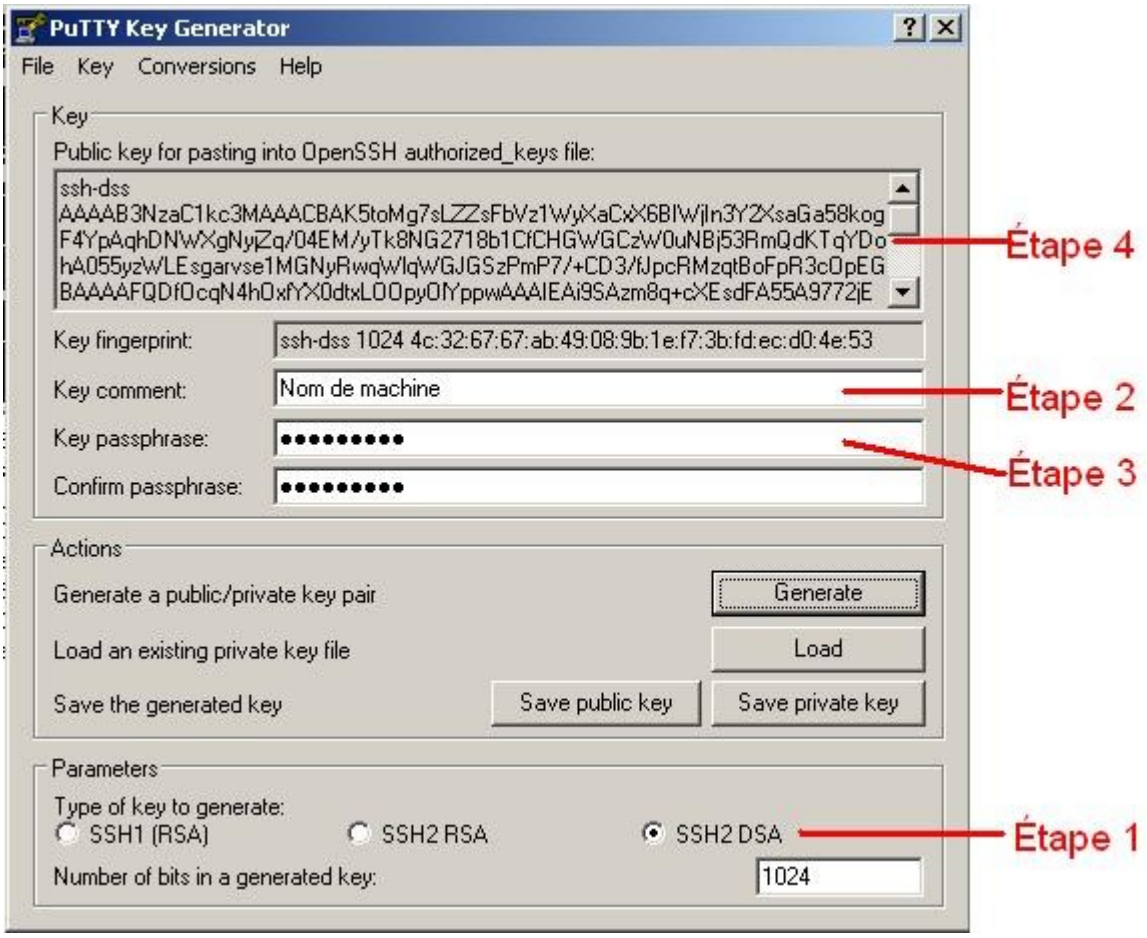
Depuis Windows :

Tout va se faire à partir de **putty** (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

En marge de ce produit, l'outil **puttygen** est mis à disposition afin de générer des paires de clés.

1. lancez **puttygen**
2. Activez la case "SSH2 DSA"(Étape 1)
3. Cliquez sur le bouton "Generate"
4. Bougez la souris dans le cadre gris « Key » pour générer les clés au hasard
5. Entrer un commentaire, quelque chose qui identifie la machine, **username@machine** par exemple (Étape 2)
6. Entrez un mot de passe. Ce mot de passe est associé à la clé et est totalement indépendant

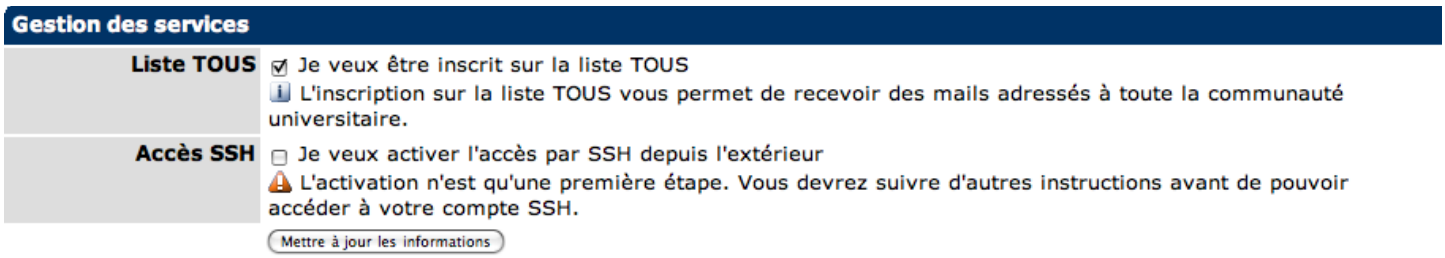
du mot de passe de votre compte sur le serveur distant. (Étape 3)
7. Cliquez sur "Save private key" et faites l'enregistrement au nom de **id_dsa.ppk** dans **C:\Documents and settings\username\Application Data\Putty.** (remplacer username par votre nom d'utilsateur windows)
8. faites un copier du texte de l'encadré « "Public key to paste into OpenSSH ..." (Étape 4) »
9. Collez ce texte dans Notepad
10. enregistrez le fichier au format ANSI dans le même dossier au nom de **id_dsa_win.pub** (pas d'extension .txt)
11. Fermez puttygen et Notepad



Demande de création du compte

Cette partie doit se faire obligatoirement depuis l'intranet de l'université. Pour cela, à partir de votre navigateur web, aller à la page https://moncompte.univ.run/, connectez vous avec votre identifiant et votre mot de passe de mail.

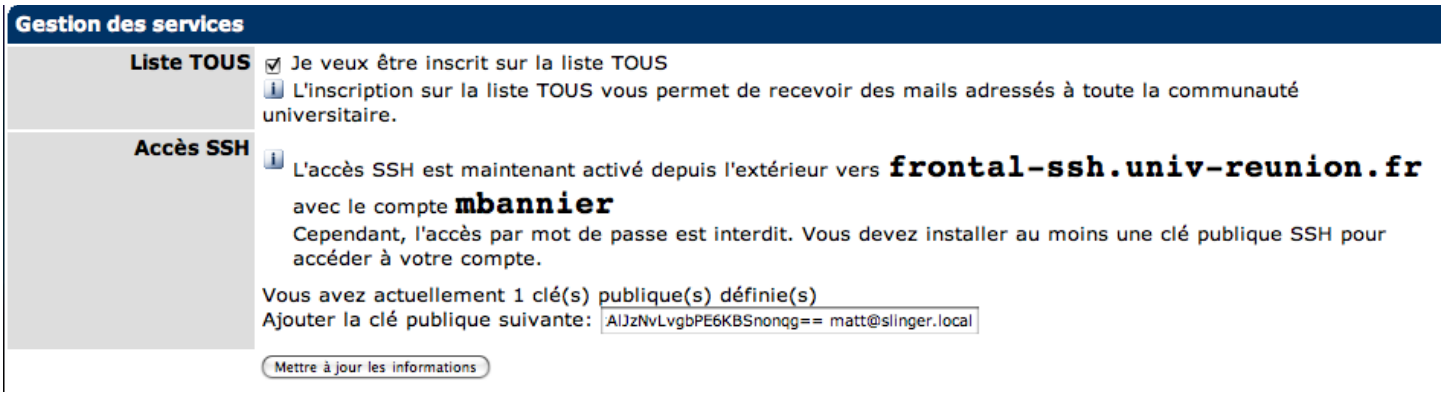
Dans la rubrique « Gestion des services », cochez la case « activation de ssh », puis sur le bouton « mettre à jour les informations ».



La partie « gestion de services » permet maintenant de saisir une clé publique à la fois. Il est

possible d'en renseigner plusieurs.

Copiez votre **clé publique** dans le cadre prévu à cet effet et cliquez sur le bouton « mettre à jour les informations ».



Votre accès ssh à la machine frontal-ssh.univ-reunion.fr sera utilisable 15 minutes après avoir validé votre demande.

Utilisation du service

15 minutes après avoir validé votre compte, vous pouvez vous connecter sur frontal-ssh.univ-reunion.fr avec votre client ssh habituel (sur le port 22 qui est le port ssh par défaut).
Si vous utilisez Putty, n'oubliez pas d'indiquer le chemin de votre clé (dans notre exemple *C:\Documents and settings\username\Application Data\Putty) dans* Connection/SSH/Auth.
Une fois connecté sur la machine frontal-ssh, vous pouvez accéder à vos serveurs habituels (de laboratoire, centre de calcul) par ssh.

Utilisation par des personnes non référencées dans notre base de compte.

Ces personnes doivent envoyer un mail à bastion-support@univ-reunion.fr avec leur clé public et le nom d'utilisateur souhaité sur la machine frontal-ssh.univ-reunion.fr. A partir de ces informations, l'équipe en gestion du service se chargera de la création de l'accès et reprendra contact avec le demandeur une fois l'opération effectuer.

Astuces d'utilisation du bastion

Etant conscient que la mise en place de ce bastion peut modifier les habitudes prises par les utilisateurs, le CRI propose des astuces afin de rendre l'utilisation de ce frontal aussi transparente que possible.
Si vous désirez vous connecter en ligne de commande sur une machine tierce au sein de l'université, vous pouvez mettre en utiliser la commande suivante qui vous permettra d'obtenir un shell directement sur la machine tierce :

```
ssh -o "ProxyCommand ssh user@frontal-ssh.univ-reunion.fr nc -w 1 %h %p"
user@machine_tierce
```

De même si vous souhaitez faire une copie de fichier vers une machine de l'université de manière transparent, vous pouvez utiliser la commande suivante.

```
scp -o "ProxyCommand ssh user@frontal-ssh.univ-reunion.fr nc -w 1 %h %p 2>/dev/null"
source user@machine-finale:/destination/
```

Pour éviter cette longue ligne de commande, vous pouvez modifier le fichier ~/.ssh/config en y ajoutant la configuration suivante (par machine destination):

```
Host machine-finale
User user
HostName machine-finale
ProxyCommand ssh user@frontal-ssh.univ-reunion.fr nc %h %p 2>/dev/null
```

En cas de souci ?

Envoyez un mail à bastion-support@univ-reunion.fr

contributeurs :

Nom	Date	type modifications	version
Bannier Matthieu	25/02/2008	Première version	1.0
Dumont Annie	27/02/2008	corrections orthographiques utilisation de windows	1.1
Bannier Matthieu	26/05/2008	astuce utilisateur externe à l'université	1.2
Steff Laurent	27/05/2008	corrections orthographiques	1.3