Procédure pour utiliser les clés publique et privée avec un dépôt Git ou SVN initialisé sur un serveur Ubuntu

Étapes :

- Générer les clés publique et privée sur Ubuntu avec OpenSSH pour SamrtGit et Toritoise SVN
- Générer les clés publique et privée sur windows avec PuTTYgen pour TortoiseSVN
- Configurer Putty pour TortoiseSVN
  - Postes dans les laboratoires informatique à l'UdeS
- Configurer Tortoise SVN
- Tester le tout

Mise à jour : 2015-09-18 v1

Générer les clés publique et privée sur Ubuntu avec OpenSSH pour SamrtGit et Toritoise SVN

(Attention pour utiliser une clé privée générée avec OpenSSH sur Ubuntu dans PuTTY sur windows avec TortoiseSVN, elle doit être convertie en .pkk avant)

(RSA est recommandé car nous avons eu des problèmes avec DSA et Gitlab)

Se connecter sur le serveur Ubuntu avec votre cip pour y générer les clés. Placer la clé publique dans le répertoire .ssh et transférer la clé privée sur le poste client (windows)
cd (afin d'être bien dans votre "home dir")
ssh-keygen -b 4096 -t rsa (après la clé privée doit être importée et convertie par puttygen)
sans passphrase (avec passphrase vous devrez utiliser Pageant sur windows)
conserver noms de fichiers par défaut (id_rsa et id_rsa.pub
Deux fichiers seront générés dans le répertoire .ssh
    id_rsa
    id_rsa.pub
cd .ssh
cp -p id_rsa.pub authorized_keys (qui restera sur le serveur pour la connexion)

Transférer la clé privée id_rsa sur votre poste de travail qui a le client Git ou SVN.

Git :

La clé privée id_rsa générée par OpenSSH peut être utilisée directement par le client Git « Smartgit » installé dans les laboratoires

Même procédure d'utilisation de Git mais en choisissant « Private key » à la place de « Password » dans « SSH Credentials » puis pointer sur la clé id_rsa générée:

- Voir section « vérification du nouveau dépôt Git » dans Documentation Redmine, Ubuntu ou Solaris :

http://www.usherbrooke.ca/informatique/intranet/ressources-et-documentation/logiciels-services-outils/gestionnaires-de-versions-svngitcvs

SVN :

Importer et convertir la clé id_rsa générée par openssh dans puttygen afin de la sauvegarder en private_key.pkk (dans un dossier qui pourra être utilisé par la suite)

- Lancer PuTTYgen

        - Conversion -> import key
        - Sélectionner le fichier id_rsa (que vous avez généré avec OpenSSH)
        - save private key (Dans private_key.ppk : celle à utiliser sur votre poste et référée dans putty)
    - Voir section plus bas « Configurer putty pour utiliser la clé privée et y faire référence dans tortoiseSVN »

    Note : Dans les laboratoires au département d'informatique vous devez placer votre clé privée (private_key.ppk) dans le répertoire u:\ssh\private_key.ppk (respecter la syntaxe) afin de pouvoir l'utiliser avec PuTTY et TortoiseSVN automatiquement.

Générer les clés publique et privée sur windows avec PuTTYgen pour TortoiseSVN

(http://tortoisesvn.net/ssh_howto.html)

Installer PuTTY et PuTTYgen (http://www.putty.org/)
lancer PuTTYgen (n'étant pas installé dans les labo vous pouvez télécharger le .exe et l'exécuter)
choisir ssh-2 RSA 4096
sans passphrase (avec passphrase vous devez utiliser Pageant non documenté ici)
cliquer sur "generate"
attendre
save public key (Dans public_key.pub : celle à importer sur le serveur Ubuntu dans votre home ~/.ssh)
save private key (Dans private_key.ppk : celle à utiliser sur votre poste et référée dans PuTTY)

Note : Dans les laboratoires au département d'informatique vous devez placer votre clé privée (private_key.ppk) dans le répertoire u:\ssh\private_key.ppk (respecter la syntaxe) afin de pouvoir l'utiliser avec PuTTY et TortoiseSVN automatiquement par défaut.

Se connecter sur le serveur Ubuntu avec votre cip pour y importer la clé publique « public_key.pub »
Copier la clé publique « public_key.pub » sur le serveur et faire les commandes suivantes :

```
mkdir ~/.ssh
chmod 700 ~/.ssh
touch .ssh/authorized_keys
chmod 600 .ssh/authorized_keys
ssh-keygen -i -f public_key.pub >> .ssh/authorized_keys
```

Configurer putty pour utiliser la clé privée et y faire référence dans tortoiseSVN via TortoisePlink.exe

Postes dans les laboratoires informatique à l'UdeS

- Lancer PuTTY
- créer une session dans Putty
- hostname = nom du serveur ubuntu
- Pour lier la clé privée (celle en lien avec la clée public qui est sur le serveur dans ~.ssh/authorized_keys), avec la clé privée de la session de putty
    - Lancer Putty

- aller dans Connection-->SSH-->Auth et puis Browse .pkk sous "Private key file for authentication"
- sélectionner votre fichier private_key.pkk
  - (devrait déjà pointer vers u:\ssh\private_key.ppk)
- retour dans Session
- entrer le nom de la session à enregistrer dans "Saved Sessions"
- cliquer sur "save"
- Si vous êtes dans les laboratoires du département, **NE PAS FERMER** votre Putty, et ouvrir un autre putty pour faire le test car lorsque la dernière fenêtre est fermer, il « reset » la configuration et perd votre « Saved Session »
-

- tester avec open et donner votre login (cip) et il ne devrait pas y avoir de mot de passe de demandé

Configurer TortoiseSVN - Windows :

Note : Dans les laboratoires au département d'informatique vous devez placer votre clé privée (private_key.ppk) dans u:\ssh\private_key.ppk afin de pouvoir l'utiliser avec TortoiseSVN (via Plink)

Putty doit rester ouvert avec votre « Saved Session »

- Insataller Tortoise SVN
- Bouton droite dans un répertoire
  - Choisir : TortoiseSVN-->Settings-->Network sous SSH client:
    - Saisir : "C:\Program Files\TortoiseSVN\bin\TortoisePlink.exe" (ou le trouver s'il est ailleurs)
    - Clique sur OK

Tester le tout :

- Bouton droite dans un répertoire
- Choisir SVN Checkout :
  - dans URL Repository : svn+ssh://**votre_CIP**@**nom_session_putty_saved**/opt/redmine/depots/svn/**nouv-depot**