

Configurer une authentification avec un couple de clés privée/publique SSH

Présentation

Pour administrer un serveur Linux, vous pouvez utiliser le compte **root** ou, ce qui est fortement conseillé, un compte que vous avez créé et à qui vous avez permis une **élévation de privilèges**.

Si vous gérez un autre serveur, il est également fortement conseillé d'utiliser **un mot de passe différent**. Cette solution n'est **pas satisfaisante et peu sécurisée** si vous devez gérer de nombreux serveurs.

Par ailleurs cela est problématique si vous avez des tâches d'administration à **automatiser** car la saisie manuelle du mot de passe sera nécessaire ou bien il faudra indiquer le **mot de passe dans les scripts** ce qui est problématique si vous n'avez pas de solution pour les chiffrer. Les solutions possibles :

- utiliser un **annuaire LDAP pour centraliser** la gestion des comptes.
- utiliser des **clés SSH publique**.

Vous aller configurer le compte **root** ou le compte linux que vous avez créé afin de permettre d'ouvrir une session en utilisant une **clé publique SSH**. Vous utiliserez **votre propre clé publique SSH** pour vous connecter. Vous permettrez à l'enseignant de se connecter en simple utilisateur avec un compte que vous devez créer et appeler ensbtssio avec sa **clé publique SSH**.

Après la création de votre **couple de clés Privée/publique**, communiquez aux enseignants votre **clé publique** dans le dossier partagé Classe. Votre clé publique sera rajoutée à la page des clés SSH du BTS SIO à la page :

- [Les clés publiques SSH Etudiant/enseignants](#)

Génération des clés avec PuttyGen

- L'utilitaire **Puttygen** est disponible à l'adresse [PuttyGen](#). IL est disponible dans le **dossier partagé de la classe**.
- Lancez PuttyGen
 - Cliquez sur le bouton **Generate** et bouger la souris sur la **zone blanche**.
- Mettez **votre nom** comme commentaire de la clé publique.
- Sélectionnez puis Copiez/Coller votre clé publique dans un fichier texte (extension **.pub**) dans votre dossier personnel.
- Cliquez sur le bouton **Save private key** pour enregistrer votre clé privée (extension **.ppk**) dans votre dossier personnel.
- Le contenu du fichier de votre clé publique

Configuration de l'accès SSH

- Utilisez **WinSCP** pour vous connecter avec le compte **root** sur votre VM Debian.
- Créez dans le dossier **/root** un dossier **.ssh** et un fichier **/root/.ssh/authorizedkeys**
 - * Copiez dans ce fichier le contenu de votre clé publique. * Créez dans le dossier du compte **/home/ensbtssio** un dossier **.ssh** et un fichier **/home/ensbtssio/.ssh/authorized_keys** * Copiez dans ce fichier la clé publique de l'enseignant disponible depuis la page [Les clés publiques SSH Etudiant/enseignants](#). ===== Accès au serveur en SSH avec Putty ===== * Configurez Putty pour avoir un accès console à votre serveur. * Indiquez l'adresse IP de votre serveur et le port **22 (SSH)**.
 - * précisez le compte **root** pour vous connecter :
 - * précisez votre clé privée

From:
/ - Les cours du BTS SIO

Permanent link:
[/doku.php/reseau/debian/clesssh?rev=1606472799](#)

Last update: 2020/11/27 11:26

