# 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
  - En utilisant **mot de passe**, vous utilisez **un seul facteur** d'authentification.
  - En utilisant une **clé publique SSH**, vous utilisez également **un seul facteur** d'authentification.

**()** 

Cependant, vous pouvez utiliser la même clé publique SSH sur plusieurs serveurs en ne retenant qu'un seul mot de passe, celui de la passphrase de votre clé privée.

En général on désactive ensuite l'authentification par mot dd passe sur les serceures afin d en'autoriser que l'authentifiazitoj apr clé SSH

### Générer une paire de clé SSH depuis un client OpenSSH

Générer une paire de clés privée/publique depuis un client Windows ou linux.



Il est conseillé de protéger l'utilisation de la clé privée avec une passphrase.

\$ ssh-keygen

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/centrecallbd/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/centrecallbd/.ssh/id_rsa.
Your public key has been saved in /home/centrecallbd/.ssh/id rsa.pub.
The key fingerprint is:
SHA256:0rjedyVuT2fzEJHgw5I9lfmTsQ6MHSD87Xrr/aXE3r4 centrecallbd@Ch2Lab1
The key's randomart image is:
+---[RSA 2048]----+
         .. .0 .0 |
          ..= +00
           + (0 + . + )
        o + B = . |
       o S . + .
        0
            .0.0
            ..0=.+|
       .
           ..+=.*+|
       . .. oo+=EB|
  ---[SHA256]----+
+-
$
```

Dans le dossier caché **.ssh** (sous Windows Linux ou MacOsX) vous avez votre couple de clés privée (id rsa) et publique (id rsa.pub).

\$ ls .ssh
id\_rsa id\_rsa.pub
\$

### Configurer un accès SSH avec une clé SSH depuis un client OpenSSH

• Copiez ensuite votre clé publique sur le serveur auquel vous souhaitez accéder avec la clé SSH.

\$ ssh-copy-id utilisateur@IP\_ordinateur\_cible



La clé publique est copiée dans le fichier **.ssh/authorized\_keys** du serveur distant.



La commande ssh-copy-id n'est pas disponible sous Windows. Vous pouvez alors :

2024/05/22 14	1:47 3/10	Configurer une authentification avec un couple de clés privée/publique SSH
	<ul> <li>utiliser la l'utilisater</li> <li>ouvrir une dans le fie</li> </ul>	commande <b>scp</b> pour copier le fichier id_rsa.pub dans le dossier ur ; e session ssh pour pouvoir ensuite ajouter le contenu du fichier id_rsa.pub chier authorized_keys :
1	C:> scp .ss compteutili C:> ssh com \$ cat id_rs	h/id_rsa.pub sateur@adresseip:/home/compteutilisateur/ pteutilisateur@adresseip a.pub >> .ssh/authorized_keys

Vous devez maintenant pouvoir vous connecter sans mot de passe au serveur distant :

```
$ ssh utilisateur@IP_ordinateur_cible
```

3/10

Il est fortement conseillé ensuite de désactiver l'authentification par mot de passe en modifiant le fichier de configuration du service ssh sur le serveur distant /etc/ssh/sshd config :

• Décommentez la ligne suivante en mettant sa valeur à no :

PasswordAuthentication no

sauvegardez le fichier /etc/ssh/sshd\_config et relancer le service ssh :

```
$ sudo systemctl restart ssh
```

Pour en savoir plus :

2024/05/22 14.47

 https://fr-wiki.ikoula.com/fr/Cl%C3%A9 SSH-\_comment\_cr%C3%A9er\_une\_cl%C3%A9\_SSH\_(Debian\_10)

### 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

le Key Conversions Help	
Key	
No key.	
Actions	
Actions Generate a public /private key pair	Generate
Actions Generate a public/private key pair	Generate
Actions Generate a public/private key pair Load an existing private key file	Generate
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Generate Load Save public key Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	Generate Load Save public key Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate:	Generate Load Save public key Save private key © SSH-2 DSA

• Cliquez sur le bouton **Generate** et bouger la souris sur la **zone blanche**.

Pu 🦻	ITTY Ke	y Generator	-				x
File	Key	Conversions	Help				
- Ke	y ease ge	nerate some rand	domness by moving t	the mouse over t	he blan	ik area.	
Ac	tions						
Ge	enerate	a public/private	key pair		[	Generate	
Lo	ad an e	xisting private ke	ey file		[	Load	
Sa	ve the g	generated key		Save public k	ey	Save private k	cey
Pa	rameter	s					
Ty	pe of ke SSH-1	ey to generate: (RSA)	SSH-2 RSA		) SSH	-2 DSA	
Nu	imber of	bits in a genera	ted key:			2048	

- Mettez votre nom comme commentaire de la clé publique.
- Sélectionnez puis Copiez/Coller votre clé publique dans un fichier texte (extention **.pub**) dans votre dossier personnel.
- Cliquez sur le bouton **Save private key** pour enregister votre clé privée (extention **.ppk**) dans votre dossier personnel.

PuTTY Key Generato	r		×
File Key Conversior	ns Help		
Key			
Public key for pasting in	nto OpenSSH authorized	d_keys file:	
+gcm7eUE1AClhKIWE	34zX5Nsi4/OMo3dh2f3	hQOL7BRixFWS/WL	oQi1EfZiBx3wMbd 🔺
+OVTO6yHczWenjgG	KhnFFRAaggaKyNrGos	TnEz3uojBzS2/FLSr7c	ouQtCN9xAWVqR
1jDqW+dMrQbL3T5xv +KYFi39Vu6NWESp9	rwoRBaKf YSBYB09NKELIUEAade	Ru9WAatZAff8XQ== C	hades Técher
Key fingemint:	ash ma 2049 9a:17:5d	50-1C-0b-07-0a-d7f2-d	4.62.2o.4b.00.ob
Rey Ingerphrit.	ssniisa 2046 Se. 17.50.	.56.16.0D.07.0C.07.15.0	14.62.3C.40.63.CD
Key comment:	Charles Técher		
Key passphrase:			
Confirm passphrase:			
Actions			
Generate a public/priva	ate kev pair		Generate
Load an existing private	e key file		Load
Save the generated ke	У	Save public key	Save private key
Parameters			3
Type of key to generate	e:		
SSH-1 (RSA)	SSH-2 RSA	© SSI	1-2 DSA
Number of bits in a gen	erated key:		2048

• Le contenu du fichier de votre clé publique

7/10

Enregistrer so	us	Strengthern, 1 of agilts, haven	and the second second	×
<b>O</b> - <b></b>	≪_echange ► s	i7  ClesPubliques	← ← Recherch	her dans : ClesPubliques 🔎
Organiser 🔻	Nouveau doss	ier		≣ ▾ 🔞
að Musique	e 🔺 N	om	Modifié le	Туре
Vidéos 🛃		Aucun élément n	e correspond à votre reche	rche.
💶 Ordinateu	r	, acan clement in		i set their
S (C:)				
	):)			
🛞 Lecteur	DVD RW			
🖵 agnes.bo	ourgeois			
🖵 valadon	(\\fileser			
🖵 progs (\	\fileserv)			
💼 Réseau				
- Nescau	<b>~</b> •		11	•
Nom du fic	hier : ClePubliqu	eCharlesTecher.pub		-
т	ype : Tous les fic	hiers (*.*)		•
Cacher les d	lossiers	Encodage : ANSI	▼ Enregist	rer Annuler
	<i></i>			
	ClePubliqueCl	arlesTecher.pub - Bloc-notes		
	Fichier Edition	Format Affichage ?	ffovo chanles T	f =h = n
	VUONWESP9YS	SYBU9NKFLIUFAQORU9WAajiZA	TT8XQ== Charles I	ecner 🔺
				_
	•			

## 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/authorized\_keys

ssh - root@10.187.37.196 repl E SSH - WinSCP		x						
Local Marquer Fichiers Commandes Session Options Distant Aide								
🏟 🔢 🗊 - 🏦 📽 관 📟 🧬 😤 🐜 🛛 - 🖂 🕅 🖉 🖉 Défaut	- 14	<b>5</b> - 1						
root@10.187.37.196 repl E SSH +								
$\blacksquare P: \bullet \textcircled{\begin{tabular}{cccccccccccccccccccccccccccccccccccc$	🞾 🚮 🙋	te						
P:\Classe_B2_SIO\_echange\si7\ClesPubliques /root/.ssh								
Nom Ext Nom Ext	Taille	Date						
<u>∎</u>		01/0						
ClePubliqueCharlesTecher.pub	395 B	01/0						
< III + IIII + IIII + III + II		Þ.						
0 B de 395 B dans 0 de 1 395 B de 395 B dans 1 de 1								
🛿 🤌 F2 Renommer 📝 F4 Editer 📸 F5 Copier 🗳 F6 Déplacer 🏄 F7 Créer un répertoire 🗙 F8 Effacer 👘 🎽								
SFTP-3	0:08:5	2						

- 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).

ĵ

PuTTY Configuration	×
Putty Configuration Category:  Session  Cogging  Terminal  Keyboard  Bell  Features  Window	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 10.187.37.196 22 Connection type: Raw Telnet Rlogin SSH Scrial
Appearance     Behaviour     Translation     Colours     Connection     Proxy     Telnet     Rlogin     SSH	Load, save or delete a stored session Saved Sessions Repl Default Settings DokuwikiPublic spock Delete
About	Close window on exit: Always Never Only on clean exit

• précisez le compte **root** pour vous connecter :

Pully Configuration					×
Category:					
Category: Terminal Weyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection	* [	Dat Login details Auto-login usemann When usemame is Prompt OL Terminal details Terminal -type string Terminal speeds Environment variab	a to send le not speci Jse syster	to the server root ified: m usemame (agne xterm 38400,38400	es.bourgec
	•	Variable Value			Add Remove

• précisez votre clé privée

#### 23 🕵 PuTTY Configuration Category: Options controlling SSH authentication E Terminal \* Keyboard Bypass authentication entirely (SSH-2 only) Bell Display pre-authentication banner (SSH-2 only) Features . indow Authentication methods Appearance Attempt authentication using Pageant Behaviour Attempt TIS or CryptoCard auth (SSH-1) Translation Attempt "keyboard-interactive" auth (SSH-2) Selection Colours Authentication parameters Connection Allow agent forwarding Data Allow attempted changes of usemame in SSH-2 Proxy Telnet Private key file for authentication: Rlogin D:\Logiciels\CleSSH\ClePrivee.ppk Browse ... 🗄 - SSH --- Kex 🗄 - Auth GSSAPI TTY - X11 • ш Þ About Open Cancel

From:

https://siocours.lycees.nouvelle-aquitaine.pro/ - Les cours du BTS SIO

Permanent link: https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/debian/clessh?rev=1637528748

Last update: 2021/11/21 22:05

