Table des matières

TABLE DES MATIERES

INSTALLATION ET CONFIGURATION GENERATION D'UNE CLE

Avant-Propos

E6:

Elaboration de documents relatifs à la production et à la fourniture de services

- A1.1.1 , Analyse du cahier des charges d'un service à produire
- A1.2.4 , Détermination des tests nécessaires à la validation d'un service
- A1.3.4, Déploiement d'un service
- A4.1.9 , Rédaction d'une documentation technique

1

2

3

Installation et configuration

Pour installer le SSH, il faut taper la commande suivante :

root@debian:~# apt–get install ssh_

Par défaut, le serveur ssh est configuré pour une authentification par mot de passe. Pour changer cela, il faut modifier le fichier /etc/ssh/sshd_config avec l'éditeur nano et rajouter les lignes, ou plus particulièrement les décommenter :

PubkeyAuthentication yes AuthorizedKeysFile %h/.ssh/authorized_keys

On redémarre ensuite le service :

root@debian:~# service ssh restart

Maintenant, on peut se connecter en SSH :

Basic options for your PuTTY set	ssion		
Specify the destination you want to connect to			
Host Name (or IP address)	Port		
192.168.1.128	22		
Connection type: ◎ Ra <u>w</u> ◎ <u>T</u> elnet ◎ Rlo <u>gi</u> n ● <u>S</u> SH	🔘 Sețial		

La première fois que l'on se connecte en SSH, un message d'alerte apparait.

On clique sur oui, pour mémoriser la clé publique dans la base de registre Windows.

PuTTY Secu	urity Alert
	WARNING - POTENTIAL SECURITY BREACH! The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server. The new rsa2 key fingerprint is: ssh-rsa 2048 fb:6b:0a:64:5c:10:11:1e:c5:9b:7c:0c:92:30:6b:4d If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting. If you want to carry on connecting but without updating the cache, hit No. If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.
	Oui Non Annuler Aide

C'est une clé publique, le serveur est propriétaire de la clé, et elle est transmise afin que le client puisse se connecter.

Génération d'une clé

Pour créer une clé, il faut lancer l'utilitaire PuTTYgen

ile	Key	Conver	sions	Help				
Ke	у							
No	key.							
Ac	tions							
Ac	tions	a public/	(orivate	kev pair				Generate
Ac Ge	tions enerate	a public/	/private	key pair				Generate
Ac Ge Lo	tions enerate ad an e	a public/ existing pr	′private ivate ke	key pair ey file				Generate
Ac Ge Lo Sa	tions enerate ad an e we the	a public/ existing pr generate	′private ivate ke d key	key pair ey file		Save pub	lic key	Generate Load Save private key
Ac Ge Lo Sa Pa	tions enerate ad an e we the rameter	a public/ existing pr generate	′private ivate ke d key	key pair ey file		Save pub	lic key	Generate Load Save private key
Ac Ge Lo Sa Pa Ty	tions enerate ad an e ve the rameter pe of k	a public/ existing pr generate rs ey to gen	′private ivate ke d key erate:	key pair ey file		Save pub	lic key	Generate Load Save private key
Ac Ge Lo Sa Pa Ty	tions enerate ad an e ve the rameter pe of k SSH-1	a public/ existing pr generate rs ey to gen I (RSA)	′private ivate ke d key erate:	key pair ey file • S	SH-2 RSA	Save pub	lic key	Generate Load Save private key H-2 DSA

On choisit le paramètre le nombre de bit puis on clique sur générer.

DUPONT ANTHONY

DATE :02/06/17

le Key Conversions He	łp
Key	
Please generate some random	ness by moving the mouse over the blank area.
Actions	
Actions Generate a public/private key	pair Generate
Actions Generate a public/private key p	pair Generate
Actions Generate a public/private key p Load an existing private key file	pair Generate
Actions Generate a public/private key p Load an existing private key file Save the generated key	pair Generate e Load Save public key Save private key
Actions Generate a public/private key p Load an existing private key file Save the generated key Parameters	pair Generate e Load Save public key Save private key
Actions Generate a public/private key p Load an existing private key file Save the generated key Parameters Type of key to generate:	pair Generate e Load Save public key Save private key
Actions Generate a public/private key p Load an existing private key file Save the generated key Parameters Type of key to generate: SSH-1 (RSA)	pair Generate Load Save public key Save private key © SSH-2 RSA © SSH-2 DSA

Il faut secouer la souris sur la fenêtre afin que la génération avance.

С	С	L	1
Э	Э	Г	

e Key Conversion	ns Help			
Key				
Public key for pasting in	nto OpenSSH authorized	d_keys file:		
ssh-rsa AAAAB3NzaC1yc2EA JZCa/U6YLm1/KIP6o +jPxPrlNsmLsd/sO4Pr VS03IYYU/bU=rsa-ke	AAABJQAAAIEAgPfLS8 5/30nl88AiXYoOCOx+J0 n7ylBc7tvWfP51H18TZ sy-20161114	3QmalMTZIK/eoAsQWy 09Ym1NlhRDMGniyEwj NRctMkY6QjP62DN4k	rAhpxTFoGPpOHt jt0lt GrMW7vEKSWp	*
Key fingerprint:	ssh-rsa 1024 4e:13:88:	:a5:f8:52:0f:f8:ab:81:d7	:0d:66:a7:5b:f4	
Key comment:	rsa-key-20161114			
Key passphrase:				
Confirm passphrase:				_
Actions				
Generate a public/priva	ate key pair		Generate	
Load an existing private	e key file		Load	
Save the generated ke	y	Save public key	Save private ke	y
Parameters				
Type of key to generat SSH-1 (RSA)	e:	© SSH	I-2 DSA	
Number of bits in a gen	erated key:		1024	

Il faut ensuite ajouter un mot de passe, parce que c'est plus sécurisé.

Key		
Public key for pasting	into OpenSSH authorized_keys file:	
ssh-rsa AAAAB3NzaC1yc2E/ JZCa/U6YLm1/KIP6c +jPxPrlNsmLsd/sO4P VS03IYYU/bU=rsa-k	AAABJQAAAIEAgPfLS8QmalMTZIK/eoAsQWyAhpxTFoGPpOHt 55/30nl88AiXYoOCOx+J09Ym1NlhRDMGniyEwijt0lt m7ylBc7tvWfP51H18TZNRctMkY6QjP62DN4K6rMW7vEKSWp ey-20161114 pour putty	*
Key fingerprint:	ssh-rsa 1024 4e:13:88:a5f8:52:0ff8:ab:81:d7:0d:66:a7:5b.f4	
Key comment:	rsa-key-20161114 pour putty	
Key passphrase:	•••••	
Confirm passphrase:	•••••	

Une fois que l'on à tout bien paramétré, il faut enregistré la clé publique et la clé privée. On clique donc sur Save public key et Save private key.

Attention, la clé privée doit avoir une extension .ppk et la clé publique une extension .pub

Nom du fichier :	public.pub
Nom du fichier :	private.ppk

Nous avons donc généré une clé privée et une clé publique. Il faut bien entendu protéger et éviter de transmettre la clé privée.

Pour charger la clé, il faut lancer le logiciel Pageant.

Pageant Key List			
	Add Key	Remove Key	
Help			Close

On clique sur Add Key et on sélectionne la clé privée.



On rentre le mot de passe que l'on a mis précédemment (dans mon cas j'avais mis Password1234)

Pageant Key List		? ×
ssh-rsa 1024	4e:13:88:a5f8:52:0ff8:ab:81:d7:0d:66:a7:5bf4	rsa-key-20161114 pour put
	Add Key Remov	e Key
Help		Close

Une fois que la clé est ajoutée on peut fermer l'utilitaire.

On lance maintenant putty et on créer une session, il suffit de marquer l'adresse IP et de lui donner un nom :

Saved Sessions	
TP SSH	
Default Settings TP SSH	Load
	Save
	Delete

Une fois que cela est fait on choisit la session en cliquant dessus puis on va dans DATA dans le menu à droite.

■ Session
Logging
🚊 · Terminal
···· Keyboard
···· Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Data
Provv
Telnet
Plagin
····· Senal

Puis il faut ajouter le nom du compte sur lequel on veut se connecter :

Data to send to the server		
Login details		
Auto-login usemame	anthony	
When usemame is not specified: Prompt Use system usemame (adupont) 		

Ensuite on va dans le menu SSH



Puis on choisit le bouton radio 20nly



Maintenant on va dans le sous-menu du SSH « Auth »



Puis on choisit le fichier de la clé privé que l'on veut utiliser.

Private key file for authentication:	
D:\cles\private.ppk	Browse

Puis on retourne sur session et on clique sur Save.

Une fois que putty est configuré, nous allons paramétrer la clé publique sur le serveur.

Il faut relancer l'utilitaire puTTYgen, cliquer sur le bouton load et charger la clé privée et rentrer le mot de passe.



Il faut ensuite copier ce qui est marqué ici dans le presse papier.

On démarre la session putty et on se connecte sur l'utilisateur qui est créé sur la machine.

Ensuite, sur le serveur, dans le home de l'user, on créer un dossier ssh.

anthony@debian:~\$ mkdir .ssh

On copie ensuite le contenu du presse papier dans un fichier qui s'appelle authorized_keys



Donc, pour ce faire, on fait le cat, puis une fois que la commande est lancée on fait shift + ins sur le clavier ce qui va copier le presse papier, puis on appuie sur Entrée et enfin on fait un ctrl + d pour fermer le cat.

On modifie ensuite les droits sur le répertoire home (lecture, écriture et exécution par le propriétaire seul, à l'exclusion de tout autre)

anthony@debian:~\$ chmod u+rwx,g+---,o+--- /home/anthony

Puis on modifie les droits sur le fichier .ssh/autorized_keys. On donne les droits de lecture/ecriture uniquement, par le propriétaire seul à l'exclusion de tous les autres.

anthony@debian:~\$ chmod u+rw-,g+---,o+--- .ssh/autorized_keys