

Skapánê : OTP Client Guide

OTP Client

1. Déclaration du client sur le serveur
2. Installation de PAM agent OTP Server
3. Configuration de PAM agent OTP Server
4. Test de l'authentification forte
5. Problème et résolution

Skapánê : OTP Client Guide

Le but de cette procédure est l'installation et la configuration du PAM agent OTP Server sur une Machine Virtuelle Debian 9, le nom de la machine sera OTP-Client. Cet agent permet à une machine d'avoir une double authentification pour se connecter en SSH.

Cette procédure fait suite à la procédure « OTP Server Guide » pour l'installation du serveur. Il n'y aura pas explication sur l'installation et la configuration des Machines Virtuelles (déjà expliqué dans « OTP Server Guide »).

PAM agent OTP Server est l'agent qui utilise le mécanisme d'authentification PAM présent de base sur toutes les machines Linux.

Nous allons commencer par déclarer la machine client sur le serveur, cela se fait sur OTP Center.

Puis l'installation et la configuration de l'agent sur la Machine Virtuelle.

Puis une fois installé, le test de l'authentification forte par un connexion SSH pourra alors être effectué.

Une dernière partie sera dédié aux problèmes rencontrés lors de l'authentification en SSH ainsi que la résolution de ces derniers.

Pré-requis :

- Avoir une Machine Virtuelle Debian
- OTP Server mis en place
- Fichier d'installation de PAM agent OTP Server
- SSH opérationnel
- Troisième machine, l'hôte par exemple, avec un openssh-client pour faire le test d'authentification
- Tester la communication entre la Machine Virtuelle du serveur, de l'agent et de l'hôte avec un ping

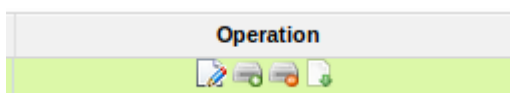
Déclaration du client sur le serveur

Skapánê : OTP Client Guide

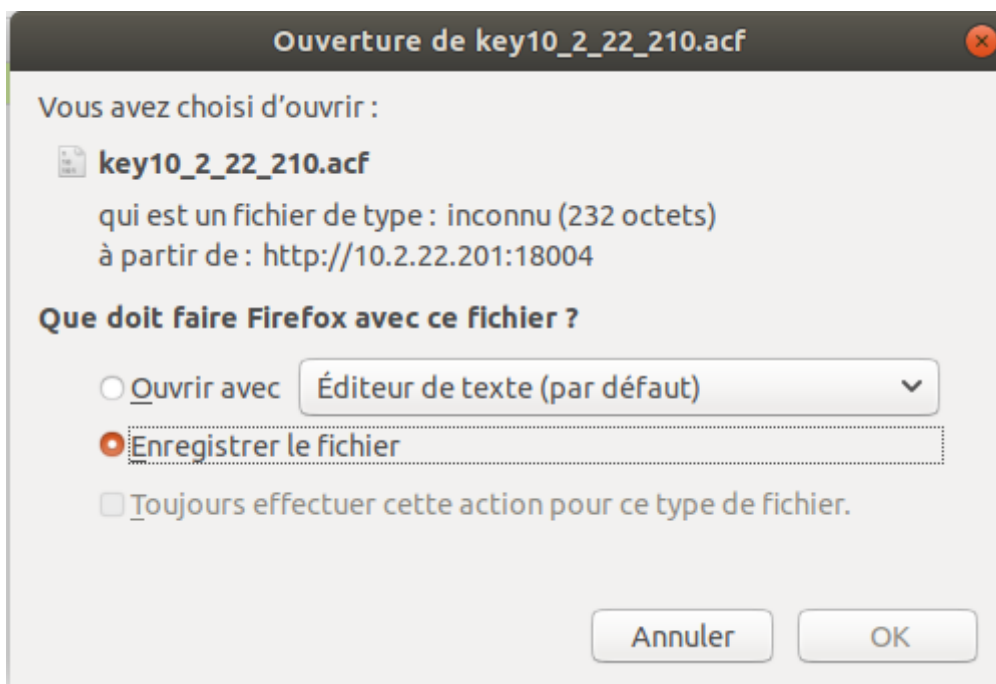
Avant de commencer l'installation de l'agent, il faut le déclarer sur le serveur, c'est à dire sur l'interface web OTP Server, cette étape se fait en première car il faut récupérer un fichier de configuration qui sera nécessaire pour lors de l'installation de l'agent.

La déclaration de l'agent est expliqué à la page 62 de la procédure « OTP Serveur Guide », mais il faut tout de même retourner sur l'interface web pour récupérer le fichier de configuration de l'agent.

Donc retournez sur l'interface web OTP Center et allez dans « Authentification », « Agent » et « List ». Regardez dans la rubrique « Opération » et cliquez sur la dernière icône.



Cochez « Enregistrer le fichier » et cliquez sur OK

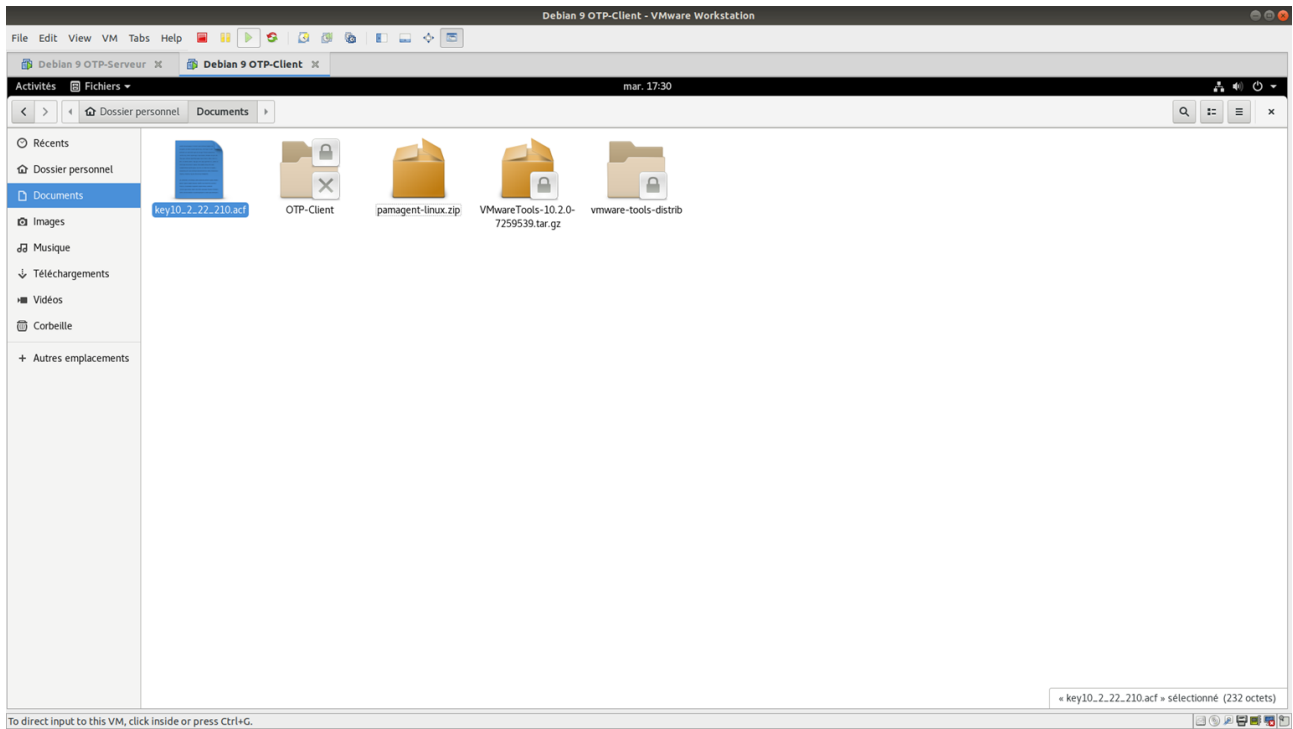


fois de

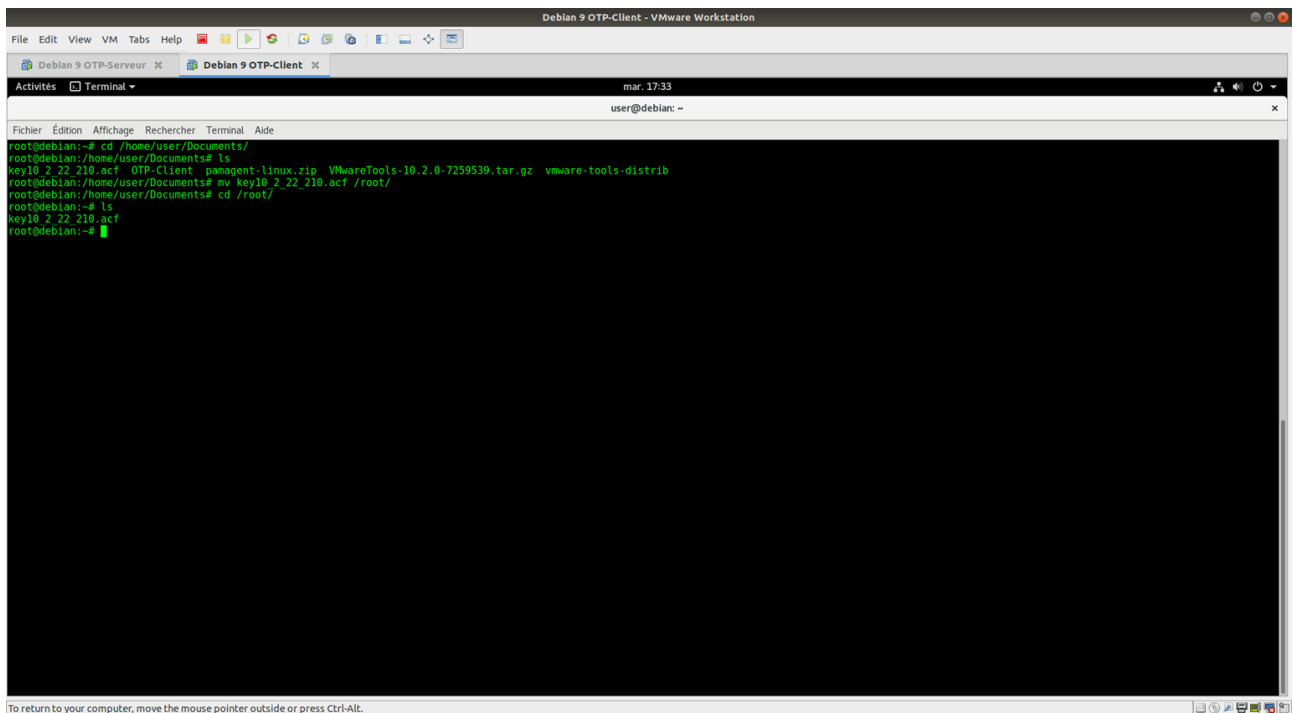
Une
le fichier

téléchargé, copier dans votre Machine Virtuelle OTP-Client

Skapánê : OTP Client Guide



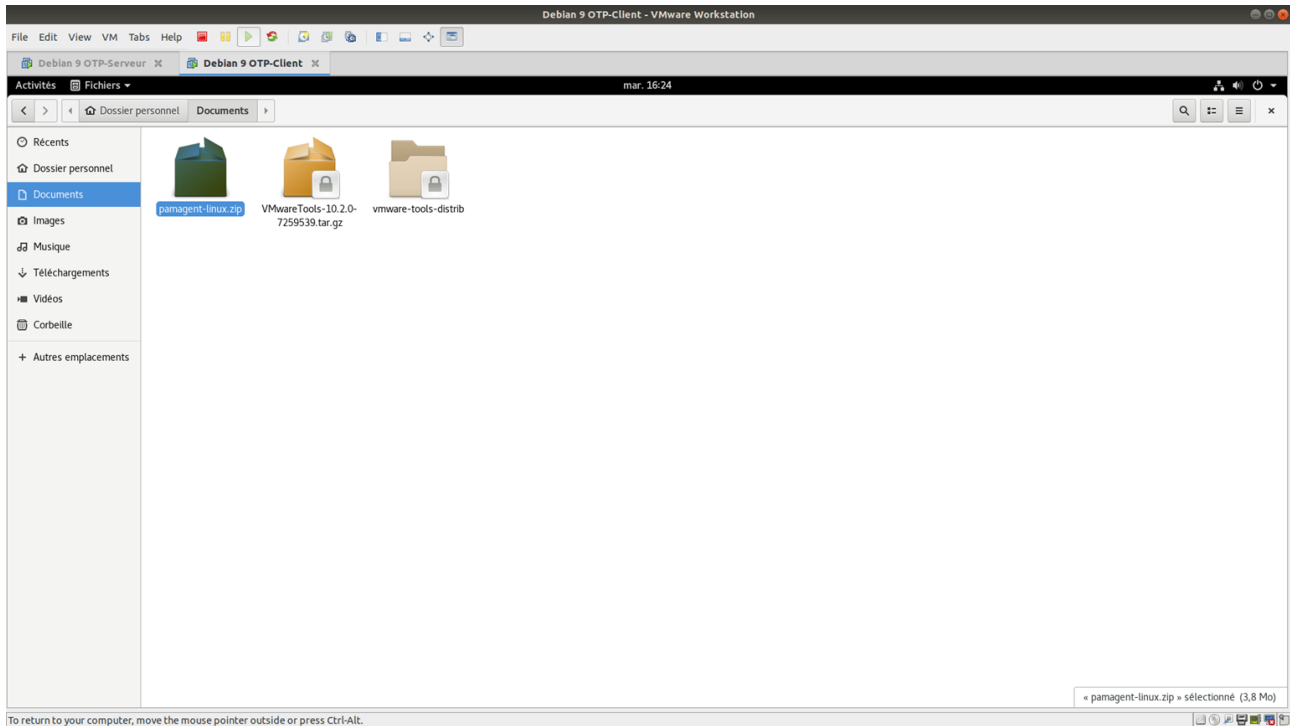
Allez dans le Terminal (toujours sur la Machine Virtuelle OTP-Client) et déplacer le fichier dans le répertoire root :



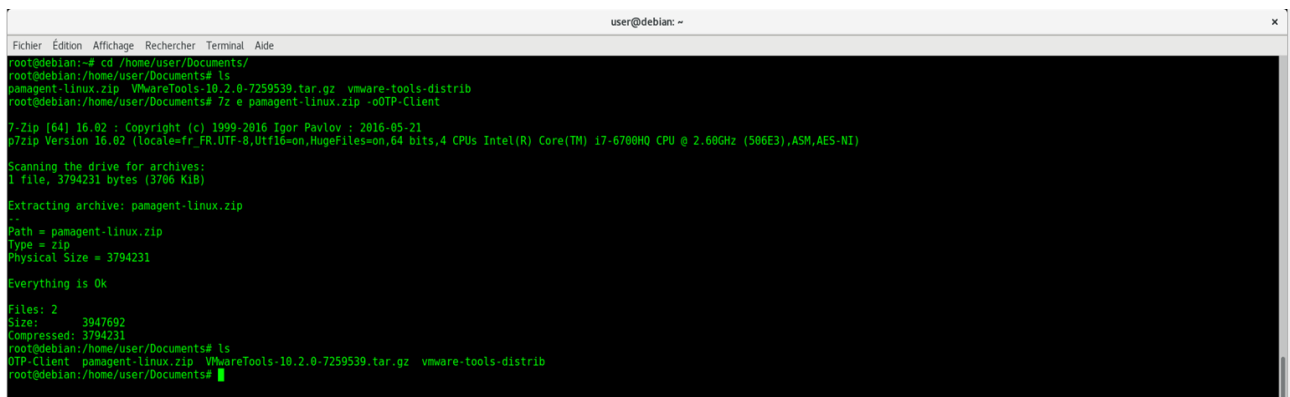
Installation de PAM agent OTP Server

Skapánê : OTP Client Guide

Maintenant l'installation peut commencer, copier l'archive « pamagent-linux.zip», qui contient le fichier d'installation de PAM agent OTP Server, dans le répertoire Document. Pour ce faire, faites tout simplement un glisser-copier (possible grâce à vmware-tools)



L'archive se trouve maintenant sur votre Machine Virtuelle, aller dans le Terminal, puis décompresser là



La décompression de l'archive vous donne un autre fichier ZIP et le manuel pour l'agent. Faites une autre décompression pour la nouvelle archive

Skapánê : OTP Client Guide

```
root@debian:/home/user/Documents/OTP-Client# 7z x pamagent-linux64-v4.0-20131018.zip
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=fr_FR.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz (506E3),ASM,AES-NI)
Scanning the drive for archives:
1 file, 2627698 bytes (2567 KiB)

Extracting archive: pamagent-linux64-v4.0-20131018.zip
--
Path = pamagent-linux64-v4.0-20131018.zip
Type = zip
Physical Size = 2627698

Everything is Ok

Folders: 4
Files: 8
Size:      8388663
Compressed: 2627698
root@debian:/home/user/Documents/OTP-Client# ls
OTP_Server_PAM_authentication_agent_user_manual_V4.0.pdf  pamagent-linux64-v4.0  pamagent-linux64-v4.0-20131018.zip
root@debian:/home/user/Documents/OTP-Client#
```

Se positionnez dans le répertoire où se trouve les fichiers de l'agent et exécutez le fichier « install »

```
root@debian:/home/user/Documents/OTP-Client# cd PAM-agent/
root@debian:/home/user/Documents/OTP-Client/PAM-agent# ls
agenttest bin conf COPYRIGHT install install-sh lib pamagent-linux64-v4.0 pam_otp.conf pam_otp.so README VERSION
root@debian:/home/user/Documents/OTP-Client/PAM-agent# ./install
```

- L'installation de l'agent se lance, il vous demande plusieurs renseignements :
- Êtes-vous d'accord avec les termes de la licences : Y
 - Le chemin absolu du fichier téléchargé auparavant (il contient plusieurs informations comme l'IP du serveur ou encore les méthodes d'authentications)

```
root@debian:/home/user/Documents/OTP-Client/pamagent-linux64-v4.0# ./install
*****
*
*      OTP Server PAMAgent for Linux      *
*
*****

Have you read and do you agree to all the terms of the license
included with this package? [y/n] y

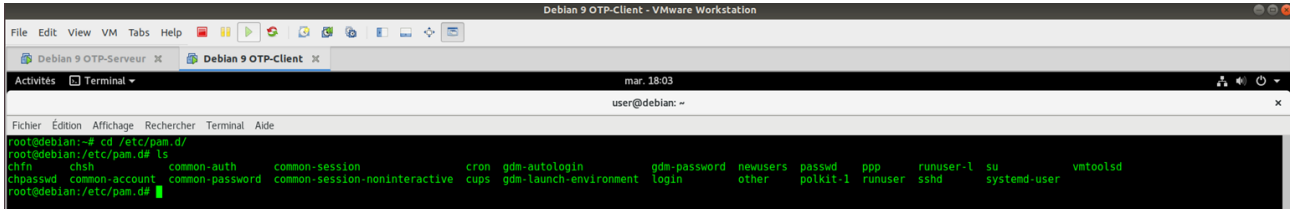
Please input your OTP Server PAMAgent config file's full path name,
the OTP Server PAMAgent config file name is like 'otpagent.acf': /root/key10_2_22_210.acf
*****
*
*      Congratulations!                  *
*      OTP Server PAMAgent has installed  *
*      These files are needed,           *
*      /etc/otpagent.acf                 *
*      /lib64/security/pam_otp.so        *
*      /etc/pam_otp.conf                  *
*      Thank you for use OTP PAMAgent.   *
*
*****
root@debian:/home/user/Documents/OTP-Client/pamagent-linux64-v4.0#
```

Configuration de PAM agent OTP Server

L'installation de l'agent est maintenant terminé, il ne reste plus qu'à le configurer. La configuration de l'agent se fait par le mécanisme d'authentification PAM (installé de base sur les distribution Linux).

Skapánê : OTP Client Guide

Placez vous dans le répertoire `/etc/pam.d/`, dans ce répertoire se trouve les fichiers de configuration qui gèrent les différents mécanismes d'authentification (exemple : LDAP, SSH, root, ...)

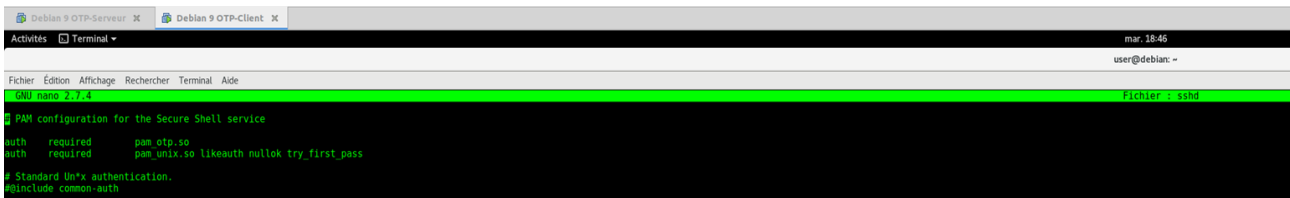


```
root@debian:~# cd /etc/pam.d/
root@debian:/etc/pam.d# ls
chfn      chsh      common-auth  common-session  cron      gdm-autologin  gdm-password  newusers  passwd  ppp      runuser-l  su      vmtocsd
chpasswd  common-account  common-password  common-session-noninteractive  cups      gdm-launch-environment  login          other      polkit-1  runuser  sshd      system-user
```

Le premier fichier PAM à modifier est le fichier `SSHD`, qui gère les différents méthodes d'authentification. Une fois dans le fichier, plusieurs modules sont déjà présent, il faut juste ajouter et modifier les lignes suivantes :

- ligne à ajouter : `auth required pam_otp.so`
- ligne à ajouter : `auth required pam_unix.so likeauth nullok try_first_pass`
- ligne à commenter « `include common-auth` »

Votre fichier doit ressembler à ceci :



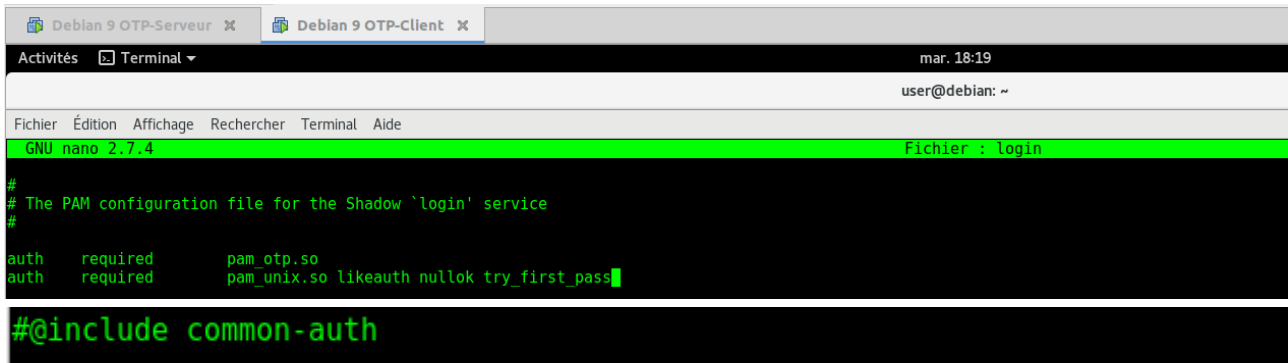
```
root@debian:~# nano /etc/pam.d/sshd
PAM configuration for the Secure Shell service
auth      required      pam_otp.so
auth      required      pam_unix.so likeauth nullok try_first_pass
# Standard Unix authentication.
#include common-auth
```

Enregistrez et quitter le fichier

Le deuxième fichier PAM à modifier est le fichier « `login` », il y a plusieurs modules aussi présents à l'intérieur du fichier, comme le précédant il faudra juste ajouter ou modifier les lignes suivantes :

- ligne à ajouter : `auth required pam_otp.so`
- ligne à ajouter : `auth requiried pam_unix.so likeauth nullok try_first_pass`
- ligne à commenter : `@include common-auth`

Skapánê : OTP Client Guide



```
Debian 9 OTP-Serveur x Debian 9 OTP-Client x
Activités Terminal mar. 18:19
user@debian: ~
Fichier Édition Affichage Rechercher Terminal Aide
GNU nano 2.7.4 Fichier : login
#
# The PAM configuration file for the Shadow `login' service
#
auth required pam_otp.so
auth required pam_unix.so likeauth nullok try_first_pass
#@include common-auth
```

Enregistrez et quittez le fichier

Maintenant, allez dans le fichier de configuration du serveur SSH pour que le service SSH demande une authentification avec le password + OTP : « /etc/ssh/sshd_config », cherchez la ligne « ChallengeResponseAuthentication » et remplacez le No par Yes :

```
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication yes
```

Enregistrez, quittez le fichier et redémarrer le service ssh

La librairie « pam_otp.so » se trouve dans le répertoire « /lib64/security », déplacer cette librairie dans le répertoire « /lib/security » (il faudra peut-être que vous le créer) sinon l'agent ne fonctionnera pas

Il faut maintenant créer un nouvel utilisateur sur la Machine Virtuelle OTP-Client ; dans la configuration de OTP Center, un utilisateur test a été créée, il s'agit de « usertest01 » avec pour mot de passe « usertest ». Créer donc l'utilisateur « usertest01 » mais avec le mot de passe de votre choix, pour le test plus tard, je vais prendre comme mot de passe « usertest » :

Skapánê : OTP Client Guide

```
root@debian:/etc/pam.d# adduser usertest01
Ajout de l'utilisateur « usertest01 » ...
Ajout du nouveau groupe « usertest01 » (1001) ...
Ajout du nouvel utilisateur « usertest01 » (1001) avec le groupe « usertest01 » ...
Le répertoire personnel « /home/usertest01 » existe déjà. Rien n'est copié depuis « /etc/skel ».
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd: password updated successfully
Changing the user information for usertest01
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Cette information est-elle correcte ? [0/n]0
```

Il est possible de voir la liste des utilisateurs présents sur la Machine Virtuelle via la commande « `cat /etc/passwd` » mais les mots de passe ne sont pas affichés, question de sécurité :

```
root@debian:/etc/pam.d# cat /etc/passwd
```

Test de l'authentification forte

Il est maintenant que tous les fichiers de configuration sont bons, il est grand temps de vérifier l'authentification forte. Pour cela, allez sur la 3ème machine c'est à dire l'hôte (la machine physique) et faite une connexion SSH vers la Machine Virtuelle OTP-Client :

```
root@kakia:~# ssh usertest01@10.2.22.210
```

Skapánê : OTP Client Guide

La connexion se fait par la demande d'un premier mot de passe, ici c'est le mot de passe du compte de l'utilisateur sur la machine OTP-Client « usertest »

```
root@kakiã:~# ssh usertest01@10.2.22.210
Password:
PassCode: █
```

La connexion demande un « Passcode » qui au « static password » de l'utilisateur sur OTP Center + l'OTP afficher sur le Token. (le static password et l'OTP doivent être mis à la suite sans caractère entre les deux)

```
root@kakiã:~# ssh usertest01@10.2.22.210
Password:
PassCode:
Linux debian 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
usertest01@debian:~$ █
```

La connexion s'effectue, le test est un succès, l'authentification forte (authentification à double temps) est opérationnel !

En résumé, le démarche à suivre pour se connecter est :

- ssh « nom de l'utilisateur de la machine cible »@ « son IP »
- Password : « mot de passe présent sur la machine cible »
- Passcode : mot de passe de l'utilisateur sur OTP Center + OTP