Configuration de l'ordinateur client SSH pour les certificats

Comment configurer un ordinateur client pour utiliser des certificats SSH pour l'authentification de l'hôte et du client.

Authentification de l'hôte:

SSH reconnaîtra les certificats d'hôte de tout hôte dont le certificat est signé par une autorité identifiée dans le fichier /etc/ssh/ssh_known_hosts.

Pour configurer cela, vous avez besoin de la ligne suivante dans /etc/ssh/ssh_config:

```
GlobalKnownHostsFile /etc/ssh/ssh_known_hosts
```

Ensuite, vous devez ajouter une ligne comme celle ci-dessous à /ets/ssh/ssh_known_hosts:

```
cat <<EOF | sudo tee -a /etc/ssh/ssh_known_hosts
@cert-authority * ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDTcMC1gp\
Ey/r0E/nolRkiOH/ppenhnbj1BFHKRi/RdxttVWSHoMg9ilKADdz6nItm2HuEZ04\
tfIIbEs9yH4VdnWbfAbgfkZBHzY4rueXuo7xlnAWx14JMFuCT2WaVRmi6Sf8eUDP\
BB3sGjE2yPWSaQUDp6kMx1V8whES0jiW7CLDOSlU6fW0T6lLgaRZ9h49Rh3jcV3I\
5ZZg1ogD0YNKgjdgnzHuFeGAZCB5fI5L+ndC8KXTKmC7shYN1adSIoWS3XgQiUHm\
ajpwFEIYOBE6/xI8QFU/F44j5EjFvfPq1k9zPEvi0SKV68Rl8JZ0X/SontVRQ/To\
gvYvftDWt32jACdv3vUk+QDpyyym+R7SCOKX/STlT3FDk/yrHMHQBzYO1KKhnVFv\
KzzZs0umsqDSGrYSLialPUJ+ZuXDTSelov+P5s200ZBAPjxYD6YIGiBsPKgHssVQ\
7GUlz1mxgOObQNVQjbrgdGwpdnYpY4YlsogtybI1QIbDtU/fIRPHHeWWBOW+iZ1w\
9/XHnSyP0EFyzk+bYz21lRxJHLBsfWehshM3Mwqs+A3cmwzUyGQCeT8XV+mKe7y1\
VAiqVVQQjhjHCoU+N4XkdM8pUzR0NkC33amlV68e1EDSD0XAtLZCUrJfil18X9/R\
hWkiDVElMOPwmsp3nJ9jU3UQRQ7Yf97V3oLw== pbz@ogopogo.biz_hostca_bzhosts
EOF
```

L'autorité ci-dessus authentifie actuellement les hôtes suivants:

Authority: pbz@ogopogo.biz (tag bzhosts)

- mamey.ogopogo.biz
- repo.ogopogo.biz
- guanabana.bernatchez.net
- relay.bernatchez.net
- relay.ogopogo.biz
- repo.bernatchez.net

Authentification du client:

Générez une paire de clés privée/publique avec cette commande :

```
/usr/bin/ssh-keygen -b 4096 -t rsa -C hote_but -f hote_but
```

Remplacez « hote » ci-dessus par le nom de l'ordinateur client et « but » par une indication de l'utilisation de la clé.

Par exemple :

```
ssh-keygen -b 4096 -t rsa -C pierreportable_telecommande -f pierreportable_telecommande
```

Envoyez un courriel à l'autorité de signature pour demander un certificat signé. Joignez la clé publique générée ci-dessus à ce courriel.

L'autorité de certification joindra un certificat vous autorisant l'accès dans un courriel de réponse.

Placez ce certificat dans le même répertoire que la clé privée.

Lorsque vous chargez la clé privée dans votre agent SSH, le certificat est également chargé.

Exemple:

```
ssh-add lancelaptop_jobberuser
```

Vous devrez répondre avec la phrase secrète correcte pour votre clé et vous obtiendrez un message similaire à celui-ci:

> Enter passphrase for pierreportable_telecommande:
>
> Identity added: pierreportable_telecommande (pierreportable_telecommande) Certificate added: pierreportable_telecommande-cert.pub (pierreportable_telecommande)

PROBLÈME:

> Sous Ubuntu, l'utilitaire ssh-add ne parvient pas à charger les fichiers de certificat. Ce problème ne se produit pas lorsque l'agent ssh est le véritable agent ssh, mais lorsqu'il est implémenté par gnome-keyring.
>
> La solution consiste à cesser d'utiliser le composant ssh de gnome-keyring.
>
> Étant donné que le processus d'initialisation démarre un véritable agent ssh, puis lance gnome-keyring-ssh.desktop, qui neutralise AUTH_SOCKET pour prendre le relais, nous revenons à l'agent ssh d'origine en désactivant gnome-keyring-ssh.desktop.

Désactiver gnome-keyring-ssh.desktop :

```
cd /etc/xdg/autostart/
sudo emacs gnome-keyring-ssh.desktop
```

Ajoutez la ligne suivante au fichier et gardez-le

```
X-GNOME-Autostart-enabled=false
```

Puis redémarrez l'ordinateur