Serveur

Fichier de configuration

sshd_config

```

```

Client

Fichier de configuration

ssh_config

```

```

Ajouter ". .sh_run_ssh-agent" au fichier .profile (et/ou "source .sh_run_ssh-agent" au fichier .zshrc).

.sh_run_ssh-agent

```
# Author: Maxime DERCHE <maxime@mouet-mouet.net>
# Date: January 8th 2014
# Based on: * /etc/X11/xinit/xinitrc on OpenBSD
#           * <http://mah.everybody.org/docs/ssh>
# With help from the #OpenBSD.fr people. Thanks. ,-)
# Use case: workstation

ssh_agent_path=/usr/bin/ssh-agent
ssh_add_path=/usr/bin/ssh-add
key_lifetime="2h"
ecdsa_key=$HOME/.ssh/id_ecdsa
rsa_key=$HOME/.ssh/id_rsa

# First, we see if ssh-agent is already running or not.
if [ -z "$SSH_AGENT_PID" ] && [ -x "$ssh_agent_path" ];
then
        eval `$ssh_agent_path -s -t $key_lifetime`
fi

# Then we load the keys in ssh-agent.
if [ -x "$ssh_add_path" ];
```

```
then
        if [ -f $ecdsa_key ];
        then
                $ssh_add_path -t $key_lifetime $ecdsa_key < /dev/null
        fi
        if [ -f $rsa_key ];
        then
                $ssh_add_path -t $key_lifetime $rsa_key < /dev/null
        fi
fi
```

.sh_run_ssh-agent

```
# Author: Maxime DERCHE <maxime@mouet-mouet.net>
# Date: January 9th 2014
# Based on: * /etc/X11/xinit/xinitrc on OpenBSD
#           * <http://mah.everybody.org/docs/ssh>
# With help from the #OpenBSD.fr people. Thanks. ,-)
# Use case: SSH gateway

ssh_agent_path=/usr/bin/ssh-agent
ssh_add_path=/usr/bin/ssh-add
ssh_env="$HOME/.ssh/environment"
key_lifetime="4h"
ecdsa_key=$HOME/.ssh/id_ecdsa
rsa_key=$HOME/.ssh/id_rsa

if [ -z `pgrep -u "$LOGNAME" ssh-agent` ] && [ -x "$ssh_agent_path" ];
then
        $ssh_agent_path -s -t $key_lifetime > $ssh_env
        chmod 600 $ssh_env
fi

eval `cat $ssh_env`

if [ -x "$ssh_add_path" ];
then
        if [ -f $ecdsa_key ] && [ -z `"$ssh_add_path" -l | grep ECDSA`
];
        then
                $ssh_add_path -t $key_lifetime $ecdsa_key < /dev/null
        fi
        if [ -f $rsa_key ] && [ -z `"$ssh_add_path" -l | grep RSA` ];
        then
                $ssh_add_path -t $key_lifetime $rsa_key < /dev/null
        fi
fi
```

Configuration

Génération de paires de clefs:

- ed25519 :

```
$ ssh-keygen -t ed25519 -C "$(whoami)@$(hostname):$(date +%F)"
```

- RSA :

```
$ ssh-keygen -t rsa -b 8192 -C "$(whoami)@$(hostname):$(date +%F)"
```

- ECDSA :

```
$ ssh-keygen -t ecdsa -b 521 -C "$(whoami)@$(hostname):$(date +%F)"
```

Bibliographie

- site web officiel : http://www.openssh.org/ ;
- Wikipedia : http://en.wikipedia.org/wiki/OpenSSH / http://fr.wikipedia.org/wiki/OpenSSH ;
- https://wiki.archlinux.org/index.php/SSH_Keys
- https://wiki.archlinux.org/index.php/SFTP-chroot
- etc.

From:
http://www.mouet-mouet.net/ - **mouet-mouet !**

Permanent link:
http://www.mouet-mouet.net/doku.php?id=maxime:openbsd:docs:openssh

Last update: **2021/10/08 00:17**