

ALOHA LOAD BALANCER

ACCES SSH PAR CLEF PUBLIQUE

"APPNOTE" #0048 — ACCES SSH PAR CLEF PUBLIQUE

Cette note vous montrera comment accéder à l'Aloha en utilisant une clef publique.

OBJECTIF

Etre capable de se connecter à un Aloha à distance sans se avoir de mot de passé à saisir.

DIFFICULTÉ



VERSIONS CONCERNEES

V 3.6 et après.

DIAGRAMME

Accès standard SSH:



CONTEXTE

Le client utilise SSH pour se connecter à l'Aloha.

CONFIGURATION COTE CLIENT

SOUS LINUX

A faire uniquement si vous n'avez pas encore de clef publique.

1. Générer la paire de clef avec la commande `ssh-keygen -t rsa`:

```
user:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
9a:1a:37:da:11:0b:9f:0e:fb:e8:b4:93:46:f8:3d:ec user@krusty
The key's randomart image is:
+--[ RSA 2048]-----+
|
|
|
|
|   . . . S
|  . . o *
|   o++X
|  .=%+o
|   oB+E.
+-----+
```

Puisque notre but est d'arriver à se connecter à l'Aloha sans avoir de mot de passé à saisir, nous ne saisissons pas de passphrase.



Il faut garder à l'esprit que si quelqu'un arrive à voler votre clef privée, alors il aura aussi accès à l'Aloha sans mot de passe.

2. Copier la clef publique sur l'Aloha:

```
user:~$ scp .ssh/id_rsa.pub admin@192.168.0.100:/tmp/
admin@192.168.0.100's password:
id_rsa.pub                               100% 393      0.4KB/s   00:00
```

CONFIGURATION ALOHA

1. Se connecter à l'Aloha en SSH :

```
user:~$ ssh admin@192.168.0.100
admin@192.168.0.100's password:
admin@ALOHA1:~$
```

2. Passer root:

```
admin@ALOHA1:~$ root
```

3. Copier la clef publique de l'utilisateur dans le repertoire des clef publique autorisées:

```
root@ALOHA1:~# cp /tmp/id_rsa.pub /etc/ssh/authorized_keys/admin
```

Si le fichier existe déjà, vous devez concaténer la nouvelle clef à la fin du fichier:

```
root@ALOHA1:~# cat /tmp/id_rsa.pub >> /etc/ssh/authorized_keys/admin
```