

Installation de la clef SSH OVH

Introduction

Afin d'intervenir sur un serveur dédié sans avoir à connaître votre mot de passe root, nous installons par défaut une clef SSH. Seuls les personnels d'OVH habilités peuvent utiliser cette clef. Ceci ne représente donc pas une faille de sécurité, bien au contraire. Grâce à cette clé, OVH possède les droits **root** sur votre serveur sans connaître votre mot de passe root et peut ainsi diagnostiquer rapidement un problème sur votre machine. Dans le cas d'une demande d'intervention en **infogérance (InfogéranceS)**, nous avons impérativement besoin d'un accès via cette clef SSH. Dans le cas d'une attaque lancée depuis votre machine (même à votre insu), cette clef est notre seul moyen d'accéder rapidement au serveur et de couper l'attaque.

Si pour des raisons de sécurité et/ou de confidentialité, vous souhaitez empêcher à OVH d'accéder à votre serveur, vous pouvez désactiver la clef SSH. Mais pour les raisons citées ci dessus, cette manipulation est **vivement déconseillée**.

Procédure

Si jamais cette clef n'était pas/plus installée sur votre serveur, voici le moyen de l'installer :

- Connectez-vous sur votre serveur en ligne de commande (SSH) sous l'utilisateur root. Voir guide : Comment se connecter sur le serveur en SSH ?

ou

- Utilisez l'interface Commande shell de Webmin : <https://nsXXXX.ovh.net:10000/shell/>
- Puis tapez la commande suivante :

```
wget ftp://ftp.ovh.net/made-in-ovh/cle-ssh-public/installer_la_cle.sh -O installer_la_cle.sh ; sh
installer_la_cle.sh
```

Si tout s'est bien passé, un fichier **authorized_keys2** a normalement été créé. Il contient des lignes de cette forme:

```
root@julien root# cat /root/.ssh/authorized_keys2
from="XX.XX.XX.XX" ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIE... root@cache.ovh.net
from="::ffff:XX.XX.XX.XX" ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIE... root@cache.ovh.net
```

Résolution des problèmes

Même si la clef est correctement installée, il est possible que nos services ne puissent pas se connecter sur votre serveur. Ceci se traduit pas un accès refusé ou une demande du mot de passe root. (OVH ne détient pas votre mot de passe root, d'où l'utilité de la clef). Il vous faut alors vérifier les points suivants :

1. Est-ce que le fichier **/root/.ssh/authorized_keys2** est bien là ? (c'est à dire "Est ce que la clef SSH est bien installée?"),
2. Est-ce que le serveur SSH est correctement configuré pour accepter les connexions **root** ? Pour cela, vous devez vérifier les paramètres suivants dans le fichier **/etc/ssh/sshd_config**:

```
PermitRootLogin yes
'AuthorizedKeysFile' .ssh/authorized_keys2
```

UsePAM yes

Puis redémarrer le serveur SSH si nécessaire.

3. Est-ce que le répertoire de base de l'utilisateur **root** est bien **/root** ? Pour cela, vous devez vérifier la configuration de l'utilisateur root :

```
root@julien /# grep root /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Le 6ème élément de la ligne (les éléments sont séparés par des ":") doit être /root

Si malgré cela, l'accès via la clef SSH est toujours impossible, vous pouvez demander l'intervention de notre service d'infogérance pour reconfigurer l'accès. Étant donné qu'il faudra alors accéder "physiquement" à votre serveur, cette intervention sera facturée 70 euros HT (voir **InfogéranceS**).

Désactivation de la clef

Si vous souhaitez que OVH ne soit plus en mesure de se connecter en SSH sur votre machine, vous avez la possibilité de désactiver la clé SSH. Cependant, cette manipulation est **vivement déconseillée** car OVH ne sera alors plus en mesure d'intervenir sur votre machine pour un diagnostic, un problème de hack ou une intervention en infogérance. Un problème qui aurait pu être résolu rapidement grâce à un accès SSH via cette clef pourra alors atteindre des délais beaucoup plus importants.

Pour désactiver la clef SSH utilisée par OVH, il vous suffit d'éditer le fichier **authorized_keys2** et de commenter (à l'aide du caractère #) ces deux lignes:

```
root@julien root# cat /root/.ssh/authorized_keys2
```

1. from="XX.XX.XX.XX" ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIE.... root@cache.ovh.net
2. from="::ffff:XX.XX.XX.XX" ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIE....
root@cache.ovh.net