Comment ajouter une clé publique SSH au serveur

L'authentification par clé publique vous permet d'accéder à un serveur via SSH sans mot de passe. Voici deux méthodes pour copier la clé publique ssh sur le serveur.

L'authentification par clé publique vous permet d'accéder à un serveur via SSH sans mot de passe. Voici deux méthodes pour copier la clé publique ssh sur le serveur.

Je pense que vous comprenez le concept de base de SSH. Votre serveur Linux a activé SSH. Vous avez généré des clés ssh sur votre ordinateur personnel. Vous souhaitez maintenant télécharger votre clé publique sur les clés autorisées du serveur afin de pouvoir y accéder sans taper à tout moment le mot de passe de votre compte.

Ce didacticiel rapide vous montre deux méthodes pour ajouter une clé SSH publique au serveur.

Exigences

Avant de voir cela, soyons clairs sur ce que vous devriez déjà avoir :

1. Votre serveur de destination devrait avoir ssh activé
2. Vous devriez avoir généré des clés ssh publiques et privées (utilisez simplement la commande ssh-keygen -t rsa)
3. Vous devez disposer d'un compte utilisateur et d'un mot de passe sur le serveur. Même le compte root fera l'affaire.
4. Vous devez connaître l'adresse IP du serveur

Maintenant que vous êtes assuré des quatre exigences ci-dessus, voyons comment utiliser l’authentification par clé publique.

L'authentification se fait par base d'utilisateurs, de sorte que la clé publique va au domicile de l'utilisateur prévu.

Méthode 1 : copier automatiquement la clé ssh sur le serveur

La première méthode consiste à copier la clé publique de son ordinateur personnel dans la liste des clés autorisées sur le serveur distant.

Ici, je suppose que vous avez pu vous connecter au serveur distant en utilisant ssh user_name@ip_of_server. Il vous demande le mot de passe de votre compte et vous entrez sur le serveur.

Si vous ajoutez votre clé publique au serveur, vous devriez pouvoir vous connecter sans saisir le mot de passe à tout moment.

OpenSSH fournit un outil pratique appelé ssh-copy-id pour copier les clés publiques ssh sur des systèmes distants. Il crée même les répertoires et fichiers requis.

Comme je l'ai mentionné plus tôt, vous devez connaître le nom d'utilisateur et le mot de passe du serveur auquel vous souhaitez accéder via l'authentification par clé publique.

```
ssh-copy-id -i ~/.ssh/id_rsa.pub YOUR_USER_NAME@IP_ADDRESS_OF_THE_SERVER
```

Lorsque vous y êtes invité, entrez le mot de passe de votre compte utilisateur sur le serveur distant. Votre clé publique doit être automatiquement copiée dans le dossier approprié sur le serveur distant.

J'ai utilisé ~/.ssh/id_rsa.pub car c'est l'emplacement par défaut de la clé publique ssh. Si vous l'avez à un autre endroit, vous devez l'utiliser dans la commande ci-dessus.

Méthode 2 : copiez manuellement la clé publique SSH sur le serveur

La première méthode avait l'action du côté utilisateur. Disons que vous êtes l'administrateur système et que votre serveur n'autorise pas la connexion SSH via un mot de passe. La seule façon d'accéder au serveur consiste à utiliser l'authentification par clé publique SSH.

Dans un tel cas, vous pouvez demander à l'utilisateur final de fournir sa clé publique. Maintenant, ce que vous pouvez faire est de créer le répertoire .ssh/authorized_keys, puis de copier la clé publique ici.

Laissez-moi vous montrer les étapes.

Étape 1 : Obtenez la clé publique

Demandez à l'utilisateur final de fournir la clé publique en tapant la commande suivante :

```
cat ~/.ssh/id_rsa.pub
```

Il affichera une longue chaîne aléatoire commençant par ssh-rsa :

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQ3GlJzTX7J6zsCrywcjAM/7Kq3O9ZIvDw2OFOSXAFVqilSFNkHlef
m1iMtPeqsIBp2t9cbGUf55xNDULz/bD/4BCV43yZ5lh0cUYuXALg9NI29ui7PEGReXjSpNwUD6ceN/78YOK
41KAcecq+SS0bJ4b4amKZIJG3JWm49NWvoo0hdM71sblF956IXY3cRLcTjPlQ84mChKL1X7+D645c7O4Z
1N3KtL7l5nVKSG81ejkeZsGFzJFNqvr5DuHdDL5FAudW23me3BDmrM9ifUmt1a00mWci/1qUlaVFft085yv
Vq7KZbF2OP2NQACUkwfwh+iSTP username@hostname

Vous pouvez obtenir ce texte par e-mail ou via des outils de messagerie. Normalement, cela ne devrait pas poser de problème.

Étape 2 : Créez le répertoire ssh dans le répertoire personnel de l'utilisateur (en tant qu'administrateur système)

Gardez à l'esprit que vous devez créer ces nouveaux répertoires et fichiers dans le répertoire personnel de l'utilisateur final, et non dans le vôtre (root/sysadmin).

```
   mkdir -p /home/user_name/.ssh && touch
/home/user_name/.ssh/authorized_keys
```

Ouvrez maintenant ce fichier /home/user_name/.ssh/authorized_keys avec un éditeur de texte comme Vim et ajoutez ici la clé publique de l'utilisateur :

```
   nano /home/user_name/.ssh/authorized_keys
```

Enregistrez et fermez le fichier. C'est presque prêt.

Étape 3 : définissez l'autorisation appropriée sur le fichier

Avoir l'autorisation de fichier appropriée sur le fichier ssh est très important, sinon vous verrez des erreurs telles que Autorisation refusée (clé publique).

Tout d'abord, assurez-vous de définir les autorisations de fichiers correctes :

chmod 700 /home/user_name/.ssh && chmod 600 /home/user_name/.ssh/authorized_keys

Vous avez créé ces fichiers avec root ou avec vos propres comptes administrateur pour un autre utilisateur. Vous devez remplacer la propriété par l'utilisateur :

```
chown -R username:username /home/username/.ssh
```

Maintenant que c'est fait, vous pouvez demander à l'utilisateur final de se connecter au serveur.

Faites-moi savoir si vous rencontrez des problèmes ou si vous avez des suggestions sur ce sujet.