DOCUMENTATION SUR L'UTILISATION D'OPENSSH SERVER POUR LES UTILISATEURS DE MANJARO LINUX

INTRODUCTION À OPENSSH SERVER

OpenSSH Server est un serveur SSH utilisé pour sécuriser les communications réseau. Il permet des connexions sécurisées depuis un client SSH à un serveur SSH, facilitant des tâches telles que le transfert de fichiers, la gestion à distance, et l'exécution de commandes à distance sur des machines Linux, y compris Manjaro.

INSTALLATION D'OPENSSH SERVER

1. **Installer OpenSSH Server** :

   ```
   sudo pacman -S openssh
   ```

2. **Activer le service SSH** : Pour que le serveur SSH démarre automatiquement au démarrage :

   ```
   sudo systemctl enable sshd
   ```

3. **Démarrer le service SSH immédiatement** :

   ```
   sudo systemctl start sshd
   ```

CONFIGURATION DE BASE D'OPENSSH SERVER

- **Configurer OpenSSH Server** : La configuration principale se trouve dans `/etc/ssh/sshd_config`. Vous pouvez éditer ce fichier pour changer les paramètres comme le port, les permissions, et les options d'authentification.

- **Changer le port** : Pour des raisons de sécurité, il est souvent conseillé de changer le port SSH par défaut (22). Modifiez la ligne `Port` dans `/etc/ssh/sshd_config`.

- **Redémarrer le service après changement de configuration** :

```
sudo systemctl restart sshd
```

CONNEXION À OPENSSH SERVER

- **Se connecter depuis un client SSH** : Utilisez la commande suivante depuis un client SSH :

```
ssh utilisateur@adresse_ip_serveur
```

Remplacez `utilisateur` par votre nom d'utilisateur sur le serveur Manjaro et `adresse_ip_serveur` par l'adresse IP du serveur.

SÉCURISATION D'OPENSSH SERVER

- **Utiliser des clés SSH au lieu de mots de passe** : La connexion par clé SSH est plus sécurisée que l'authentification par mot de passe. Générez une paire de clés SSH sur le client et ajoutez la clé publique dans le fichier `~/.ssh/authorized_keys` sur le serveur.

- **Désactiver l'authentification par mot de passe** : Après avoir configuré l'authentification par clé, désactivez l'authentification par mot de passe en modifiant `PasswordAuthentication` en `no` dans `/etc/ssh/sshd_config`.

- **Mettre à jour régulièrement** : Gardez OpenSSH Server à jour avec les dernières sécurités en exécutant régulièrement `sudo pacman -Syu`.

DÉPANNAGE

- **Vérifier le statut du service SSH** :

```
sudo systemctl status sshd
```

- **Vérifier les logs** : Les logs de SSH peuvent fournir des informations utiles en cas de problème. Ils se trouvent généralement dans `/var/log/auth.log`.

CONCLUSION

OpenSSH Server est un outil essentiel pour la gestion à distance sécurisée sous Manjaro Linux. Sa configuration et sa gestion requièrent une attention particulière en termes de sécurité, mais une fois configuré correctement, il offre une méthode robuste et sécurisée pour l'accès à distance et le transfert de fichiers.