Services ssh et sftp

Debian

Pour installer le paquet :

```
# apt install openssh-server
```

Pour permettre à l'utilisateur 'root' de se connecter directement via ssh, modifier le fichier de configuration `/etc/ssh/sshd_config` afin d'obtenir :

```
"PermitRootLogin yes"
```

Une fois le fichier modifié, redémarrer le service :

```
# systemctl restart ssh
```

Fedora

Pour installer le paquet :

```
# dnf install openssh-server
```

Le service doit être activé au démarrage de la machine (et démarré à l'instant) :

```
# systemctl enable --now sshd
```

Pour se connecter via le terminal à un hôte distant :

```
$ ssh user@IP
```

Pour naviguer dans une arborescence distante via le gestionnaire de fichiers :

File Manager > Autres emplacements > Connection à un serveur

La syntaxe est :

```
sftp://user@IP
```

Lors de la première connexion à une machine distante, un avertissement concernant l'authenticité de la machine distante est affiché. Les empreintes (*fingerprint*) de la clef publique de cette machine sont affichées car la clef publique n'est pas encore connue. Répondre 'yes' pour se connecter.

Accepter la connexion ajoute un entrée dans le fichier 'known_hosts' du dossier caché '.ssh'.
Ce dossier caché se trouve dans le dossier personnel de l'utilisateur initiant la connexion.
Cette entrée consiste en une ligne associant l'adresse IP à la clef publique de la machine distante.

Si d'aventure vous vous connectiez sur une nouvelle machine disposant de la même adresse IP, le client ssh refusera la connexion (même IP mais clef publique différente).
Pour autoriser la connexion malgré tout, supprimer la ligne concernant l'ancienne machine dans le fichier 'known_hosts'.