Installation d'OpenSSH Server

BTS SIO - Option SISR
Étudiant : [Votre nom]
Date : Mars 2026
Procédure rapide : Installation et configuration OpenSSH

Prérequis

- Système Debian 12 ou Ubuntu Server 24.04 fonctionnel
- Connexion Internet active
- Accès root ou sudo
- Système à jour

Installation

1. Mise à Jour du Système

sudo apt update
sudo apt upgrade -y

2. Installation d'OpenSSH Server

sudo apt install openssh-server -y

Paquets installés :

- `openssh-server` : Serveur SSH
- `openssh-client` : Client SSH (si absent)
- Dépendances nécessaires

3. Vérification de l'Installation

Vérifier le statut du service SSH

sudo systemctl status ssh

Sortie attendue :
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service)
Active: active (running)

4. Activation au Démarrage

Activer SSH au démarrage automatique

sudo systemctl enable ssh

Test de Connexion

Vérifier l'Adresse IP du Serveur

Afficher l'IP du serveur

ip addr show

Identifier l'adresse IP : `192.168.x.x` ou `10.x.x.x`

Connexion SSH Locale (Test)

Test de connexion depuis le serveur lui-même

ssh localhost

Première connexion :

- Message : "Are you sure you want to continue connecting?"

- Répondre : `yes`
- Saisir le mot de passe utilisateur

Connexion SSH à Distance

Depuis une autre machine (Windows, Mac, Linux) :

ssh utilisateur@IP_serveur

Exemple :
ssh admin@192.168.1.50

Avec un port spécifique (si modifié) :
ssh -p 2222 utilisateur@IP_serveur

Configuration de Base (Optionnel)

Fichier de Configuration Principal

Emplacement : `/etc/ssh/sshd_config`

Éditer la configuration SSH

sudo nano /etc/ssh/sshd_config

Options de Sécurité Recommandées

Paramètre	Valeur recommandée	Description
Port	22 (ou 2222)	Port d'écoute SSH
PermitRootLogin	no	Désactiver connexion root
PasswordAuthentication	yes	Autoriser mot de passe
PubkeyAuthentication	yes	Autoriser clés SSH

Table 1: Paramètres de sécurité SSH

Exemple de modification :

Désactiver connexion root directe (sécurité)

PermitRootLogin no

Changer le port (optionnel)

Port 2222

Appliquer les Modifications

Redémarrer SSH après modification config

sudo systemctl restart ssh

Vérifier le statut

sudo systemctl status ssh

Commandes Utiles

Action	Commande
Démarrer SSH	sudo systemctl start ssh
Arrêter SSH	sudo systemctl stop ssh
Redémarrer SSH	sudo systemctl restart ssh
Statut du service	sudo systemctl status ssh
Activer au boot	sudo systemctl enable ssh
Désactiver au boot	sudo systemctl disable ssh
Voir logs SSH	sudo journalctl -u ssh -n 50
Connexion distante	ssh user@IP

Table 2: Commandes de gestion OpenSSH

Fichiers Importants

Fichier	Description
/etc/ssh/sshd_config	Configuration serveur SSH
/etc/ssh/ssh_config	Configuration client SSH
/var/log/auth.log	Logs authentification
~/.ssh/authorized_keys	Clés publiques autorisées

Table 3: Fichiers de configuration SSH

Dépannage Rapide

SSH ne démarre pas

Vérifier les erreurs de configuration

sudo sshd -t

Voir les logs détaillés

sudo journalctl -u ssh -n 100

Impossible de se connecter

Vérifications :

- Service SSH actif : `sudo systemctl status ssh`
- Firewall autorise port 22 : `sudo ufw status`
- IP correcte : `ip addr show`
- Nom d'utilisateur et mot de passe valides

Autoriser SSH dans le Firewall (si UFW actif)

Autoriser SSH dans UFW

sudo ufw allow ssh

Ou autoriser port spécifique

sudo ufw allow 2222/tcp

Checklist Validation

- [ ] apt update && apt upgrade exécuté
- [ ] apt install openssh-server -y terminé
- [ ] systemctl status ssh = active (running)
- [ ] systemctl enable ssh exécuté
- [ ] IP serveur identifiée : ip addr show
- [ ] Test connexion locale : ssh localhost fonctionne
- [ ] Test connexion distante : ssh user@IP fonctionne
- [ ] Configuration sécurité (optionnel) :
  - [ ] PermitRootLogin no configuré
  - [ ] Port modifié si souhaité
  - [ ] SSH redémarré après modification
- [ ] Firewall autorise SSH (si UFW actif)

Temps total : 5 minutes

OpenSSH opérationnel ✅