# Documentation d’installation – Projet Tunnel (Technicien)

Cette procédure décrit les étapes à exécuter pour installer le projet Tunnel sur deux machines distinctes :

* **Machine Client**
* **Machine Serveur**

Il est important de suivre les étapes dans l’ordre indiqué.

## 1. Pré-requis

### 1. Ports à libérer Assurez-vous que les ports nécessaires soient libres et ouverts dans le pare-feu : - Machine Client : 8080, 2200 **-** Machine Serveur : 2200, 2201

### 2. Installation et configuration de Docker

L’utilisateur doit pouvoir exécuter sudo (Linux) ou disposer des droits d’écriture (Windows).

#### **a) Sous Linux**

sudo apt update

sudo apt install -y docker.io  
  
Cette commande installe Docker et la version moderne de Docker Compose (v2).

#### **b) Sous Windows (Docker Desktop)**

1. Installer **Docker Desktop**.
2. Activer **WSL2** si l’installation le demande.
3. Créer les dossiers nécessaires pour stocker les logs et les messages :  
   C:\def\tunnel-logs et C:\def\messageStore
4. Partager des dossiers avec Docker Desktop (pour lui donner le droit de lecture et d’écriture) :  
   - Ouvrir **Docker Desktop → Settings → Resources → File Sharing**  
   - Vérifier que C:\ est coché, ou ajouter C:\def ou ajouter chacun des dossiers créés

## 2. Configuration des certificats

### 1. Générer le keystore sur le serveur (Machine Serveur) :

cd projetTunnel/Server/tunnelConfig

keytool -genkeypair \  
 -alias server \  
 -keyalg RSA -keysize 2048 \  
 -keystore keystore.jks \  
 -storepass changeit \  
 -keypass changeit \  
 -validity 365 \  
 -dname "CN=server-host, OU=IT, O=Example, L=Paris, C=FR" \  
 *-*ext "SAN=dns:server-host"

keytool -exportcert \  
 -alias server \  
 -keystore keystore.jks \  
 -storepass changeit \  
 -rfc \  
 -file cert.pem

### Copier le certificat généré tunnelConfig\cert.pem dans le répertoire tunnelConfig\ du client (Machine Client)

### Créer le truststore côté client et y importer le certificat (Machine Client) :

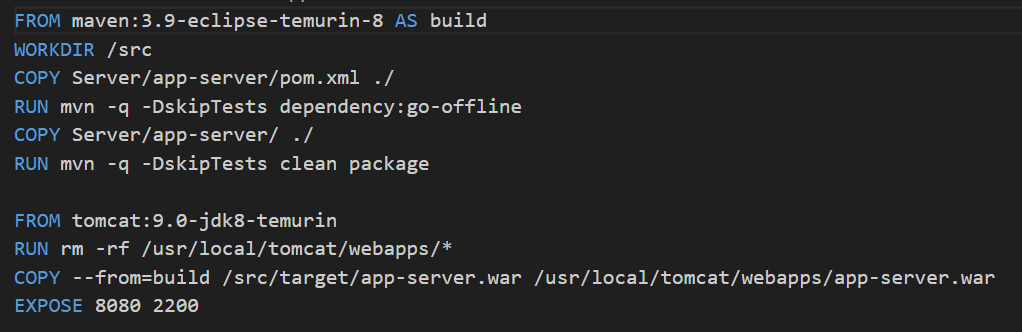
cd projetTunnel/Client/tunnelConfig

keytool -importcert \  
 -alias server \  
 -file cert.pem \  
 -keystore truststore.jks \  
 -storepass changeit \  
 -noprompt

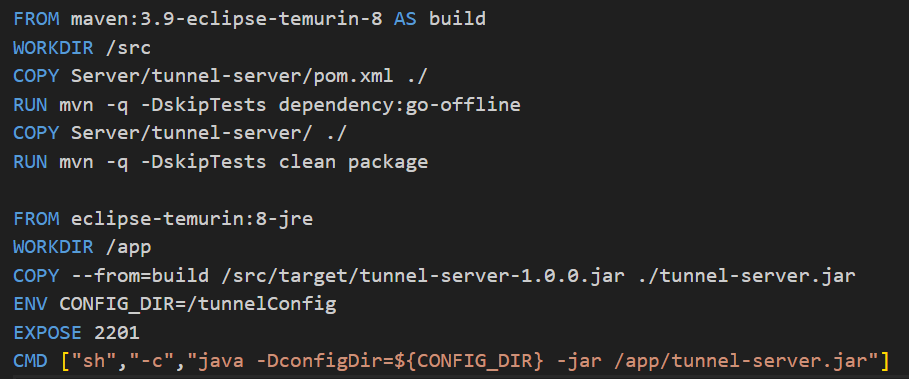
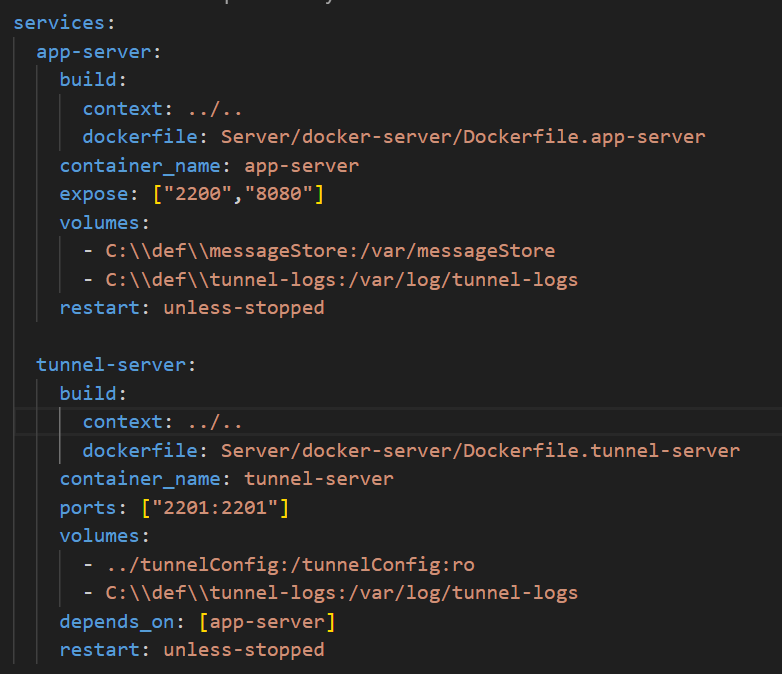
## Configuration des services

* **Côté Serveur :**

Pour configurer app-server et tunnel-server, vous devez changer les paramètres nécessaires dans les fichiers suivants, notamment les chemins des logs au besoin  :

* **App-Server :**
* Modifier **web.xml  
  **
* Modifier **Dockerfile.app-server**
* **Tunnel-Server:**
* Modifier **Server/tunnelConfig/parameters.xml**

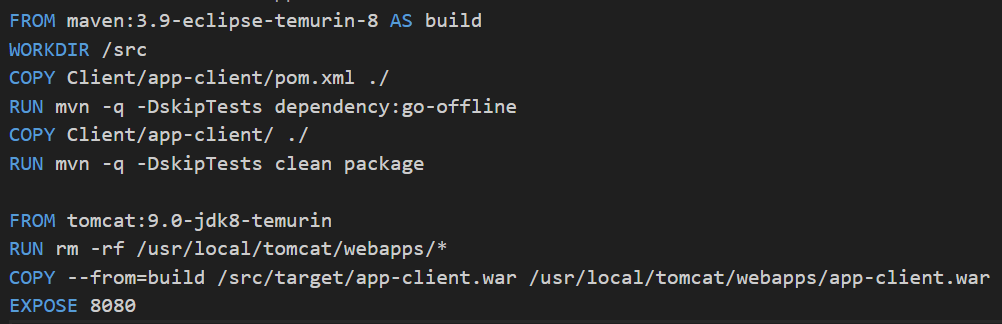
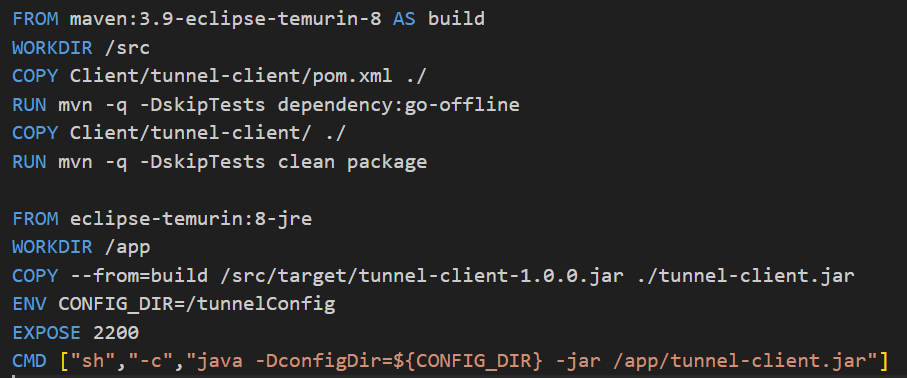
****

* Modifier **Dockerfile.tunnel-server**
* Puis pour le Docker compose côté server **compose.server.yaml :**
* **Côté Client :**

Pour configurer app-client et tunnel-client, vous devez changer les paramètres nécessaires dans les fichiers suivants, notamment :

* **App-Client :**
* Modifier **web.xml**

****

* Modifier **Dockerfile.app-client**
* **Tunnel-Client:**
* Modifier **Client/tunnelConfig/parameters.xml  
  **
* Modifier **Dockerfile.tunnel-client**
* ****Puis pour le Docker compose côté client **compose.client.yaml :**

**4. Déploiement**

* **Côté serveur :**

cd projetTunnel/Server/docker-server  
docker compose -f compose.server.yaml build  
docker compose -f compose.server.yaml up -d

* **Côté Client :**

cd projetTunnel/Client/docker-client  
docker compose -f compose.client.yaml build  
docker compose -f compose.client.yaml up -d

**5. Vérifications**

* **Conteneurs actifs :**  
  Exécuter la commande :docker ps  
  Il doit afficher tous les conteneurs lancés :
  + **Côté Serveur :** app-server (8080, 2200)  
     tunnel-server (2201)
  + **Côté Client :** app-client (8080)  
     tunnel-client (2200)
* **Interface Web**Depuis la machine Client : <http://localhost:8080/app-client/formulaire/index.html>  
  Remplir le formulaire et cliquer sur le bouton Générer et Envoyer le message*.*
* **Logs et Messages :**  
    
  + **Côté Serveur :**
* le répertoire C:\def\tunnel-logs contient logs\_app-server.log (actuellement vide car debug mis à 0, à changer si besoin) et logs\_tunnel-server.log
* Il est lié au volume /var/log/tunnel-logs à l’intérieur du conteneur, qu’on peut accéder par la commande :   
  docker exec -it tunnel-server cat /var/log/tunnel-logs/logs\_tunnel-server.log
* Pour voir la sortie standard d’un conteneur : docker log <Nom\_conteneur>
* **Les messages HL7 reçus** sont dans le dossier C:\def\messageStore, lié au volume /var/messageStore  
  + **Côté Client :**
* le répertoire C:\def\tunnel-logs contient logs\_app-client.log et logs\_tunnel-client.log
* Il est lié au volume /var/log/tunnel-logs à l’intérieur du conteneur, qu’on peut accéder par la commande :   
  docker exec -it tunnel-client cat /var/log/tunnel-logs/logs\_tunnel-client.log
* Pour voir la sortie standard d’un conteneur : docker log <Nom\_conteneur>