Documentation Technique : Installation et Configuration du Serveur WAPT sous Windows

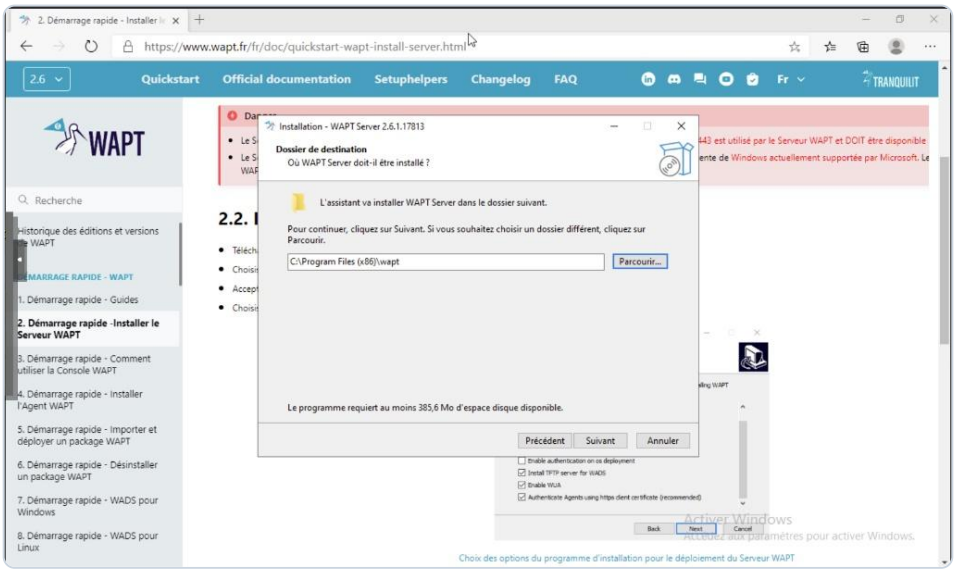
1. Introduction

Ce document constitue le dossier technique complet relatif au déploiement de l'infrastructure de gestion de parc **WAPT Server** en environnement Windows. Il retrace la chronologie exacte des opérations associées aux captures d'écran selon l'ordre d'implémentation spécifié.

2. Phase d'Installation du Serveur WAPT

Étape 2.1 : Sélection du répertoire de destination

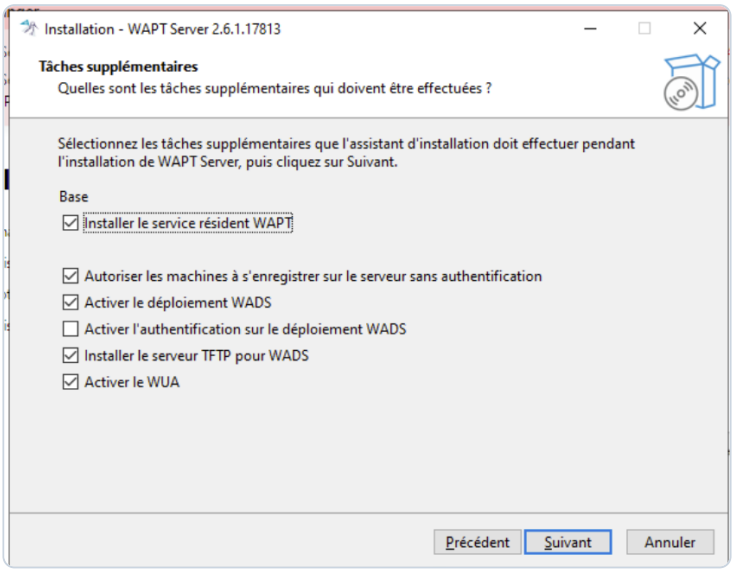
Au lancement de l'assistant d'installation Windows, le chemin racine par défaut est validé pour accueillir les fichiers binaires de l'application et les arborescences de configuration.



Étape 2.2 : Sélection des tâches d'infrastructure (WADS, TFTP, WUA)

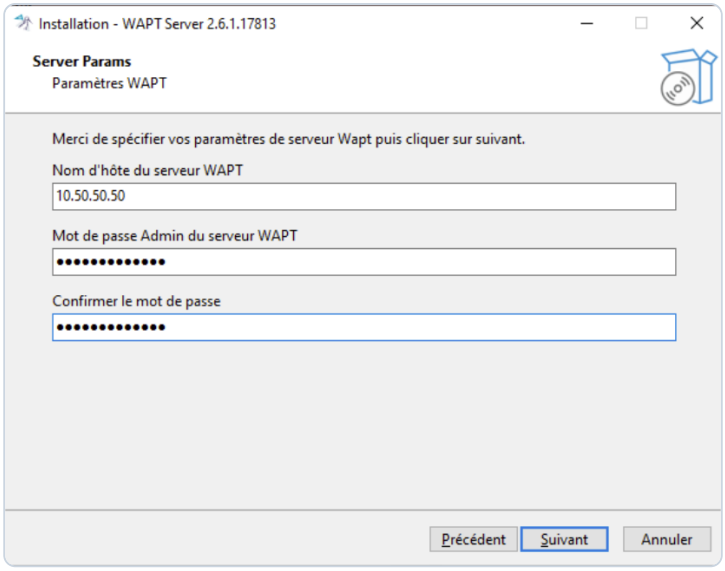
Les composants clés sont activés pour structurer les services du serveur : intégration du service résident, activation du système de déploiement d'images de systèmes d'exploitation **WADS** (avec

son serveur de distribution TFTP), et le module **WUA** pour le contrôle et l'approbation centralisés des mises à jour Windows.



Étape 2.3 : Paramétrage réseau fixe du serveur et mot de passe administrateur

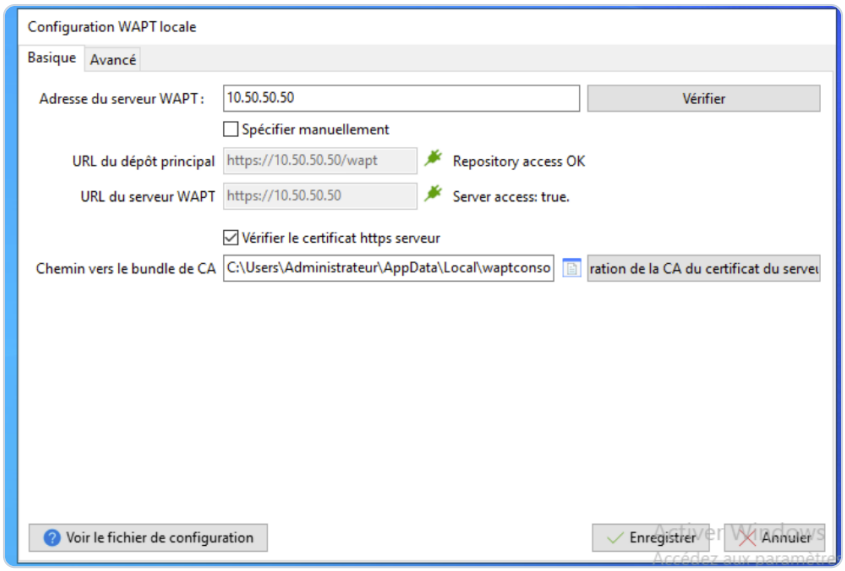
L'adressage réseau statique du serveur est renseigné sur l'IP fixe `10.50.50.50` pour sceller les communications. Le mot de passe associé au profil d'administration général (`admin`) est configuré simultanément.



3. Liaisons de la Console Locale et Sécurité Cryptographique

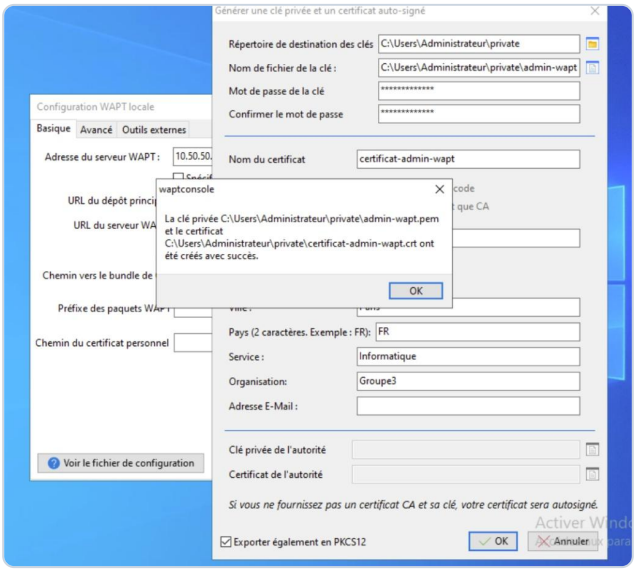
Étape 3.1 : Test de communication avec les dépôts HTTPS

La console d'administration locale interroge les liaisons réseau et valide les accès aux URL du dépôt principal et du serveur web Nginx sous-jacent.



Étape 3.2 : Génération de la clé et du certificat de signature de confiance

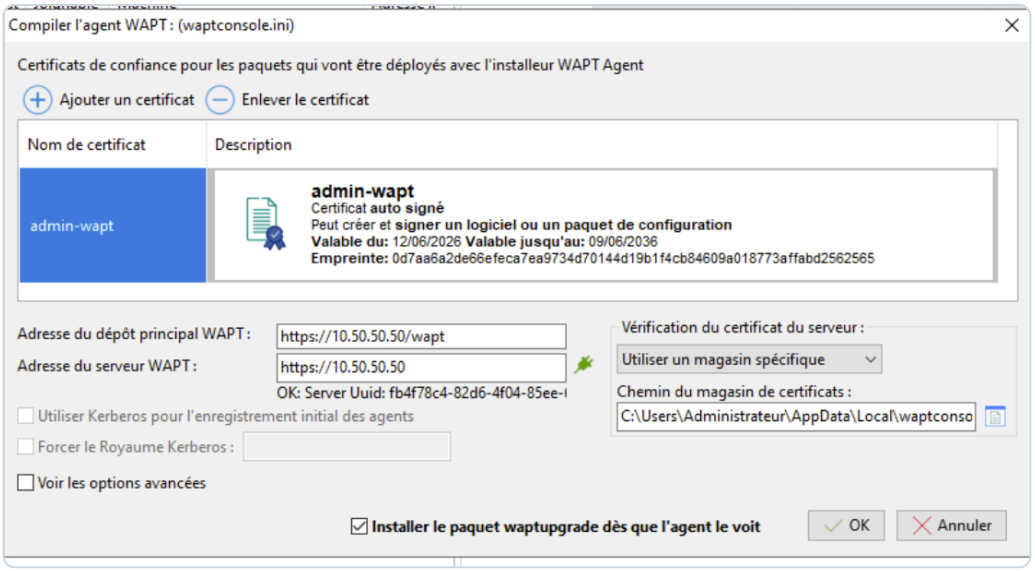
La sécurité asymétrique exige la création d'une entité de confiance. Un certificat d'administration `admin-wapt` et sa clé privée associée sont générés pour signer numériquement les futurs paquets applicatifs.



4. Assistant de Compilation de l'Agent Client

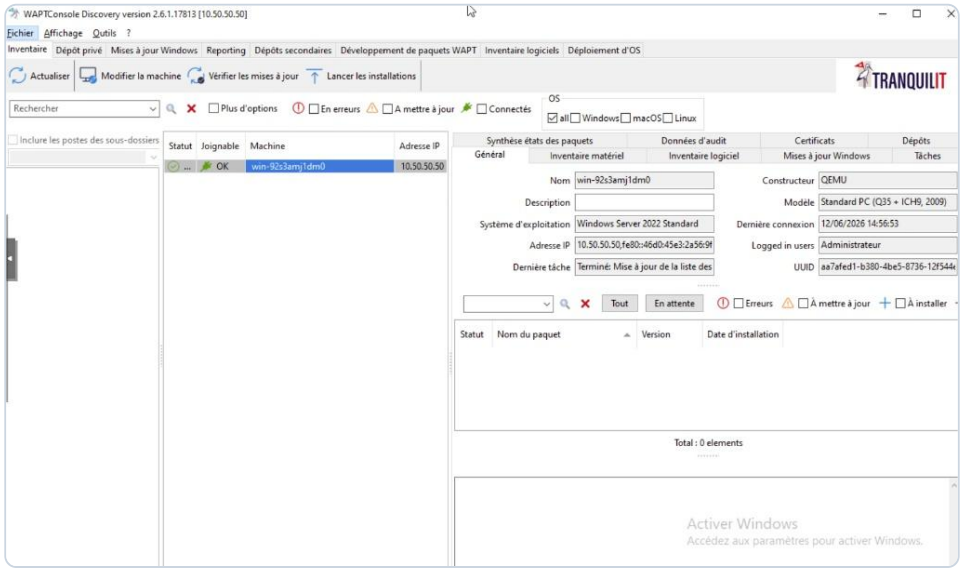
Étape 4.1 : Injection des règles de sécurité de l'organisation

Pour l'enrôlement des machines du parc, l'agent d'installation est généré depuis la console en y injectant de manière native le certificat public de confiance afin que les machines acceptent les ordres du serveur.



5. Supervision Centrale de l'Inventaire du Parc Informatique

Une fois déployé sur le réseau, l'agent force l'enregistrement de l'hôte. La console **WAPTConsole Discovery** offre une visibilité totale et en temps réel de l'inventaire matériel et logiciel des machines clientes.



Note d'exploitation (Invite de commandes CMD Windows) :

Sur les postes hôtes, l'exécution des mises à jour logicielles peut être forcée manuellement via :

```
wapt-get update && wapt-get upgrade
```