Documentation

WAPT

Entreprise Concept Hygiene.com

Eythan RONCIER-LEMEE
01/09/2025

Sommaire

1. Installation / Modification 4

1.1. Mise en place du serveur 4

1.1.1. Topologie 4

1.1.2. Ports réseau 4

1.1.3. Nom d'hôte 4

1.1.4. Réseau - Fichier hosts 4

1.1.5. Interface réseau 5

1.1.6. Locales 5

1.1.7. Heure et date 5

1.1.8. Certification 5

1.1.9. Configuration - Documentation WAPT 5

1.1.10. Paquets obligatoires 6

1.1.11. Dépôt - Ajout de la clé 6

1.1.12. Ajout du dépôt 6

1.1.13. Paquets supplémentaires 6

1.1.14. Post-conf 7

1.2. Mise en place de la console 10

1.2.1. Installation 10

1.2.2. Configuration 12

1.2.3. Clé 13

1.2.4. Licence 14

1.2.5. Création agent 14

2. Configuration déploiement serveur 16

2.1. Extinction des services 16

2.2. Accès au fichier waptserver.ini 16

2.3. Modification des valeurs 16

2.4. Mise en place du démarrage automatique 16

2.5. Lancement des services 17

2.6. Ajout des règles DHCP + configuration http 17

3. Déploiement 18

3.1. Modification de la configuration console 18

3.1.1. Paquets WinPE 18

3.2. Déploiement ISO 19

3.2.1. Récupération de l'image Windows 19

Pour Windows 11 / 10 19

Astuce navigateur (ISO direct sans outil) 19

3.2.2. Intégration de l'ISO 19

3.3. Configuration 20

3.3.1. Description du script XML 20

3.3.2. Phases du déploiement 24

3.3.3. Composants 24

3.3.4. Erreurs courantes 25

3.3.5. Pilotes 25

4. Magasin d'applications 26

4.1. Withsecure 26

4.1.1. Ajout du paquet 26

4.1.2. Configuration du paquet 26

4.1.3. Installation 27

4.2. Forticlient 27

4.2.1. Modification du fichier setup.py 28

4.2.2. Installation 29

5. Résolution de pannes 29

5.1. Rapport d'intervention 02/2026 29

5.1.1. Analyse Réseau 29

5.1.2. Analyse système 30

5.1.3. Configuration console & environnement WinPE 30

5.1.4. Conclusion 30

6. Procédures 30

6.1. Déploiement de poste 30

6.1.1. Prérequis 30
6.1.2. Paramétrage du BIOS (Poste Client) 31
6.1.2.1. Configuration de la connectivité (Modèles Wi-Fi) 31
6.1.2.2 Configuration du stockage (Mode AHCI) 32
6.1.3. Gestion du déploiement 32
6.1.3.1 Enregistrement de la machine 32
6.1.3.2 Lancement du déploiement 33
6.1.4. Finitions et Logiciels Complémentaires 33
6.2. Vente de poste 34
6.2.2.1. Configuration de la connectivité (Modèles Wi-Fi) 34
6.2.2.2 Configuration du stockage (Mode AHCI) 35
6.2.3. Gestion du déploiement 35
6.2.3.1. Enregistrement de la machine 35
6.2.3.2. Lancement du déploiement 36

1. Installation / Modification

1.1. Mise en place du serveur

1.1.1. Topologie

Dans la configuration actuelle de l'infra de test, voici les caractéristiques :

- Le nom FQDN est **srvwapt.test-wapt.local** ;
- Le nom court du Serveur WAPT est **srvwapt** ;
- Le suffixe DNS est **test-wapt.local** ;
- L'adresse IP est **10.35.1.11/24** ;

1.1.2. Ports réseau

Service	Ports	Protocoles	Justification
HTTP(S)	**443**	TCP	Canal principal sécurisé pour le transfert de paquets, l'inventaire, et la configuration. Requis pour la communication Console/Agent -> Serveur.
HTTP	**80**	TCP	Requis pour le service iPXE (utilisé lors du Déploiement d'OS) pour charger la configuration initiale, comme défini dans les scripts DHCP.
TFTP	**69**	UDP	Essentiel pour le déploiement d'OS (PXE). Utilisé pour le transfert des fichiers de démarrage initiaux (ex. snponly.efi) aux clients qui démarrent par le réseau.
Kerberos (AD)	**88**	UDP/TCP	Requis pour l'authentification auprès de l'Active Directory (AD) de la part du serveur WAPT, notamment pour l'enregistrement Kerberos des agents WAPT.

1.1.3. Nom d'hôte

Pour modifier le nom de la machine, on peut faire la commande suivante :
nano /etc/hostname afin d'écrire le FQDN du serveur WAPT à la place de l'entrée déjà présente.
Cela sera plus simple pour retrouver la machine avec un nom plus parlant.

1.1.4. Réseau - Fichier hosts

La modification du fichier etc/hosts sur le serveur WAPT est une étape essentielle de la configuration qui permet de garantir une stratégie de nommage et d'adressage réseau appropriée pour le bon fonctionnement de WAPT.

```
# /etc/hosts of the WAPT Server
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
10.35.1.10 srvwapt.test-wapt.local srvwapt
```

1.1.5. Interface réseau

Pour assurer la bonne communication entre les agents et le serveur, il est essentiel et fondamental :

```
# /etc/network/interfaces of the WAPT Server
auto eth0
iface eth0 inet static
    address 10.35.1.11
    netmask 255.255.255.0
    gateway 10.35.1.254
```

Il faudra ensuite redémarrer la machine pour s'assurer de la bonne prise en compte des modifications via la commande reboot et ajouter l'entrée DNS sur le serveur qui possède ce service.

1.1.6. Locales

Pour avoir des journaux non localisés et faciliter la recherche des erreurs courantes, il est nécessaire de définir les locales. Pour ce faire :

```
apt install locales-all -y
localectl set-locale LANG=en_US.UTF-8
localectl status
```

- Si cela affiche un **access denied** il faudra faire dpkg-reconfigure locales

Une fois les locales configurés, il faudra reboot.

1.1.7. Heure et date

À des fins de bonne connectivité, de traçabilité et de sécurité, il faudra vérifier la bonne synchronisation de la date et de l'heure. Pour ce faire, il faudra exécuter la commande timedatectl status, si la date et l'heure ne sont pas à jour il faudra se référer à la documentation.

1.1.8. Certification

Selon Debian.org Le paquet ca-certificates permet aux applications basées sur SSL de vérifier l'authenticité des connexions SSL. Ce qui sera particulièrement utile dans le cadre de l'accès en HTTPS à l'interface web de WAPT, mais aussi il pourra être utile lors de l'ajout de paquets dans le dépôt local. Pour procéder à l'installation :

```
apt install ca-certificates -y
```

1.1.9. Configuration - Documentation WAPT

Documentation WAPT

1.1.10.Paquets obligatoires

La commande suivante installe les utilitaires nécessaires pour sécuriser et préparer l'ajout du dépôt WAPT :

```
apt install apt-transport-https lsb-release gnupg wget -y
```

Paquet	Rôle dans l'installation de WAPT
apt-transport-https	Permet au gestionnaire de paquets apt de télécharger les paquets depuis des dépôts sécurisés utilisant le protocole **HTTPS** (nécessaire pour le dépôt Tranquil IT).
Lsb-release	Fournit un utilitaire pour identifier la distribution et la version du système d'exploitation (par exemple, "Debian 12"). Cette information est utilisée pour construire l'URL exacte du dépôt WAPT compatible.
Gnupg	Installe les outils GnuPG (GNU Privacy Guard) requis pour importer et vérifier la **clé GPG** du dépôt WAPT, assurant l'authenticité et l'intégrité des paquets téléchargés.
Wget	Outil de ligne de commande pour télécharger des fichiers (ici, utilisé pour récupérer la clé GPG de Tranquil IT).
-y	Argument de confirmation automatique, permettant une exécution non interactive de la commande.

1.1.11.Dépôt - Ajout de la clé

Il faut importer la clé publique GPG de Tranquil IT pour authentifier l'origine des paquets WAPT.

```
sudo bash -c 'wget -qO- https://wapt.tranquil.it/$(lsb_release -is)/tiswapt-pub-2026.gpg > /usr/share/keyrings/tiswapt-pub.gpg'
```

1.1.12.Ajout du dépôt

Pour obtenir les paquets provenant de provenant de Tranquil IT, il faudra ajouter ce dépôt :

```
echo "deb [signed-by=/usr/share/keyrings/tiswapt-pub.gpg] https://wapt.tranquil.it/$(lsb_release -is)/wapt-2.6/ $(lsb_release -c -s) main" > /etc/apt/sources.list.d/wapt.list
```

1.1.13.Paquets supplémentaires

Mettre à jour l'index des paquets et installer le Serveur WAPT ainsi que les outils de configuration associés, en mode non interactif pour garantir une installation fluide.

```
export DEBIAN_FRONTEND=noninteractive
apt update
apt install tis-waptserver tis-waptsetup -y
unset DEBIAN_FRONTEND
```

1.1.14.Post-conf

Enfin, pour configurer notre serveur WAPT, il faudra exécuter un script (postconf.sh) présent au chemin suivant : /opt/wapt/waptserver/scripts/postconf.sh
Qui se décompose de cette manière :

- Cliquez sur **Oui** pour exécuter le script de post-configuration.

```
Do you want to launch post configuration tool?
< yes > < no >
```

- Choisissez un mot de passe (si ce n'est pas déjà défini) pour le compte SuperAdmin du Serveur WAPT (longueur minimale de 10 caractères).

```
Please enter the wapt server password (min. 10 characters)
*****************
< OK > < Cancel >
```

- Confirmez le mot de passe.

```
Please enter the server password again:
*****************
< OK > < Cancel >
```

Choisissez le mode d'authentification pour l'enregistrement initial des Agents WAPT :

- Le choix n°1 : Permet d'enregistrer les ordinateurs sans authentification. Le Serveur WAPT enregistre tous les ordinateurs qui demandent à être enregistrés.

Sans certificat, il n'est pas possible de télécharger les paquets WAPT et d'interroger certains points d'accès du serveur WAPT. Cette méthode est recommandée si vous installez WAPT pour la première fois.

- Le choix n°2 (celle que j'ai choisi) : Active l'enregistrement initial basé sur Kerberos (vous pourrez l'activer aussi plus tard). Si vous rencontrez des problèmes lors de la mise à jour **OU** si vous utilisez un reverse proxy, cette méthode est recommandée pour le temps de la mise à jour.

Si vous voulez utiliser l'option 2 et que votre keytab Kerberos n'existe pas, le script postconf.sh le créera, après que vous aurez validé l'option 2. Il faudra lire la sous-partie **keytab**.

- Le choix n°3 : N'active pas le mécanisme d'authentification Kerberos pour l'enregistrement initial des hôtes équipés de WAPT. Le Serveur WAPT exigera un login et un mot de passe pour chaque hôte s'enregistrant auprès de lui.

```
WaptAgent Authentication type?
------------------------------------------------------------------------
( ) 1 Allow unauthenticated registration
(x) 2 Enable kerberos authentication required for machines registration.
Registration will ask for password if kerberos not available
( ) 3 Disable kerberos but registration require strong authentication
------------------------------------------------------------------------
< OK > < Cancel >
```

- Si vous souhaitez utiliser WAPT pour le déploiement de systèmes d'exploitation, sélectionnez Oui.

Si vous avez choisi Oui pour activer le déploiement d'OS, la post-configuration vous demandera si vous souhaitez utiliser une authentification sécurisée pour déployer les images d'OS. Il vous demandera un utilisateur / mot de passe lorsque vous allez déployer des images d'OS en utilisant WADS (mon cas).

- Si vous avez choisi Non, Nginx n'activera pas les points d'extrémité de l'API WADS pour les Agents WAPT.

```
Do you want to activate os deployment?
< Yes > < No >
```

L'authentification sécurisée pour WADS exige que l'utilisateur soit authentifié sur la machine où le système d'exploitation sera déployé.

```
Would you like to activate secure authentication on wads?
< Yes > < No >
```

Toujours en ce qui concerne la fonction WADS, si vous avez répondu Oui aux 2 dernières questions, vous aurez une dernière question :

```
Would you like to mention subnet ip exempt from wads authentication
< Yes > < No >
```

- Si vous répondez Oui à cette question, vous devrez donner un sous-réseau IP en format liste : **192.168.0.0/24**,**192.168.1.0/24**. Cela permettra à ce que les machines présentes au sein du/des sous-réseaux puisse se connecter avec wads sans authentification.

Choisissez si vous voulez utiliser WAPT WUA pour Windows Update.

```
Do you want to activate WUA?
< Yes > < No >
```

- Si vous choisissez Oui, Nginx activera les points de terminaison de l'API WUA pour les Agents WAPT.

Sélectionnez Oui pour configurer Nginx.

```
Do you want to configure nginx?
< Yes > < No >
```

Indiquez le FQDN du Serveur WAPT.

```
FQDN for the WAPT Server (eg. wapt.example.com)
-----------------------------------------------
srvwapt.mydomain.lan
-----------------------------------------------
< OK > < Cancel >
```

Sélectionner OK et un certificat auto-signé sera généré. Cette étape peut prendre un certain temps.

```
Generating DH parameters, 2048 bit long safe prime, generator 2 This is going
to take a long time
.....................................+.............................+...
```

Nginx est maintenant configuré, sélectionnez OK pour redémarrer Nginx :

```
The Nginx config is done.
We need to restart Nginx?
< OK >
```

Sélectionnez OK pour démarrer le Serveur WAPT.

```
Press OK to start waptserver and wapttasks daemons
< OK >
```

La post-configuration est maintenant terminée.

```
Postconfiguration completed.
Please connect to https://srvwapt.test-wapt.local/ to access the WAPT Server.
< OK >
```

- Ajouté dans la version 2.5: L'accès à l'interface web de WAPT est désormais protégé par un mot de passe.

Enfin, le postconf affiche quelques informations sur le certificat SSL du Serveur WAPT et l'URL pour télécharger WaptSetup et l'installer sur l'ordinateur de l'Administrateur WAPT.

Création de votre Keytab, après selection de l'activation kerberos pour la première fois.

```
Enter Kerberos REALM (domain name)
----------------------------------
MYDOMAIN.LAN
----------------------------------
< Yes > < Cancel >

Enter a Domain Controller name in write mode
----------------------------------
srvads1.mydomain.lan
----------------------------------
< Yes > < Cancel >

Enter a username authorized to join machines to the domain.
----------------------------------
administrator
----------------------------------
< Yes > < Cancel >
```

```
Enter administrator password
----------------------------------
**************
----------------------------------
< Yes >  < Cancel >

Enter the URL that will be used by the WAPTAgent
----------------------------------
srvwapt.mydomain.lan
----------------------------------
< Yes >  < Cancel >

Choose the name of the computer used by the waptserver
----------------------------------
SRVWAPT
----------------------------------
< Yes >  < Cancel >

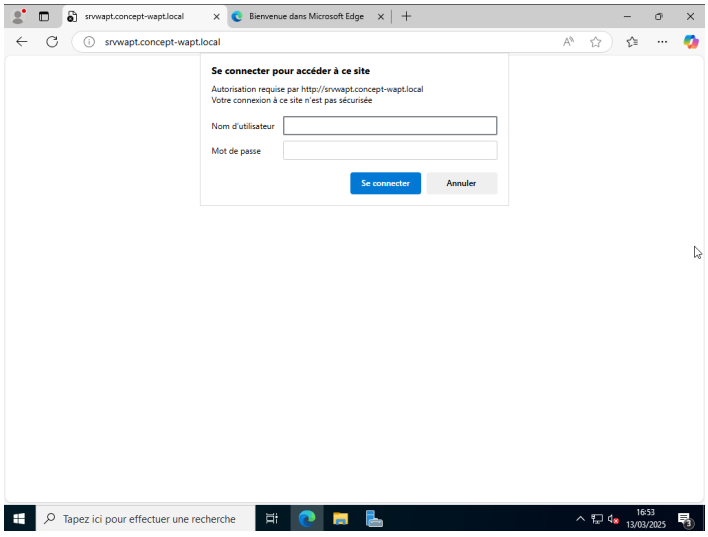
Keytab file is correctly generated in /etc/nginx/http-krb5.keytab
< OK >
```

1.2. Mise en place de la console

1.2.1. Installation

Pour installer la console WAPT, il est nécessaire de se rendre à l'adresse indiquée en fin de script postconf.sh qui correspond au FQDN du serveur.

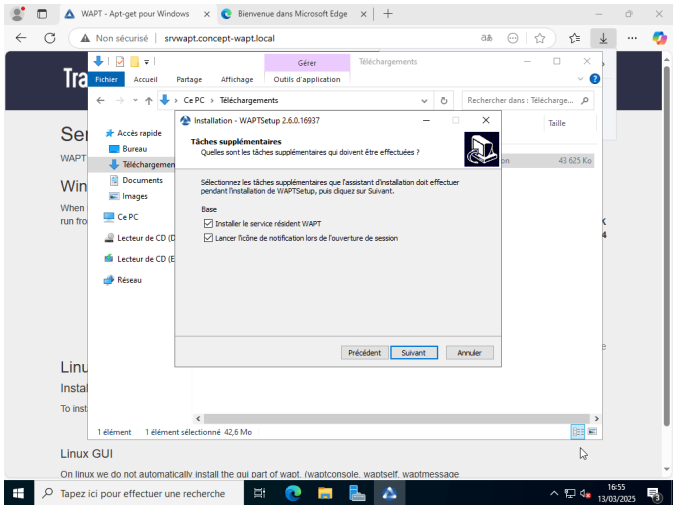
- Comme mentionné à la page Mise en place du serveur, Pour se connecter l'ID est admin et le mot de passe est celui entrer dans le script post-conf.



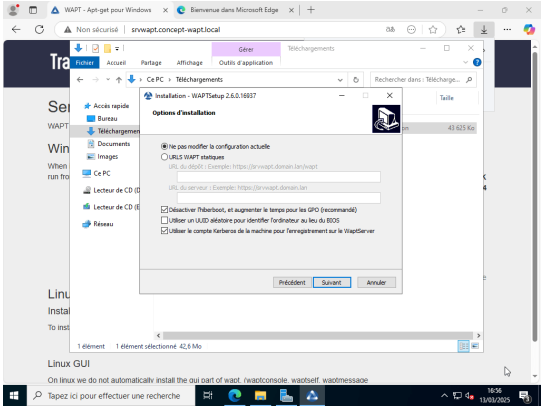
- Une fois les identifiants entrés on se retrouve sur l'interface web WAPT qui nous permet de télécharger le "**WAPT Setup**" pour Windows.



Lancer le programme d'installation et accepter les termes de licences. La coche "Installer le service résident WAPT" permet d'avoir le service WAPT d'installé sur le poste. La coche "Lancer l'icône de notification lors de l'ouverture de session" permet de lancer le service de la console (*wapttray*) au démarrage du poste, pratique, dans le cadre d'une machine dédiée à la console WAPT.



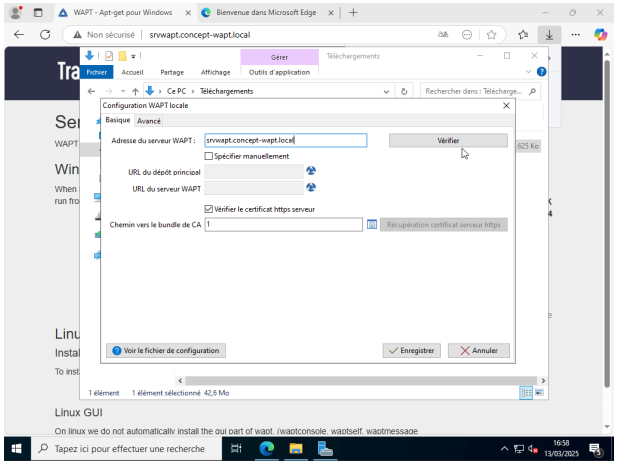
Le but est, de ne pas modifier la configuration actuelle car, on va pouvoir modifier la configuration au premier lancement de la console. De plus, je laisse cocher la case Kerberos car ma configuration actuelle le permet et est configuré.



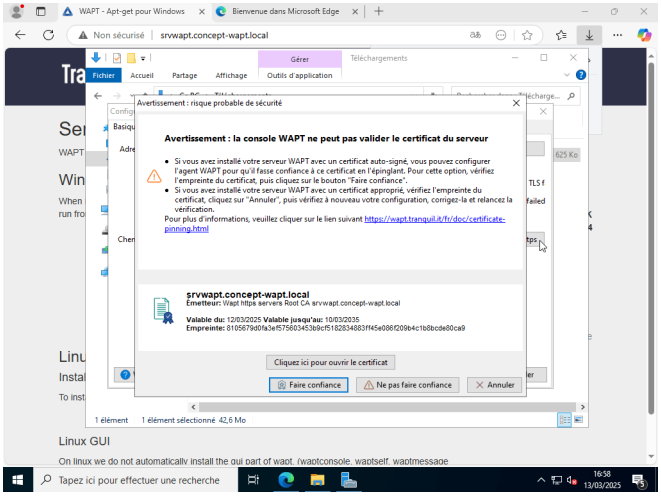
1.2.2. Configuration

Dans cette partie on va configurer notre console mais aussi notre agent afin de pouvoir déployer au mieux la solution au sein de l'infrastructure.

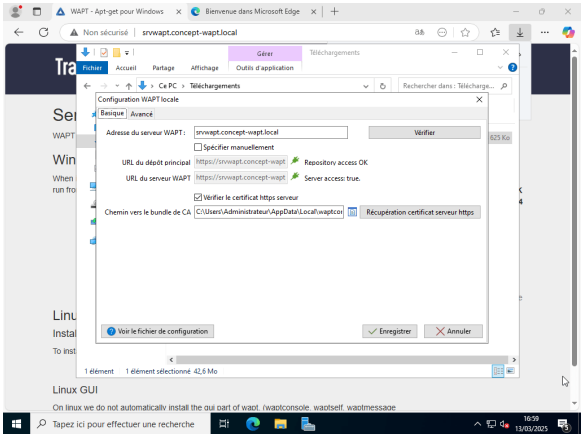
- Dans un premier temps, il est demandé de remplir le FQDN dans le premier champ.



- On fait confiance au certificat générer par le post script.



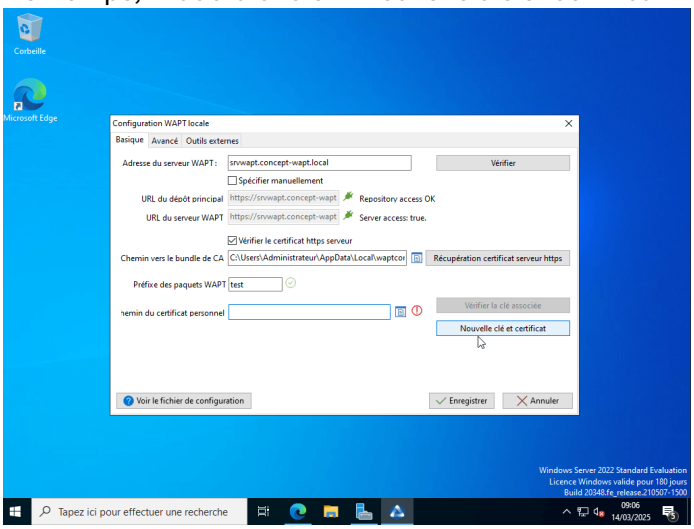
- Voici ce que cela donne après confirmation de confiance et récupération du certificat. Il est possible de passer à la sous-partie suivante.



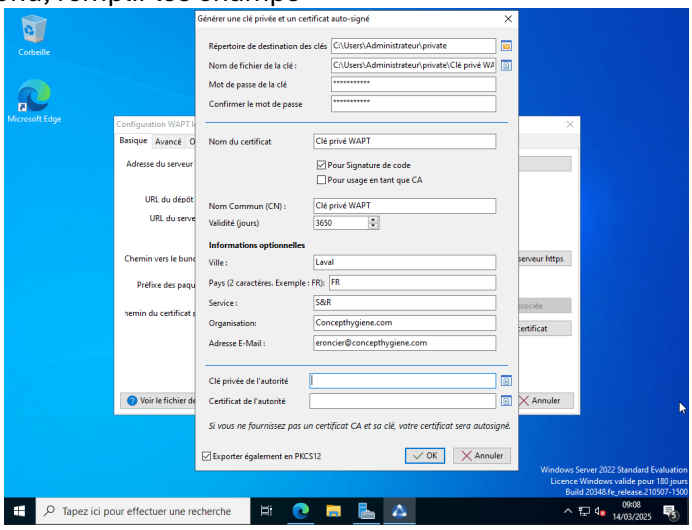
1.2.3. Clé

Cette partie n'est pas très complexe mais est nécessaire notamment pour la signature de paquet et même de l'agents qui sera installer sur le poste console et/ou sur les postes utilisateur.

- Dans un premier temps, il faudra choisir "Nouvelle clé et certificat"



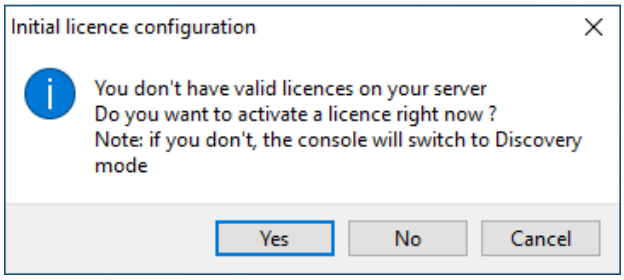
- Dans un second, remplir les champs



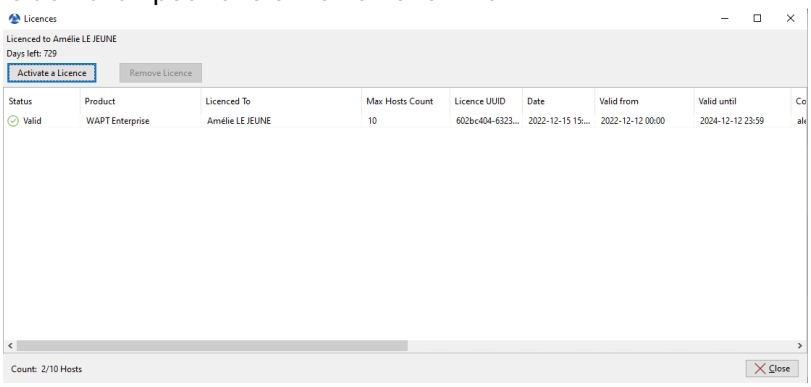
Une fois les champs remplis, il faudra confirmer les informations, et vérifier la clé en rentrant le mot de passe associé.

1.2.4. Licence

WAPT est une solution qui peut s'utiliser de manière gratuite via la formule Discovery mais en y intégrant une licence dit "Entreprise" on débloque tout le potentiel de la solution notamment, la fonctionnalité de déploiement de poste qui va nous intéresser dans la suite de cette documentation. Pour la licence rien de plus simple une fois le courriel de confirmation reçu de la part de Tranquil IT un fichier en .lic y est inclus. Ce fichier est un fichier licence qui sera à intégrer la première fois que la console est ouverte, cette étape intervient après la configuration initiale. D'ailleurs un pop-up s'affiche nous informant de la possibilité d'y glisser le fichier de licence.

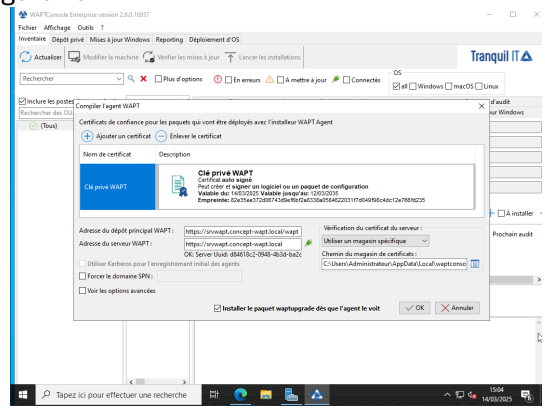


Après avoir confirmé le choix d'affectation de licence, il faudra choisir "Activer une licence. De parcourir le poste de travail pour choisir le fichier en .lic.



1.2.5. Création agent

Lors de la configuration de la console, WAPT demandera que l'agent soit présent sur la machine où la console a été installé. De ce fait un pop-up s'affichera invitant l'utilisateur à cocher ou non des options selon sa configuration.



Quelques précisions sur les informations de base :

Valeur	Description	Requis	Entreprise
Certificats de paquets autorisés	Définit tous les certificats de confiance intégrés au programme d'installation de l'Agent WAPT et définis dans la configuration par défaut.	Non	Oui
Adresse du Dépôt WAPT	Définit l'URL du dépôt WAPT principal.	Oui	Oui
Adresse du serveur WAPT	Définit l'URL du Serveur WAPT.	Oui	Oui
Vérifier le certificat HTTPS serveur	Définit si l'authentification client du certificat HTTPS est activée sur le Serveur WAPT.	Non	Oui
Utiliser Kerberos pour l'enregistrement initial	Définit si l'authentification Kerberos des Agents WAPT doit être utilisée avec le Serveur WAPT.	Non	Oui

Lorsque l'on coche la case "Voir les options avancées" voici quelques précisions :

Valeur	Description	Requis	Entreprise
Toujours installer ces paquets « profile »	Définit s'il faut installer automatiquement les packages du groupe lors de l'installation de l'Agent WAPT.	Non	Oui
Autoriser l'installation automatique (AD)	Permet l'installation des packages de profil basés sur les groupes AD. Peut dégrader les performances.	Non	Oui
Autoriser le redémarrage à distance	Définit si les redémarrages à distance sont autorisés à partir de la Console WAPT.	Non	Oui
Autoriser l'arrêt à distance	Définit si les arrêts à distance sont autorisés à partir de la Console WAPT.	Non	Oui
Inclure les infos DMI dans l'inventaire	Obtenir des informations sur les DMI dans l'inventaire de l'agent.	Non	Oui
Inclure les infos WMI dans l'inventaire	Obtenir des informations WMI dans l'inventaire de l'agent.	Non	Oui
Utiliser les règles d'accès au dépôt	Définit si les règles d'accès aux dépôts doivent être utilisées pour répliquer les dépôts distants.	Non	**Non**
Utiliser le FQDN comme UUID	Définit si les FQDN (Full Qualified Domain Name) doivent être utilisés pour identifier les Agents WAPT.	Non	Oui
Utiliser un UUID hôte aléatoire	À utiliser pour les BIOS bogués. Définit si des UUID aléatoires identifient les Agents WAPT.	Non	Oui
Gérer les mises à jour Windows (WUA)	Active ou désactive WAPT WUA (Windows Update Agent).	Non	Oui
Maturité du paquet Waptupgrade	Permet de choisir la maturité (prod, test, etc.) du paquet de mise à jour de l'agent.	Non	Oui

Enfin si une fenêtre s'affiche afin de vous demander d'appliquer la configuration sur la machine, accepter, sinon à la fin de création lancer l'agent crée, au répertoire ouvert automatiquement. Pour vérifier le fonctionnement de l'agent, il faut regarder si l'appareil est présent dans l'inventaire.

2. Configuration déploiement serveur

2.1. Extinction des services

Les services à éteindre sont waptserver, waptservice.

```
systemctl stop waptserver
systemctl stop waptservice
```

2.2. Accès au fichier waptserver.ini

Description : Le fichier de configuration principal du serveur WAPT contient tous les paramètres critiques pour WADS (déploiement OS).

Chemin : /opt/wapt/conf/waptserver.ini

Sauvegarde recommandée :

```
cp /opt/wapt/conf/waptserver.ini /opt/wapt/conf/waptserver.ini.bak
```

2.3. Modification des valeurs

Activation des modules de déploiement et configuration de l'authentification WADS.

```
wads_enable = True                    # Active WAPT Deployment Services (WADS)
waptwua_enable = True                 # Active Windows Update via WAPT (WUA)
login_on_wads = True                  # Authentification requise pour WADS
list_subnet_skip_login_wads = 10.35.1.0/24  # Sous-réseau exempt
d'authentification
```

2.4. Mise en place du démarrage automatique

Description : Configuration du service TFTP pour un démarrage automatique au boot du serveur.

```
systemctl enable wapttftpserver
```

Vérification : systemctl is-enabled wapttftpserver doit retourner "enabled".

2.5. Lancement des services

Description : Redémarrage des services avec les nouvelles configurations activées.

```
systemctl start waptserver
systemctl start waptservice
systemctl start wapttftpserver
```

Vérification complète

```
systemctl status waptserver waptservice wapttftpserver
netstat -tlnp | grep :69  # Port TFTP actif
```

2.6. Ajout des règles DHCP + configuration http

Description : Configuration DHCP spécifique au sous-réseau de déploiement avec politiques PXE avancées pour BIOS/UEFI et iPXE + Configuration DHCP globale (tous scopes) pour compatibilité maximale avec différents firmwares PXE.

Configuration complète disponible sur le site de Tranquil IT

Cela devrait donner ceci :

```
$scopeId = "10.35.1.0"
$waptserver_ipaddress_tftp = "10.35.1.11"
$url_waptserver = "http://srvwapt.test-wapt.local"
$keymap = "fr"

# 1. Classes DHCP
Add-DhcpServerv4Class -Name "legacy_bios" -Type Vendor -Data "PXEClient:Arch:00000" -ErrorAction
SilentlyContinue
Add-DhcpServerv4Class -Name "iPXE" -Type User -Data "iPXE" -ErrorAction SilentlyContinue

# 2. Option 66 (serveur TFTP)
Set-DhcpServerv4OptionValue -ScopeId $scopeId -OptionId 66 -Value $waptserver_ipaddress_tftp

# 3. Politiques PXE (4 cas)
# Legacy BIOS sans iPXE → pxeboot.n12
Add-DhcpServerv4Policy -ScopeId $scopeId -Name "pxebootn12" -Condition AND -UserClass NE,iPXE -
VendorClass EQ,legacy_bios* -ErrorAction SilentlyContinue
Set-DhcpServerv4OptionValue -ScopeId $scopeId -PolicyName "pxebootn12" -OptionID 67 -Value
"boot/pxeboot.n12"

# iPXE + Legacy BIOS → WAPT iPXE script
Add-DhcpServerv4Policy -ScopeId $scopeId -Name "wapt-ipxe-url-legacy" -Condition AND -UserClass EQ,iPXE
-VendorClass EQ,legacy_bios* -ErrorAction SilentlyContinue
Set-DhcpServerv4OptionValue -ScopeId $scopeId -PolicyName "wapt-ipxe-url-legacy" -OptionID 67 -Value
"$url_waptserver/api/v3/baseipxe?uefi=false&keymap=$keymap"

# Non-iPXE + UEFI → bootmgfw.efi
Add-DhcpServerv4Policy -ScopeId $scopeId -Name "bootmgfw.efi" -Condition AND -UserClass NE,iPXE -
VendorClass NE,legacy_bios* -ErrorAction SilentlyContinue
Set-DhcpServerv4OptionValue -ScopeId $scopeId -PolicyName "bootmgfw.efi" -OptionID 67 -Value
"efi/boot/bootmgfw.efi"

# iPXE + UEFI → WAPT iPXE script UEFI
Add-DhcpServerv4Policy -ScopeId $scopeId -Name "wapt-ipxe-url-uefi" -Condition AND -UserClass EQ,iPXE -
VendorClass NE,legacy_bios* -ErrorAction SilentlyContinue
Set-DhcpServerv4OptionValue -ScopeId $scopeId -PolicyName "wapt-ipxe-url-uefi" -OptionID 67 -Value
"$url_waptserver/api/v3/baseipxe?keymap=$keymap"

# -----------------------------------HTTP-----------------------------------------
```

```
# Classes de base
Add-DhcpServerv4Class -Name "legacy_bios" -Type Vendor -Data "PXEClient:Arch:00000"
Add-DhcpServerv4Class -Name "iPXE" -Type User -Data "iPXE"

# Option 66 globale (TFTP)
Set-DhcpServerv4OptionValue -OptionId 66 -Value $waptserver_ipaddress_tftp

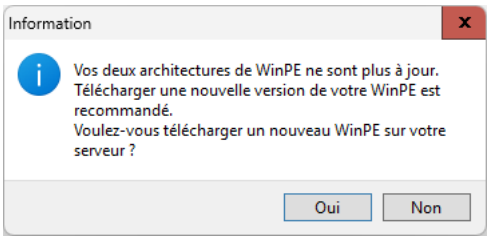
# Politiques globales
Add-DhcpServerv4Policy -Name "wapt-ipxe-url-legacy" -Condition AND -UserClass EQ,iPXE -VendorClass
EQ,legacy_bios* -Set-DhcpServerv4OptionValue -PolicyName "wapt-ipxe-url-legacy" -OptionID 67 -Value
"$url_waptserver/api/v3/baseipxe?uefi=false&keymap=$keymap"
Add-DhcpServerv4Policy -Name "wapt-ipxe-url-uefi" -Condition AND -UserClass EQ,iPXE -VendorClass
NE,legacy_bios* -Set-DhcpServerv4OptionValue -PolicyName "wapt-ipxe-url-uefi" -OptionID 67 -Value
"$url_waptserver/api/v3/baseipxe?keymap=$keymap"

# Fallbacks
Add-DhcpServerv4Policy -Name "snponly.efi" -Condition AND -UserClass NE,iPXE -VendorClass
NE,legacy_bios* -Set-DhcpServerv4OptionValue -PolicyName "snponly.efi" -OptionID 67 -Value
"snponly.efi"
Add-DhcpServerv4Policy -Name "undionly.kpxe" -Condition AND -UserClass NE,iPXE -VendorClass
EQ,legacy_bios* -Set-DhcpServerv4OptionValue -PolicyName "undionly.kpxe" -OptionID 67 -Value
"undionly.kpxe"
```

3. Déploiement

3.1. Modification de la configuration console

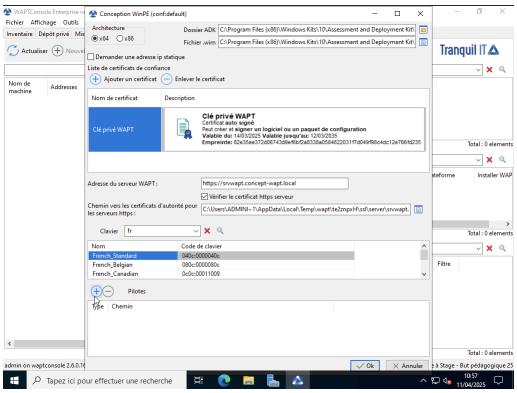
3.1.1. Paquets WinPE



Il faudra aller d'abord chercher les paquets tis-wads-requirement-minimal-x64 et tis-wadsrequirement-minimal trouvable dans le dépôt de TranquilIT depuis la console, pour les installer sur notre machine d'administration.

Ce paquet contient une image de WinPE qui est la version poche de Windows et qui sert notamment pour l'installation du système, même pour un environnement hors PXE.

Point de précision important : Après installation du paquet sur la machine d'administration de la solution, il sera nécessaire de diposer de pilotes à inclure dans la prochaine ce qui nous renvoi au point 3.3.5.



- Une fois cliqué sur "oui" on arrive sur cet assistant de conception. On pourra cliquer sur la configuration de clavier qui nous intéresse et choisir le dossier de pilote afin de confirmer la création.

3.2. Déploiement ISO

3.2.1. Récupération de l'image Windows

Pour Windows 11 / 10

1. **Accédez à la page officielle** :
   https://www.microsoft.com/fr-fr/software-download/windows11 (ou windows10)
2. **Téléchargez l'outil de création** :
   - Cliquez "Télécharger maintenant l'outil"
   - Exécutez → Choisissez **"Fichier ISO"** au lieu de clé USB
   - Sélectionnez **Français** + **Windows 11 Pro** (index 6 dans unattend.xml)
   - **~5 Go** téléchargés directement

Astuce navigateur (ISO direct sans outil)

1. Ouvrez la page Microsoft dans Edge/Chrome
2. F12 → Mode mobile (toggle device toolbar)
3. Rafraîchissez → Liens ISO directs apparaissent
4. Téléchargez l'ISO français x64

3.2.2. Intégration de l'ISO

L'image ISO doit être mise à disposition du service WADS (WAPT Deployment Services) pour être exploitée lors du déploiement.

1. **Accéder à l'interface de Déploiement d'OS :**
Sur la **Console WAPT**, naviguez vers l'onglet **Déploiement d'OS** (Déploiement de postes).

2. **Importer l'ISO d'installation :**
Dans la section **Déploiement d'OS**, cherchez l'option ou l'icône **Importer des machines depuis un CSV** ou **Ajouter une ISO d'installation**.
Suivez l'assistant :
Pointez vers le chemin local où vous avez stocké votre fichier ISO Windows.
La Console WAPT analyse l'image pour détecter les versions de Windows (WIM files) qu'elle contient.

3. **Sélectionner l'Architecture :**
Choisissez l'architecture correspondante (ex. x64).

4. **Enregistrement de l'ISO :**
La Console WAPT enregistre l'ISO, la rendant disponible pour être liée à un profil de déploiement.

3.3. Configuration

3.3.1. Description du script XML

Le fichier **unattend.xml** est un fichier de configuration qui permet de contourner la configuration du système appelée OOBE (Out-of-Box Experience), ainsi que de passer outre certaines options d'installation du système d'exploitation. Celui que je présente ici permet :

- Windows 11 Pro INDEX=6 (explicite)
- Français + AZERTY (040c:0000040c)
- Partition fixe Disque0/Partition3
- Jointure AD online
- Pilotes c:\installdir\drivers
- Superadmin local + Romance Standard Time
- OOBE 100% automatisé
- Post-install wads.exe + SetupComplete.cmd

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="windowsPE">
        <component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="{{architecture}}" publicKeyToken="31bf3856ad364e35" language="neutral"
versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <SetupUILanguage>
                <UILanguage>fr-FR</UILanguage>
            </SetupUILanguage>
            <InputLocale>040c:0000040c</InputLocale>
            <SystemLocale>fr-FR</SystemLocale>
            <UILanguage>fr-FR</UILanguage>
            <UILanguageFallback>fr-FR</UILanguageFallback>
            <UserLocale>fr-FR</UserLocale>
        </component>
        <component name="Microsoft-Windows-Setup" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <ImageInstall>
                <OSImage>
                    <InstallTo>
                        <PartitionID>3</PartitionID>
                        <DiskID>0</DiskID>
                    </InstallTo>
                    <InstallToAvailablePartition>false</InstallToAvailablePartition>
                    <WillShowUI>OnError</WillShowUI>
                    <InstallFrom>
```

```
                        <MetaData>
                            <Key>/IMAGE/INDEX</Key>
                            <Value>6</Value>
                        </MetaData>
                    </InstallFrom>
                </OSImage>
            </ImageInstall>
            <UserData>
                <ProductKey>
                    <Key/>
                </ProductKey>
                <AcceptEula>true</AcceptEula>
            </UserData>
        </component>
    </settings>
    <settings pass="offlineServicing">
        <component name="Microsoft-Windows-PnpCustomizationsNonWinPE"
processorArchitecture="{{architecture}}" publicKeyToken="31bf3856ad364e35" language="neutral"
versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DriverPaths>
                <PathAndCredentials wcm:keyValue="1" wcm:action="add">
                    <Path>c:\installdir\drivers</Path>
                </PathAndCredentials>
            </DriverPaths>
        </component>
    </settings>
    <settings pass="generalize">
        <component name="Microsoft-Windows-Security-SPP" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <SkipRearm>1</SkipRearm>
        </component>
    </settings>
    <settings pass="specialize">
        <component name="Microsoft-Windows-UnattendedJoin" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <Identification>
                <Credentials>
                    <Domain>mydomain.lan</Domain>
                    <Password>password</Password>
                    <Username>wadsjoin</Username>
                </Credentials>
                <JoinDomain>mydomain.lan</JoinDomain>
```

```
            </Identification>
        </component>
        <component name="Microsoft-Windows-International-Core" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <InputLocale>040c:0000040c</InputLocale>
            <SystemLocale>fr-FR</SystemLocale>
            <UILanguage>fr-FR</UILanguage>
            <UILanguageFallback>fr-FR</UILanguageFallback>
            <UserLocale>fr-FR</UserLocale>
        </component>
        <component name="Microsoft-Windows-Security-SPP-UX" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <SkipAutoActivation>true</SkipAutoActivation>
        </component>
        <component name="Microsoft-Windows-SQMApi" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <CEIPEnabled>0</CEIPEnabled>
        </component>
        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <ComputerName>{{hostname}}</ComputerName>
            <!-- <ProductKey>W269N-WFGWX-YVC9B-4J6C9-T83GX</ProductKey> -->
        </component>
        <component name="Microsoft-Windows-Deployment" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <RunSynchronous>
                <RunSynchronousCommand wcm:action="add">
                    <Path>"c:\installdir\wads.exe" --setup-startup
script="c:\installdir\SetupComplete.cmd"</Path>
                    <Order>2</Order>
                    <Description>postinstall</Description>
                </RunSynchronousCommand>
            </RunSynchronous>
        </component>
    </settings>
    <settings pass="oobeSystem">
```

```
        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="{{architecture}}"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm=http://schemas.microsoft.com/WMIConfig/2002/State
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <OOBE>
                <HideEULAPage>true</HideEULAPage>
                <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
                <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
                <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
                <NetworkLocation>Work</NetworkLocation>
                <SkipUserOOBE>true</SkipUserOOBE>
                <SkipMachineOOBE>true</SkipMachineOOBE>
                <ProtectYourPC>1</ProtectYourPC>
            </OOBE>
            <UserAccounts>
                <LocalAccounts>
                    <LocalAccount wcm:action="add">
                        <Password>
                            <Value>LOCAL_ADMIN_PASSWORD_PLACE_HOLDER</Value>
                            <PlainText>true</PlainText>
                        </Password>
                        <Description/>
                        <DisplayName>superadmin</DisplayName>
                        <Group>Administrators</Group>
                        <Name>superadmin</Name>
                    </LocalAccount>
                </LocalAccounts>
            </UserAccounts>
            <RegisteredOrganization/>
            <RegisteredOwner>superadmin</RegisteredOwner>
            <DisableAutoDaylightTimeSet>false</DisableAutoDaylightTimeSet>
            <TimeZone>Romance Standard Time</TimeZone>
        </component>
    </settings>
</unattend>
```

3.3.2. Phases du déploiement

Phase	Pass XML	Durée	Prérequis	Actions détaillées	Résultat
1. Boot WinPE	windowsPE	2-3 min	PXE OK	Langue : Interface FR + AZERTY	Partition formatée + WIM copié
				Sélection : INDEX 6 (Pro)	
				Partition : Disque 0 / Partition 3	
2. Pilotes	offlineServicing	1-2 min	Dossier drivers	Injection : Scan c:\installdir\drivers	Matériel reconnu
				Réseau/Stockage : Pilotes .inf auto	
3. Préparation	generalize	30s	-	Licence : SkipRearm=1	Image sysprep prête
				Généralisation : Image nettoyée	
4. Spécialisation	specialize	3-5 min	AD joignable	Domaine : mydomain.lan via wadsjoin	PC nommé + joint domaine
				Nom : {{hostname}} auto	
				Scripts : wads.exe SetupComplete.cmd	
5. OOBE	oobeSystem	2 min	-	Bypass : Tous écrans cachés	Bureau prêt !
				Admin : superadmin créé	
				Timezone : Romance Standard Time	

3.3.3. Composants

Composant	Phase	Paramètres critiques	Rôle WADS	Configuration requise
International-Core-WinPE	windowsPE	fr-FR, 040c:0000040c	**Interface** : Première écran en français + AZERTY	ISO FR x64
Microsoft-Windows-Setup	windowsPE	<Key>/IMAGE/INDEX</Key>, <Value>6</Value>	**Édition** : **Windows 11 Pro explicite**	ISO multieditions
PnpCustomizationsNonWinPE	offlineServicing	<Path>c:\\installdir\\drivers</Path>	**Pilotes** : Réseau/Chipset/Stockage injectés	Dossier \\srv-wapt\installdir\drivers
UnattendedJoin	specialize	<JoinDomain>mydomain.lan</>, wadsjoin/password	**Domaine** : Jointure AD online	Compte AD wadsjoin + mot de passe
Shell-Setup (specialize)	specialize	<ComputerName>{{hostname}}</>	**Nom PC** : Auto-généré par WADS	Variable WADS {{hostname}}
Deployment	specialize	wads.exe --setup-startup-script	**Post-install** : Agent WAPT + apps	SetupComplete.cmd sur serveur
Shell-Setup (oobeSystem)	oobeSystem	superadmin, Romance Standard Time	**Finalisation** : Admin local + timezone FR	Remplacer LOCAL_ADMIN_PASSWORD_PLACE_HOLDER

3.3.4. Erreurs courantes

Il est défendable devant un service cybersécurité de dire que **mettre LAPS et BitLocker "dans l'unattend.xml" n'est ni essentiel, ni souhaitable**, car cela augmente la surface d'attaque sans apporter de bénéfice par rapport à un pilotage par GPO/MDM, qui est la pratique recommandée.

- Les mots de passe locaux définis via des réponses d'installation (unattend.xml) sont stockés dans un fichier lisible sur le support d'installation et souvent laissé sur le disque après déploiement ; on trouve de nombreux retours de mots de passe admin en clair ou simplement encodés en Base64 dans des unattend.xml, ce qui est trivial à récupérer en post-compromission.
- Des ressources de tests d'intrusion et de pentest listent explicitement les fichiers unattended comme cibles pour la recherche de mots de passe locaux afin d'escalader les privilèges.
- Microsoft LAPS et Windows LAPS, au contraire, sont conçus pour être pilotés par stratégie(GPO/MDM) : on y configure centralement la rotation automatique, la complexité, l'intervalle de changement et le stockage sécurisé du mot de passe dans AD/Entra, sans jamais exposer ce mot de passe dans un fichier de réponse ou un script.
- Des guides d'implémentation récents recommandent explicitement de créer une GPO dédiée (ex. C_LAPS) et de l'appliquer aux OU cibles, ce qui garantit une configuration homogène et auditables, tout en réduisant les secrets "cachés" dans l'infra de déploiement.

En bref, inclure la logique LAPS dans l'unattend.xml reviendrait à réintroduire des mots de passe locaux statiques ou prévisibles dans un fichier facilement récupérable, alors que la bonne pratique actuelle est d'externaliser complètement cette gestion vers LAPS via GPO/MDM, avec rotation et stockage centralisé protégés

3.3.5. Pilotes

Pour exporter les pilotes nous avons plusieurs choix :

1. Possibilité d'utiliser des pilotes génériques dans ce cas, il est possible d'utiliser les pilotes de machine virtuelles (oui oui de VM). Puis de faire les maj, après dans les paramètres ou via Dell Command Update.

2. (plus fiable) Possibilité de démarrer un pc fraichement arrivé, le configurer, faire les maj de pilotes et de les exporter via la commande :

```
Export-WindowsDriver -Online -Destination FICHIER_DE_DESTINATION
```

3. Voir avec le fabricant, pour qu'il fournisse les fichiers en .inf répartie dans des dossiers distincts. Exemple pour la carte réseau d'une VM :

netkvm.inf
|-> netkvm.cat
|-> netkvm.inf
|-> netkvm.pnf
|-> netkvm.sys
|-> netkvmp.exe

4. Magasin d'applications

4.1. Withsecure

4.1.1. Ajout du paquet

Le paquet WithSecure étant présent dans le dépôt officiel de WAPT, son intégration ne nécessite pas de modifications structurelles lourdes.

Procédure d'importation :
Se rendre dans l'onglet **Dépôt privé** de la console WAPT.
Cliquer sur **Importer un paquet depuis Internet**.
Dans la fenêtre contextuelle affichant les paquets disponibles (dépôts Tranquil IT), rechercher le terme withsecure.
Sélectionner le paquet tis-withsecure-agent-desktop.

L'ajouter au panier et valider l'importation vers votre dépôt privé

4.1.2. Configuration du paquet

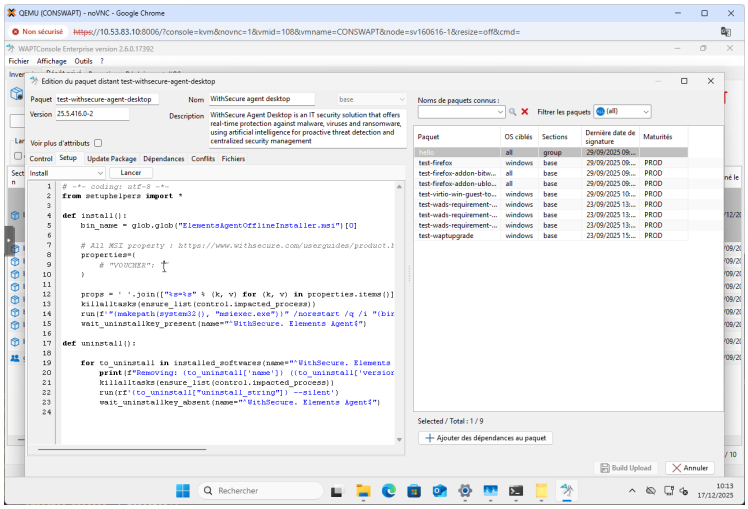
La documentation du paquet précise que la configuration s'effectue via le fichier setup.py. Pour lier l'agent à votre console de gestion, vous devez renseigner votre clé d'abonnement. La documentation WithSecure indique l'argument suivant :

VOUCHER : Définit la clé d'abonnement. Exemple : --voucher aaaa-bbbb-cccc-dddd-eeee

Modification du fichier de configuration : Il est possible de modifier le script d'installation directement depuis la console WAPT :
1. Faire un clic droit sur le paquet importé et sélectionner l'onglet **Setup**.
2. Localiser la ligne contenant le paramètre « VOUCHER».
3. Décommenter la ligne et insérer votre licence entre les guillemets.

Avant :

```
"VOUCHER": ""
```



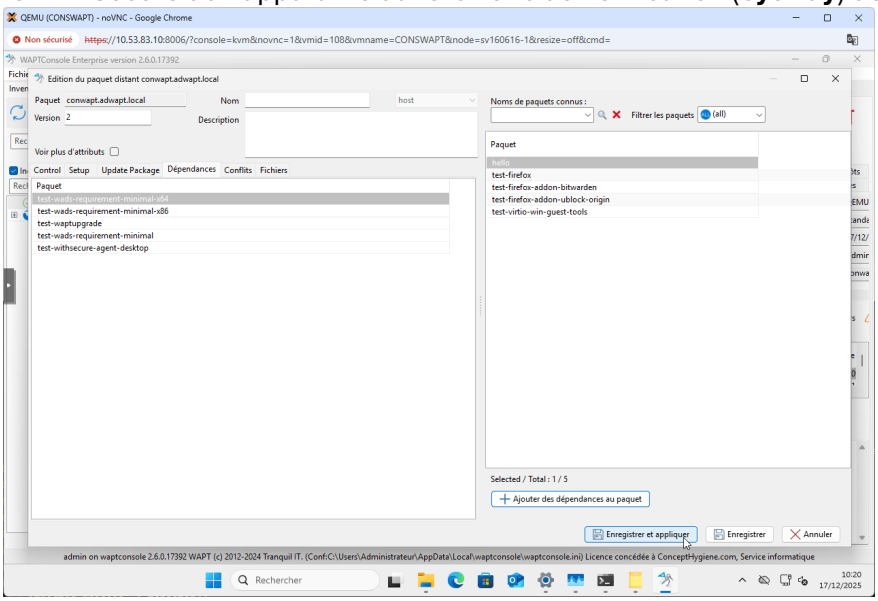
Après :

```
"VOUCHER": "aaaa-bbbb-cccc-dddd-eeee"
```

4.1.3. Installation

L'installation sur les postes clients suit la procédure standard de WAPT :
1. Sélectionner la machine cible dans l'inventaire.
2. Cliquer sur **Modifier la machine**.
3. Ajouter le paquet tis-withsecure-agent-desktop à la liste des logiciels à installer.
4. Enregistrer et appliquer les modifications.

Une fois le déploiement terminé (généralement après un redémarrage ou une mise à jour de l'agent), l'icône WithSecure doit apparaître dans la zone de notification (**systray**) de Windows.

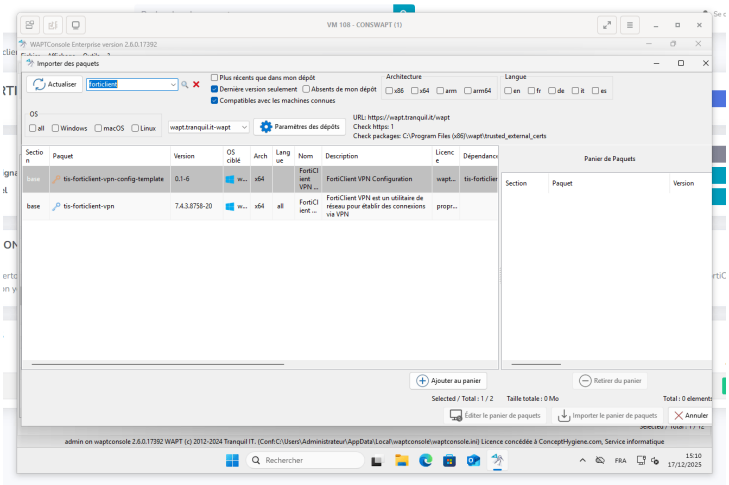


4.2. Forticlient

Les paquets FortiClient étant présents dans le dépôt officiel de WAPT, leur intégration est simplifiée.

Procédure d'importation :

1. Se rendre dans l'onglet **Dépôt privé** de la console WAPT.
2. Cliquer sur **Importer un paquet depuis Internet**.
3. Dans la fenêtre contextuelle affichant les paquets disponibles (dépôts Tranquil IT), rechercher le terme forticlient.
4. Sélectionner les deux paquets suivants :
   - tis-forticlient-vpn (Le logiciel)
   - tis-forticlient-vpn-config-template (Le modèle de configuration)
5. Les ajouter au panier et valider l'importation vers votre dépôt privé



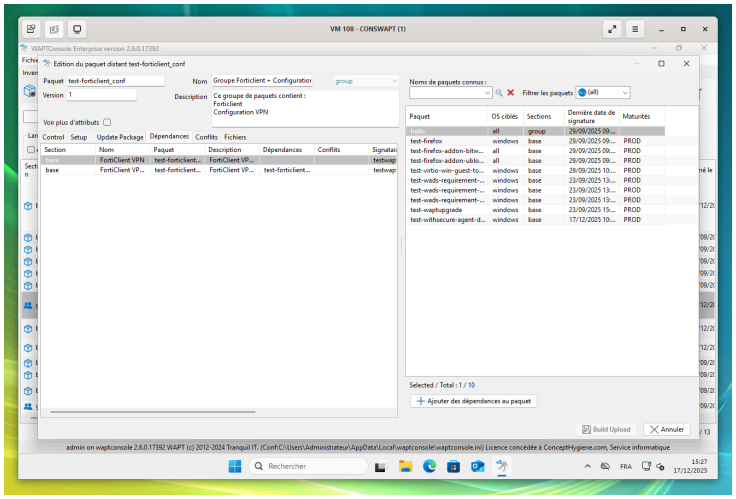
Contrairement à d'autres agents, FortiClient nécessite une attention particulière. Il demande une confirmation de licence et ne centralise pas sa configuration dans un simple fichier

accessible, celle-ci étant répartie dans le registre Windows (regedit.exe) pour des raisons de sécurité.
La méthode préconisée consiste à utiliser le paquet "Template". Le principe est de télécharger ce paquet en local, puis d'y injecter votre fichier de configuration .conf (exporté depuis un poste témoin).

Bonne pratique : Il est recommandé de créer un **groupe de paquets** WAPT contenant :

- Le logiciel de base (tis-forticlient-vpn)
- La configuration personnalisée (tis-forticlient-vpn-config-template)

Cela rend l'administration et le déploiement plus fluides.



4.2.1. Modification du fichier setup.py

1. Se rendre dans l'onglet **Dépôt privé** de la console WAPT.
2. Faire un clic droit sur le paquet tis-forticlient-vpn-config-template et sélectionner **Éditer le paquet**.
3. Dans la section def install() , localiser et renseigner les variables suivantes :

```
conf_name = "" # Nom de la configuration tel qu'il apparaîtra dans l'interface FortiClient
conf_file = "" # Nom exact du fichier de configuration (doit obligatoirement finir par .conf)
unencrypted_password = "" # Mot de passe utilisé lors de l'export (si applicable)
```

1. Export depuis un poste témoin Si FortiClient est déjà installé et correctement configuré sur un poste, il est possible d'exporter cette configuration pour la déployer massivement :

- Ouvrir l'interface de FortiClient et se rendre dans l'onglet de gestion (paramètres système).
- Cliquer sur le bouton **Sauvegarder** (Backup).
- Un mot de passe de protection sera demandé. Pour des raisons de sécurité, choisissez un mot de passe fort.

Note importante : Ce mot de passe devra être reporté tel quel (en clair) entre les guillemets de la variable unencrypted_password dans le fichier setup.py.

2. Intégration du fichier dans le paquet WAPT Une fois le fichier de configuration .conf obtenue, il doit être intégré aux sources du paquet tis-forticlient-vpn-config-template. La procédure est la suivante :

- Dans la fenêtre d'édition du paquet de la console WAPT, basculer sur l'onglet **Fichiers** (Project Files).
- Faire un clic droit dans l'espace vide et sélectionner **Ouvrir l'emplacement du fichier**.
- Si une fenêtre demande de confirmer le téléchargement des sources en local, accepter.
- L'explorateur de fichiers s'ouvre : y déposer (glisser-déposer) le fichier de configuration .conf précédemment exportée.

Pour finaliser l'opération, enregistrez les modifications et **reconstruisez le paquet** (Build and Upload) afin de le rendre disponible sur le dépôt

4.2.2. Installation

L'installation sur les postes clients suit la procédure standard de WAPT :

1. Sélectionner la machine cible dans l'inventaire.
2. Cliquer sur **Modifier la machine**.
3. Ajouter le groupe de paquets (ou les deux paquets distincts) à la liste des logiciels à installer.
4. Enregistrer et appliquer les modifications.

Une fois le déploiement terminé (généralement après un redémarrage du poste ou du service), l'icône FortiClient doit apparaître dans la zone de notification (**systray**) de Windows avec la configuration appliquée.

5. Résolution de pannes

5.1. Rapport d'intervention 02/2026

Objet : Diagnostic et rétablissement du service de déploiement réseau (WADS/WAPT).
Statut : Résolu.

5.1.1. Analyse Réseau

La première phase du diagnostic a porté sur la validation de la couche transport et de l'adressage :

- **Capture de paquets :** L'analyse Wireshark confirme que les options DHCP sont correctement transmises au client dans leur intégralité.
- **Conformité :** La configuration du serveur DHCP est validée conforme à la documentation technique de référence.

L'infrastructure réseau est donc hors de cause

5.1.2. Analyse système

L'anomalie ayant été isolée au niveau de la couche application, les tests se sont portés sur le protocole de transfert de fichiers (TFTP).

Test client : La commande `tftp -i 10.53.96.65 get snponly.efi` a retourné une erreur de connexion.

Analyse des sockets : L'inspection via `ss -pantul | grep 69` a montré une instabilité dans l'écoute du port, bien que `systemctl status wapttftpserver.service` indique un service actif sans erreur apparente dans les logs (`journalctl`).

Résolution : Un redémarrage à chaud (`reboot`) du serveur a été nécessaire pour réinitialiser correctement le service et libérer les ressources réseau.

Résultat : Le téléchargement du fichier `snponly.efi` est de nouveau fonctionnel après redémarrage.

5.1.3. Configuration console & environnement WinPE

À la suite du rétablissement du flux TFTP, un conflit de certificat a été identifié lors de l'initialisation de l'image WinPE.

Action : Régénération complète de l'image WinPE via la console WAPT en suivant la documentation interne.

Ajustement technique : En l'absence de documentation spécifique sur la chaîne de certification locale, l'image a été générée sans vérification de certificat afin de garantir la disponibilité immédiate du déploiement.

5.1.4. Conclusion

Le diagnostic a couvert l'ensemble des couches du modèle OSI, permettant d'identifier un blocage au niveau du socket TFTP et un conflit de certificat applicatif. Le flux de déploiement est de nouveau opérationnel.

6. Procédures

6.1. Déploiement de poste

Contrairement à MDT, la méthode **WADS (WAPT OS Deployment)** s'articule autour de trois phases clés : la préparation de l'infrastructure, le paramétrage du BIOS et la gestion via la console WAPT.

6.1.1. Prérequis

Avant de commencer, assurez-vous que :

- Le **serveur WAPT** est joignable sur le réseau.
- La **Console WAPT** est installée et configurée avec les droits suffisants.

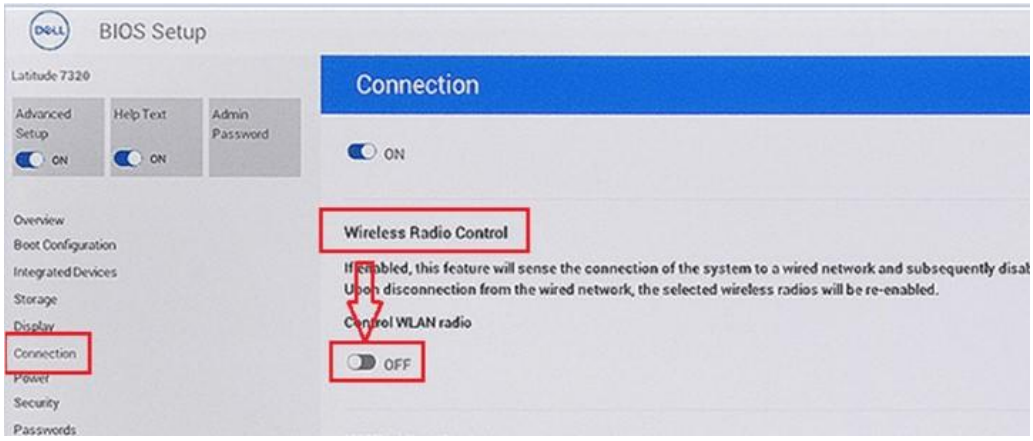
6.1.2. Paramétrage du BIOS (Poste Client)

Au démarrage du poste, tapotez la touche F12 pour accéder au menu de démarrage (Boot Menu). Pour les modifications suivantes, entrez dans le BIOS Setup.

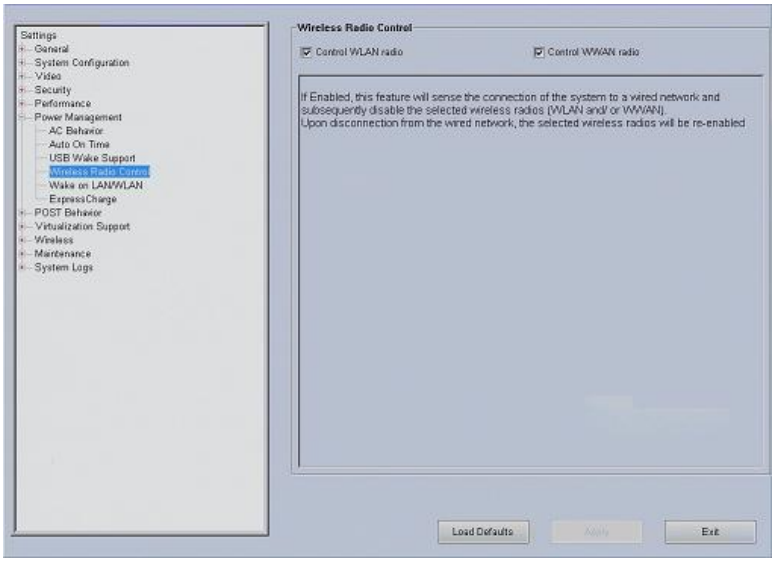
6.1.2.1. Configuration de la connectivité (Modèles Wi-Fi)

Il est nécessaire d'activer le contrôle radio pour permettre la gestion hybride.

- **BIOS Récent (Interface Graphique)** : Allez dans le volet de gauche sous Connection. Dans la partie droite, activez les options Control WLAN radio et Control WWAN radio.



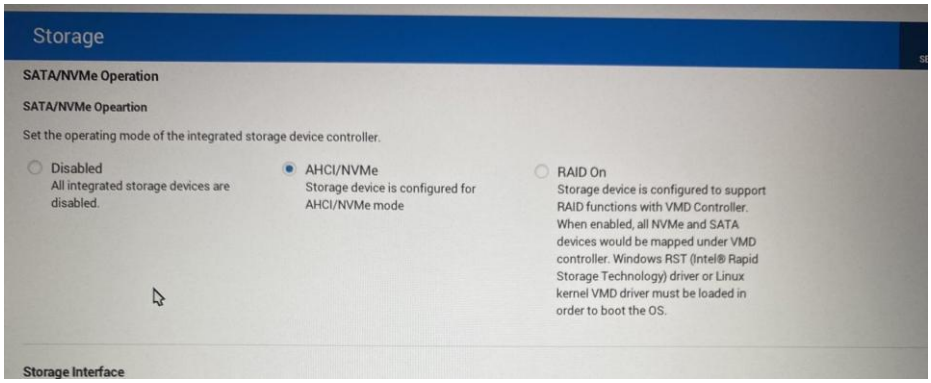
- **Ancien BIOS (Interface Texte**) : Allez dans Power Management > Wireless Radio Control et activez les options équivalentes.



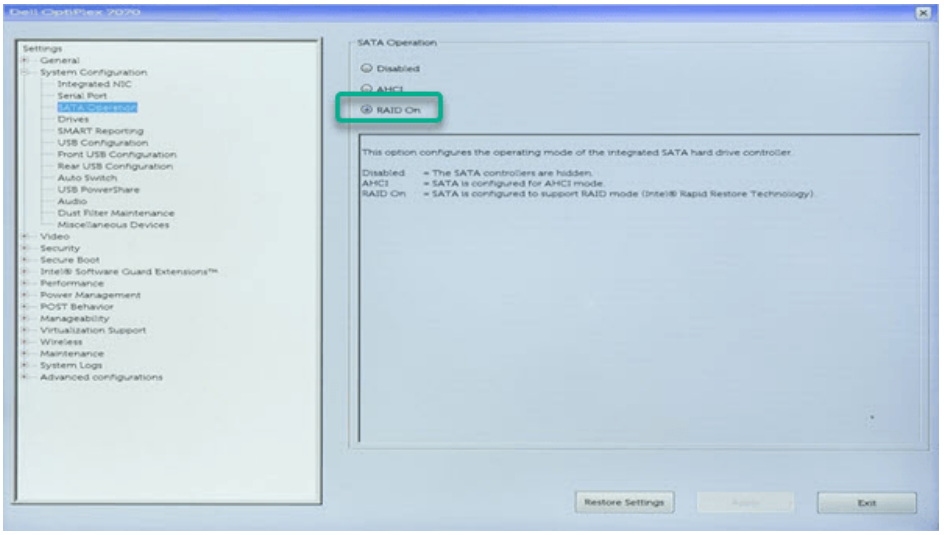
6.1.2.2 Configuration du stockage (Mode AHCI)

Pour garantir la compatibilité sans injecter les pilotes Intel Rapid Storage (IRST), le contrôleur doit être configuré en **AHCI**.

- **BIOS Récent** : Sous l'onglet Storage ou Connection, sélectionnez l'option AHCI/NVMe.



- **Ancien BIOS :** Allez dans System Configuration > SATA Operation et sélectionnez AHCI.



Note : Le passage en mode AHCI est indispensable si le poste était initialement configuré en "RAID ON".

Une fois le BIOS configuré, démarrez le poste sur le réseau (PXE/WADS).

6.1.3. Gestion du déploiement

6.1.3.1 Enregistrement de la machine

Sur le poste client, attendez l'invite de commande pour saisir le **Hostname**.

- Note : Ce nom sera utilisé pour la console WAPT, l'affichage réseau et l'objet Ordinateur dans l'Active Directory.

Validez le nom d'hôte, puis cliquez sur **Retry Deployment**.
Basculez sur la console WAPT, onglet **Déploiement d'OS**.

6.1.3.2 Lancement du déploiement

Dans l'onglet "Déploiement d'OS", les machines sont centralisées au centre, tandis que les images, configurations et pilotes sont à droite.

- **Vérification :** Assurez-vous que la machine apparaît correctement dans la liste des machines en attente.
- **Assignation :** Faites un clic droit sur la machine cible :
- Sélectionnez **Choisir une configuration**.
- Sélectionnez **Pousser les pilotes (selon le modèle).**
- **Exécution :** Faites un clic droit sur la machine et sélectionnez Démarrer le déploiement.

Une fois le déploiement WADS terminé, une intervention locale est requise pour finaliser l'environnement utilisateur.

6.1.4. Finitions et Logiciels Complémentaires

Connectez-vous au poste avec un compte Administrateur (compte technicien) et procédez à l'installation des outils disponibles sur le partage commun :

- F-Secure
- Forticlient
- UltraVNC
- Office

Vérifications finales :

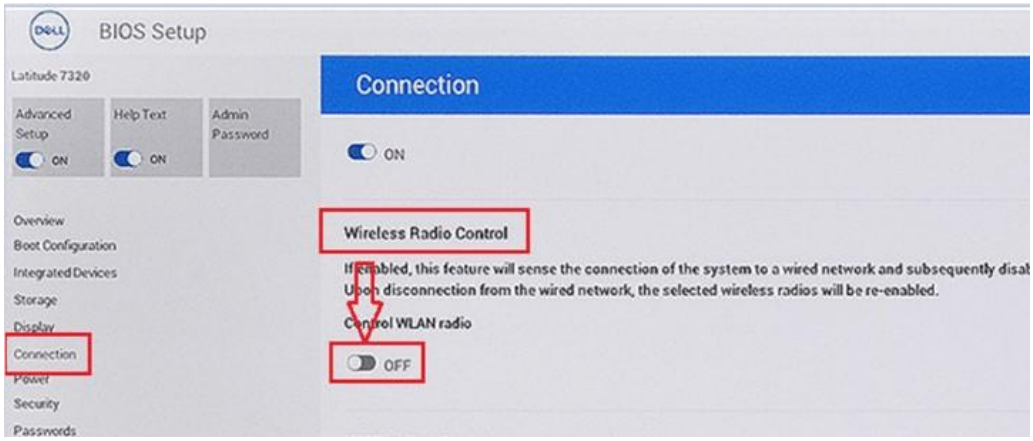
- Vérifier la jonction au domaine AD.
- S'assurer que l'agent WAPT remonte correctement les inventaires.
- Tester la connectivité réseau (LAN/Wi-Fi)

6.2. Vente de poste

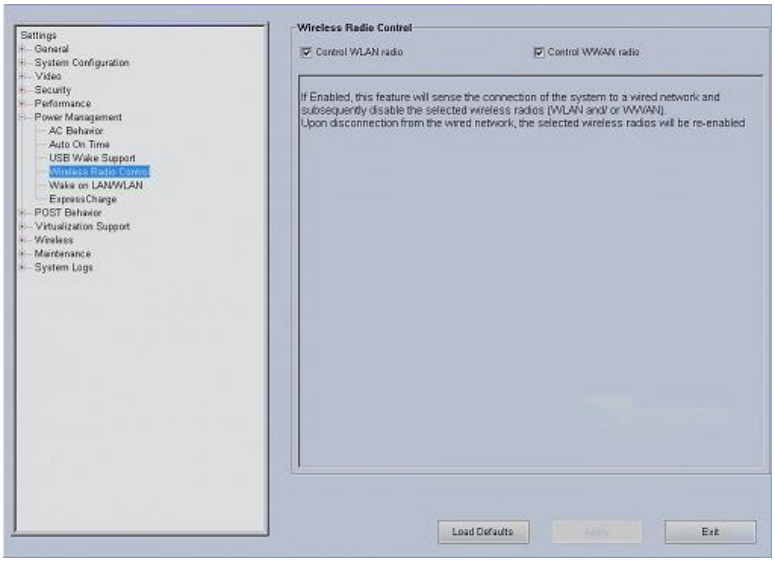
6.2.2.1. Configuration de la connectivité (Modèles Wi-Fi)

Il est nécessaire d'activer le contrôle radio pour permettre la gestion hybride.

- **BIOS Récent (Interface Graphique)** : Allez dans le volet de gauche sous Connection. Dans la partie droite, activez les options Control WLAN radio et Control WWAN radio.



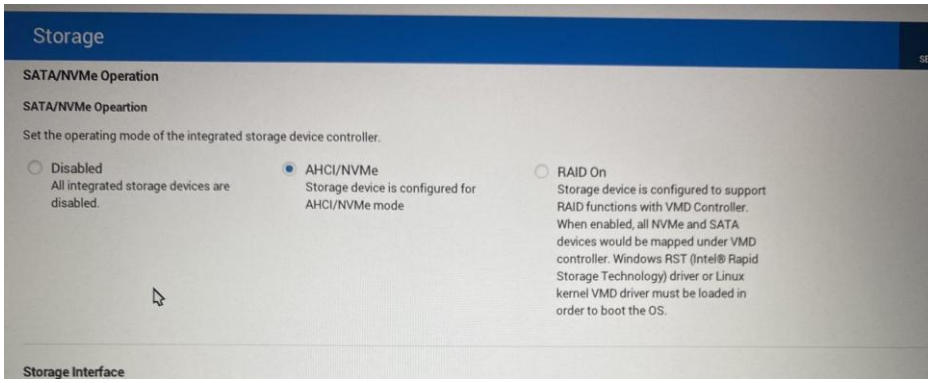
- **Ancien BIOS (Interface Texte**) : Allez dans Power Management > Wireless Radio Control et activez les options équivalentes.



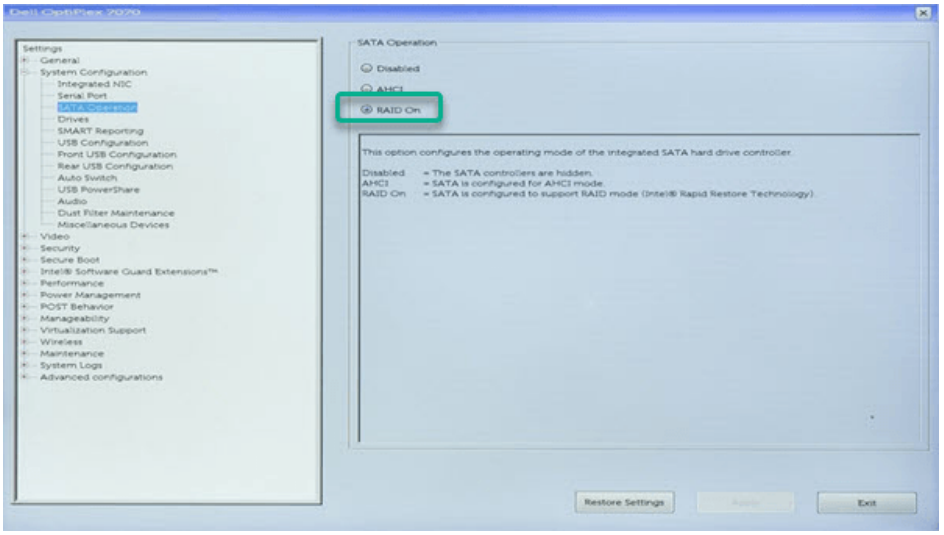
6.2.2.2 Configuration du stockage (Mode AHCI)

Pour garantir la compatibilité sans injecter les pilotes Intel Rapid Storage (IRST), le contrôleur doit être configuré en **AHCI**.

- **BIOS Récent** : Sous l'onglet Storage ou Connection, sélectionnez l'option AHCI/NVMe.



- **Ancien BIOS :** Allez dans System Configuration > SATA Operation et sélectionnez AHCI.



Note : Le passage en mode AHCI est indispensable si le poste était initialement configuré en "RAID ON".

Une fois le BIOS configuré, démarrez le poste sur le réseau (PXE/WADS).

6.2.3. Gestion du déploiement

6.2.3.1. Enregistrement de la machine

Sur le poste client, attendez l'invite de commande pour saisir le **Hostname**.

- Validez le nom d'hôte, puis cliquez sur **Retry Deployment**.
- Basculez sur la console WAPT, onglet **Déploiement d'OS**.

6.2.3.2. Lancement du déploiement

Dans l'onglet "Déploiement d'OS", les machines sont centralisées au centre, tandis que les images, configurations et pilotes sont à droite.

- **Vérification :** Assurez-vous que la machine apparaît correctement dans la liste des machines en attente.
- **Assignation :** Faites un clic droit sur la machine cible :
- Sélectionnez **Choisir une configuration**.
- Sélectionnez **Pousser les pilotes** (selon le modèle).
- **Exécution :** Faites un clic droit sur la machine et sélectionnez Démarrer le déploiement.

Une fois le déploiement WADS terminé, une intervention locale est requise pour finaliser l'environnement utilisateur.