Institut Universitaire de Technologie,

Aix-Marseille Université

ANNEXES

RAPPORT DE STAGE de fin de deuxième année

Bachelor Universitaire de Technologie

Spécialité Réseaux et Télécommunications

Parcours cybersécurité

Déploiement d'un serveur WAPT

Eliott AUROUZE

Institut de Neurosciences de la Timone

Responsable entreprise : Mr Arnaud CRUZEL

Responsable académique : Mr Éric SOCCORCI

2023

Table des matières

1 Wapt Documentation

1.1 Informations générales

Version Wapt 2.3 FQDN = Wapt.int.univ-amu.fr nom du serveur Wapt = Wapt dns = l'adresse IP est = 10.164.0.227/24 passerelle = 10.164.0.1 Domain contrôleur =

1.1.2 Conteneur

Le serveur Wapt est basé sur Debian 11 dans un conteneur qui tourne sur le cluster Proxmox il a 8Gb de RAM et 4 cœur CPU

1.1.3 Configuration réseau

- Modifier le fichier `/etc/hostname` et y renseigner le nom FQDN du serveur.

```
# /etc/hostname of the WAPT Server
Wapt.int.univ-amu.fr
```

- Configurer le fichier `/etc/hosts`, s'assurer de mettre à la fois le FQDN et le nom court du serveur.

```
127.0.0.1       localhost
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
# --- BEGIN PVE ---
10.164.0.227 Wapt.int.univ-amu.fr Wapt
# --- END PVE ---
```

- Configurer l'adresse IP du serveur WAPT dans `/etc/network/interfaces`

```
# /etc/network/interfaces of the WAPT Server
```

```
auto eth0
iface eth0 inet static
  address 10.164.0.227
  netmask 255.255.255.0
  gateway 10.164.0.1
```

- Appliquer la configuration réseau en redémarrant la machine avec un `reboot`

```
reboot
```

- Après le redémarrage, configurer la langue du système en anglais afin d'avoir des journaux non localisés pour faciliter la recherche des erreurs courantes.

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

- Vérifier si la machine est correctement synchronisée avec le serveur NTP. Si elle n'est pas synchronisée, se référer à la documentation du système d'exploitation pour configurer **timedatectl**.

```
timedatectl status
```

- Mettre à jour et à niveau le système d'exploitation et s'assurer que le paquet d'Autorités de Certification par défaut de Debian est installé.

```
apt update && apt upgrade
apt install ca-certificates -y
```

- Redémarrer le serveur.

```
reboot
```

1.2 Installation et configuration de Wapt

- Mettre à jour la source APT, récupérer la clé « *.gpg* » de Tranquil IT, puis ajouter le dépôt de Tranquil IT.

```
apt install apt-transport-https lsb-release gnupg wget -y
wget -O - https://Wapt.tranquil.it/$(lsb_release -is)/tisWapt-pub.gpg | apt-key add -
echo "deb https://Wapt.tranquil.it/$(lsb_release -is)/Wapt-2.3/ $(lsb_release -c -s) main" >
/etc/apt/sources.list.d/Wapt.list
```

- Installer les paquets du Serveur WAPT.

```
export DEBIAN_FRONTEND=noninteractive
apt update
apt install tis-Waptserver tis-Waptsetup -y
unset DEBIAN_FRONTEND
```

1.2.3 Script de post-configuration du serveur WAPT

- Lancer le script.

```
/opt/Wapt/Waptserver/scripts/postconf.sh
```

- Cliquer sur Oui pour lancer le script de post-configuration.

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

- Choisir 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 >
```

- Choisir le mode d’authentification pour l’enregistrement initial des agents WAPT (dans notre cas option 2):
- Le choix #1 permet d’enregistrer les ordinateurs sans authentification. Le serveur WAPT enregistre tous les ordinateurs qui demandent à être enregistré.
- Le choix #2 active l’enregistrement initial basé sur Kerberos (vous pouvez l’activer plus tard).
- Le choix #3 n’active pas le mécanisme d’authentification Kerberos pour l’enregistrement initial des machines équipées de WAPT. Le serveur WAPT va demander un identifiant et mot de passe pour chaque machine qui s’enregistre.

```
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 >
```

- Choisir si l'on veut l'option de déploiement d'os dans notre cas "yes"

```
Do you want to activate os deployment?

      < Yes >       < No >
```

- L'étape d'après demande s’il faut un mot de passe pour déployer des os, dans notre cas on sélectionne oui

```
Would you like to activate secure authentication on wads?
```

```
< Yes >      < No >
```

- Vous pouvez choisir le sous réseau dans notre cas nous allons passer cette étape

```
Would you like to mention an IP subnet exempt from wads authentication
```

```
< Yes >      < No >
```

- Sélectionnez Oui pour configurer Nginx.

```
Do you want to configure nginx?
```

```
< Yes >      < No >
```

- Remplir le FQDN du serveur WAPT.

```
FQDN for the WAPT Server (eg. Wapt.example.com)
```

```
----------------------------------------------
Wapt.int.univ-amu.fr
----------------------------------------------
```

```
< OK >      < Cancel >
```

- Nginx est maintenant configuré, sélectionner OK pour redémarrer **Nginx**:

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

```
< OK >
```

- La post-configuration est terminéé veuillez vous connecter sur la page pour voir si le serveur marche

```
Postconfiguration completed.
```

Please connect to https://Wapt.int.univ-amu.fr/ to access the WAPT Server.

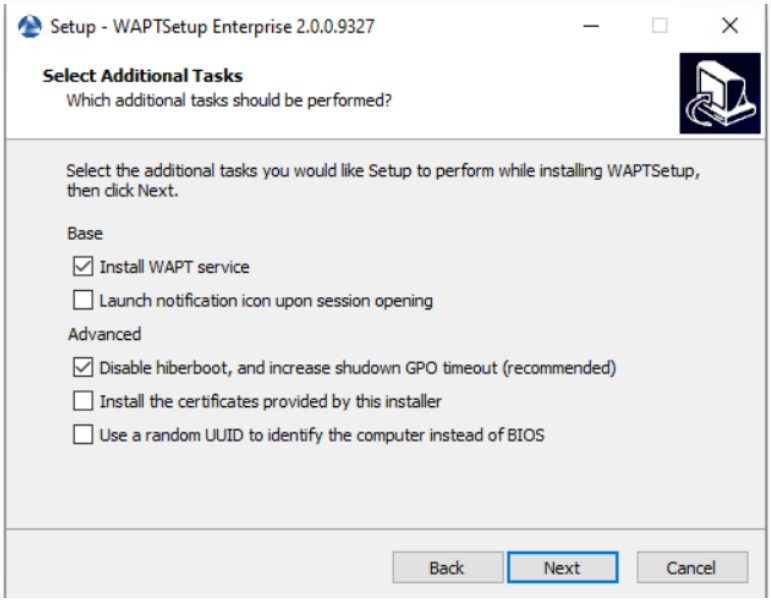
< OK >

1.3 Console de gestion WAPT

1.3.1 Installation de la console

Nous allons maintenant nous connecter à la console de gestion

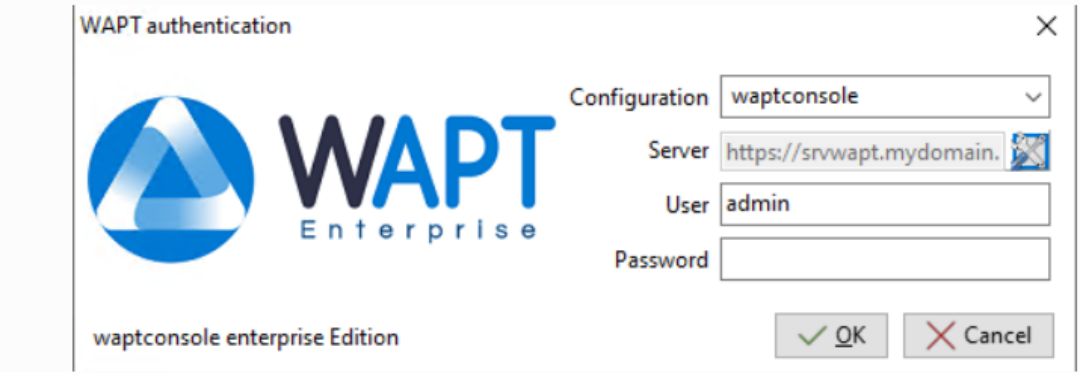
- aller sur la page https://Wapt.univ-amu.fr et cliquer sur Wapt serveur dans la barre de menu en haut puis WAPTsetup (pour installer sur une machine d'administration) cela va vous télécharger le soft, installer le sur votre machine administrateur, je ne détaille que les étapes importantes
-



- Remplir les deux url par
- Repository URL : https://Wapt.int.univ-amu.fr/Wapt
- Server URL: https://Wapt.univ-amu.fr

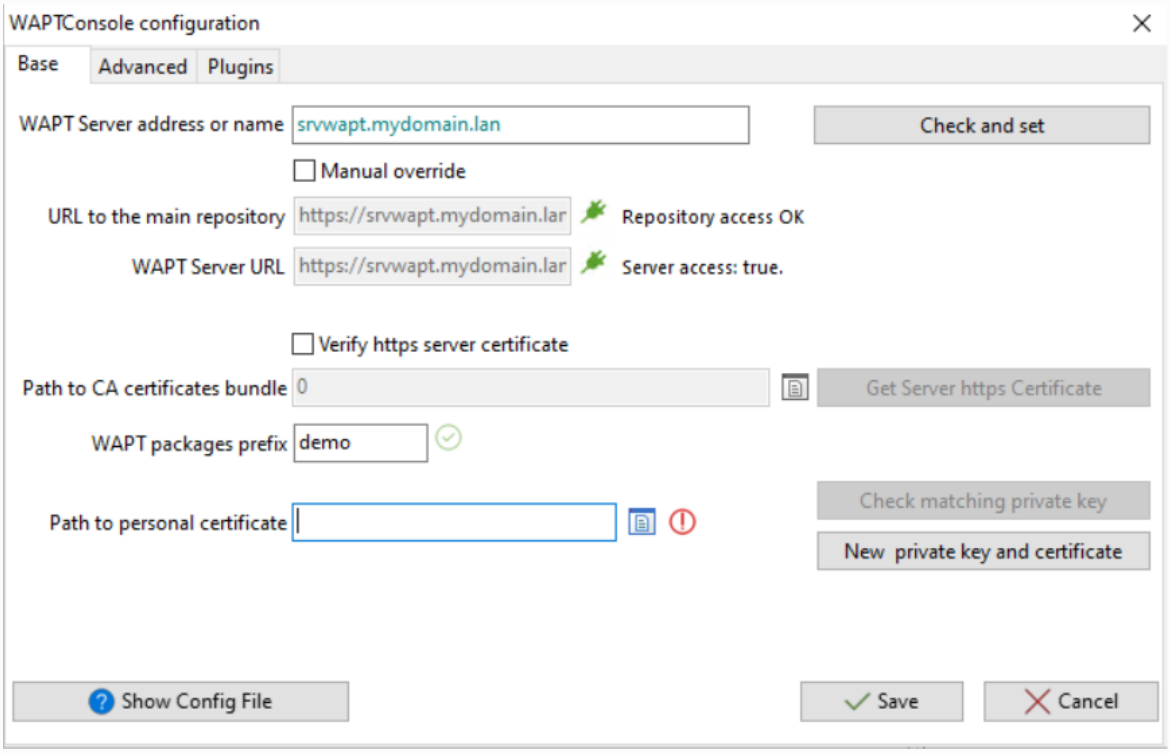
1.4 Démarrer la console WAPT

- Rentrer en utilisateur admin et en mot de passe le mot de passe configuré dans la configuration initial

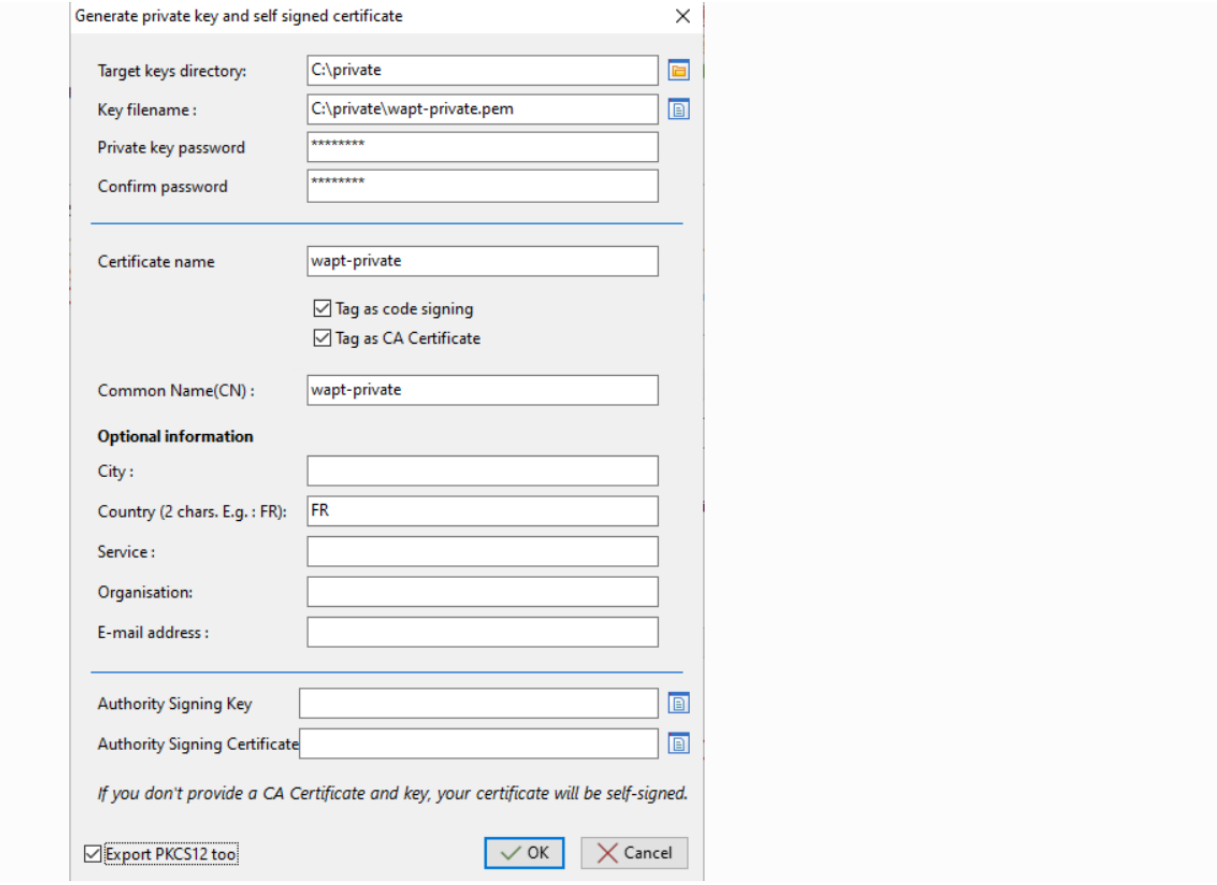


1.4.1 Si erreur du certificat (ce qui est normal pour la première connexion)

- Cliquer sur oui pour ouvrir la fenêtre de création

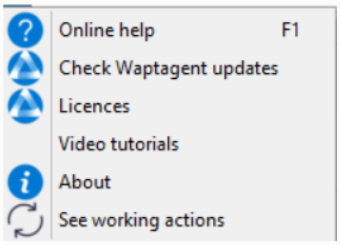


- Ensuite cliquer sur New private key and certificate et remplir comme ci dessous

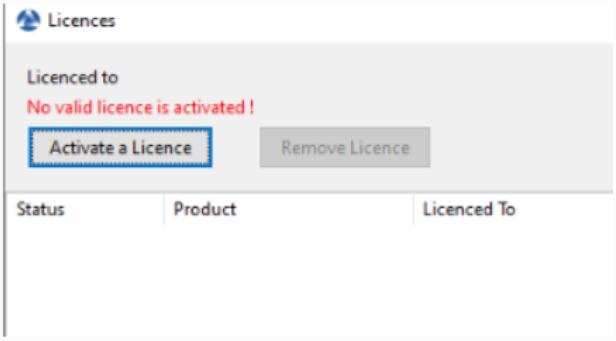


1.4.2 Activer la licence

- Dans la console WAPT, cliquer sur l'onglet ? :



- Choisir Licences :



- Sélectionner le fichier `licence.lic`
- Si cela ne fonctionne pas fermer la fenêtre des license et la re ouvrir

1.5 Kerberos et SSO

Nous allons maintenant configurer Kerbos pour que les utilisateurs administrateur et les utilisateurs lambda puissent se connecter grâce à l'active directory

1.5.1 Installation des composants Kerberos et configuration du fichier krb5.conf

- installer krb5

```
apt install krb5-user msktutil libnginx-mod-http-auth-spnego
```

- modifier le fichier /etc/krb5.conf

```
[libdefaults]
    default_realm = MYDOMAIN.LAN
    dns_lookup_kdc = true
    dns_lookup_realm=false
```

- créer votre Keytab HTTP avec la commande **msktutil**.

```
msktutil --server DOMAIN_CONTROLER --precreate --host $(hostname) -b cn=computers --service HTTP --
description "host account for Wapt server" --enctypes 24 -N
msktutil --server DOMAIN_CONTROLER --auto-update --keytab /etc/nginx/http-krb5.keytab --host $(hostname) -N
```

1.5.2 configuration de Kerberos pour le serveur WAPT

- Utiliser le script de post-configuration pour configurer le serveur WAPT afin d'utiliser Kerberos

```
/opt/Wapt/Waptserver/scripts/postconf.sh --force-https
```

L'authentification Kerberos sera maintenant configurée.

1.5.3 Activer le ssl/tls

- Pour que kerberos fonctionne il faut activer le ssl/tls, on a donc mis le certificat dans le dossier /usr/local/share/ca-certificates/ puis effectuer la commande suivante

```
update-ca-certificates
```

==Attention de bien mettre l'extention en .crt==

- Rajouter cette ligne de commande dans le fichier de conf

```
ldap_auth_ssl_enabled = True
```

1.5.4 SSO

Il existe 3 méthodes pour l'authentification SSO, nous utilisons ici la troisième qui est la plus sécurisée il ne faut pas oublier l'étape "activer le ssl/tls" juste au-dessus

- activer Kerberos pour relancer le script de post configuration (/opt/Wapt/Waptserver/scripts/postconf.sh) et mettre

```
use_kerbos = True
```

Normalement cela est déjà activé si vous avez suivi les étapes au-dessus

- Activer ldap et la vérification du certificat de ldap comme suit (/opt/Wapt/conf/Waptserver.ini):

```
ldap_auth_ssl_enabled = True
verify_cert_ldap = True
```

- Mettre toute ces options dans le fichier de configuration``

```
ldap_account_service_login = Wapt-ldap@intlocal.univ-amu.fr
ldap_account_service_password = **********
ldap_auth_server = pdcad0.intlocal.univ-amu.fr
ldap_auth_base_dn = DC=intlocal,DC=univ-amu,DC=fr
use_Kerberos = True
```

Les options `ldap_account_service_login` et `ldap_account_service_password` nécessitent un compte utilisateur dans votre Active Directory, ce compte doit juste avoir les droits pour lire les groupes et les membres des groupes. WAPT doit avoir des droits de lecture sur l'attribut `memberof` dans l'Active Directory.

- Redémarrer le serveur

```
systemctl restart Waptserver Wapttasks
```

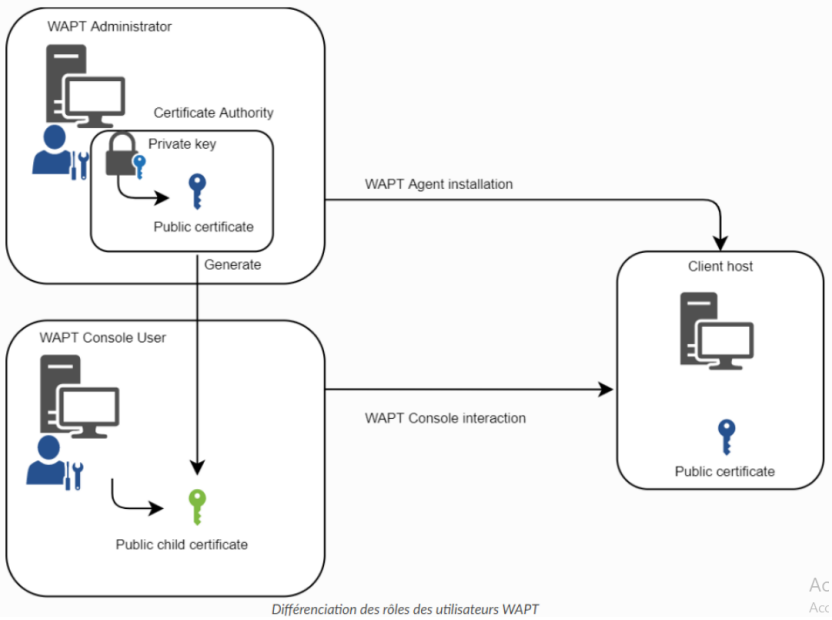
1.6 Créer un nouvel utilisateur admin

1.6.1 Principe de certificat et de droit dans Wapt

Il y a plusieurs éléments à prendre en compte il y a le compte administrateur qui permet de mettre les droits administrateur à d'autres comptes mais si il n'y a pas de certificat lié à un compte administrateur celui-ci ne pourra rien faire

Pour ce faire il faut créer un certificat avec le certificat originel ce qui crée un sous certificat de confiance

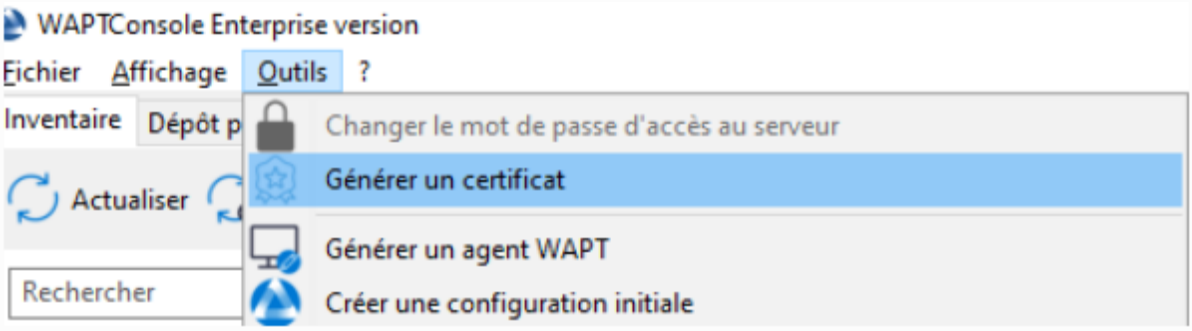
- Si le certificat public utilisé sur la console WAPT n'est pas dérivé de la clé privée utilisée pour générer les agents WAPT, aucune interaction ne sera possible.
- Les certificats enfants des clés privées sont fonctionnels pour les interactions.



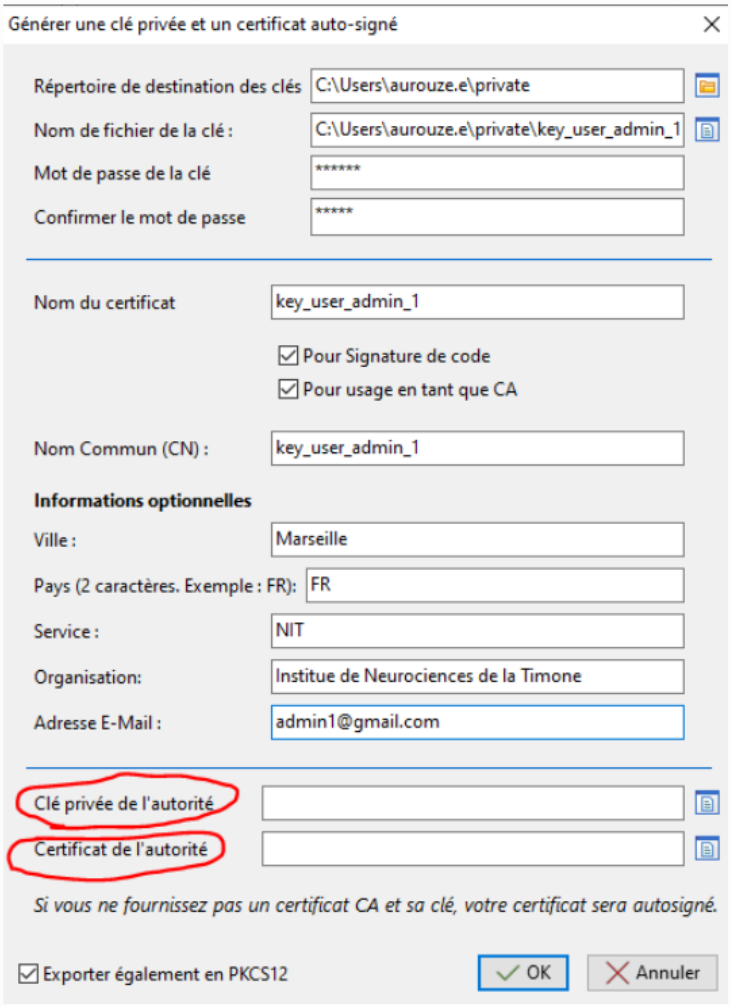
Différenciation des rôles des utilisateurs WAPT

1.6.2 Tutoriel

- Pour commencer on va devoir créer un certificat pour notre nouvel utilisateur

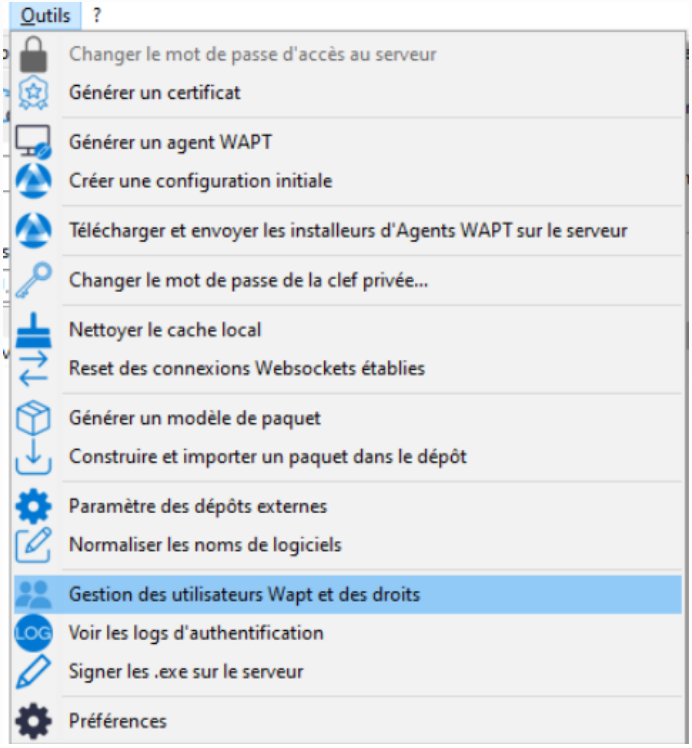


- Remplir toutes les informations, le plus important étant les deux dernières cases, on doit mettre la clef privée et le certificat de l'administrateur qui a créé l'agent Wapt ou du moins qui est considéré par certificat de confiance lors de la génération du client Wapt, dans notre cas nous avons donné le certificat administrateur le tout premier créé.

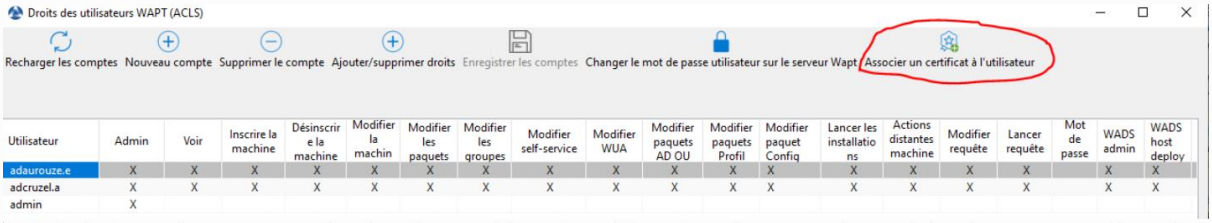


Le certificat alors créé hérite alors des droits du certificat administrateur

- Une fois que vous avez le certificat, aller dans Gestion des utilisateur Wapt.



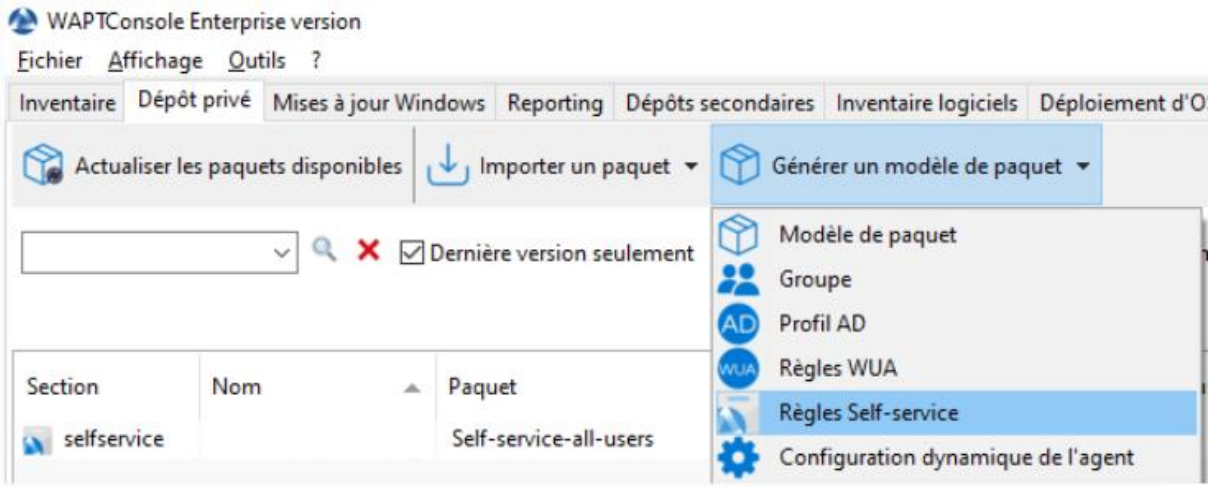
Vous aller avoir la liste des utilisateurs qui se sont connectés via l'active directory sur la console Wapt, cliquer sur l'utilisateur à qui vous souhaitez donner les droits et cliquer sur Associer un certificat à l'utilisateur, cela vous ouvre une fenêtre d'explorateur Windows à ce moment l'associer au certificat précédemment créé.



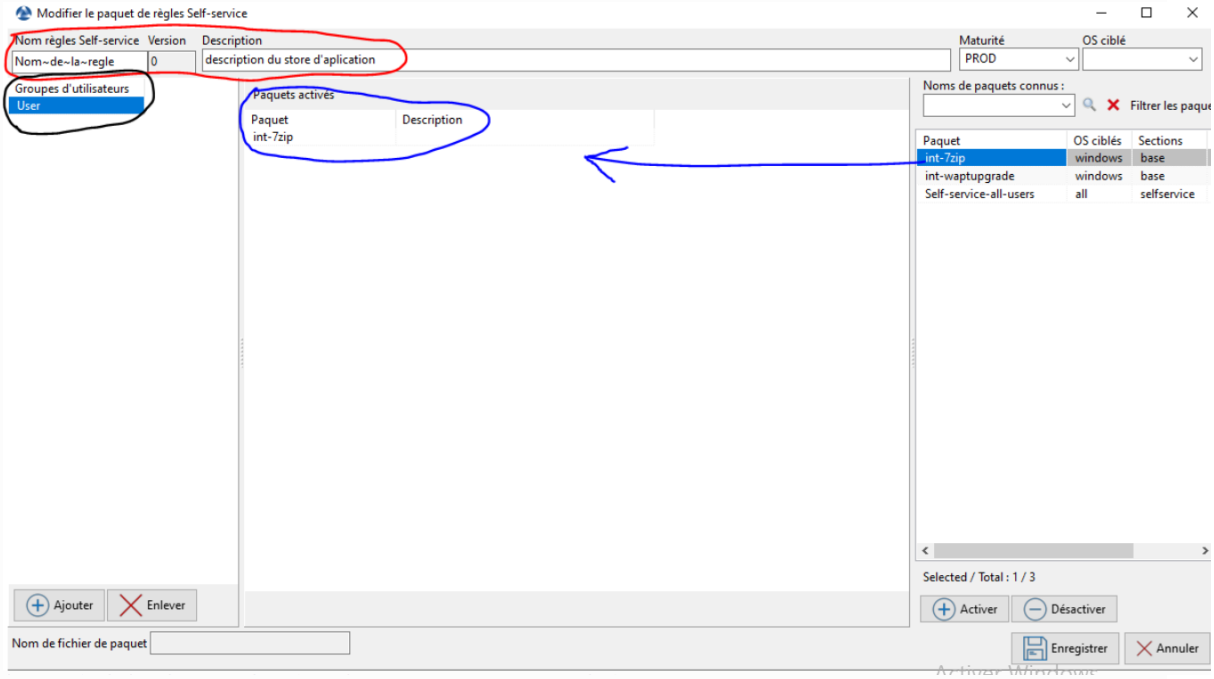
* Une fois cela fait, votre utilisateur peut envoyer des ordres au client Wapt de l'INT par exemple il peut envoyer des messages sur les postes, déployer des paquets etc.…, n'oublier pas de cocher les options d'administration que vous souhaitez car même avec le certificat valide cela ne suffit pas pour avoir les droits.

1.7 Comment activer le self-service

- aller dans l'onglet dépôt privé > générer un modèle de paquet > Règles self-service



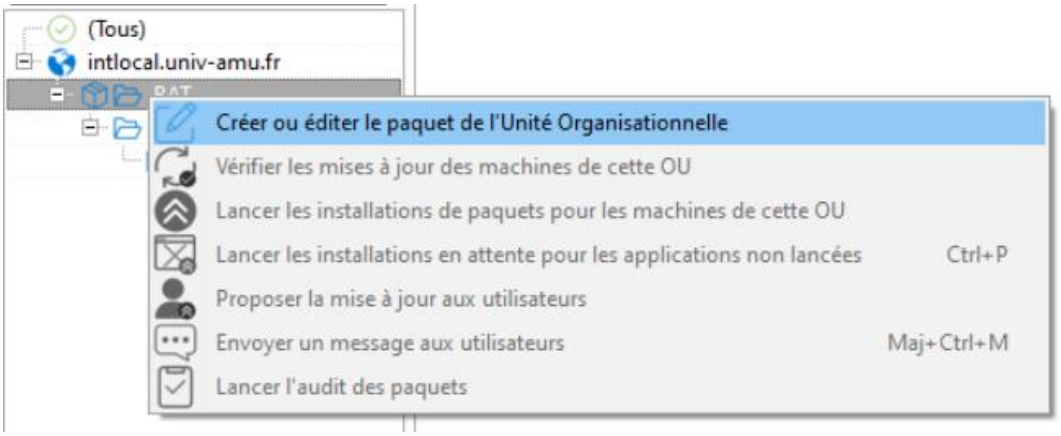
- Sur la fenêtre il y a plusieurs options à remplir **En rouge** Nom du store et sa description, en **Noir** le ou les groupe(s) de l'active directory qui ont le droit d'accéder au store, et en **Bleu** tous les paquets du dépôt sont à droite il faut les glisser au milieu pour les rajouter au store.

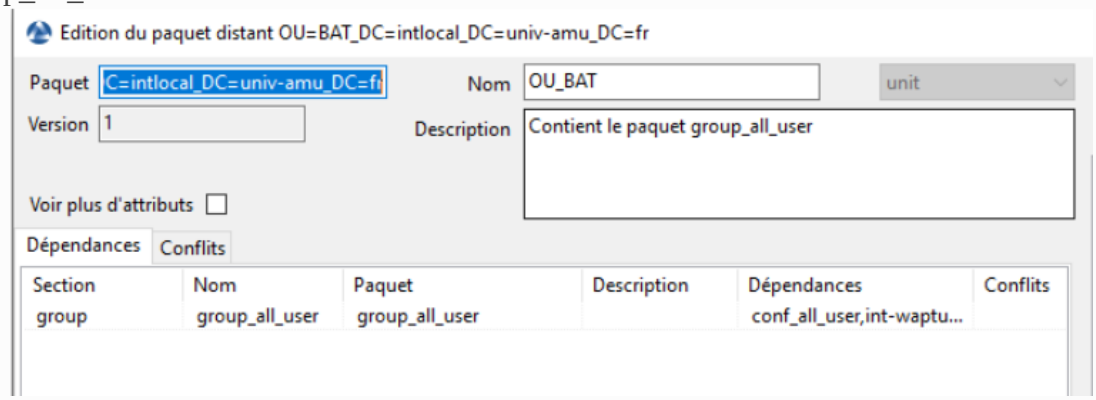


- Il faut ensuite déployer le paquet self-service sur les postes comme pour un paquet classique.

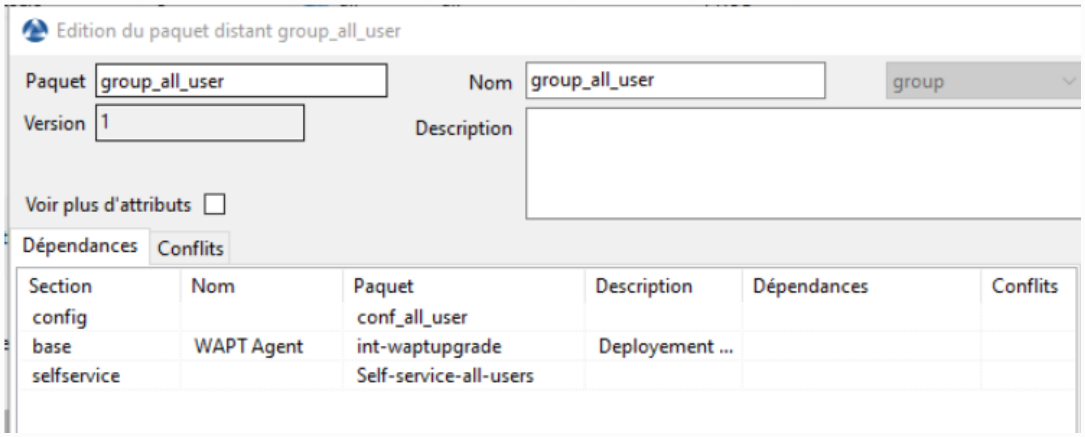
1.8 Comment la configuration Wapt et les paquets importants sont déployés dès l'installation

1. Nous avons créé un paquet d'organisation

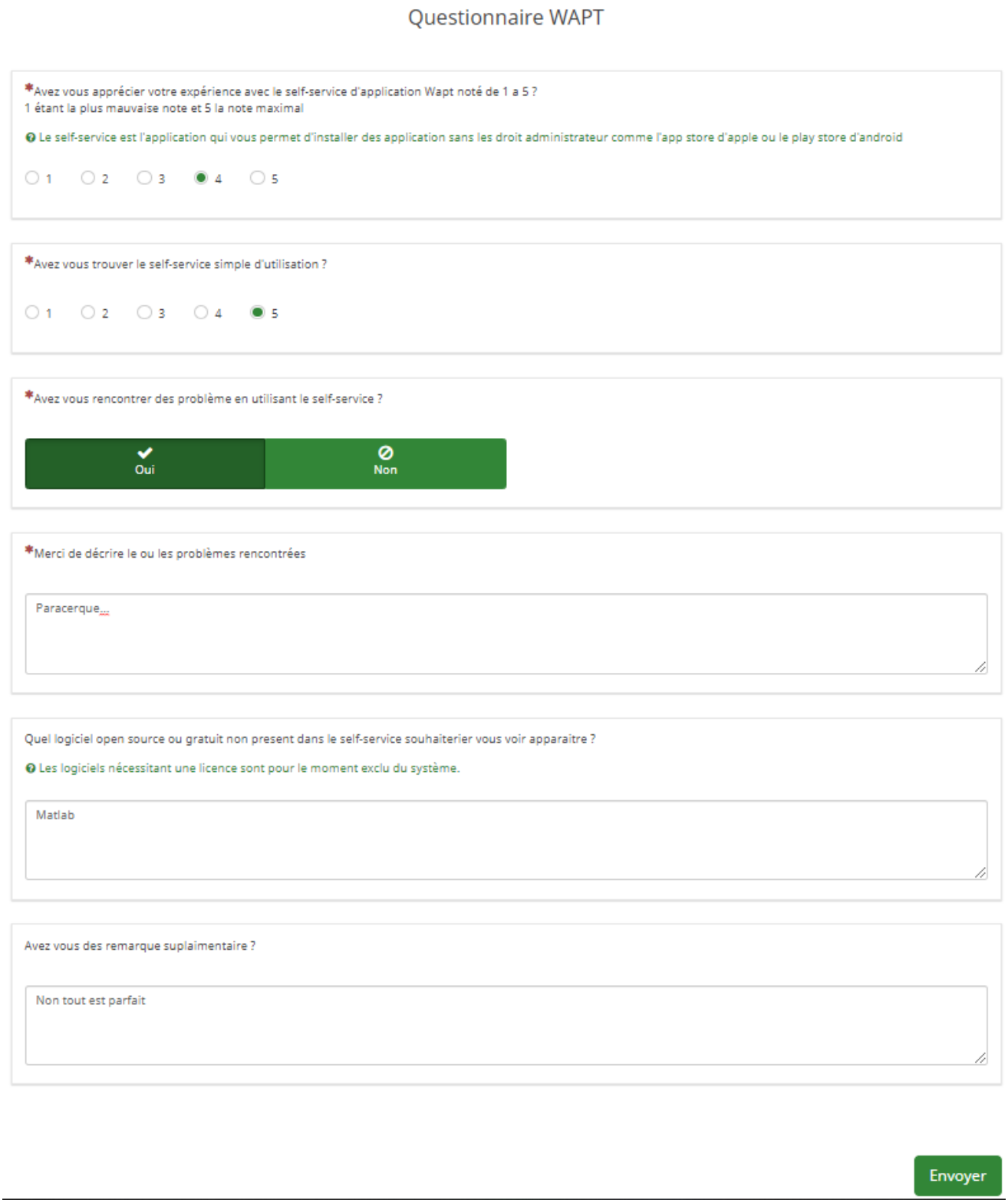
2. 

3. Dans ce paquet nous avons demandé d'installer le paquet de type paquet group, group_all_user
4. 

5. Le paquet group_all_user contient les paquets suivants :
6. conf_all_user = est un paquet de configuration qui vas configurer les agent Wapt
7. int-Waptupgrade = est le paquet de l'agent Wapt
8. Self-service-all-user = le paquet self service avec tous les logiciels que tout le monde a le droit d'avoir accès par exemple chrome, Firefox, etc...



Questionnaire de retour d'expérience des utilisateurs



Documentation Utilisateur

Wapt qu'est-ce que c'est ?

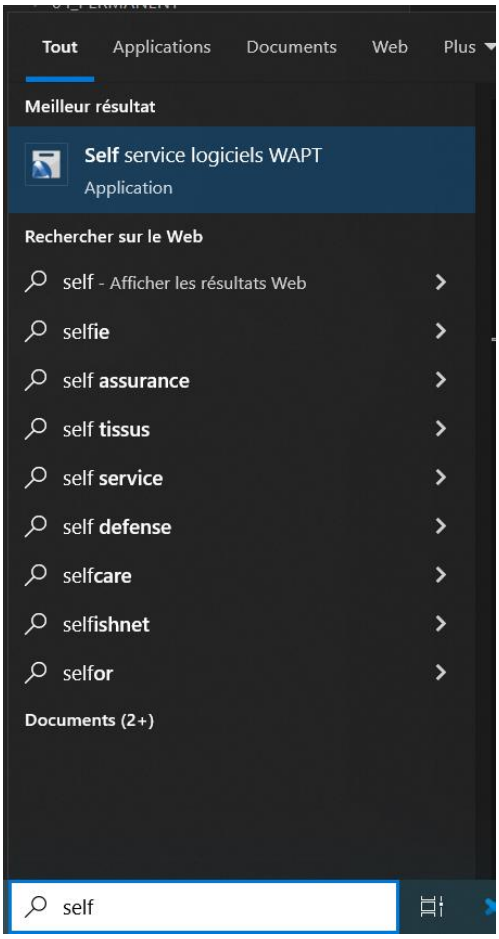
Wapt est un outil qui vous permet d'avoir accès à un store d'application, un peu comme les stores tel que : l'App store d'Apple, Play store de Google ou encore le Windows store de Windows.

Voici ci-dessous ce qu'en dit le site officiel.

Pour accéder à ce store applicatif il vous suffit d'aller dans la barre de recherche Windows est de taper self-service. Une fois connecté au Self-Service WAPT, vous avez accès :

- Aux logiciels que vous pouvez installer ou mettre à jour sur le poste.
- Aux logiciels installés sur votre poste pour les désinstaller.
- À des fonctions de recherche et de filtrage des logiciels, surtout pour les grosses entreprises.
- À de nombreuses informations sur les logiciels avant de les installer.

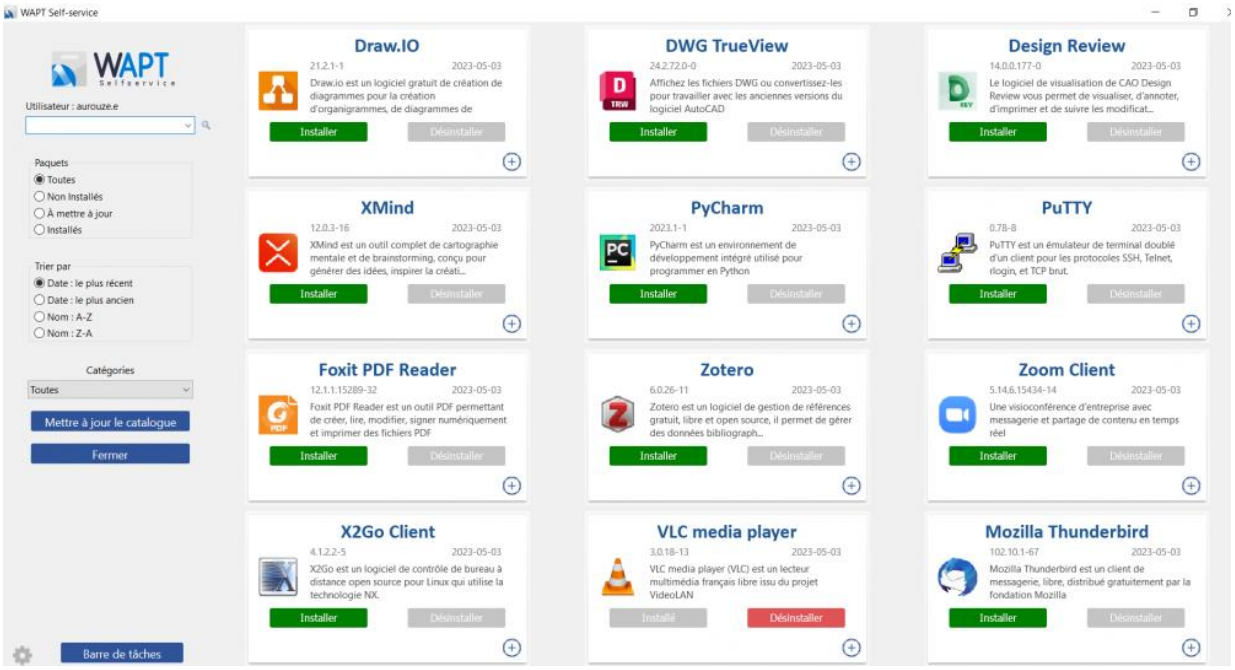
Du côté de l'installation des logiciels, il est possible de lancer plusieurs installations en même temps, ce qui peut être pratique à l'arrivée de nouveaux collaborateurs. Vous pouvez également consulter la barre des tâches pour obtenir plus d'informations sur l'installation d'une application.



Utilisation

Une fois ouvert il vous suffit d'appuyer sur installer pour installer l'application de votre choix, pour désinstaller il faut appuyer sur le bouton désinstaller c'est aussi simple que ça :

PS : Si cela vous demande un mot de passe de connexion il faut rentrer votre mot de passe de session Windows celui qui vous serre à vous connecter à votre ordinateur à son allumage.



Si les icones ne s’affichent pas, appuyez sur mettre à jour le catalogue

Si vous n'avez pas accès au service alors il faut vous connecter en filaire au laboratoire ou en VPN à distance puis, ouvrir une invite de commande et taper "gpupdate /force", ensuite redémarrez votre ordinateur, si tout s’est bien passé vous devriez accéder à Wapt.

```
C:\Users\aurouze.e>gpupdate
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.


C:\Users\aurouze.e>
```