

OCS



- 1) Installation OCS**
- 2) Travail sur OCS**
- 3) CVE Search**

# Partie 1

## Question A :

En relisant la procédure fournie par le stagiaire, on constate qu'elle se limite à un enchaînement de commandes réalisées en tant que super-utilisateur (mise à jour du système, installation de nombreux paquets, utilisation de **cpan**, création de la base MySQL « ocsweb », téléchargement du code source sur GitHub, lancement d'un script interactif, etc.). Elle ne contient ni contexte ni justification des choix, ne décrit pas l'environnement ni les prérequis (version exacte de Debian, accès réseau, rôle du serveur). Elle n'explique pas non plus ce que font les paquets installés ni les réponses à donner durant les étapes interactives ; par exemple, on demande de répondre par huit fois « Entrée » ou « y » sans dire à quelles questions cela correspond. De plus, la procédure est écrite pour une Debian 11 alors que l'objectif est une Debian 13, ce qui peut entraîner des incohérences de version.

Utiliser automatiquement : `apt -y full-upgrade` en production peut installer des paquets non testés, et l'absence de vérification des retours de commande ou de journalisation rend difficile tout diagnostic.

Enfin, l'étape de configuration MySQL crée l'utilisateur **ocs** avec un mot de passe très faible (ocs) et lui attribue tous les privilèges sur la base. Pour une procédure d'entreprise, on s'attendrait à une documentation structurée (objectif, prérequis, étapes détaillées, validation), à un script automatisé reproductible avec gestion des erreurs et à l'utilisation des dépôts officiels plutôt que des compilations manuelles. La procédure actuelle ne répond pas à ces exigences.

## Question B :

Sur le plan de la sécurité, de nombreuses bonnes pratiques ne sont pas respectées. La procédure utilise le compte **root** sans recourir à **sudo** et ne demande pas de mot de passe fort pour le compte MySQL, alors que la commande **mysql\_secure\_installation** sert justement à renforcer la base ; ici on répond « n » à la protection du compte root et on conserve un compte MySQL sans mot de passe. Le mot de passe de l'utilisateur **ocs** est faible et prévisible ; l'interface web est accessible en HTTP sans chiffrement (<http://.../ocsreports>), ce qui expose les identifiants en clair.

Le téléchargement de l'archive OCS se fait par **wget** sans vérification d'empreinte ni signature. La procédure ne met en place ni pare-feu ni SELinux/AppArmor, n'isole pas le service web et n'indique pas comment restreindre l'accès à l'interface d'administration. Il n'y a aucune recommandation sur la rotation des journaux, la sauvegarde de la base ou la mise à jour régulière du logiciel.

Pour améliorer la sécurité, il faudrait : créer les utilisateurs MySQL avec des mots de passe générés et limiter leurs privilèges au strict nécessaire ; exiger la mise en place d'un certificat TLS et forcer l'accès en HTTPS ; vérifier l'empreinte de l'archive téléchargée ou, mieux, utiliser les paquets disponibles dans les dépôts Debian ; n'installer que les dépendances indispensables afin de réduire la surface d'attaque ; mettre en place un pare-feu pour n'ouvrir que les ports nécessaires (HTTP/HTTPS et éventuellement 3306 si accès MySQL distant requis) ; documenter précisément chaque réponse aux scripts interactifs ; changer les identifiants par

défaut de l'interface OCS et, si possible, restreindre l'accès par adresse IP ou VPN ; enfin, exécuter le serveur web avec un compte de service au lieu de root. Ces mesures permettraient d'aligner l'installation sur les bonnes pratiques en vigueur en entreprise.

## Question C :

### C) 1) Installation du serveur Web Apache, la base Maria DB et PHP avec les modules nécessaires

```
root@vbox:/home/sio# apt install -y curl wget sudo vim
```

```
root@vbox:/home/sio# sudo apt install apache2 mariadb-server libapache2-mod-perl2 php php-cli php-mysql php-gd php-curl php-xml php-zip liba
pache-dbi-perl
apache2 is already the newest version (2.4.65-2).
mariadb-server is already the newest version (1:11.8.3-0+deb13u1).
php is already the newest version (2:8.4+96).
php-mysql is already the newest version (2:8.4+96).
php-gd is already the newest version (2:8.4+96).
php-curl is already the newest version (2:8.4+96).
php-xml is already the newest version (2:8.4+96).
php-zip is already the newest version (2:8.4+96).
Installing:
 libapache2-dbi-perl libapache2-mod-perl2 php-cli php-xml
```

### 2) Sécurisation de Maria DB

```
root@vbox:/home/sio# sudo mariadb-secure-installation

NOTE: MariaDB is secure by default in Debian. Running this script is
useless at best, and misleading at worst. This script will be
removed in a future MariaDB release in Debian. Please read
mariadb-server.README.Debian for details.

Enter root user password or leave blank:

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] y
Enabled successfully (or at least no errors was emitted)!
Reloading privilege tables..
... Success!

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!
```

### 3) Création de la base et utilisateur OCS

Se connecter à MySQL en tant que root

```
sudo mysql -u root -p
```

1. Créez la base de données

```
CREATE DATABASE ocsweb;
```

2. Créez un utilisateur 'ocs' dédié qui ne peut se connecter que en localhost et avec un MOT DE PASSE SOLIDE.

```
CREATE USER 'ocs'@'localhost' IDENTIFIED BY 'OCSPASSWORD';
```

```
GRANT ALL PRIVILEGES ON ocsweb.* TO 'ocs'@'localhost';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

### 4) Installation OCS Server

**Etape 1 :** En premier lieu on télécharge et décompresse les fichiers avec les commandes suivantes

```
cd /tmp/
```

```
wget https://github.com/OCSInventory-NG/OCSInventory-ocsreports/releases/download/2.11.1/OCSNG_UNIX_SERVER-2.11.1.tar.gz [cite: 41, 42] tar xfvz OCSNG_UNIX_SERVER-2.11.1.tar.gz
```

```
cd OCSNG_UNIX_SERVER-2.11.1
```

**Etape 2 :** On lance le script d'installation avec la commande :

```
sudo sh setup.sh | tee /tmp/installOCS.log
```

**Etape 3 :** On applique ensuite les permissions et active la configuration Apache.

```
sudo chown -R www-data:www-data /var/lib/ocsinventory-reports/
```

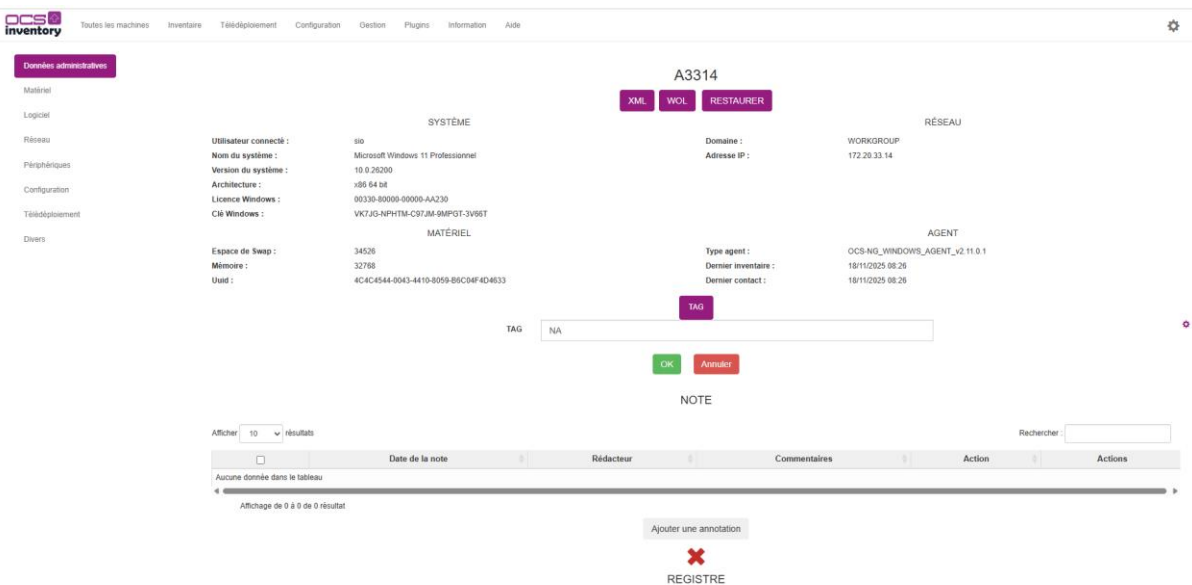
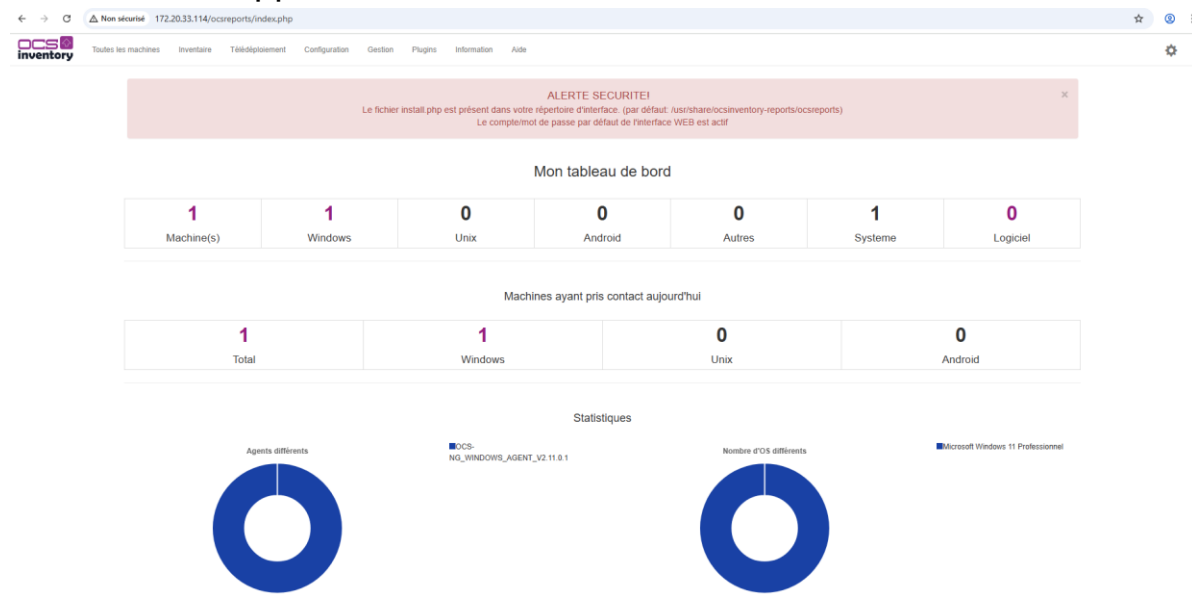
**sudo a2enconf ocsinventory-reports && sudo a2enconf z-ocsinventory-server && sudo a2enconf ocsinventory-restapi**  
**sudo systemctl restart apache2**

**Etape 4 :** On peut ensuite se connecter à l'interface web via "notreip/ocsreports"

**Etape 5 :** Il faut ensuite se connecter à la base de données

**Etape 6 :** Il faut ensuite se connecter à ocs.

**Etape 7 :** Une fois l'agent installé sur le poste souhaité, on peut remonter un rapport au serveur



Waïl BOUHLAGHEM  
Kilian MOLIERE

ocs inventory Toutes les machines Inventaire Télédéploiement Configuration Gestion Plugins Information Aide ⚙️

**ALERTE SECURITE!**

Le fichier install.php est présent dans votre répertoire d'interface. (par défaut: ./usr/share/ocsinventory-reports/ocsreports)  
Le compte/mot de passe par défaut de l'interface WEB est actif

TOUS LES ORDINATEURS ORDINATEURS ACTIFS ORDINATEURS ARCHIVES

Afficher / Cacher : Sélectionner la colonne à afficher / masquer

Ajouter une disposition  
1 Résultat(s) (Télécharger)

Rechercher

	Account info : TAG	Dernier inventaire	Machine	Utilisateur connecté	Système	RAM (Mo)	CPU (MHz)	Actions
<input type="checkbox"/>	NA	2025-11-18 08:24:44	A3314	vis	Microsoft Windows 11 Professionnel	32768	3101	<span style="color: red;">✖</span> <span style="font-size: 0.7em;">⬇</span>

Affichage de 1 à 1 de 1 résultats

Supprimer Lock du résultat Traitement par lots Configuration Télédéploier

✖

On voit maintenant l'appareil avec toutes ses informations.

## Question D :

- 1) Il faut supprimer le fichier install.php, la présence de ce fichier est un risque majeur car il pourrait permettre à un attaquant de réinitialiser ou de modifier l'installation.
- 2) Le compte "ocs" dans MySQL utilise un mot de passe par défaut " ocs " , ce qui est très dangereux. Il faut donc le modifier.
- 3) Il faut également modifier le mot de passe administrateur du serveur web qui est souvent admin/admin.

## Question E :

```

INVENTORY => Inventory changed since last run
INVENTORY => Generating XML document with Device properties
INVENTORY => XML Update BIOS
INVENTORY => XML Update 1 CPU(s)
INVENTORY => XML Update 4 Memory Slot(s)
INVENTORY => XML Update 2 Input Device(s)
INVENTORY => XML Update 32 System Port(s)
INVENTORY => XML Update 5 System Controller(s)
INVENTORY => XML Update 0 System Slot(s)
INVENTORY => XML Update 3 Sound Device(s)
INVENTORY => XML Update 3 Storage Peripheral(s)
INVENTORY => XML Update 3 Logical Drive(s)
INVENTORY => XML Update 1 Modem(s)
INVENTORY => XML Update 7 Network Adapter(s)
INVENTORY => XML Update 2 Video Adapter(s)
INVENTORY => XML Update 2 Monitor(s)
INVENTORY => XML Update 3 Printer(s)
INVENTORY => XML Update 97 Software
INVENTORY => XML Update 0 Registry Value(s)
INVENTORY => XML Update Administrative Information(s)
INVENTORY => XML Update common Device properties
COM SERVER => Initializing cURL library for sendRequest
COM SERVER => Using cURL without server authentication
COM SERVER => Disabling cURL proxy support
COM SERVER => Enabling cURL SSL server validation support using CA Bundle <C:\ProgramData\OCS Inventory NG\Agent\cacert.pem>
COM SERVER => Sending HTTP post request to URL <http://172.20.33.114/ocsinventory>
COM SERVER => HTTP Post response received <HTTP Status Code #200>
COM SERVER => Cleaning cURL library
AGENT => Inventory successfully sent
INVENTORY => Writing new inventory state
AGENT => Communication Server asked for Package Download
DOWNLOAD => Package history file successfully cleaned for duplicate IDs
DOWNLOAD => Download disabled by server
AGENT => Unloading communication provider
AGENT => Unloading plug-in(s)
AGENT => Execution duration: 00:00:18.

```

# PARTIE 2 : TRAVAIL SUR OCS

1. Vous réaliserez alors une procédure de mise en œuvre pour un agent au choix pour Linux ou Android. Vous détaillerez les tests de bon fonctionnement.

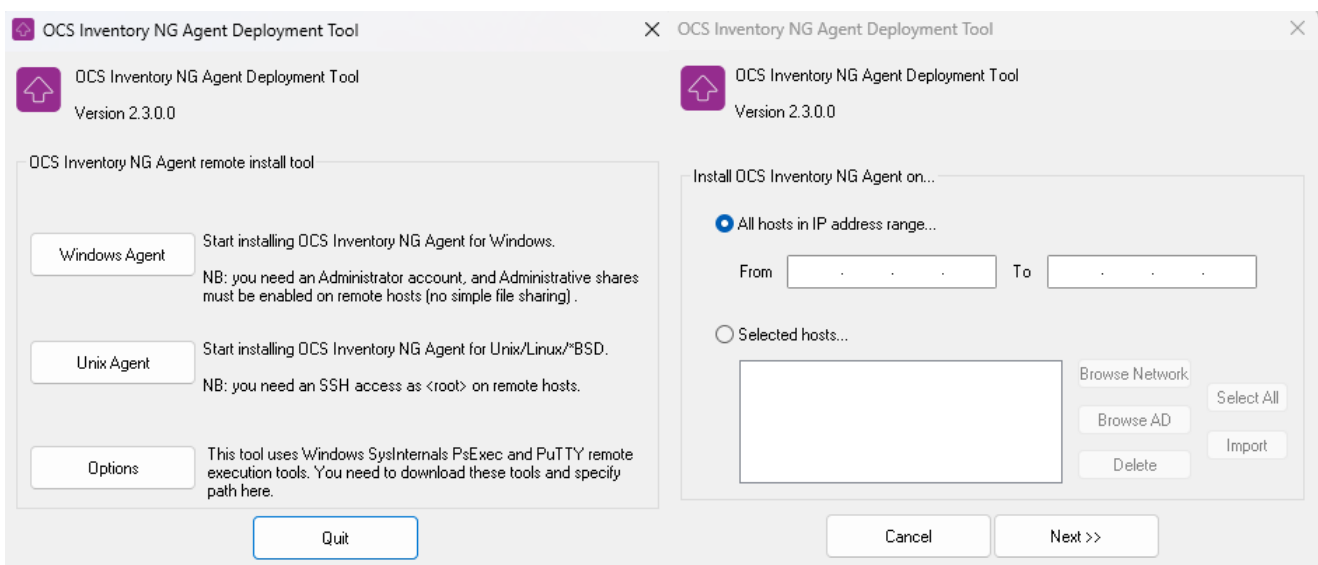
**Etape 1 :** Nous avons donc installé un agent OCS Android sur une tablette.

**Etape 2 :** Nous nous sommes après connecter sur le serveur OCS

**Etape 3 :** Puis depuis la tablette, nous avons remonté les informations au serveur OCS LINUX.

<input type="checkbox"/>	Account info : TAG	Last inventory	Computer	Connected user	Operating system	RAM (MB)	CPU (MHz)	Actions
<input type="checkbox"/>	Smartphone	2025-11-18 08:54:17	SM-T560-4554602c68aa5271	dpi	Android linux 4.4.4	1454	1300	
<input type="checkbox"/>	Smartphone	2025-11-18 08:59:12	SM-T560-fadc87835fb5b7ea	dpi	Android linux 4.4.4	1454	1300	

2. Proposez et expliquez toutes les solutions possibles ; Choisissez-en une que vous mettez en œuvre et pour laquelle vous rédigez une procédure d'installation automatique de l'agent OCS pour un poste Windows 10 ou pour un poste Windows 11.



Nous avons installé OCS AGENT DEPLOYMENT TOOL sur Windows, il permet de déployer l'agent OCS sur un parc informatique.

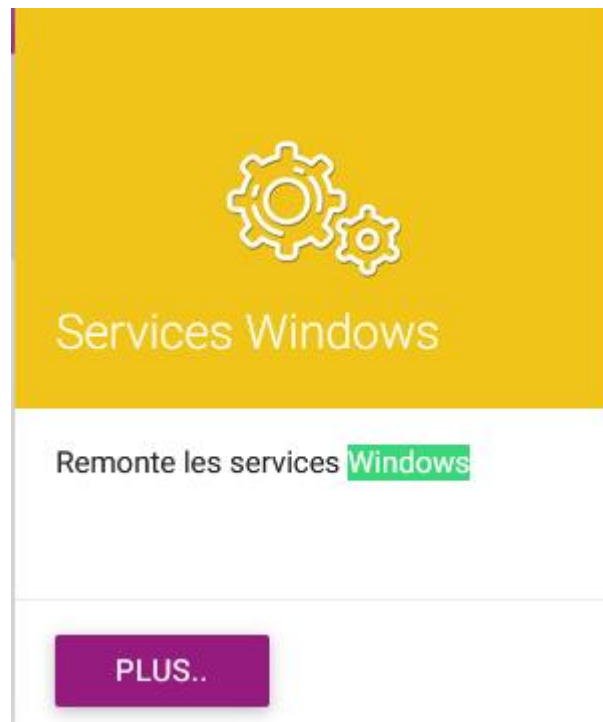
Il suffit d'aller dans l'onglet "Windows Agent" et de sélectionner ou d'entrer la range des IP ou nous souhaitons déployer l'agent.

On peut également utiliser différentes méthodes afin de déployer un agent sur plusieurs postes :

- On peut utiliser un script de démarrage machine (PowerShell ou .bat) qui exécute l'installateur de l'agent OCS en mode silencieux.
- Outils de télédistribution tiers : Si l'entreprise possède déjà un outil comme Microsoft SCCM/MECM, ManageEngine, ou PDQ Deploy, il est préférable de l'utiliser pour "pousser" l'agent.
- Script de connexion (Logon Script) : Moins fiable que la GPO "démarrage machine" car il s'exécute à l'ouverture de session utilisateur (et peut nécessiter des droits admin).
- Outil de déploiement OCS "Agent Deployment Tool" : OCS fournit un outil qui scanne le réseau et tente d'installer l'agent à distance via les partages administratifs.

**3. Vous mettrez en œuvre trois de ces plugins au choix et réaliserez un mode opératoire. Précisez les tests fonctionnels nécessaires.**

Nous avons choisis d'installer un plugin permettant de remonter les services windows



### Étape suivante : Télécharger le plugin avec `wget`

Maintenant que la résolution DNS fonctionne, tu devrais pouvoir utiliser `wget` pour télécharger le fichier ZIP du plugin depuis GitHub. Voici la commande que tu peux essayer :

```
bash Copier le code  
sudo wget https://github.com/PluginsOCSInventory-NG/services/archive/refs/heads/master.zip
```

Cela devrait télécharger le fichier `master.zip` dans le répertoire où tu te trouves. Ensuite, tu pourras extraire et installer le plugin.

### Continuer avec l'installation du plugin

#### 1. Extraire le fichier ZIP :

Une fois le fichier téléchargé, tu peux l'extraire :

```
bash Copier le code  
sudo unzip master.zip
```

Cela créera un dossier appelé `services-master`.

#### 2. Renommer le dossier du plugin (facultatif, pour simplifier) :

Tu peux renommer le dossier extrait pour le rendre plus facile à gérer :

```
bash Copier le code  
sudo mv services-master services
```

#### 3. Donner les bonnes permissions :

Assure-toi que les fichiers du plugin sont accessibles par le serveur web (généralement `www-data` pour

```

root@vbox:/usr/share/ocsinventory-reports/ocsreports/extensions# sudo wget https://github.com/PluginsOCInventory-NG/services/archive/refs/heads/master.zip
--2025-11-24 09:23:14-- https://github.com/PluginsOCInventory-NG/services/archive/refs/heads/master.zip
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/PluginsOCInventory-NG/services/zip/refs/heads/master [following]
--2025-11-24 09:23:15-- https://codeload.github.com/PluginsOCInventory-NG/services/zip/refs/heads/master
Resolving codeload.github.com (codeload.github.com)... 140.82.121.9
Connecting to codeload.github.com (codeload.github.com)|140.82.121.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'master.zip'

master.zip [ <-> ] 46.02K --.-KB/s in 0.04s

2025-11-24 09:23:15 (1.15 MB/s) - 'master.zip' saved [47121]

root@vbox:/usr/share/ocsinventory-reports/ocsreports/extensions# sudo unzip master.zip
unzip: cannot find or open master.zip, master.zip.zip or master.zip.ZIP.
root@vbox:/usr/share/ocsinventory-reports/ocsreports/extensions# sudo unzip master.zip
Archive: master.zip
856cea971ffe1e656c7510e2315e67c1f077b372
  creating: services-master/
  inflating: services-master/.travis.yml
  creating: services-master/APACHE/
  inflating: services-master/APACHE/Map.pm
  extracting: services-master/APACHE/services.conf
  inflating: services-master/LICENSE
  inflating: services-master/README.md
  creating: services-master/agent/
  inflating: services-master/agent/services.ps1
  creating: services-master/cd_services/
  inflating: services-master/cd_services/cd_services.php
  inflating: services-master/hook.xml
  inflating: services-master/infos.json
  inflating: services-master/install.php
  creating: services-master/language/
  creating: services-master/language/en_GB/
  extracting: services-master/language/en_GB/en_GB.txt
  creating: services-master/language/fr_FR/
  extracting: services-master/language/fr_FR/fr_FR.txt
  inflating: services-master/preview.png
root@vbox:/usr/share/ocsinventory-reports/ocsreports/extensions# mv services-master services
root@vbox:/usr/share/ocsinventory-reports/ocsreports/extensions# chown -R www-data:www-data services
root@vbox:/usr/share/ocsinventory-reports/ocsreports/extensions#

```

### Installer une extension

officepack

L'extension a été installée avec succès !  
 Merci de vous déconnecter et reconnecter afin de terminer l'installation.  
 Il peut être nécessaire de mettre à jour les permissions des profils pour accéder à la page de l'extension.

### Extensions installées

Afficher / Cacher :

[Ajouter une disposition](#)

3 Résultat(s) (Télécharger)

[Afficher les colonnes par défaut](#)

Afficher 10 résultats

Rechercher :

Nom de l'extension	Version	Auteur	Actions
Office Pack	3.4	Guillaume PROTET	✖
Services Windows	2	Benoit SARDA	✖
Winusers	4.1	J.C.BELLAMY	✖

Affichage de 1 à 3 de 3 résultats

**4. Rédiger une procédure explicative pour la mise en œuvre de la découverte réseau ainsi que pour la fonctionnalité de déploiement (télédiffusion). Pour cette dernière fonctionnalité, vous choisirez le déploiement d'un logiciel sous Windows indispensable pour une entreprise (contexte à préciser).**

Nous avons dû changer la limite de taille des fichiers téléchargeables afin de ne pas être bloqué par la taille du fichier que nous allons choisir.

```
; Maximum allowed size for uploaded files.  
; https://php.net/upload-max-filesize  
upload_max_filesize = 950M
```

```
; https://php.net/post-max-size  
post_max_size = 951M
```

On choisit l'installation pour windows, puis le type de fichier donc msi, puis après on nomme notre installation et on sélectionne notre fichier d'installation puis nous pouvons valider.

The screenshot shows a web browser window with the URL `172.20.33.110/ocsreports/?function=tele_build`. The page title is "Fabrication d'un paquet de télédéploiement". Below the title is a "Recharger" button. A progress bar at the bottom of the page shows four stages: "SYSTEME", "INTERACTIONS", "OPTIONS", and "CATALOGUE DE SERVICES", with "OPTIONS" being the active stage. The main heading is "Installer une application MSI". The form contains the following fields:

- Nom du paquet:
- Description:
- Fichier MSI:
- Arguments (optionnel):

A "Valider" button is located at the bottom of the form.

### Fabrication d'un paquet de télédéploiement

Recharger

Votre paquet a bien été créé dans le répertoire /var/lib/ocsinventory-reports/download/1764658819

- SYSTEME
- INTERACTIONS
- OPTIONS
- CATALOGUE DE SERVICES

### Resume

Nom	Description	Nombre de fragments	Taille totale	Priorité	Activé
Firefox	Installation de firefox	1	86357855	5	NON

Ensuite nous arrivons sur cette page-là qui nous indique que le fichier de Firefox est chargé et qu'il est prêt à être télédéployer. Or pour le moment il n'est pas activé donc nous allons le faire.

### Activation de paquets

Paquets disponibles

Paquets supprimés

Paquets créés man





Afficher / Cacher : Sélectionner la colonne à

Ajouter une disposition

1 Résultat(s) (Télécharger)

Afficher 10 résultats





Rechercher :

<input type="checkbox"/>	Timestamp	Date de création	Nom	Notifié	Succès	Erreur	Actions
<input type="checkbox"/>	1764658819	2025-12-02 08:00:19	Firefox				   

Affichage de 1 à 1 de 1 résultats



Ensuite nous arrivons sur cette page-là puis pour actionner l'activation nous cliquons sur le bouton vert valider.

<input type="checkbox"/>	Timestamp	Date de création	Nom	Notifié	Succès	Erreur	Actions
<input type="checkbox"/>	1764663554	2025-12-02 09:19:14	test				   

Serveur de fichiers 172.20.33.114/download /1764663554

Serveur https 172.20.33.114/download /1764663554

OK Annuler

Pour finir après avoir cliqué sur le bouton un pop-up va apparaître nous indiquant que le fichier d'installation est actif et qu'il peut être télédeployer maintenant.

## PARTIE 3 CVE SEARCH

Nous allons installer les dépôts git sur le serveur OCS pour pouvoir ensuite récupérer les dépôts git de CVE Search.

```
apt install git -y
```

Une fois git installer nous clonons les dépôts git de CVE Search sur le serveur OCS.

```
git clone https://github.com/cve-search/cve-search.git
```

Nous allons configurer l'environnement nécessaire pour utiliser CVE Search et MongoDB, nous allons installer les dépendances puis créer un environnement virtuel isolé pour le projet et ainsi de préparer l'installation de MongoDB.

```
xargs apt install -y < cve-search/requirements.system
```

```
apt install python3-venv -y
```

```
apt install python3-virtualenv -y
```

```
python3 -m venv /pythonENV/
```

```
/pythonENV/bin/pip3 install -r cve-search/requirements.txt
```

```
apt install gnupg curl -y
```

```
curl -fsSL https://www.mongodb.org/static/pgp/server-8.0.asc | gpg -o
```

```
/usr/share/keyrings/mongodb-server-8.0.gpg --dearmor
```

Ensuite nous ajoutons le dépôt de MongoDB sur le serveur OCS.

```
echo "deb [signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg]
```

```
https://repo.mongodb.org/apt/debian bookworm/mongodb-org/8.0 main" | tee
```

```
/etc/apt/sources.list.d/mongodb-org-8.0.list
```

Après nous mettons à jour la liste des paquets et nous installons les paquets MongoDB.

```
apt update
```

```
apt install -y mongodb-org
```

Une fois tous les paquets installés nous pouvons activer et démarrer tous les services nécessaires.

```
systemctl daemon-reload
```

```
systemctl start mongod  
systemctl enable mongod
```

Nous vérifions que le service fonctionne correctement.

```
systemctl status mongod
```

```
root@serveurocs:~# systemctl daemon-reload  
root@serveurocs:~# systemctl start mongod  
root@serveurocs:~# systemctl status mongod  
● mongod.service - MongoDB Database Server  
   Loaded: loaded (/usr/lib/systemd/system/mongod.service; disabled; preset: enabled)  
   Active: active (running) since Tue 2025-12-02 09:32:54 CET; 39s ago  
 Invocation: be467f575c394372a7cfe1b90c64d7e9  
    Docs: https://docs.mongodb.org/manual  
   Main PID: 3138 (mongod)  
    Memory: 102.5M (peak: 102.8M)  
     CPU: 878ms  
   CGroup: /system.slice/mongod.service  
           └─3138 /usr/bin/mongod --config /etc/mongod.conf  
  
déc. 02 09:32:54 serveurocs systemd[1]: Started mongod.service - MongoDB Database Server.  
déc. 02 09:32:54 serveurocs mongod[3138]: {"t":{"$date":"2025-12-02T08:32:54.628Z"},"s":"I",  
lines 1-13/13 (END)  
^C  
root@serveurocs:~#
```

Pour continuer nous ajoutons sur notre serveur OCS un utilisateur cve puis nous nous connectons avec sur le serveur OCS.

```
adduser cve --home /opt/cve
```

```
su - cve
```

Après nous allons configurer un environnement de développement isolé pour le projet CVE Search, garantissant que toutes les dépendances sont en place et sans conflits avec d'autres projets.

```
virtualenv cve-env
```

```
source ./cve-env/bin/activate
```

```
git clone https://github.com/cve-search/cve-search.git
```

```
cd cve-search
```

```
pip3 install -r requirements.txt
```

```
exit
```

Ensuite nous préparons le fichier de configuration de CVE Search et nous mettons à jour la base de données avec les dernières données sur les vulnérabilités.

```
cp ./cve-search/etc/configuration.ini.sample ./cve-search/etc/configuration.ini
```

```
source /pythonENV/bin/activate
```

```
./cve-search/sbin/db_updater.py -f -c
```