

Ansinelli Yohann, Ralite Justin, Mathéo Balazuc

Installation OpenWEC

Build OpenWEC

Dans un premier, on va venir construire OpenWEC pour cela il faudra installer l'ensemble de paquet suivant :

```
apt install libclang-dev libkrb5-dev libgssapi-krb5-2 msktutil rustc cargo  
libssl-dev
```

Ensuite on va venir créer un user 'openwec' :

```
adduser openwec
```

```
root@WECC:/home/test/openwec# sudo adduser openwec  
Ajout de l'utilisateur « openwec » ...  
Ajout du nouveau groupe « openwec » (1001) ...  
Ajout du nouvel utilisateur « openwec » (1001) avec le groupe « openwec » (1001) ...  
Création du répertoire personnel « /home/openwec » ...  
Copie des fichiers depuis « /etc/skel » ...  
Nouveau mot de passe :  
Retapez le nouveau mot de passe :  
passwd : mot de passe mis à jour avec succès  
Modifier les informations associées à un utilisateur pour openwec  
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut  
  NOM []:  
  Numéro de chambre []:  
  Téléphone professionnel []:  
  Téléphone personnel []:  
  Autre []:  
Cette information est-elle correcte ? [0/n]0  
Ajout du nouvel utilisateur « openwec » aux groupes supplémentaires « users » ...  
Ajout de l'utilisateur « openwec » au groupe « users » ...
```

Une fois l'utilisateur 'openwec' créé, on peut lancer la construction de OpenWEC avec la commande suivante :

```
cargo build --release
```

Attention ! vous pouvez retrouver des erreurs de téléchargements si vous ne mettez pas à jour le paquet rust, pour cela simplement exécuter la commande :

```
rustup update
```

Une fois openwec construit, on se place dans le dossier et on exécute les deux commandes suivantes :

```
cp ./target/release/openwecd /usr/local/bin/  
cp ./target/release/openwec /usr/local/bin/
```

Configuration du système

ATTENTION cette démonstration se fera sur le DC03 !

Maintenant on veut pouvoir lancer OpenWEC avec un utilisateur qui n'a pas de privilège, pour cela on va créer un systemd service avec la commande suivante :

```
systemctl edit openwec.service --full --force
```

La configuration à mettre sera la suivante :

```
GNU nano 7.2 /etc/systemd/system/.#openwec.servicebb7526e06fe302ad  
### openwec.service  
[Unit]  
Description=Windows Events Collector  
After=network.target  
[Service]  
Type=simple  
User=openwec  
Restart=always  
RestartSec=5s  
ExecStart=/usr/local/bin/openwecd -c /etc/openwec.conf.toml  
[Install]  
WantedBy=multi-user.target
```

Comme précisé sur le github de openwec, il ne faut pas oublier de créer le dossier openwec pour que la base de données se crée dans celui-ci :

```
mkdir /var/db/openwec/
```

Notre utilisateur n'a pour l'instant aucun droit, on va venir changer cela en le mettant owner du dossier openwec qu'on vient de créer avec la commande :

```
chown -R openwec:openwec /var/db/openwec
```

On va maintenant venir éditer notre fichier de configuration pour OpenWEC, de base il n'existe pas, par conséquent on va le créer et le mettre dans /etc/ :

```
touch /etc/openwec.conf.toml
```

Désormais peut éditer le fichier et y ajouter la configuration suivante :

```
GNU nano 7.2 /etc/openwec.conf.toml
# /etc/openwec.conf.toml par default
[logging]
[server]
verbosity = "info"
db_sync_interval = 5
flush_heartbeats_interval = 5
keytab = "/etc/krb5.keytab"
[database]
type = "SQLite"
# You need to create /var/db/openwec yourself
path = "/var/db/openwec/db.sqlite"
[[collectors]]
hostname = "openwec.essos.local"
listen_address = "0.0.0.0"
[collectors.authentication]
type = "Kerberos"
service_principal_name = "HTTP/openwec.essos.local@ESSOS.LOCAL"
```

Dans ce fichier on peut voir qu'on indique une entrée DNS à savoir **openwec.essos.local**, on indique également un compte active directory qui est automatiquement créé par le GOAD

HTTP/openwec.essos.local@ESSOS.local, enfin préciser le chemin pour la keytab qui sera générer par notre DC.

Le fichier de configuration prêt, on va venir initialiser la base de donnée avec la commande suivante :

```
openwec -c /etc/openwec.conf.toml db init
```

Création d'une nouvelle subscription

Avec OpenWEC on peut créer des subscriptions qui vont contenir les requêtes d'un fichier xml pour extraire des informations spécifiques des logs du système.

On va créé une nouvelle subscription mais avant cela on va venir récupérer un fichier xml de l'ANSSI qui dispose des meilleurs conseils en termes de sécurités, on exécute la commande suivante pour récupérer le fichier :

```
wget https://raw.githubusercontent.com/ANSSI-FR/guide-journalisation-microsoft/main/Standard_WEC_query.xml
```

Et on crée la subscription avec la commande suivante :

```
openwec -c /etc/openwec/openwec.conf.toml subscriptions new anssi-subscription ./Standard_WEC_query.xml
```

```
root@WECC:/home/test/openwec# openwec -c /etc/openwec/openwec.conf.toml subscriptions new anssi-subscription ./Standard_WEC_query.xml
Subscription anssi-subscription has been created successfully. You need to configure its outputs using `openwec subscriptions edit anssi-subscription outputs add --help`. When you are ready, you can enable it using `openwec subscriptions edit anssi-subscription --enable`
```

On nous indique que la subscription n'est pas 'enable', il va donc falloir l'activer mais avant cela on va venir la modifier pour lui ajouter un chemin pour les logs avec la commande suivante :

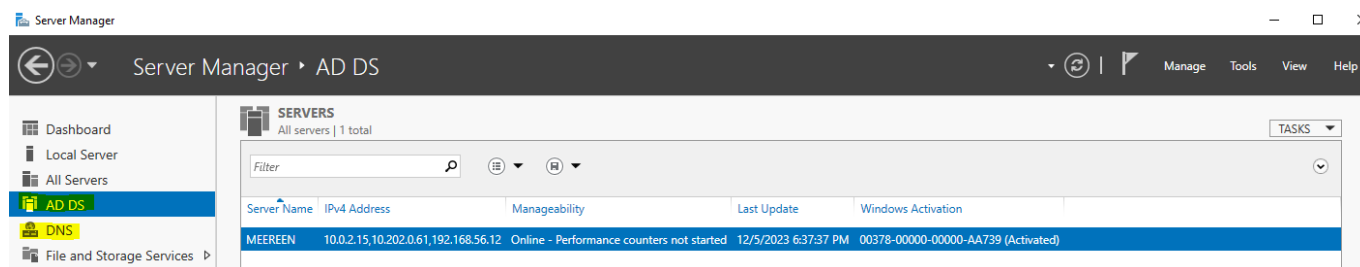
```
openwec subscriptions edit anssi-subscription outputs add --format json files /openwec/logssho
```

On peut désormais activer la subscription avec la commande :

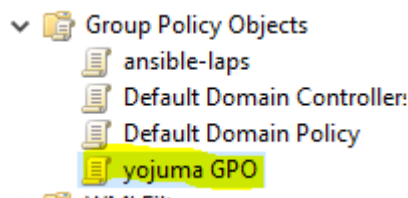
```
openwec subscriptions enable anssi-subscription
```

Configuration DC Windows

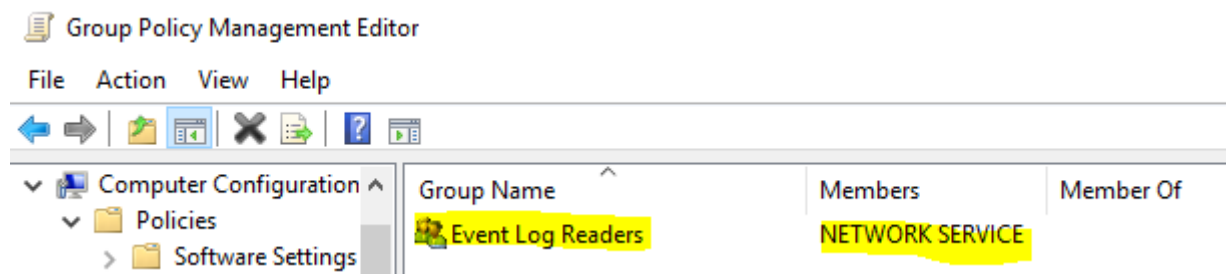
Dans un premier temps je vais regarder sur le DC qu'il y est bien un AD de créé par défaut par le GOAD, pour cela je me rend dans **Server Manager** :



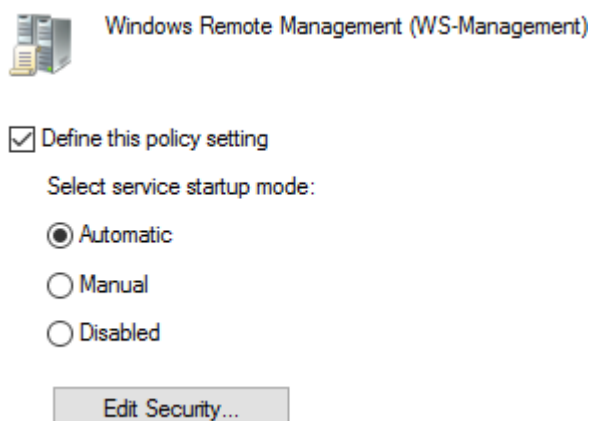
On constate qu'il y a déjà un AD de créé avec le DNS. On va maintenant venir créer une GPO, pour cela on va ouvrir l'outil **Group Policy Management Tools** et on va venir ajouter dans "Group Policy Objects" une nouvelle GPO qu'on va nommer "yojuma" en référence à notre groupe.



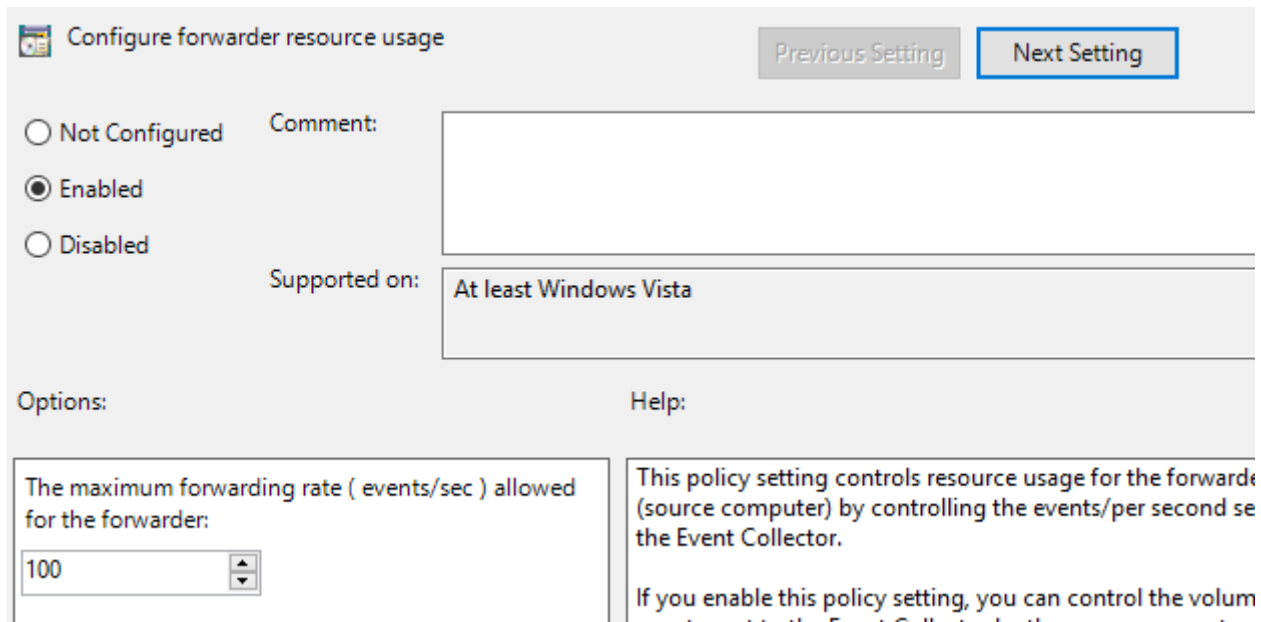
On va maintenant venir éditer notre GPO. Dans un premier temps on va venir donner le droit de lecture aux logs en se rendant dans "Network Service" pour venir ajouter ceci :



Une fois cela fait, on va mettre en démarrage automatique WinRM, pour ce faire on va suivre le chemin suivant : Computer Configuration > Policies > Windows Settings > Security Settings > System Services > Windows Remote Management > Startup Mode > Automatic.



On va pouvoir maintenant configurer les ressources aux chemins suivant : Computer Configuration > Policies > Administrative Templates > Windows Components > Event Forwarding > Configure Forwarder Ressource Usage On met sur "Enabled" et on précise la valeur de forwarding rate à 100.



Configure forwarder resource usage

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Vista

Options:

The maximum forwarding rate (events/sec) allowed for the forwarder:

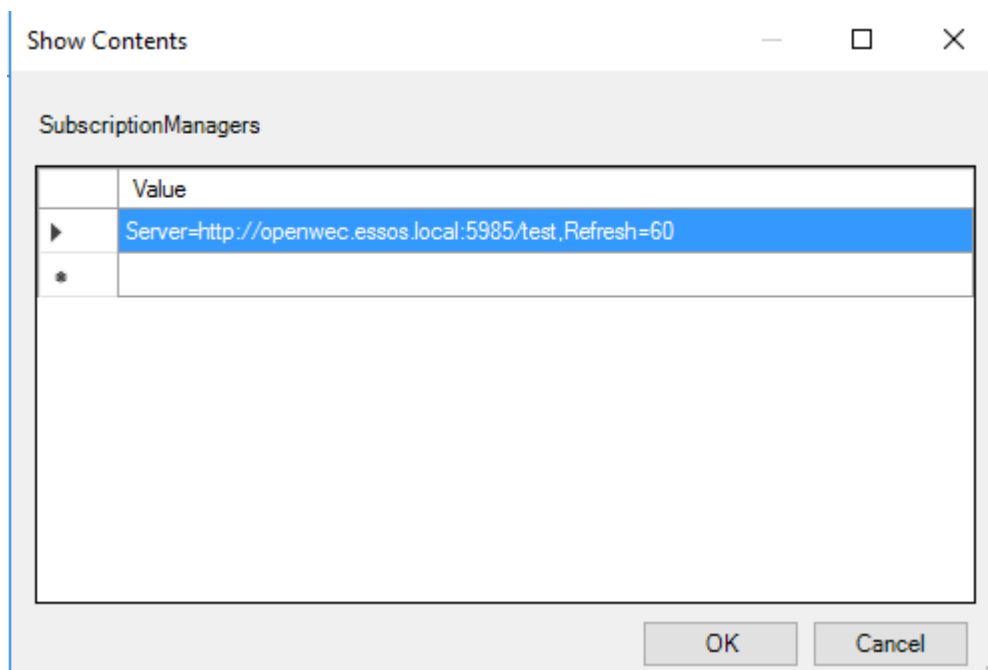
100

Help:

This policy setting controls resource usage for the forwarder (source computer) by controlling the events/per second sent to the Event Collector.

If you enable this policy setting, you can control the volume of events sent to the Event Collector by the source computer.

On clique ensuite sur Next Setting et on va également mettre sur "Enabled" puis cliquer sur show pour rentrer le server suivant :



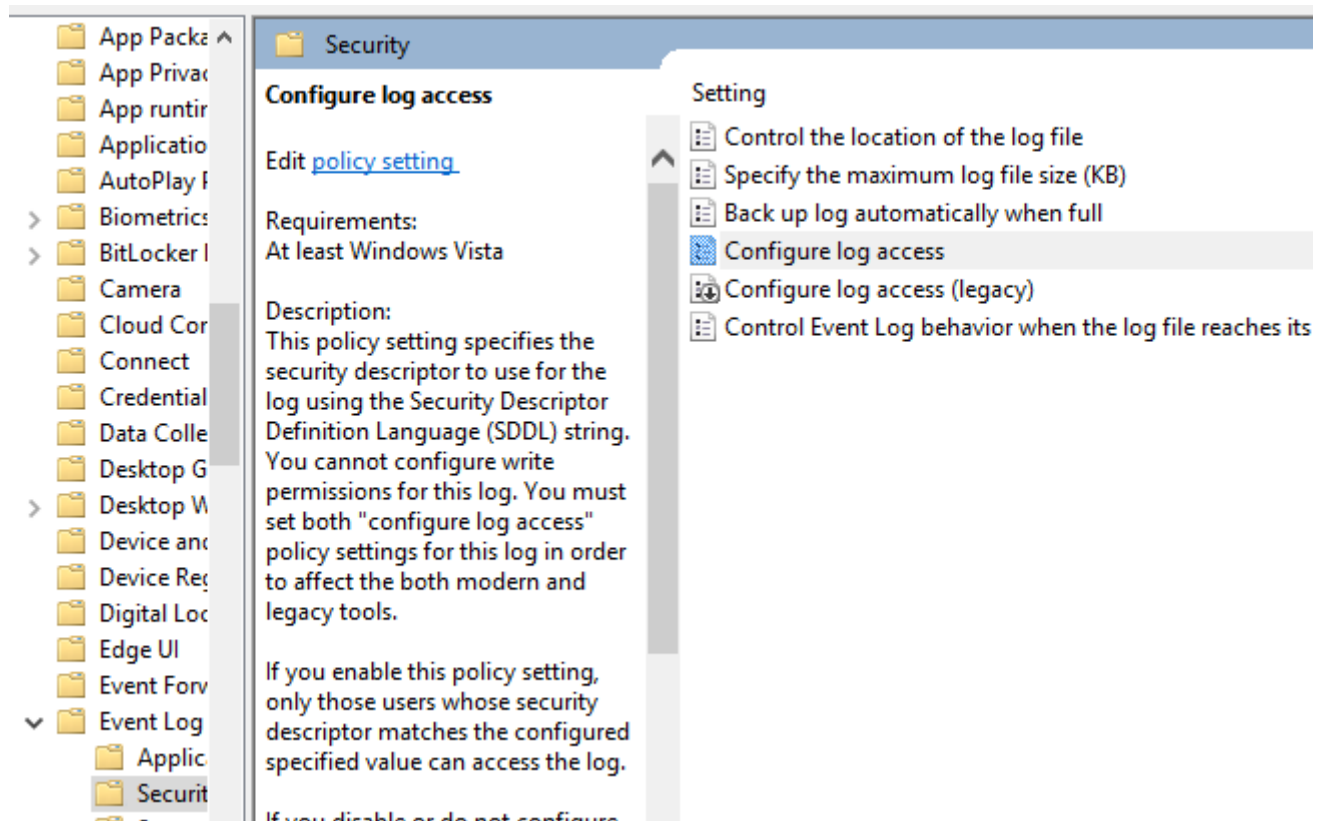
Show Contents

SubscriptionManagers

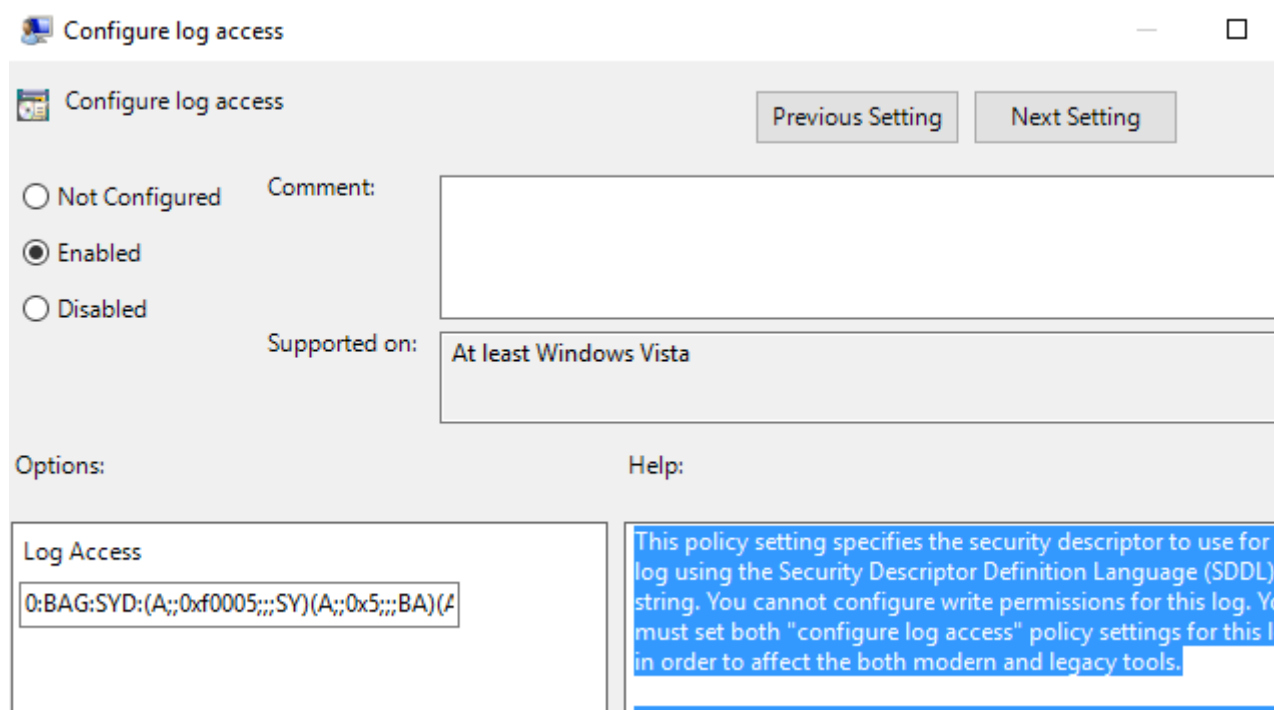
	Value
▶	Server=http://openwec.essos.local:5985/test,Refresh=60
*	

OK Cancel

On donne maintenant les droits sur chaque channel de log à l'utilisateur "EventLogReader" et à "NetworkService" pour pouvoir lire les logs : Computer Configuration > Politiques > Administrative Templates > Windows Components > Event Log Service > Security > Configure log access.



On va venir mettre dans le champ "Log Access" le SDDL fournit sur le github de OpenWEC à savoir : `O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)`. **ATTENTION** sur le github de OpenWEC il est également précisé de refaire la manipulation pour "Configure log access (legacy)".



On peut vérifier sur l'onglet "Settings" que notre GPO est bien configuré avec les bonnes informations.

yojuma GPO

Scope Details Settings Delegation Status

yojuma GPO
Data collected on: 12/5/2023 6:46:08 PM [show all](#)

Computer Configuration (Enabled) [hide](#)

Policies [hide](#)

Windows Settings [hide](#)

Security Settings [hide](#)

Restricted Groups [show](#)

System Services [show](#)

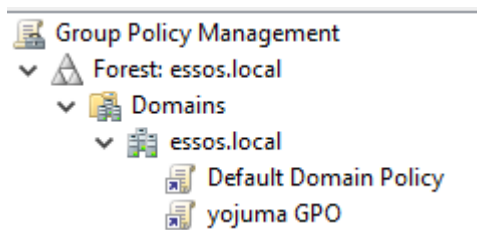
Administrative Templates [hide](#)

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Event Forwarding [hide](#)

Policy	Setting	Comment
Configure forwarder resource usage	Enabled	
The maximum forwarding rate (events/sec) allowed for the forwarder:		100
Configure target Subscription Manager	Enabled	
SubscriptionManagers		
Server=http://openwec.essos.local:5985/test,Refresh=60		

Une fois la vérification effectuée, on va lier notre GPO au domaine :



On fait maintenant la propagation forcée de la GPO sur les serveurs forwarders avec la commande "gpupdate /Force" :

```
C:\Users\vagrant>gpupdate /Force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

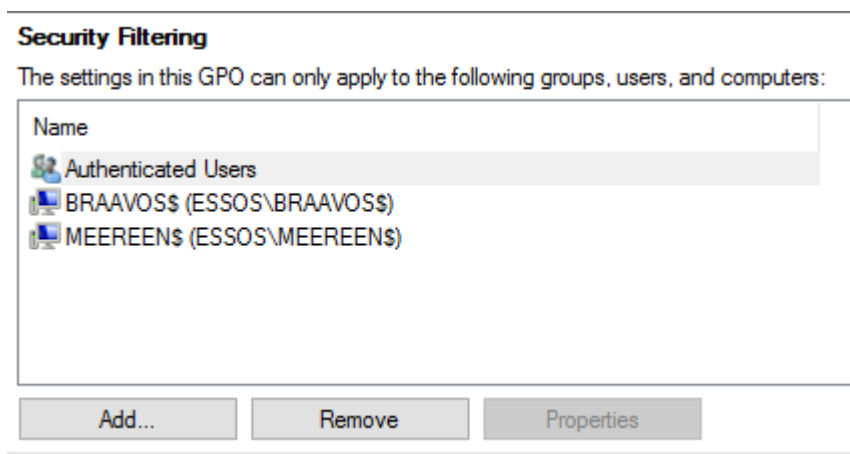
Et on vient regarder la propagation avec la commande "gpresult /R" :


```
RSOP data for ESSOS\vagrant on MEEREEN : Logging Mode
-----
OS Configuration:          Primary Domain Controller
OS Version:                10.0.14393
Site Name:                 N/A
Roaming Profile:           N/A
Local Profile:             C:\Users\vagrant
Connected over a slow link?: No

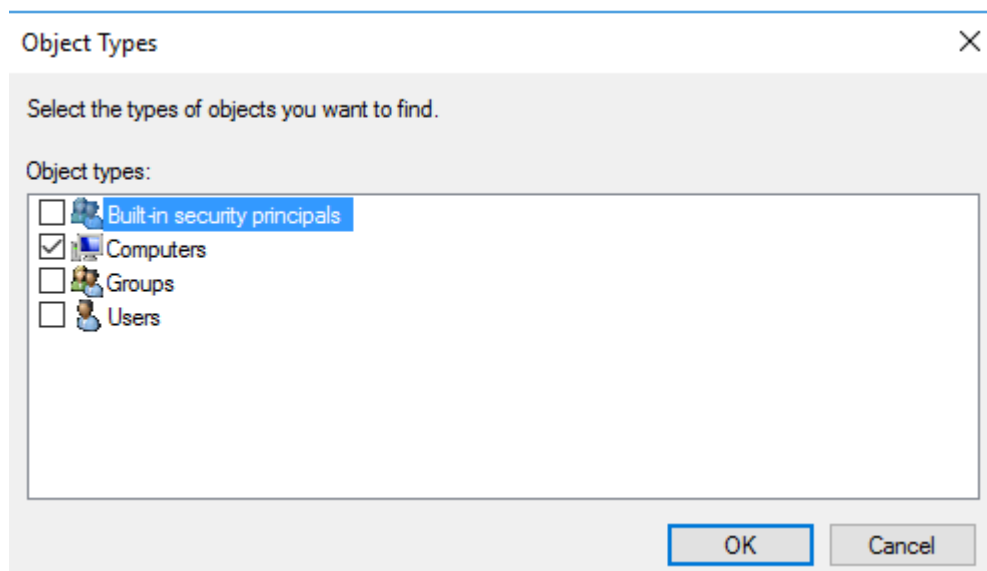
USER SETTINGS
-----
CN=vagrant,CN=Users,DC=essos,DC=local
Last time Group Policy was applied: 12/5/2023 at 11:21:54 AM
Group Policy was applied from:      meereen.essos.local
Group Policy slow link threshold:   500 kbps
Domain Name:                      ESSOS
Domain Type:                      Windows 2008 or later

Applied Group Policy Objects
-----
```

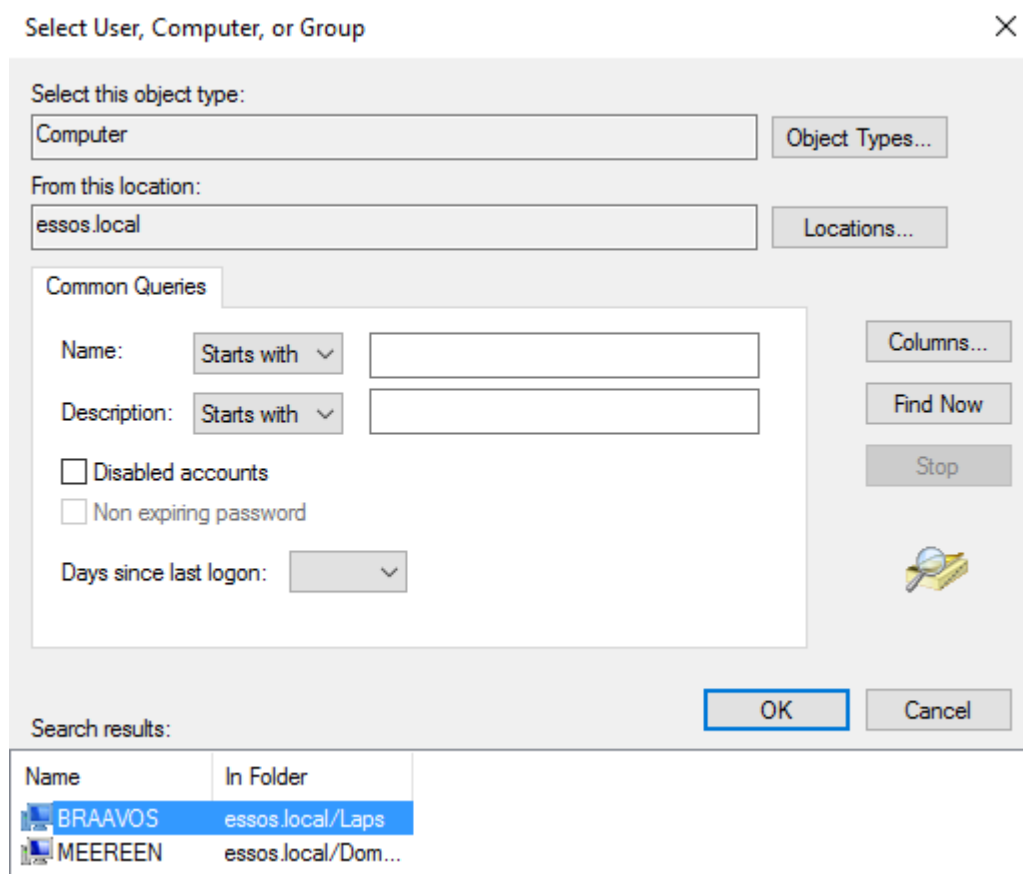
Maintenant il ne faut pas oublier d'ajouter l'ensemble des machines du DC à la GPO, pour cela on se rend à nouveau sur l'outil **Group Policy Management Tools**, on va cliquer sur notre GPO et on pourra voir en bas à droite la possibilité d'ajouter des machines :



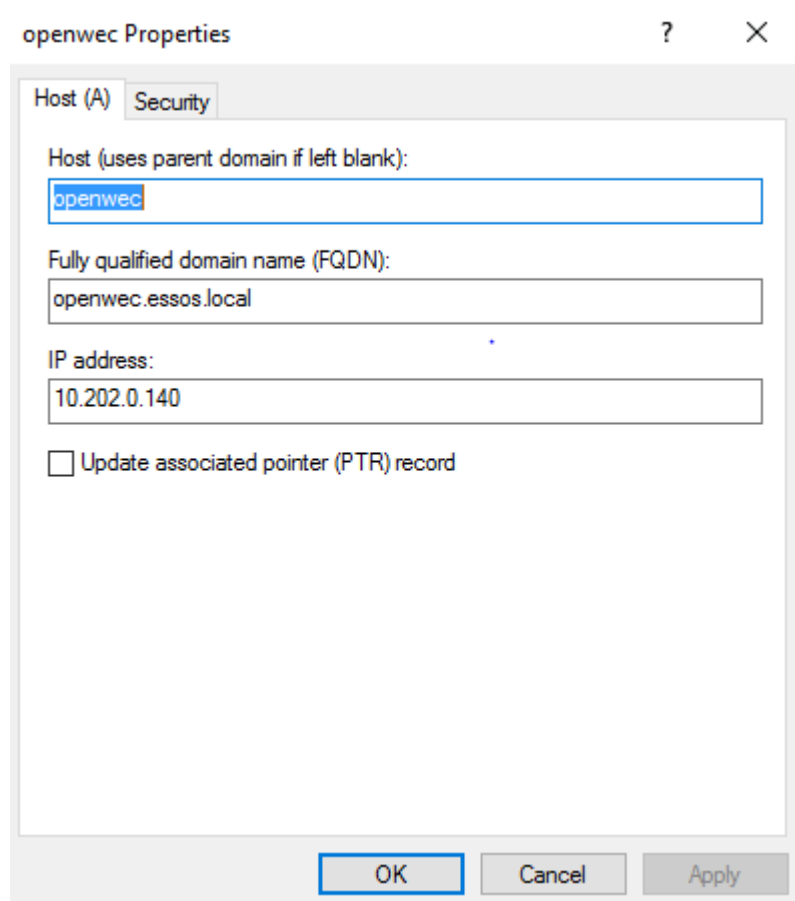
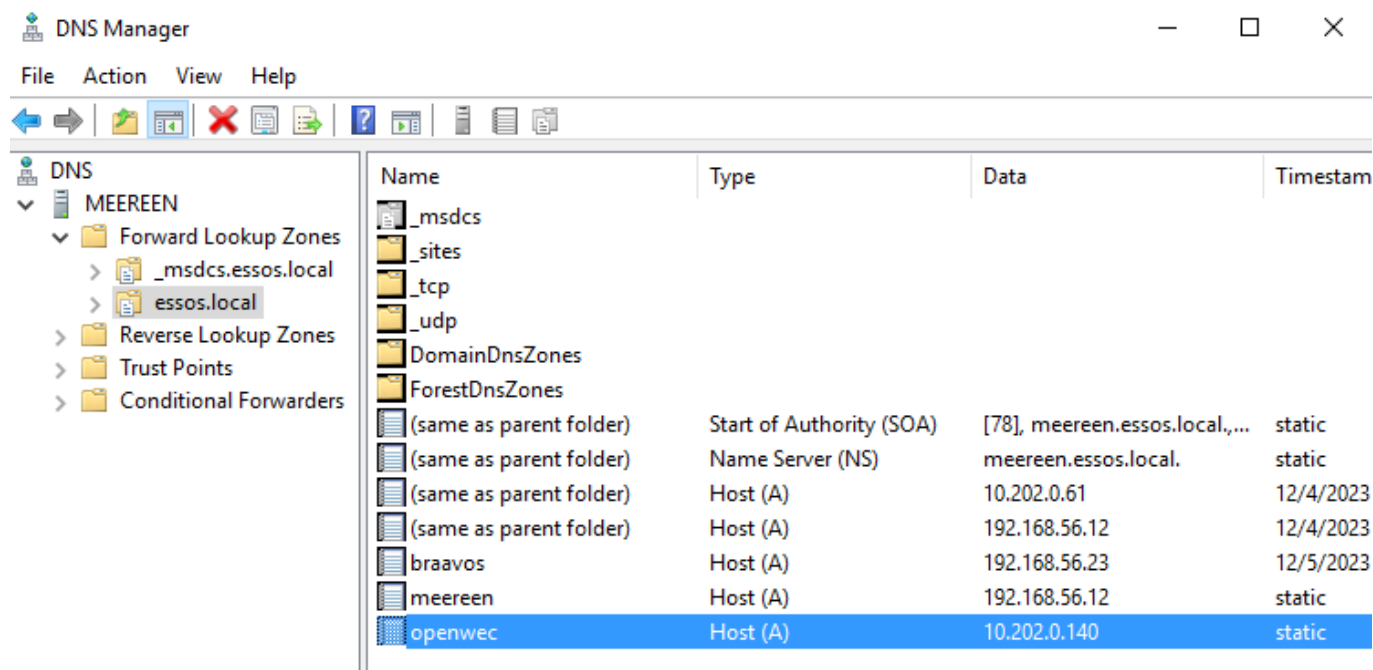
On va venir cliquer sur "Add" puis sur "Object Types" et on va seulement cocher "Computers" :



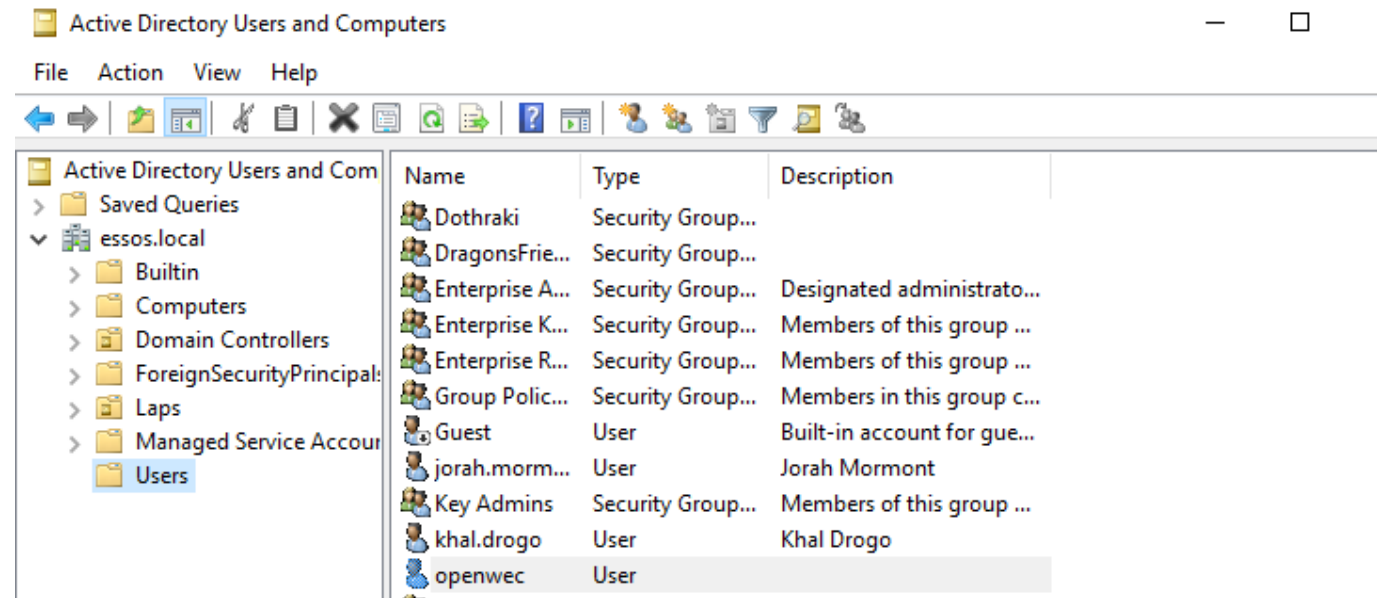
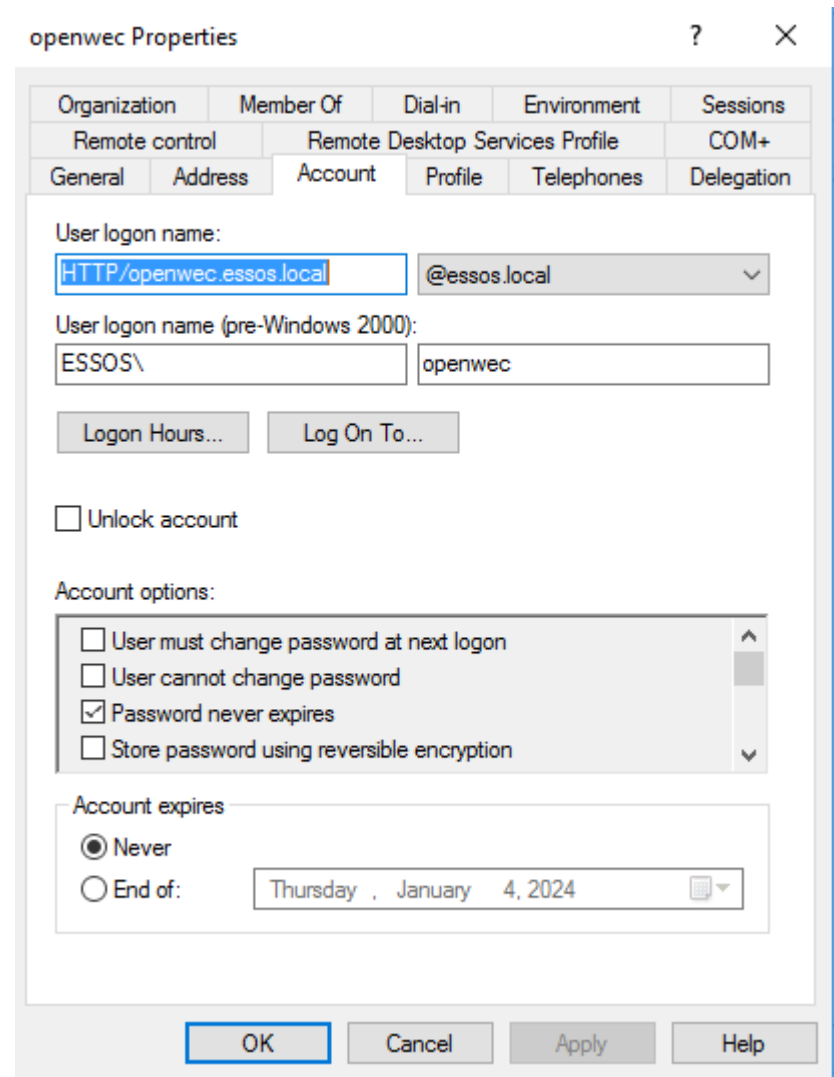
On vérifie bien que la "location" corresponde bien au domaine et on va cliquer sur "Find Now" pour obtenir la liste des machines et ensuite les ajouter. **ATTENTION** on ne peut ajouter qu'une machine à la fois, il faut donc répéter le processus pour chaque machine qu'on souhaite ajouter.



Une fois les machines ajoutées à la GPO on va ajouter l'adresse IP du serveur OpenWEC au dns de windows sur l'outil **DNS MANAGER** en suivant le chemin MEEREEN > Forward Lookup Zones > essos.local :



Il ne faudra pas oublier de créer l'utilisateur openwec sur le DC en utilisant la console de l'AD :



Enfin on va venir relier le SPN à l'utilisateur OpenWEC avec la succession de commande suivante :
(**ATTENTION** Il faut être en administrateur pour exécuter ces commandes, de même pour générer la keytab)

```

C:\Windows\system32>setspn -d HTTP/openwec.essos.local openwec
Unregistering ServicePrincipalNames for CN=openwec,CN=Users,DC=essos,DC=local
HTTP/openwec.essos.local
Updated object

C:\Windows\system32>setspn -S HTTP/openwec.essos.local openwec
Checking domain DC=essos,DC=local

Registering ServicePrincipalNames for CN=openwec,CN=Users,DC=essos,DC=local
HTTP/openwec.essos.local
Updated object

C:\Windows\system32>setspn -L openwec
Registered ServicePrincipalNames for CN=openwec,CN=Users,DC=essos,DC=local:
HTTP/openwec.essos.local

```

La première commande avec l'option "-d" vient supprimer le lien si il existe déjà
p/home/test/Téléchargements/23.png pour être sûre de ne faire un lien clair, l'option "-S" va venir créer le lien si
il n'existe pas déjà et l'option "-L" va venir vérifier si le lien est bien enregistré. On va maintenant pouvoir
générer la keytab avec la commande suivante :

```

C:\Windows\system32>ktutil -princ HTTP/openwec.essos.local@ESSOS.LOCAL -mapuser openwec -crypto ALL -mapop set -ptype KRB5_NT_PRINCIPAL -pass yojuma34500 -kvno 0 -out c:\Users\vagrant\Desktop\openwec.keytab
Targeting domain controller: meereen.essos.local
Successfully mapped HTTP/openwec.essos.local to openwec.
Password successfully set!
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to c:\Users\vagrant\Desktop\openwec.keytab:
Keytab version: 0x502
keysize 63 HTTP/openwec.essos.local@ESSOS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x1 (DES-CBC-CRC) keylength 8 (0xfd9b29ec10f2cb15)
keysize 63 HTTP/openwec.essos.local@ESSOS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x3 (DES-CBC-MD5) keylength 8 (0xfd9b29ec10f2cb15)
keysize 71 HTTP/openwec.essos.local@ESSOS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x17 (RC4-HMAC) keylength 16 (0x2f250326392c9b10efa953a916c227a8)
keysize 87 HTTP/openwec.essos.local@ESSOS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x12 (AES256-SHA1) keylength 32 (0x5b961c5eddf47d0f98624e66dad95cf8a538cf6d9a9693873f10c7d00fa35a)
keysize 71 HTTP/openwec.essos.local@ESSOS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x11 (AES128-SHA1) keylength 16 (0x4129221640bd40b5c81ad93a81ab7c29)

```

La commande ktpass permet de générer clés de service Kerberos, l'option "-princ" va venir définir le nom principal Kerberos pour lequel la clé doit être créée, l'option "mapuser" sert à indiquer l'utilisateur, l'option "-crypto" spécifie les types de chiffrement à utiliser pour la clé, l'option "-mapop" spécifie les options de mappage, l'option "-ptype" permet de spécifier le type de principal (par défaut KRB5_NT_PRINCIPAL), l'option "-pass" sert à donner le mot de passe de l'utilisateur qu'on a défini, l'option "-kvno" va permettre d'indiquer le numéro de version de la clé et enfin l'option "-out" va servir à donner le chemin de sorti de la keytab.

On oublie pas d'ajouter le DNS dans le fichier "/etc/hosts" :

GNU nano 7.2	/etc/hosts
127.0.0.1	localhost
127.0.1.1	WECC.myguest.virtualbox.org WECC
10.202.0.140	openwec.essos.local

On peut maintenant exécuter la dernière commande pour voir si les logs remontent :

```
/usr/local/bin/openwecd -c /etc/openwec.conf.toml
```

```
openwec stats
```

14 / 14