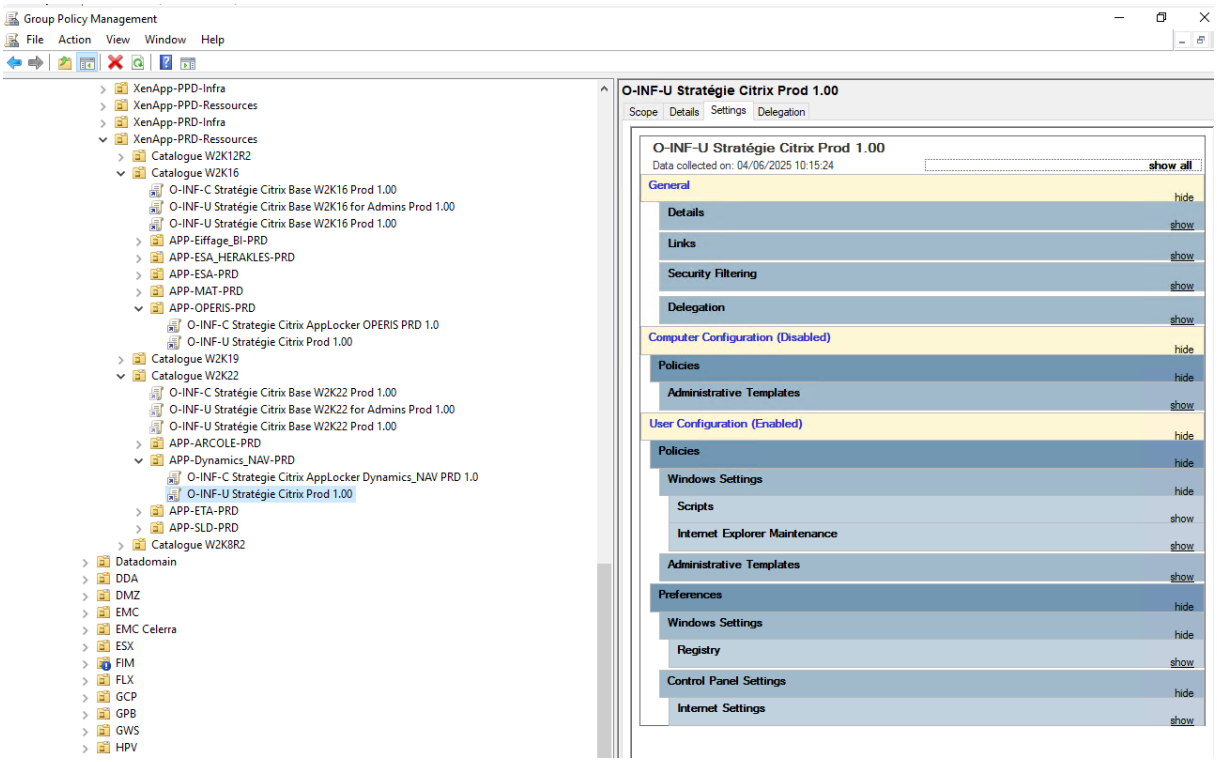
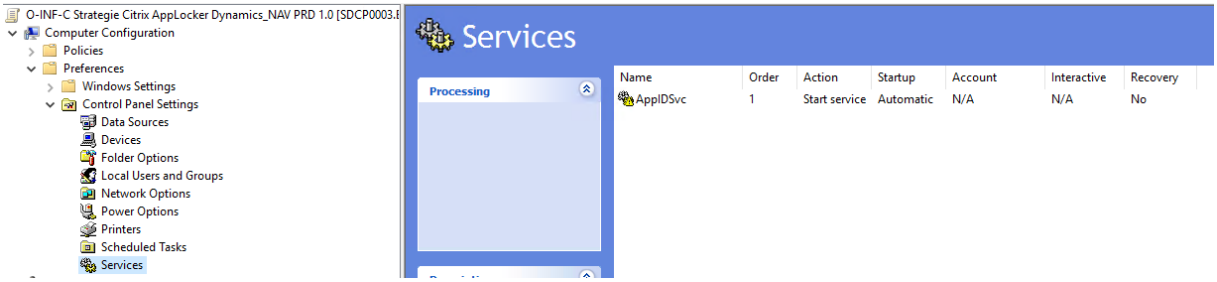
# 10. Annexes

## 10.1 Sécurisation des serveurs Citrix

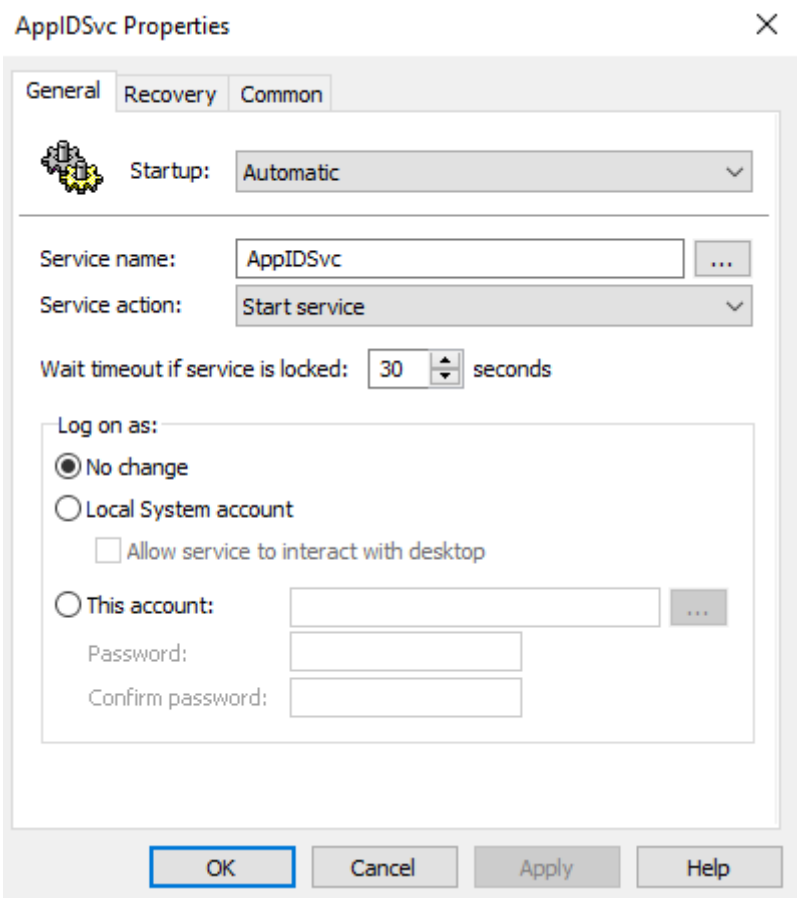
Voici la GPO en question




On n'oublie pas d'activer le service AppIDSvc pour que la GPO s'applique bien, en allant dans ce chemin-là.

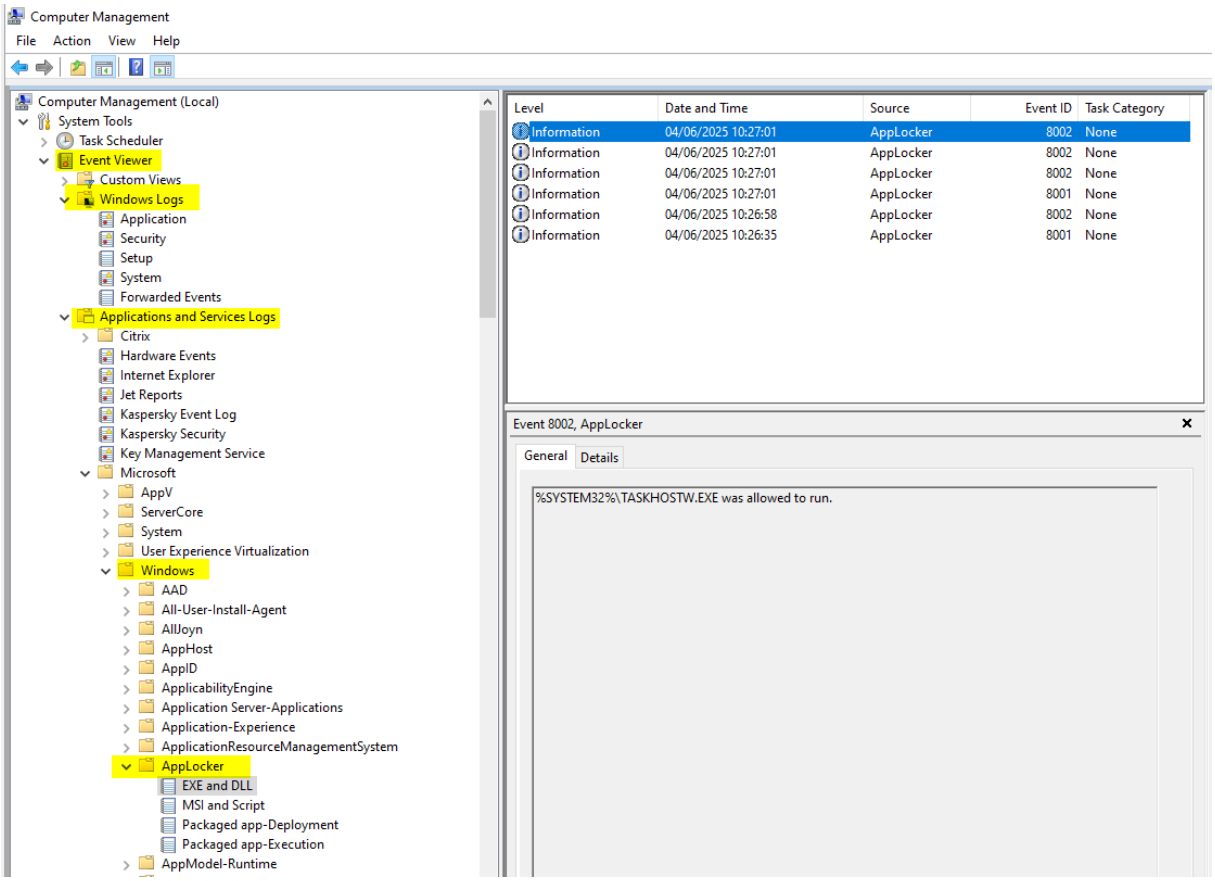


On l'active comme ceci :

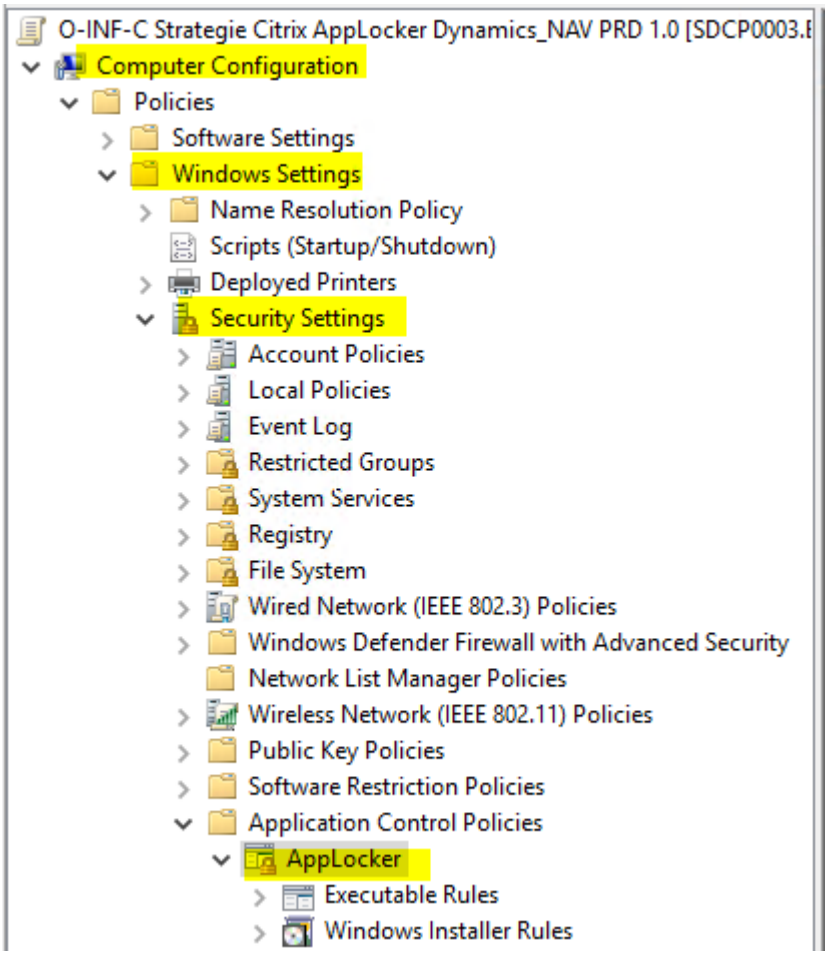


Chemin pour regarder les logs de l'application qui permet de savoir quelle exécutables l'application a besoin d'utiliser et manque plus qu'a filtré ce qu'on autorise ou non.

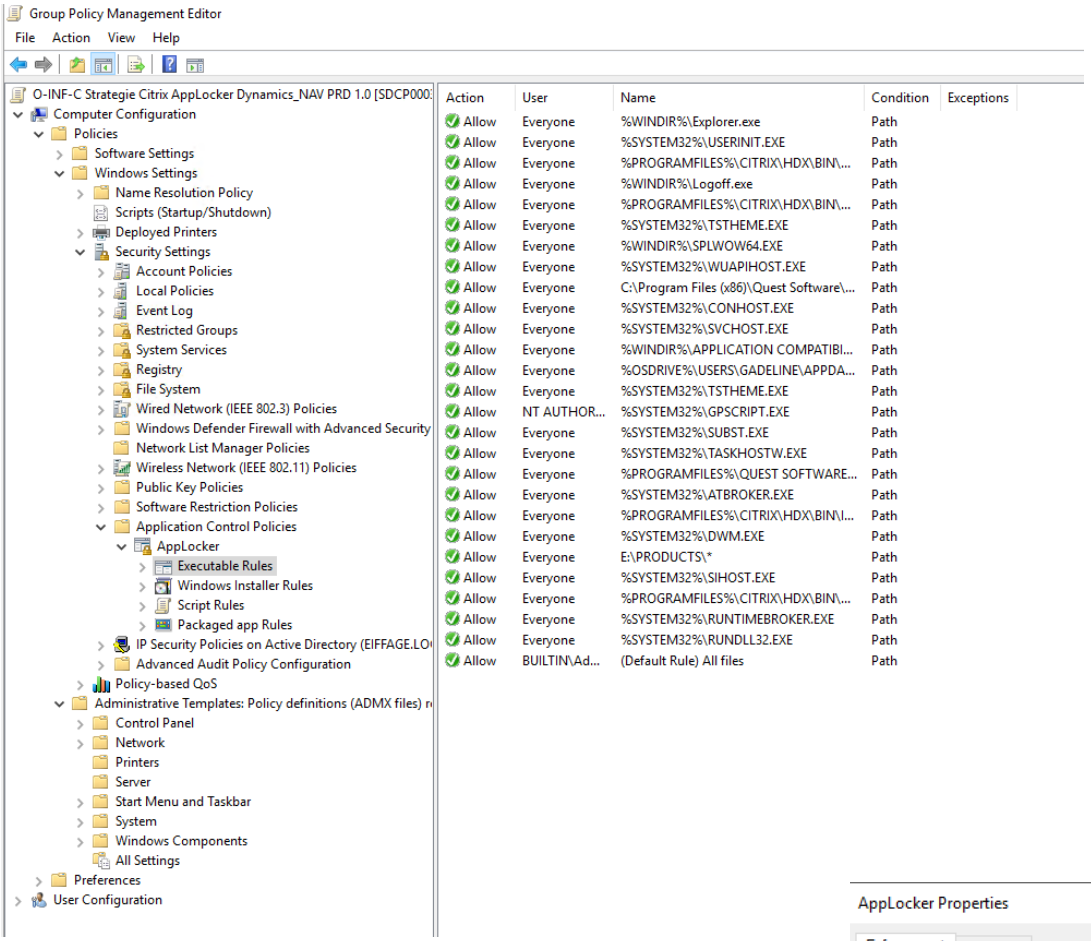
Cette action est à réaliser en mode audit et après avoir activer AppLocker



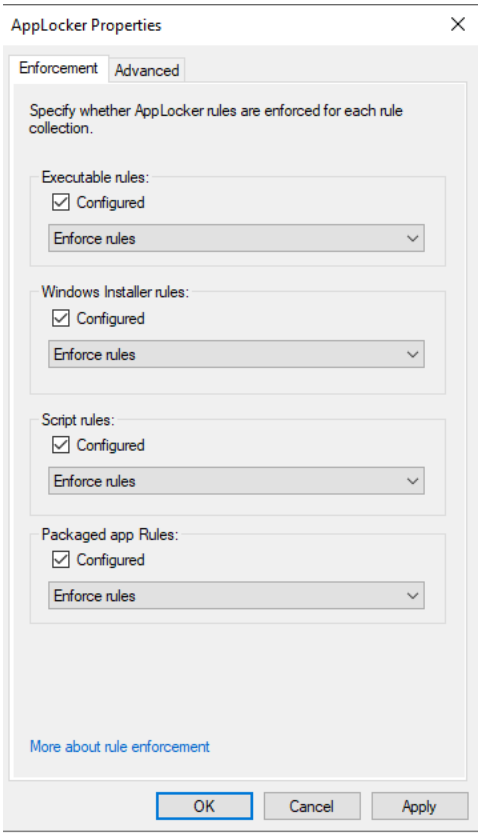
On accède ensuite au chemin pour accéder à AppLocker et pouvoir gérer les « Executable Rules » après avoir analyser tout ce dont avait besoin l'application.



Et voici les exécutables qu'on a autorisé




On applique et enregistre tout et on se remet en mode Enforce Rules.



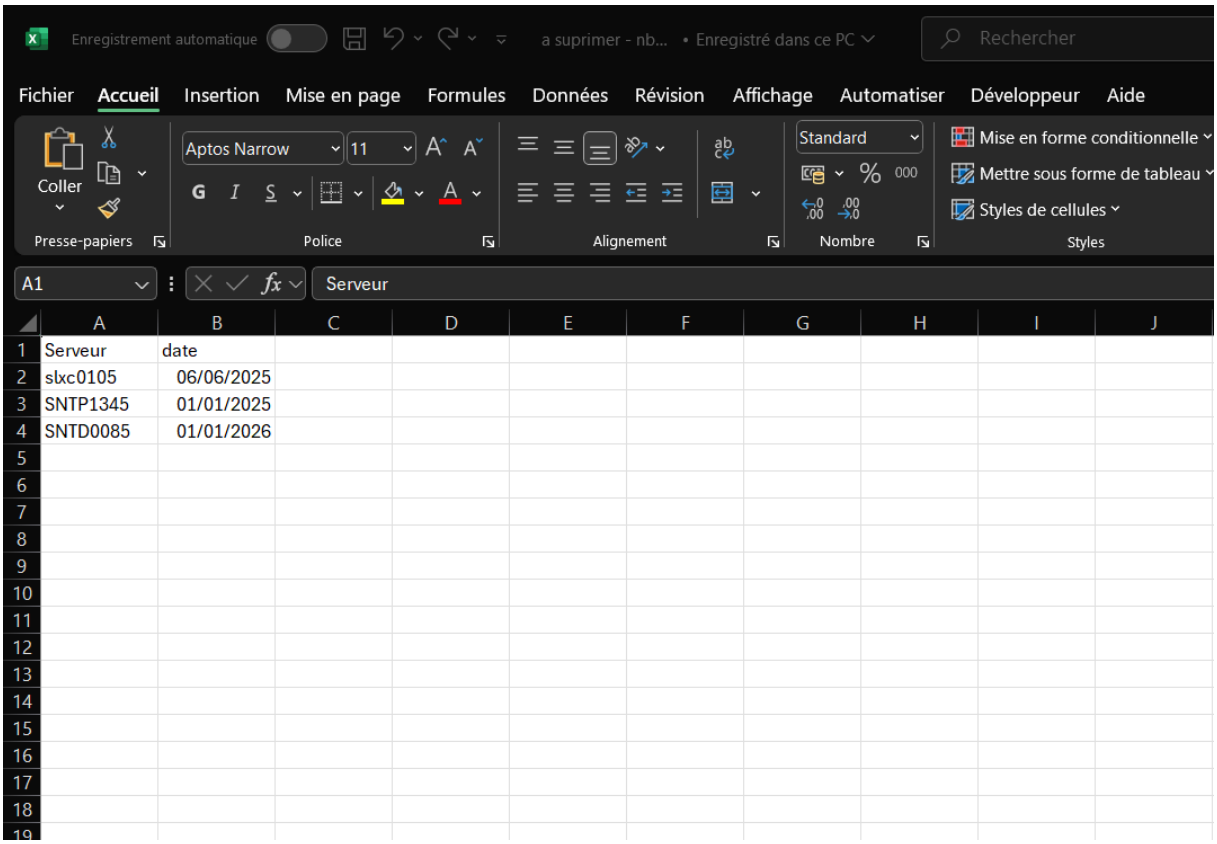
## 10.2 Exercice PowerShell

Voici le code PowerShell crée qui en l'exécutant me supprime les donner demander dans le fichier que je souhaite traiter :

```
# Définir les chemins
$toDeletePath = "C:\Users\Ayoub El Maghrebi\Desktop\a suprimer - nbu.csv"
$exportPath = "C:\Users\Ayoub El Maghrebi\Desktop\export 2.csv"

# Spécifier les noms de colonnes du fichier à filtrer
$exportServerColumn = "NBU_server"
$exportDateColumn = "last_backup"

# Lire les fichiers CSV
$toDelete = Import-Csv -Path $toDeletePath -Delimiter ";"
$exportData = Import-Csv -Path $exportPath -Delimiter ";"

# Obtenir la date d'aujourd'hui
$today = Get-Date

# Filtrer les données à conserver     where-object garde que les lignes valides
$filteredData = $exportData | Where-Object {
   $row = $_
   -not ($toDelete | Where-Object {
      $serverMatch = $_.Serveur -eq $row.$exportServerColumn  #permet de verifier le nom du serv
```

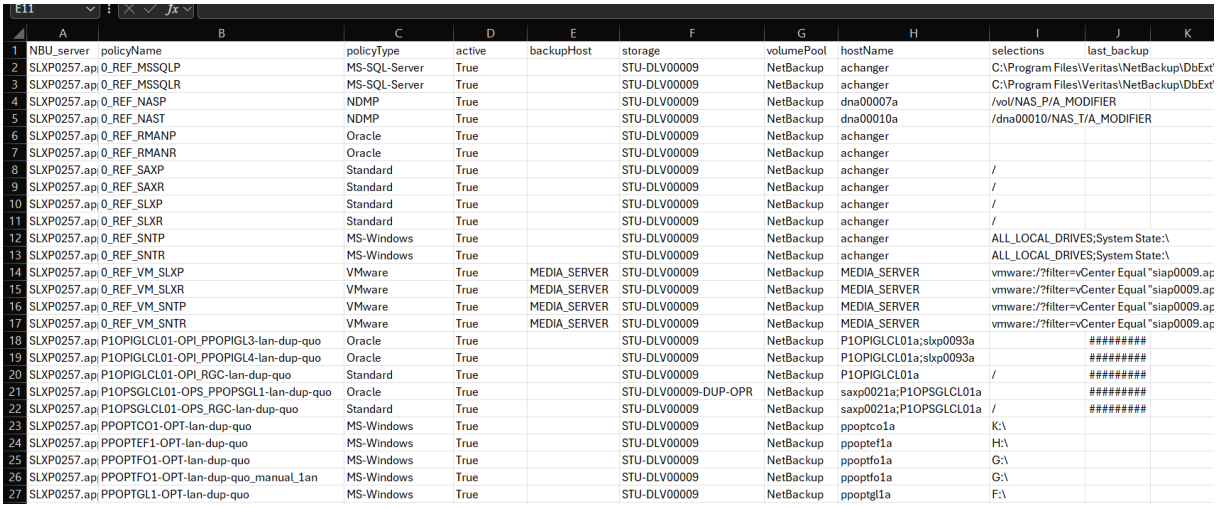
```
    try {
      $toDeleteDate = [datetime]::ParseExact($_.date, 'dd/MM/yyyy', $null)
      $exportDate = [datetime]::ParseExact($row.$exportDateColumn, 'dd/MM/yyyy', $null)
    } catch {
      return $false
    }

    $dateMatch = $toDeleteDate -le $today -and $toDeleteDate -eq $exportDate   # permet de verifier si la date du fichier à suppr est aujourd'hui ou dans le passé et si elle correspond à celle de la ligne
    return $serverMatch -and $dateMatch
  })
}

# Remplacer le fichier d'origine avec les données filtrées
$filteredData | Export-Csv -Path $exportPath -NoTypeInformation -Encoding UTF8 -Delimiter ";"

Write-Output "✅ Export terminé. Le fichier original a été mis à jour : $exportPath"
```

Voici le fichier csv ou sont indiquer les donner à supprimer :



| | A | B | C | D | E | F | G | H | I | J |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Serveur | date | | | | | | | | |
| 2 | slxc0105 | 06/06/2025 | | | | | | | | |
| 3 | SNTP1345 | 01/01/2025 | | | | | | | | |
| 4 | SNTD0085 | 01/01/2026 | | | | | | | | |
| 5 | | | | | | | | | | |
| 6 | | | | | | | | | | |
| 7 | | | | | | | | | | |
| 8 | | | | | | | | | | |
| 9 | | | | | | | | | | |
| 10 | | | | | | | | | | |
| 11 | | | | | | | | | | |
| 12 | | | | | | | | | | |
| 13 | | | | | | | | | | |
| 14 | | | | | | | | | | |
| 15 | | | | | | | | | | |
| 16 | | | | | | | | | | |
| 17 | | | | | | | | | | |
| 18 | | | | | | | | | | |

Et pour finir le fichier csv ou je dois retirer les données :



| | A | B | C | D | E | F | G | H | I | J | K |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | NBU_server | policyName | policyType | active | backupHost | storage | volumePool | hostName | selections | last_backup | |
| 2 | SLXP0257.ap | 0_REF_MSSQLP | MS-SQL-Server | True | | STU-DLV00009 | NetBackup | achanger | C:\Program Files\Veritas\NetBackup\DbExt' | | |
| 3 | SLXP0257.ap | 0_REF_MSSQLR | MS-SQL-Server | True | | STU-DLV00009 | NetBackup | achanger | C:\Program Files\Veritas\NetBackup\DbExt' | | |
| 4 | SLXP0257.ap | 0_REF_NASP | NDMP | True | | STU-DLV00009 | NetBackup | dna00007a | /vol/NAS_P/A_MODIFIER | | |
| 5 | SLXP0257.ap | 0_REF_NAST | NDMP | True | | STU-DLV00009 | NetBackup | dna00010a | /dna00010/NAS_T/A_MODIFIER | | |
| 6 | SLXP0257.ap | 0_REF_RMANP | Oracle | True | | STU-DLV00009 | NetBackup | achanger | | | |
| 7 | SLXP0257.ap | 0_REF_RMANR | Oracle | True | | STU-DLV00009 | NetBackup | achanger | | | |
| 8 | SLXP0257.ap | 0_REF_SAXP | Standard | True | | STU-DLV00009 | NetBackup | achanger | / | | |
| 9 | SLXP0257.ap | 0_REF_SAXR | Standard | True | | STU-DLV00009 | NetBackup | achanger | / | | |
| 10 | SLXP0257.ap | 0_REF_SLXP | Standard | True | | STU-DLV00009 | NetBackup | achanger | / | | |
| 11 | SLXP0257.ap | 0_REF_SLXR | Standard | True | | STU-DLV00009 | NetBackup | achanger | / | | |
| 12 | SLXP0257.ap | 0_REF_SNTP | MS-Windows | True | | STU-DLV00009 | NetBackup | achanger | ALL_LOCAL_DRIVES;System State:\ | | |
| 13 | SLXP0257.ap | 0_REF_SNTR | MS-Windows | True | | STU-DLV00009 | NetBackup | achanger | ALL_LOCAL_DRIVES;System State:\ | | |
| 14 | SLXP0257.ap | 0_REF_VM_SLXP | VMware | True | MEDIA_SERVER | STU-DLV00009 | NetBackup | MEDIA_SERVER | vmware:/?filter=vCenter Equal "siap0009.ap | | |
| 15 | SLXP0257.ap | 0_REF_VM_SLXR | VMware | True | MEDIA_SERVER | STU-DLV00009 | NetBackup | MEDIA_SERVER | vmware:/?filter=vCenter Equal "siap0009.ap | | |
| 16 | SLXP0257.ap | 0_REF_VM_SNTP | VMware | True | MEDIA_SERVER | STU-DLV00009 | NetBackup | MEDIA_SERVER | vmware:/?filter=vCenter Equal "siap0009.ap | | |
| 17 | SLXP0257.ap | 0_REF_VM_SNTR | VMware | True | MEDIA_SERVER | STU-DLV00009 | NetBackup | MEDIA_SERVER | vmware:/?filter=vCenter Equal "siap0009.ap | | |
| 18 | SLXP0257.ap | P1OPIGLCL01-OPI_PPOPIGL3-lan-dup-quo | Oracle | True | | STU-DLV00009 | NetBackup | P1OPIGLCL01a;slxp0093a | | ######### | |
| 19 | SLXP0257.ap | P1OPIGLCL01-OPI_PPOPIGL4-lan-dup-quo | Oracle | True | | STU-DLV00009 | NetBackup | P1OPIGLCL01a;slxp0093a | | ######### | |
| 20 | SLXP0257.ap | P1OPIGLCL01-OPI_RGC-lan-dup-quo | Standard | True | | STU-DLV00009 | NetBackup | P1OPIGLCL01a | / | ######### | |
| 21 | SLXP0257.ap | P1OPSGLCL01-OPS_PPOPSGL1-lan-dup-quo | Oracle | True | | STU-DLV00009-DUP-OPR | NetBackup | saxp0021a;P1OPSGLCL01a | | ######### | |
| 22 | SLXP0257.ap | P1OPSGLCL01-OPS_RGC-lan-dup-quo | Standard | True | | STU-DLV00009 | NetBackup | saxp0021a;P1OPSGLCL01a | / | ######### | |
| 23 | SLXP0257.ap | PPOPTCO1-OPT-lan-dup-quo | MS-Windows | True | | STU-DLV00009 | NetBackup | ppoptco1a | K:\ | | |
| 24 | SLXP0257.ap | PPOPTEF1-OPT-lan-dup-quo | MS-Windows | True | | STU-DLV00009 | NetBackup | ppoptef1a | H:\ | | |
| 25 | SLXP0257.ap | PPOPTFO1-OPT-lan-dup-quo | MS-Windows | True | | STU-DLV00009 | NetBackup | ppoptfo1a | G:\ | | |
| 26 | SLXP0257.ap | PPOPTFO1-OPT-lan-dup-quo_manual_1an | MS-Windows | True | | STU-DLV00009 | NetBackup | ppoptfo1a | G:\ | | |
| 27 | SLXP0257.ap | PPOPTGL1-OPT-lan-dup-quo | MS-Windows | True | | STU-DLV00009 | NetBackup | ppoptgl1a | F:\ | | |

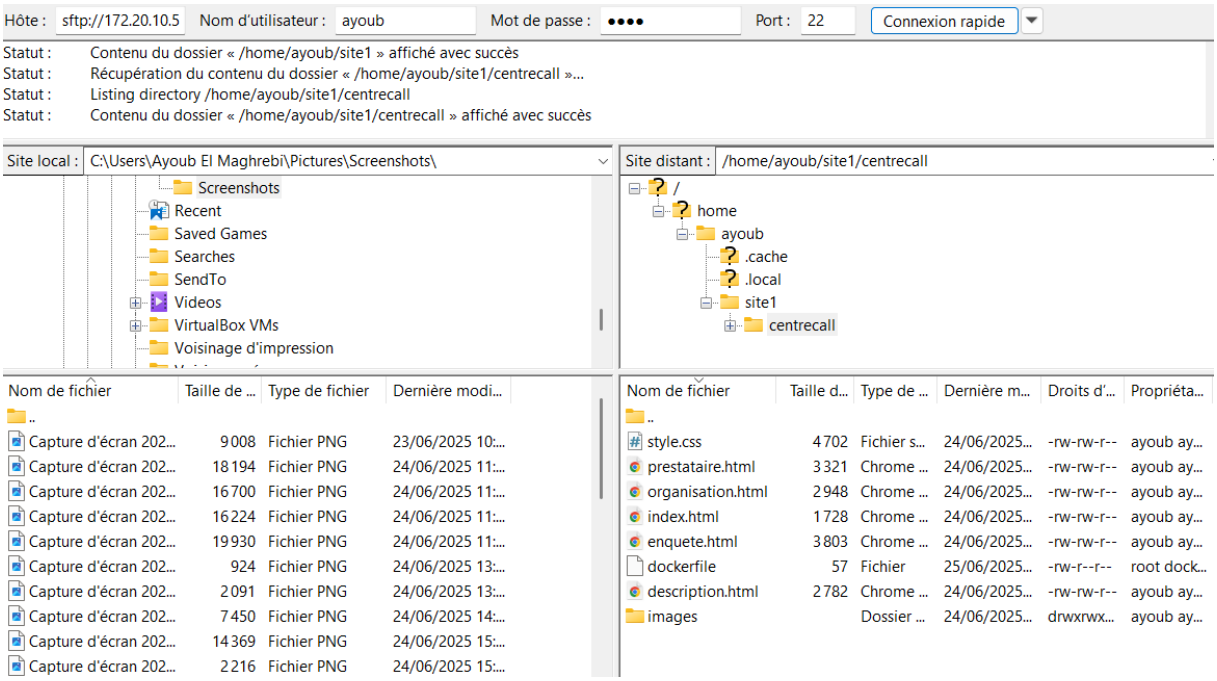
## 10.3 Exercice : hébergement site sur serveur Ubuntu 24.04 avec docker.

Dans un premier temps j'ai configuré le serveur pour activer ssh en utilisant le port 22:

```
sudo apt update
sudo apt install openssh-server -y
sudo systemctl enable --now ssh
sudo ufw allow 22/tcp  # Autorise le port 22 dans le firewall
```

Ensuite, j'ai utilisé FileZilla pour pouvoir déposer mon site sur ma vm en me connectant avec l'adresse IP du serveur et mon utilisateur ayoub qui est admin et qui a tous les droits dans le chemin que j'ai créé : /home/ayoub/site1/centrecall.

Comme ci-dessous :



Après j'ai utilisé snap pour installer docker, j'ai donc installé snap en faisant : apt-get install snap et Docker grâce à la commande : snap list | grep docker , snap permet d'installer docker de manière simplifier et de mettre à jour automatiquement docker.

```
root@bunt:~# apt-get install snap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  snap
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 377 kB of archives.
After this operation, 2,756 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 snap amd64 2013-11-29-11 [377 kB]
Fetched 377 kB in 1s (648 kB/s)
Selecting previously unselected package snap.
(Reading database ... 87065 files and directories currently installed.)
Preparing to unpack .../snap_2013-11-29-11_amd64.deb ...
Unpacking snap (2013-11-29-11) ...
Setting up snap (2013-11-29-11) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@bunt:~#
root@bunt:~#
root@bunt:~# snap docker
error: unknown command "docker", see 'snap help'.
root@bunt:~# snap install docker
2025-06-25T08:58:27Z INFO Waiting for automatic snapd restart...
Run configure hook of "docker" snap if present
[ 4429.494107] overlayfs: missing 'lowerdir'
docker 27.5.1 from Canonical✓ installed
root@bunt:~#
```

```
root@bunt:~# snap list | grep docker
docker  27.5.1    3064   latest/stable  canonical**  -
root@bunt:~# docker --version
*Docker version 28.3.0, build 38b7060
root@bunt:~# *
error: unknown command "vboxpostinstall.sh", see 'snap help'.
root@bunt:~#
root@bunt:~#
root@bunt:~# addgroup --system docker
info: The group `docker' already exists as a system group. Exiting.
root@bunt:~# adduser ayoub docker
info: The user `ayoub' is already a member of `docker'.
root@bunt:~# adduser root docker
info: Adding user `root' to group `docker' ...
root@bunt:~# newgrp docker
root@bunt:~# snap start docker
Started.
root@bunt:~# docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
e6590344b1a5: Pull complete
Digest: sha256:940c619fbd418f9b2b1b63e25d8861f9cc1b46e3fc8b018ccfe8b78f19b8cc4f
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```

Ensuite dans le chemin ou j'ai déposé mon site je crée un fichier nommer dockerfile qui contient la conf suivante :

```
# Utilise l'image officielle Nginx (version légère Alpine)

FROM nginx:alpine

# Copie tous les fichiers du dossier courant dans le conteneur

COPY . /usr/share/nginx/html

# Expose le port 80 (HTTP)

EXPOSE 80
```

Et je crée ensuite l'image docker en faisant : docker build -t site1 .

**Explications** :

- -t site1 : Nomme l'image "site1"
- . : Utilise le dossier courant comme contexte de construction

Et je fini par le lancement du conteneur grâce à la commande : docker run -d -p 80 :80 –name centrecall site1

**Options** :

- -d : Détache le conteneur (arrière-plan)
- -p 80:80 : Mappe le port 80 du conteneur → port 80 de l'hôte
- --name centrecall : Nomme le conteneur

Pour être sûr que le firewall ne dérange pas j'autorise le port 80 grâce à la commande :

```
Ufw allow 80/tcp

Ufw reload
```

Et voilà le résultat

## 10.4 Exercice : Hébergement site web avec IIS

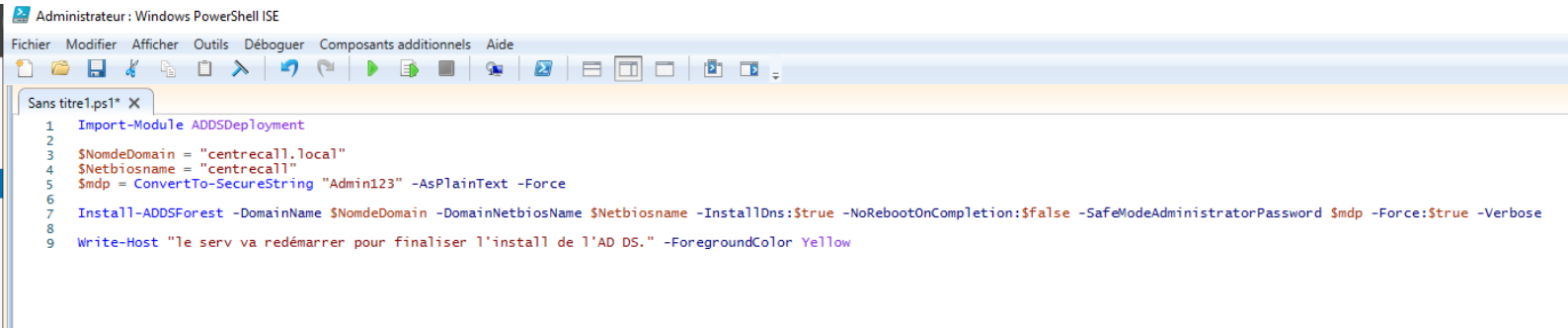
Après la création des deux vm serveur et cliente, je configure le serveur en installant tous les services utiles en commande PowerShell. J'ai installé IIS, AD DS et DNS que j'ai installé directement dans le gestionnaire de serveur. Pour savoir tous ce qu'il fallait installer j'utiliser la commande get-windowsfeature et le début du nom du service souhaiter avec une étoile.

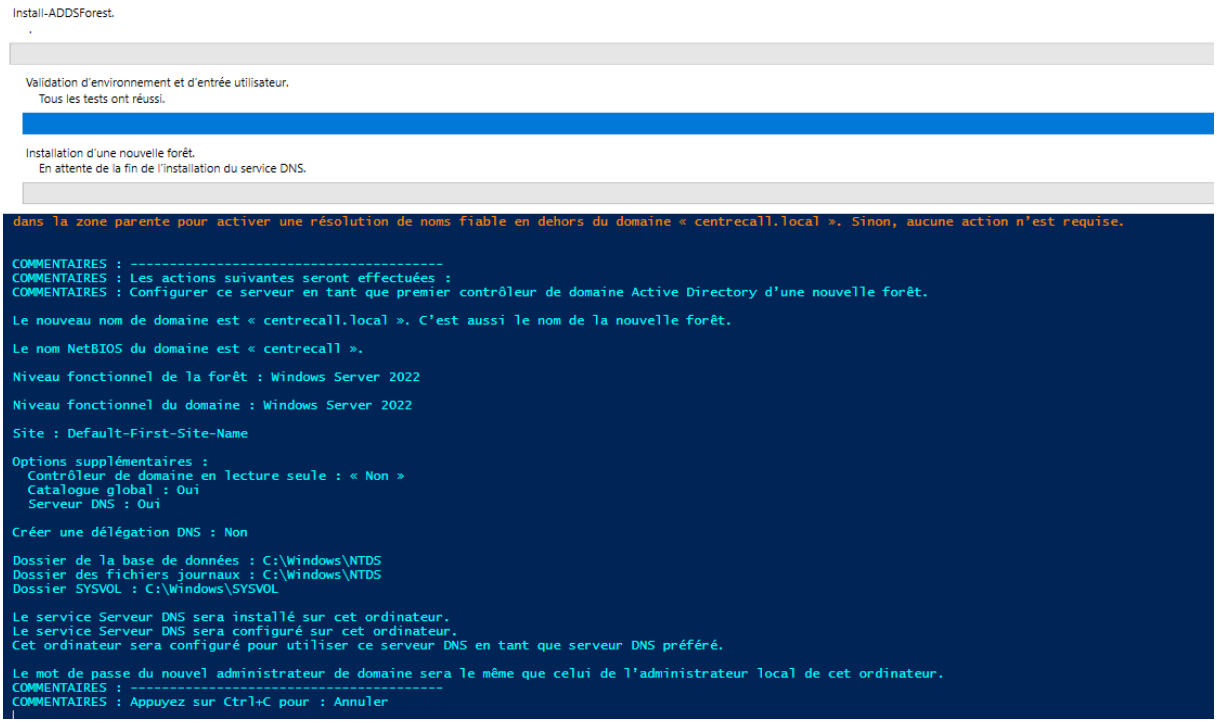
```
PS C:\Users\Administrateur> install-windowsfeature web-server -IncludeAllSubFeature
```

```
PS C:\Users\Administrateur> get-windowsfeature ad*

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[ ] Services AD DS                                      AD-Domain-Services          Available
[ ] Services AD LDS (Active Directory Lightweight Di... ADLDS                       Available
[ ] Services AD RMS (Active Directory Rights Managem... ADRMS                       Available
    [ ] Active Directory Rights Management Server       ADRMS-Server                Available
    [ ] Prise en charge de la fédération des identités  ADRMS-Identity              Available
[ ] Services de certificats Active Directory            AD-Certificate              Available
    [ ] Autorité de certification                       ADCS-Cert-Authority         Available
    [ ] Inscription de l'autorité de certification v... ADCS-Web-Enrollment         Available
    [ ] Répondeur en ligne                              ADCS-Online-Cert            Available
    [ ] Service d'inscription de périphérique réseau    ADCS-Device-Enrollment      Available
    [ ] Service Web Inscription de certificats          ADCS-Enroll-Web-Svc         Available
    [ ] Service Web Stratégie d'inscription de certi... ADCS-Enroll-Web-Pol         Available
[ ] Services de fédération Active Directory (AD FS)     ADFS-Federation             Available

PS C:\Users\Administrateur> install-windowsfeature ad-domain-services -IncludeAllSubFeature
```

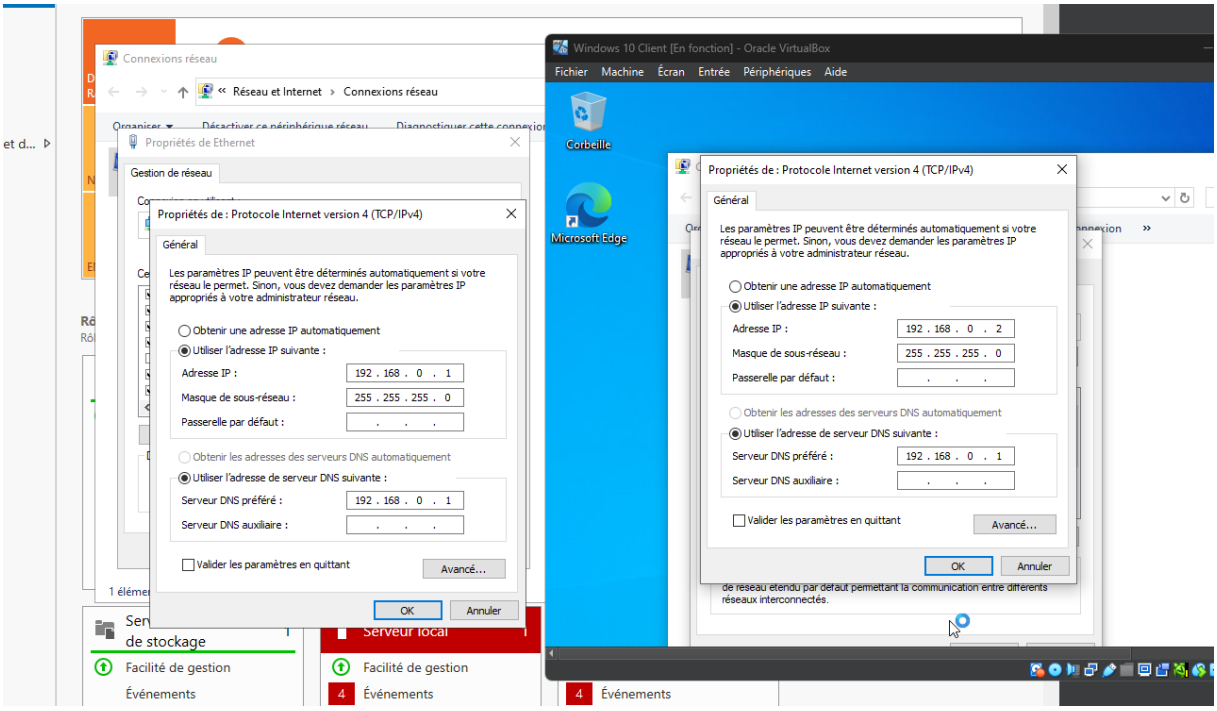
```
PS C:\Users\Administrateur> install-windowsfeature ad-domain-services -IncludeAllSubFeature
```

Ensuite j'ai configuré le service AD DS en PowerShell

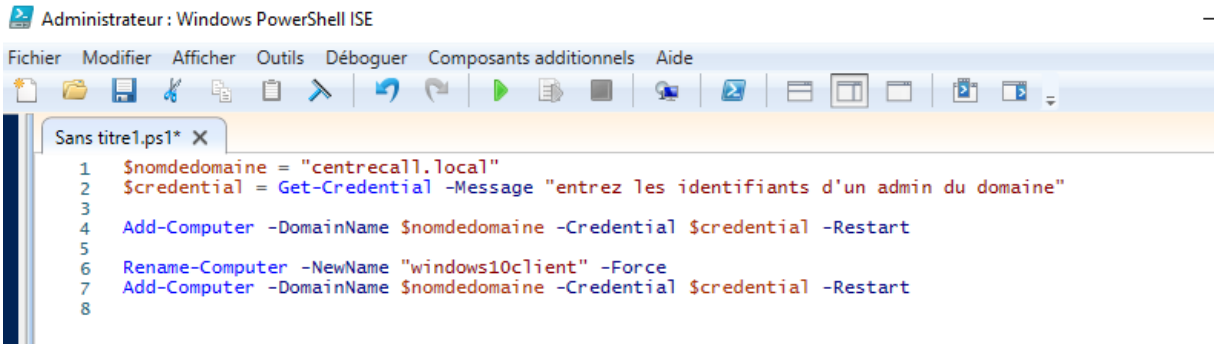




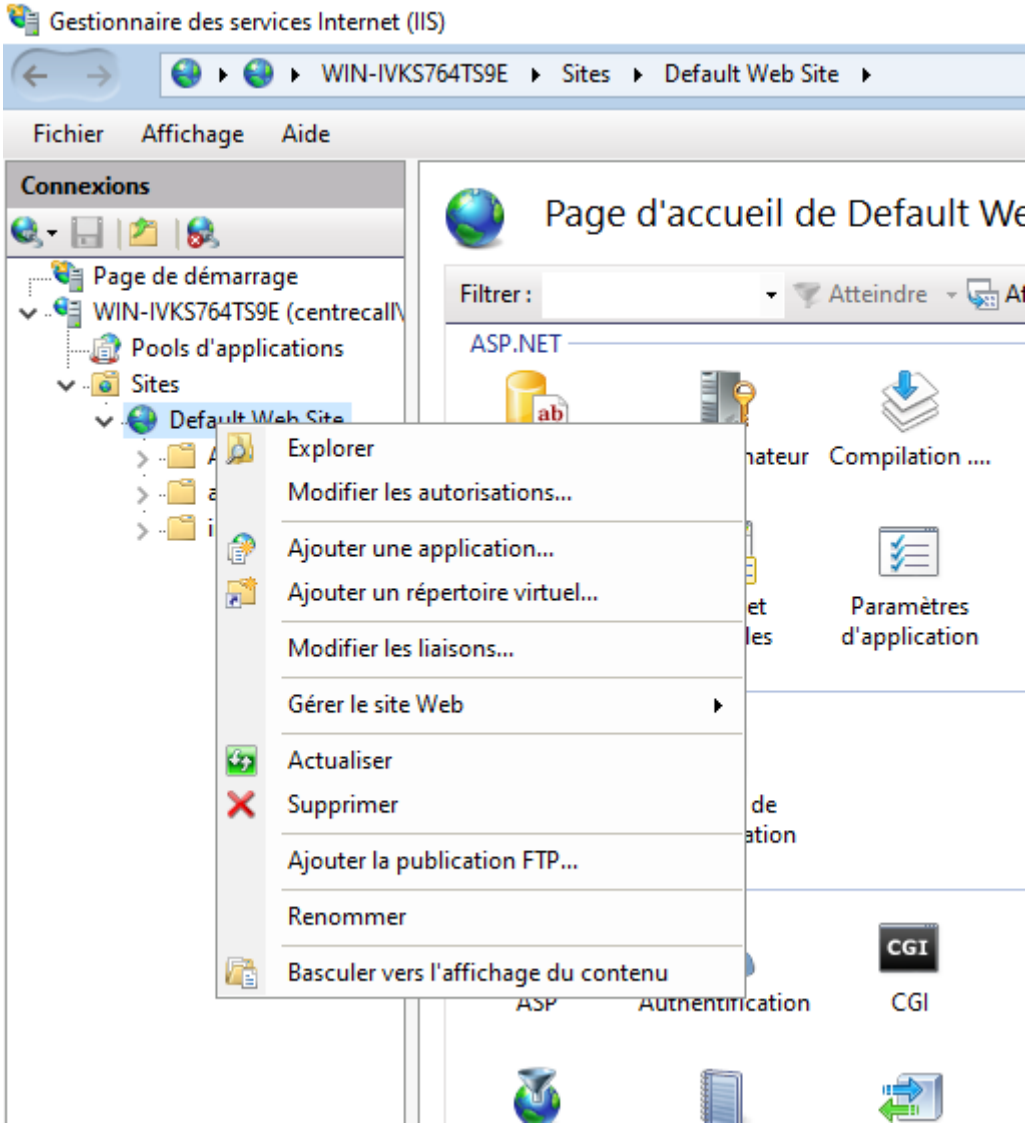

Après avoir bien configurer les IP en statique de deux vm comme ceci :

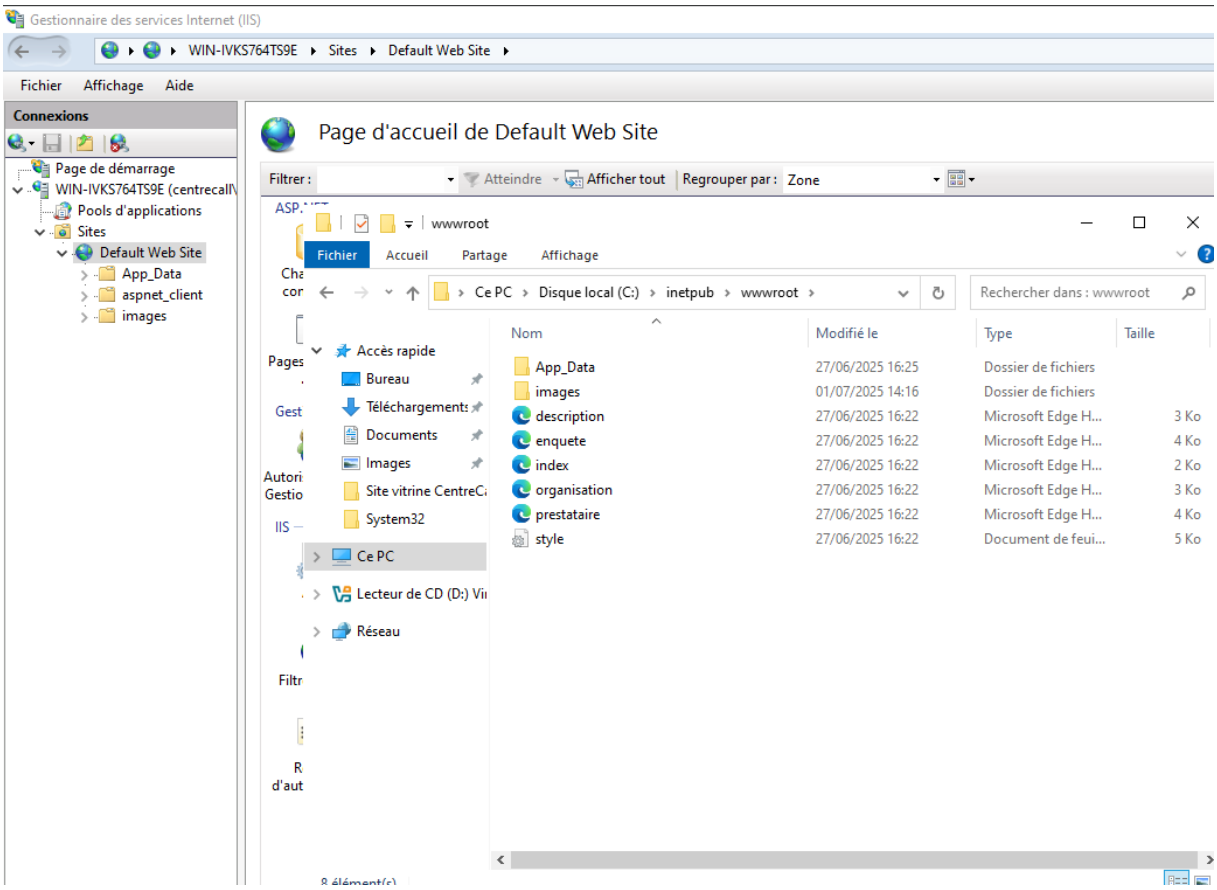


Je fais un script PowerShell qui va me faire rejoindre ma cliente au domaine de mon serveur

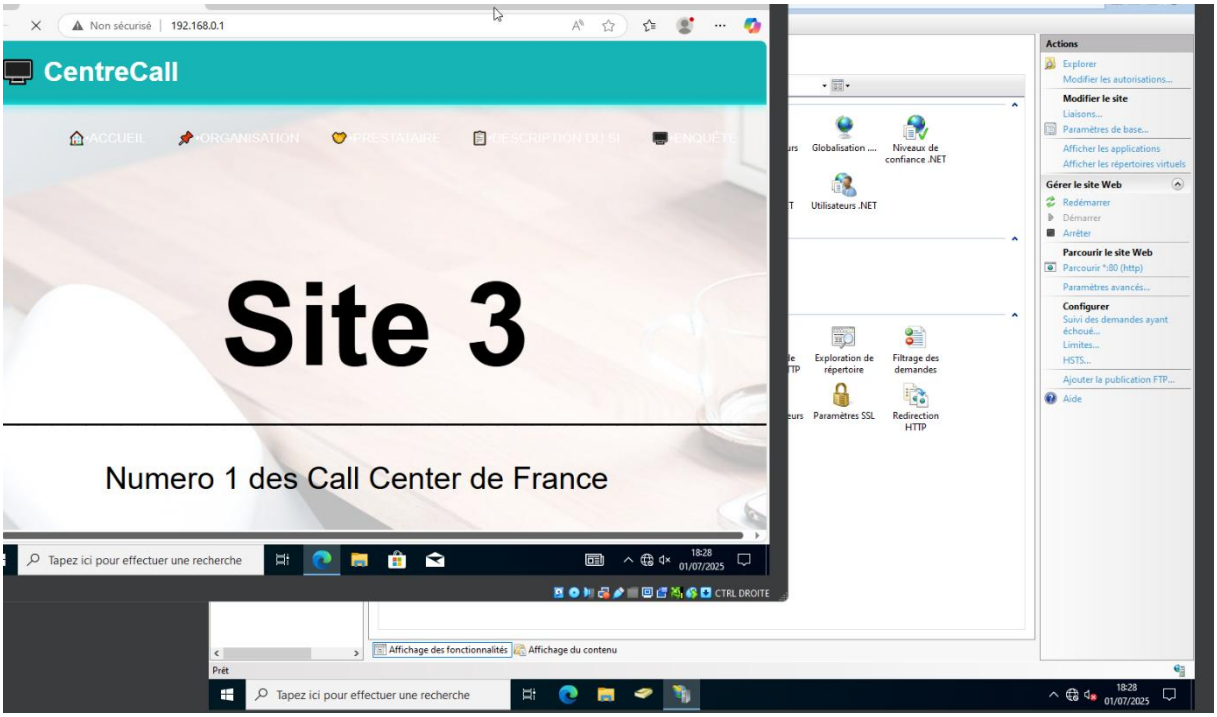



Je vais ensuite sur mon serveur dans gestionnaire des services internet et je fais un clic droit sur default web site, je clic sur explorer et je supprime le contenu et le remplace par mon site


Gestionnaire des services Internet (IIS)
WIN-IVKS764TS9E ▸ Sites ▸ Default Web Site ▸
Fichier Affichage Aide
Connexions
Page de démarrage
WIN-IVKS764TS9E (centrecall\
Pools d'applications
Sites
Default Web Site
Page d'accueil de Default We
Filtrer :
Atteindre
ASP.NET
Compilation ....
Paramètres d'application
CGI
Explorer
Modifier les autorisations...
Ajouter une application...
Ajouter un répertoire virtuel...
Modifier les liaisons...
Gérer le site Web
Actualiser
Supprimer
Ajouter la publication FTP...
Renommer
Basculer vers l'affichage du contenu


Gestionnaire des services Internet (IIS)
WIN-IVKS764TS9E ▸ Sites ▸ Default Web Site ▸
Fichier Affichage Aide
Connexions
Page de démarrage
WIN-IVKS764TS9E (centrecall\
Pools d'applications
Sites
Default Web Site
App_Data
aspnet_client
images
Page d'accueil de Default Web Site
Filtrer :
Atteindre
Afficher tout
Regrouper par : Zone
wwwroot
Fichier Accueil Partage Affichage
Ce PC › Disque local (C:) › inetpub › wwwroot ›
Rechercher dans : wwwroot
Accès rapide
Bureau
Téléchargements
Documents
Images
Site vitrine CentreC
System32
Ce PC
Lecteur de CD (D:) Vi
Réseau
Nom
Modifié le
Type
Taille
App_Data 27/06/2025 16:25 Dossier de fichiers
images 01/07/2025 14:16 Dossier de fichiers
description 27/06/2025 16:22 Microsoft Edge H... 3 Ko
enquete 27/06/2025 16:22 Microsoft Edge H... 4 Ko
index 27/06/2025 16:22 Microsoft Edge H... 2 Ko
organisation 27/06/2025 16:22 Microsoft Edge H... 3 Ko
prestataire 27/06/2025 16:22 Microsoft Edge H... 4 Ko
style 27/06/2025 16:22 Document de feui... 5 Ko

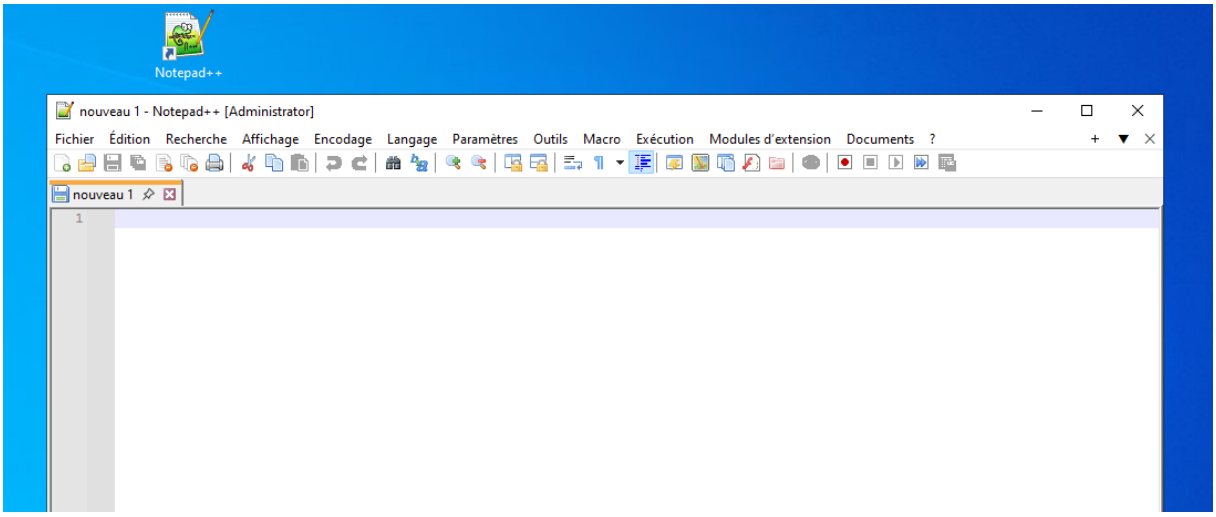
Et je redémarre ensuite le site pour que ça s'applique bien et je test sur mon serveur et ma cliente.



## 10.5 Exercice : déploiement d'une application et mise en place de GPO AppLocker

### 1. Installation de Notepad++

- Téléchargement manuel de l'installateur depuis le site officiel
- Vérification du bon fonctionnement après installation
-

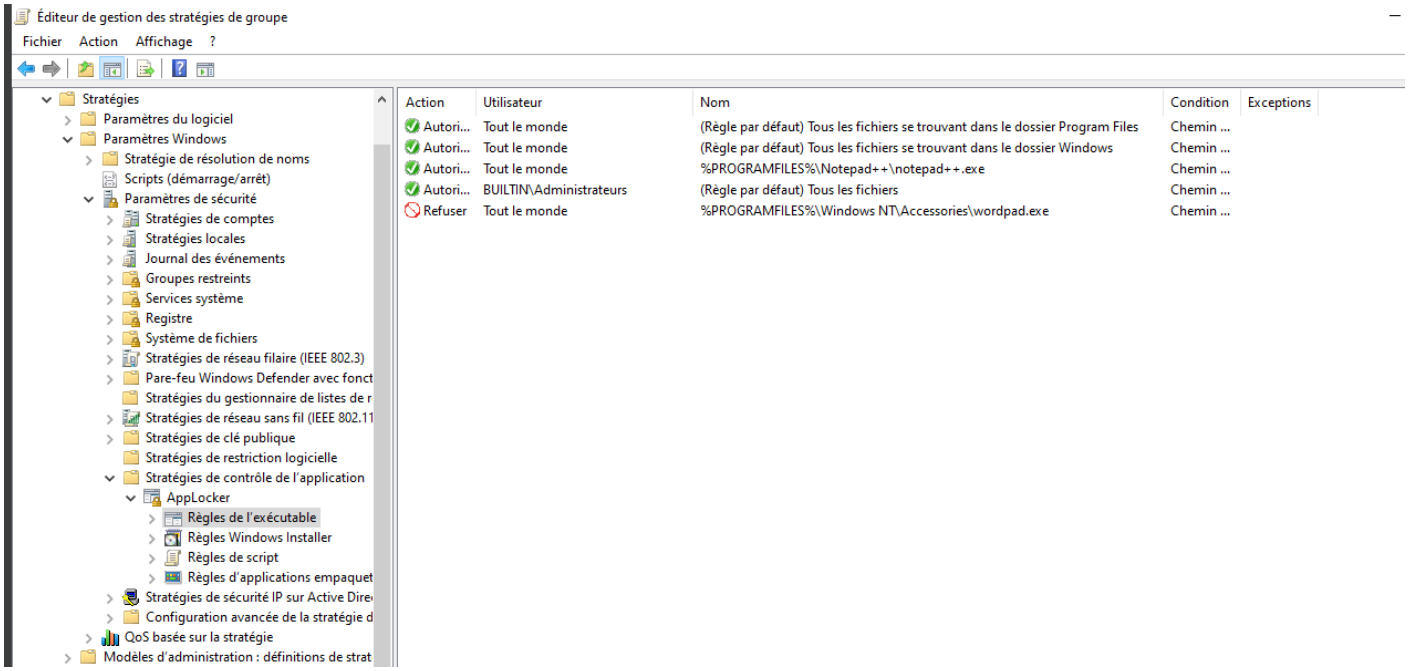



### 2. Configuration des GPO AppLocker

*Via l'éditeur de stratégie de groupe :*

1. Activation du service Application Identity (prérequis pour AppLocker)
2. Création de règles dans :
   Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de contrôle d'application > AppLocker
3. Ajout d'une règle d'autorisation pour Notepad++ :
   - Type : Règle de chemin
   - Chemin : C:\Program Files\Notepad++\notepad++.exe
   - Utilisateurs : Tous

4. Ajout d'une règle d'interdiction pour wordpad :
    - Type : Règle de chemin
    - Chemin : C:\Program Files\Windows NT\Accessories\wordpad.exe
    - Utilisateurs : Tous



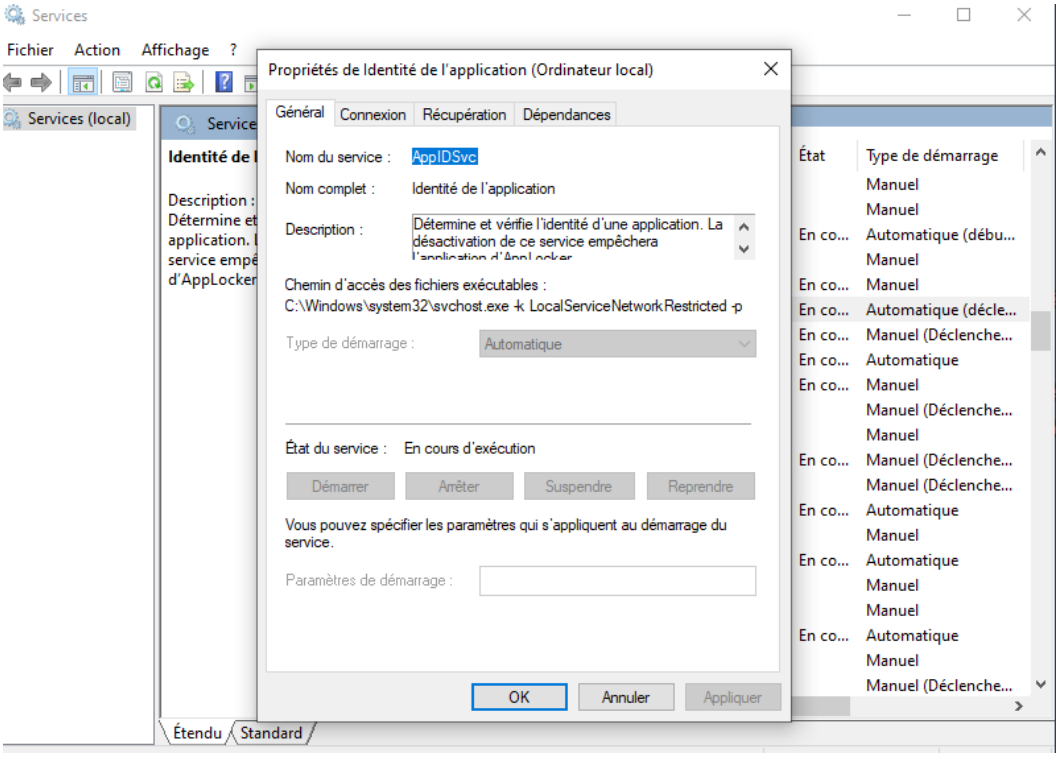
## 4. Activation de AppIDSvc pour que AppLocker s'applique

J'utilise un script powershell pour l'activer en automatique

```
PS C:\Windows\system32> Set-Service -Name AppIDSvc -StartupType Automatic
Set-Service : La description du service «Identité de l'application (AppIDSvc)» ne peut pas être configurée en raison
de l'erreur suivante: Accès refusé
Au caractère Ligne:1 : 1
+ Set-Service -Name AppIDSvc -StartupType Automatic
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (System.ServiceProcess.ServiceController:ServiceController) [Set-Servi
   ce], ServiceCommandException
    + FullyQualifiedErrorId : CouldNotSetServiceDescription,Microsoft.PowerShell.Commands.SetServiceCommand

PS C:\Windows\system32> Get-Service AppIDSvc | Select Name, StartType, Status

Name     StartType  Status
----     ---------  ------
AppIDSvc Automatic Stopped


PS C:\Windows\system32> Start-Service AppIDSvc -ErrorAction SilentlyContinue
PS C:\Windows\system32>
PS C:\Windows\system32> Get-Service AppIDSvc | Select Nmae, StartType, Status

Nmae StartType  Status
---- ---------  ------
     Automatic Running


PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
```

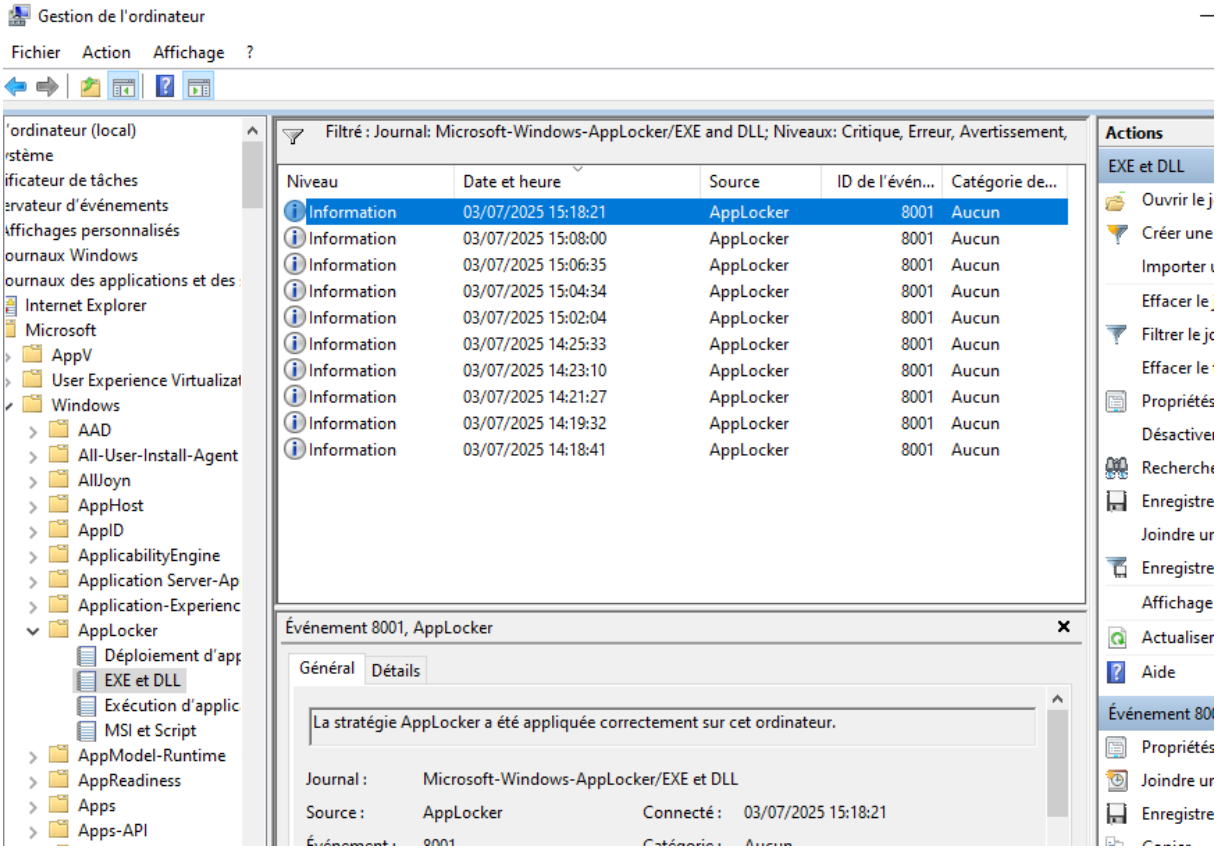


L'erreur indique que l'accès est refusé mais cela à bien fonctionner

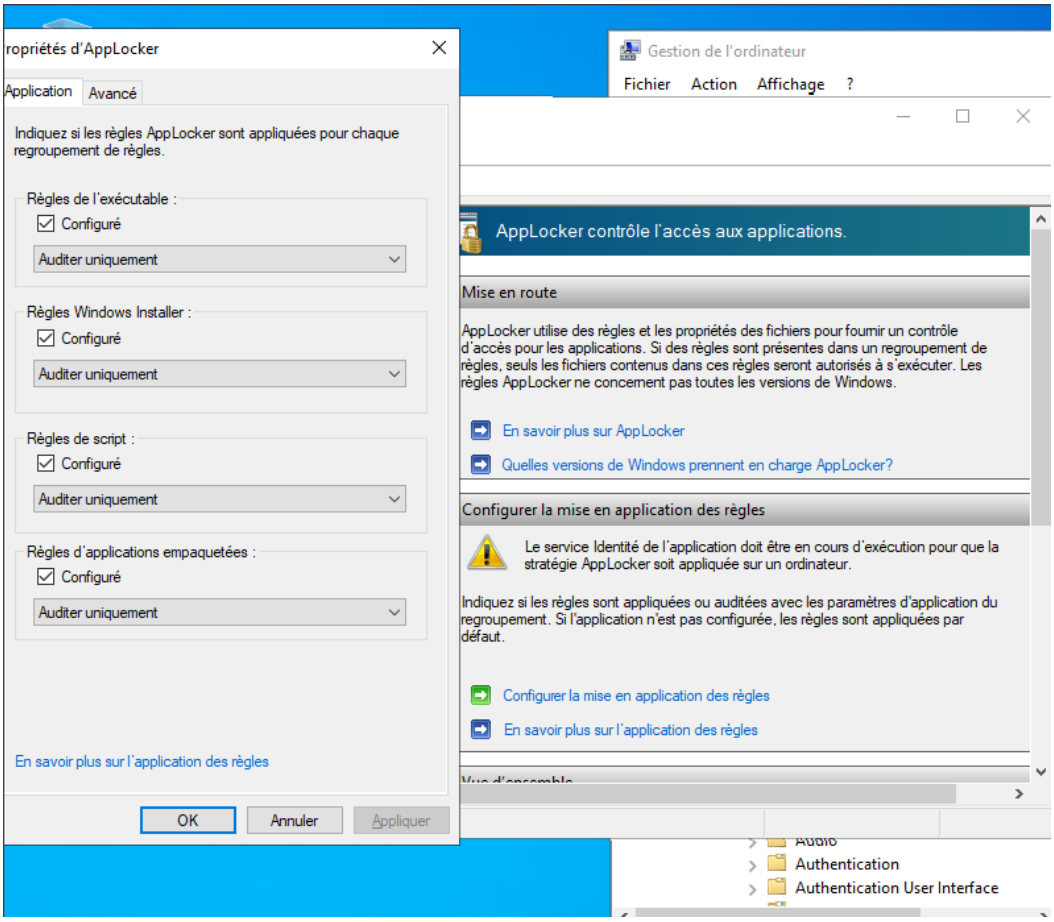


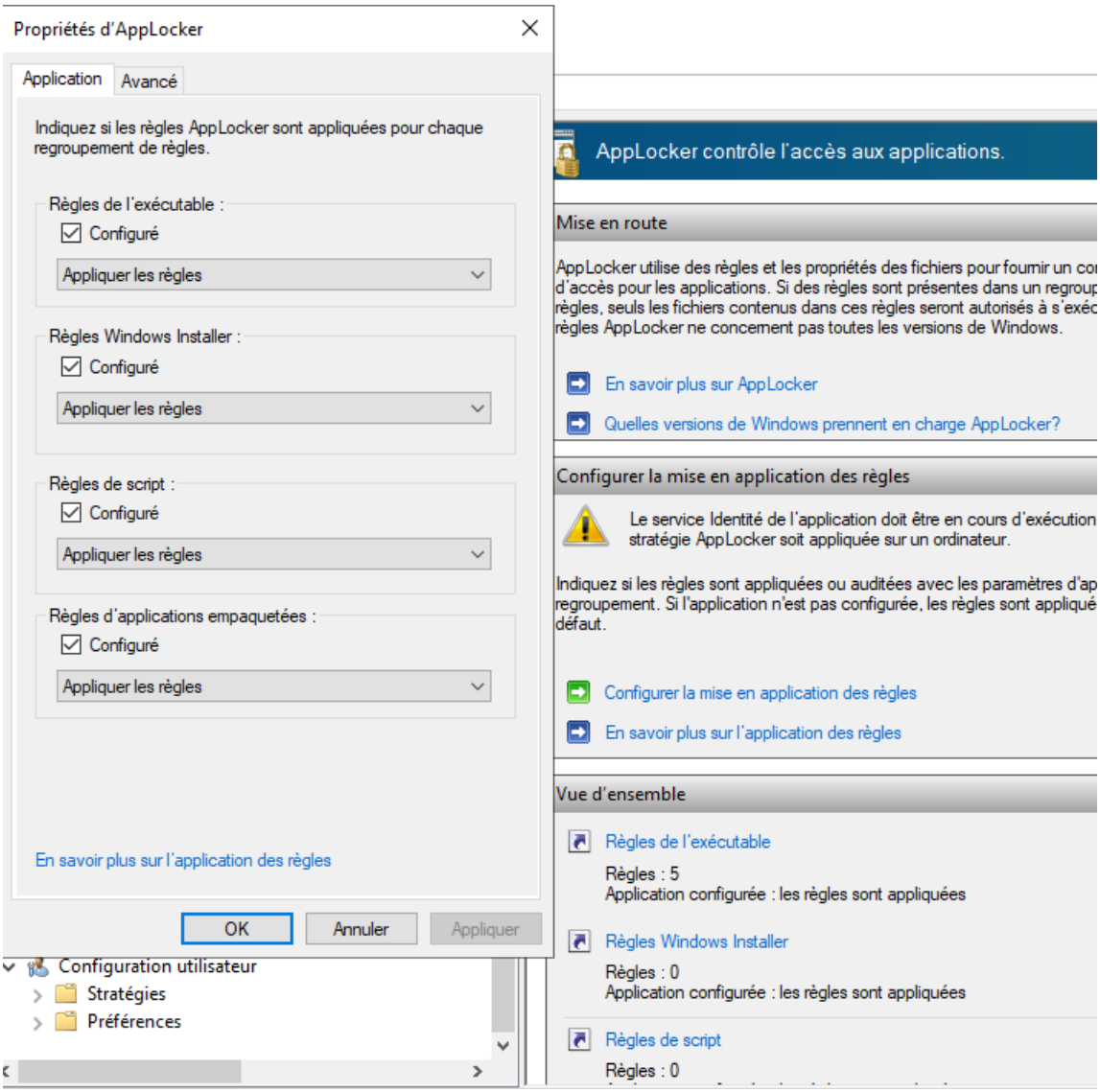
## 5. Validation en deux phases

1. Mode Audit :
    - Surveillance des logs dans l'Observateur d'événements
    - Vérification des éventuels faux positifs



2. Mode Enforcement :
    - Application des restrictions définitives
    - Blocage des autres éditeurs texte non autorisés




Propriétés d'AppLocker
Application
Avancé
Indiquez si les règles AppLocker sont appliquées pour chaque regroupement de règles.
Règles de l'exécutable :
Configuré
Appliquer les règles
Règles Windows Installer :
Configuré
Appliquer les règles
Règles de script :
Configuré
Appliquer les règles
Règles d'applications empaquetées :
Configuré
Appliquer les règles
En savoir plus sur l'application des règles
OK
Annuler
Appliquer
Configuration utilisateur
Stratégies
Préférences
AppLocker contrôle l'accès aux applications.
Mise en route
AppLocker utilise des règles et les propriétés des fichiers pour fournir un co
d'accès pour les applications. Si des règles sont présentes dans un regroup
règles, seuls les fichiers contenus dans ces règles seront autorisés à s'exéc
règles AppLocker ne concernent pas toutes les versions de Windows.
En savoir plus sur AppLocker
Quelles versions de Windows prennent en charge AppLocker?
Configurer la mise en application des règles
Le service Identité de l'application doit être en cours d'exécution
stratégie AppLocker soit appliquée sur un ordinateur.
Indiquez si les règles sont appliquées ou auditées avec les paramètres d'ap
regroupement. Si l'application n'est pas configurée, les règles sont appliqué
défaut.
Configurer la mise en application des règles
En savoir plus sur l'application des règles
Vue d'ensemble
Règles de l'exécutable
Règles : 5
Application configurée : les règles sont appliquées
Règles Windows Installer
Règles : 0
Application configurée : les règles sont appliquées
Règles de script
Règles : 0

## 10.6 Présentation de l'application ACRU (IAM)