

## WDS

1. Entrer le PC WDS dans le domaine
2. Installer le service de déploiement Windows depuis l'ajout de fonctionnalité du gestionnaire de serveur en sélectionnant les valeurs par défaut
3. Lancer le service de déploiement Windows et activer le serveur en faisant clique droit dessus
4. Installer ADK 1809 (pareil pour les extensions PE) depuis le site de Microsoft afin de pouvoir faire du déploiement sur des architectures en x86 parce que les versions ultérieures ne prennent plus en charge le support pour ce type là (<https://learn.microsoft.com/fr-fr/windows-hardware/get-started/adk-install> )
5. Durant la configuration de l'install cocher seulement les fonctionnalités suivantes: Outil de déploiement, Concepteur de fonctions d'acquisition etc, Concepteur de configuration et Outil de migration utilisateur
6. Ensuite télécharger et installer MDT avec les valeurs par défauts (<https://www.microsoft.com/en-us/download/details.aspx?id=54259> )
7. Lancer "Deployment Workbench"
8. Clic droit sur "Deployment Share" puis clic sur "New Deployment Share"
9. Laisser les paramètres par défaut et lancer la création
10. Dans l'explorateur de fichier → "C:." nous devons avoir un dossier "Deployment Share"
11. Ouvrir Powershell en admin et rentrer le code suivant afin de créer un utilisateur local pour MDT:
12. **# Spécifier le nom et le mot de passe du compte de service**
13. `$ServiceAccountName = "Service_MDT"`
14. `$ServiceAccountPassword = ConvertTo-SecureString "P@ssword123!" -AsPlainText -Force`
- 15.
16. **# Créer le compte local**
17. `New-LocalUser $ServiceAccountName -Password $ServiceAccountPassword -FullName "MDT" -Description "Compte de service pour MDT"`
- 18.
19. **# Ajouter les droits en lecture sur le partage**
20. `Grant-SmbShareAccess -Name "DeploymentShare$" -AccountName "Service_MDT" -AccessRight Read -Force`
- 21.
22. **# Attribuer au compte de service les permissions nécessaires pour accéder aux fichiers de déploiement MDT**
23. `$MDTSharePath = "\\$env:COMPUTERNAME\DeploymentShare$"`
24. `$Acl = Get-Acl $MDTSharePath`
25. `$Rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Service_MDT","ReadAndExecute", "ContainerInherit, ObjectInherit", "None", "Allow")`
26. `$Acl.SetAccessRule($Rule)`
27. `Set-Acl $MDTSharePath $Acl`
- 28.

29. L'utilisateur doit par la suite avoir accès au dossier "Deployment Share" en lecture seule
30. Ouvrir Workbench → clic droit sur "Operating System" puis clic "Import Operating System" (on peut au préalable créer un dossier pour mieux organiser)
31. Sélectionner "Full set of source files" → Sélectionner le répertoire de l'image (si elle n'est pas de base sur la machine il faut télécharger l'iso et ensuite clic droit sur le fichier puis "monter" → nommer l'image → attendre la fin de l'import)
32. Ensuite plusieurs éditions devraient apparaître → supprimer toutes celles qui nous intéressent pas
33. Clic droit sur "Task sequences" → clic "New Task Sequences" → donner un id (ex: INSTWIN10), un nom et le dernier champ on le laisse → "Standard Task Sequence" → sélectionner le fichier ".wim" → "Do not specify a product key" → mettre un nom (ex: Administrateur), nom d'organisation, ne pas toucher au 3ème champ → établir un mot de passe admin et lancer
34. Clic droit sur le fichier qui vient d'apparaître → propriétés → "Task Sequence" → déployer le dossier "States Restore" → "Windows Update..." → Option → décocher la case "Disable this app" et cocher "Continue on error"
35. Ensuite si nous allons dans les propriétés du Windows Share dans "Windows PE" nous devrions avoir un message d'erreur mais c'est normal, nous allons y apporter un correctif
36. Ouvrez un CMD en admin et rentrez la commande `"mkdir "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\WinPE_OCs"`
37. En retournant dans le menu "Windows PE" nous ne devrions plus avoir ce message
38. Ouvrez le gestionnaire de fichiers et allez dans `"C:\Program Files\Microsoft Deployment Toolkit\Templates"` → clic droit sur le fichier "Unattted\_PE\_x64.xml" → "Propriétés" et remplacer l'entièreté de son contenu par celui ci "dispo sur: [https://learn.microsoft.com/en-us/intune/configmgr/mdt/known-issues?WT.mc\\_id=AZ-MVP-5004580#hta-applications-report-script-error-after-upgrading-to-adk-for-windows-11-version-22h2?WT.mc\\_id=AZ-MVP-5004580](https://learn.microsoft.com/en-us/intune/configmgr/mdt/known-issues?WT.mc_id=AZ-MVP-5004580#hta-applications-report-script-error-after-upgrading-to-adk-for-windows-11-version-22h2?WT.mc_id=AZ-MVP-5004580)":
39. Puis sauvegardez le fichier
40. Clic droit sur le Deployment Share → Propriétés → Rules

```
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="windowsPE">
    <component name="Microsoft-Windows-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State">
      <Display>
        <ColorDepth>32</ColorDepth>
        <HorizontalResolution>1824</HorizontalResolution>
        <RefreshRate>60</RefreshRate>
        <VerticalResolution>768</VerticalResolution>
      </Display>
      <RunSynchronous>
        <RunSynchronousCommand wcm:action="add">
          <Description>Fix HTA scripts error Windows 11 ADK 22H2</Description>
          <Order>1</Order>
          <Path>reg.exe add "HKLM\Software\Microsoft\Internet Explorer\Main" /t REG_DWORD /v JscriptReplacement /d 0 /f</Path>
        </RunSynchronousCommand>
        <RunSynchronousCommand wcm:action="add">
          <Description>Lite Touch PE</Description>
          <Order>2</Order>
          <Path>wscript.exe X:\Deploy\Scripts\LiteTouch.wsf</Path>
        </RunSynchronousCommand>
      </RunSynchronous>
    </component>
  </settings>
</unattend>
```

 Filtrer par titre

## Bien démarrer

Bien démarrer

**Téléchargez et installez Windows ADK**

Installer ADK hors connexion

Vue d'ensemble des kits et des outils

Nouveautés de Windows ADK

Nouveautés de Windows 11

Conception

Personnaliser

Fabriquer

Service

Tester les performances et la compatibilité

- Windows ADK pour Windows 10, version 1903 [🔗](#)
- Extension Windows PE pour ADK, version 1903 [🔗](#)

Windows 10, version 1909.

Téléchargez ADK pour Windows 10, version 1809 :

- Windows ADK pour Windows 10, version 1809 [🔗](#)
- Extension Windows PE pour ADK, version 1809 [🔗](#)

Nouveautés d'ADK pour Windows 10, version 1809

Nouveau à partir de Windows 10, version 1809, l'environnement de préinstallation Windows (WinPE) est disponible séparément du kit d'évaluation et de déploiement (ADK)

ADK pour Windows 10, version 1803 [🔗](#)

Nouveautés d'ADK pour Windows 10, version 1803

ADK pour Windows 10, version 1709 [🔗](#)

Nouveautés d'ADK pour Windows 10, version 1709. Pour IoT Core pour Windows 10 version 1709, téléchargez [Extension IoT Core Add pour ADK](#)

## **CHANGER D'IP SUR WINDOWS**

1. Se rendre dans le panneau de Configuration
2. Changer les Icônes en petite (ou grandes pour les aveugles)
3. Aller dans "Modifier les paramètres de la carte Réseau"
4. Trouver la carte utilisé (wifi ou ethernet)
5. Modifier l'ip, la passerelle et le DNS

Se connecter sur le serveur Centreon en ssh.

Taper la commande :

```
apt install centreon-plugin-network-cisco-standard-snmp
```

Se connecter sur le Switch Cisco en ssh.

```
en
```

Active le mode de modification

```
conf t
```

Active le mode de configuration

```
snmp-server community public RO
```

Fait rejoindre le serveur SNMP Public

Si il ne remonte pas automatiquement :

```
en
```

```
conf t
```

```
no snmp-server community public RO
```

Retire le serveur SNMP Public

```
snmp-server community "nom communauté" RW
```

Fait rejoindre le serveur SNMP "x"

Dans le contexte le nom de la communauté est GSB.

# **CONF VLAN**

**Remise à zéro:** en → enable  
del flash:vlan.dat → effacer la conf des vlan  
write erase → remise à zéro des paramètres  
reload → redémarrer

## **Configuration d'un VLAN:**

**1)**

```
en
conf t
vlan 10 → déclarer le vlan
name admin → le nommer
```

**2)**

```
conf t
interface vlan10
ip address 172.16.230.0 255.255.255.192
no shut
ex
```

("no" au début d'une ligne de commande pour l'annuler dans la conf)

## **Sauvegarder la conf:**

copy run start → sauvegarde de la conf

shru → affiche la conf en cours

show vlan → voir les vlan configurés

ip access-list sta + nom → créer une access list (ACL)

permit any/deny...

ip access-group ACL10 out

ACL standard = filtrage sur l'IP source

ACL étendue = filtrage par IP (source et destinataire) par protocole et par port d'origine (source et destinataire)

## **AD - Problème réplication**

Si la réplication entre les deux AD ne se fait pas il faut:

1. Faire un snapshot des deux machines
2. Dans le terminale Powershell en admin effectuer la commande "repadmin /replsummary"
3. Regarder si cela donne lieu à des erreurs en DSA Source et DSA Destination
4. Vérifier si dans la conf de la carte réseau le DNS préféré est celui-ci de la deuxième machine afin qu'elles se pointent entre elles
5. Dans les deux machines AD, terminale Powershell en admin entrer la commande "net stop netlogon" puis "net start netlogon"
6. Entrer la commande "nslookup ad2.tondomaine.local" et vérifier si elle ressort bien l'IP correspondante
7. Ensuite relancer la réplication avec "repadmin /syncall /AdeP"
8. Redémarrer les deux machines et regarder si la réplication est cette fois effectuée
9. Pour finir refaire un "repadmin /replsummary"

## **Délai avant synchro GPO**

Si une GPO est créée sur l'un des deux AD mais qu'elle n'est pas répliquée sur l'autre alors suivre les étapes suivantes depuis la machine ne recevant pas les nouvelles GPO :

1. Relancer l'éditeur de gestion des stratégies de groupes
2. Si ça ne change rien alors ouvrir le terminal Powershell en admin et rentrer "net stop netlogon" puis une fois le service éteint le redémarrer avec "net start netlogon"
3. Puis entrer "dfsrdiag pollad" pour forcer la réplication "normalement ce service se lance automatiquement toutes les 5min"
4. Entrer la commande "Get-Service dfsr, netlogon" et vérifier qu'ils soient bien en "running"
5. Vérifier de nouveau et ça devrait être bon



# Conf Fortinet

## **Conf Fortinet**

1. Brancher le poste sur le port 1
2. Attribuer l'adresse IP indiquée sur le Fortinet (ici 192.168.1.1 255.255.255.0) OU activer le DHCP
3. Ouvrir un navigateur et rentrer "<https://192.168.1.99>" (ip par défaut du Fortinet)
4. Si il s'agit de la première connexion id = "admin" et mot de passe laisser vide puis "se connecter". Il demandera ensuite de saisir l'ancien mot de passe, ici rien et ensuite le nouveau puis le confirmer
5. Configurer la WAN1 en lui mettant une adresse IP fixe et la bonne depuis Network → Interfaces → wan1
6. Désactiver le Firewall dans Policy & Objects → Firewall Policy → sélectionner celui souhaité
7. Si il n'y a pas de connexion à Internet alors vérifier s' il y a bien la route par défaut dans Static Routes. Si elle n'y est pas alors l'ajouter en cliquant sur "Create New"

### **Remise à zéro:**

Dans ce cas, il faut allumer le Fortinet en le branchant, par la suite entre 30 et 60s la led "statut" devrait commencer à clignoter lentement. A ce moment là il faut maintenir 10s le bouton reset qui se trouve à l'arrière à gauche. Suite à cela la led devrait commencer à clignoter rapidement et ensuite le Fortinet devrait redémarrer.

# **CENTREON WINDOWS**

## **Déploiement de la configuration (A faire plus tard!):**

1. Depuis la version web: **Configuration** → **Pollers** → **Pollers** puis sélectionner le serveur centrale et cliquer sur “Export configuration”

Configuration > Pollers

Poller

<input type="checkbox"/>	Name	IP Address	Server type	Is running ?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status	Actions
<input checked="" type="checkbox"/>	Central	127.0.0.1	Central	YES	YES	10793	16 hours 42 minutes	April 15, 2025 11:15:03 AM	Centreon Engine 24.10.6	Yes	ENABLED	

2. Cocher les cases: “Generate configuration files” / “Run monitoring engine debug (-v)” / “Restart monitoring engine” (choisir **Reload** si on modifié, créé ou supprimé des objets surveillés / **Restart** si on a modifié la communication entre le poller et le serveur central ou la configuration du moteur) **ICI il nous faut Reload**

Configuration > Pollers > Export configuration

| Configuration Files Export

Polling instances

Actions

☒ Generate Configuration Files

☒ Run monitoring engine debug (-v)

☒ Move Export Files

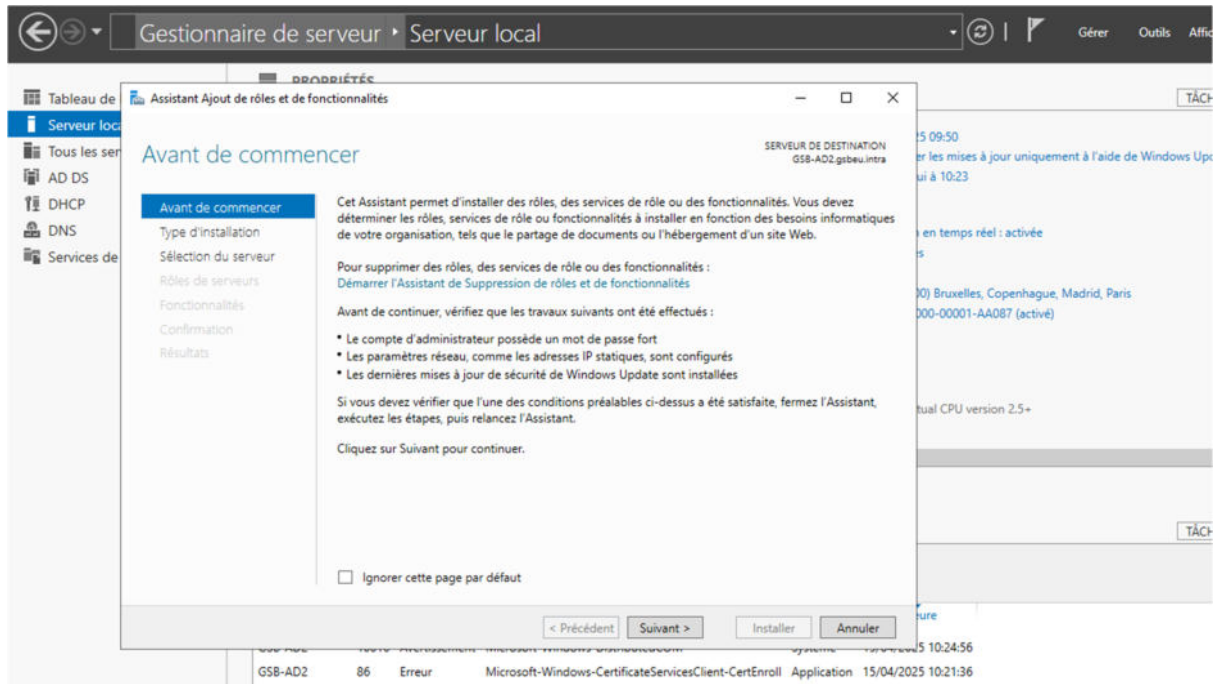
☒ Restart Monitoring Engine Method

☐ Post generation command

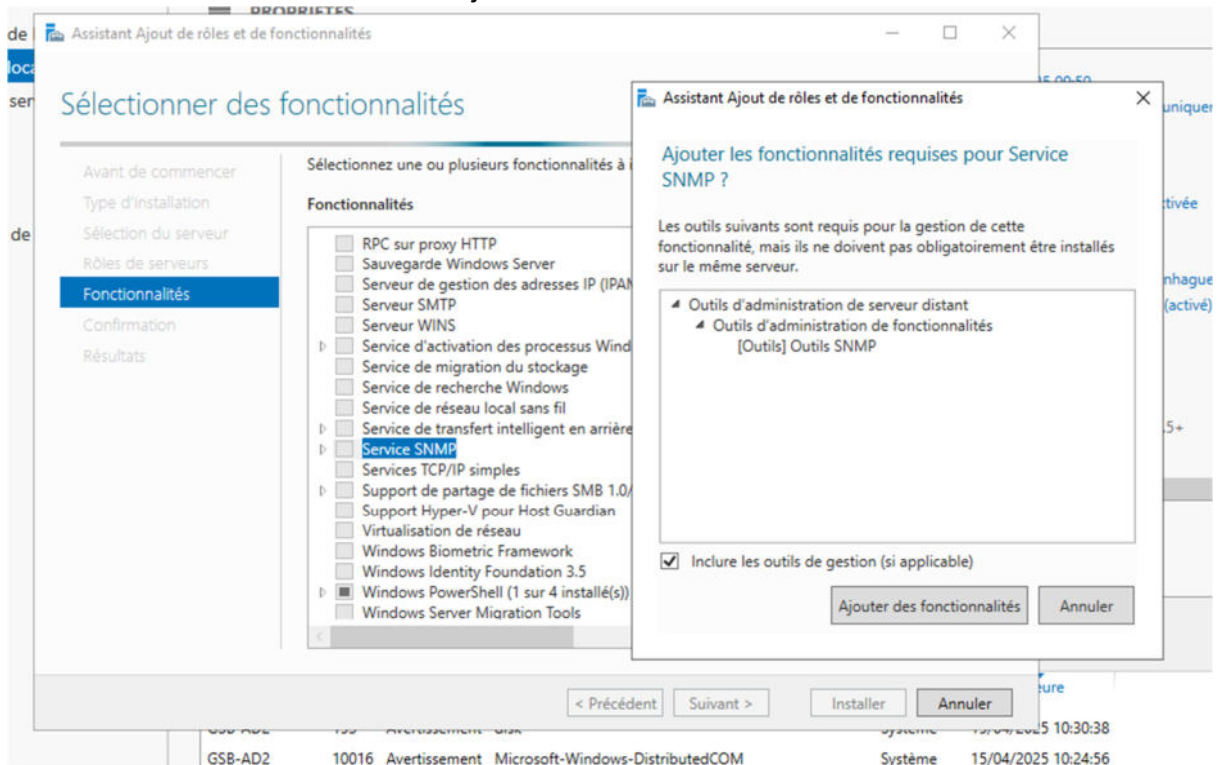
3. Cliquer sur “Exporter” et regarder à la fin des les logs si il n’y a pas d’erreurs

## **1/ Depuis le serveur client:**

1. Se rendre dans le gestionnaire de serveur → “gérer” → “ajouter des rôles et fonctionnalités



2. Sauter les 4èmes étapes avec les paramètres par défaut et sélectionner “Service SNMP” → ajouter toutes les fonctionnalités → installer



3. Dans Powershell en admin entrer la commande “ Add-WindowsCapability -Online -Name "SNMP.Client~0.0.1.0" “ afin d’installer le client

```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur.GSBEU> Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"
```

4. Puis “ Get-WindowsFeature -Name \*snmp\* | Install-WindowsFeature “

```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur.GSBEU> Get-WindowsFeature -Name *snmp* | Install-WindowsFeature
```

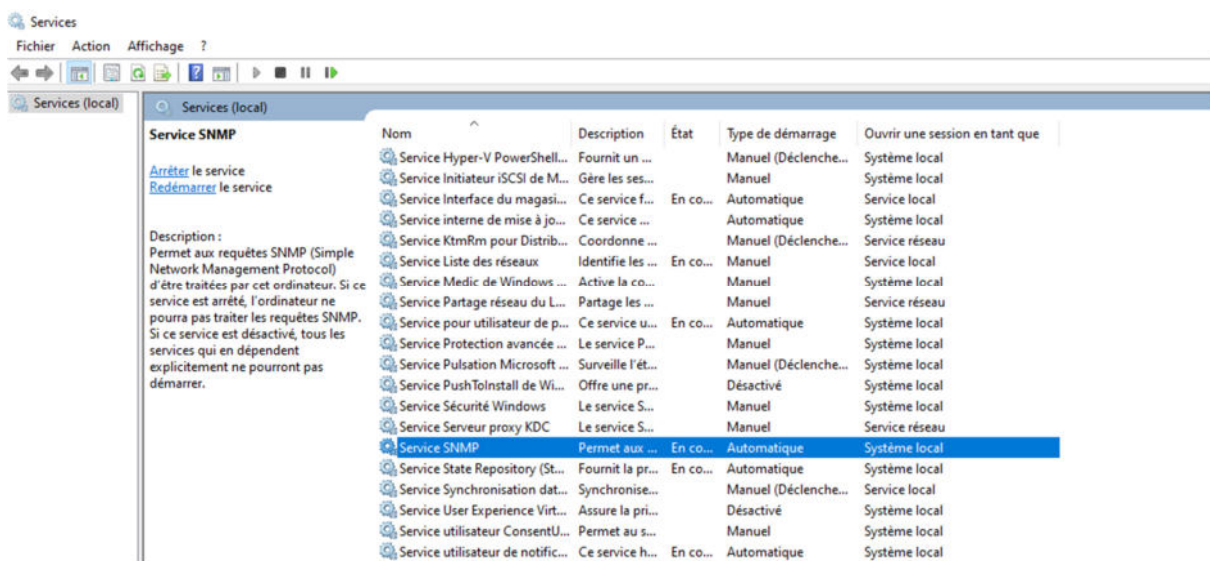
5. Pour finir “ Get-WindowsFeature -Name \*snmp\* “ afin d’être sûr que tout soit ok

```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur.GSBEU> Get-WindowsFeature -Name *snmp*
```

Display Name	Name	Install State
[X] Outils SNMP	RSAT-SNMP	Installed
[X] Service SNMP	SNMP-Service	Installed
[X] Fournisseur WMI SNMP	SNMP-WMI-Provider	Installed

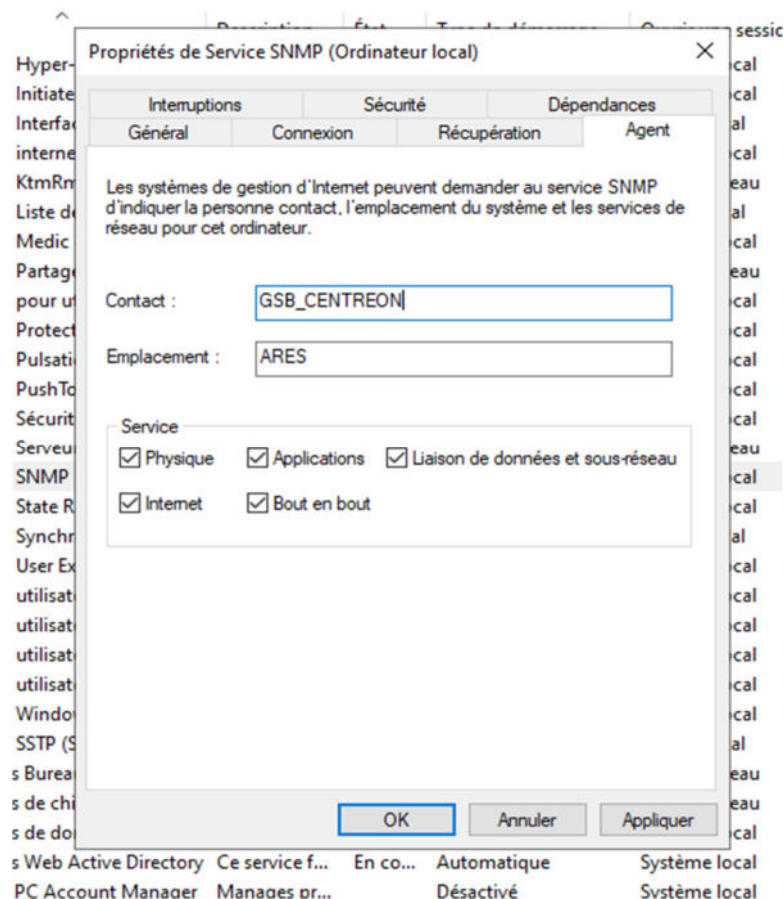
6. Ouvrir l’utilitaire “Services”

7. Recherchez “Service SNMP”

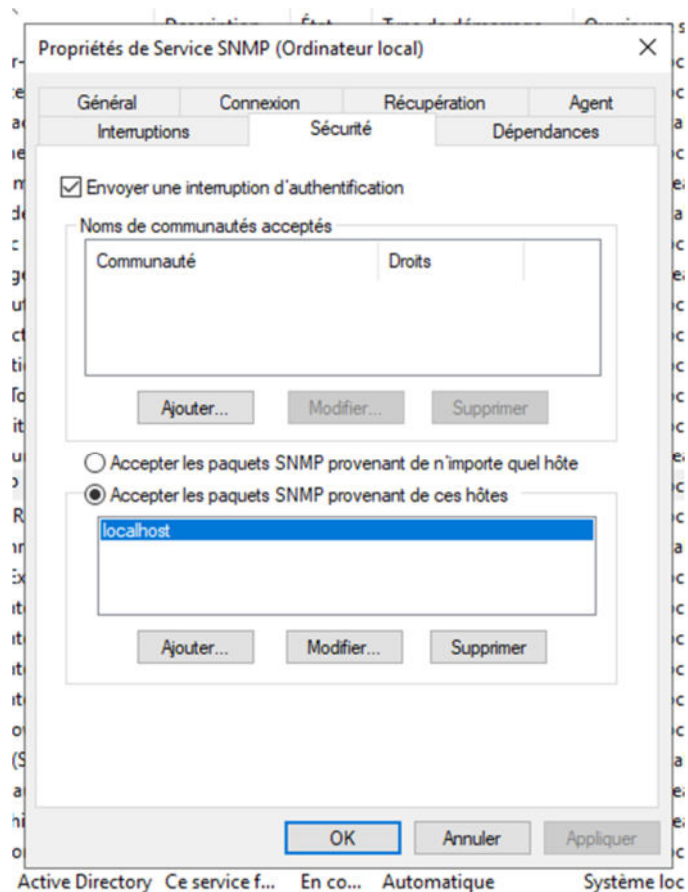


8. Clic droit → Propriétés → Agent → remplir les champs “Contact” et “Location” puis cocher les services sur lesquels on autorise la récupération de données

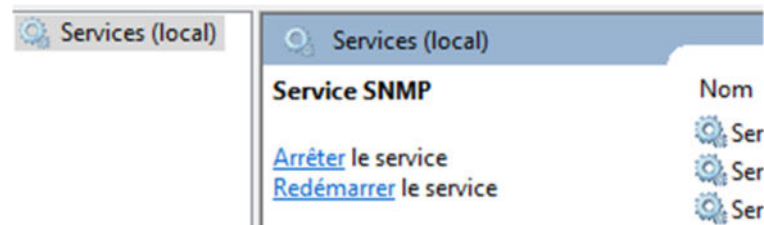
9. “Appliquer”



- Sécurité → ajouter le nom de communauté et le mettre en lecture seule → sélectionnez "Accepter les paquets SNMP provenant de ces hôtes" puis ajouter l'adresse IP du serveur Centreon → Appliquer et OK

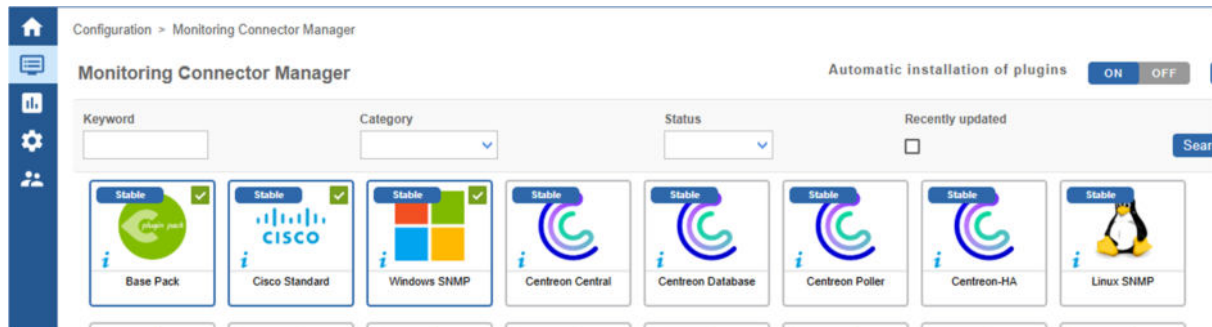


## 11. Redémarrer le service

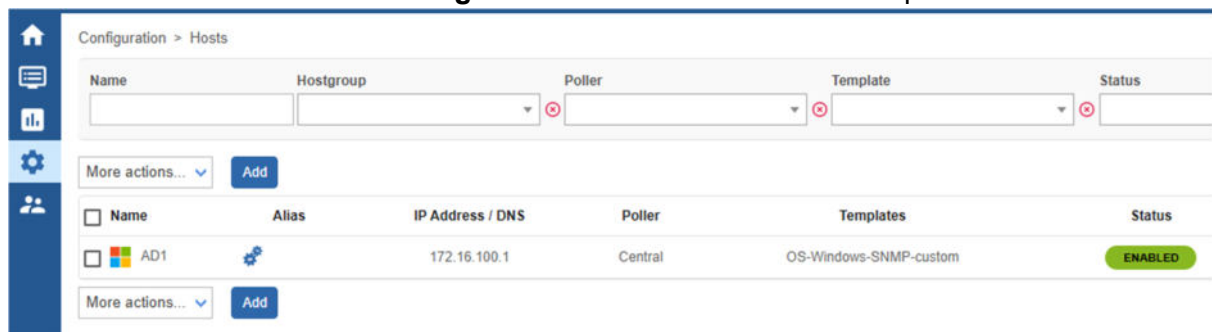


## 2/ Depuis Centreon web et serveur:

1. Depuis la machine du serveur Centreon entrez la commande “ dnf install centreon-plugin-Operatingsystems-Windows-Snmp ” afin d’installer les plugins pour Windows
2. Aller sur l’interface web aller dans **Configuration** → **Connectors** → **Monitoring Connectors** et installer le connecteur de surveillance “SNMP Windows”



3. Ensuite dans **Configuration** → **Hosts** → **Hosts** et cliquer sur Add en haut



4. Entrer le nom de serveur (ex:AD) → Mettre l’IP du serveur cible → Le nom de communauté (en général il faut choisir la version 2C car elle est plus sécurisée que la 1 et plus polyvalente que la 3, merci de faire des vérifications pour faire le choix face au besoin) → Sélectionner le poller qui surveillera le serveur (Central par défaut) → Dans Templates cliquer sur “Add a new entry” et sélectionner “OS-Windows-SNMP-custom” → Save



Host Configuration Notification Relations Data Processing Host Extended Infos Save Reset

**Modify a Host**

Host basic information

Name \* AD2

Alias

Address \* 176.16.100.2 Resolve

SNMP Community & Version GSB 2c

Monitoring server Central

Timezone Europe/Paris

Templates

A host or host template can have several templates. See help for more details.

+ Add a new entry

OS-Windows-SNMP-custom

Create Services linked to the Template too ☐ Yes ☒ No

Host check options

Check Command Check Command

Args

Custom macros

+ Add a new entry

Template inheritance Command inheritance

Name SNMPXTRAOPTIONS Value Password

Scheduling options

5. Aller dans **Configuration** → **Services** → **Services by host** et nous devrions voir un nouvel indicateur apparu automatiquement

Configuration > Services > Services by host

Hosts Services Templates Status ☐ Disabled hosts Search

More actions... Add 30

Host	Service	Scheduling	Template	Status	Options
<input type="checkbox"/> AD1	Cpu	5 min / 1 min	→ OS-Windows-Cpu-SNMP-custom → OS-Windows-Cpu-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Memory	15 min / 1 min	→ OS-Windows-Memory-SNMP-custom → OS-Windows-Memory-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Ping	5 min / 1 min	→ Base-Ping-LAN-custom → Base-Ping-LAN → generic-active-service-custom → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Swap	15 min / 1 min	→ OS-Windows-Swap-SNMP-custom → OS-Windows-Swap-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/> AD2	Cpu	5 min / 1 min	→ OS-Windows-Cpu-SNMP-custom → OS-Windows-Cpu-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Memory	15 min / 1 min	→ OS-Windows-Memory-SNMP-custom → OS-Windows-Memory-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Ping	5 min / 1 min	→ Base-Ping-LAN-custom → Base-Ping-LAN → generic-active-service-custom → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Swap	15 min / 1 min	→ OS-Windows-Swap-SNMP-custom → OS-Windows-Swap-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/> Switch	Cpu	5 min / 1 min	→ Net-Cisco-Standard-Cpu-SNMP-custom → Net-Cisco-Standard-Cpu-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Environment	15 min / 1 min	→ Net-Cisco-Standard-Environment-SNMP-custom → Net-Cisco-Standard-Environment-SNMP... → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Memory	10 min / 1 min	→ Net-Cisco-Standard-Memory-SNMP-custom → Net-Cisco-Standard-Memory-SNMP → ...	ENABLED	<input type="checkbox"/> 1
<input type="checkbox"/>	Ping	5 min / 1 min	→ Base-Ping-LAN-custom → Base-Ping-LAN → generic-active-service-custom → ...	ENABLED	<input type="checkbox"/> 1

More actions... Add 30

6. FAIRE LE DÉPLOIEMENT DE CONF EN HAUT
7. Accéder à Monitoring → Resources Status et enlever ce qu'il y a dans la barre de recherche et vérifier que tout s'affiche et que tout remonte et n'ait pas d'erreur (Cela peut prendre entre 5 à 10 min)