

Document Technique : Création et Configuration d'un Serveur WSUS sous Windows Server 2022 sur VMware vSphere

Semaine : 10/01/2025

Titre de la mission : Mise en place d'un serveur WSUS avec supervision SMTP (POM)

Mon objectif dans cette mission était de mettre en œuvre un serveur WSUS (Windows Server Update Services) sous Windows Server 2022, configuré comme machine virtuelle (VM) sur VMware vSphere. Le serveur devait être intégré au domaine Active Directory, configuré pour stocker les mises à jour sur un disque dédié, et supervisé via la plateforme POM avec des notifications par email.

(Suite à un ticket simulé par mon maître de stage)

Installation WSUS

Installation d'un nouveau serveur avec les caractéristiques suivantes et les contraintes:

Les MAJ seront stockées dans D:\WSUS\

Serveur

- OS : Windows 2022
- CPU : 4
- RAM : 8 Go
- Lecteur C: 100 Go --> Windows
- Lecteur D: 100 Go --> MAJ téléchargées

WSUS

Logiciels

- Windows 2012 et +
- SQL Server 2012
- SQL Server 2017
- SQL Server 2019
- SQL Server 2022

Actualisation de la liste des MAJ sur le serveurs en automatique

Approbation des MAJ manuelle

Installation des MAJ le samedi

Mail d'alertes à gr-infosys@wibaie.fr

- Liste des MAJ le jeudi à 21h
- Etats des MAJ le lundi à 7h

2. Prérequis

Matériel et logiciel nécessaires

- Accès à l'hôte VMware vSphere.
- Image ISO de Windows Server 2022.
- Licence Windows Server 2022 Standard.
- Accès administrateur au domaine Active Directory.

Rôles et fonctionnalités nécessaires

- WSUS (Windows Server Update Services).
- SMTP pour l'envoi de notifications.

Disques alloués

- **C** : 100 Go (Système).

- **D** : 100 Go (Stockage des mises à jour WSUS).

Informations réseau

- Adresse IP statique fournie par l'administrateur réseau.
- DNS pointant vers le ou les contrôleurs de domaine.
- Nom DNS et serveur SMTP de l'entreprise.

3. Étapes détaillées de la mise en place

Étape 1 : Création de la VM sur VMware vSphere

J'ai commencé par créer une nouvelle machine virtuelle :

1. J'ai accédé à VMware vSphere et cliqué sur **Create / Register VM**.
2. J'ai sélectionné **Create a new virtual machine** et renseigné les paramètres suivants :
 - **Nom de la VM** : SWIBAIE032.
 - **OS** : Windows Server 2022 (64 bits).
3. J'ai configuré les ressources matérielles :
 - **vCPU** : 4.
 - **RAM** : 8 Go.
 - **Disques** :
 - **C** : 100 Go (Thin provisioned).
 - **D** : 100 Go (ajouté plus tard pour le stockage WSUS).
 - **Carte réseau** : VMXNET3, connectée au VLAN approprié.
4. J'ai monté l'image ISO de Windows Server 2022 sur le lecteur CD/DVD virtuel et validé la création.

Modifier les paramètres | SWIBAIE032



Matériel virtuel

Options VM

AJOUTER UN PÉRIPHÉRIQUE ▾

> CPU	4 ▾	
> Mémoire	8 ▾	Go ▾
> Disque dur 1	100	Go ▾
> Disque dur 2	100	Go ▾
> Contrôleur SCSI 0	Paravirtuel VMware	
> Adaptateur réseau 1	VM Network ▾	<input checked="" type="checkbox"/> Connecté
> Lecteur CD/DVD 1	Fichier ISO banque de données ▾	<input checked="" type="checkbox"/> Connecté
> Contrôleur USB xHCI	USB 3.1	
> Carte vidéo	Spécifier les paramètres personnalisés ▾	
> Périphériques de sécurité	Non configuré	
Périphérique VMCI		
Contrôleur SATA 0	AHCI	
> Autre	Matériel supplémentaire	

ANNULER

OK

○

2. Validation et démarrage de la VM.

Étape 2 : Installation de Windows Server 2022

Ajout des rôles et fonctionnalités

1. J'ai ouvert le **Gestionnaire de Serveur** et sélectionné **Ajouter des rôles et fonctionnalités**.
2. J'ai ajouté le rôle **Windows Server Update Services (WSUS)**.
3. Lors de l'installation, j'ai configuré le stockage des mises à jour sur le disque **D :WSUS**.
1. se sécurisé pour le compte Administrateur.


Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

Nom d'utilisateur

Mot de passe

Entrez de nouveau le mot de passe

 Retour Terminer

2. Configuration post-installation :

- Renommez le serveur (par ex. :SWIBAIE032).
- Configurez une adresse IP statique :

Exemple :

IP : 192.168.1.X

Masque : 255.255.255.0

Passerelle : 192.168.1.X

DNS1 : 192.168.1.X (contrôleur de domaine primaire)

DNS2 : 192.168.1.X (contrôleur de domaine secondaire)

-
- Rejoignez le domaine Active Directory :



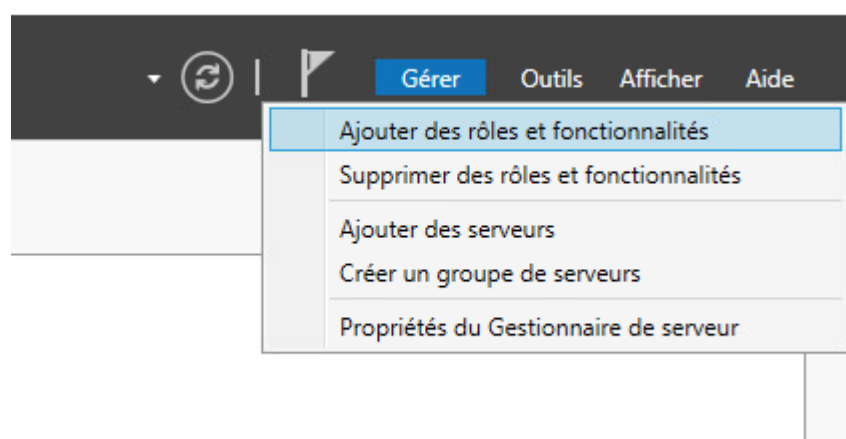
Étape 3 : Installation de WSUS

Avant cela dans VSphere je me rend sur Action ⇒ modifier des paramètres et rajouter un disque dur ou seront mise les mises à jour installer (D:)

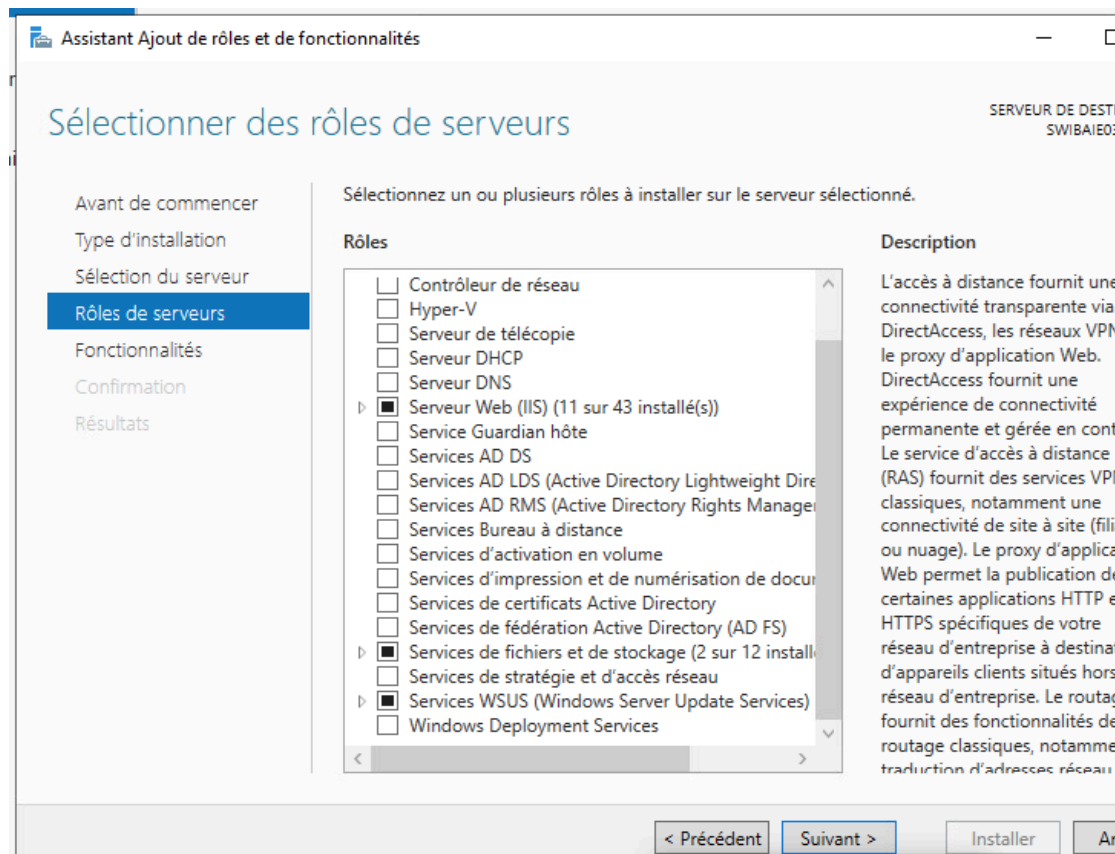


1. Ajout des rôles et fonctionnalités WSUS :

- Ouvrez le Gestionnaire de Serveur.
- Allez dans Ajouter des rôles et des fonctionnalités :

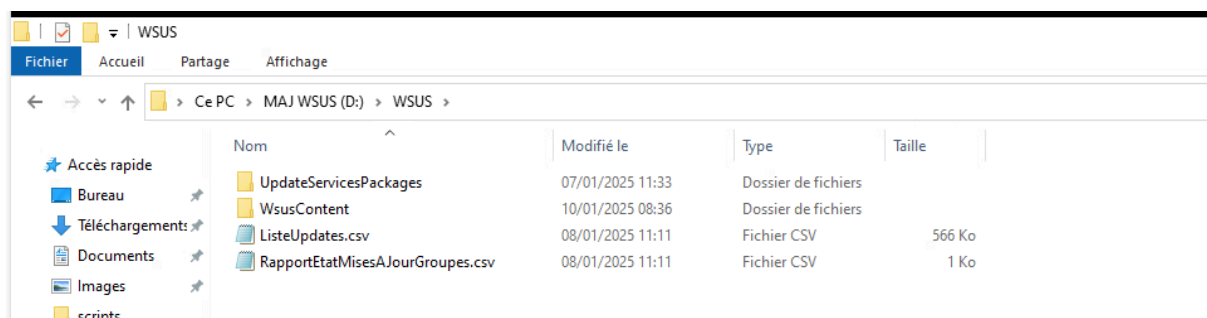


- - Sélectionnez Windows Server Update Services.



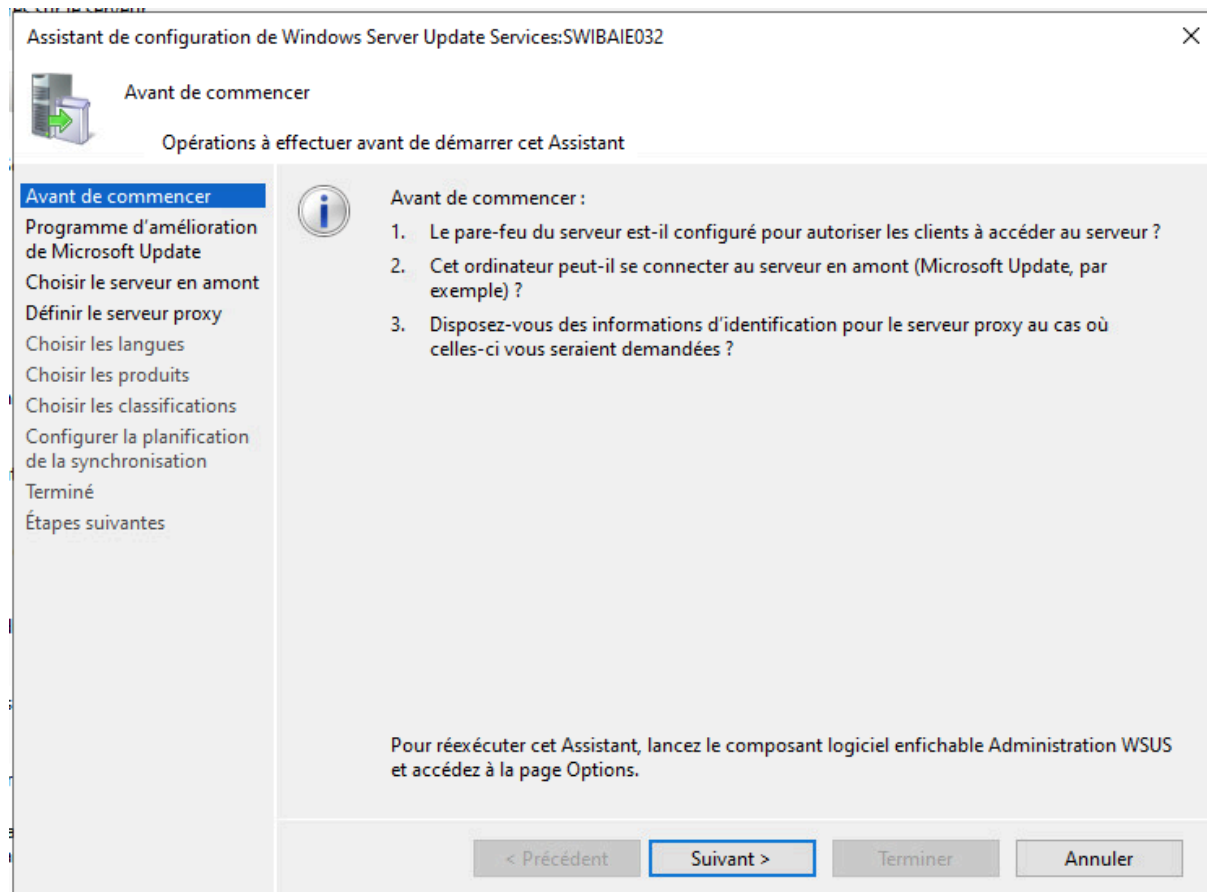
-
- Sélectionnez l'option pour stocker les mises à jour localement et indiquez D : \WSUS\.
- Installez les outils de gestion WSUS.

vérifier si des dossiers se sont créés dans le (D:)

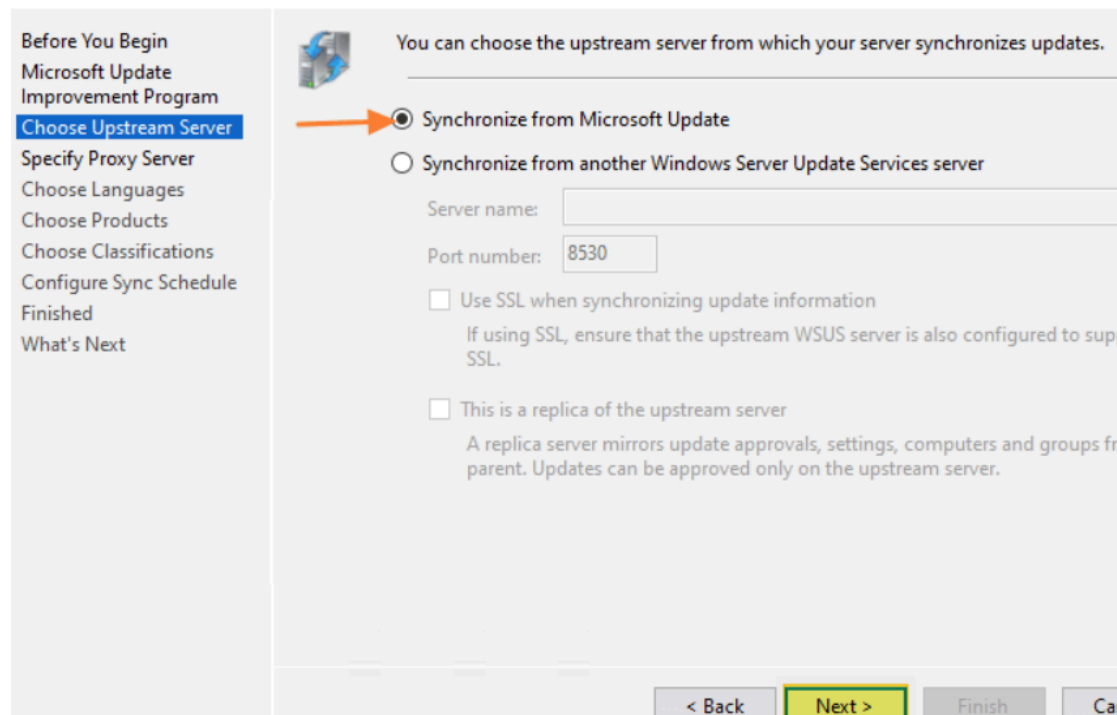


2. Configuration initiale de WSUS :

- Lancez la console WSUS.

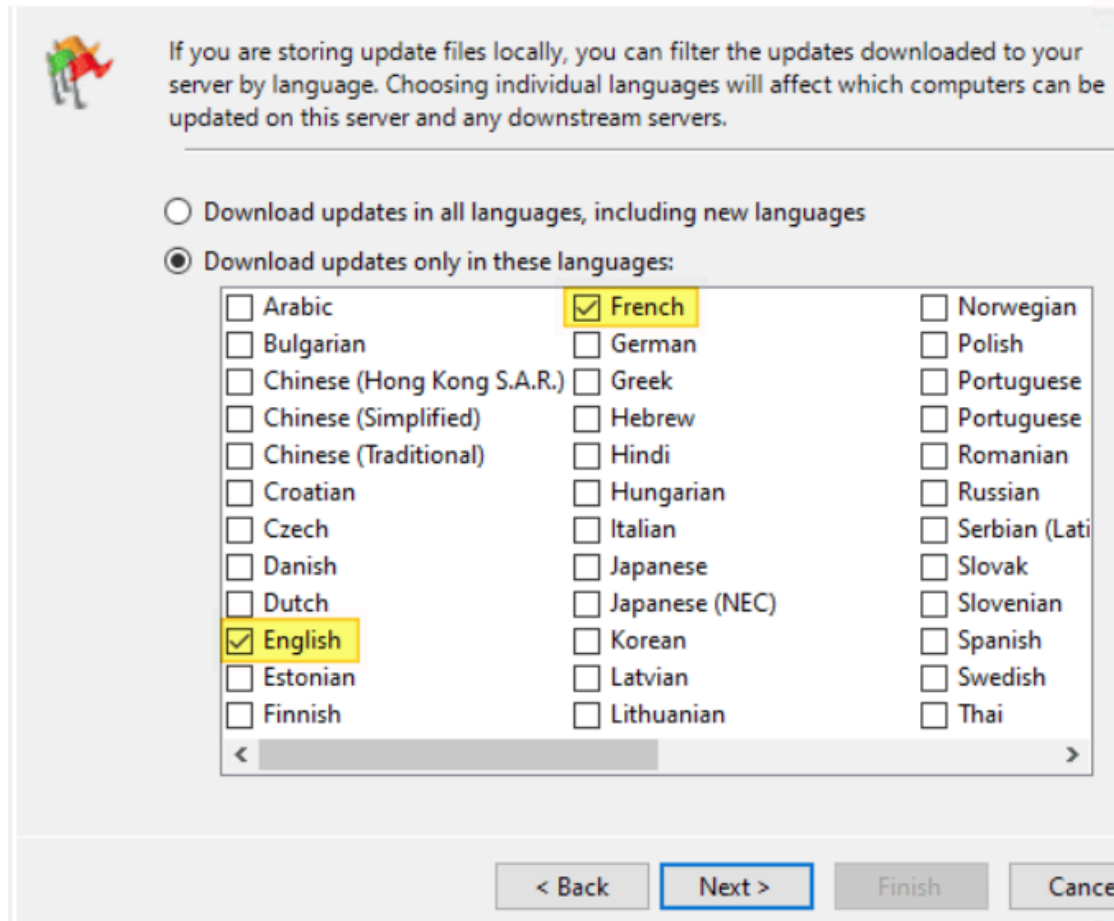


-
- Configurez les paramètres :
 - Source de synchronisation : Microsoft Update.



- Produits :
 - Windows Server 2012 et versions ultérieures.

- SQL Server (2012, 2017, 2019, 2022).
- Langues : Français et Anglais.



If you are storing update files locally, you can filter the updates downloaded to your server by language. Choosing individual languages will affect which computers can be updated on this server and any downstream servers.

☐ Download updates in all languages, including new languages
☒ Download updates only in these languages:

<input type="checkbox"/> Arabic	<input checked="" type="checkbox"/> French	<input type="checkbox"/> Norwegian
<input type="checkbox"/> Bulgarian	<input type="checkbox"/> German	<input type="checkbox"/> Polish
<input type="checkbox"/> Chinese (Hong Kong S.A.R.)	<input type="checkbox"/> Greek	<input type="checkbox"/> Portuguese
<input type="checkbox"/> Chinese (Simplified)	<input type="checkbox"/> Hebrew	<input type="checkbox"/> Portuguese
<input type="checkbox"/> Chinese (Traditional)	<input type="checkbox"/> Hindi	<input type="checkbox"/> Romanian
<input type="checkbox"/> Croatian	<input type="checkbox"/> Hungarian	<input type="checkbox"/> Russian
<input type="checkbox"/> Czech	<input type="checkbox"/> Italian	<input type="checkbox"/> Serbian (Latin)
<input type="checkbox"/> Danish	<input type="checkbox"/> Japanese	<input type="checkbox"/> Slovak
<input type="checkbox"/> Dutch	<input type="checkbox"/> Japanese (NEC)	<input type="checkbox"/> Slovenian
<input checked="" type="checkbox"/> English	<input type="checkbox"/> Korean	<input type="checkbox"/> Spanish
<input type="checkbox"/> Estonian	<input type="checkbox"/> Latvian	<input type="checkbox"/> Swedish
<input type="checkbox"/> Finnish	<input type="checkbox"/> Lithuanian	<input type="checkbox"/> Thai

< >

- Calendrier de synchronisation : Automatique, tous les jours.

1. Approbation manuelle des mises à jour :


- Désactivez l'approbation automatique dans les options WSUS en supprimant toute les règles

Approbations automatiques

×

Règles de mise à jour

Avancé



Vous pouvez définir des règles afin d'approuver automatiquement les nouvelles mises à jour au moment de leur synchronisation.

Nouvelle règle...

Modifier...

✕ Supprimer

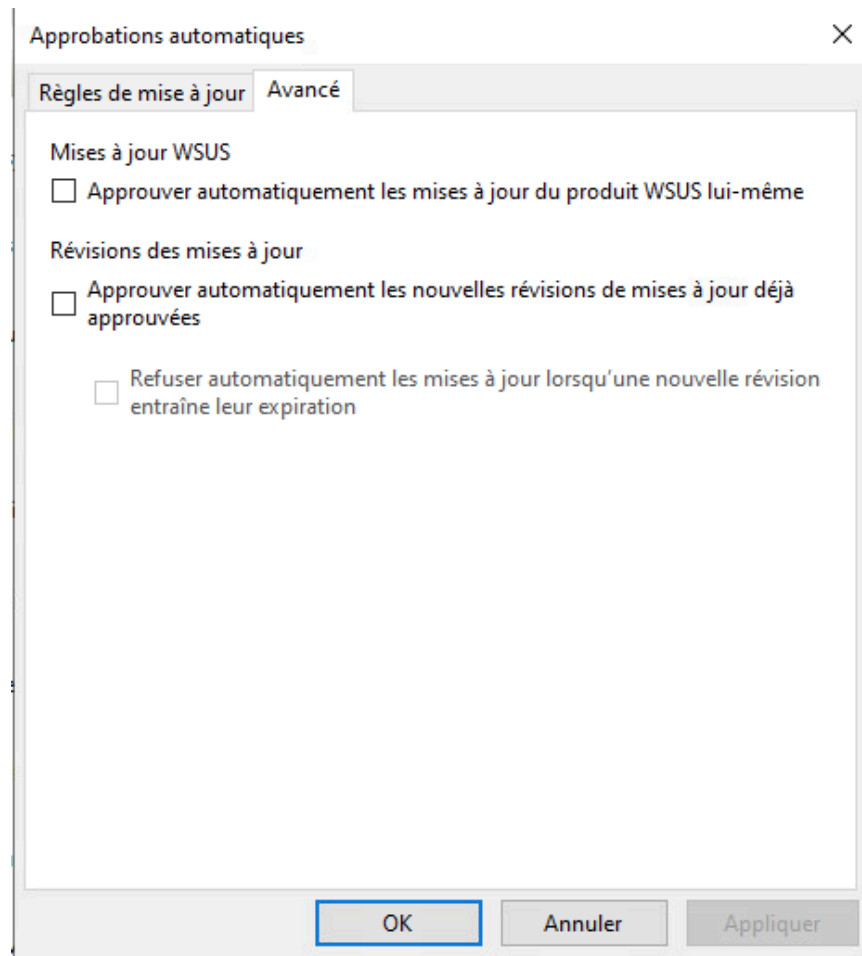
Exécuter la règle

Propriétés de règle (cliquez sur une valeur soulignée pour la modifier)

OK

Annuler

Appliquer



2. Planification de l'installation des mises à jour :

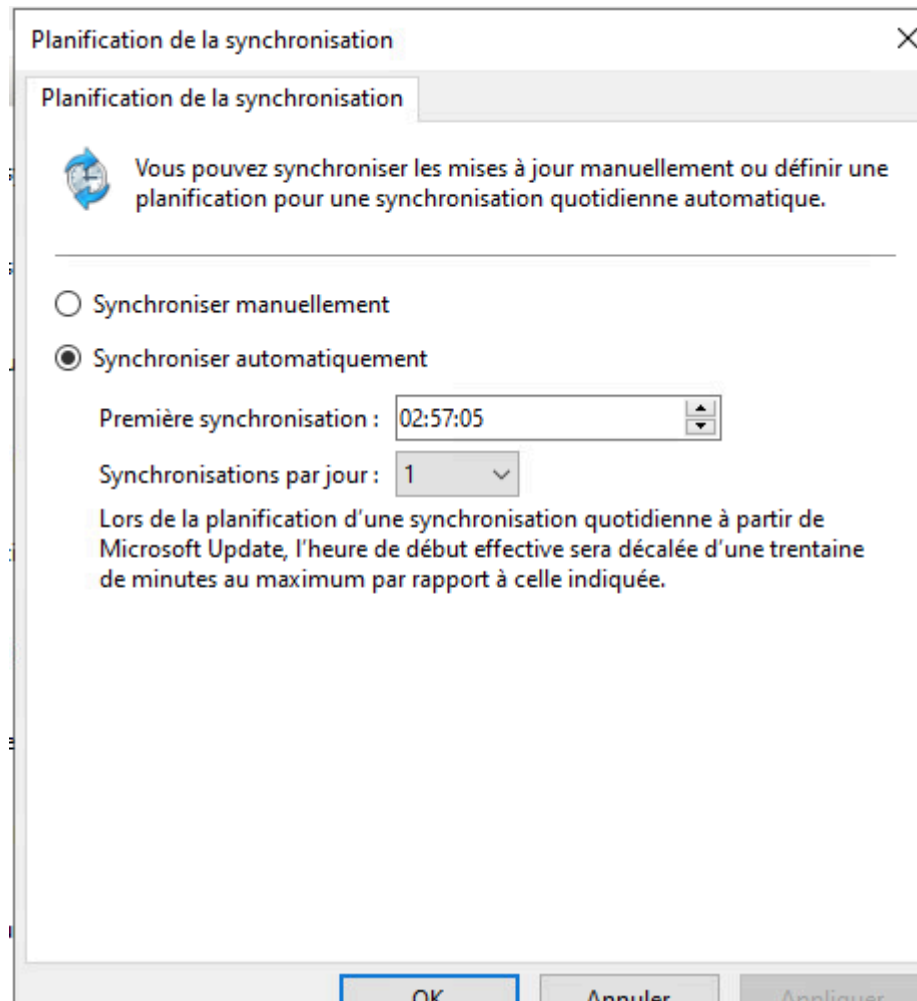
- Définissez la tâche d'installation le samedi.

3. Gestion des rapports :

- Configurez l'envoi de la liste des mises à jour le jeudi à 21h.
- Configurez l'état des mises à jour à envoyer le lundi à 7h.

(au final mon mettre de stage ma dit de pas membetter avec des script powershell mais cetait bien possible avec des script executer avec les

planification de tâche.)



Étape 5 : Configuration SMTP pour les notifications


1. Installation du rôle SMTP :

- Ajoutez le rôle SMTP via le Gestionnaire de Serveur.
- Configurez le serveur pour envoyer des emails :
 - Serveur SMTP : `smtp.entreprise.local` (serveur de mail de l'entreprise)
 - Port : 25.

2. Configuration dans WSUS :

Notifications par courrier électronique

Général Serveur de messagerie

 Windows Server Update Services peut envoyer des notifications par courrier électronique relatives aux nouvelles mises à jour et aux rapports d'état.

☒ Envoyer une notification par courrier électronique lorsque de nouvelles mises à jour sont synchronisées

Destinataires :

Remarque : séparez les adresses de messagerie des destinataires par des virgules.

☒ Envoyer les rapports d'état

Fréquence :

Envoyer les rapports :

Destinataires :

Remarque : séparez les adresses de messagerie des destinataires par des virgules.

Langue :

OK Annuler Appliquer

Notifications par courrier électronique

Général Serveur de messagerie

Informations sur le serveur

Serveur des courriers électroniques sortants (SMTP) :

Numéro du port :

Informations sur l'expéditeur

Nom de l'expéditeur :

Adresse de messagerie :

Informations d'ouverture de session

☐ Mon serveur SMTP nécessite une authentification

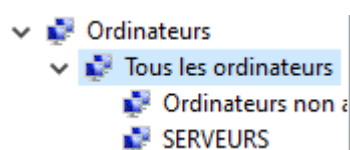
Nom d'utilisateur :

Mot de passe :

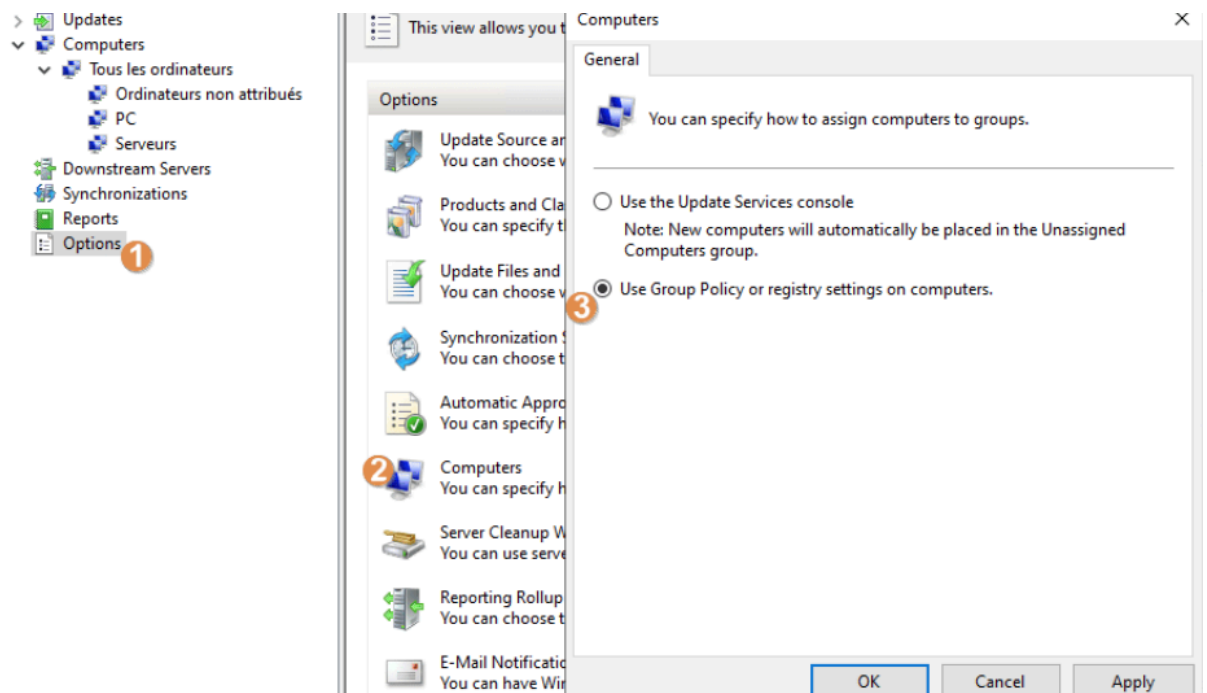
Tester

OK Annuler Appliquer

en parallèle créer les uo et une gpo pour que les machines soient dans wsus, on crée aussi un groupe d'ordinateurs dans wsus



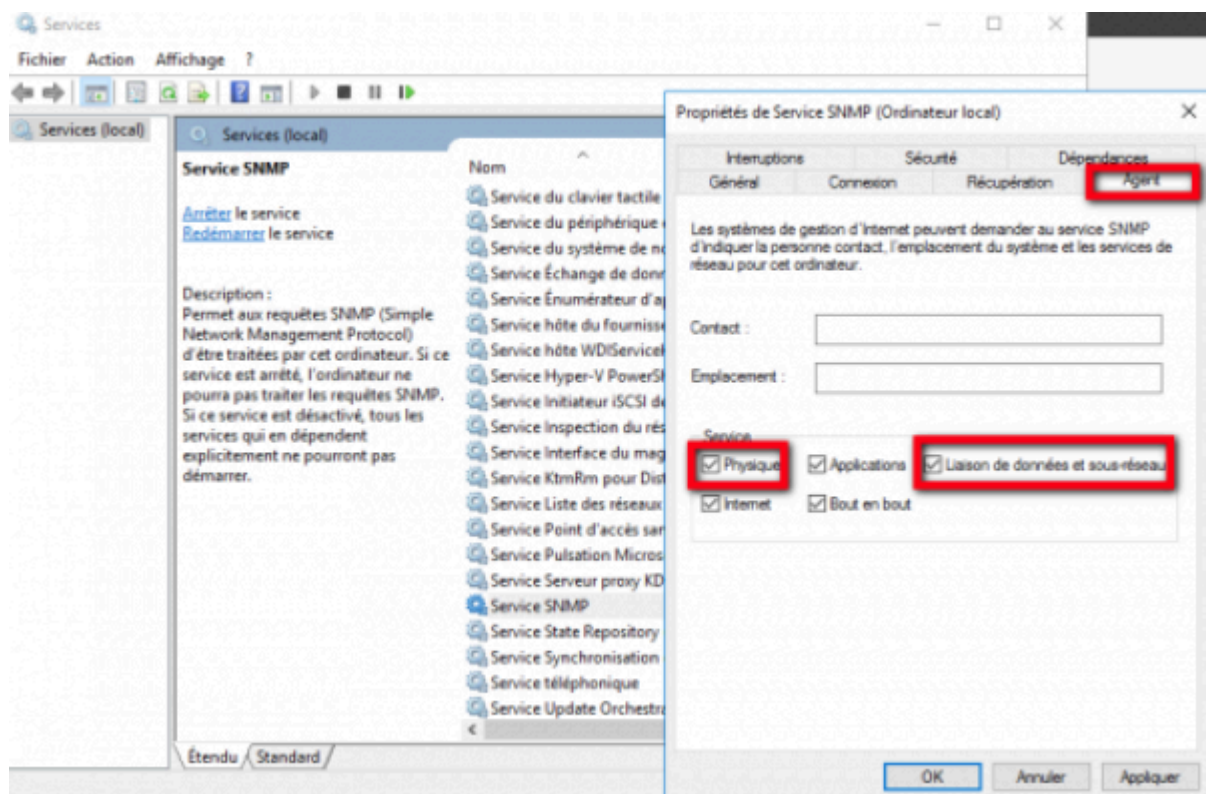
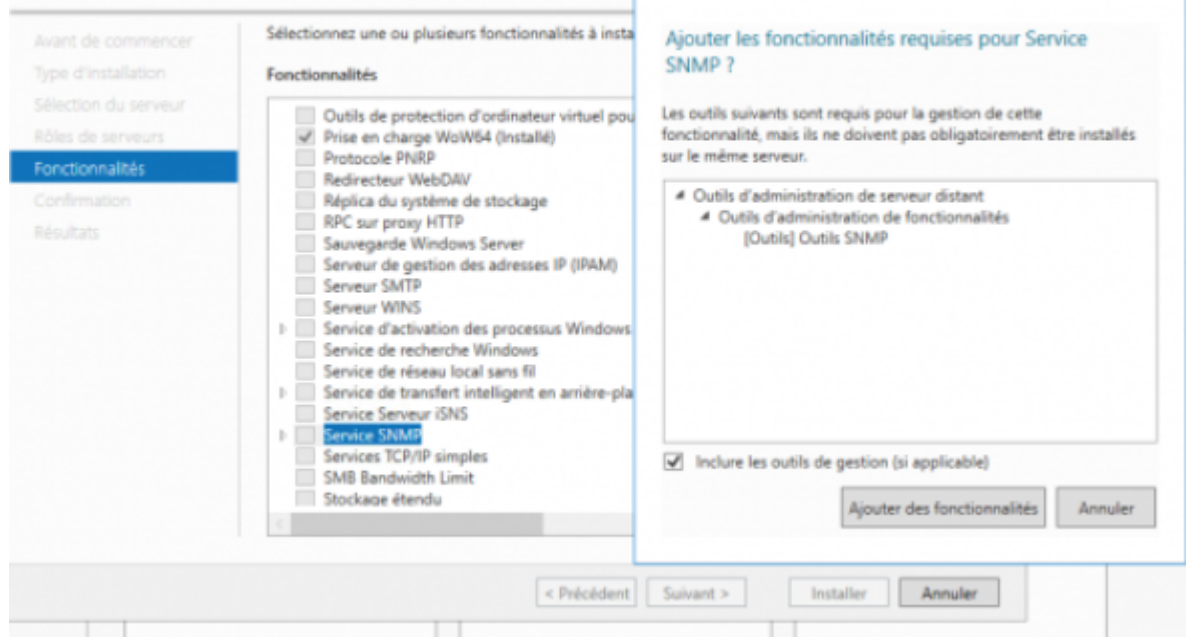
- Ouvrez la console WSUS
- Cliquez sur « Options » à gauche (1)
- Cliquez sur « Computers » / « Ordinateurs » à droite (2)
- Cochez l'option « Use Group Policy or registry settings on computers » / « Utiliser les paramètres de stratégie de groupe ou de Registre sur les ordinateurs » (3).
- Validez



3. Étape 6 : Intégration à la supervision POM

Installation de snmp client car c'est le protocole utiliser par POM pour requérir des information sur les machine

Sélectionner des fonctionnalités



- Vérifiez que la supervision affiche correctement l'état du serveur et des mises à jour.

Update Services

- SWIBAIE032
 - Mises à jour
 - Ordinateurs
 - Tous les ordinateurs
 - Ordinateurs non a
 - SERVEURS**
 - Serveurs en aval
 - Synchronisations
 - Rapports
 - Options

SERVEURS (44 ordinateurs sur 44 affichés, 45 au total)

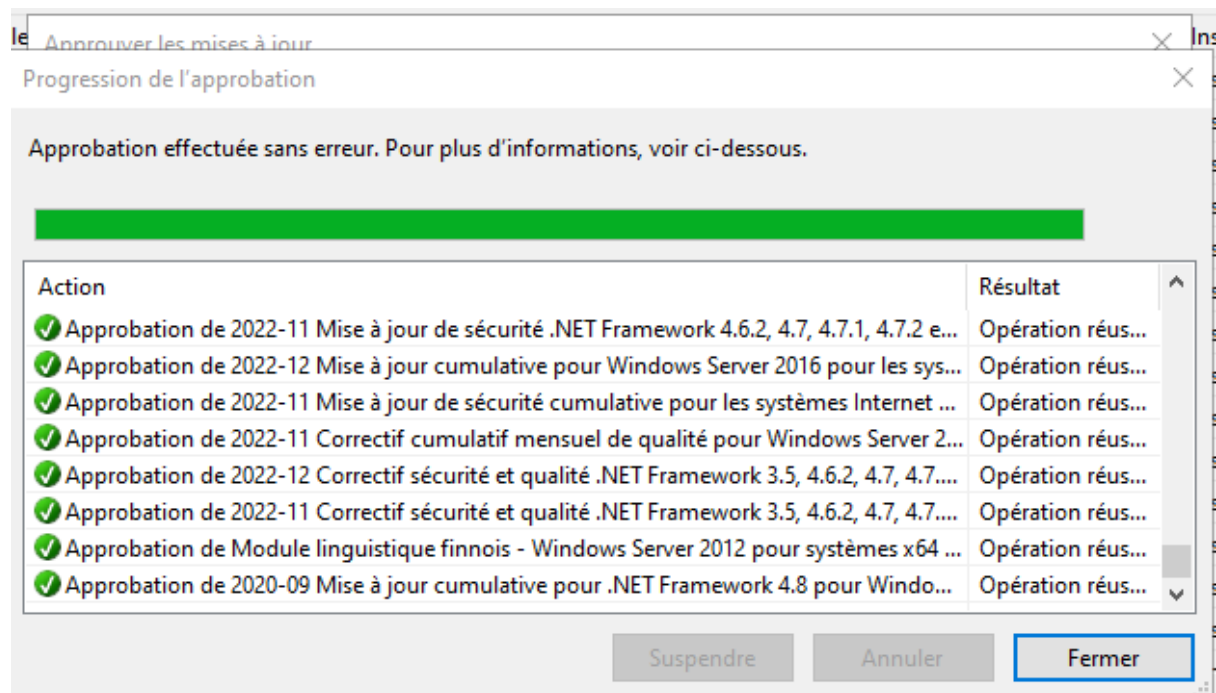
État : Toutes Actualiser

Nom
⚠ scaib61.caib.fr
⚠ scaib31.caib.fr
swibaie028.caib.fr
swibaie020.caib.fr
swibaie022.caib.fr
swibaie011.caib.fr
swibaie024.caib.fr
swibaie030.caib.fr
swibaie017.caib.fr
swibaie021.caib.fr
swibaie026.caib.fr
swibaie032.caib.fr
swibaie012.caib.fr
swibaie027.caib.fr
swibaie010.caib.fr
swibaie018.caib.fr
scaib29.caib.fr

J'ai configuré les machines pour pointer vers le serveur **SWIBAIE032**.

J'ai validé l'application de la GPO avec la commande :

```
gpupdate /force
```



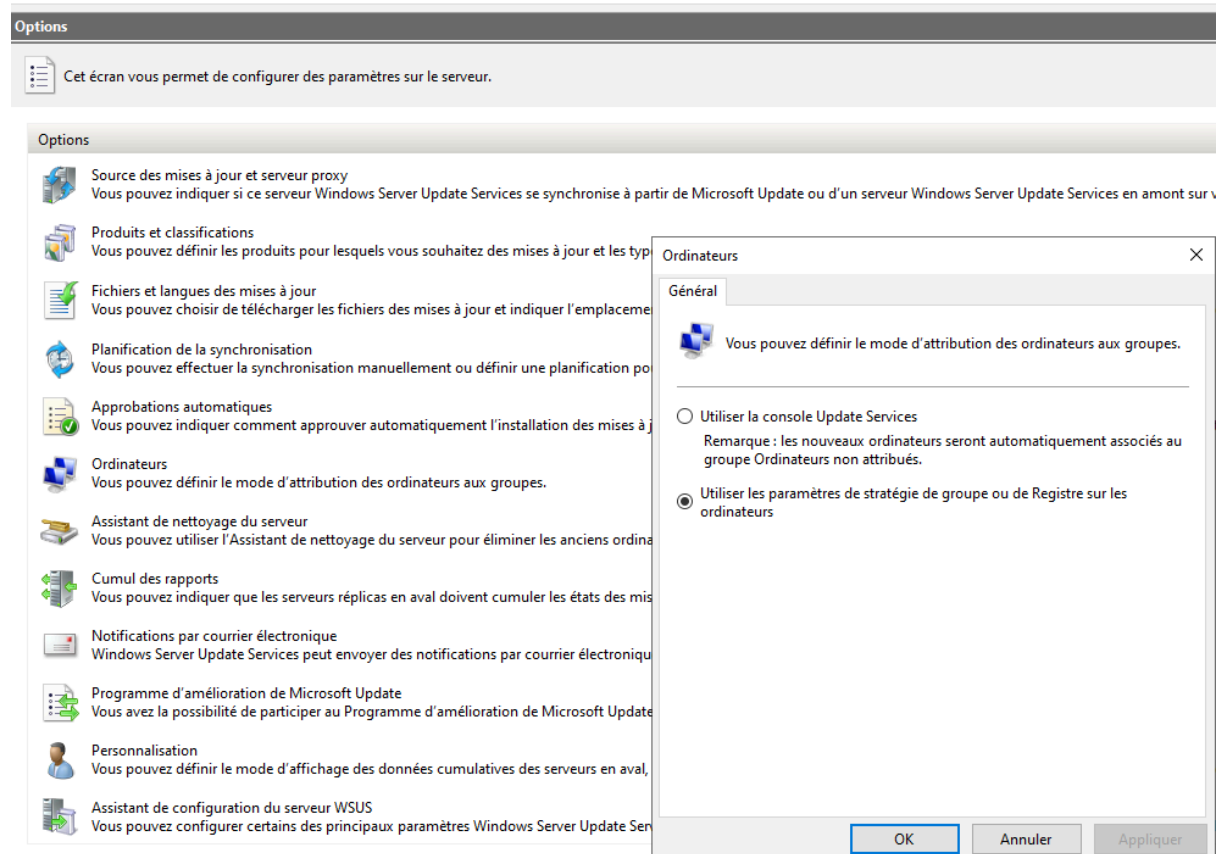
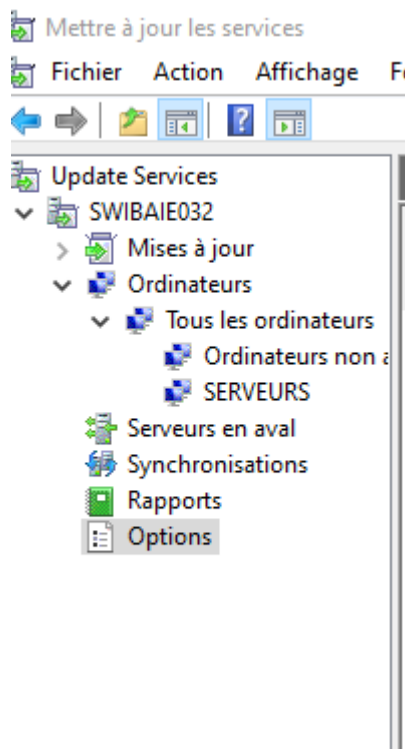
on approuve les mises a jours pour qu'elles se fond
Validation POM :

- Vérifiez la remontée dans la supervision POM :
 - Statut de la VM.
 - Espace disque.
 - Alertes WSUS.

Fin de la documentation.

Lier les machines du domaine au serveur WSUS

dans



Désormais, l'affectation sera effectuée selon la valeur définie par stratégie de groupe ou directement dans le Registre de la machine.

II. Créer des groupes d'ordinateurs dans WSUS

Pour indiquer aux machines qu'elles doivent se connecter à un serveur WSUS (plutôt qu'au serveur de Microsoft), nous devons créer une nouvelle stratégie de groupe. D'ailleurs, il y a divers paramètres de stratégies de groupe qui permettent de configurer la fonctionnalité « Windows Update » de Windows (*desktop et server*).

Nous verrons qu'il y a un paramètre pour spécifier l'emplacement du serveur WSUS, donc ce sera commun à toutes les machines, que ce soit des postes de travail ou des serveurs.

Il y a également un paramètre qui permet d'indiquer dans quel groupe du serveur WSUS la machine doit être intégrée (afin d'avoir une attribution automatique, comme je l'évoquais précédemment). Si l'on veut organiser le serveur WSUS en créant des groupes d'ordinateurs, par exemple un groupe « PC » et un groupe « Serveurs », il faut que l'on configure deux GPO pour appliquer des noms de groupe différents. Au total, cela fait 3 GPO à créer.

Lier les PC et les serveurs à WSUS par GPO

A. GPO WSUS pour les paramètres communs

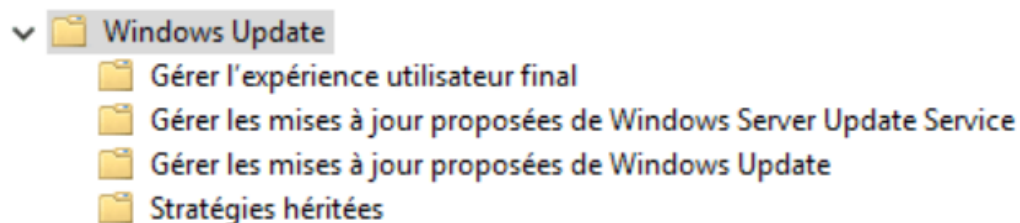
Sur votre contrôleur de domaine, ou à partir d'une machine équipée des outils d'administration, ouvrez la console de « Gestion de stratégie de groupe ».

Créez une nouvelle GPO liée sur la racine du domaine pour gérer l'intégralité des machines du domaine via le serveur WSUS. Pour ma part, je nomme la GPO « WSUS – Paramètres communs ».

Note : si vous souhaitez utiliser WSUS uniquement sur certaines machines, appliquez un filtrage de sécurité sur un groupe de sécurité spécifique ou liez la GPO uniquement sur certaines OUs.

Modifiez la GPO et parcourez les paramètres de cette façon :

Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update



Passons à la configuration des paramètres.

Tout d'abord, nous allons devoir définir l'adresse de notre serveur WSUS, à savoir « `http://srv-wsus.it-connect.local:8530` » (8530 étant le port par défaut lorsque le WSUS est accessible en http), dans le paramètre « Spécifier l'emplacement intranet du service de mise à jour Microsoft » (sous « *Gérer les mises à jour proposées de Windows Server Update Service* »). Dans un autre chapitre, nous verrons comment sécuriser la connexion via le protocole HTTPS.

Il faut commencer par activer ce paramètre (1), puis définir l'adresse du serveur WSUS comme emplacement pour la détection des mises à jour (2), mais aussi pour les statistiques (3). Les autres options peuvent être laissées par défaut.

Spécifier l'emplacement intranet du service de mise à jour Microsoft

Spécifier l'emplacement intranet du service de mise à jour Microsoft Paramètre précédent Paramètre suivant

☐ Non configuré
☒ **Activé** 1
☐ Désactivé

Commentaire :

Pris en charge sur : Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion de Windows RT

Options :

Configurer le service de Mise à jour pour la détection des mises à jour :

http://srv-wsus.it-connect.local:8530 2

Configurer le serveur intranet de statistiques : http://srv-wsus.it-connect.local:8530 3

Définir le serveur de téléchargement alternatif :

(exemple: https://IntranetUpd01)

☐ Téléchargez les fichiers sans URL dans les métadonnées si un serveur de téléchargement alternatif est défini.
☐ Ne pas appliquer l'épingle de certificat TLS du client Windows Update pour la détection mises à jour.

Sélectionnez le comportement du proxy pour le client Windows Update pour la détection des jour :

Utiliser uniquement le proxy système pour détecter les mises à jour (par défaut)

Aide :

Spécifie un serveur intranet qui héberge les mises à jour provenant de Microsoft Update. Vous pouvez ensuite utiliser ce service de mise à jour pour procéder à la mise à jour automatique des ordinateurs de votre réseau.

Ce paramètre vous permet de spécifier un serveur de votre réseau devant fonctionner comme un service de mise à jour interne. Le client Mises à jour automatiques recherchera dans ce service les mises à jour qui s'appliquent aux ordinateurs de votre réseau.

Pour utiliser ce paramètre, vous devez définir deux noms de serveur : celui à partir duquel le client Mises à jour automatiques détecte et télécharge les mises à jour, et celui vers lequel les postes de travail mis à jour chargent les statistiques. Vous pouvez également définir un seul serveur qui effectue les deux fonctions. Il vous est possible de spécifier un

OK Annuler Appliquer

Le second paramètre à configurer se nomme « Configuration du service Mises à jour automatique » (sous « *Gérer l'expérience utilisateur final* »). Il sert à agir sur le comportement des machines notamment pour télécharger et installer les mises à jour.

Il faut commencer par activer ce paramètre. Je vous laisse prendre connaissance de ma configuration ci-dessous puis des explications à la suite.

Configuration du service Mises à jour automatiques

Configuration du service Mises à jour automatiques Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :

☒ Activé

☐ Désactivé

Pris en charge sur : Windows XP Professionnel Service Pack 1 ou au minimum Windows 2000 Service Pack 3
Option 7 uniquement prise en charge sur les serveurs ou au moins édition Windows Server 2016

Options :

Configuration de la mise à jour automatique : 4 - Téléchargement automatique et planification des installations

Les paramètres suivants ne sont nécessaires et ne s'appliquent que si l'option 4 est sélectionnée.

☐ Installer durant la maintenance automatique

Jour de l'installation planifiée : 0 - Tous les jours

Heure de l'installation planifiée : 12:00

Si vous avez sélectionné « 4 – Téléchargement automatique et planification des installations » pour le jour de l'installation planifiée et que vous spécifiez une planification, vous pouvez également limiter l'exécution des mises à jour de manière hebdomadaire, bihebdomadaire ou mensuelle à l'aide des options ci-dessous :

☐ Chaque semaine

☐ Première semaine du mois

☐ Deuxième semaine du mois

☒ Troisième semaine du mois

☒ Quatrième semaine du mois

☒ Installer les mises à jour d'autres produits Microsoft

L'option « Configuration de la mise à jour automatique » est déterminée sur « 4 – Téléchargement automatique et planification des installations » afin que Windows Update télécharge et installe régulièrement les mises à jour, quand elles sont approuvées en amont sur le serveur WSUS.

Par défaut, Windows recherche les mises à jour toutes les 22 heures environ. Là, on précise que les mises à jour seront téléchargées (sur le WSUS, donc) et installées à 12:00 tous les jours. Néanmoins, on n'installe pas les mises à jour toutes les semaines : seulement en troisième et quatrième semaine du mois.

Un troisième paramètre est à configurer afin d'empêcher les machines de se connecter sur les serveurs Microsoft Update pour appliquer des mises à jour.

Il s'agit du paramètre « Ne pas se connecter à des emplacements Internet Windows Update » (sous « *Gérer les mises à jour proposées de Windows Server Update Service* ») et il suffit de l'activer.

Ne pas se connecter à des emplacements Internet Windows Update

Paramètre précédent Paramètre suivant

☐ Non configuré ☒ **Activé** ☐ Désactivé

Commentaire :

Pris en charge sur : Au minimum Windows Server 2012 R2, Windows 8.1 ou Windows RT 8.1

Options :

Aide :

Même quand Windows Update est configuré pour recevoir des mises à jour à partir d'un service de mise à jour intranet, il extrait régulièrement des informations du service Windows Update public afin d'activer les connexions ultérieures à Windows Update et à d'autres services tels que Microsoft Update ou le Windows Store.

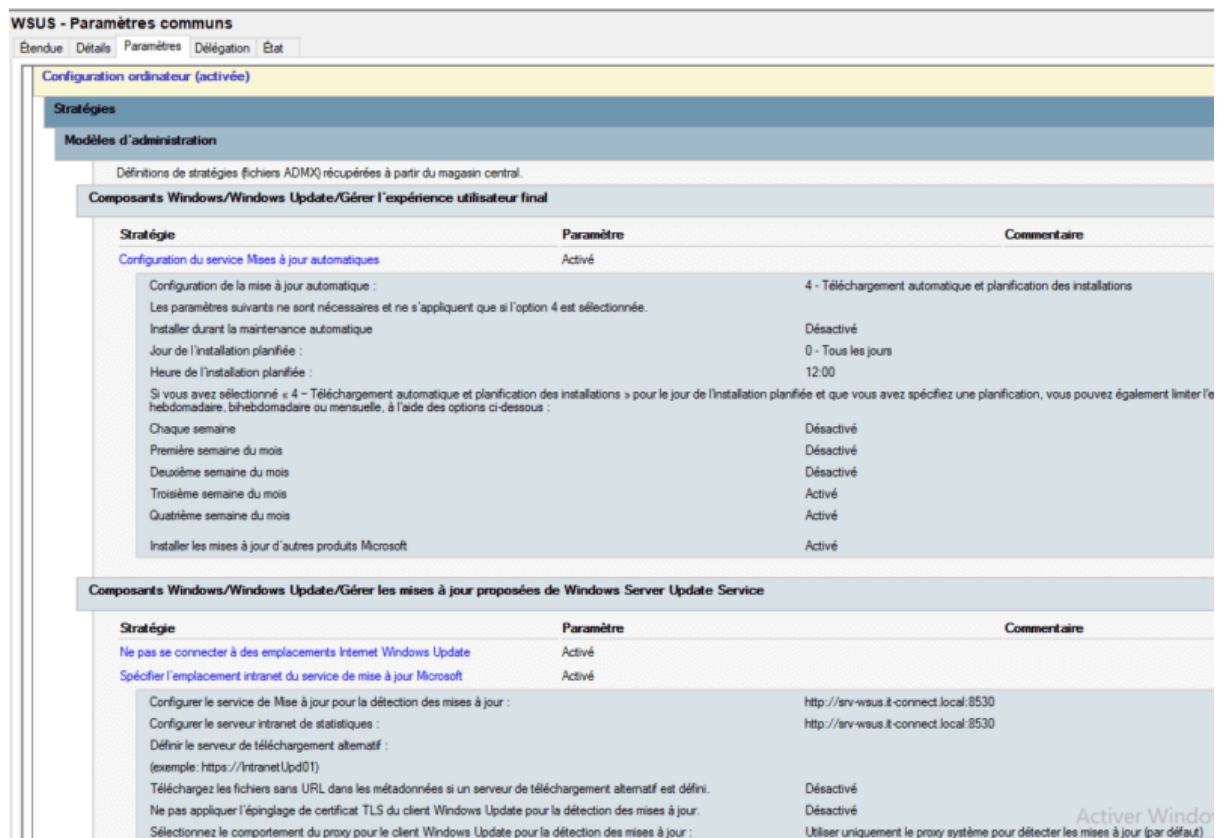
L'activation de cette stratégie désactive cette fonctionnalité et peut provoquer le non-fonctionnement de la connexion à des services publics tels que le Windows Store.

Remarque : cette stratégie s'applique uniquement quand ce PC est configuré pour se connecter à un service de mise à jour intranet à l'aide de la stratégie « Spécifier l'emplacement intranet du service de Mise à jour Microsoft ».

OK Annuler Appliquer

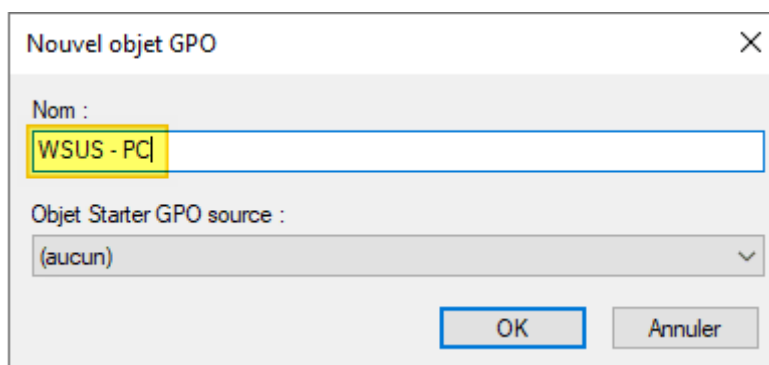
Validez, cette première GPO est prête !

Pour terminer, voici un résumé de la configuration de cette stratégie de groupe :



B. GPO WSUS spécifique aux postes de travail

Créez une nouvelle stratégie de groupe nommée « WSUS – PC » et liez cette GPO à l'unité d'organisation qui contient vos postes de travail. Au sein de mon annuaire, il s'agit de l'OU « PC ».



Cette stratégie va servir à déterminer deux paramètres pour :

- Indiquer le nom du groupe WSUS dans lequel doivent aller les postes de travail

- Indiquer la plage horaire correspondante aux heures d'activité

Les paramètres se situent au même endroit, à savoir :

Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update

Commencez par configurer le paramètre « Autoriser le ciblage côté client » (sous « *Gérer les mises à jour proposées de Windows Server Update Service* »). Pour cela, activez le paramètre et pour l'option « Nom du groupe cible de cet ordinateur », indiquez « PC », car je vous rappelle que c'est le nom du groupe créé sur le serveur WSUS.

Ce qui donne :

Gérer les mises à jour proposées de Windows Server Update Service

Autoriser le ciblage côté client

Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :
☒ **Activé**
☐ Désactivé

Pris en charge sur : Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion de Windows RT

Options : Aide :

Nom du groupe cible de cet ordinateur

PC

Indique le ou les noms de groupe cible à utiliser pour recevoir les mises à jour à partir d'un service intranet de Mise à jour Microsoft.

Si l'état Activé est sélectionné, les informations sur le groupe cible spécifié seront envoyées au service intranet de Mise à jour Microsoft qui les utilisera pour déterminer les mises à jour à déployer sur cet ordinateur.

Si le service intranet de Mise à jour Microsoft prend en charge plusieurs groupes cibles, cette stratégie peut définir plusieurs noms de groupes en les séparant à l'aide de points-virgules. Dans le cas contraire, un seul groupe doit être indiqué.


Si l'état Désactivé ou Non configuré est sélectionné, aucune information de groupe cible ne sera envoyée au service intranet de Mise à jour Microsoft.

Remarque : cette stratégie ne s'applique que lorsque le service intranet de Mise à jour Microsoft sur lequel cet ordinateur est dirigé est configuré pour prendre en charge le ciblage côté client.

OK Annuler Appliquer

Dans cette GPO, nous allons configurer un deuxième paramètre nommé « Désactiver le redémarrage automatique pour les mises à jour pendant les heures d'activité » (sous « *Gérer l'expérience utilisateur final* ») dans le but d'éviter les redémarrages intempestifs en pleine production !

Par exemple, voici la configuration à appliquer pour définir une plage horaire de 07h00 à 19h00 sur les postes de travail :

 Désactiver le redémarrage automatique pour les mises à jour pendant les heures d'activité

☐ Non configuré Commentaire :

☒ **Activé**

☐ Désactivé

Pris en charge sur :

Options : Aide :

Heures d'activité

Début :

Fin :

Si vous activez cette stratégie, le PC ne redémarrera pas automatiquement après les mises à jour pendant les heures d'activité. Il tentera de redémarrer en dehors des heures d'activité.

Notez que la prise en compte de certaines mises à jour nécessite le redémarrage du PC.

Si vous désactivez cette stratégie ou ne la configurez pas et que vous n'avez défini aucune autre stratégie de groupe de redémarrage, les heures d'activité sélectionnées par l'utilisateur sont appliquées.

Cette stratégie n'a aucun effet si l'une ou l'autre des stratégies suivantes est activée :

1. Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées de mises à jour automatiques.
2. Toujours redémarrer automatiquement à l'heure planifiée.

Remarque : la plage horaire des heures d'activité peut représenter au maximum un total de 18 heures.

La stratégie de groupe propre aux ordinateurs est prête, voici un résumé :

WSUS – PC

Données recueillies le : 25/03/2022 15:17:13

Général	
Détails	
Liaisons	
Filtrage de sécurité	
Délégation	
Configuration ordinateur (activée)	
Stratégies	
Modèles d'administration	
Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.	
Composants Windows/Windows Update/Gérer l'expérience utilisateur final	
Stratégie	Paramètre
Désactiver le redémarrage automatique pour les mises à jour pendant les heures d'activité	Activé
Heures d'activité	
Début :	7 h 00
Fin :	19 h 00
Composants Windows/Windows Update/Gérer les mises à jour proposées de Windows Server Update Service	
Stratégie	Paramètre
Autoriser le ciblage côté client	Activé
Nom du groupe cible de cet ordinateur	PC

Passons à la stratégie de groupe propre aux serveurs.

C. GPO WSUS spécifique aux serveurs

Créez une nouvelle stratégie de groupe nommée « WSUS – Serveurs » et liez cette GPO à l'unité d'organisation qui contient vos serveurs, ainsi qu'à l'OU « *Domain Controllers* » pour cibler les contrôleurs de domaine. Au sein de mon annuaire, il s'agit de l'OU « *Serveurs* ».

Cette stratégie va servir à déterminer deux paramètres pour :

- Indiquer le nom du groupe WSUS dans lequel doivent aller les serveurs
- Indiquer la plage horaire correspondante aux heures de production

Le processus de création de cette stratégie de groupe est similaire à celle des postes de travail, alors je passe directement à la synthèse :

WSUS - Serveurs	
Données recueillies le : 25/03/2022 15:15:48	
Général	
Détails	
Liaisons	
Filtrage de sécurité	
Délégation	
Configuration ordinateur (activée)	
Stratégies	
Modèles d'administration	
Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.	
Composants Windows/Windows Update/Gérer l'expérience utilisateur final	
Stratégie	Paramètre
Désactiver le redémarrage automatique pour les mises à jour pendant les heures d'activité	Activé
Heures d'activité	
Début :	5 h 00
Fin :	23 h 00
Composants Windows/Windows Update/Gérer les mises à jour proposées de Windows Server Update Service	
Stratégie	Paramètre
Autoriser le ciblage côté client	Activé
Nom du groupe cible de cet ordinateur	
Serveurs	
Configuration utilisateur (désactivée)	

Pour les serveurs, on définit une plage horaire beaucoup plus large pour les heures d'activités : de 05h00 à 23h00.

