
Installation WSUS

Un serveur WSUS permet de gérer les MAJ windows desktop et server, windows update qui est installé sur chaque machine contacte un server WSUS pour effectuer les dernières MAJ.

Avec un WSUS on peut valider ou non une MAJ quand est ce qu'elle a lieu etc.

Installation :

Dans rôle on installe rôle WSUS

On fait ajouter fonctionnalité (il necessite un serveur web IIS)

Partie stockage des données car il ce base sur BDD, WID (dans windows directement pas besoin d'installer autre chose)

Donc on installe avec WID

Ensuite on définit ou on veut stocker nos MAJ etc il est mieux d'avoir une partition appeler (W)

Ensuite partie web car les clients ce connecte au serveur WSUS via une connection http, on garde oarametre par default

Ensuite on installe

Lancer les taches de postainstallation

On démarre la console WSUS (Services WSUS)

Ensuite on effectue la configuration de base

Next

Ensuite on nous demande si on veut synchroniser les MAJ a partir de Microsoft Update ou un autre serveur WSUS

On selectionne Windows Update

Ensuite on peut définir un proxy

Ensuite start connecting pour connexion aux serveurs microsoft

Ensuite on choisi les langues pour les MAJ

Ensuite on choisit les produits pour lesquelles on veut récupérer les MAJ

Ensuite on peut choisir les mises à jour précise

Ensuite on indique quand est ce qu on veut synchroniser WSUS

On peut dire tout les jours à 1h00

Après on dit qu'on veut faire une synchronisation initial

Après on est sur la console WSUS

Quand on se positionne sur le nom du serveur on aura un tableau de bord

Le menu update permet de voir toutes les MAJ synchro sur le srv

Ensuite on a partie ordinateur on pourra créer différents groupes et valider une maj pour un groupe et pas l'autre

Menu options qui a beaucoup de sous-menus

On peut définir source d'installation, on peut faire une règle approbation automatique pour les MAJ critiques

Intégration des machines :

Il faut configurer le serveur WSUS pour gérer les groupes WSUS via une gpo, aller dans option > Computers on choisit la deuxième utiliser stratégie de groupe ou paramètre de registre

On va créer deux groupes : PC,server

Sur le contrôleur de domaine créer une gpo

Télécharger ADMX de vidéo et copier coller contenu dans
\\SYSVOL\domain\Policies\PolicyDefinitions

On crée trois GPO :

WSUS Paramètre commun : Adresse du serveur WSUS

WSUS PC :

WSUS Serveurs

Paramètre commun : On va dans configuration ordinateur > Stratégie > Modèle d'administration > Composant d'administration > Windows update > Gérer mise à jour proposer par WSUS > Spécifier emplacement intranet du service de mise à jour Microsoft

On met l'adresse web : <http://srvWSUS.info:8530>

On met même adresse pour intranet statistique

Toujours dans la même GPO on retourne dans Windows update > Gérer l'expérience utilisateur final > Configuration du service mise à jour automatique > Activé

Ensuite mettre téléchargement automatique et planification des installations ensuite on choisit tout les jours à 12h ou 13h

Ensuite on retourne encore une fois dans Windows update > Ne pas se connecter à des emplacements Internet Windows Update on fait activé

GPO PC :

Config PC > Strategie > Modele d'administration > Gerer les mises à jour proposée de WSUS > Autoriser le ciblage coté client > Ensuite donner nom du groupe > Mettre nom du groupe

Gérer experience utilisateur final > Désactiver redémarrage automatique pour MAJ > Activé > 8H à 18h

GPO serveur :

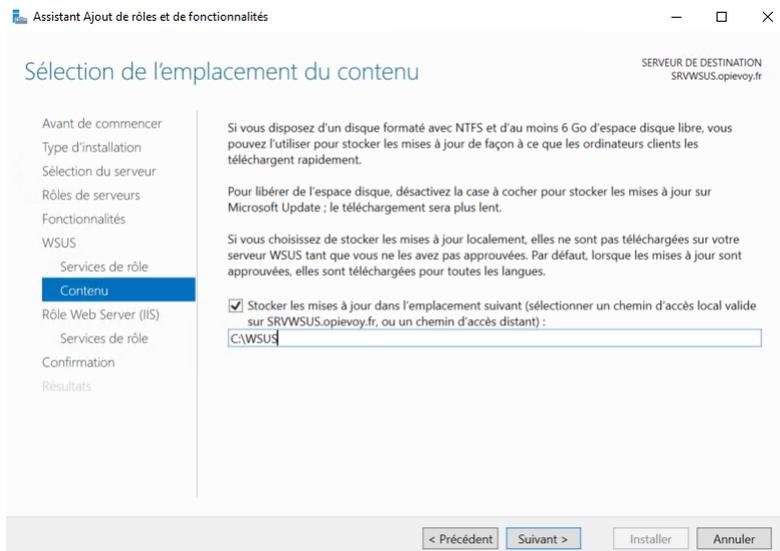
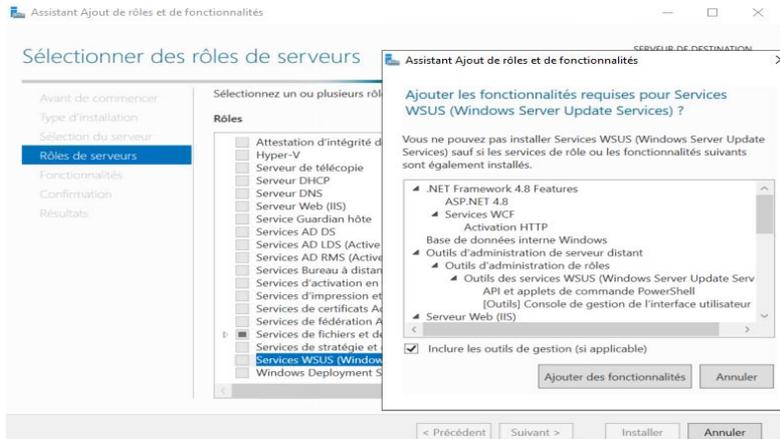
Config PC > Strategie > Modele d'administration > Gerer les mises à jour proposée de WSUS > Autoriser le ciblage coté client > Ensuite donner nom du groupe > Mettre nom du groupe

Gérer experience utilisateur final > Désactiver redémarrage automatique pour MAJ > Activé > 8H à 20h

Lié la GPO à l'OU

Sur pc client : gpudpate /force

Installation :



Meilleur résultat



Services **WSUS** (Windows Server Update Services)

Application

Assistant de configuration de Windows Server Update Services:SRVWSUS

Choisir le serveur en amont

Indiquez le serveur en amont à partir duquel le contenu doit être synchronisé

Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Étapes suivantes

Vous pouvez choisir le serveur en amont à partir duquel votre serveur doit synchroniser les mises à jour.

Synchroniser à partir de Microsoft Update

Synchroniser à partir d'un autre serveur Windows Server Update Services

Nom du serveur :

Numéro du port :

Utiliser SSL pour la synchronisation des informations de mise à jour
Si vous utilisez le protocole SSL, vérifiez que le serveur WSUS en amont est également configuré pour prendre en charge ce protocole.

Il s'agit d'un réplica du serveur en amont
Les serveurs réplicas reflètent les approbations de mises à jour, les paramètres, les ordinateurs et les groupes associés à leurs parents. Les mises à jour peuvent être approuvées uniquement sur le serveur en amont.

< Précédent Suivant > Terminer Annuler

Assistant de configuration de Windows Server Update Services:SRVWSUS

Se connecter au serveur en amont

Téléchargez les informations de mise à jour à partir de Microsoft Update

Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Étapes suivantes

Pour configurer Windows Server Update Services sur les écrans suivants, nous devons appliquer vos paramètres de serveur en amont et de serveur proxy, et synchroniser les informations relatives aux mises à jour disponibles.

Les informations à télécharger comprennent :

- les types de mises à jour disponibles ;
- les produits qui peuvent être mis à jour ;
- les langues disponibles.

Cliquez sur Démarrer la connexion pour enregistrer et télécharger les informations relatives au serveur en amont et au serveur proxy. Ce processus peut prendre plusieurs minutes selon la vitesse de votre connexion.

Démarrer la connexion Arrêter la connexion

< Précédent Suivant > Terminer Annuler



Choisir les produits

Sélectionnez les produits Microsoft à mettre à jour

Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Étapes suivantes

Vous pouvez indiquer les produits pour lesquels vous souhaitez des mises à jour.

Produits :

- Tous les produits
 - Microsoft
 - Active Directory
 - Services AD RMS (Active Directory Rights Management Services) Client 2.
 - AKS-EE
 - AksEdge Category
 - Antigen
 - Antigen for Exchange/SMTP
 - ASP.NET Web and Data Frameworks
 - ASP.NET Web Frameworks
 - Azure Connected Machine Agent
 - Azure Connected Machine Agent 3
 - Azure File Sync

Tous les produits, y compris ceux ajoutés ultérieurement.

< Précédent **Suivant >** Terminer Annuler



Terminé

Configuration initiale de votre serveur terminée

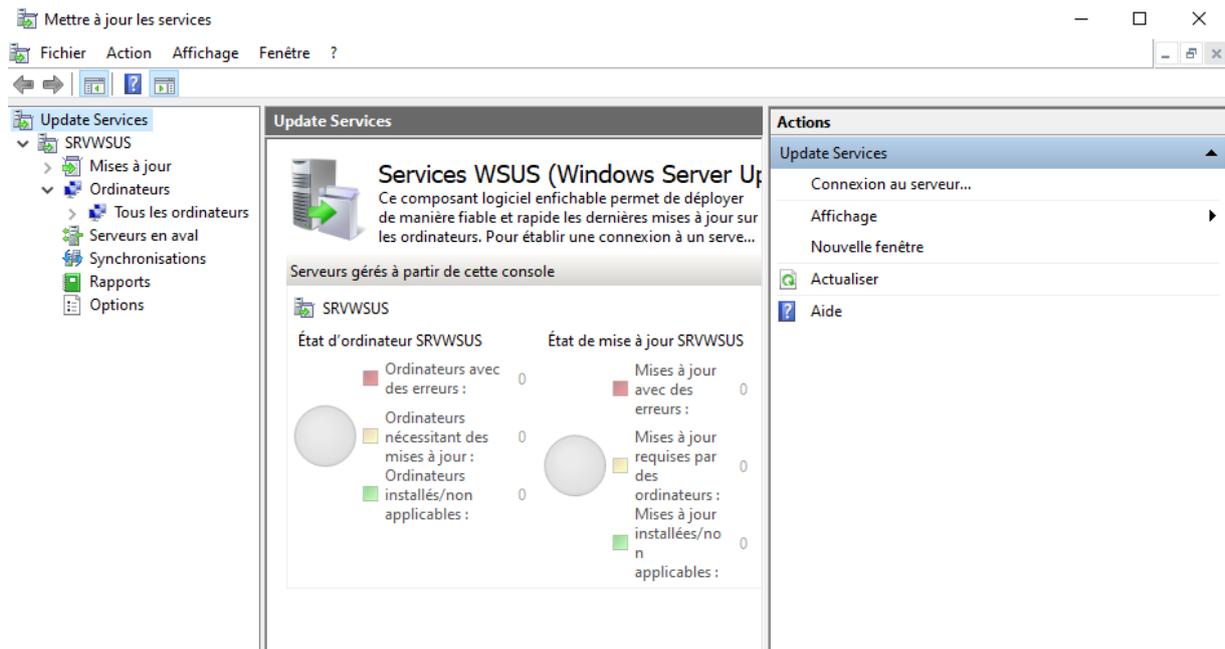
Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Étapes suivantes

 Vous avez terminé la configuration de votre serveur WSUS. Vous pouvez à présent lancer la console d'administration WSUS ou démarrer la synchronisation initiale.

Lancer la console d'administration Windows Server Update Services
Commencez à administrer votre organisation en lançant la console d'administration Windows Server Update Services.

Commencer la synchronisation initiale
La synchronisation initiale avec Microsoft Update ou votre serveur en amont peut prendre du temps. La durée de l'opération dépend du nombre de produits, de classifications des mises à jour et de langues sélectionnées, ainsi que de la vitesse de votre connexion Internet.

< Précédent **Suivant >** Terminer Annuler



Avant de définir les GPO on va demander au serveur WSUS de prendre en compte les GPO et paramètres des PC.

Pour que lorsqu'un nouveau PC se connecte au serveur il ne soit pas directement dans ordinateur non attribués mais dans un groupe.

Pour utiliser ce mode de fonctionnement :

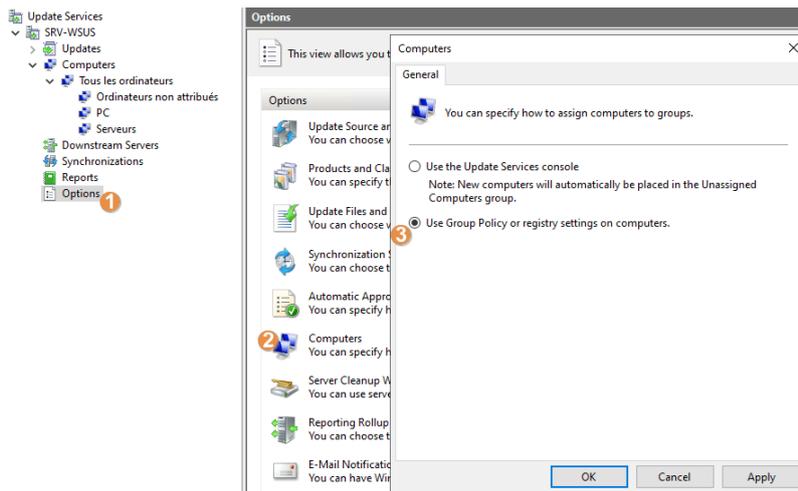
Ouvrez la console WSUS

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).

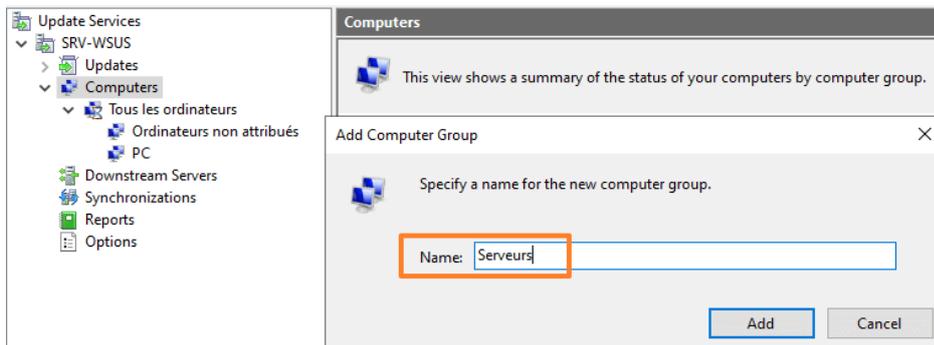
Validez



Création de la gpo commune :

On va créer deux groupes un groupe PC et un autre Serveur.

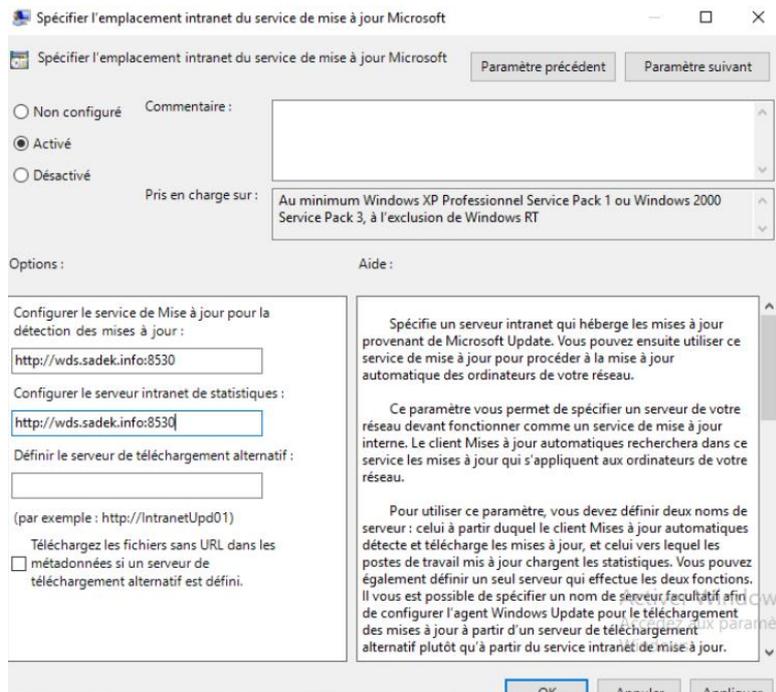
Ouvrez la console « WSUS », effectuez un clic droit sur « Tous les ordinateurs » puis cliquez sur « Add Computer Group ». Nommez ce premier groupe « PC » puis recommencez pour le second groupe.



Pour la gpo commune

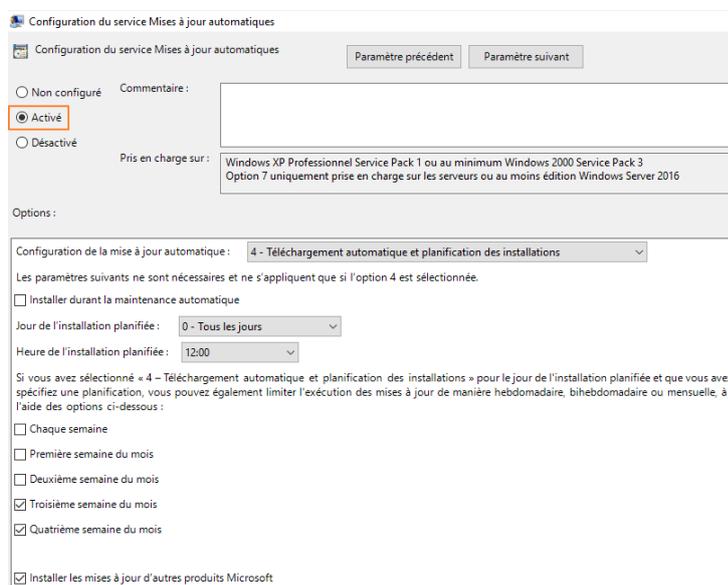
Je vais ici Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update

Ensuite je commence par définir l'ip du serveur wsus et le port qui est 8530 par défaut



Mon WSUS est sur mon WDS

Ensuite



'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.

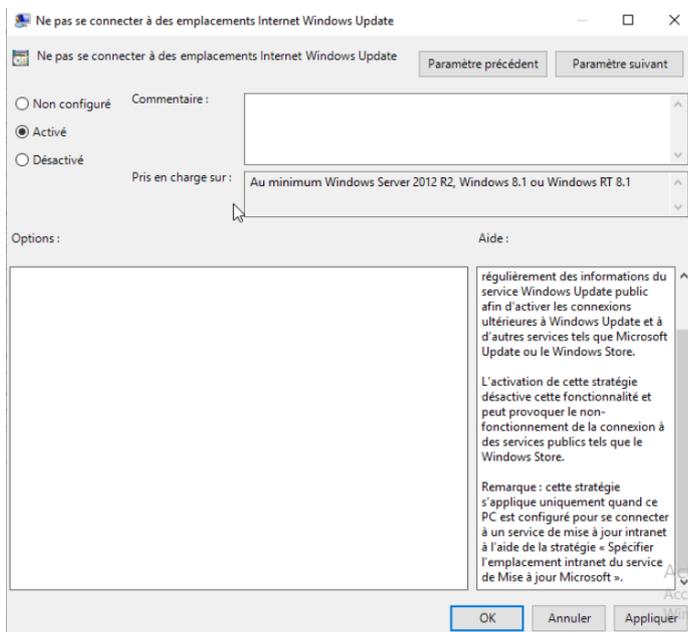
Pourquoi ? Je vous rappelle que Microsoft publie ses mises à jour le second mardi de chaque mois, donc si l'on installe les mises à jour en fin de mois, cela permet de récupérer les dernières mises à jour.

Autrement dit, sur la deuxième partie du mois, les machines chercheront à installer les nouvelles mises à jour disponibles.

Note : Ici, nous sommes sur la configuration des paramètres communs, donc aussi bien ordinateurs que serveurs. Si vous souhaitez définir des horaires différentes, il vaut mieux configurer ce paramètre de GPO dans deux stratégies distinctes.

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.



C'est bon pour la gpo commune

Un petit résumer ici.

Composants Windows/Windows Update			masquer
Stratégie	Paramètre	Commentaire	
Configuration du service Mises à jour automatiques	Activé		
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	Désactivé		
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 avez spécifié 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	Désactivé		
Première semaine du mois	Désactivé		
Deuxième semaine du mois	Désactivé		
Troisième semaine du mois	Activé		
Quatrième semaine du mois	Activé		
Installer les mises à jour d'autres produits Microsoft	Activé		
Stratégie	Paramètre	Commentaire	
Ne pas se connecter à des emplacements Internet Windows Update	Activé		
Spécifier l'emplacement intranet du service de mise à jour Microsoft	Activé		
Configurer le service de Mise à jour pour la détection des mises à jour :	http://wds.sadek.info:8530		
Configurer le serveur intranet de statistiques :	http://wds.sadek.info:8530		
Définir le serveur de téléchargement alternatif : (par exemple : http://IntranetUpd01)			
Téléchargez les fichiers sans URL dans les métadonnées si un serveur de téléchargement alternatif est défini.	Désactivé	Activer Windows Accédez aux paramètres pour activer	

GPO pour poste de travail

Je l'appellerai WSUS-PC

On repart au même endroit

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

Seulement 2 paramètres à définir ici.

Je définis le groupe de machines des PC communs

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 :

Nom du groupe cible de cet ordinateur : PC

Aide :

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

J'empêche le redémarrage pendant les périodes d'activités.

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

Paramètre précédent Paramètre suivant

Non configuré Commentaire :

Activé

Désactivé

Pris en charge sur : Au moins Windows Server 2016 ou Windows 10

Options :

Heures d'activité

Début : 7 h 00

Fin : 18 h 00

Aide :

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.

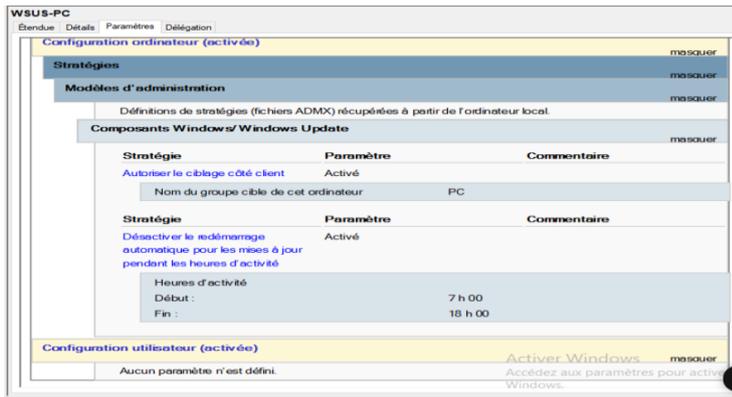
Si vous désactivez cette stratégie ou ne la configurez pas et que vous n'avez défini aucune autre stratégie de groupe de redémarrage, les heures d'activité sélectionnées par l'utilisateur sont appliquées.

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.

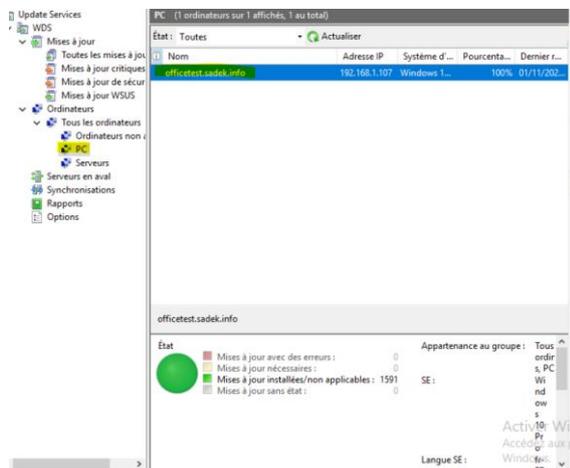
OK Annuler Appliquer

Résumé de la nouvelle GPO



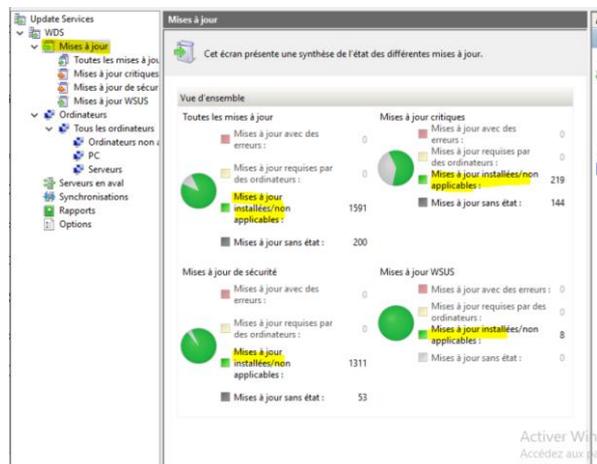
Pour l'instant avant de faire l'autre GPO je teste si mes deux GPO fonctionnent.

J'ai fait un gpupdate force sur l'un de mes postes de travail je le vois apparaître dans le groupe PC c'est parfait.

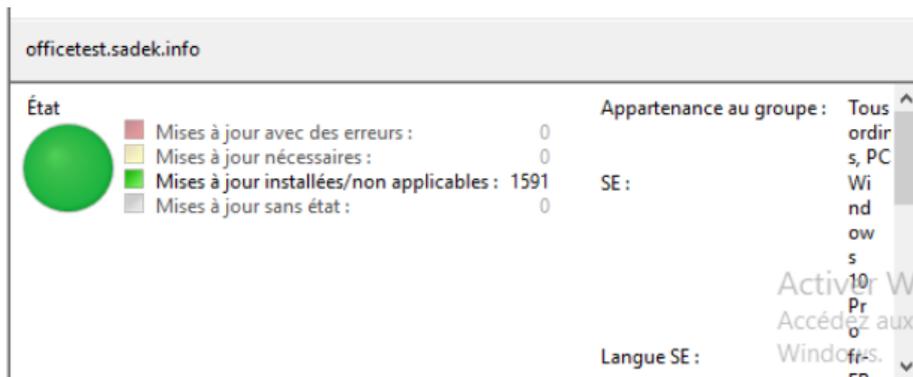


Dans le menu « Mises à jours »

On voit les mises à jours installées sur le serveur WSUS



Maintenant ça c'est quand je choisis un PC précisément



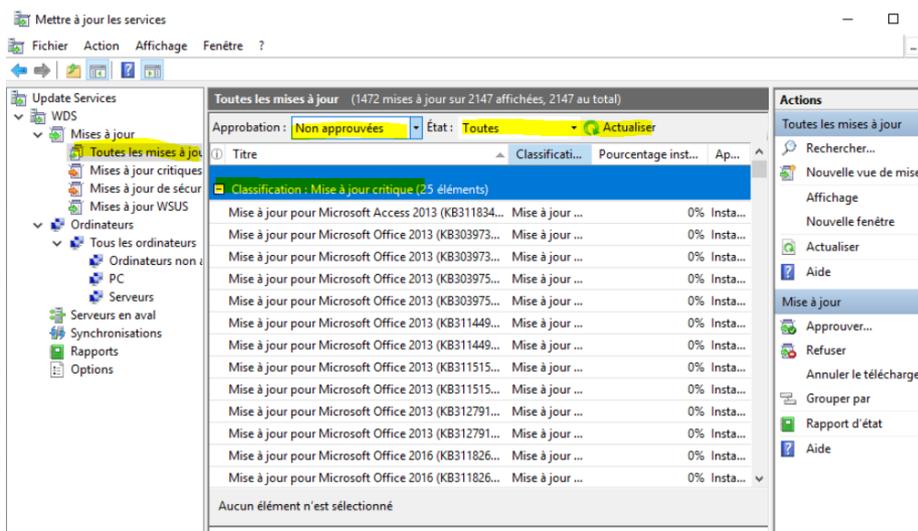
Lorsque je vais dans les paramètres de mon pc client wsus windows 10 voila ce que je vois

Historique des mises à jour

- ✓ Mises à jour qualité (5)
 - 2023-06 Mise à jour cumulative pour Windows 10 Version 21H2 de x64 avec systèmes basés dessus (KB5027215)
Installée le 31/10/2023
 - 2023-08 Mise à jour pour Windows 10 Version 21H2 sur systèmes x64 (KB4023057)
Installée le 31/10/2023
 - 2023-06 Mise à jour cumulative de .NET Framework 3.5, 4.8 et 4.8.1 Windows 10 Version 21H2 pour x64 (KB5027537)
Installée le 31/10/2023
 - 2023-04 Mise à jour pour Windows 10 Version 21H2 sur systèmes x64 (KB5026037)
Installée le 31/10/2023
 - 2022-11 Mise à jour pour Windows 10 Version 21H2 sur systèmes x64 (KB5020683)
Installée le 31/10/2023

Nous sommes bien le 31 des MAJ ont bien été effectués

Approbation des MAJ :



Ensuite je fais un click droit j'approuve ou refuse et définit pour quelle groupe j'approuve

Lorsqu'on a validé une mise à jours on peut voir à quel niveau elle est installé sur les pc en repartant dans notre groupe ici

PC (2 ordinateurs sur 3 affichés, 3 au total)				
État : Échec ou Nécessaire Actualiser				
Nom	Adresse IP	Système d'...	Pourcent...	Dernier rap...
sadeka.sadek.info	192.168.1...	Windows 10...	94%	01/11/2023 ...
wds.sadek.info	fe80::44c1...	Windows Se...	99%	01/11/2023 ...

Je continue ce tuto un jours après on voit bien que les MAJ sont effectués

[Désinstaller des mises à jour](#)

[Options de récupération](#)

Historique des mises à jour

∨ Mises à jour qualité (5)

2023-06 Mise à jour cumulative pour Windows 10 Version 21H2 de x64 avec systèmes basés dessus (KB5027215)

Installée le 01/11/2023

2023-08 Mise à jour pour Windows 10 Version 21H2 sur systèmes x64 (KB4023057)

Installée le 31/10/2023

2023-06 Mise à jour cumulative de .NET Framework 3.5, 4.8 et 4.8.1 Windows 10 Version 21H2 pour x64 (KB5027537)

Installée le 31/10/2023

2023-04 Mise à jour pour Windows 10 Version 21H2 sur systèmes x64 (KB5026037)

Installée le 31/10/2023

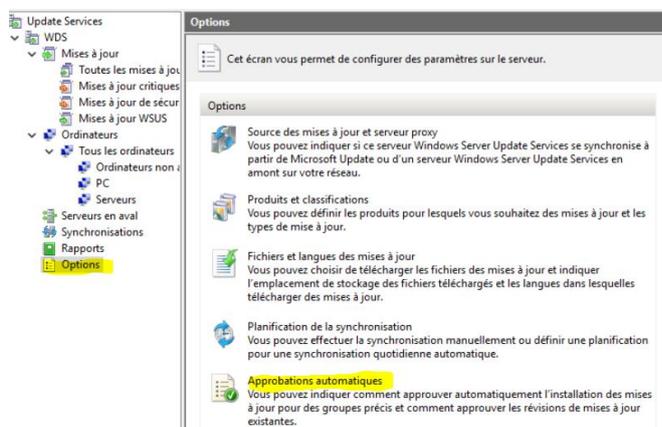
2022-11 Mise à jour pour Windows 10 Version 21H2 sur systèmes x64 (KB5020683)

Installée le 31/10/2023

> Mises à jour de définitions (1)

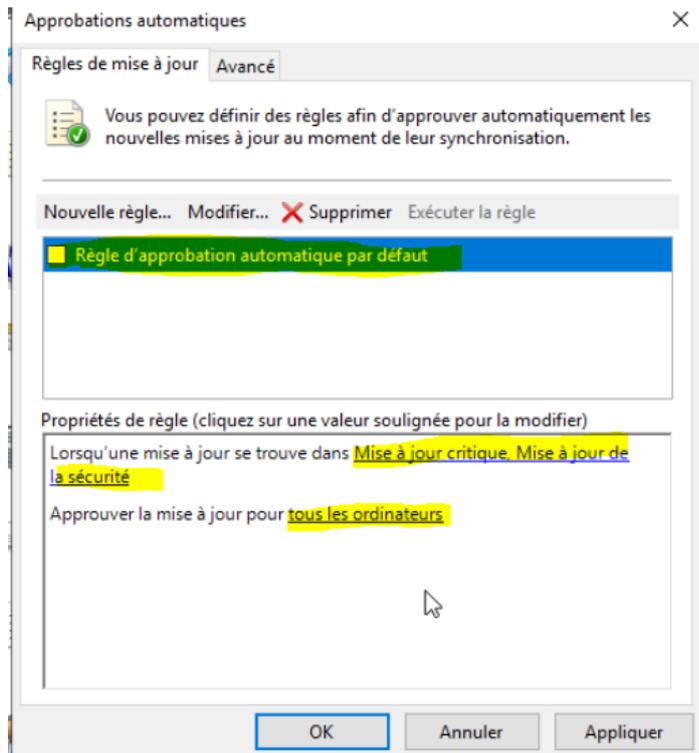
Mise en place d'une règle pour approuver les MAJ automatiquement

Aller ici

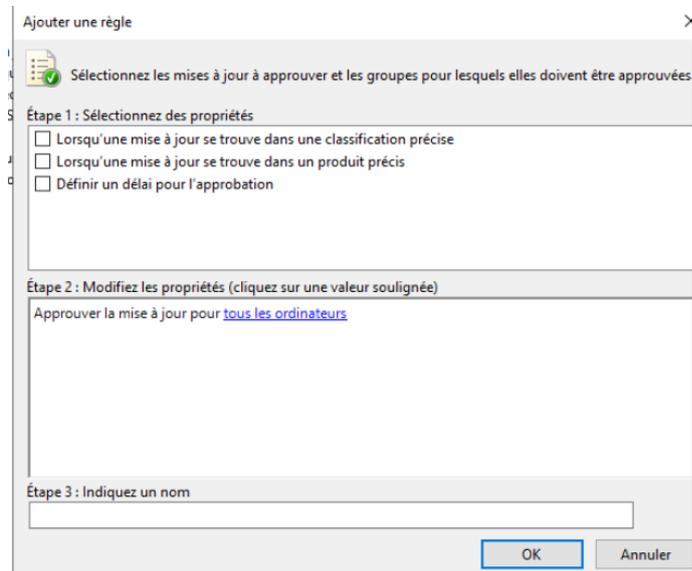


Je clique sur approbation automatique.

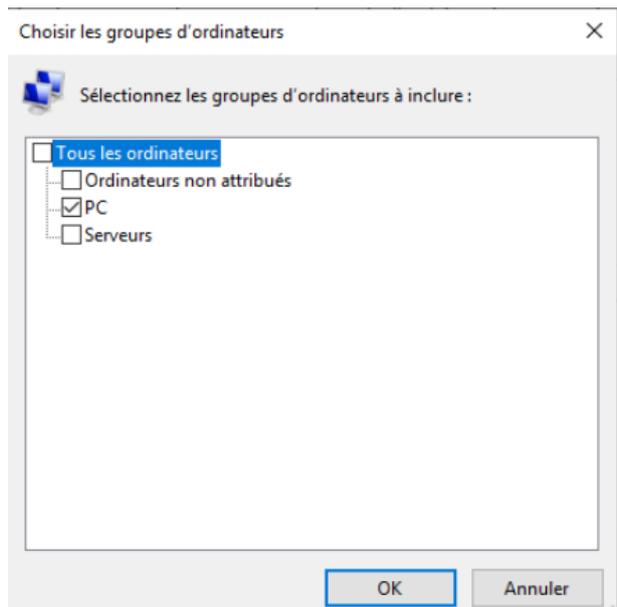
Il y'a cette règle par défaut qui n'est pas activé que je trouve très bien je l'active et j'applique



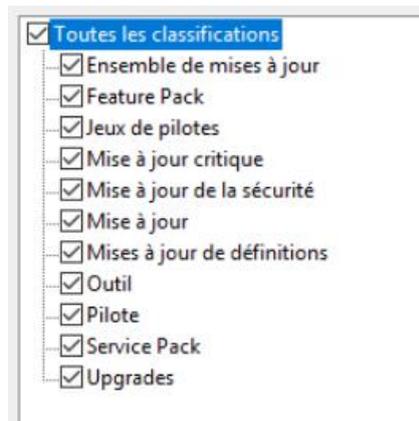
Je peux aussi crée une nouvelle règle ici.



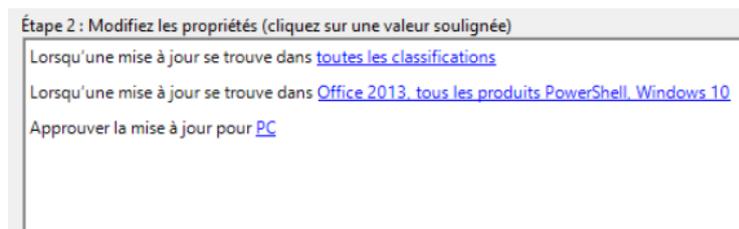
En appuyant sur la partie bleuter ordinateur je peux définir sur quel groupe s'applique la règle.



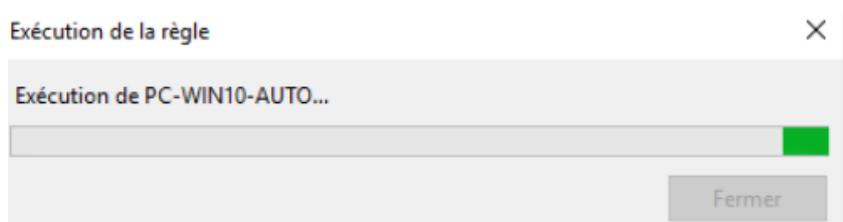
Je peux aussi choisir quelle classification



Je peux aussi définir dans quelle produits.

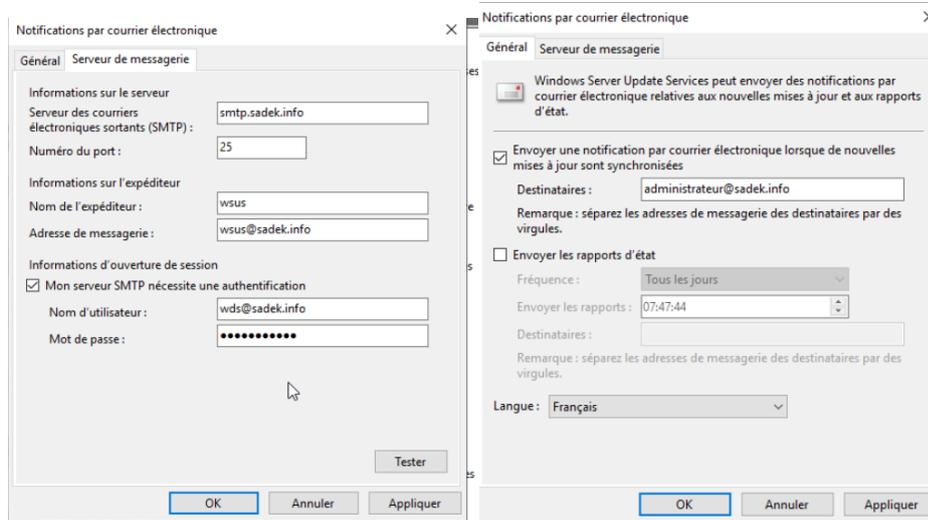


Ensuite je peux appuyer sur exécuter la règle dans le menu de base pour la mettre à exécution directement au lieu d'attendre un comportement qui appel à effectuer cette règle



Notification via email

Je définis que je veux me faire notifier toute mise à jour et je définis les infos du serveur smtp et le nom d'utilisateur et mdp que je vais utiliser



Je réalise un test je regarde sur le mail administrateur@sadek.info

C'est parfait

