WSUS

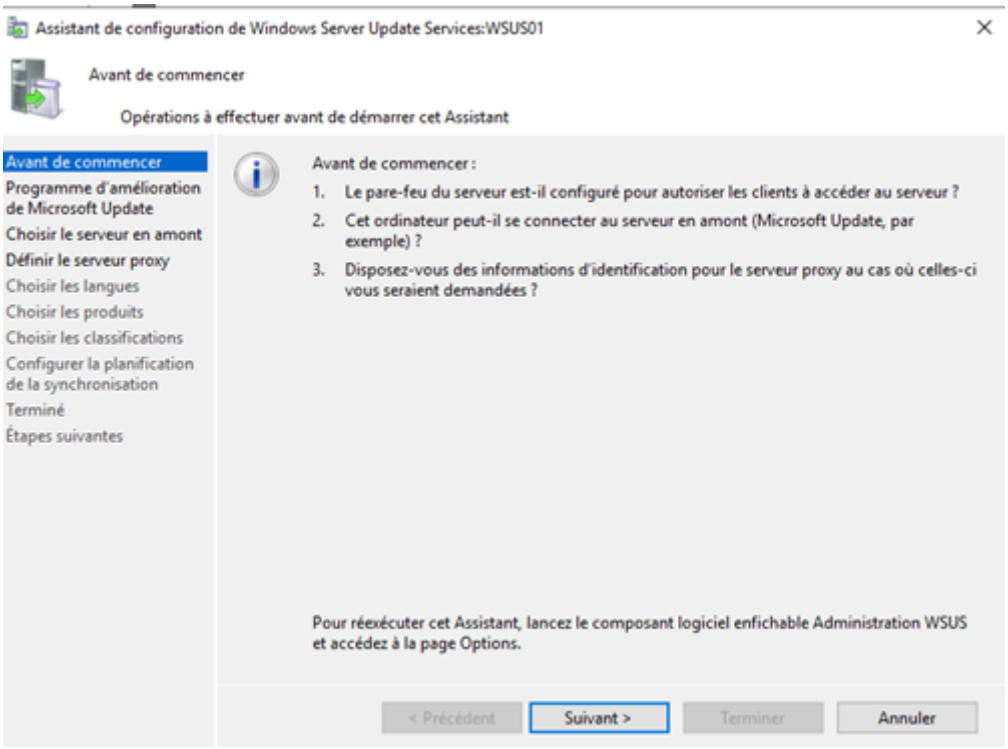
Toutes les pages liées au WSUS

- Installation du rôle WSUS et synchronisation
- Optimisation de WSUS
- Ciblage des postes clients pour les mises à jour via le serveur WSUS
- Création de vues
- Création des GPO pour le ciblage WSUS et des groupes de tests des mises à jour
- Approbation des mises à jour
- Installation du runtime Microsoft Report Viewer
- Approbation automatique des mises à jour de définition (Windows Defender)
- Mise en place du TLS/SSL pour WSUS
- Résoudre l'apparition de duplicatas de WSUS dans la console
- Installation automatique des définitions de Microsoft Defender
- Windows Server 2022 et WSUS

Installation du rôle WSUS et synchronisation

On fait comme pour les autres rôles, en choisissant Services WSUS (Windows Server Update Services) en laissant tout par défaut.

Ensuite, depuis le menu Démarrer, on cherche "Windows Server Update Services" depuis "Outils d'administration Windows".



On clique sur "Suivant >" puis on choisit le serveur en amont. On choisit "Synchroniser depuis Windows Update".

On choisit ensuite le serveur Proxy s'il y en a un.

On clique sur "Démarrer la connexion". Cela va récupérer les types de mises à jour disponibles, les produits pouvant être mis à jour et les langues disponibles.

On clique ensuite sur "Suivant", on sélectionne uniquement la langue Française.

Pour les produits, on choisit selon notre parc.

Les produits qui doivent être mis à jour sont **Windows Server 2019** et **Windows 10 1903 and later (On coche aussi Windows 10 s'il y a des machines plus vieilles) et « Gestionnaire de serveur Windows – Programme d'installation dynamique de Windows Server Update Services »**, **Developer Tools, Runtimes, and Redistributables (Visual C++ Runtime libraries, etc).**

On coche tout sauf Pilote (Driver) et jeux de pilotes puis on clique sur "Suivant".

Pour la synchronisation, on choisit 4 fois par jour.

Ensuite, la console se lance. On choisit le noeud SRV-WSUS01 (nom du serveur) puis le noeud "Synchronisations" puis on clique sur "Synchroniser maintenant". C'est une étape très longue.

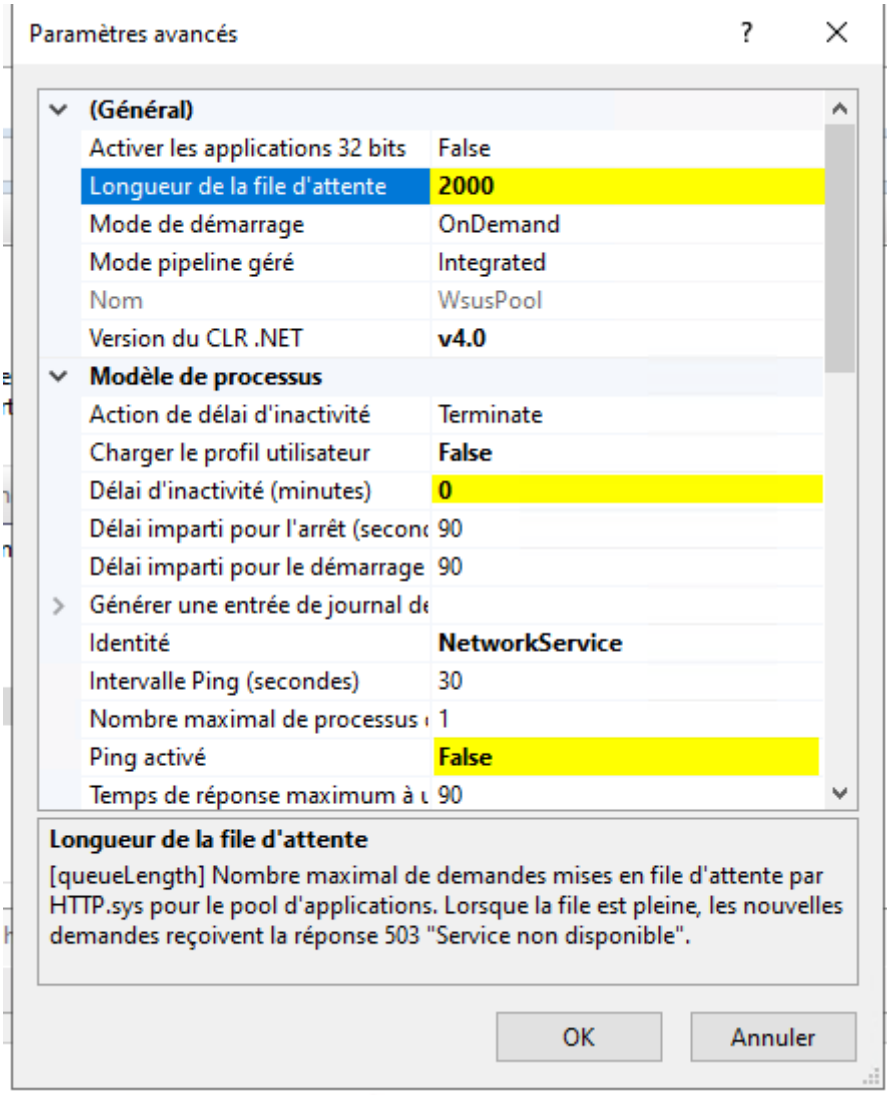
Avant d'approuver les mises à jour, les postes clients et les autres serveurs doivent être connectés aux serveurs WSUS.

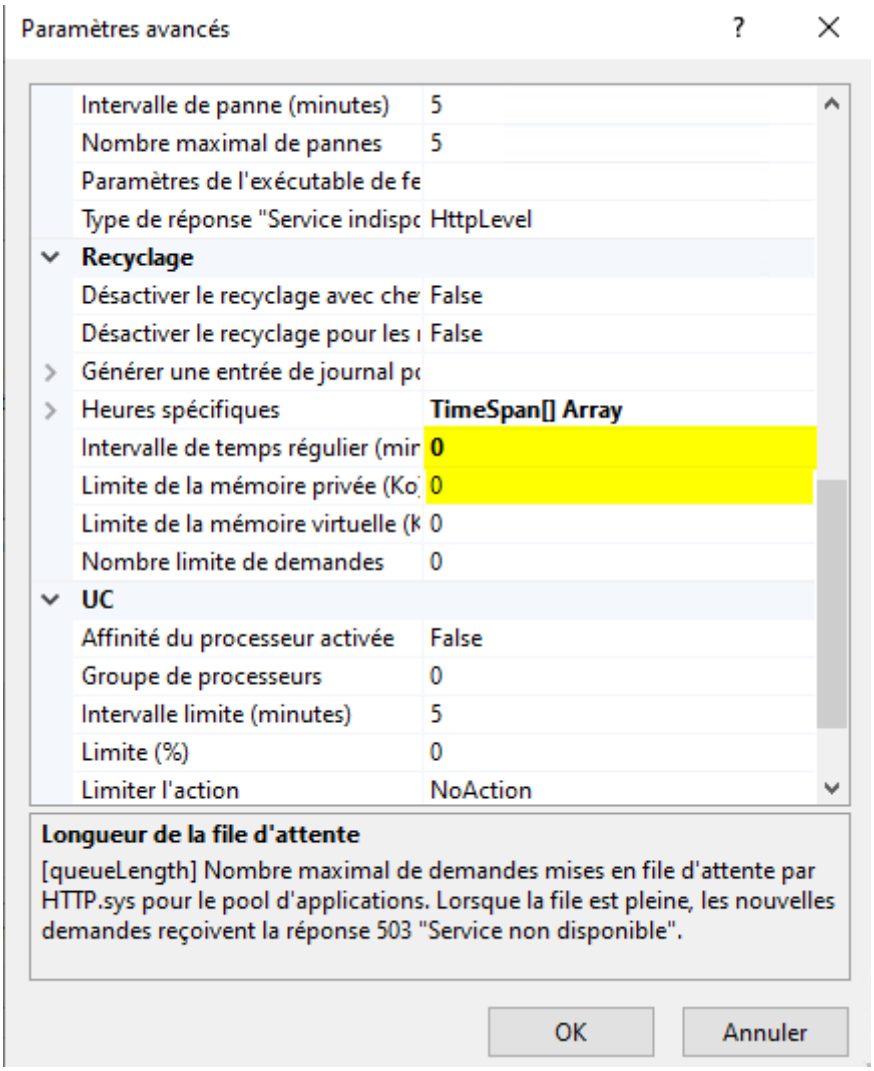
Optimisation de WSUS

Tout d'abord, on va modifier les paramètres du pool d'application "**WsusPool**".

On se rend dans le "**Gestionnaire des services Internet (IIS)**".

Sous "**Pools d'applications**", on clique droit sur "**WsusPool**" puis "**Paramètres avancés**".





On clique droit sur "**WsusPool**" puis "**Arrêter**". On attend quelques secondes puis on le redémarre.

Ciblage des postes clients pour les mises à jour via le serveur WSUS

On lance la console "Windows Server Update Services".

On développe le nœud "Ordinateurs" et on clique droit sur "Tous les ordinateurs" puis on sélectionne "Ajouter un groupe d’ordinateurs".

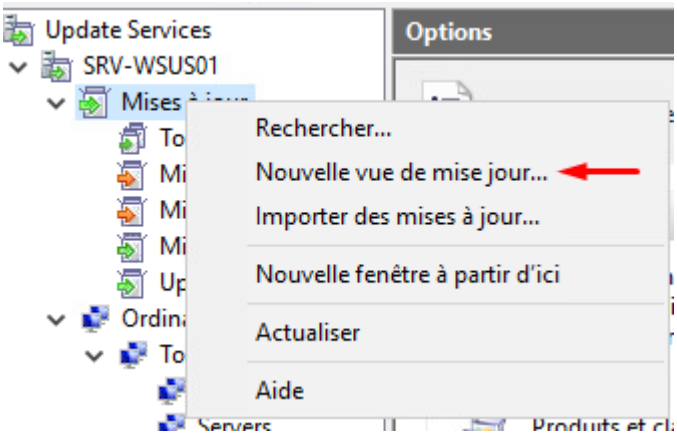
On va ensuite ajouter 4 groupes : "Servers", "Workstations", "Test – Servers", "Test – Workstations".

On clique maintenant sur "Options" puis sur "Ordinateurs".

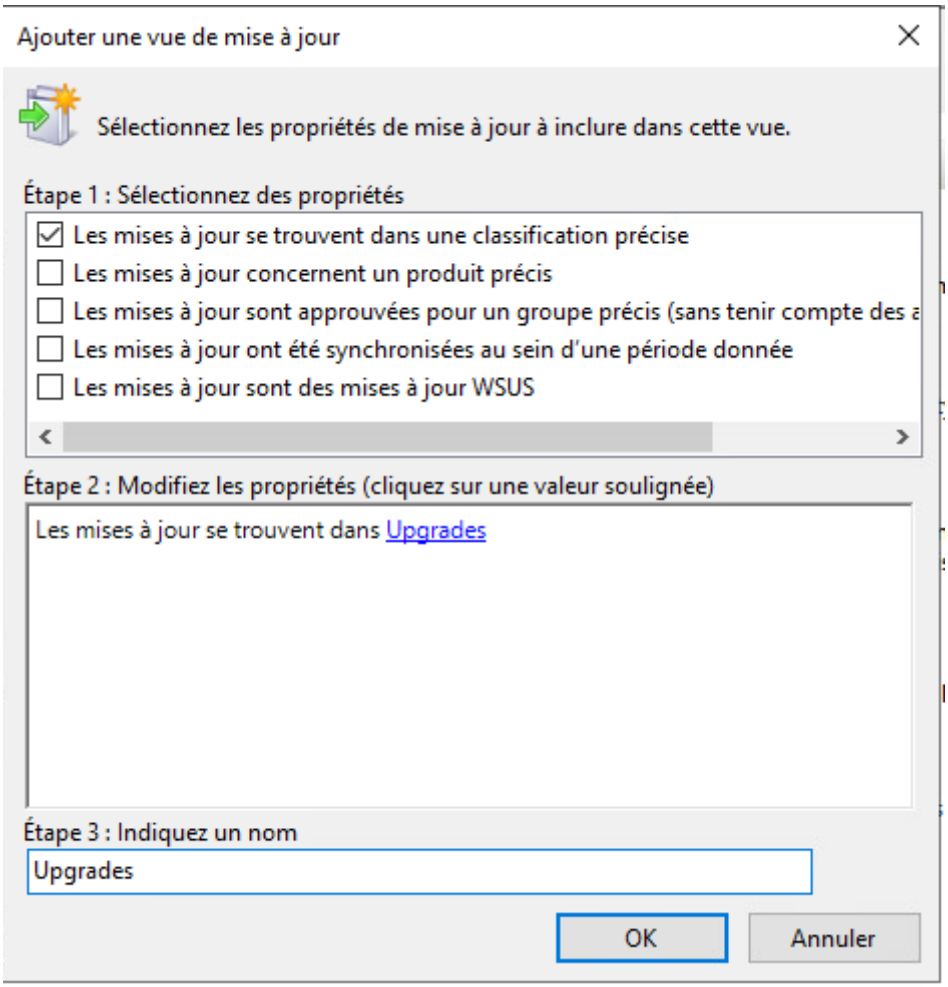
On coche Utiliser les paramètres de stratégie de groupe ou de Registre sur les ordinateurs puis cliquez sur OK.

Création de vues

Dans la console de Services WSUS, on clique droit sur "Mises à jour".

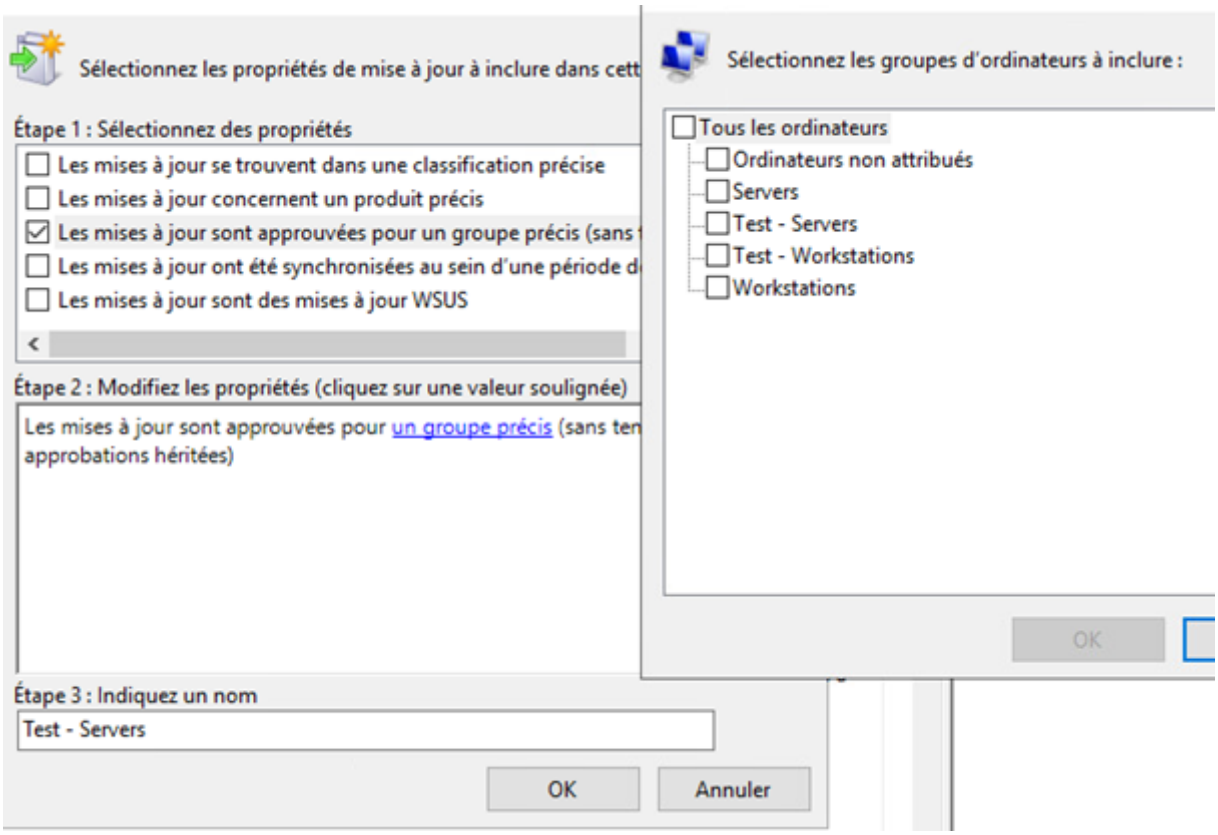


On clique sur "Nouvelle vue de mise à jour...". On coche la première option, on clique sur "Toutes les classifications" et on coche uniquement "Upgrade". On clique ensuite sur "OK".

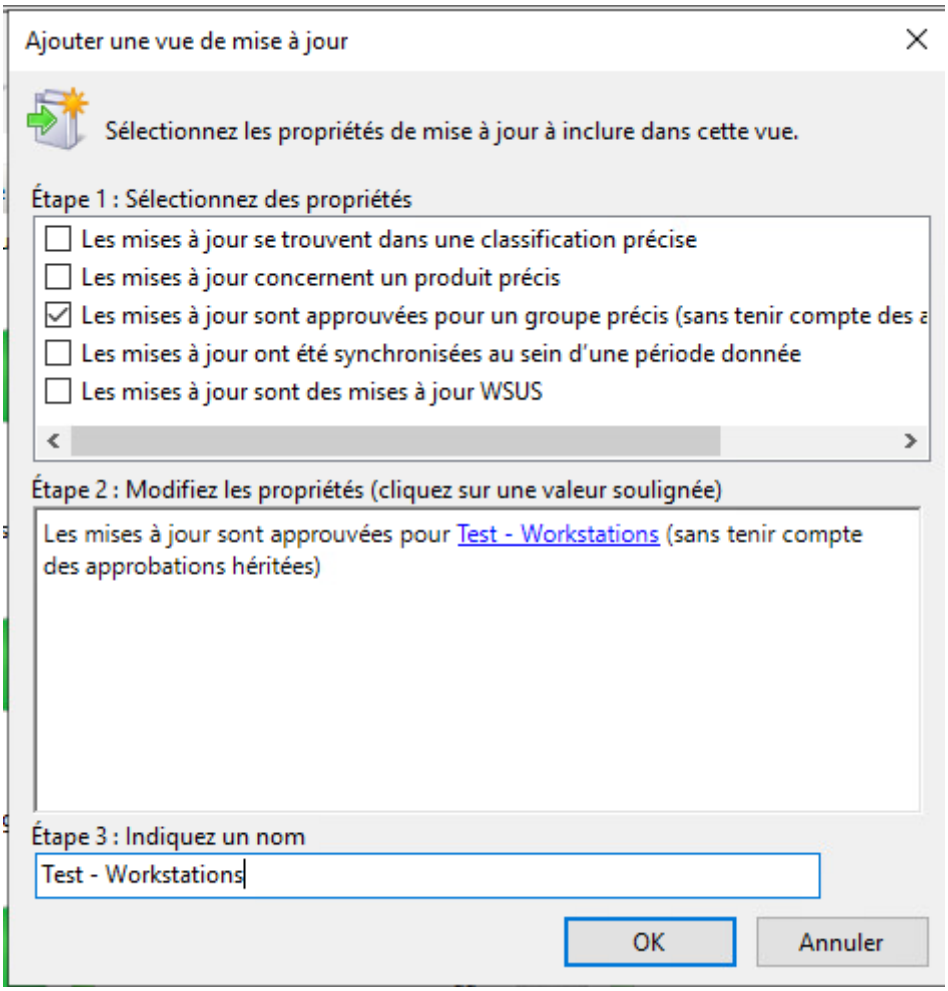


On ajoute ensuite 2 vues pour les mises à jour approuvées pour un groupe précis, ici Test Servers et Test - Workstations

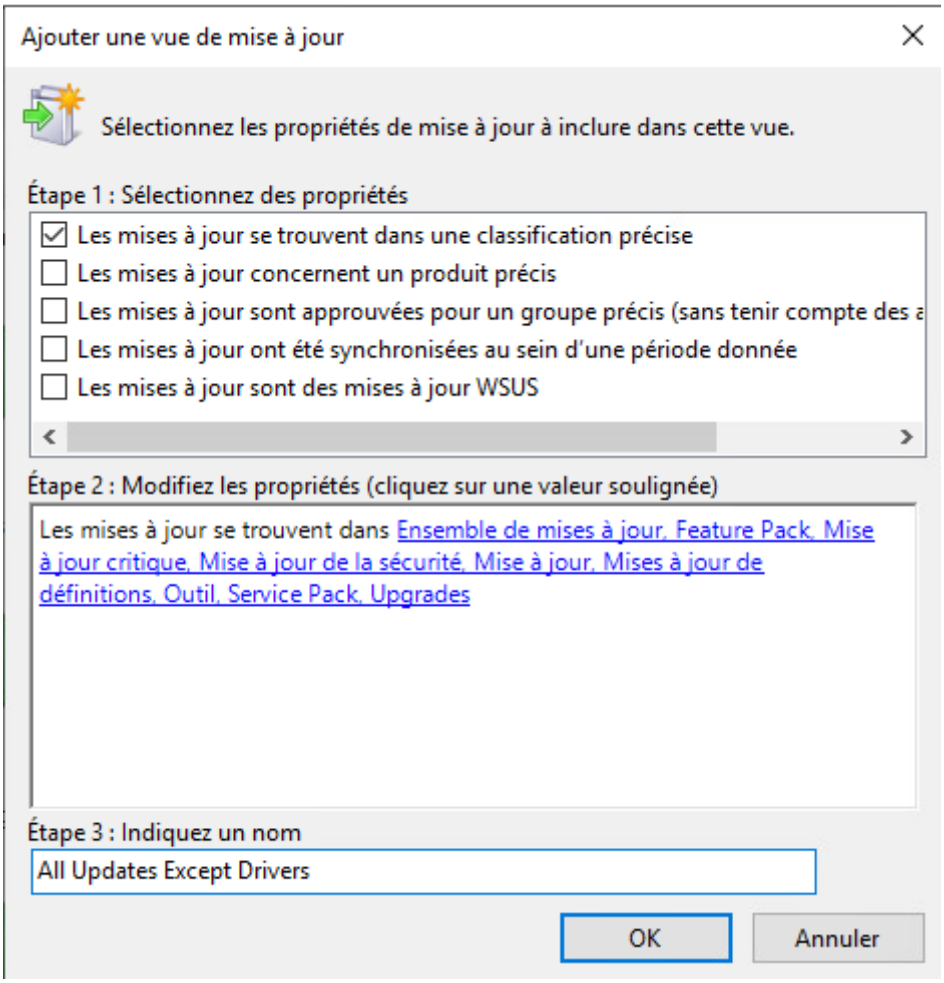
Test - Servers



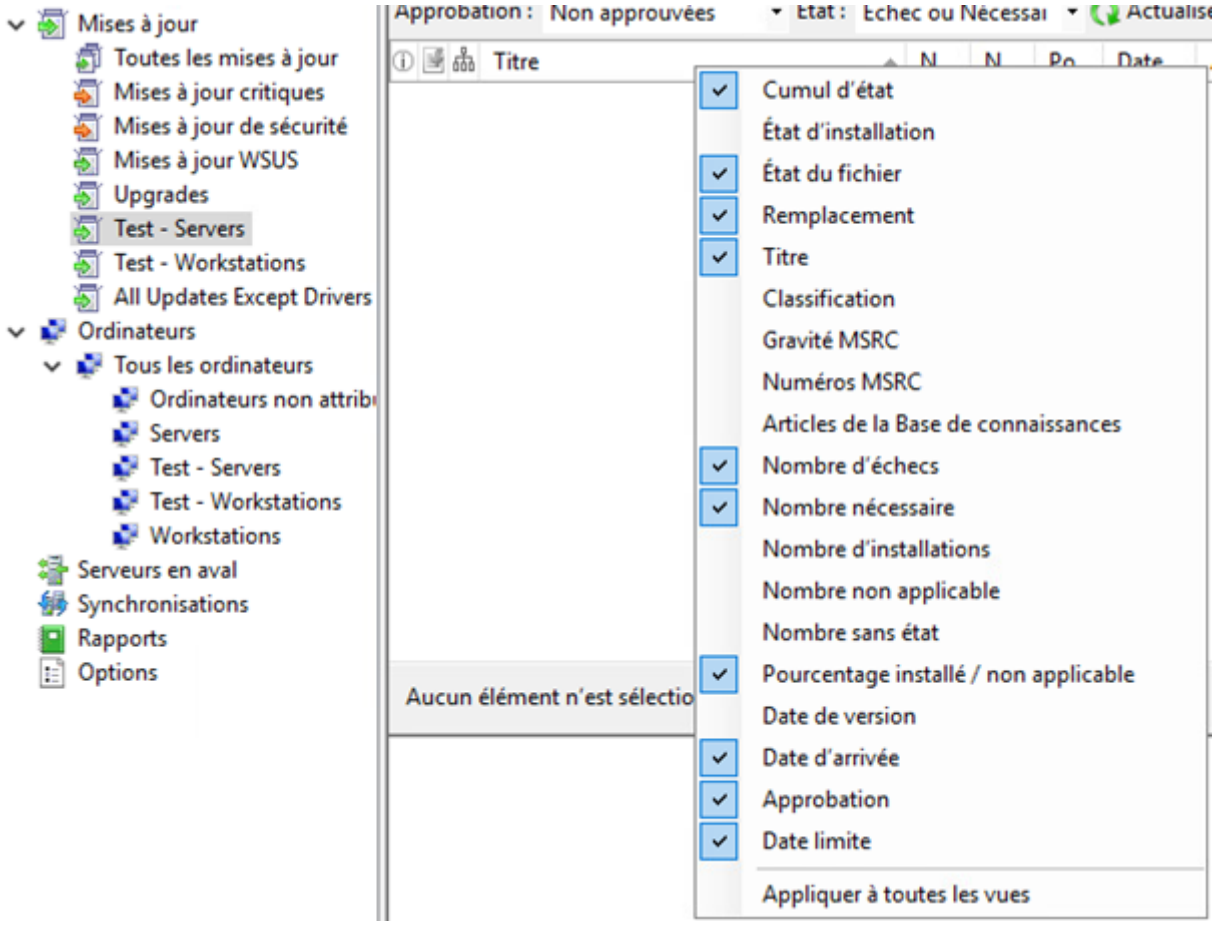
Test - Workstations



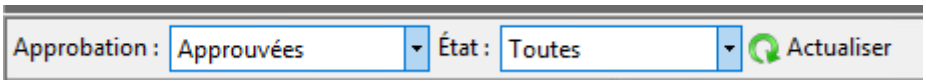
On crée ensuite une vue pour toutes les mises à jour sauf les pilotes.



Ensuite, on clique droit sur une colonne et on rajoute différents éléments :

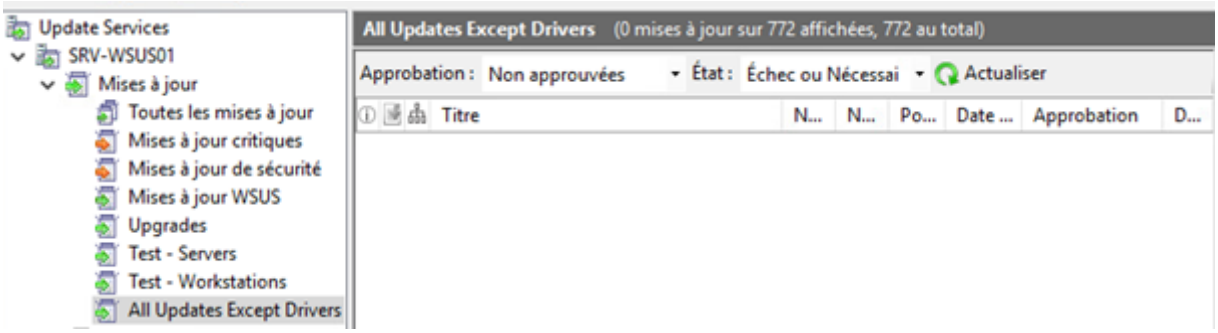


On modifie l'Approbation et l'Etat.

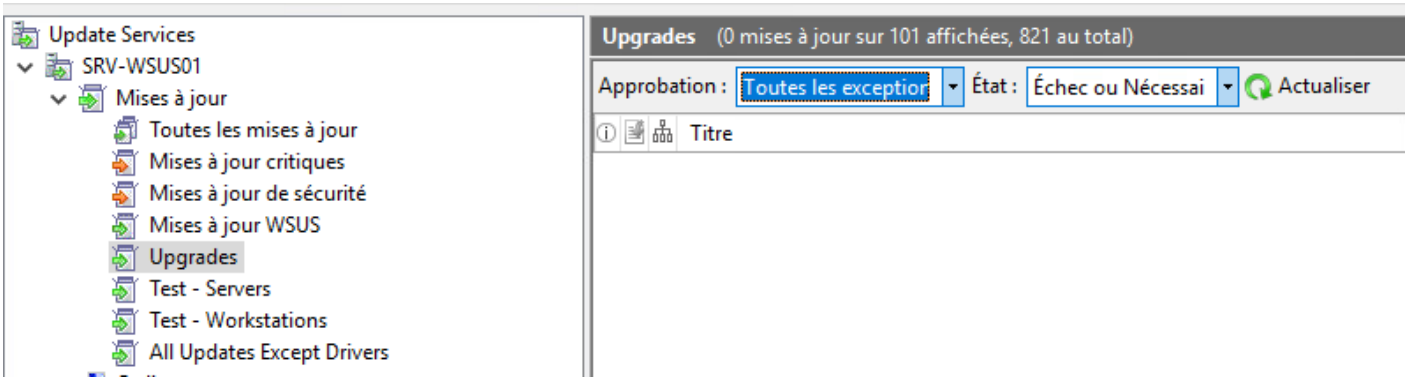


On applique la même chose pour la vue "Test – Workstations".

Pour "All Updates Except Drivers", idem mais "Non Approuvées" et "Echec ou Nécessaires".



Pour "Upgrades", idem qu'avant sauf "Toutes les exceptions sauf celles refusées" et "Echec ou Nécessaire".


Update Services
SRV-WSUS01
Mises à jour
Toutes les mises à jour
Mises à jour critiques
Mises à jour de sécurité
Mises à jour WSUS
Upgrades
Test - Servers
Test - Workstations
All Updates Except Drivers
Upgrades (0 mises à jour sur 101 affichées, 821 au total)
Approbation :
Toutes les exceptior
État :
Échec ou Nécessai
Actualiser
Titre

Création des GPO pour le ciblage WSUS et des groupes de tests des mises à jour

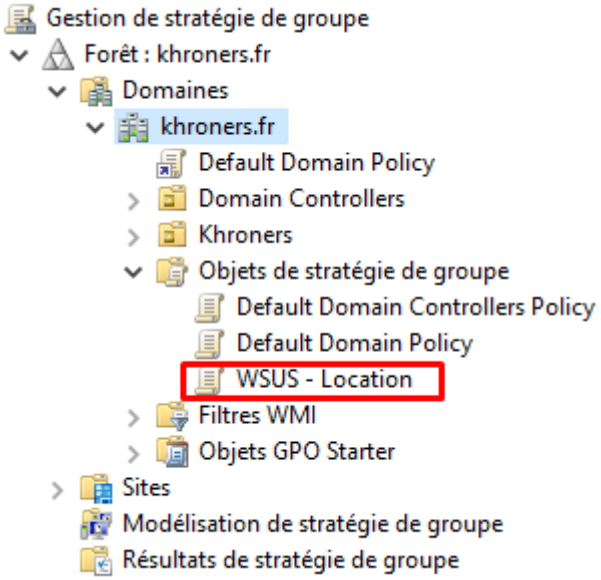
Présentation

Il faut ensuite créer des GPO pour que les postes de travails et serveurs du domaine puissent se mettre à jour via le WSUS et non par les serveurs de Microsoft.

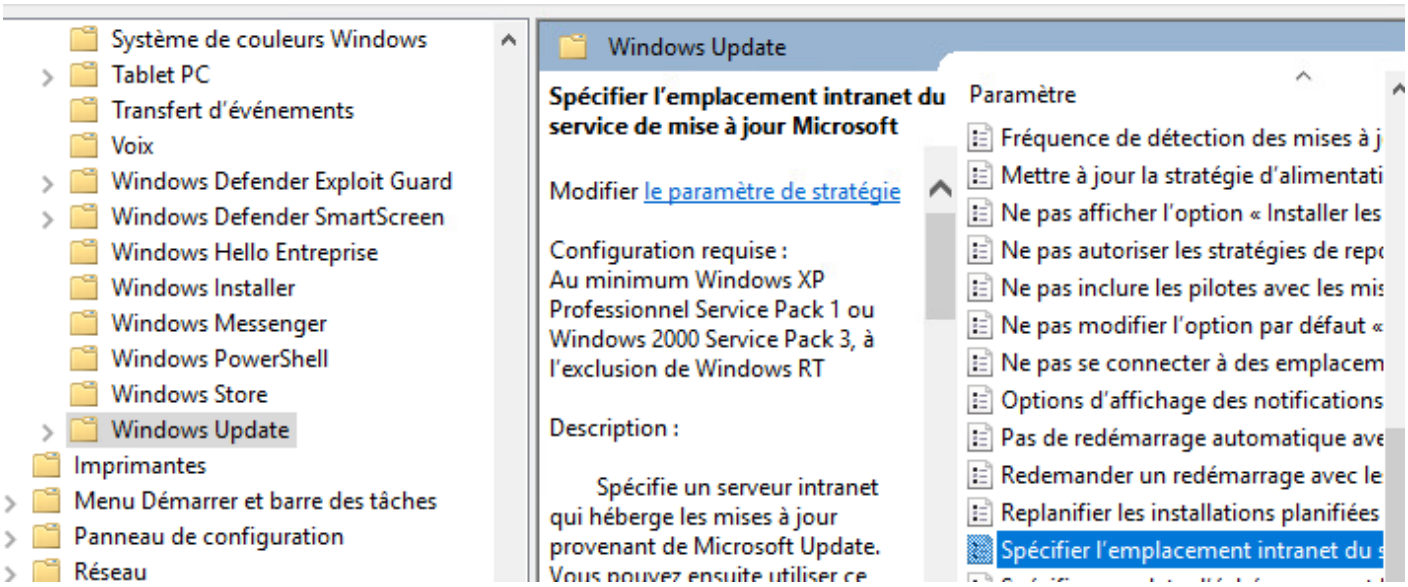
Création des GPO

WSUS - Location

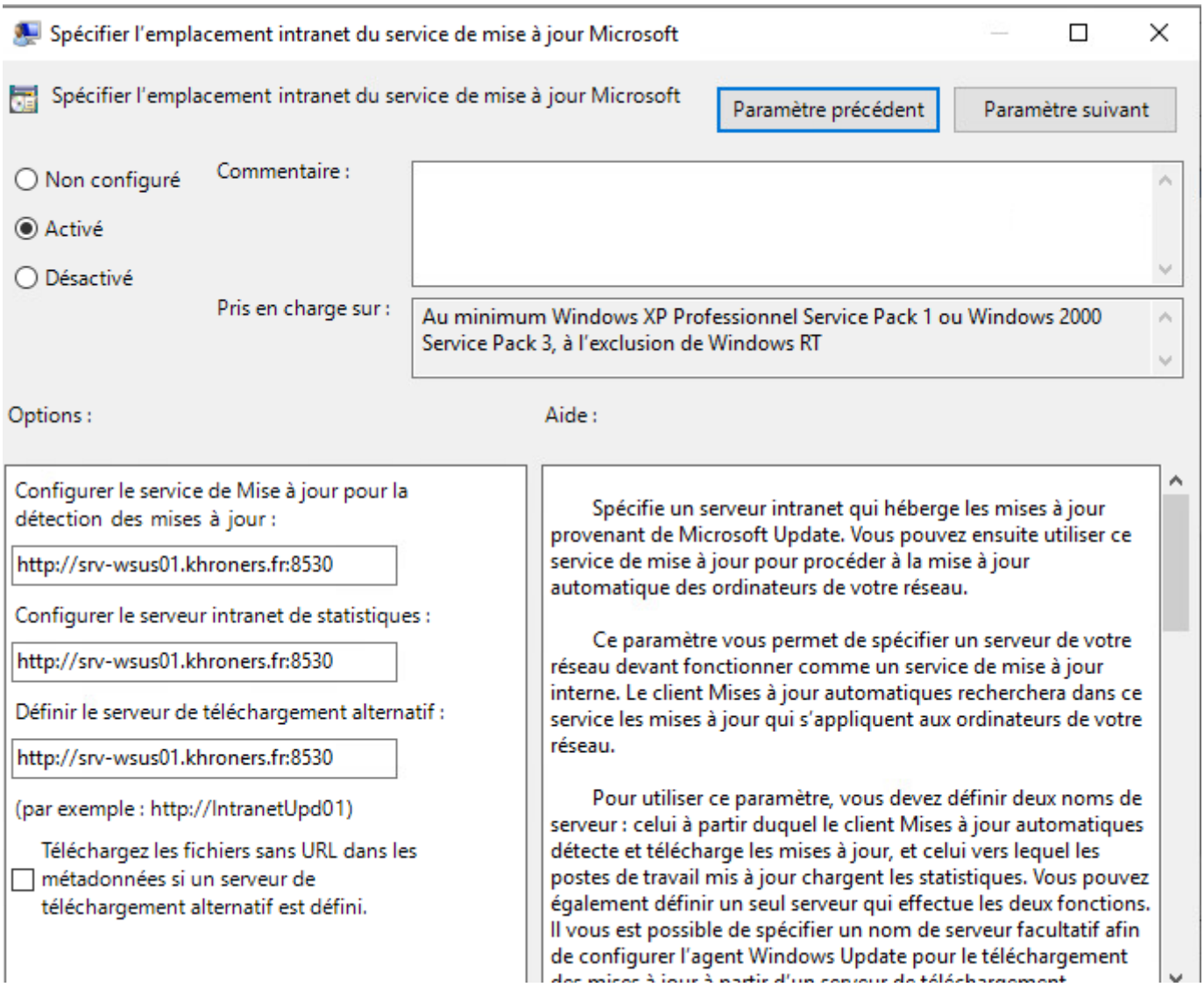
On se rend dans la console de Gestion de stratégie de groupe, on clique droit sur "Objets de stratégie de groupe" puis on crée une nouvelle GPO nommée "WSUS - Location".



On clique droit sur la nouvelle GPO puis "Modifier". On se rend dans Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows et Windows Update.



"Spécifier l'emplacement intranet du serveur de mise à jour..." On active et on définit l'url.
(L'entrée DNS pour le serveur WSUS doit être présente)

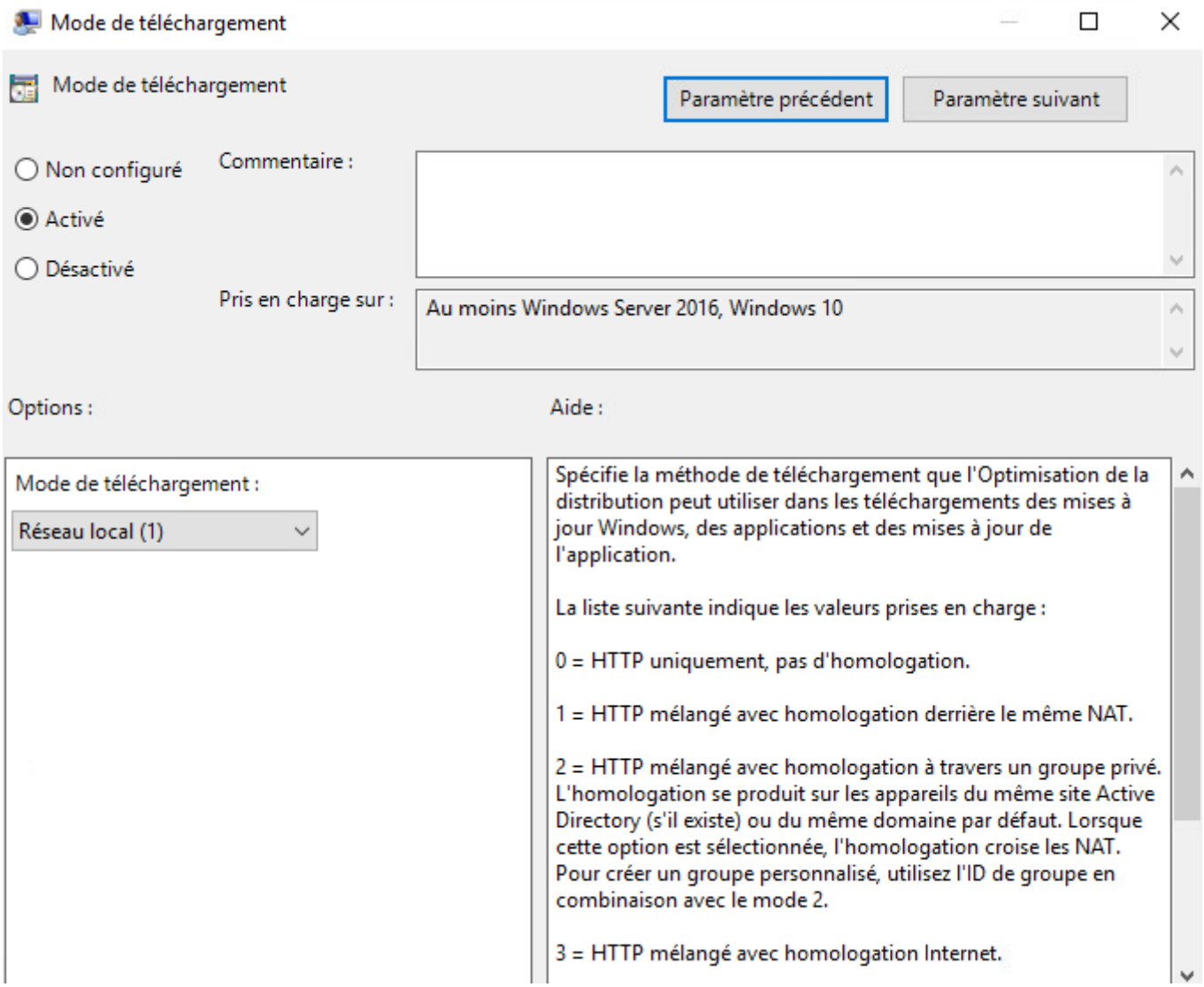


WSUS - Workstations

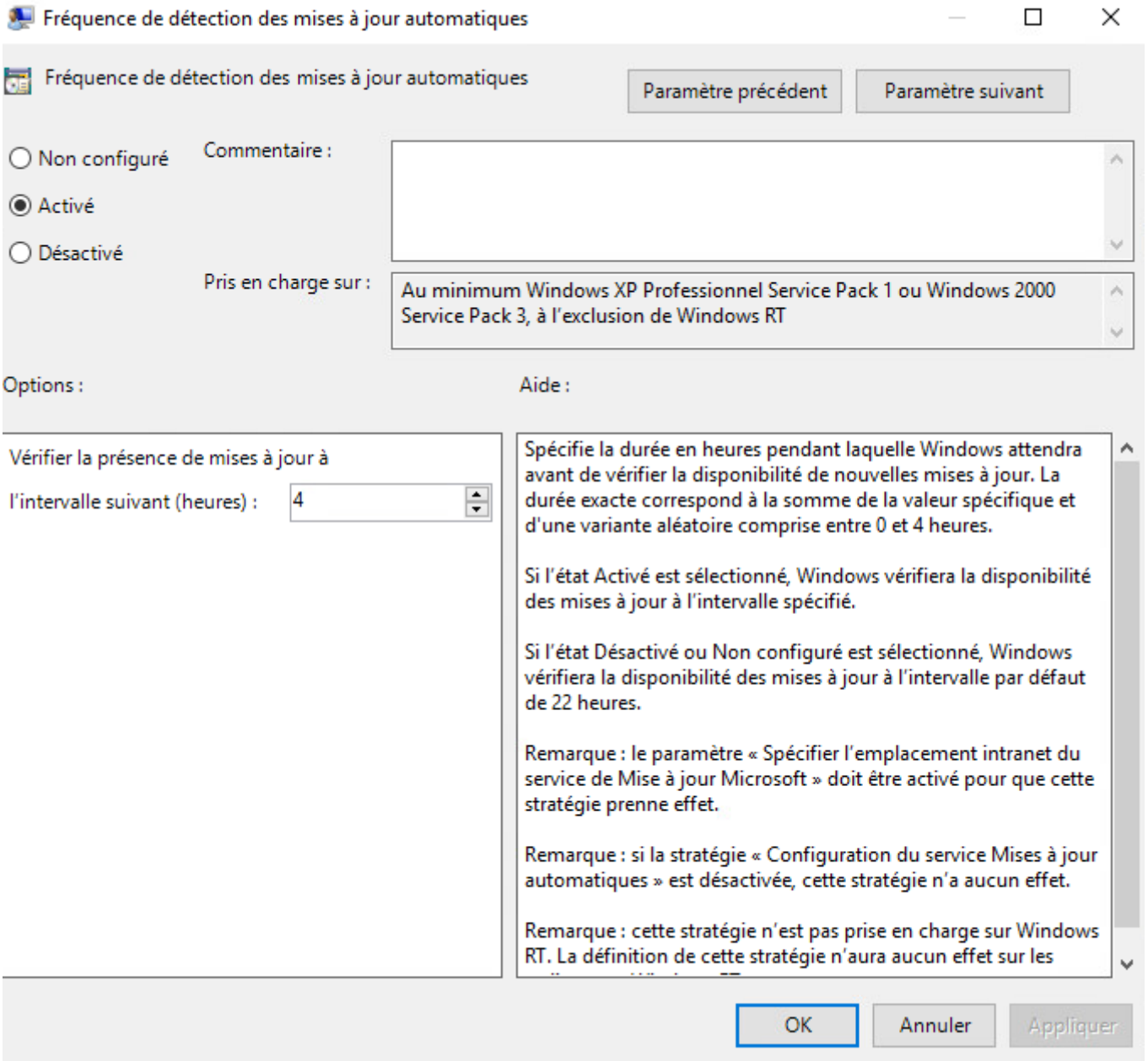
On crée ensuite une nouvelle GPO pour les postes de travail nommée "WSUS - Workstations".

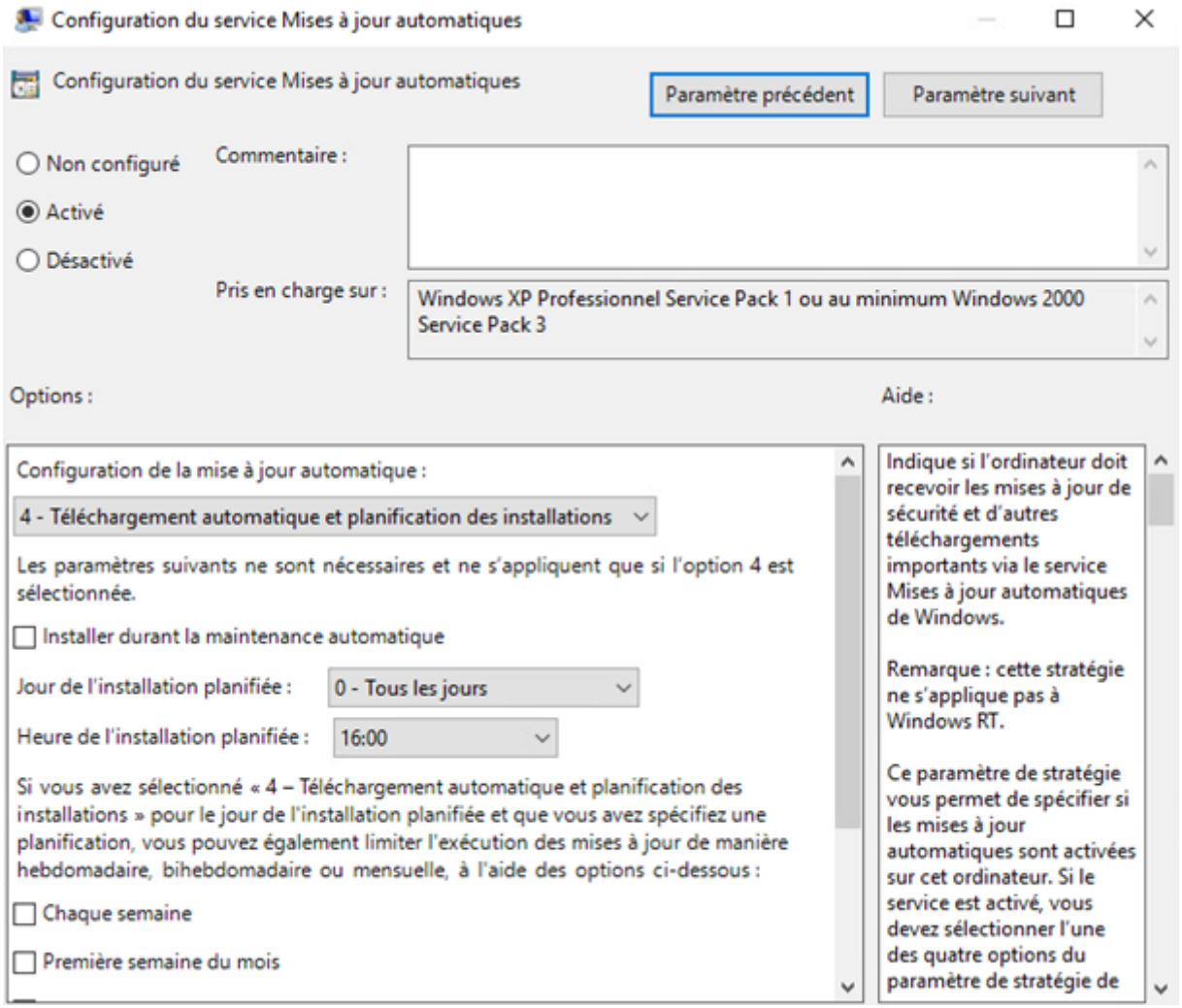
On la modifie et on se rend dans Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Optimisation de la distribution.

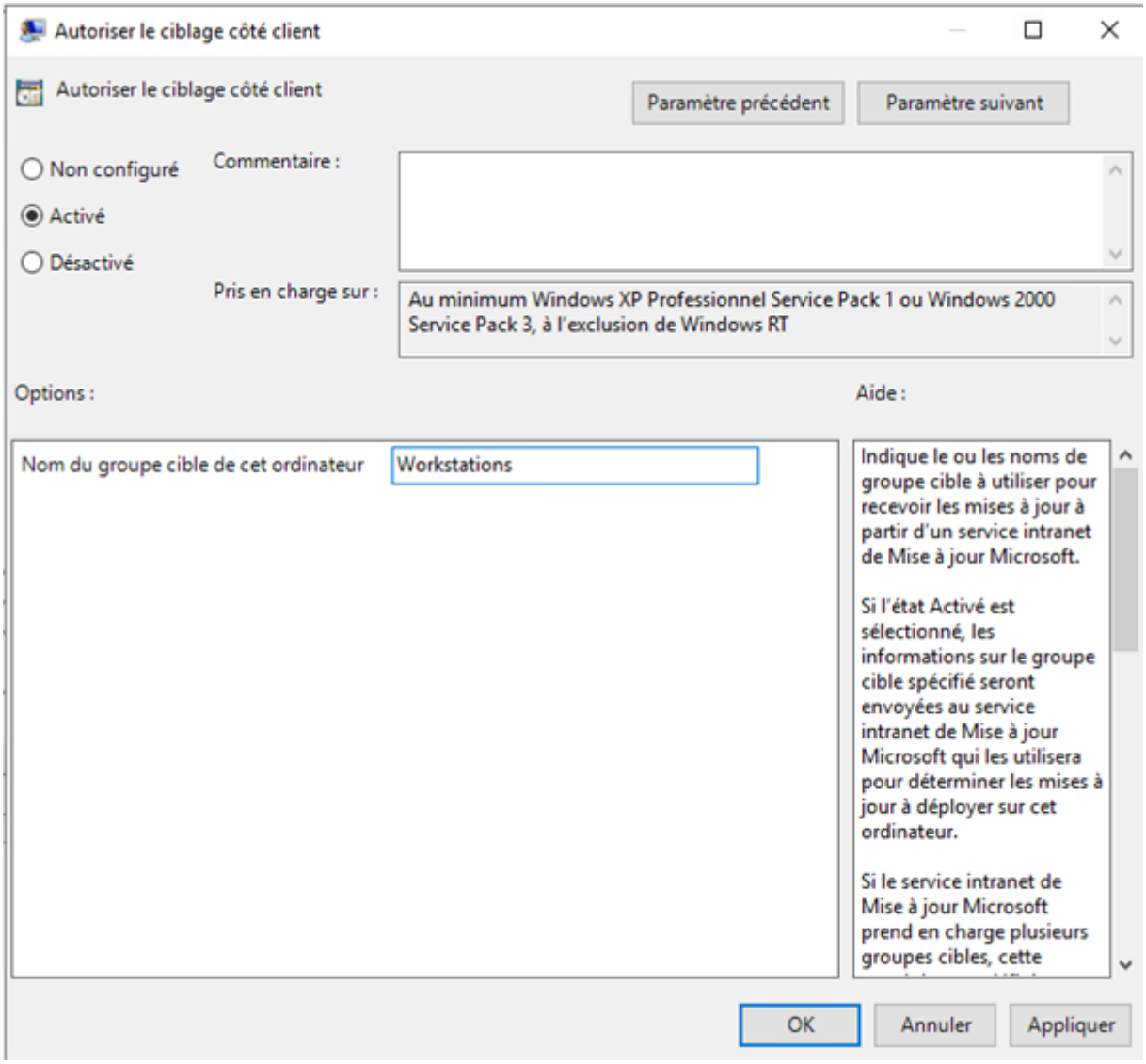
On active "Mode de téléchargement" sur "Réseau local".



On se rend ensuite dans Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Windows Update

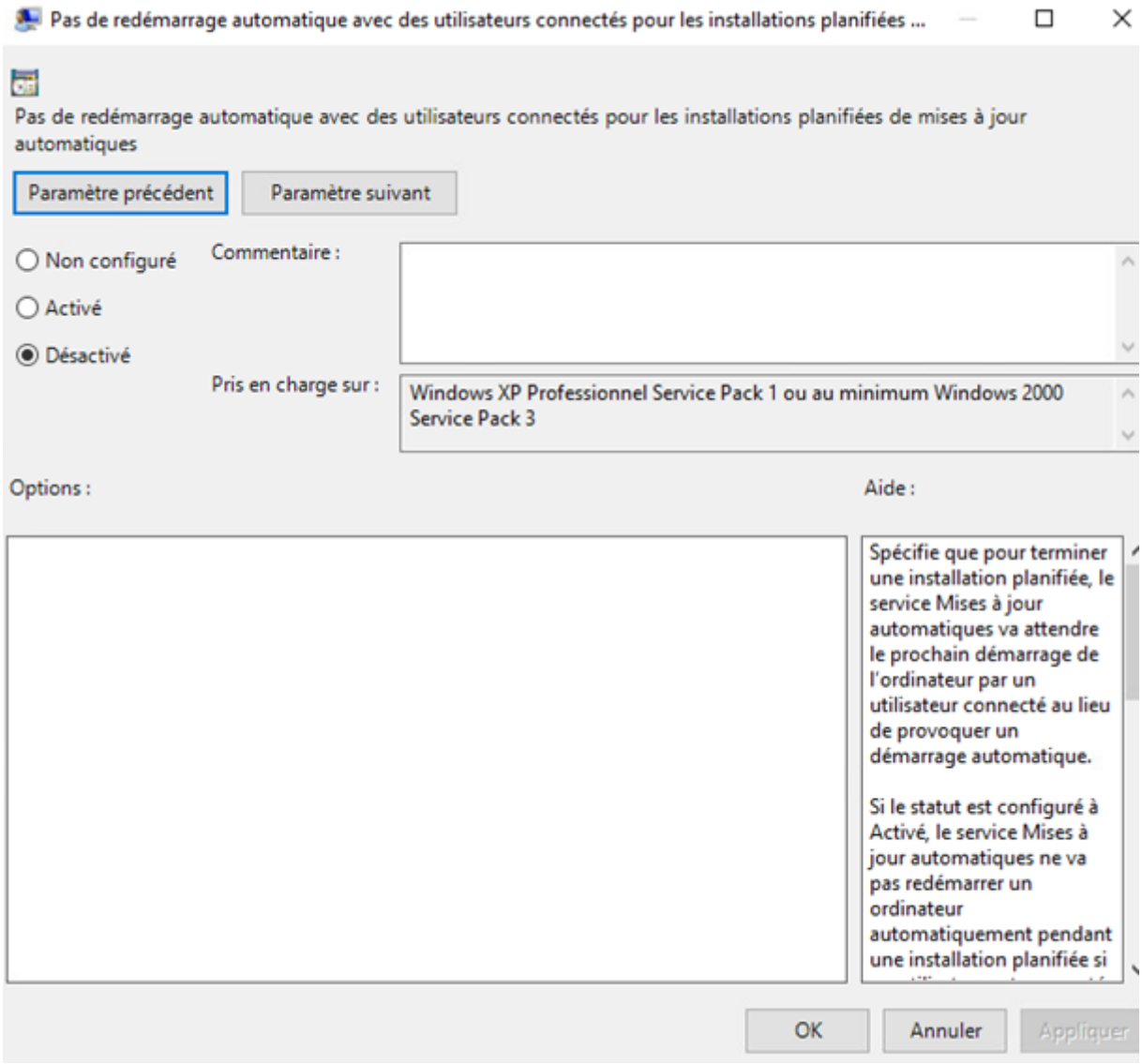

Fréquence de détection des mises à jour automatiques
Fréquence de détection des mises à jour automatiques
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion de Windows RT
Options :
Aide :
Vérifier la présence de mises à jour à
l'intervalle suivant (heures) :
4
Spécifie la durée en heures pendant laquelle Windows attendra avant de vérifier la disponibilité de nouvelles mises à jour. La durée exacte correspond à la somme de la valeur spécifique et d'une variante aléatoire comprise entre 0 et 4 heures.
Si l'état Activé est sélectionné, Windows vérifiera la disponibilité des mises à jour à l'intervalle spécifié.
Si l'état Désactivé ou Non configuré est sélectionné, Windows vérifiera la disponibilité des mises à jour à l'intervalle par défaut de 22 heures.
Remarque : le paramètre « Spécifier l'emplacement intranet du service de Mise à jour Microsoft » doit être activé pour que cette stratégie prenne effet.
Remarque : si la stratégie « Configuration du service Mises à jour automatiques » est désactivée, cette stratégie n'a aucun effet.
Remarque : cette stratégie n'est pas prise en charge sur Windows RT. La définition de cette stratégie n'aura aucun effet sur les
OK
Annuler
Appliquer


Configuration du service Mises à jour automatiques
Configuration du service Mises à jour automatiques
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Windows XP Professionnel Service Pack 1 ou au minimum Windows 2000 Service Pack 3
Options :
Aide :
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 :
16:00
Si vous avez sélectionné « 4 – Téléchargement automatique et planification des installations » pour le jour de l'installation planifiée et que vous avez 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
Indique si l'ordinateur doit recevoir les mises à jour de sécurité et d'autres téléchargements importants via le service Mises à jour automatiques de Windows.
Remarque : cette stratégie ne s'applique pas à Windows RT.
Ce paramètre de stratégie vous permet de spécifier si les mises à jour automatiques sont activées sur cet ordinateur. Si le service est activé, vous devez sélectionner l'une des quatre options du paramètre de stratégie de

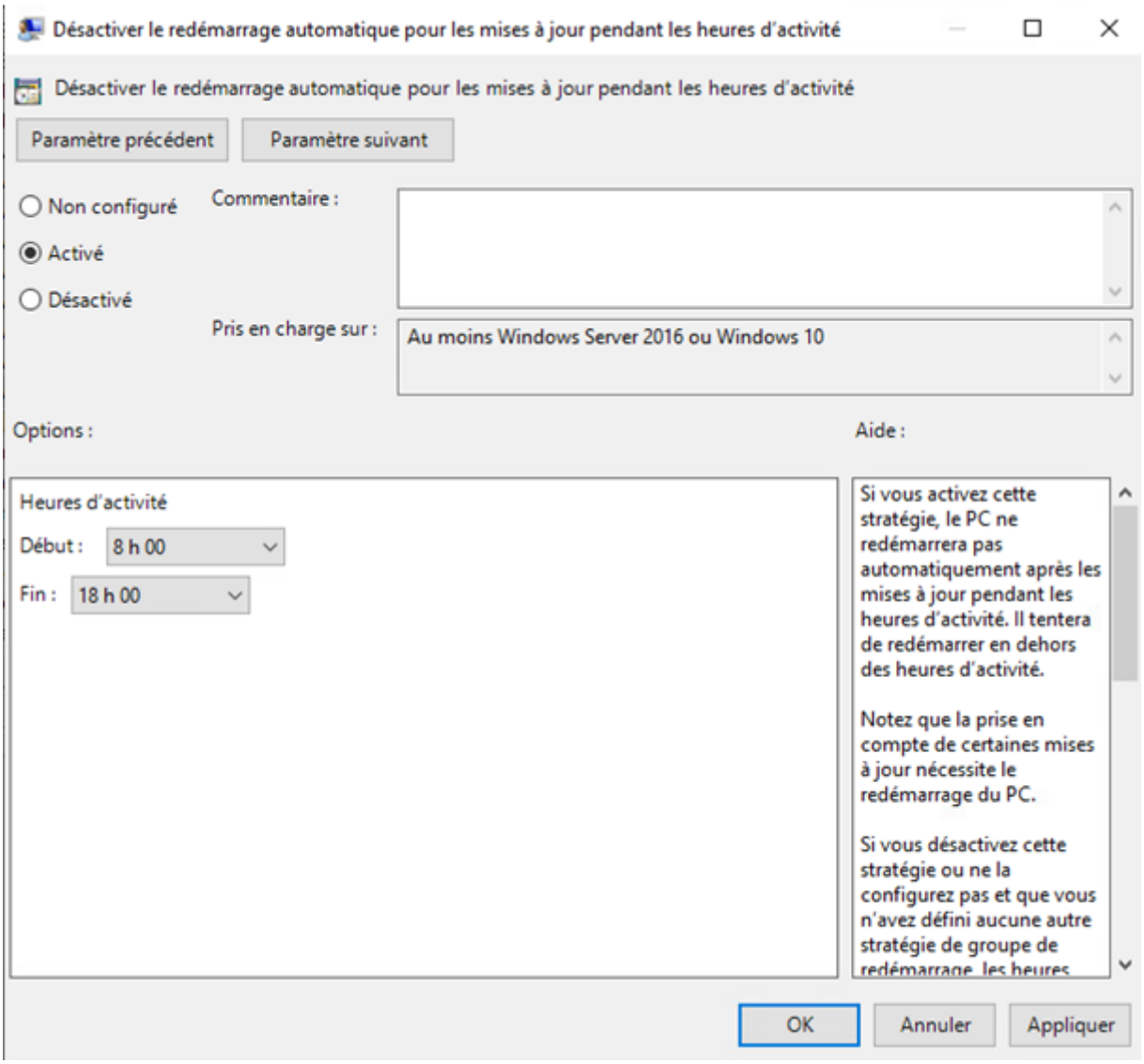


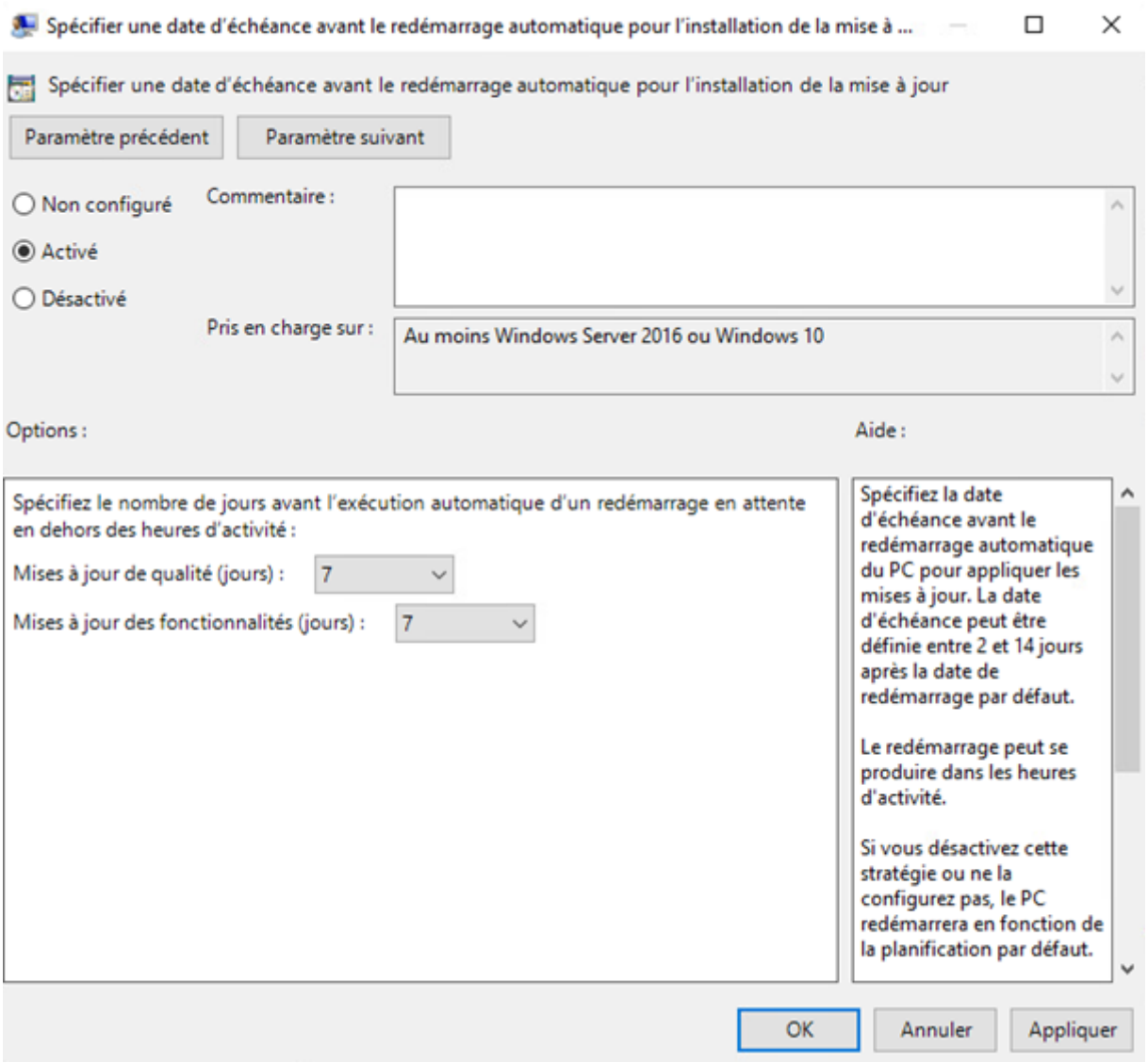
EDIT : la GPO ci-dessous n'a pas le résultat escompté d'après Microsoft. (https://techcommunity.microsoft.com/t5/windows-it-pro-blog/why-you-shouldn-t-set-these-25-windows-policies/ba-p/3066178?WT.mc_id=AZ-MVP-5004580)

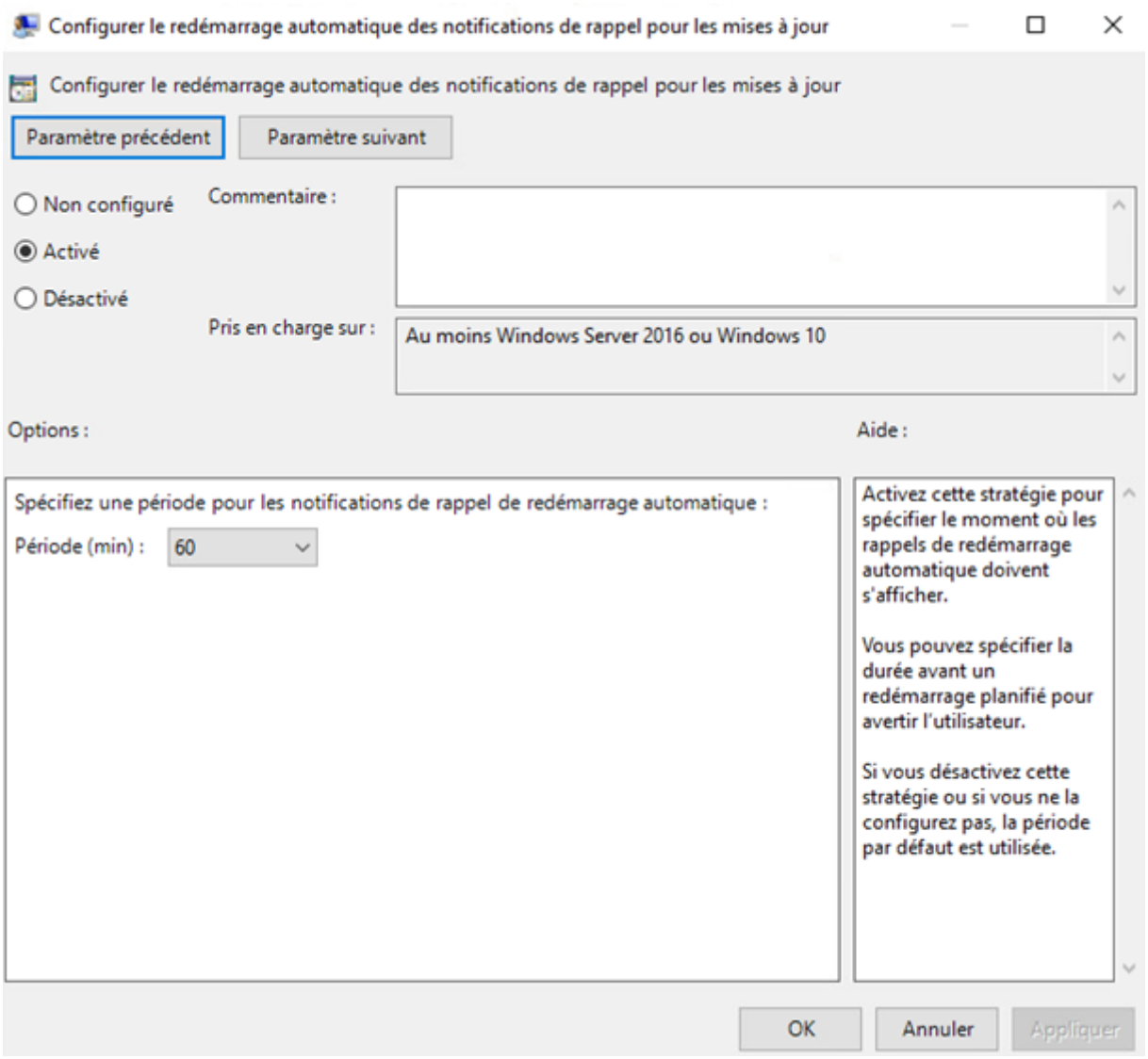
Il faut la remplacer. Voir la page suivante disponible dans ce chapitre :



On adapte ici les heures d'activités.


Désactiver le redémarrage automatique pour les mises à jour pendant les heures d'activité
Désactiver le redémarrage automatique pour les mises à jour pendant les heures d'activité
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au moins Windows Server 2016 ou Windows 10
Options :
Aide :
Heures d'activité
Début : 8 h 00
Fin : 18 h 00
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
OK
Annuler
Appliquer

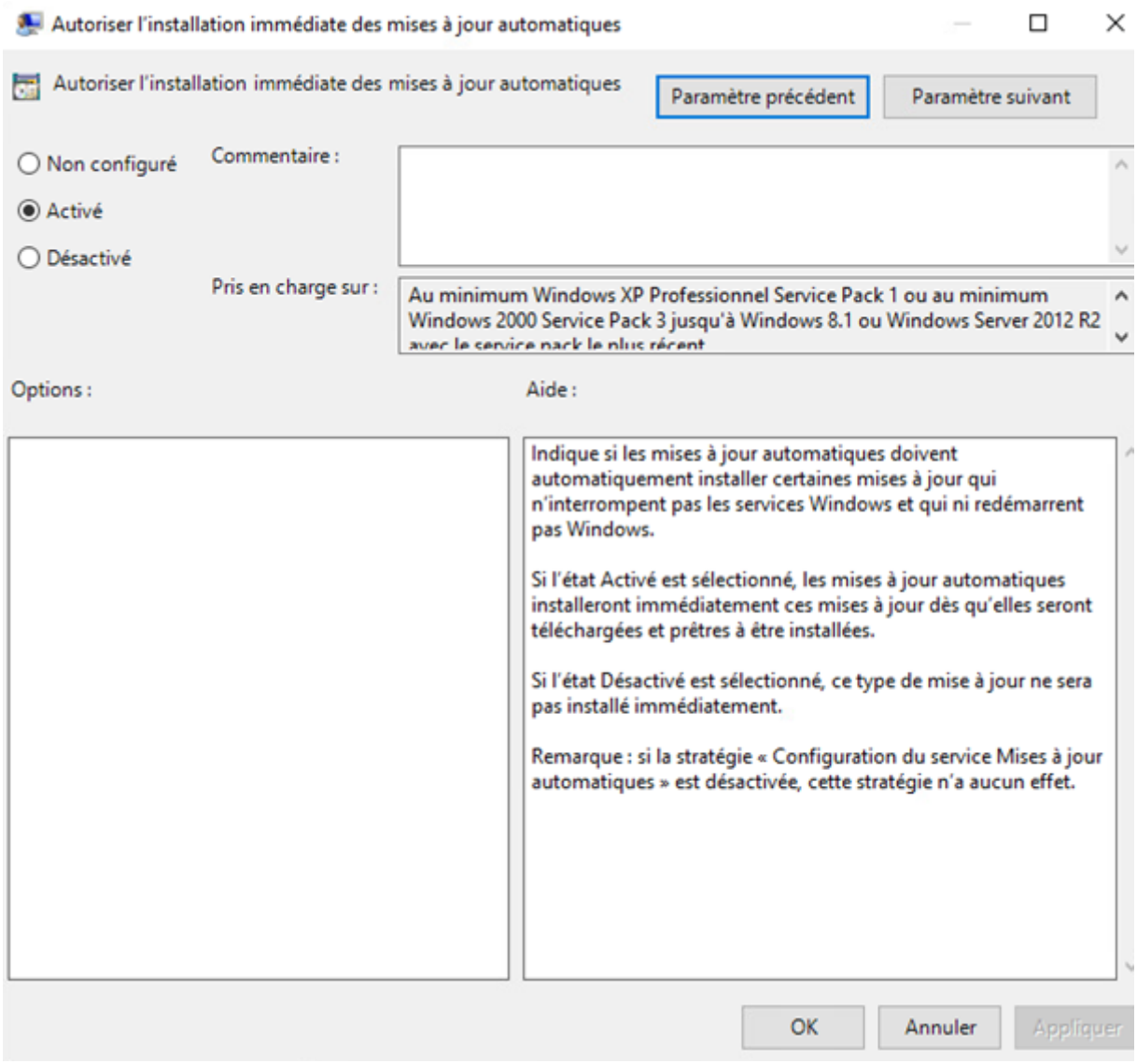

Spécifier une date d'échéance avant le redémarrage automatique pour l'installation de la mise à ...
Spécifier une date d'échéance avant le redémarrage automatique pour l'installation de la mise à jour
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au moins Windows Server 2016 ou Windows 10
Options :
Aide :
Spécifiez le nombre de jours avant l'exécution automatique d'un redémarrage en attente en dehors des heures d'activité :
Mises à jour de qualité (jours) :
7
Mises à jour des fonctionnalités (jours) :
7
Spécifiez la date d'échéance avant le redémarrage automatique du PC pour appliquer les mises à jour. La date d'échéance peut être définie entre 2 et 14 jours après la date de redémarrage par défaut.
Le redémarrage peut se produire dans les heures d'activité.
Si vous désactivez cette stratégie ou ne la configurez pas, le PC redémarrera en fonction de la planification par défaut.
OK
Annuler
Appliquer

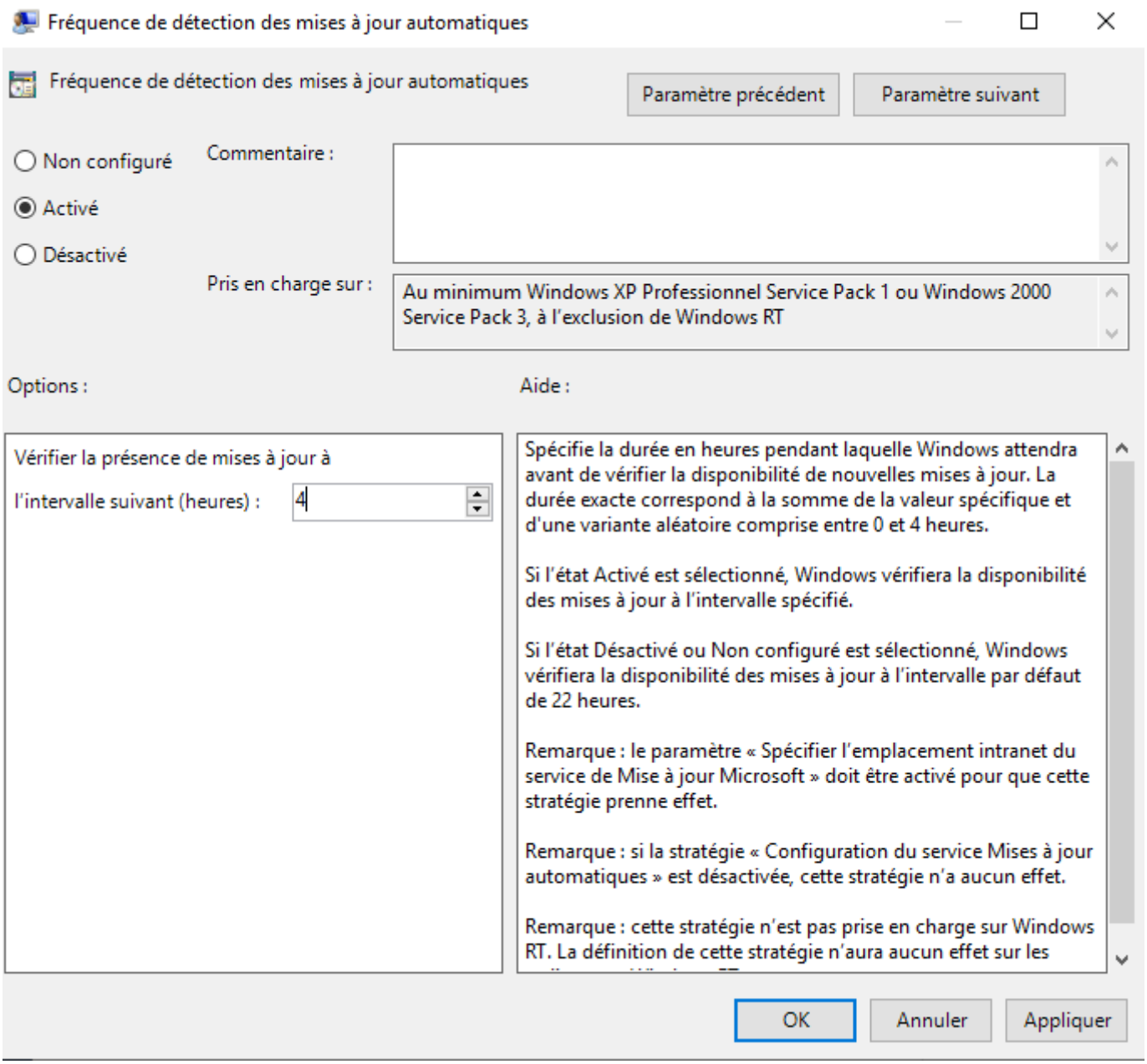


WSUS - Servers

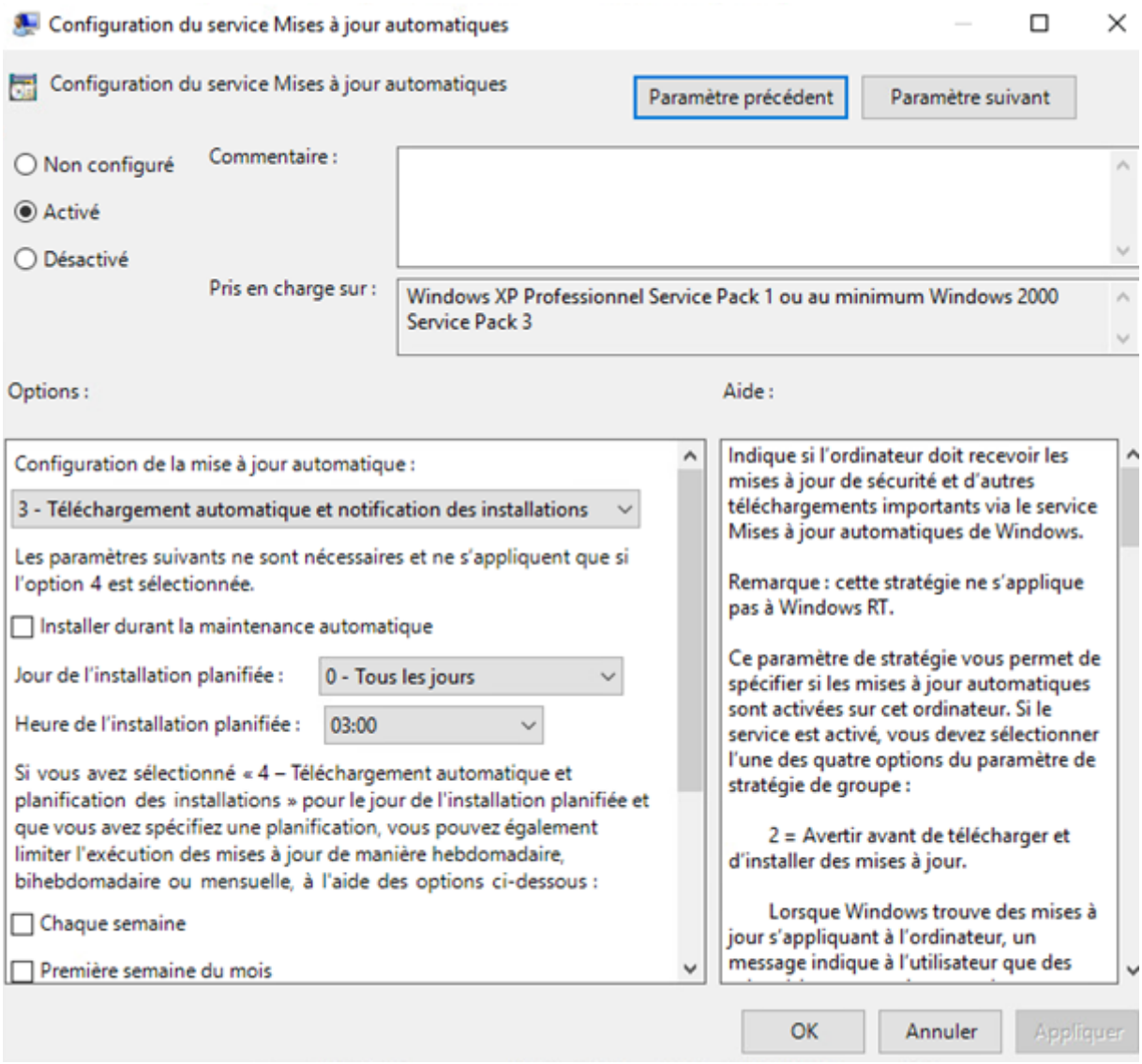
On ne veut pas que les mises à jour s'installent automatiquement sur nos serveurs, sauf pour les mises à jour des définitions de l'antivirus. On va donc activer une option.

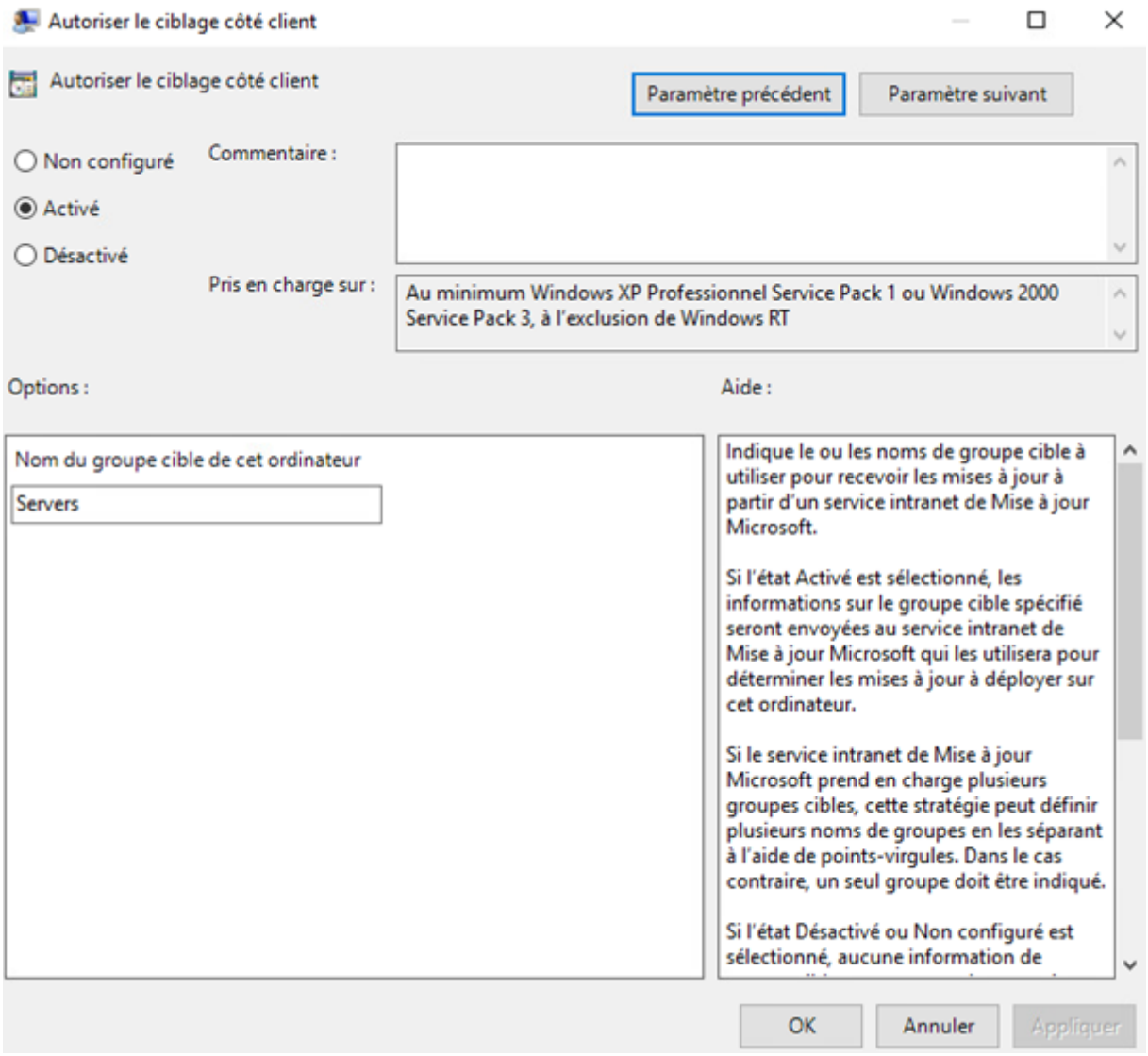
Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Windows Update.


Autoriser l'installation immédiate des mises à jour automatiques
Autoriser l'installation immédiate des mises à jour automatiques
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au minimum Windows XP Professionnel Service Pack 1 ou au minimum Windows 2000 Service Pack 3 jusqu'à Windows 8.1 ou Windows Server 2012 R2
Options :
Aide :
Indique si les mises à jour automatiques doivent automatiquement installer certaines mises à jour qui n'interrompent pas les services Windows et qui ni redémarrent pas Windows.
Si l'état Activé est sélectionné, les mises à jour automatiques installeront immédiatement ces mises à jour dès qu'elles seront téléchargées et prêtres à être installées.
Si l'état Désactivé est sélectionné, ce type de mise à jour ne sera pas installé immédiatement.
Remarque : si la stratégie « Configuration du service Mises à jour automatiques » est désactivée, cette stratégie n'a aucun effet.
OK
Annuler
Appliquer



Ensuite, pour les autres options :


Configuration du service Mises à jour automatiques
Configuration du service Mises à jour automatiques
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Windows XP Professionnel Service Pack 1 ou au minimum Windows 2000 Service Pack 3
Options :
Aide :
Configuration de la mise à jour automatique :
3 - Téléchargement automatique et notification 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 :
03:00
Si vous avez sélectionné « 4 – Téléchargement automatique et planification des installations » pour le jour de l'installation planifiée et que vous avez 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
Indique si l'ordinateur doit recevoir les mises à jour de sécurité et d'autres téléchargements importants via le service Mises à jour automatiques de Windows.
Remarque : cette stratégie ne s'applique pas à Windows RT.
Ce paramètre de stratégie vous permet de spécifier si les mises à jour automatiques sont activées sur cet ordinateur. Si le service est activé, vous devez sélectionner l'une des quatre options du paramètre de stratégie de groupe :
2 = Avertir avant de télécharger et d'installer des mises à jour.
Lorsque Windows trouve des mises à jour s'appliquant à l'ordinateur, un message indique à l'utilisateur que des
OK
Annuler
Appliquer



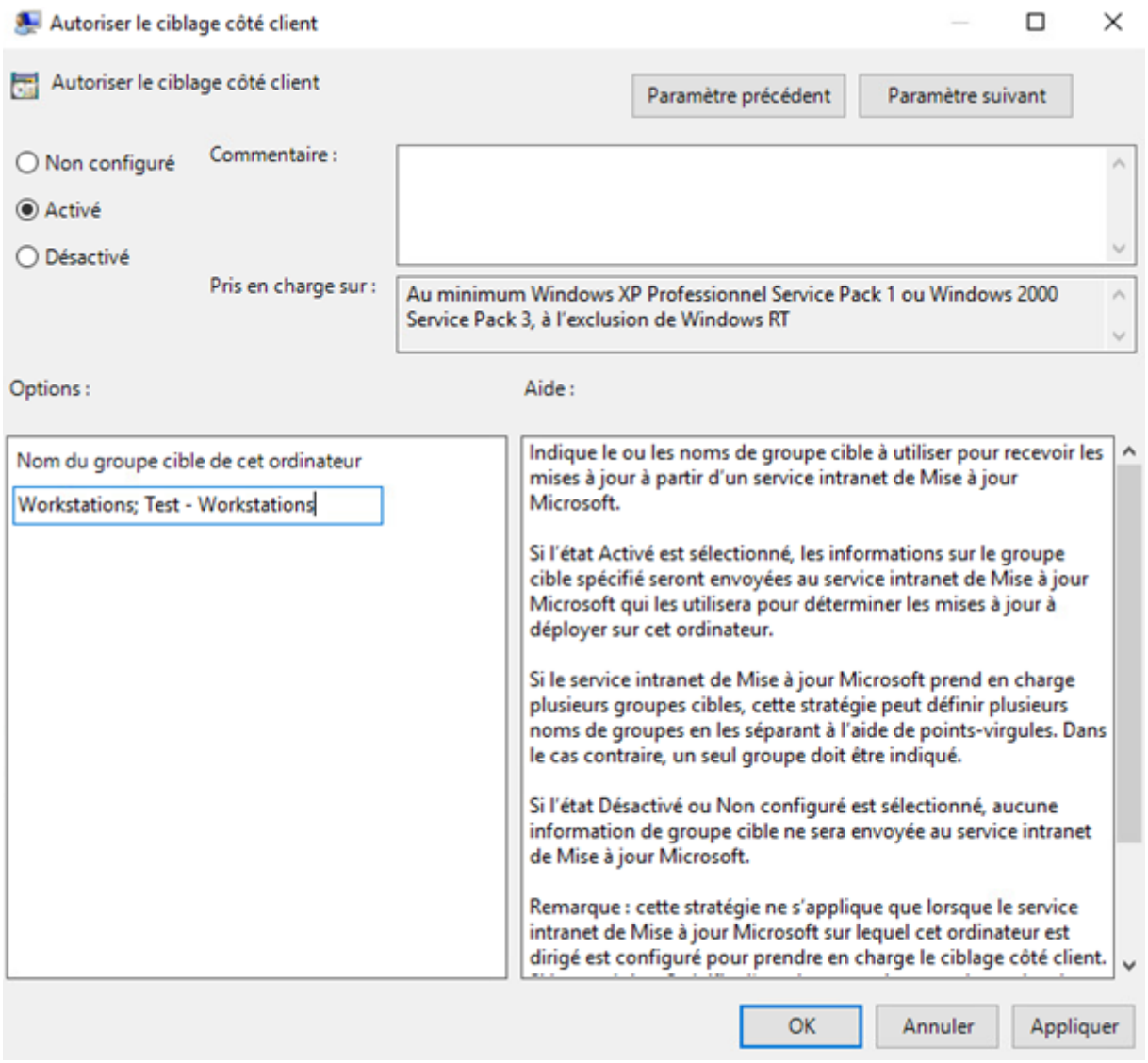
Si on a une farm de serveurs, il est préférable de créer plusieurs 'anneaux' de planifications et groupes, en choisissant l'option 4 : "Téléchargement automatique et planifier l'installation" et forcer le redémarrage lors de la maintenance des serveurs.

Pour conclure, ici les mises à jour seront téléchargées automatiquement sur les serveurs, mais ne seront pas installées automatiquement, à l'exception de Windows Defender.

WSUS - Workstations, Test - Workstations

C'est une GPO pour le groupe de ciblage.

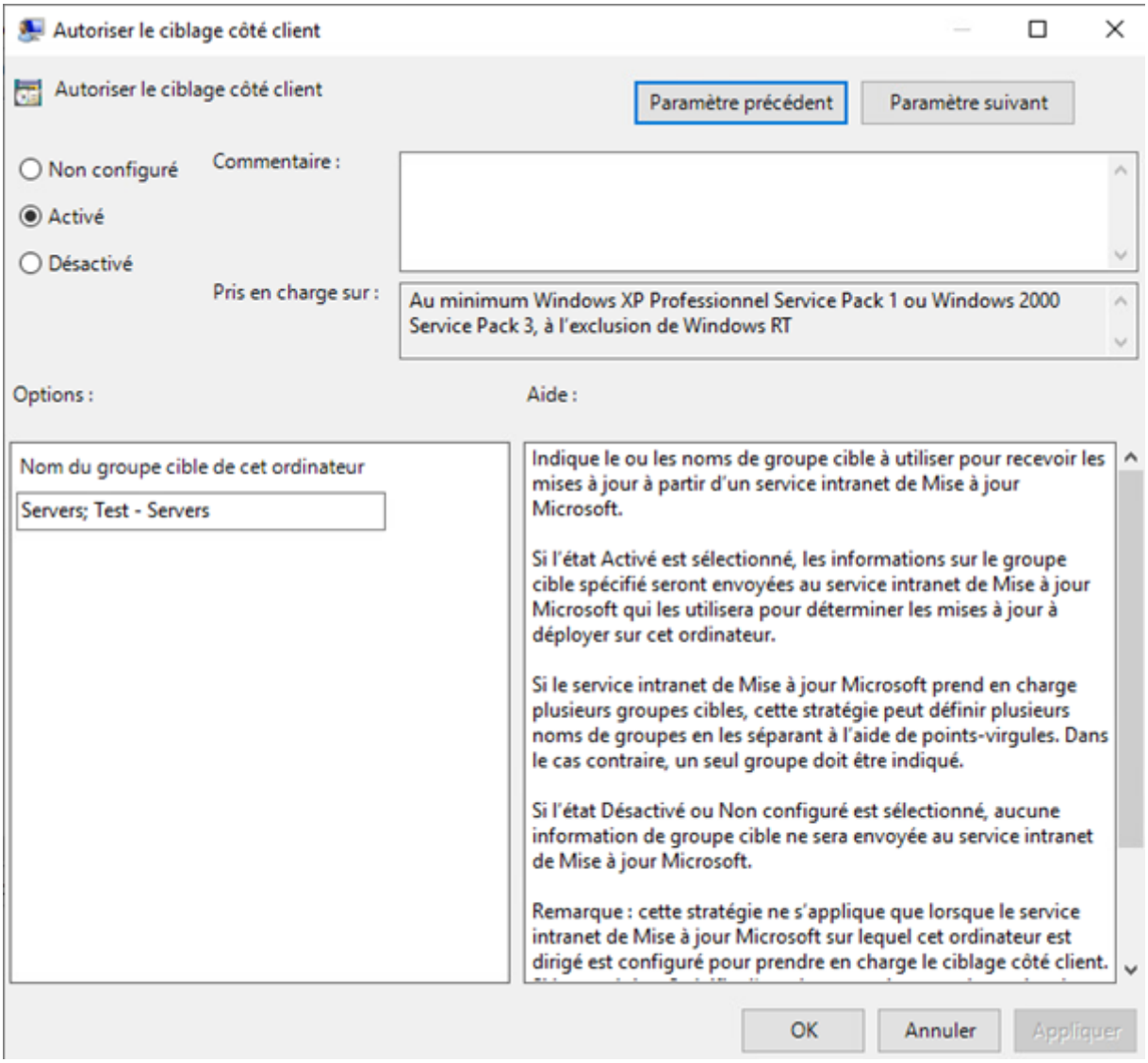
Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Windows Update



WSUS - Servers, Test - Servers

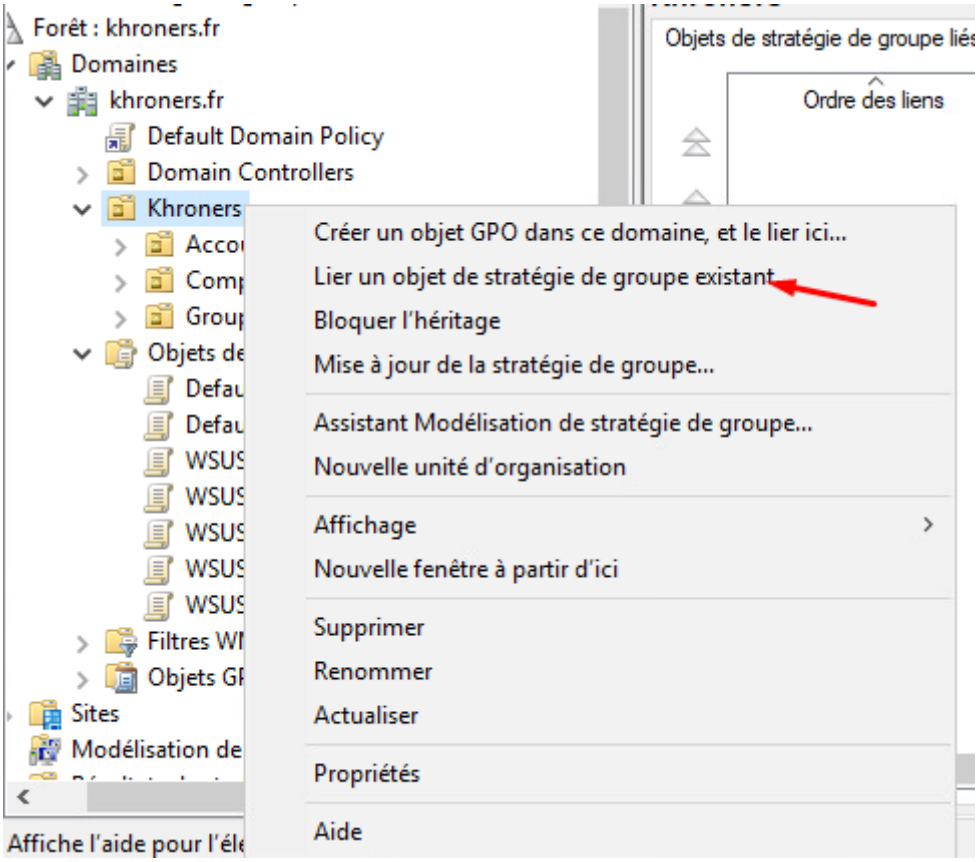
C'est une GPO pour le groupe de ciblage.

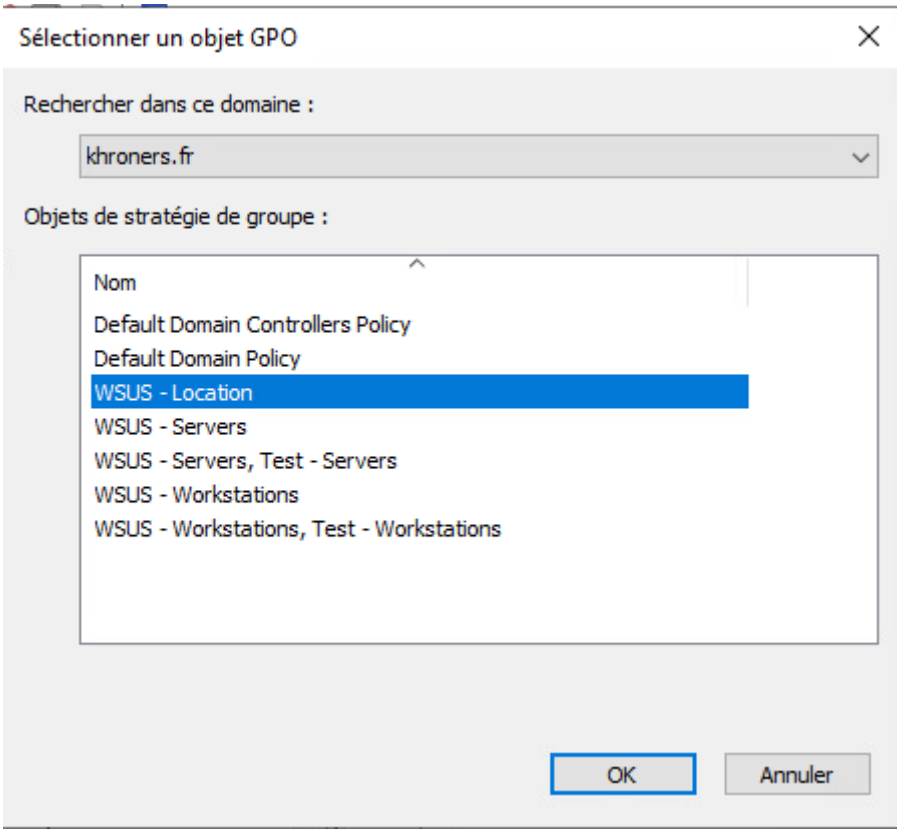
Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Windows Update



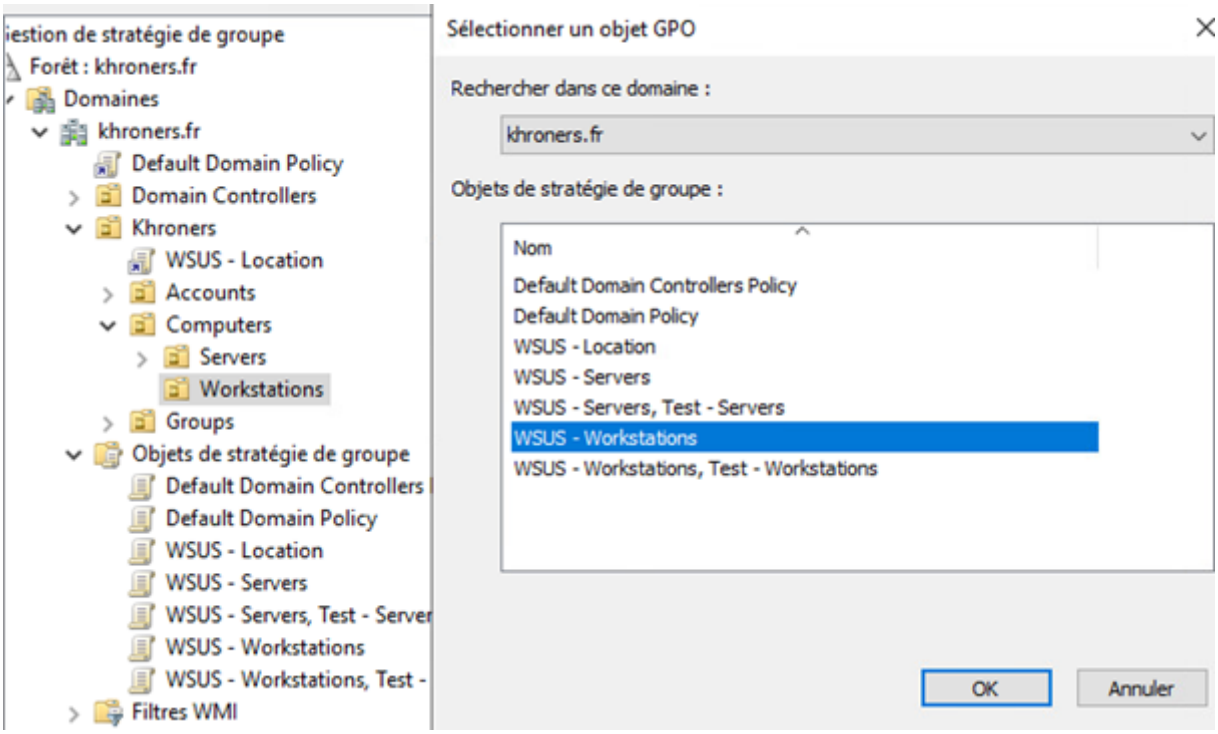
Lier les GPO aux bonnes OU

On applique la GPO de l'emplacement à toute l'OU.

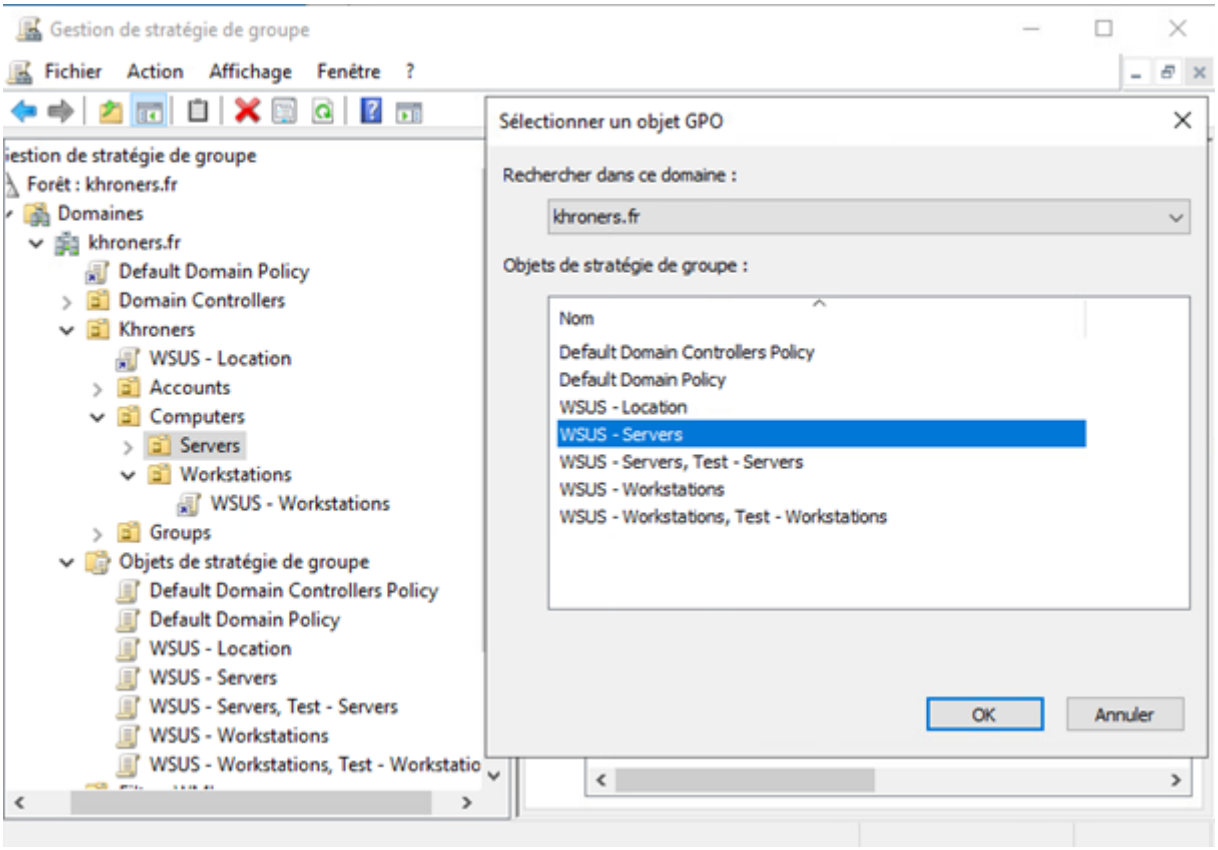




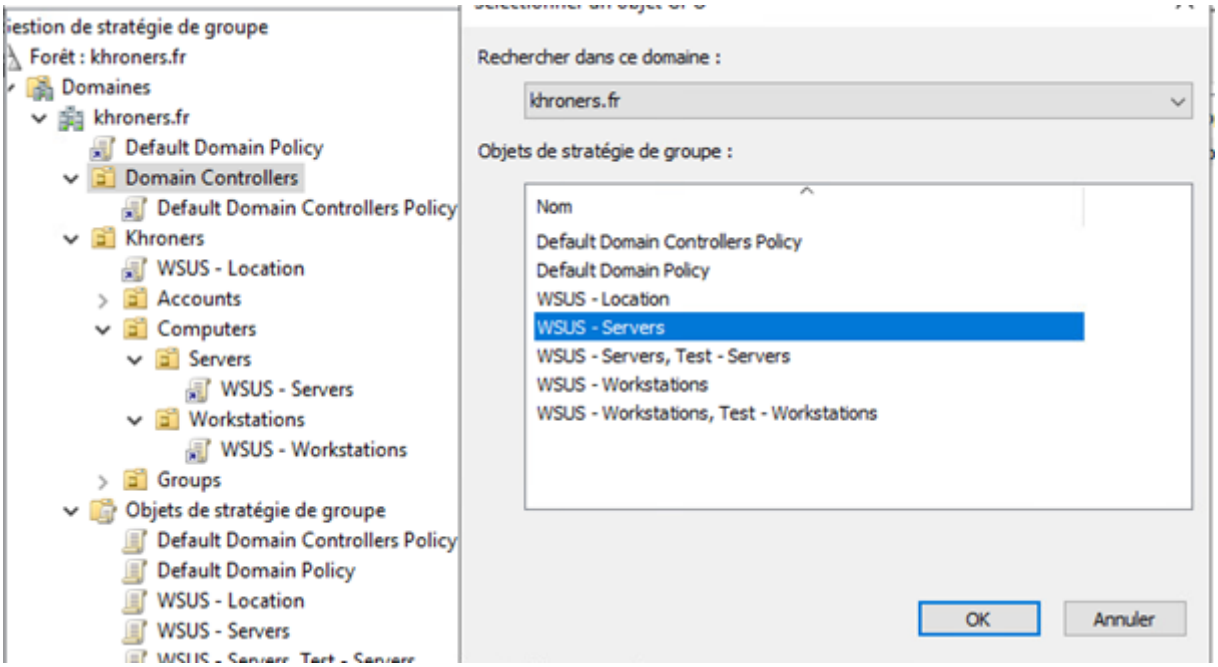
On applique pour les postes de travails la GPO correspondante.



De même pour les serveurs.



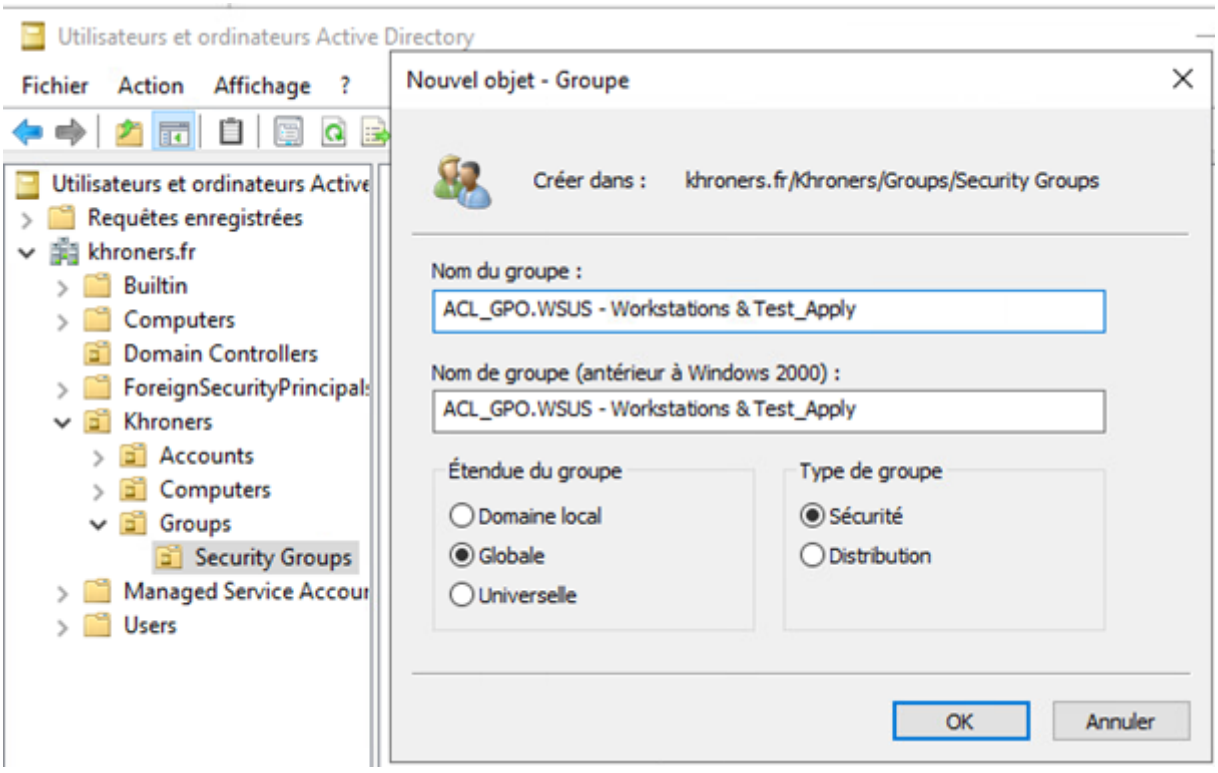
On n'oublie pas les contrôleurs de domaine.



Création des groupes de tests

On va créer 4 groupes dans l'OU "Security Groups".

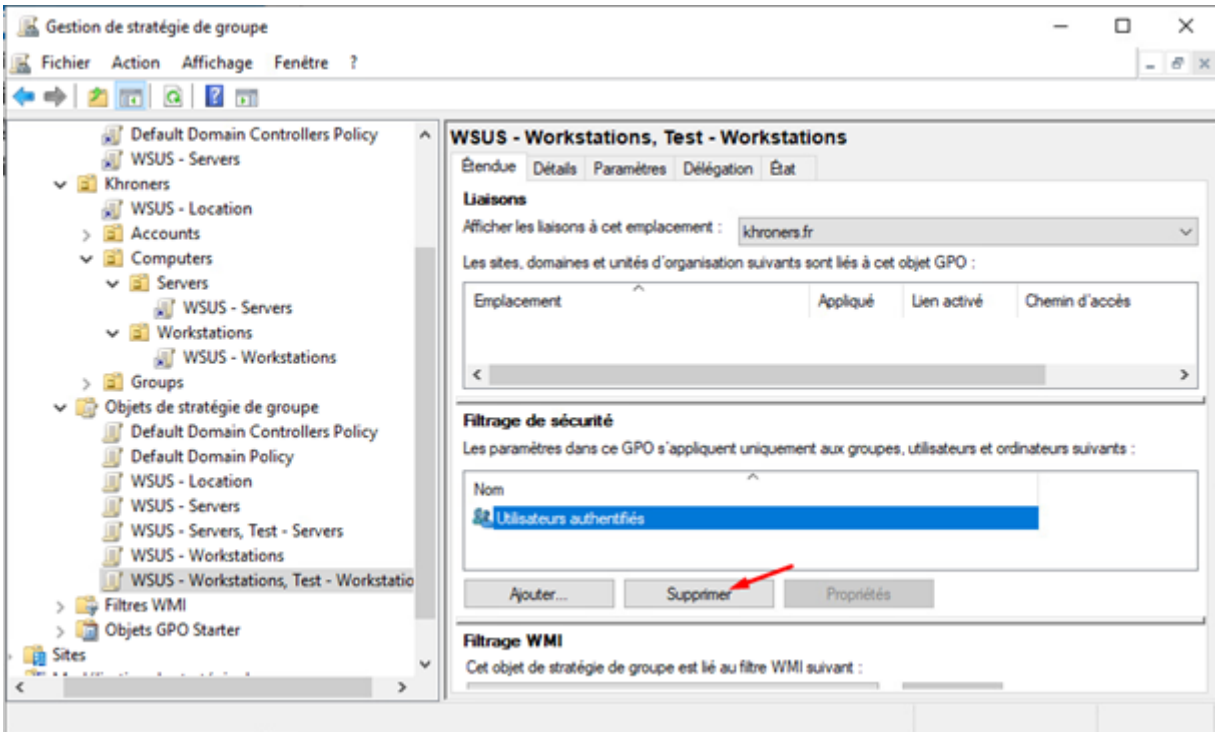
- ACL_GPO.WSUS - Workstations & Test_Apply
- ACL_GPO.WSUS - Workstations & Test_Deny
- ACL_GPO.WSUS - Servers & Test_Apply
- ACL_GPO.WSUS - Servers & Test_Deny



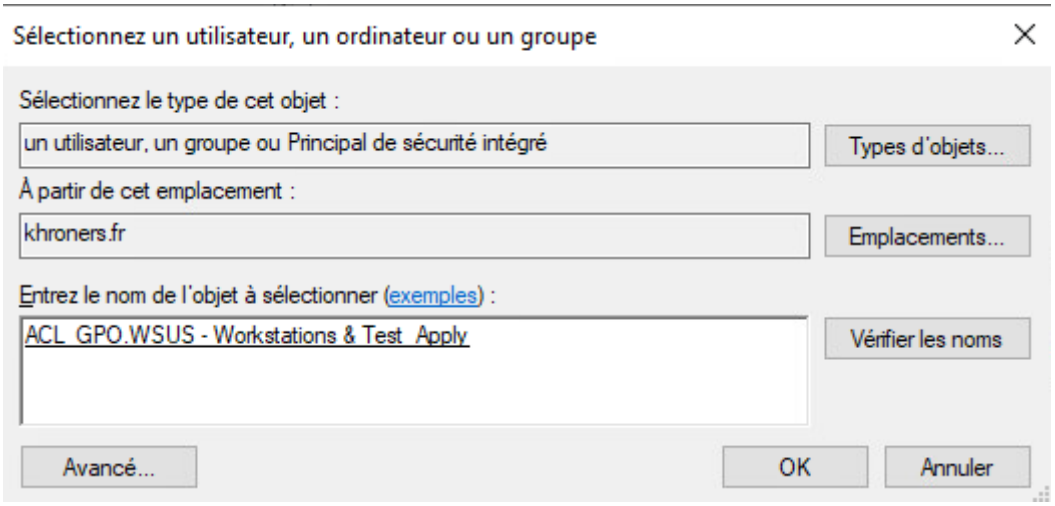
On fait la même chose pour les 3 autres groupes à créer.

Nom	Type
ACL_GPO.WSUS - Servers & Test_Apply	Groupe de séc...
ACL_GPO.WSUS - Servers & Test_Deny	Groupe de séc...
ACL_GPO.WSUS - Workstations & Test_Apply	Groupe de séc...
ACL_GPO.WSUS - Workstations & Test_Deny	Groupe de séc...

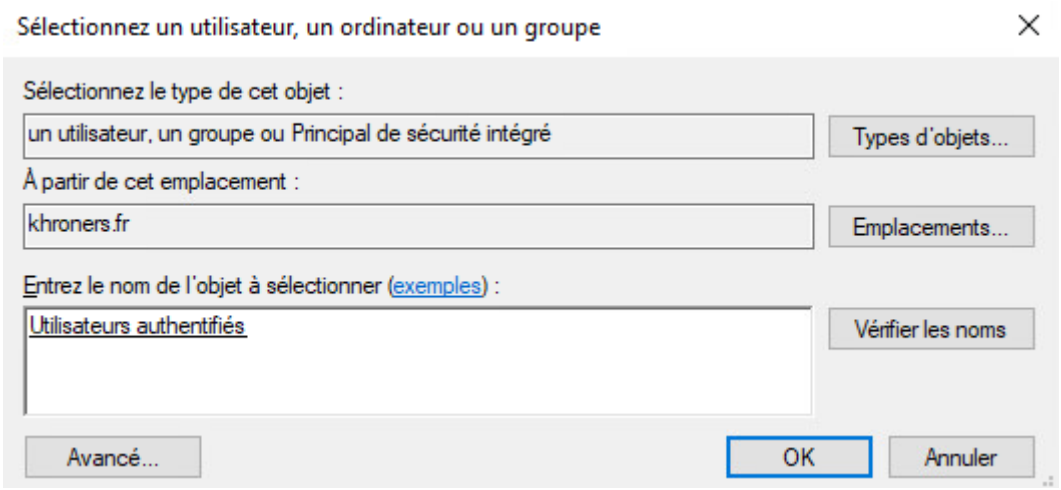
Dans la console de Gestion de stratégie de groupe, on clique sur la GPO "WSUS - Workstations, Test - Workstations", dans la partie "Filtrage de sécurité", on supprime "Utilisateurs authentifiés".

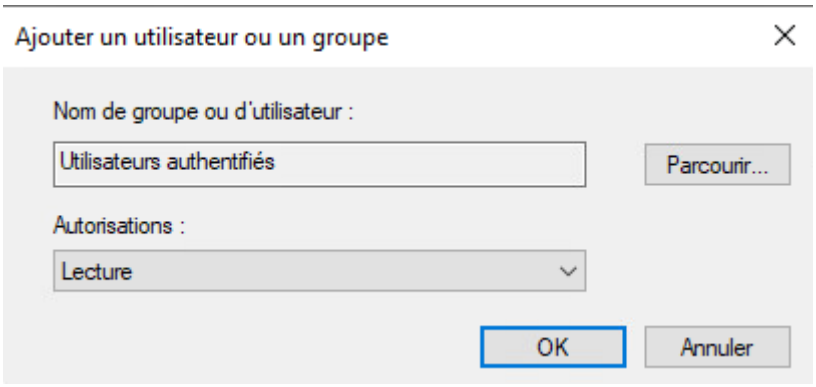


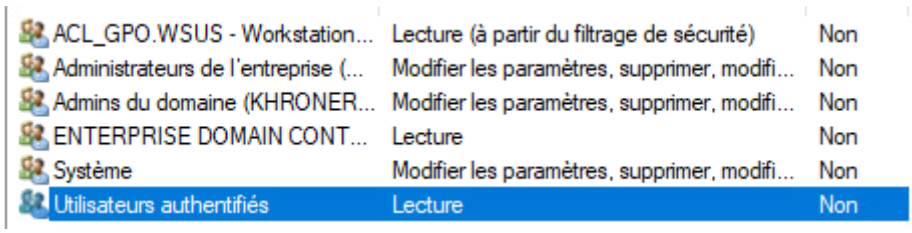
On clique ensuite sur "Ajouter..." puis on ajoute le groupe "ACL_GPO.WSUS - Workstations & Test_Apply".



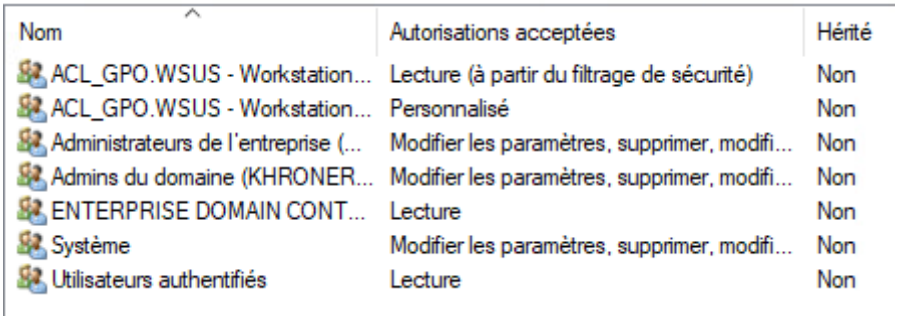
Dans l'onglet Délégation, on ajoute « Utilisateurs authentifiés » en lecture.







On clique sur Avancé et on ajoute ACL_GPO.WSUS – Workstations & Test_Deny avec les permissions refusées.



On fait la même chose pour l'autre GPO pour les tests sur serveurs (WSUS - Servers, Test - Servers) avec les deux groupes ACL.

Approbation des mises à jour

Présentation

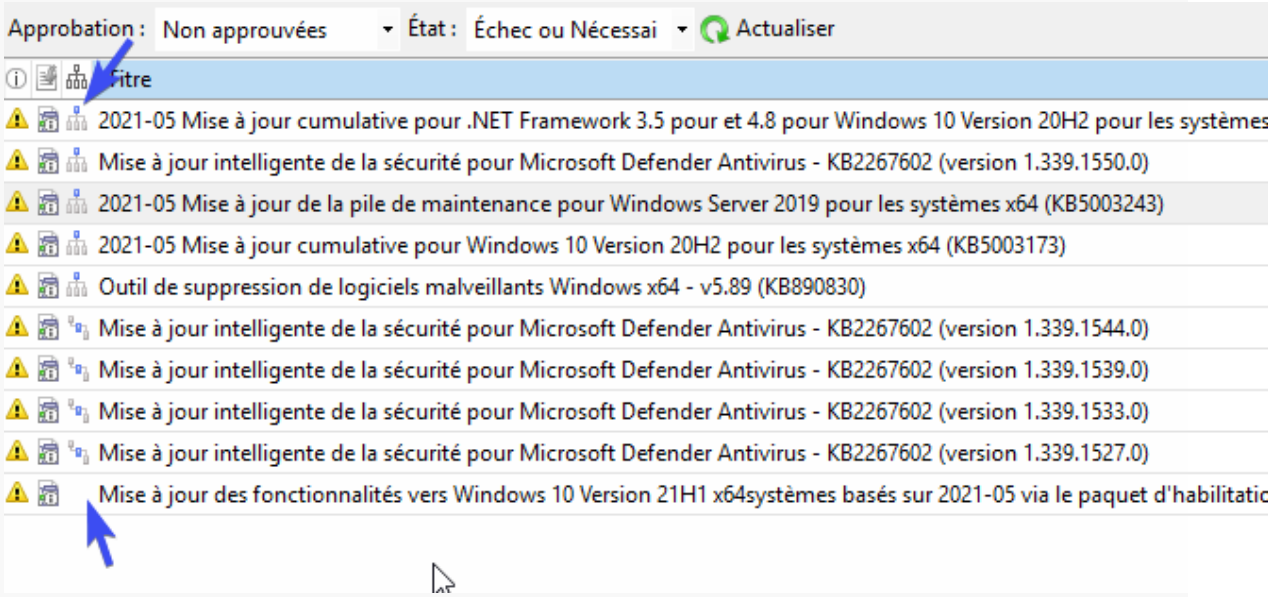
Il est désormais nécessaire d'approuver les mises à jour manuellement. Il ne faut pas accepter toutes les mises à jour, automatiquement, sans se renseigner et les tester sur le parc informatique.

Approbation

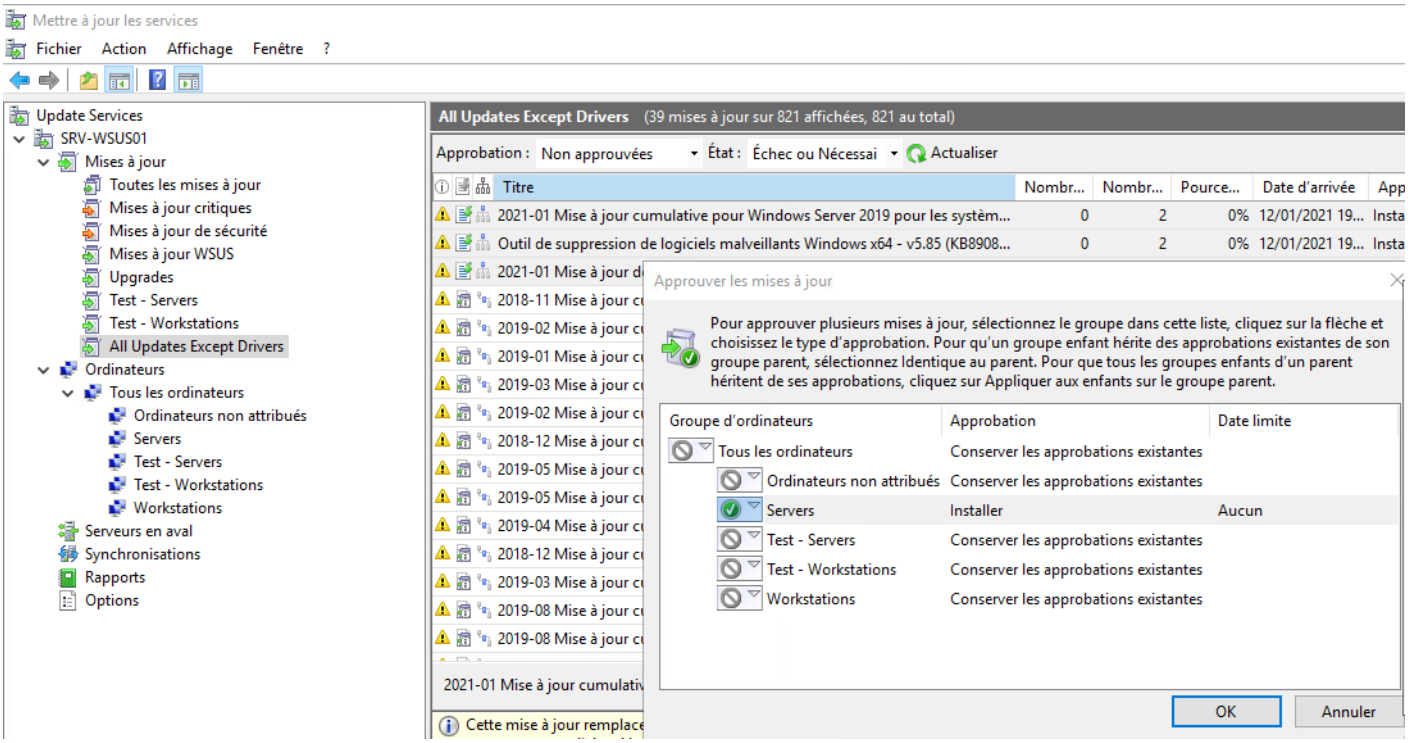
Dans "All Updates Except Drivers", on choisit les mises à jour que l'on veut approuver puis on clique droit, et "Approuver". On sélectionne le groupe d'ordinateurs. Ici, serveurs.

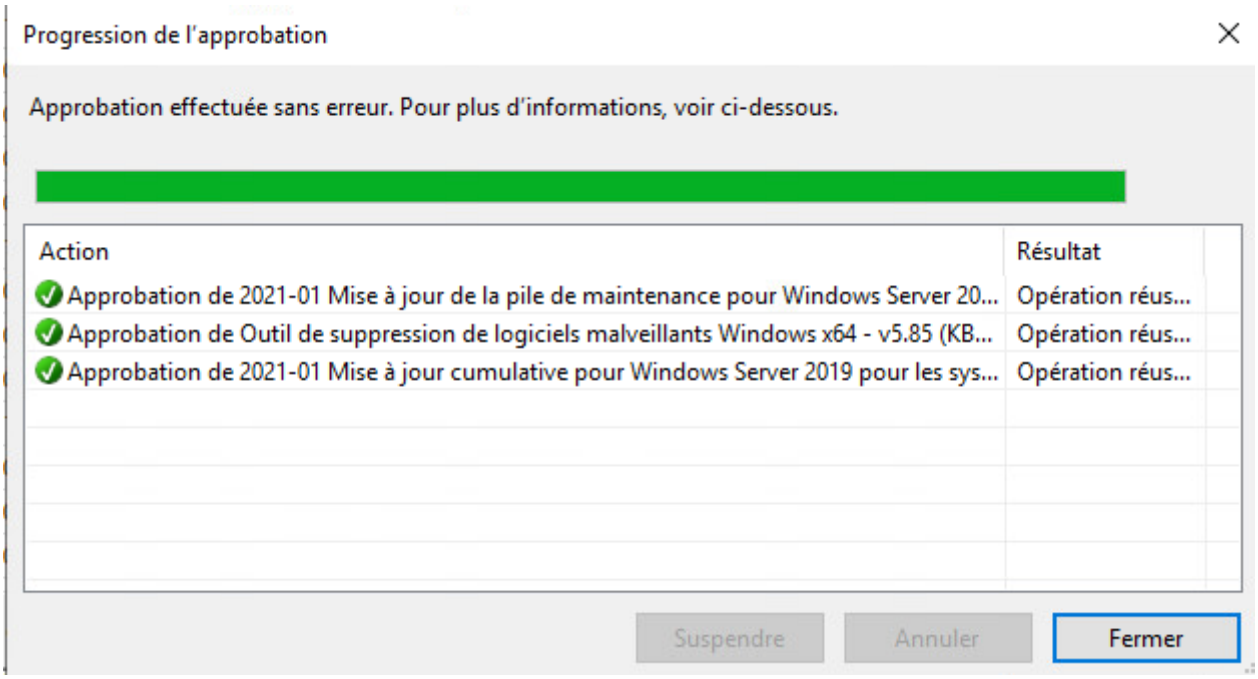
Les mises à jour que l'on souhaite approuver sont celles qui remplacent les anciennes, et celle qui n'ont pas été remplacées et qui n'en remplacent aucune (il n'y aura donc pas d'icône dans la colonne "Remplacement".

Celles-ci par exemple :



Il est préférable d'avoir un groupe de test pour les grosses mises à jour (2004, 20H2, 21H1 par exemple) pour voir leur comportement sur les postes du parc.

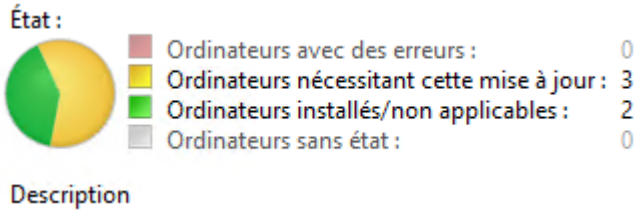




Installation du runtime Microsoft Report Viewer

Présentation

Avant l'approbation d'une mise à jour, on peut voir quels ordinateurs ont besoin de cette mise à jour.



Cependant, s'il ont clique, il est nécessaire d'avoir "Microsoft Report Viewer 2012 runtime".

Installation

> **Attention :** avant l'installation, il faut fermer la console WSUS.

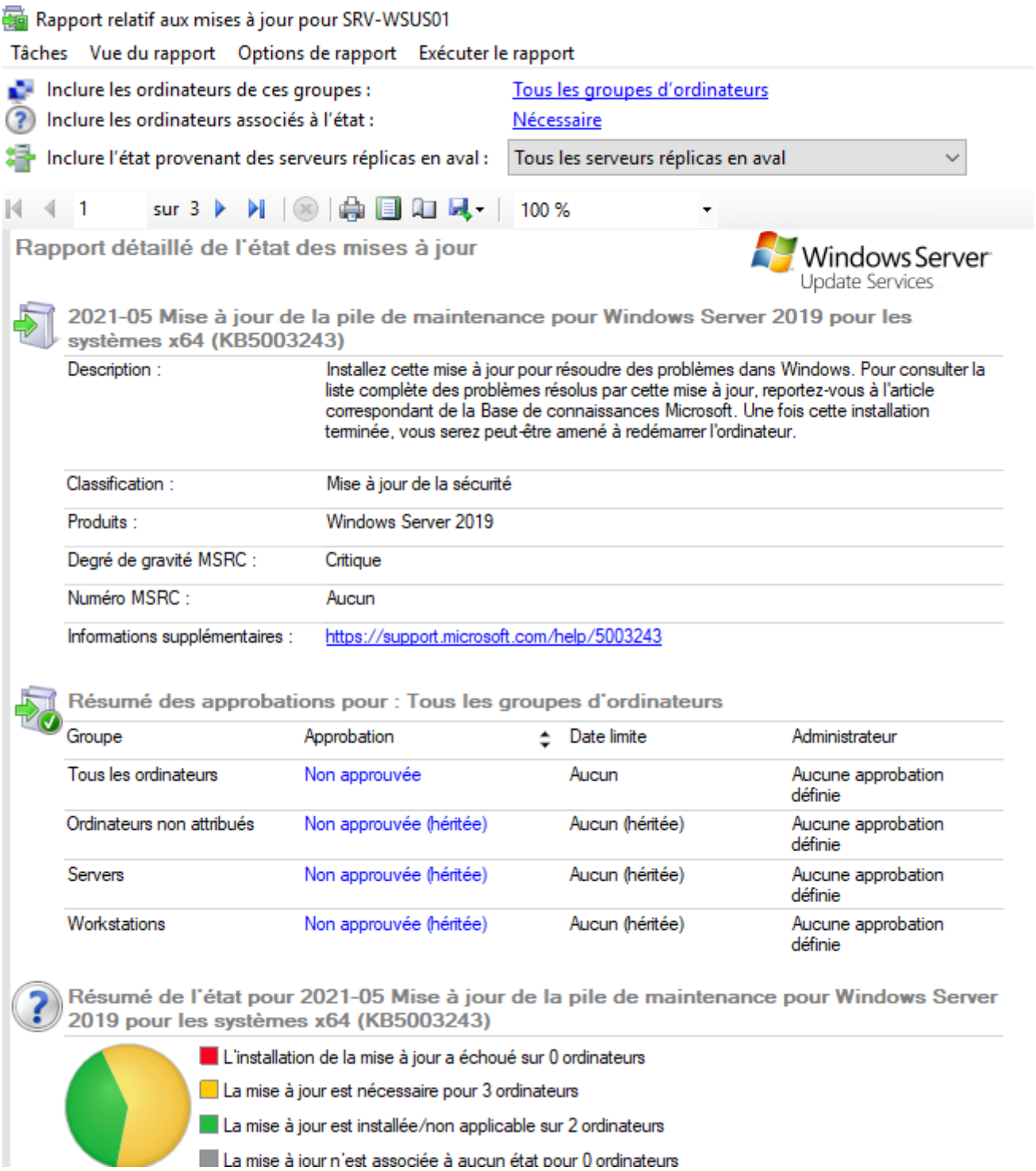
Avant son installation, il faut installer "Microsoft System CLR Types for Microsoft SQL Server 2012".

Sur cette page, dans la partie "Install Instructions", on choisit "Microsoft® System CLR Types for Microsoft® SQL Server® 2012" et on télécharge la version x64 puis on l'installe.

On installe ensuite "Microsoft Report Viewer 2012 Runtime".

Conclusion

Désormais, en cliquant, la fenêtre de rapport s'ouvre.



On trouve bien les ordinateurs ayant besoin de cette mise à jour.

Approbation automatique des mises à jour de définition (Windows Defender)

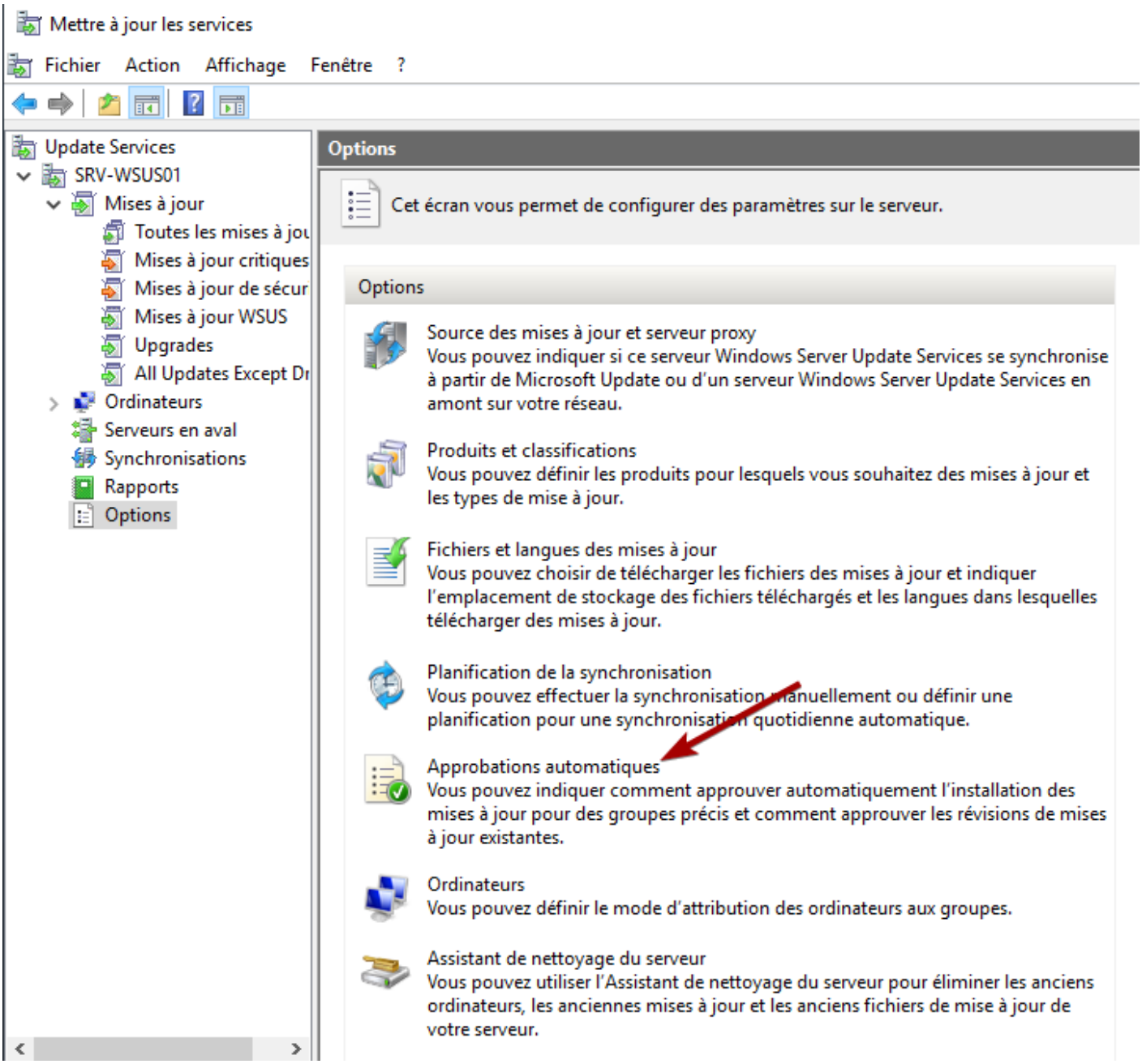
Présentation

Il est important d'approuver automatiquement les mises à jour de définition de Windows Defender, dans le but d'avoir l'anti-virus à jour et donc protégé au mieux le parc.

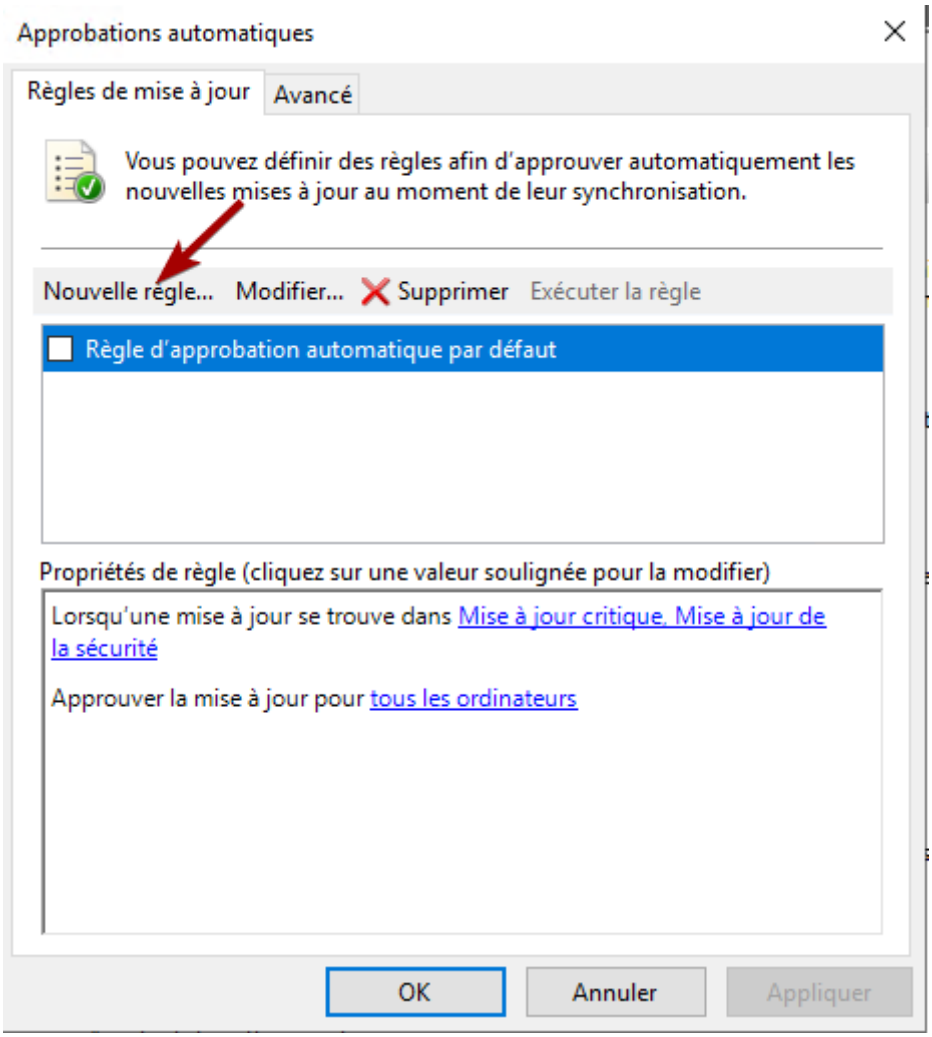
> En soit, déployer via WSUS les mises à jour de Defender n'est pas primordial. A chaque mise à jour, WSUS retélécharge tout (60-70mo en moyenne pour le moment), alors que de passer d'une mise à jour à une autre prend environ 1mo, selon la mise à jour des définitions.
> Cela peut être utile en cas de déploiement massif d'appareils, pour éviter que tous les postes, lors du déploiement, téléchargent chacun les définitions.

Approbation automatique

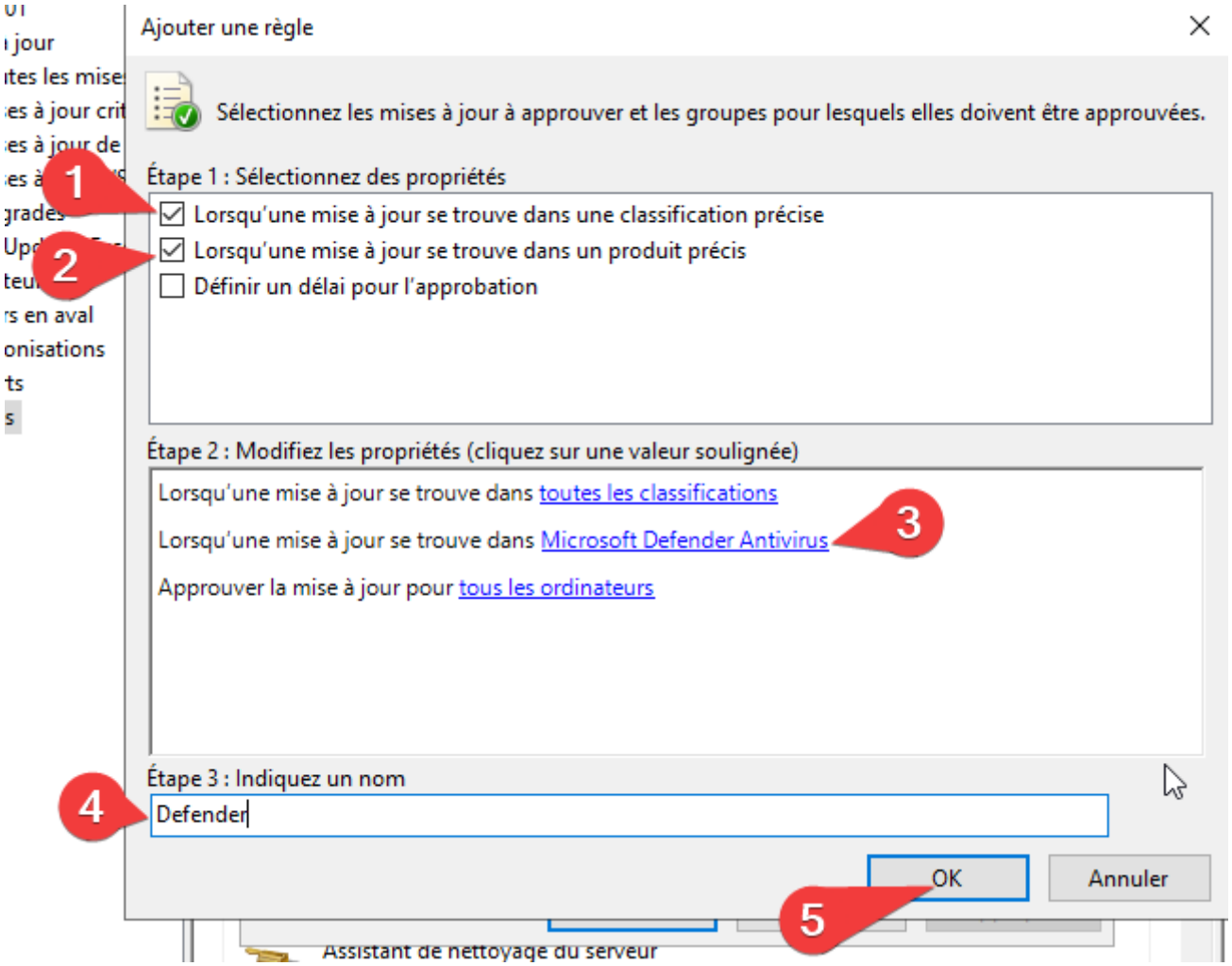
Dans la console WSUS, on se rend dans Options, puis Approbations automatiques.



On crée une nouvelle règle.



On coche les deux premières cases, on choisit Microsoft Defender Antivirus, puis on donne un nom à la règle.



Conclusion

Ainsi, à chaque synchronisation et ajout d'une mise à jour de définition de Microsoft Defender Antivirus, elle sera automatiquement approuvée par le serveur WSUS.

Mise en place du TLS/SSL pour WSUS

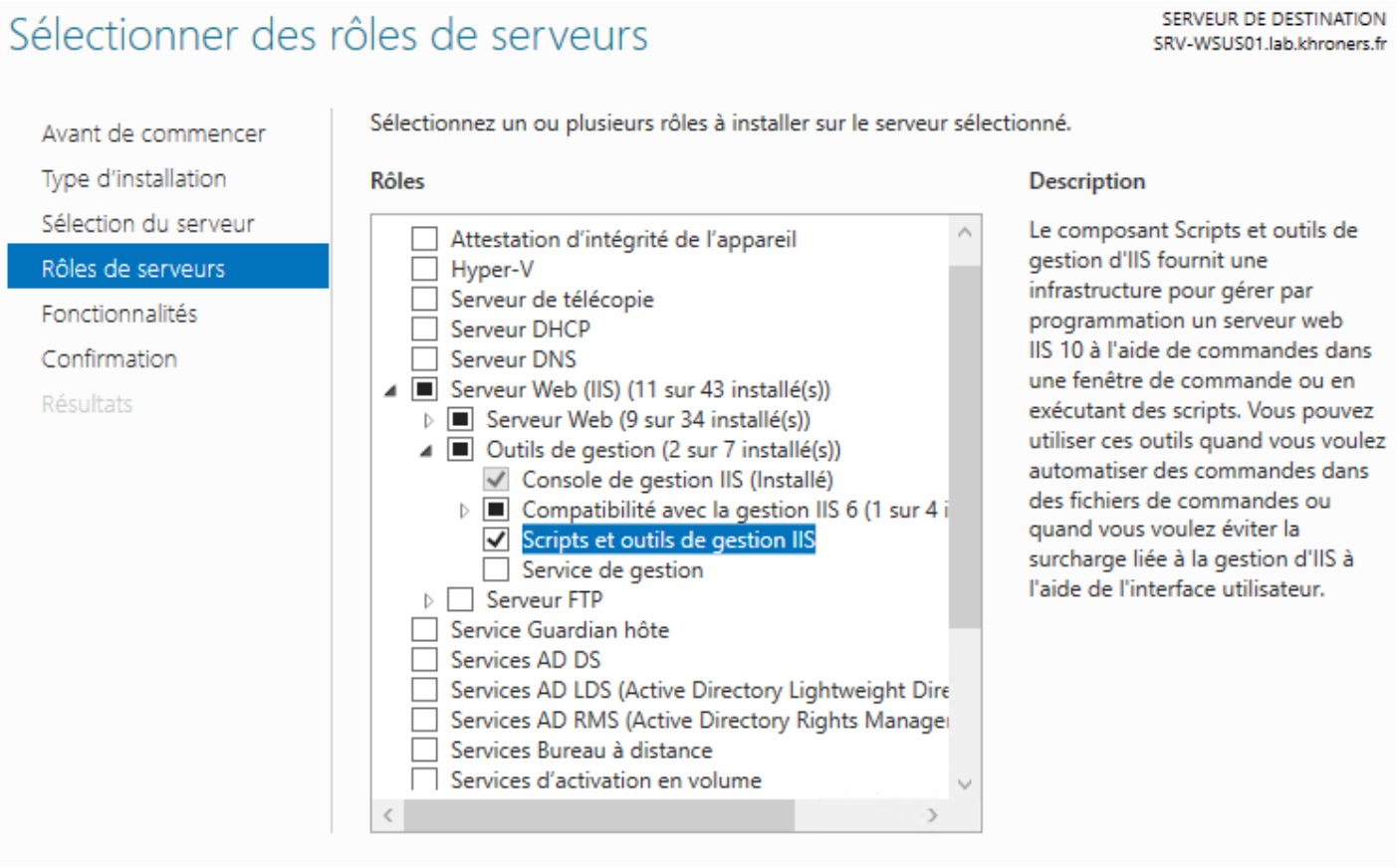
Présentation

Par défaut, WSUS ne chiffre pas les données. De nombreuses failles ont été découvertes, et pour les corriger, il faut activer le SSL. Pour cela, on aura besoin de modifier la GPO de l'emplacement du WSUS (remplacer http:// par https:///) et d'ajouter un certificat.
Un exemple de l'importance du SSL :

Vidéo YouTube faite par 2 intervenants au Black Hat

> La mise en place du SSL demandera plus de performance sur le serveur, dû au chiffrement.

> Pour la suite, il est nécessaire d'avoir de nombreux modules, comme "Scripts et outils de gestion IIS", GroupPolicy.



Activation du SSL sur WSUS

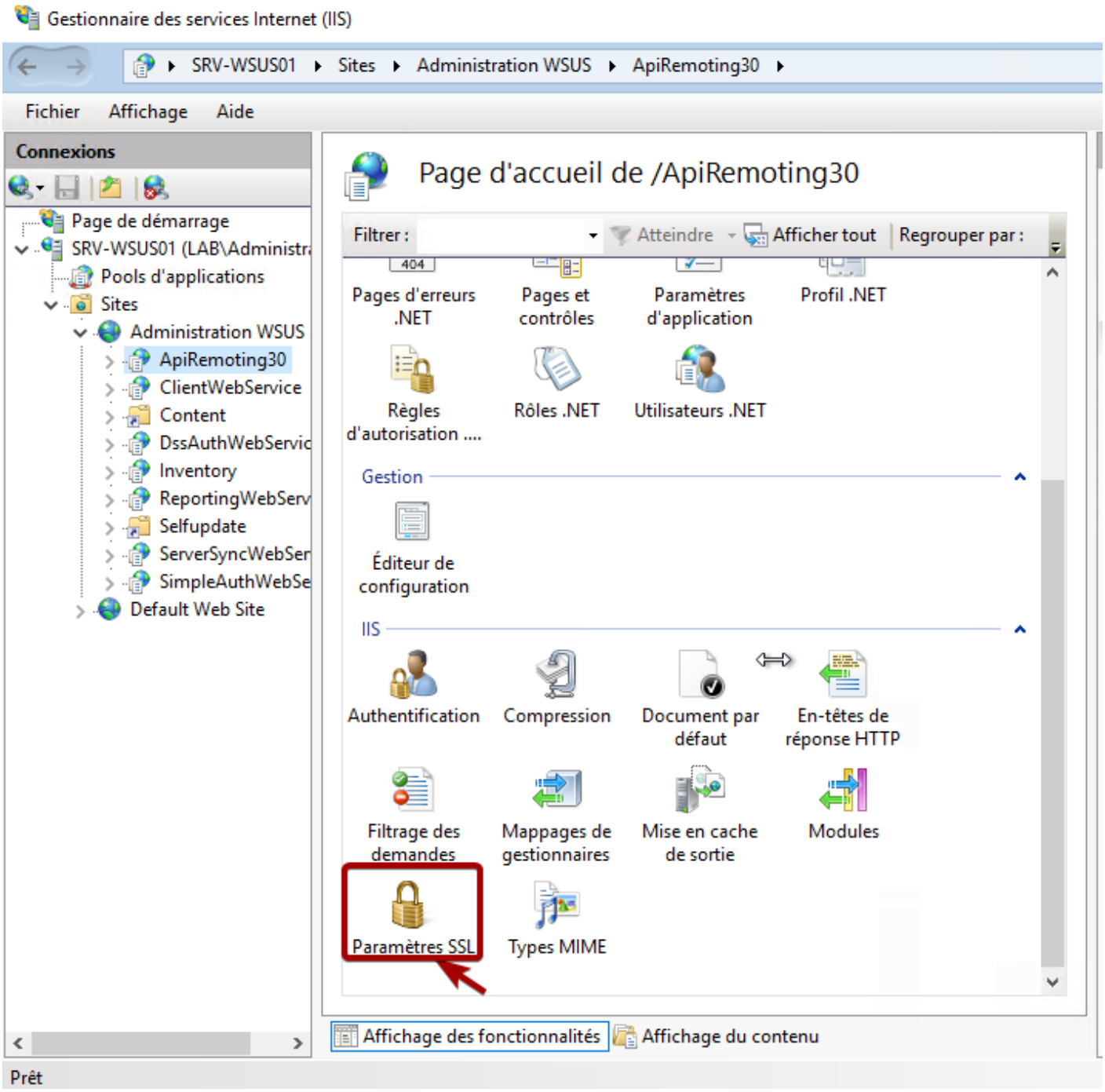
Dans mon cas, j'ai récupéré le certificat et la clé privée depuis mon serveur web (fullchain.pem et privkey.pem). J'ai converti en .pfx. Une page est disponible pour cela. De plus j'ai défini un mot de passe.

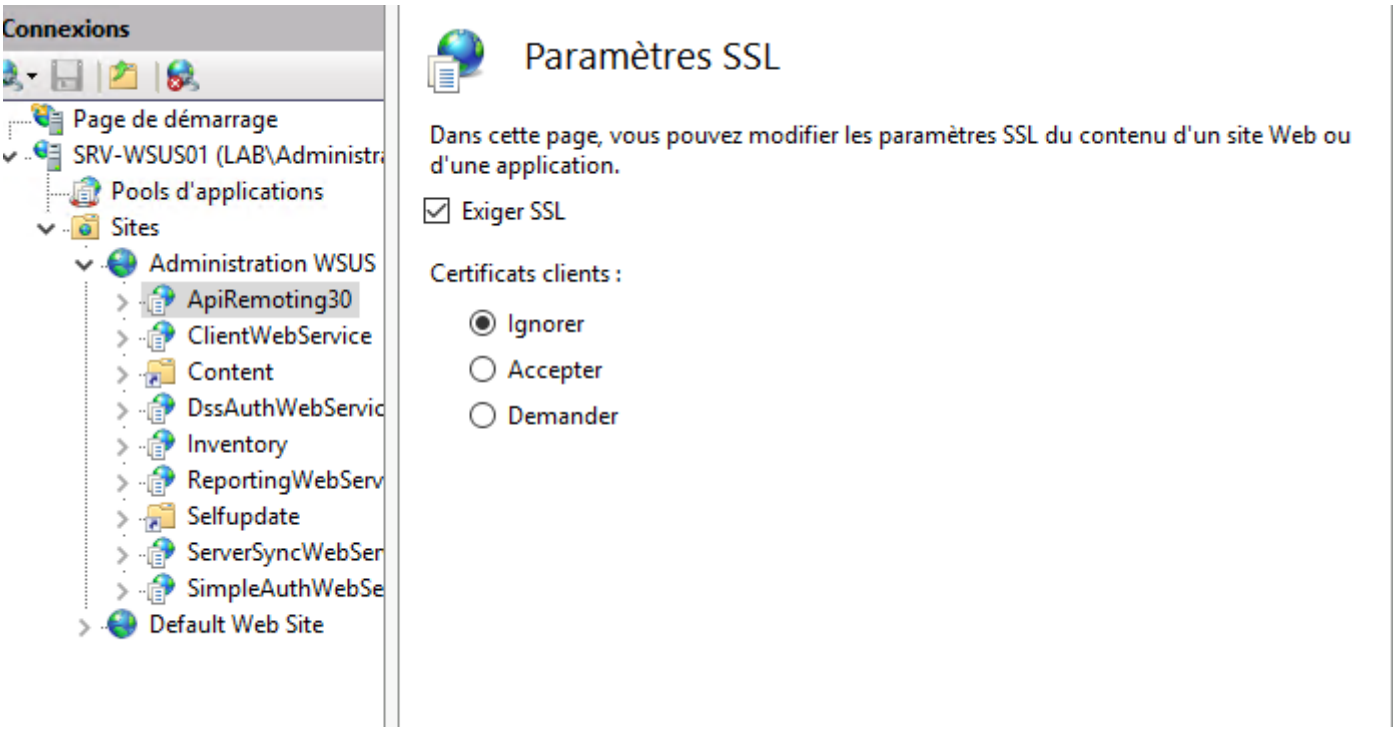
```
Import-Module ServerManager
Add-WindowsFeature Web-Scripting-Tools
Install-WindowsFeature GPMC
Install-Module -Name PowerShellGet -Force
Install-Module –Name IISAdministration
Import-Module WebAdministration
Import-Module IISAdministration
Import-Module GroupPolicy

$myFQDN=(Get-WmiObject win32_computersystem).DNSHostName+"."+(Get-WmiObject
win32_computersystem).Domain ; Write-Host $myFQDN
# 1. Create a self-signed certificate
```

```
$SelfSignedHT = @{
 DnsName = "$($env:COMPUTERNAME).$($env:USERDNSDOMAIN)".ToLower()
 CertStoreLocation = "Cert:\LocalMachine\My"
}
New-SelfSignedCertificate @SelfSignedHT
$cert = Get-ChildItem -Path Cert:\LocalMachine\My -SSLServerAuthentication
# 2. Export its public key
Export-Certificate -Cert $cert -Type CERT -FilePath ~/documents/cert.cer
# 3. Import the public key in the Trusted Root Certificate Authorities store
Import-Certificate -FilePath ~/documents/cert.cer -CertStoreLocation Cert:\LocalMachine\Root
# 4. Select this certificate in the SSL bindings
$cert | New-Item IIS:\SslBindings\0.0.0.0!8531
# MANUALLY require SSL IIS - voir plus bas
# 6. Switch WSUS to SSL
&'C:\Program Files\Update Services\Tools\WsusUtil.exe' configuressl $("$myFQDN".ToLower())
# 7. Change your GPO to point to the new URL
$key = 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate'
$uri = 'https://{0}:8531' -f $("$myFQDN".ToLower())
Get-GPO -All | Foreach-Object {
 if ($_ | Get-GPRegistryValue -Key $key -ValueName WUServer -EA 0) {
  $_ | Set-GPRegistryValue -Key $key -ValueName WUServer       -Value $uri -Type String
  $_ | Set-GPRegistryValue -Key $key -ValueName WUStatusServer -Value $uri -Type String
 }
}
```

Sur IIS, pour chaque page, on change les paramètres SSL.

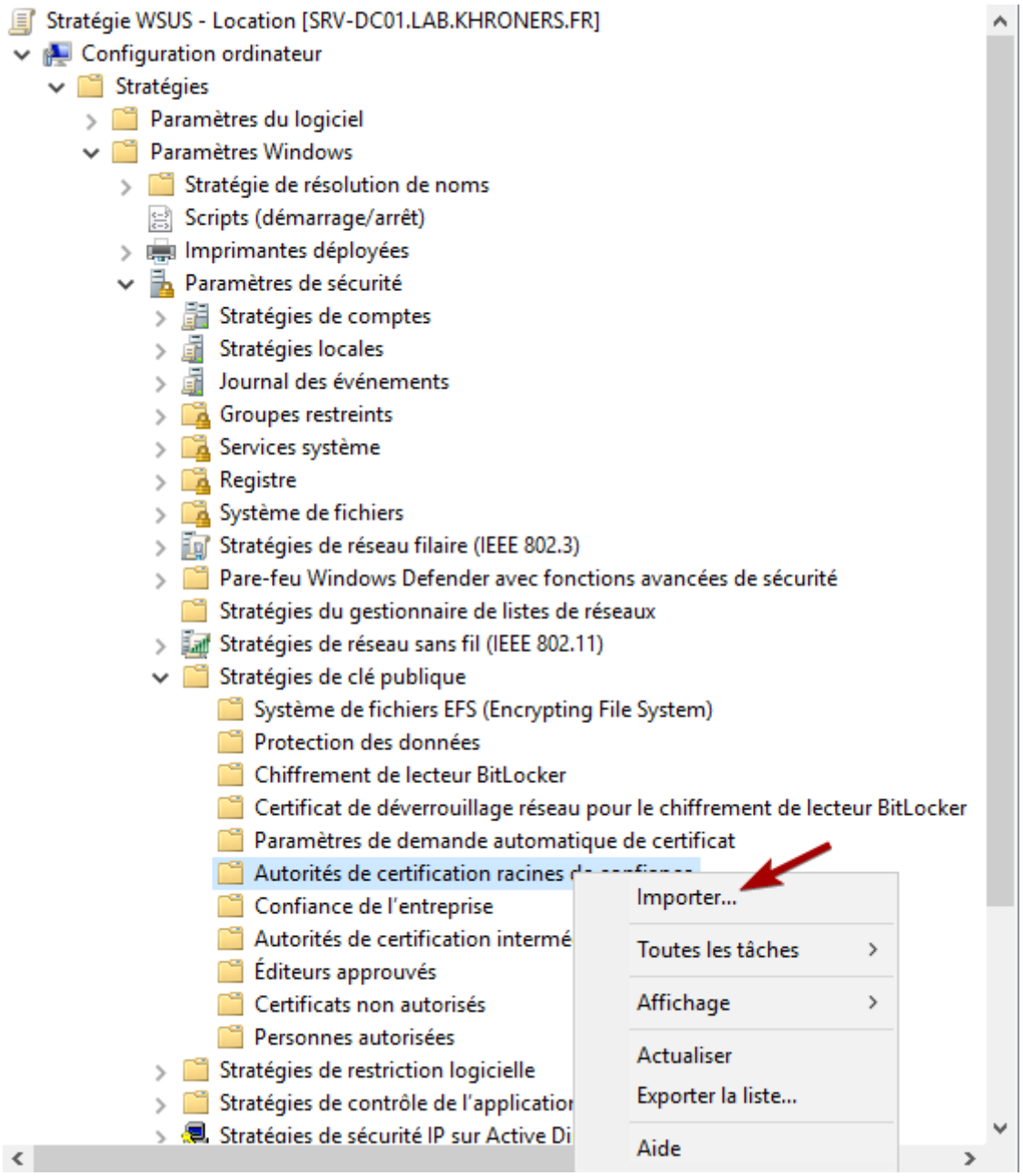

Gestionnaire des services Internet (IIS)
SRV-WSUS01 ▸ Sites ▸ Administration WSUS ▸ ApiRemoting30 ▸
Fichier Affichage Aide
Connexions
Page de démarrage
SRV-WSUS01 (LAB\Administra
Pools d'applications
Sites
Administration WSUS
ApiRemoting30
ClientWebService
Content
DssAuthWebServic
Inventory
ReportingWebServ
Selfupdate
ServerSyncWebSer
SimpleAuthWebSe
Default Web Site
Page d'accueil de /ApiRemoting30
Filtrer :
Atteindre
Afficher tout
Regrouper par :
Pages d'erreurs .NET
Pages et contrôles
Paramètres d'application
Profil .NET
Règles d'autorisation ....
Rôles .NET
Utilisateurs .NET
Gestion
Éditeur de configuration
IIS
Authentification
Compression
Document par défaut
En-têtes de réponse HTTP
Filtrage des demandes
Mappages de gestionnaires
Mise en cache de sortie
Modules
Paramètres SSL
Types MIME
Affichage des fonctionnalités
Affichage du contenu
Prêt



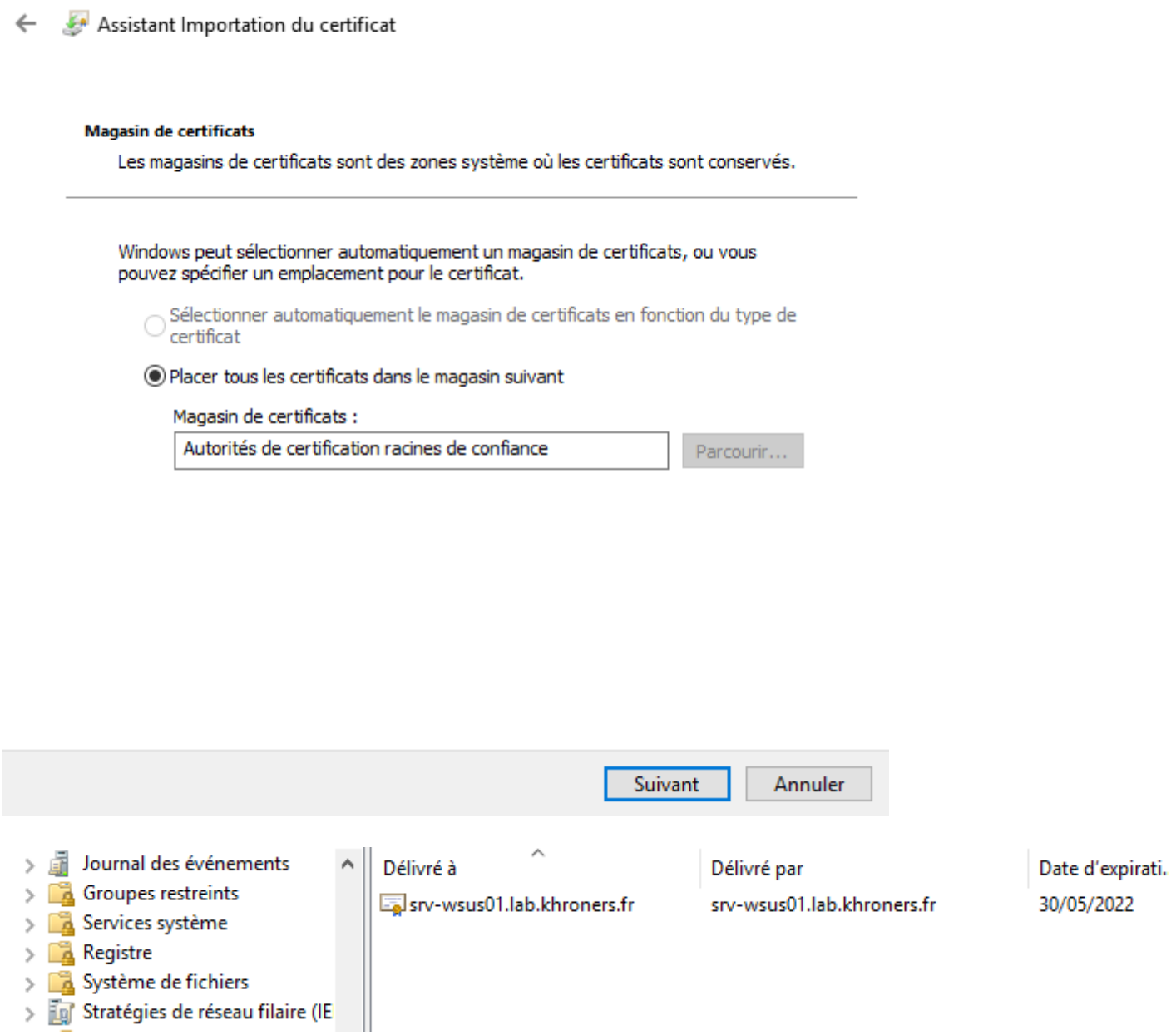
On fait cela pour SimpleAuthWebService, DSSAuthWebService, ServerSyncWebService, APIRemoting30 et ClientWebService.

Publication du certificat

Dans la GPO "WSUS - Location", on importe le certificat.

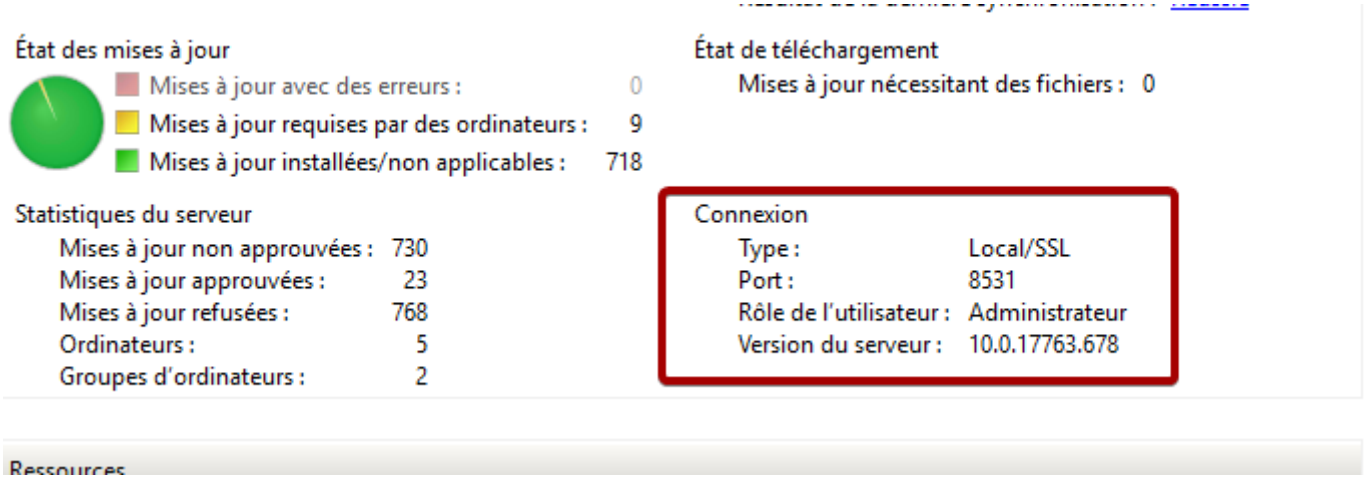


On importe ~/documents/cert.cer.



Conclusion

Dans la console WSUS, on est bien en SSL.



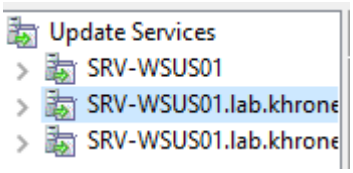
On peut vérifier les logs de Windows Update d'un client via l'invité Powershell :

```
Get-Windowsupdatelog
```

Résoudre l'apparition de duplicatas de WSUS dans la console

Présentation

Après la mise en place du SSL, j'ai des duplicatas dans la console WSUS.



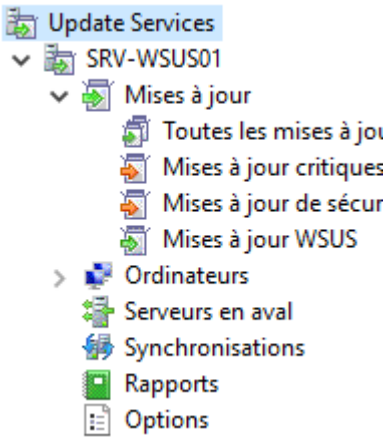
Résolution

On se rend dans %appdata%\Microsoft\MMC\ et on supprime tous les fichiers de ce dossier. On redémarre ensuite le serveur WSUS.

> Il faudra sûrement recréer les vues précédemment créées.

Conclusion

On a désormais qu'un seul serveur dans la console.


Update Services
SRV-WSUS01
Mises à jour
Toutes les mises à jou
Mises à jour critiques
Mises à jour de sécur
Mises à jour WSUS
Ordinateurs
Serveurs en aval
Synchronisations
Rapports
Options

Installation automatique des définitions de Microsoft Defender

---

Présentation

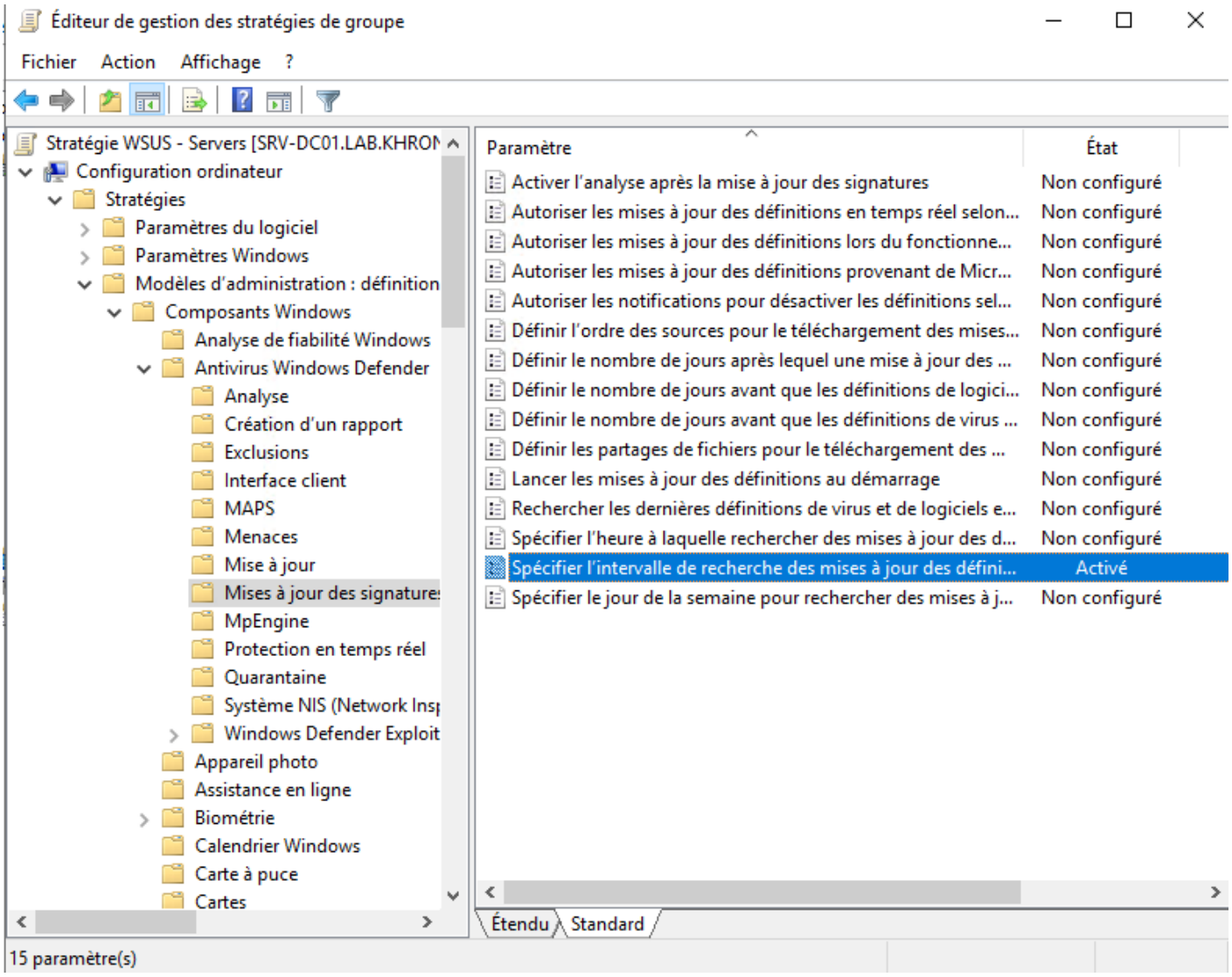
Par défaut, les définitions de Microsoft Defender sont mises à jour toutes les 24 heures, ou via Windows Update selon la fréquence de recherche de mises à jour. Cependant, selon les GPO mises en place précédemment, elles ne s'installent pas automatiquement (sauf à l'heure planifiée pour les Workstations).

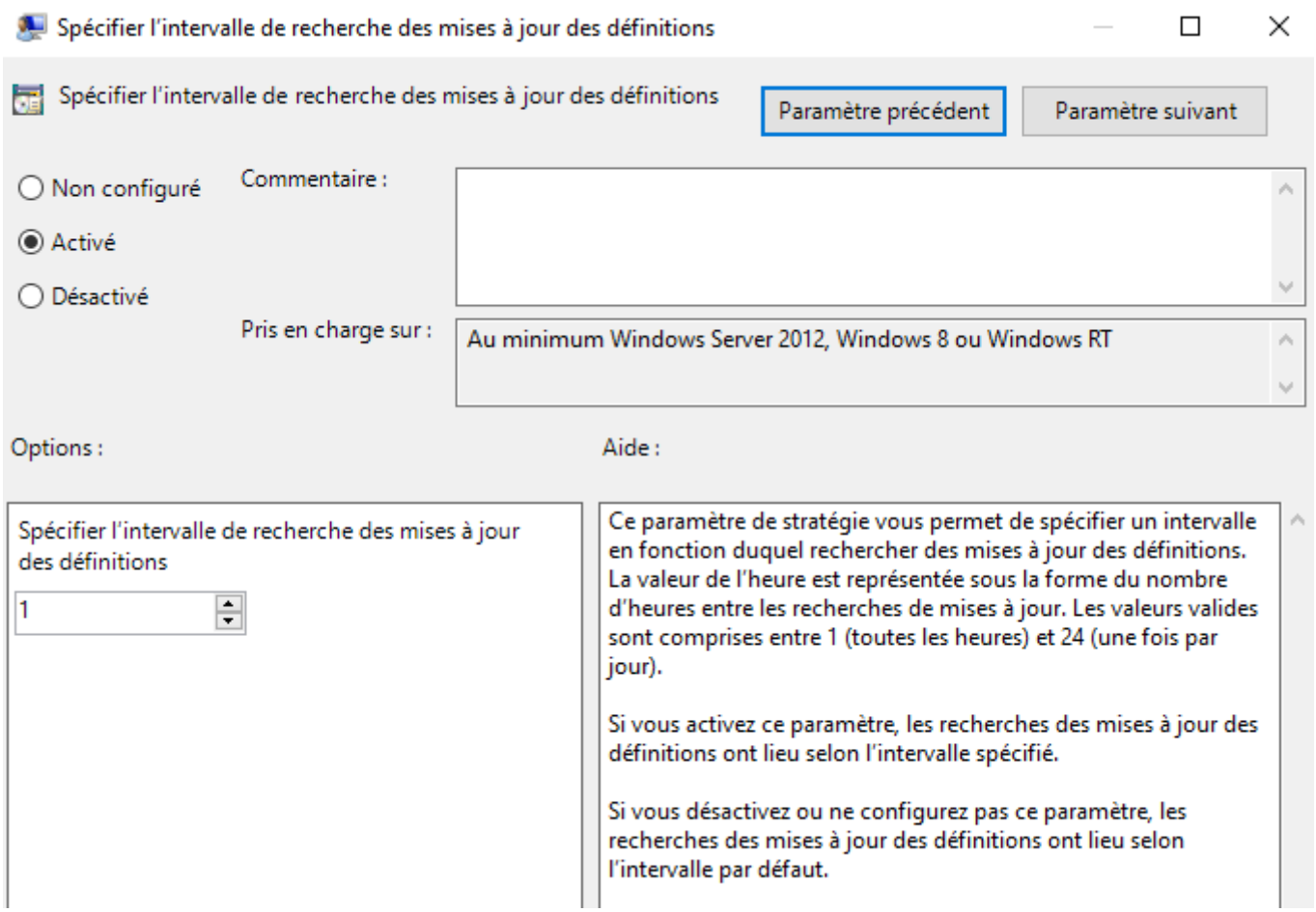
> En soit, déployer les mises à jour de Defender n'est pas primordial. A chaque mise à jour, WSUS retélécharge tout (60-70mo en moyenne pour le moment), alors que de passer d'une mise à jour à une autre prend environ 1mo, selon la mise à jour des définitions.
> Cela peut être utile en cas de déploiement massif d'appareils, pour éviter que tous les postes, lors du déploiement, téléchargent chacun les définitions.

Installation automatique des définitions

Pour résoudre ce problème, on va utiliser une GPO.

Dans WSUS - Servers et WSUS - Workstations, on se rend ici, et on définit la fréquence pour une heure. Pourquoi une heure ? Dans le but d'avoir des définitions toujours à jour.


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie WSUS - Servers [SRV-DC01.LAB.KHRON
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Modèles d'administration : définition
Composants Windows
Analyse de fiabilité Windows
Antivirus Windows Defender
Analyse
Création d'un rapport
Exclusions
Interface client
MAPS
Menaces
Mise à jour
Mises à jour des signatures
MpEngine
Protection en temps réel
Quarantaine
Système NIS (Network Insp
Windows Defender Exploit
Appareil photo
Assistance en ligne
Biométrie
Calendrier Windows
Carte à puce
Cartes
Paramètre
État
Activer l'analyse après la mise à jour des signatures Non configuré
Autoriser les mises à jour des définitions en temps réel selon... Non configuré
Autoriser les mises à jour des définitions lors du fonctionne... Non configuré
Autoriser les mises à jour des définitions provenant de Micr... Non configuré
Autoriser les notifications pour désactiver les définitions sel... Non configuré
Définir l'ordre des sources pour le téléchargement des mises... Non configuré
Définir le nombre de jours après lequel une mise à jour des ... Non configuré
Définir le nombre de jours avant que les définitions de logici... Non configuré
Définir le nombre de jours avant que les définitions de virus ... Non configuré
Définir les partages de fichiers pour le téléchargement des ... Non configuré
Lancer les mises à jour des définitions au démarrage Non configuré
Rechercher les dernières définitions de virus et de logiciels e... Non configuré
Spécifier l'heure à laquelle rechercher des mises à jour des d... Non configuré
Spécifier l'intervalle de recherche des mises à jour des défini... Activé
Spécifier le jour de la semaine pour rechercher des mises à j... Non configuré
Étendu
Standard
15 paramètre(s)



Conclusion

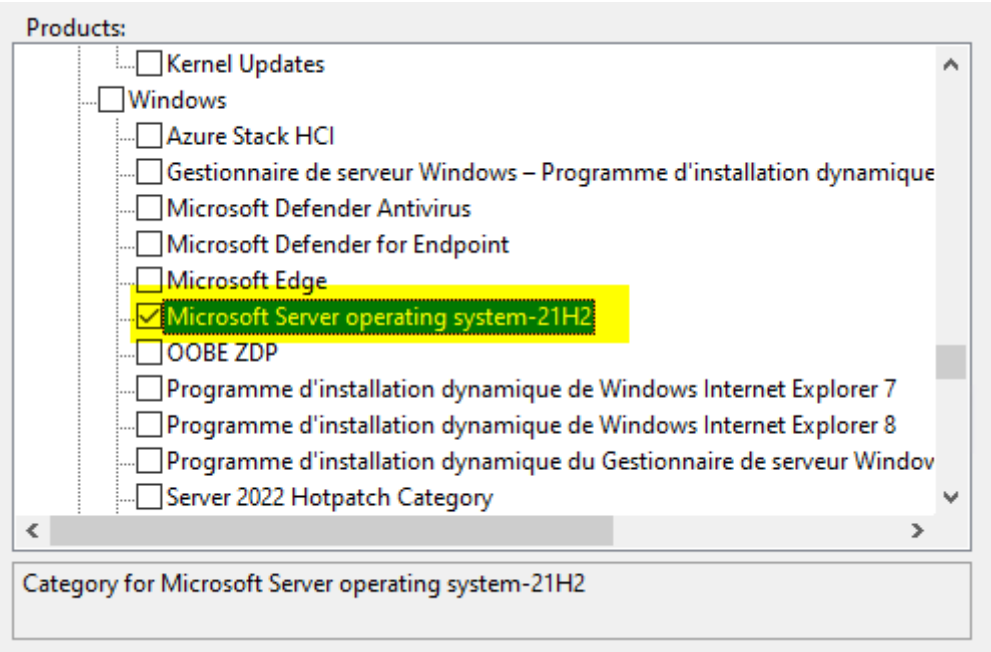
Ainsi, les définitions seront mises à jour automatiquement.

> Si le serveur WSUS n'a pas la mise à jour des définitions la plus récente, elle sera téléchargée depuis Microsoft. Il est donc nécessaire d'augmenter la fréquence de synchronisation du serveur WSUS

> Il est possible que sur les serveurs, on retrouve tout de même la demande d'installation en manuel. La mise à jour est pourtant déjà installée.

Windows Server 2022 et WSUS

Pour avoir les mises à jour de Windows Server 2022 dans WSUS, il faut ajouter un produit nommé "**Microsoft Server operating system-21H2**".



En effet, Windows Server est basé sur Windows 10 21H2.