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

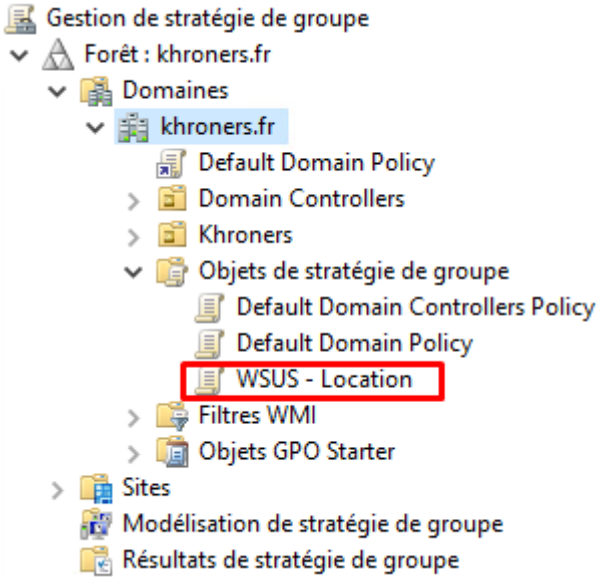
Présentation

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.

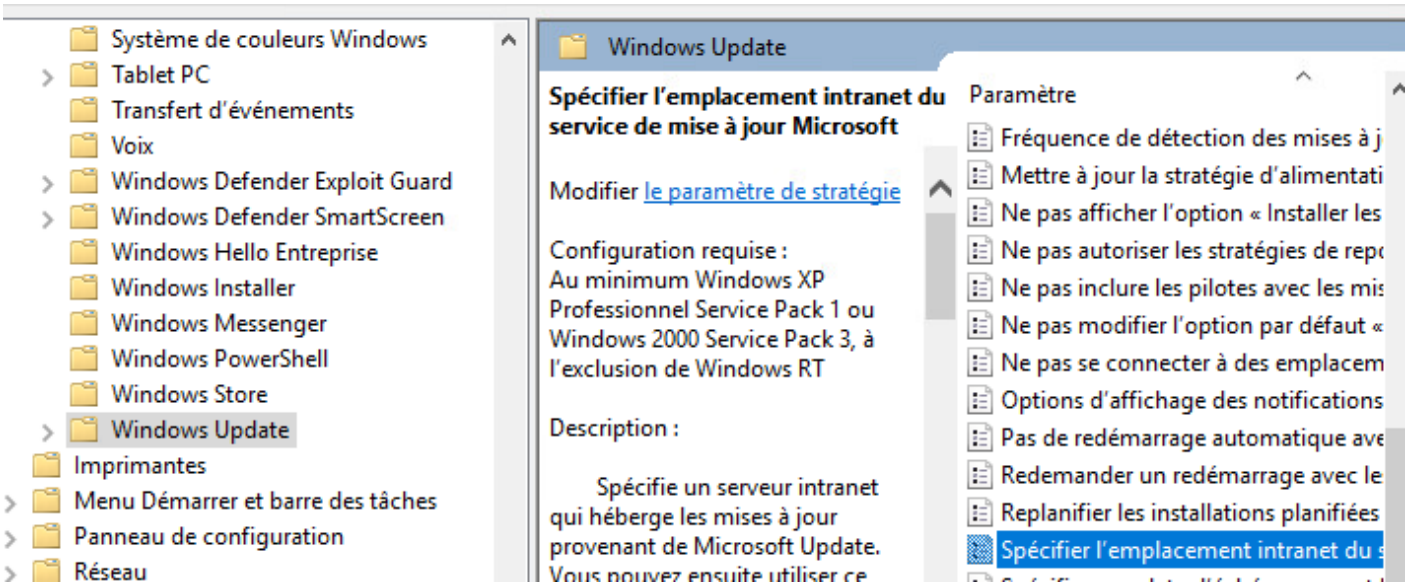
Création des GPO

WSUS - Location

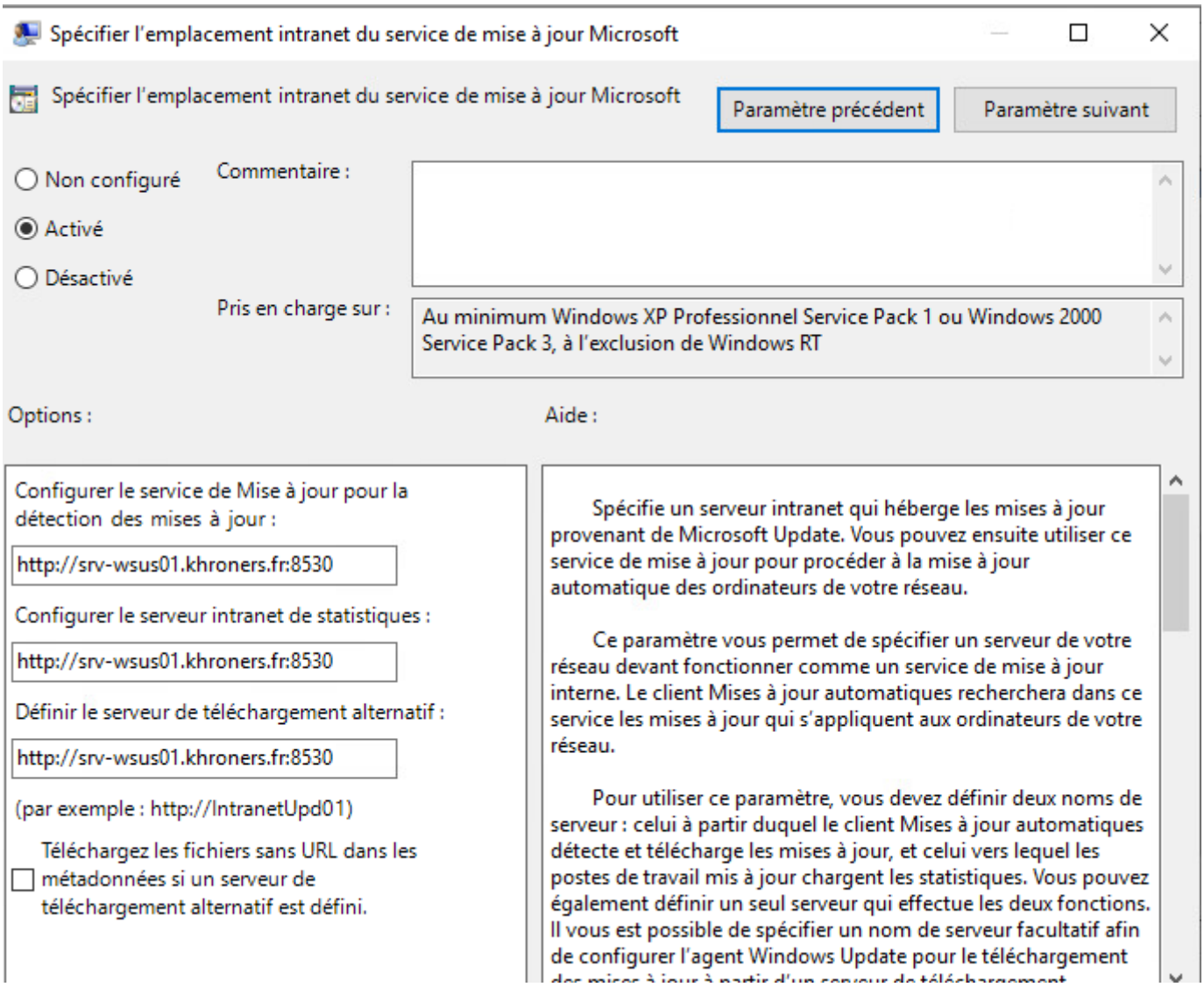
On se rend dans la console de Gestion de stratégie de groupe, on clique droit sur "Objets de stratégie de groupe" puis on crée une nouvelle GPO nommée "WSUS - Location".



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)

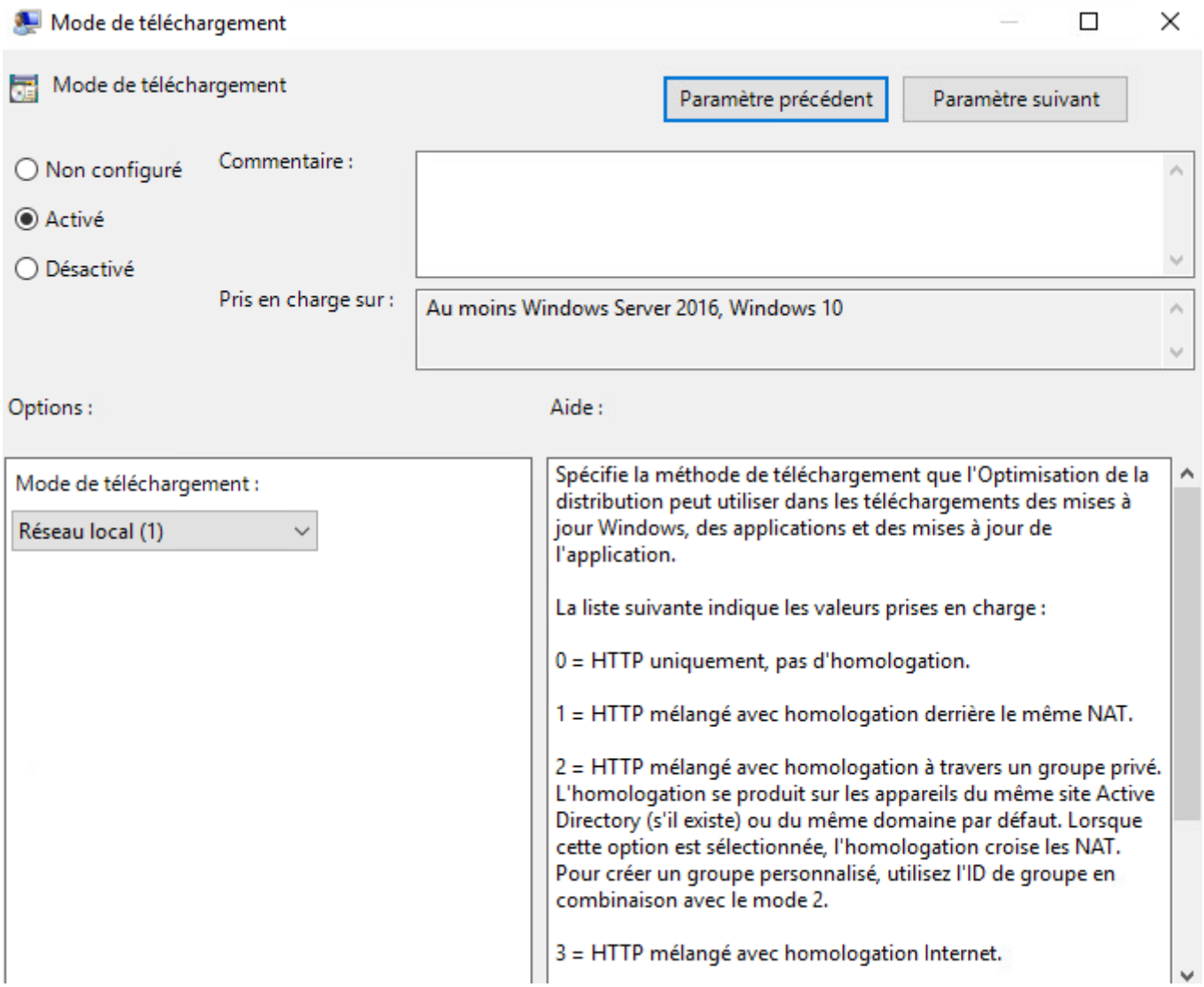


WSUS - Workstations

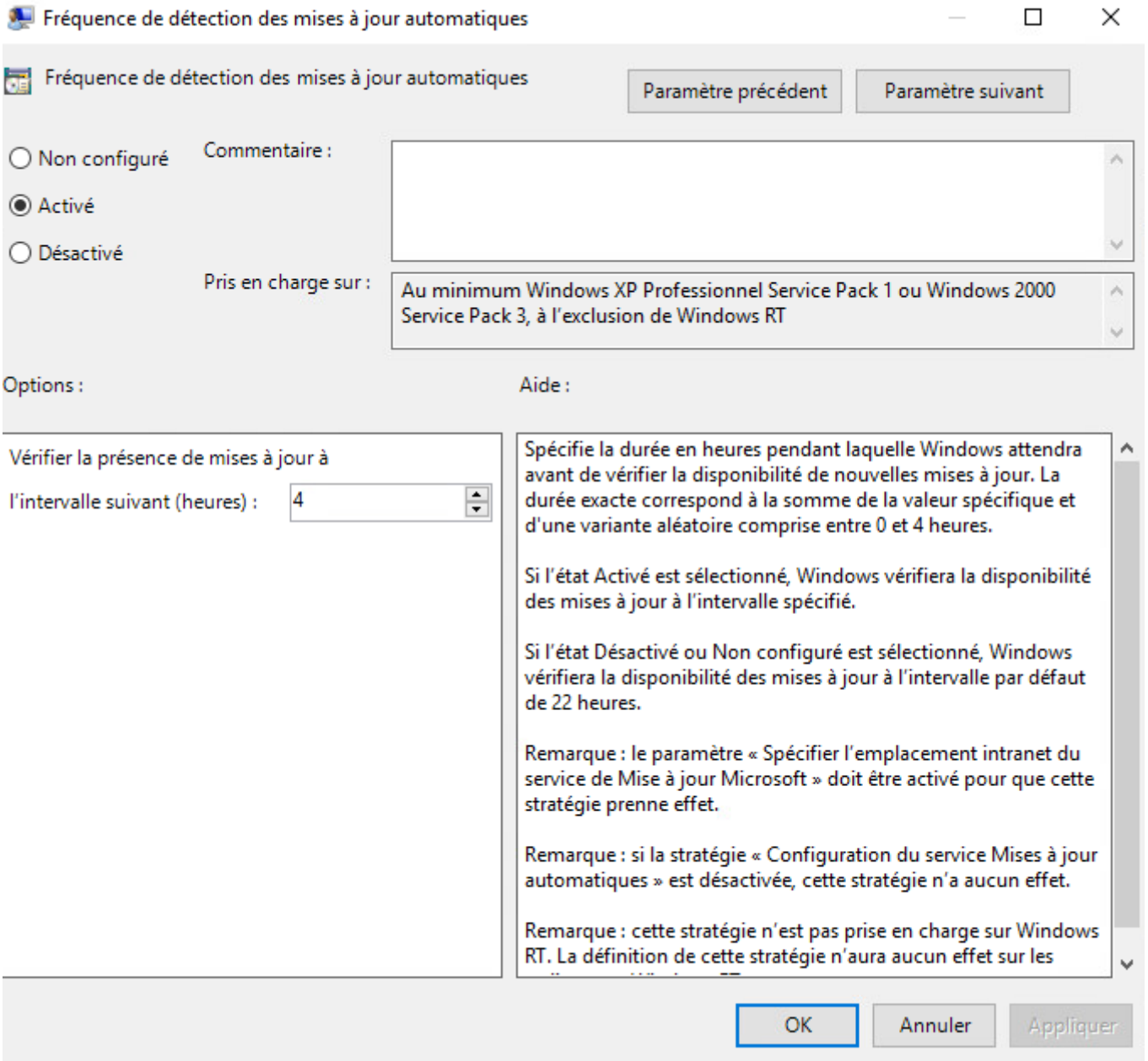
On crée ensuite une nouvelle GPO pour les postes de travail nommée "WSUS - Workstations".

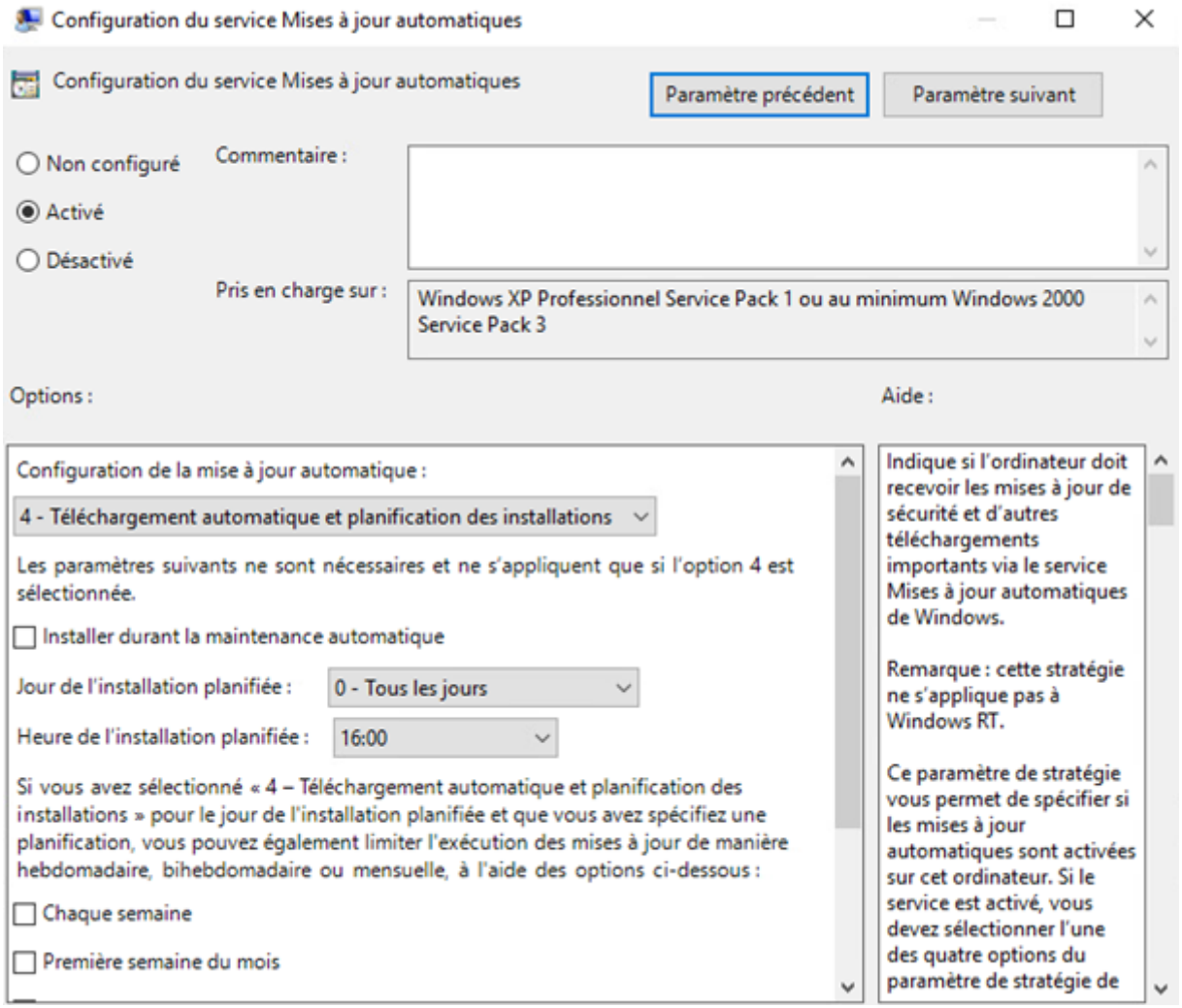
On la modifie et on se rend dans Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Optimisation de la distribution.

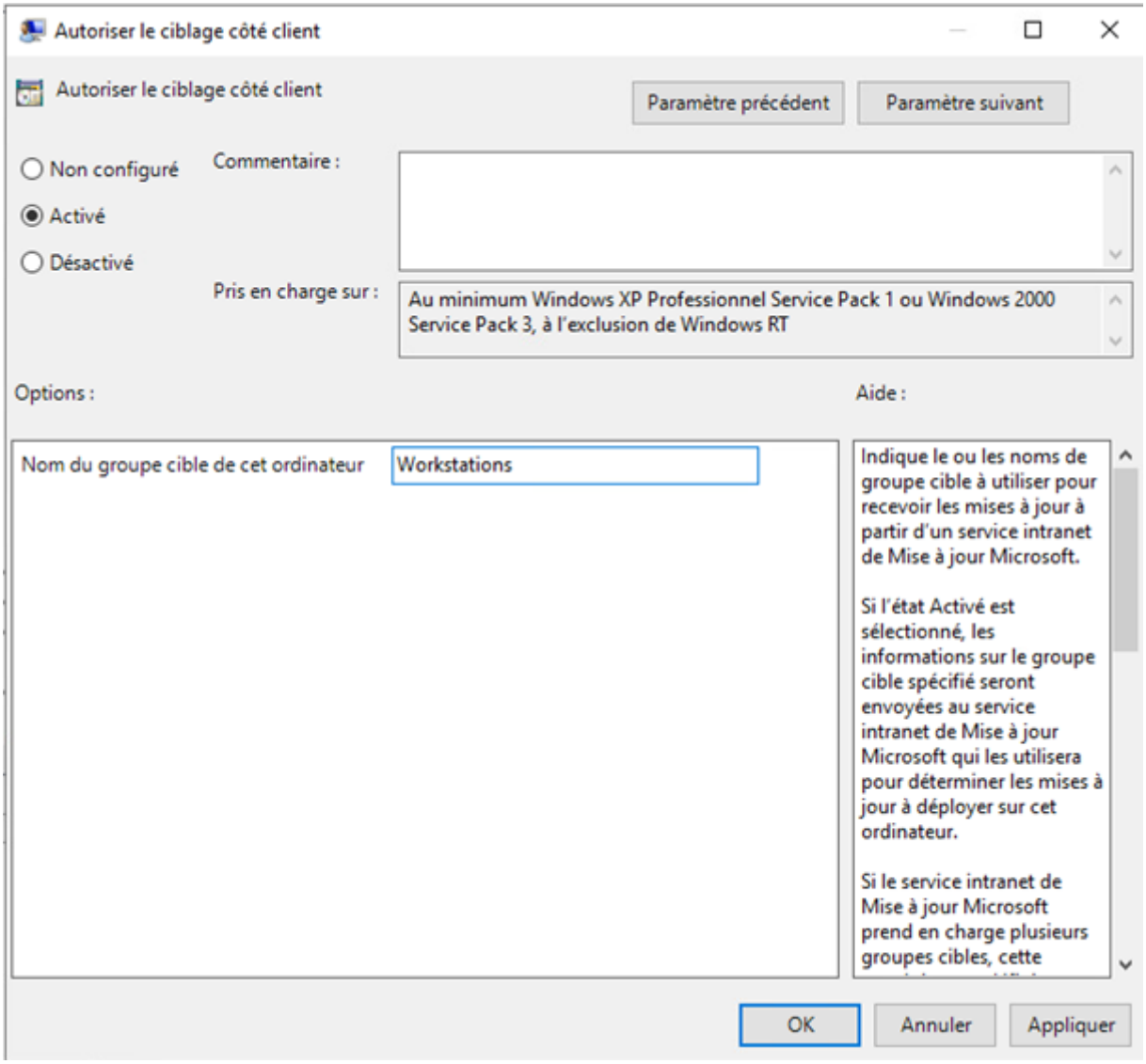
On active "Mode de téléchargement" sur "Réseau local".



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

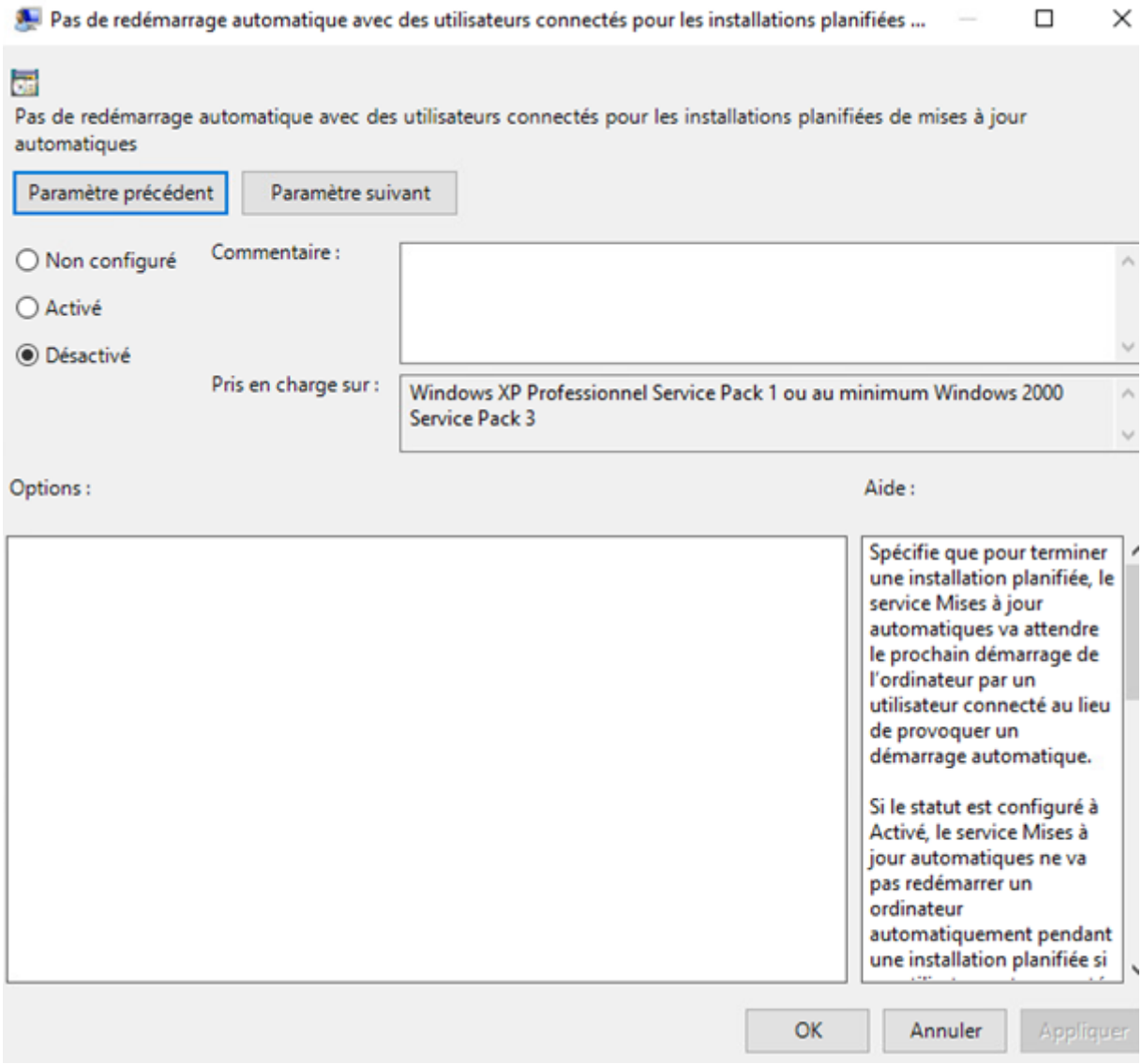

Fréquence de détection des mises à jour automatiques
Fréquence de détection des mises à jour automatiques
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion 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

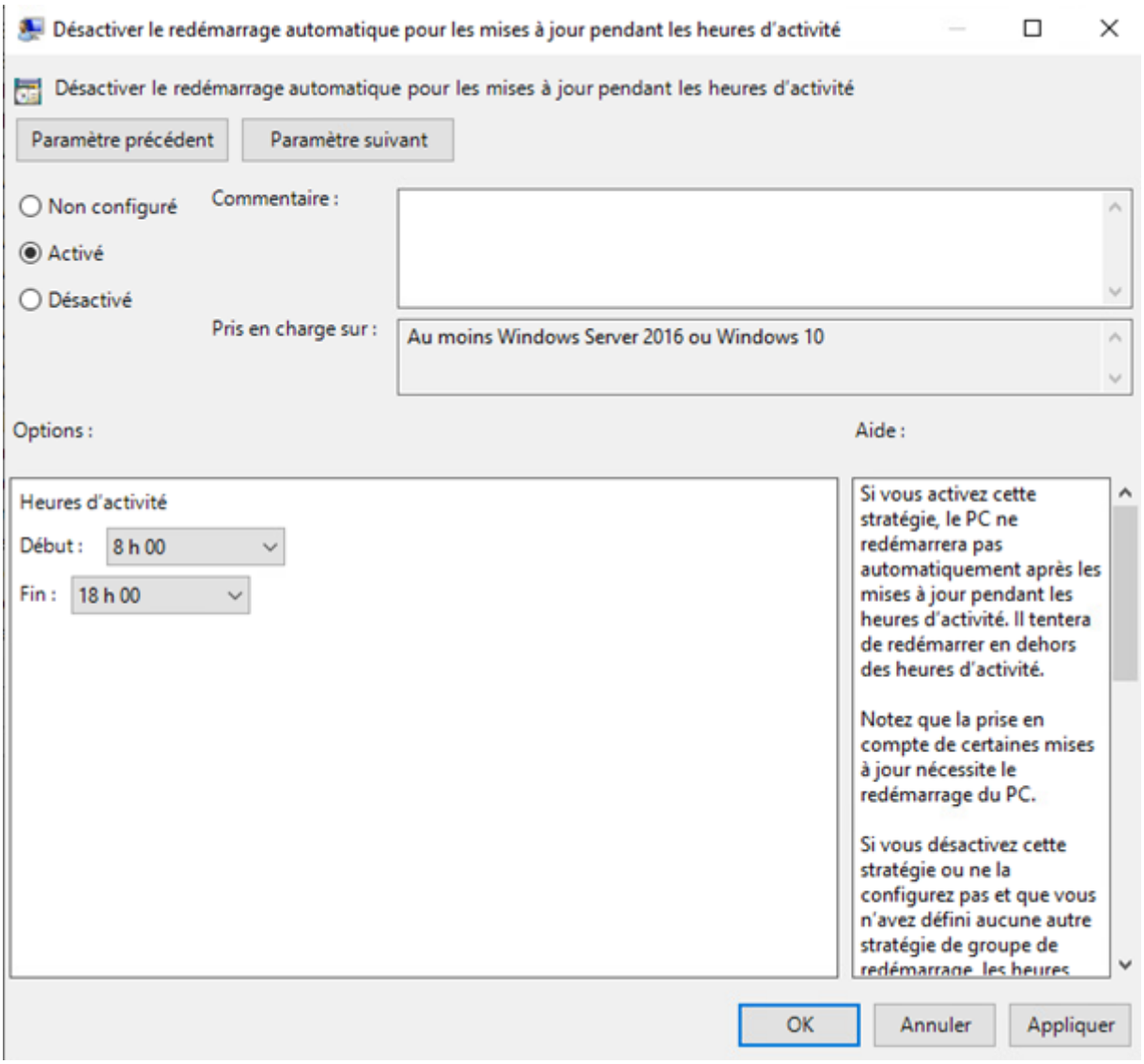


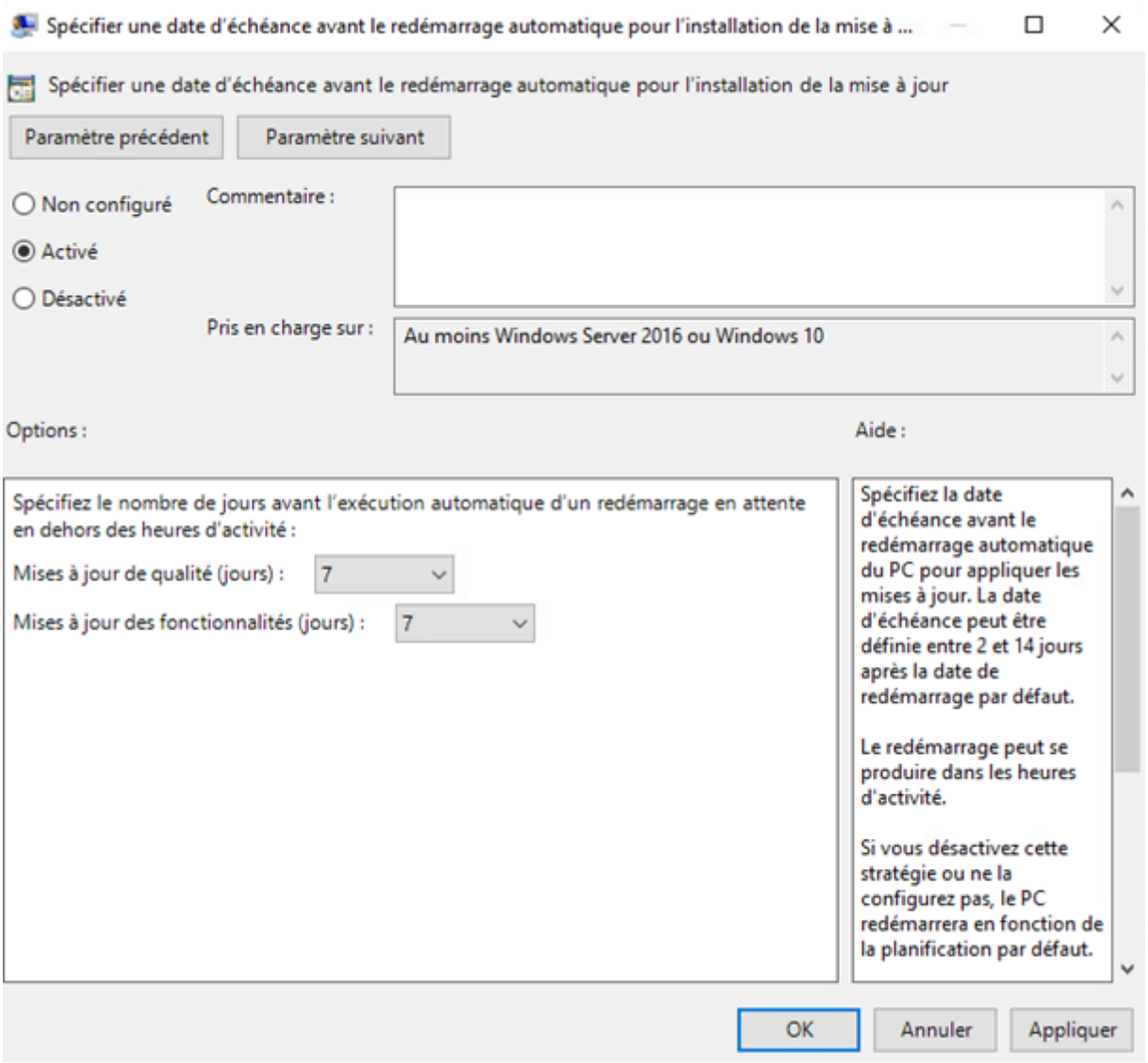
EDIT : la GPO ci-dessous n'a pas le résultat escompté d'après Microsoft. (https://techcommunity.microsoft.com/t5/windows-it-pro-blog/why-you-shouldn-t-set-these-25-windows-policies/ba-p/3066178?WT.mc_id=AZ-MVP-5004580)

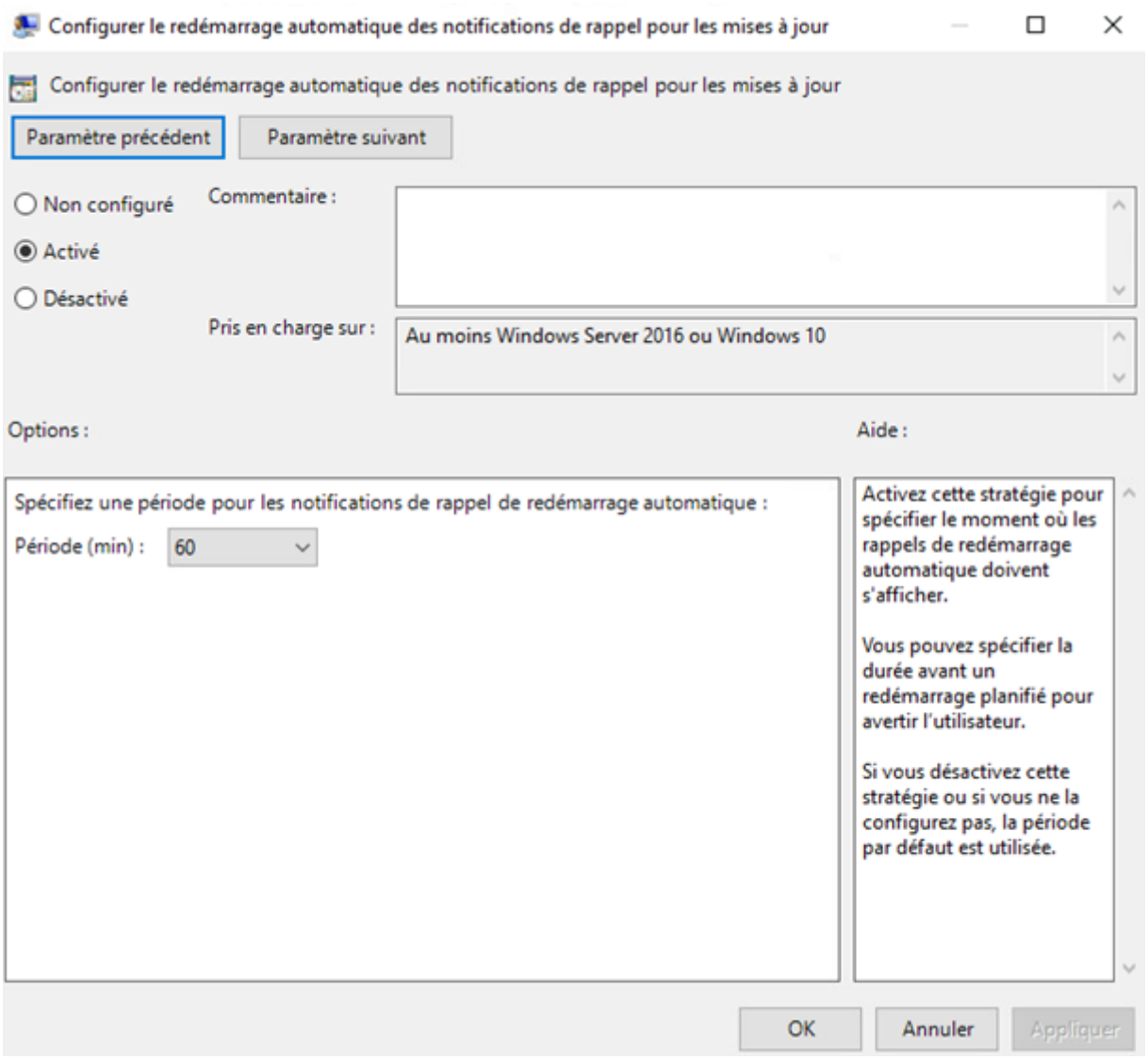
Il faut la remplacer. Voir la page suivante disponible dans ce chapitre :



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

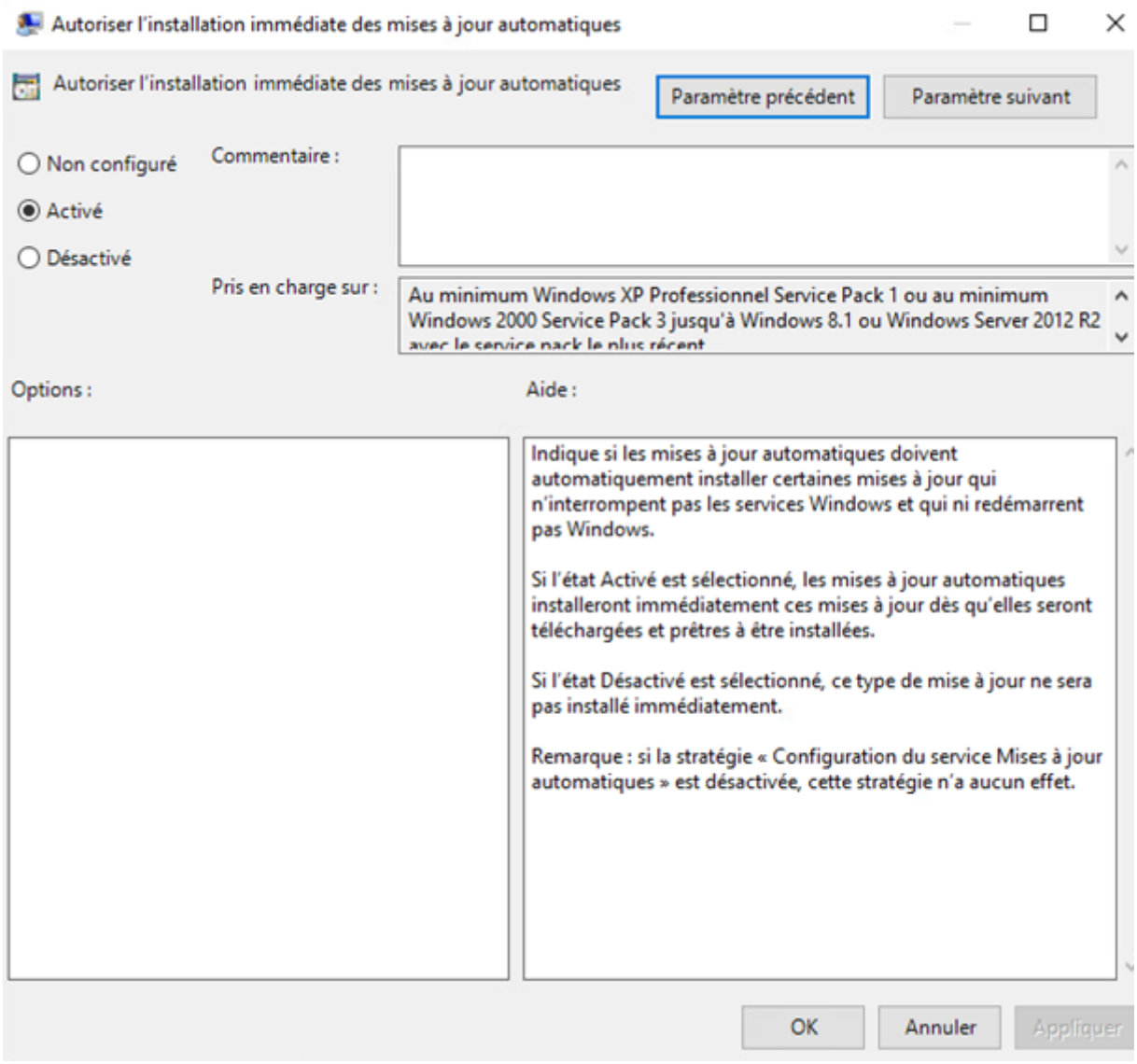

Spécifier une date d'échéance avant le redémarrage automatique pour l'installation de la mise à ...
Spécifier une date d'échéance avant le redémarrage automatique pour l'installation de la mise à jour
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
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

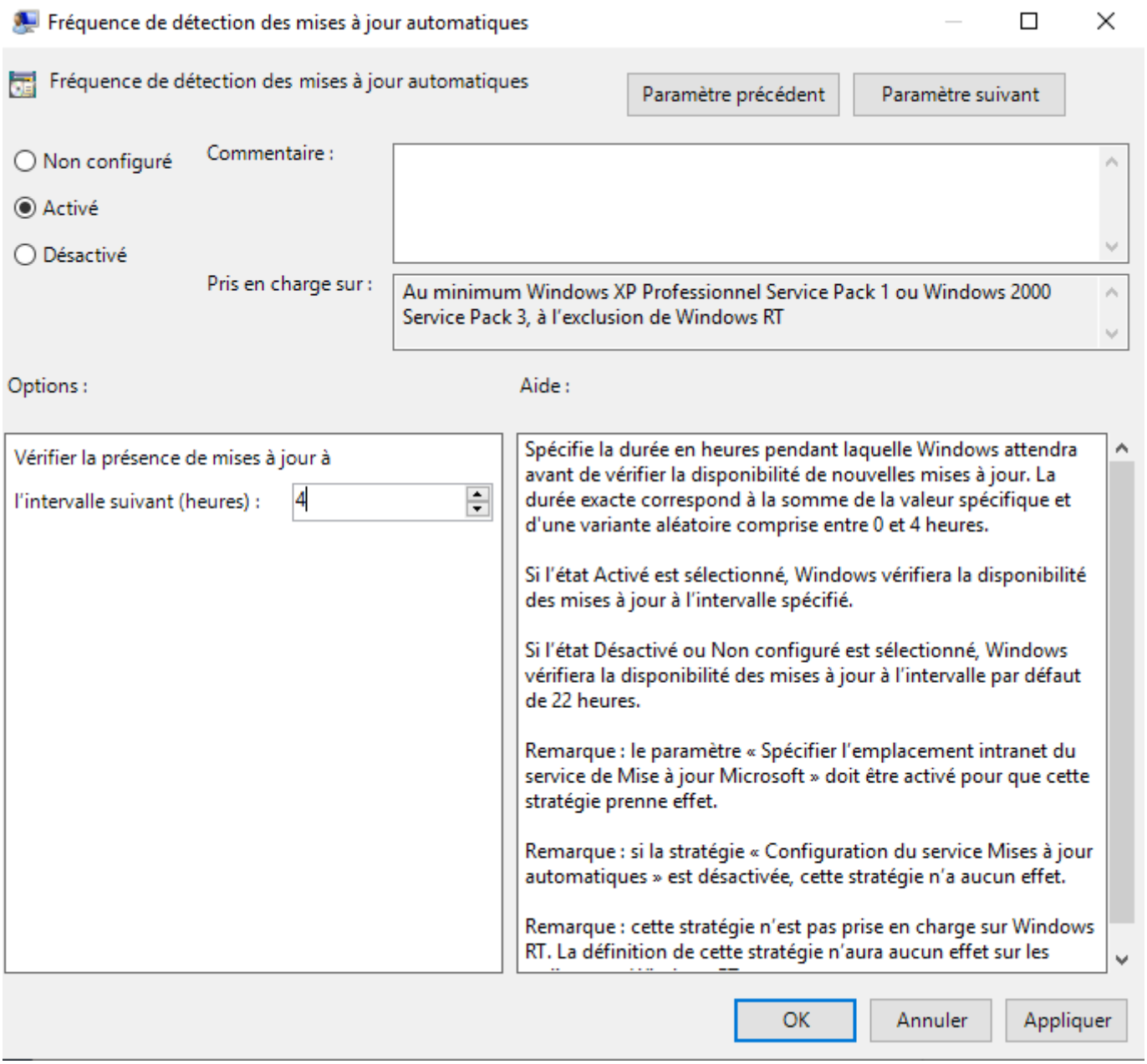


WSUS - Servers

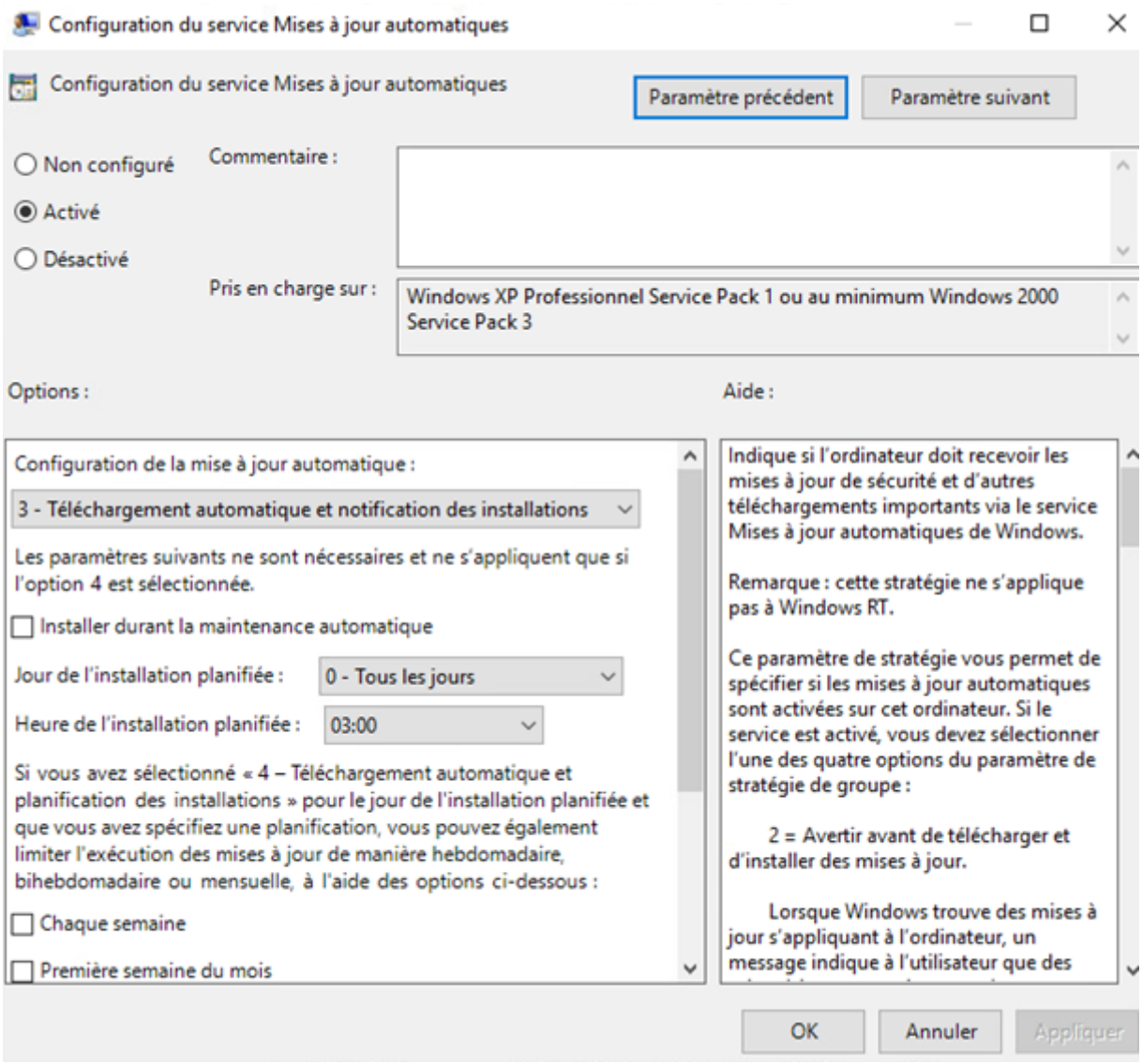
On ne veut pas que les mises à jour s'installent automatiquement sur nos serveurs, sauf pour les mises à jour des définitions de l'antivirus. On va donc activer une option.

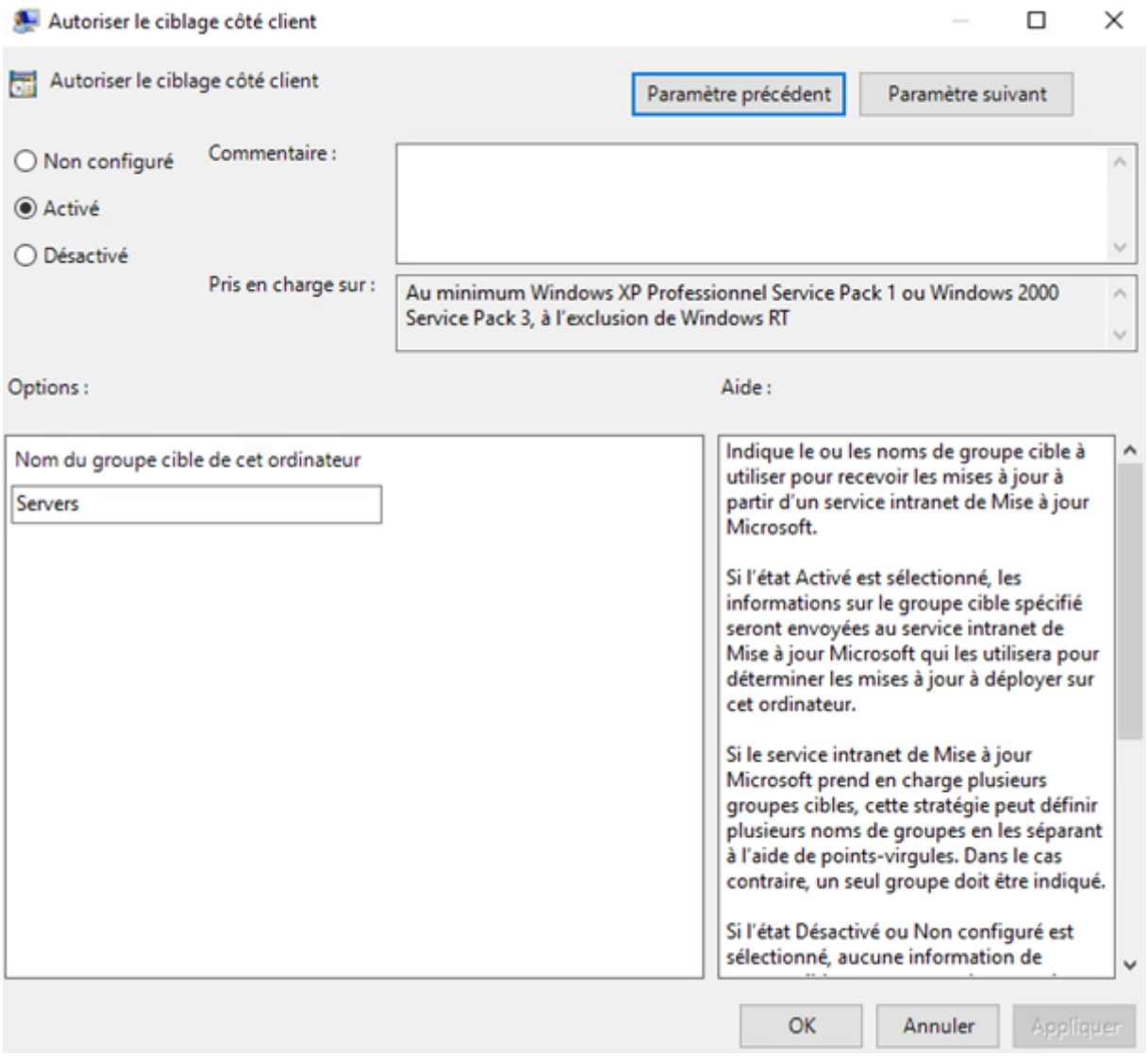
Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Windows Update.


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



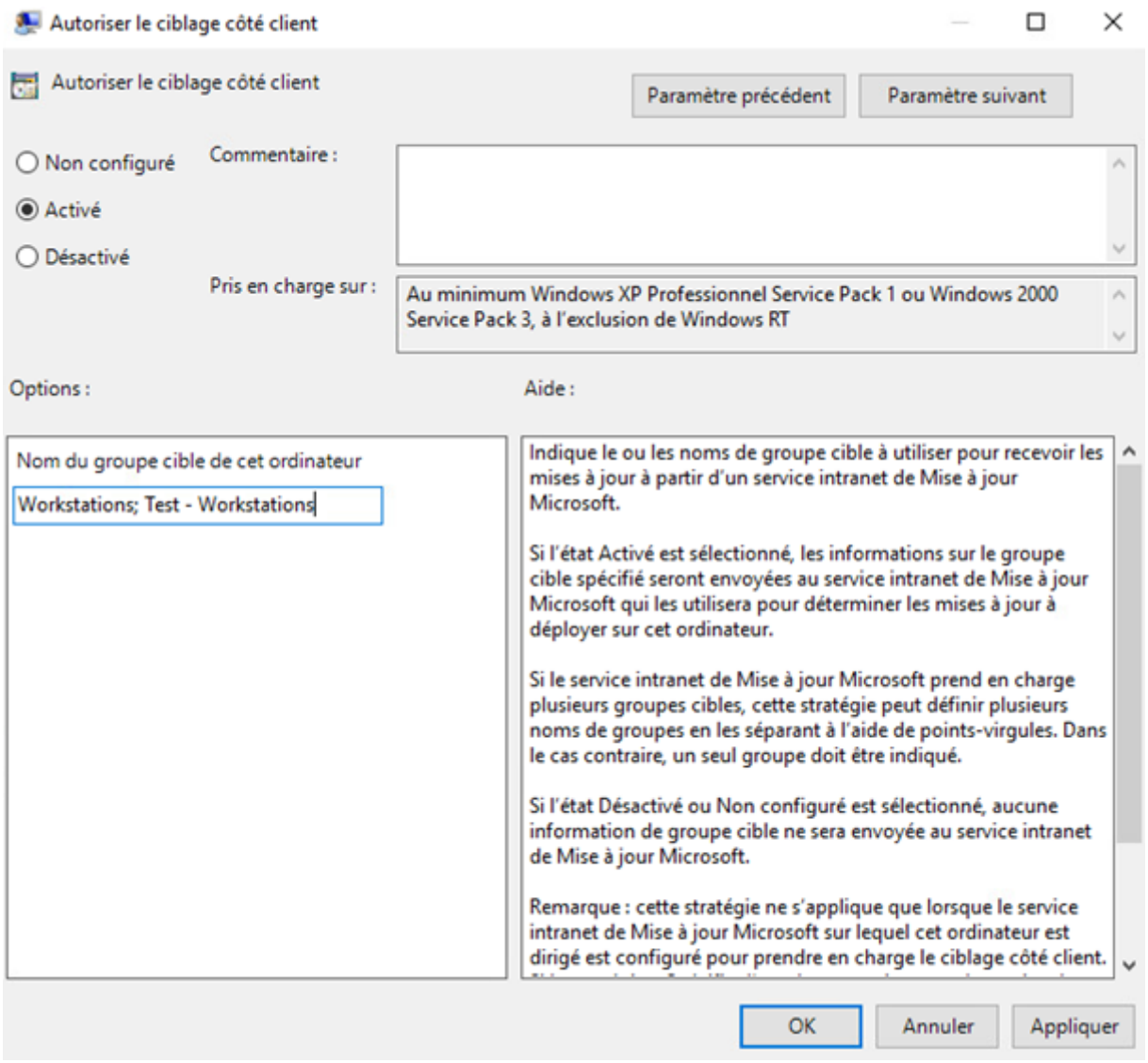
Si on a une farm de serveurs, il est préférable de créer plusieurs 'anneaux' de planifications et groupes, en choisissant l'option 4 : "Téléchargement automatique et planifier l'installation" et forcer le redémarrage lors de la maintenance des serveurs.

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.

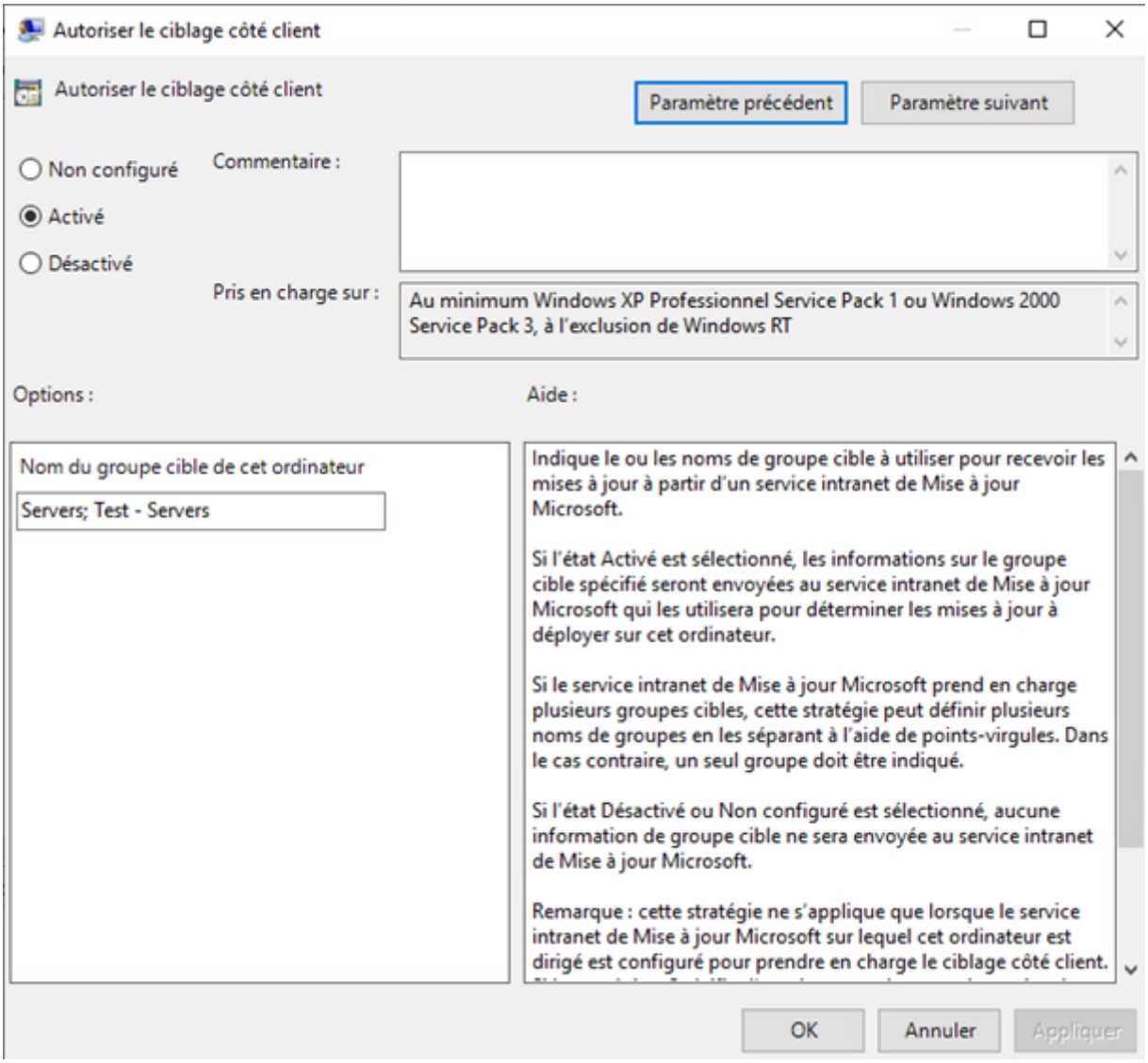
Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Windows Update



WSUS - Servers, Test - Servers

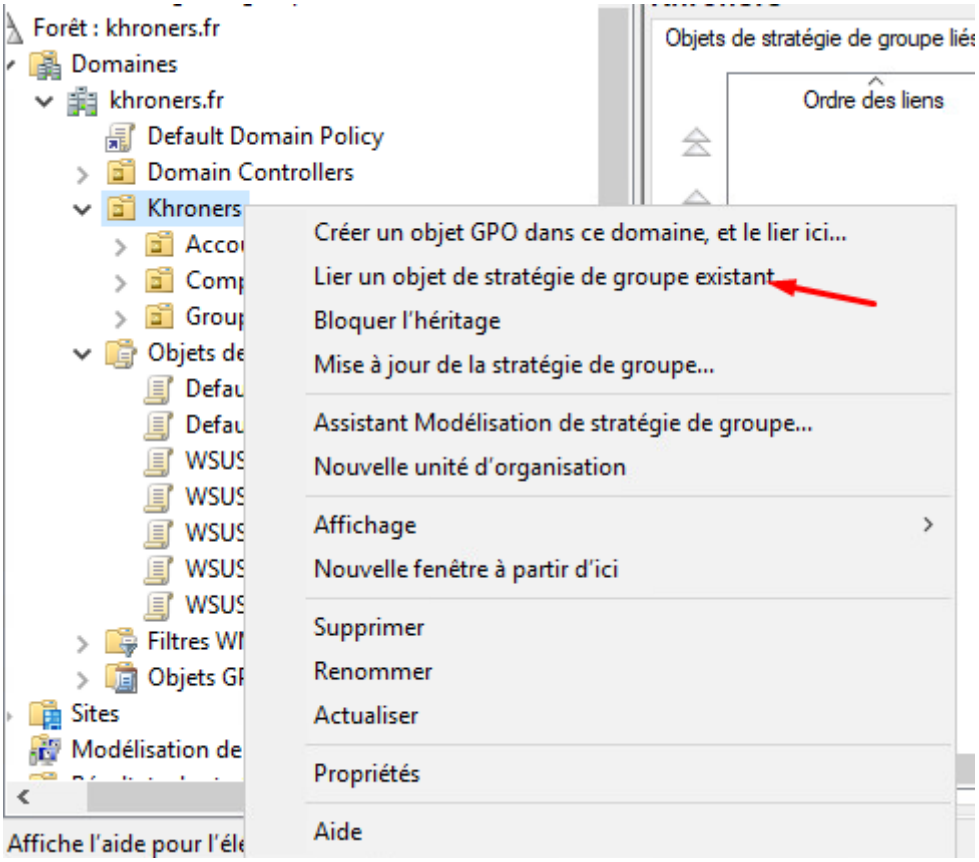
C'est une GPO pour le groupe de ciblage.

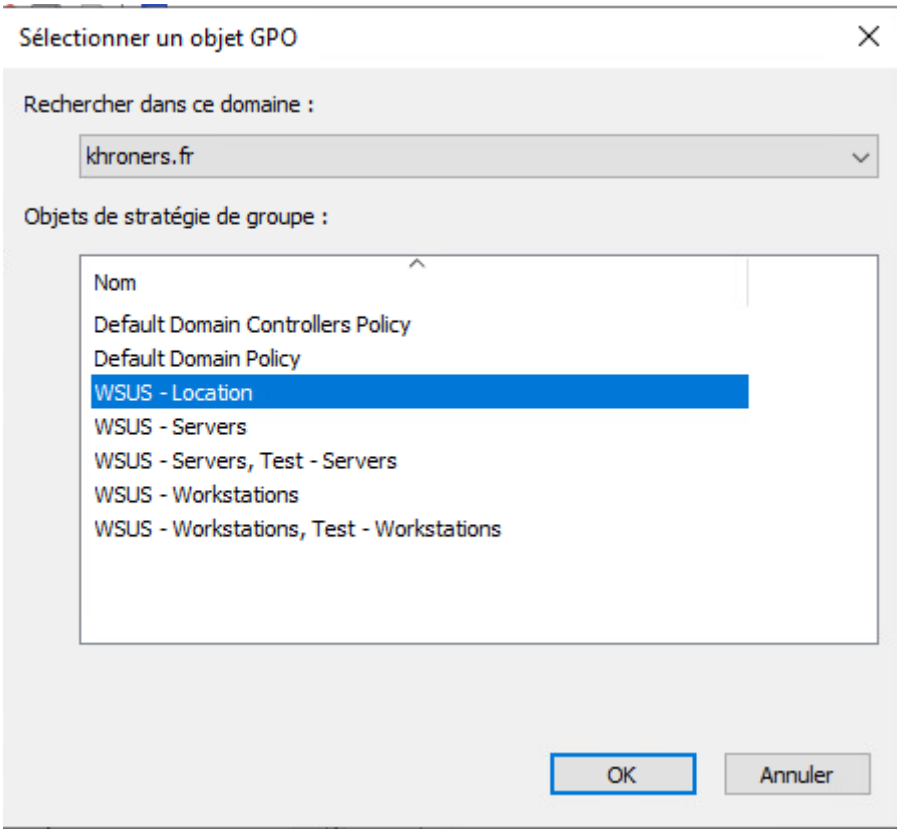
Configuration de l'ordinateur, Stratégies, Modèles d'administration, Composants Windows, Windows Update



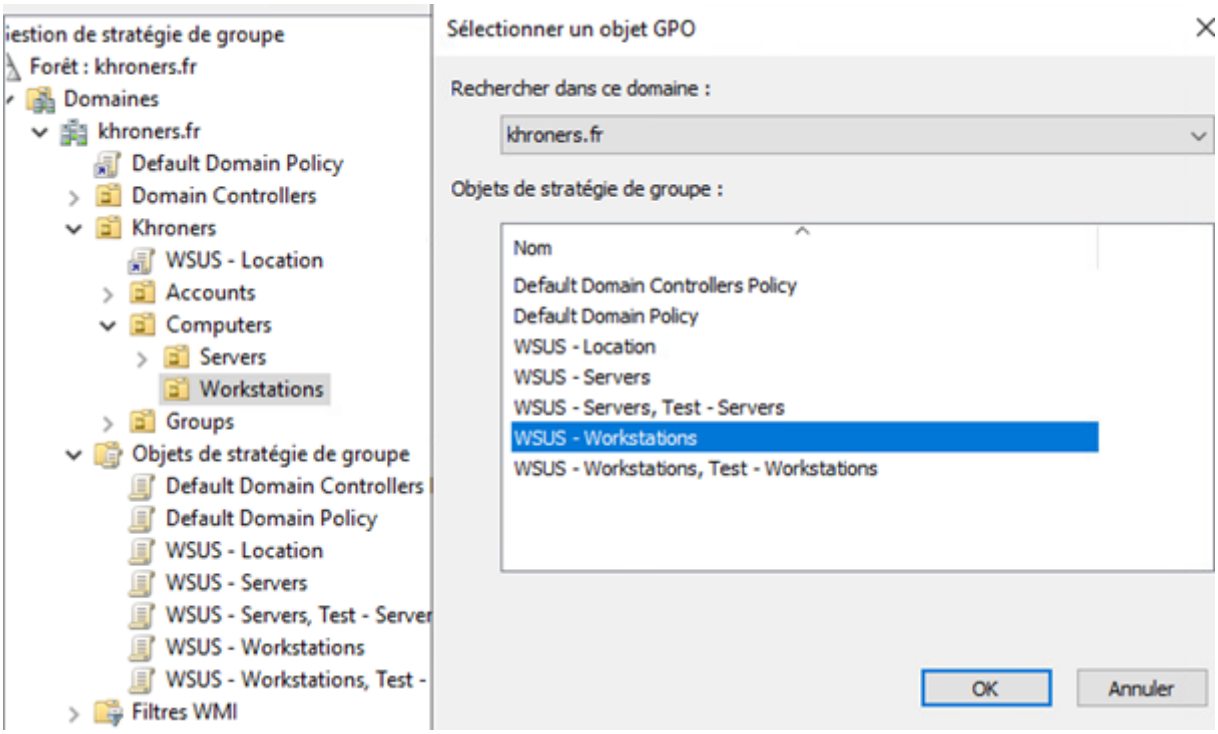
Lier les GPO aux bonnes OU

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

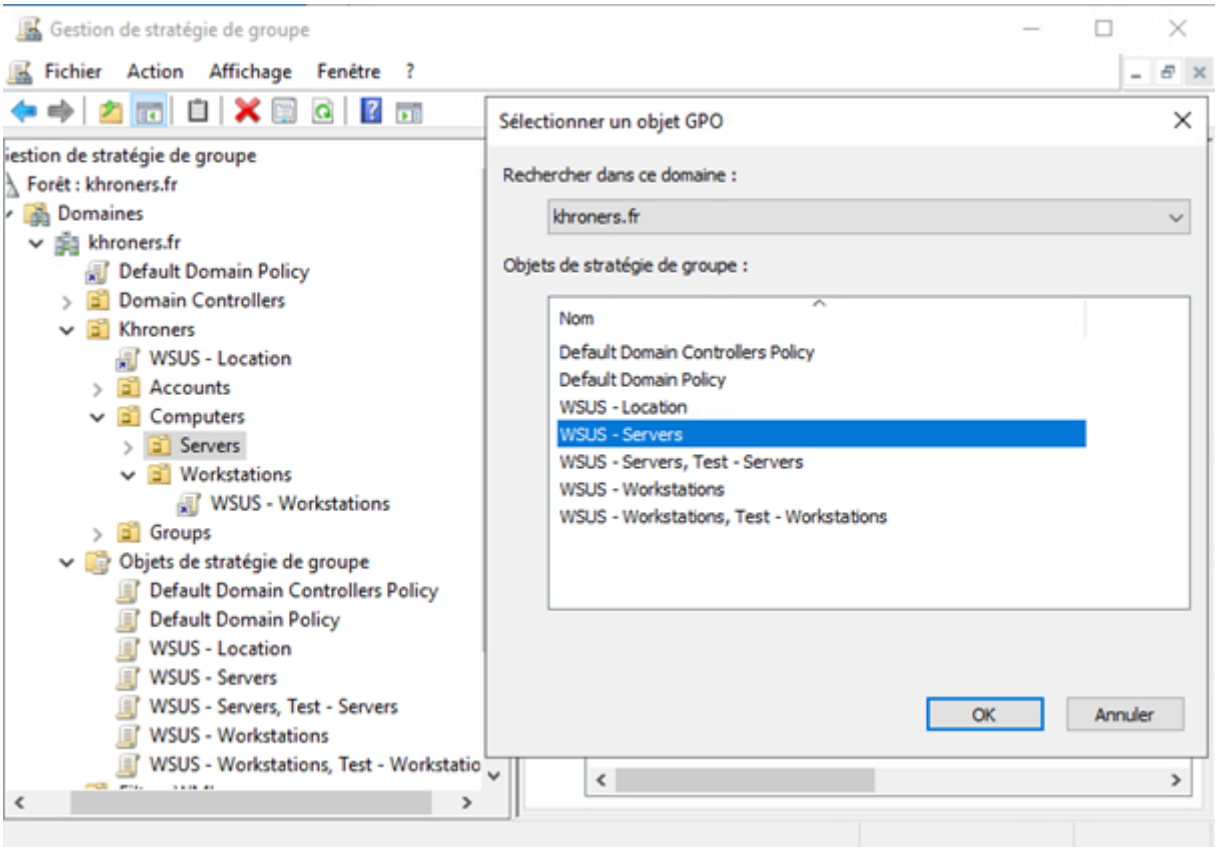




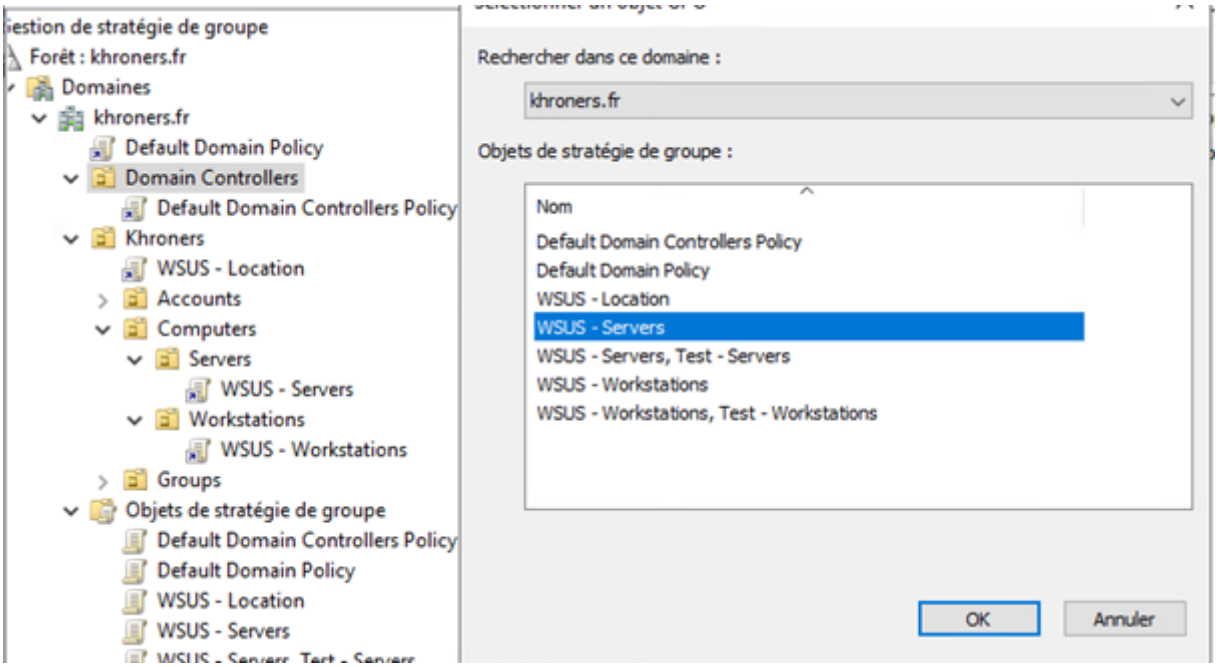
On applique pour les postes de travails la GPO correspondante.



De même pour les serveurs.



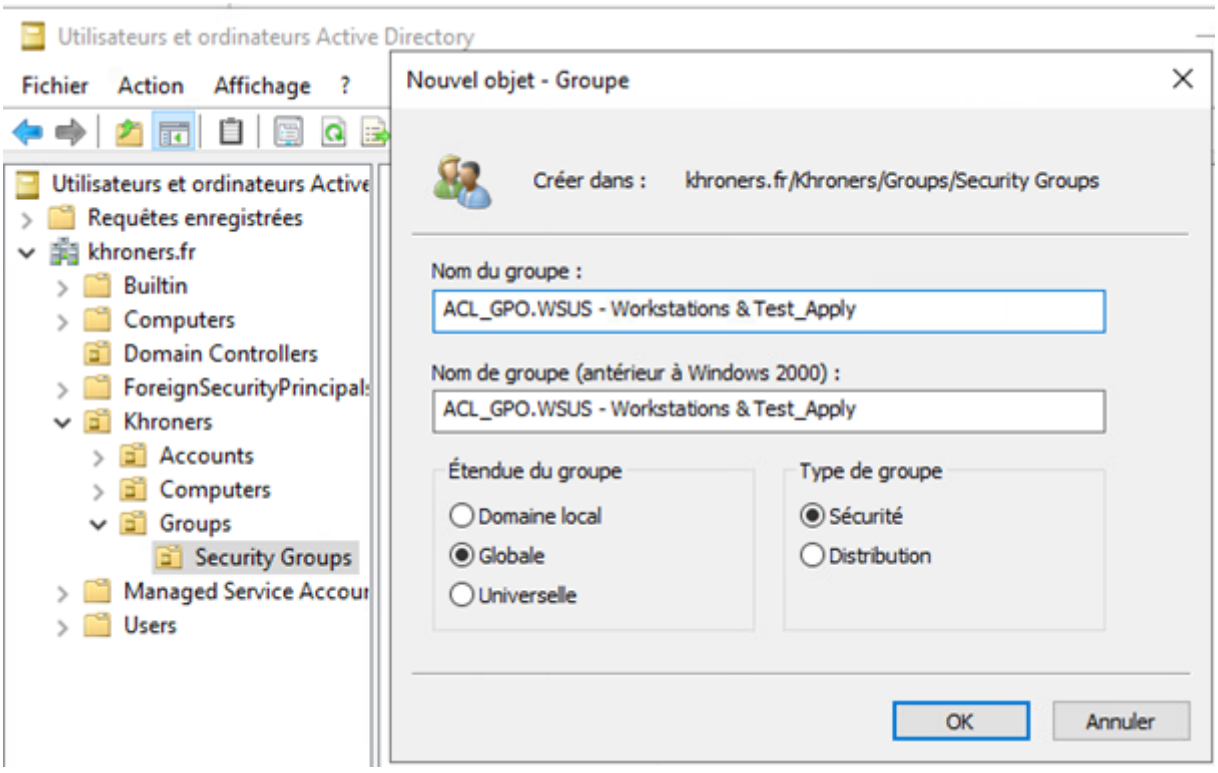
On n'oublie pas les contrôleurs de domaine.



Création des groupes de tests

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

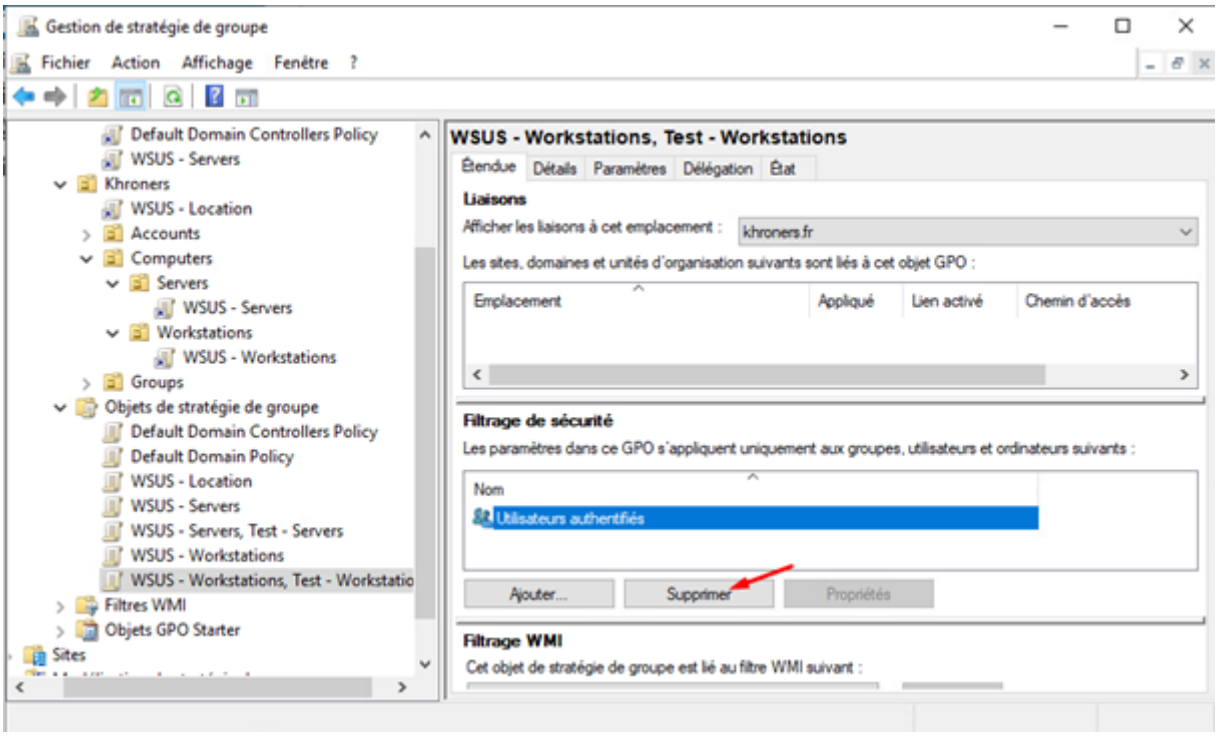
- ACL_GPO.WSUS - Workstations & Test_Apply
- ACL_GPO.WSUS - Workstations & Test_Deny
- ACL_GPO.WSUS - Servers & Test_Apply
- ACL_GPO.WSUS - Servers & Test_Deny



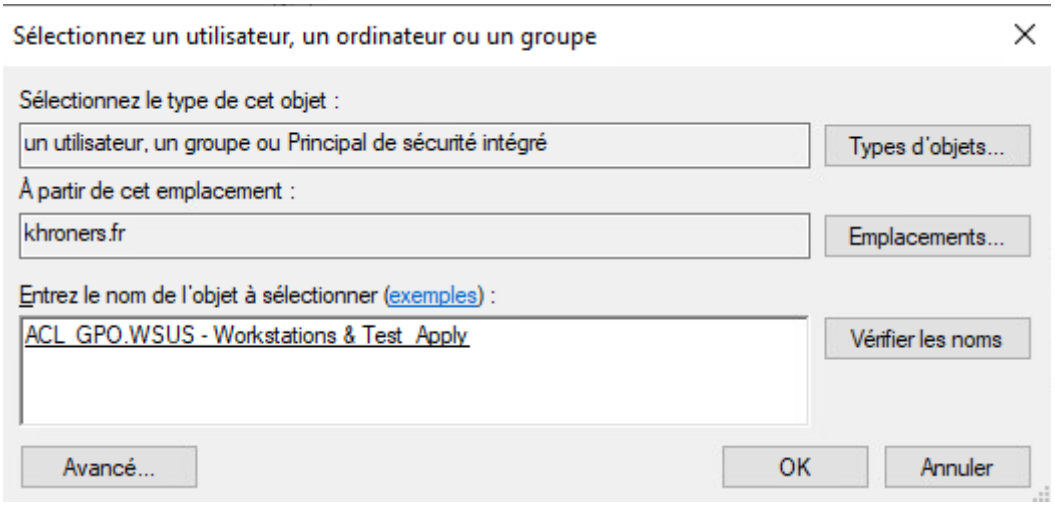
On fait la même chose pour les 3 autres groupes à créer.

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...

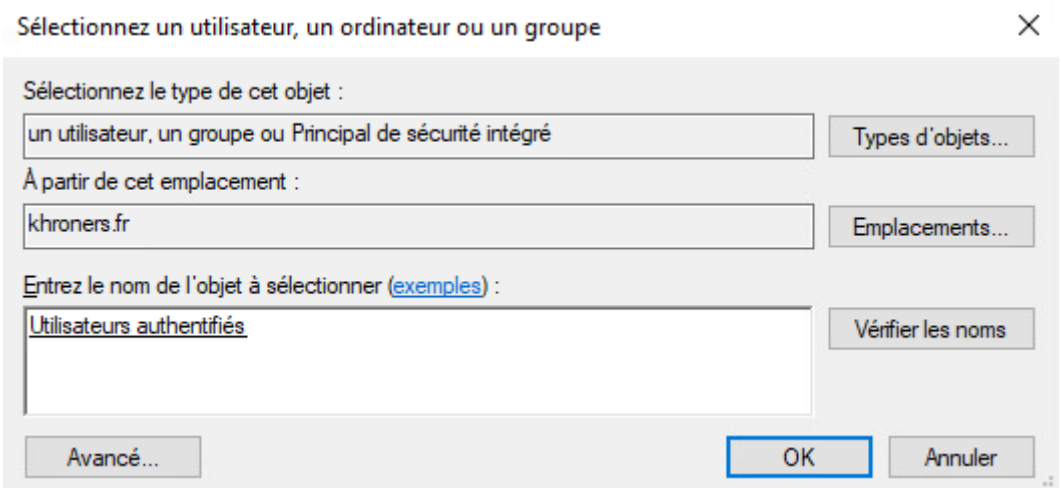
Dans la console de Gestion de stratégie de groupe, on clique sur la GPO "WSUS - Workstations, Test - Workstations", dans la partie "Filtrage de sécurité", on supprime "Utilisateurs authentifiés".

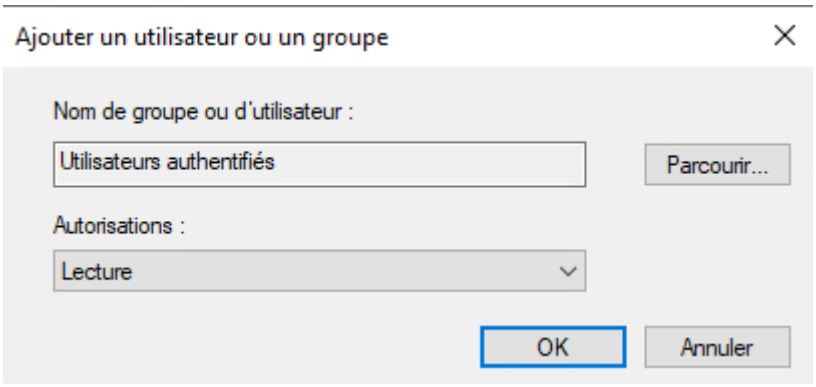


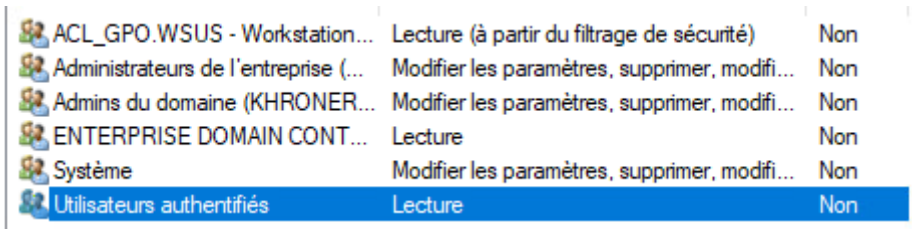
On clique ensuite sur "Ajouter..." puis on ajoute le groupe "ACL_GPO.WSUS - Workstations & Test_Apply".



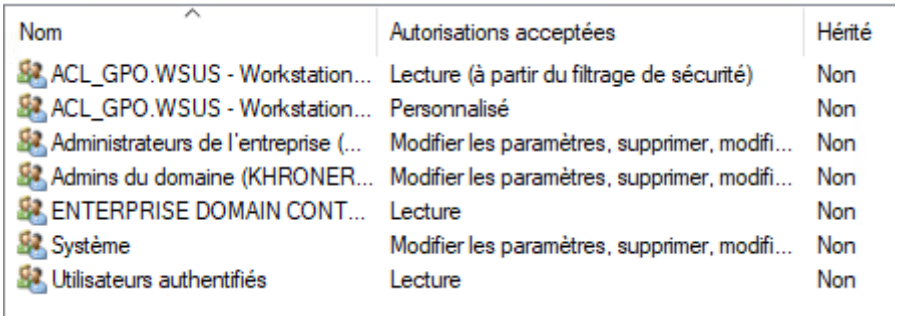
Dans l'onglet Délégation, on ajoute « Utilisateurs authentifiés » en lecture.







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.

Revision #7
Created 18 January 2021 17:59:56 by Khroners
Updated 12 March 2023 09:36:29 by Khroners