

# 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 travail et serveurs du domaine puissent se mettre à jour via le WSUS et non par les serveurs de Microsoft.

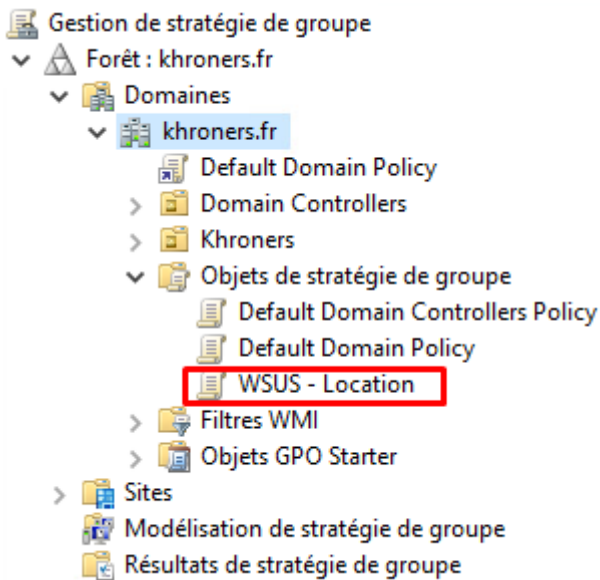
---

## Création des GPO

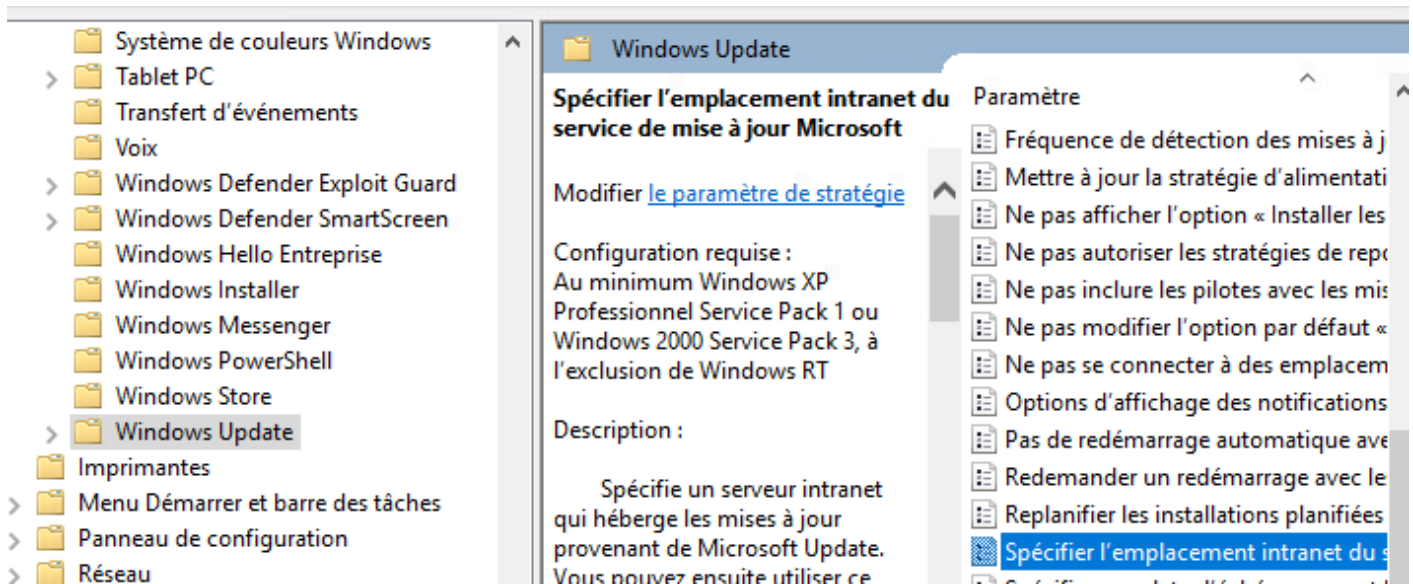
---

### 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)

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    Commentaire :

Activé

Désactivé

Pris en charge sur :

Options : Aide :

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

Configurer le serveur intranet de statistiques :

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.

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 nom de serveur facultatif afin de configurer l'agent Windows Update pour le téléchargement des mises à jour à partir d'un serveur de téléchargement

## 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".

Mode de téléchargement

Mode de téléchargement

Paramètre précédent Paramètre suivant

Non configuré    Commentaire :

Activé

Désactivé

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

Options :

Mode de téléchargement : Réseau local (1)

Aide :

Spécifie la méthode de téléchargement que l'Optimisation de la distribution peut utiliser dans les téléchargements des mises à jour Windows, des applications et des mises à jour de l'application.

La liste suivante indique les valeurs prises en charge :

0 = HTTP uniquement, pas d'homologation.

1 = HTTP mélangé avec homologation derrière le même NAT.

2 = HTTP mélangé avec homologation à travers un groupe privé. L'homologation se produit sur les appareils du même site Active Directory (s'il existe) ou du même domaine par défaut. Lorsque cette option est sélectionnée, l'homologation croise les NAT. Pour créer un groupe personnalisé, utilisez l'ID de groupe en combinaison avec le mode 2.

3 = HTTP mélangé avec homologation Internet.

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

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 :

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

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

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 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 :

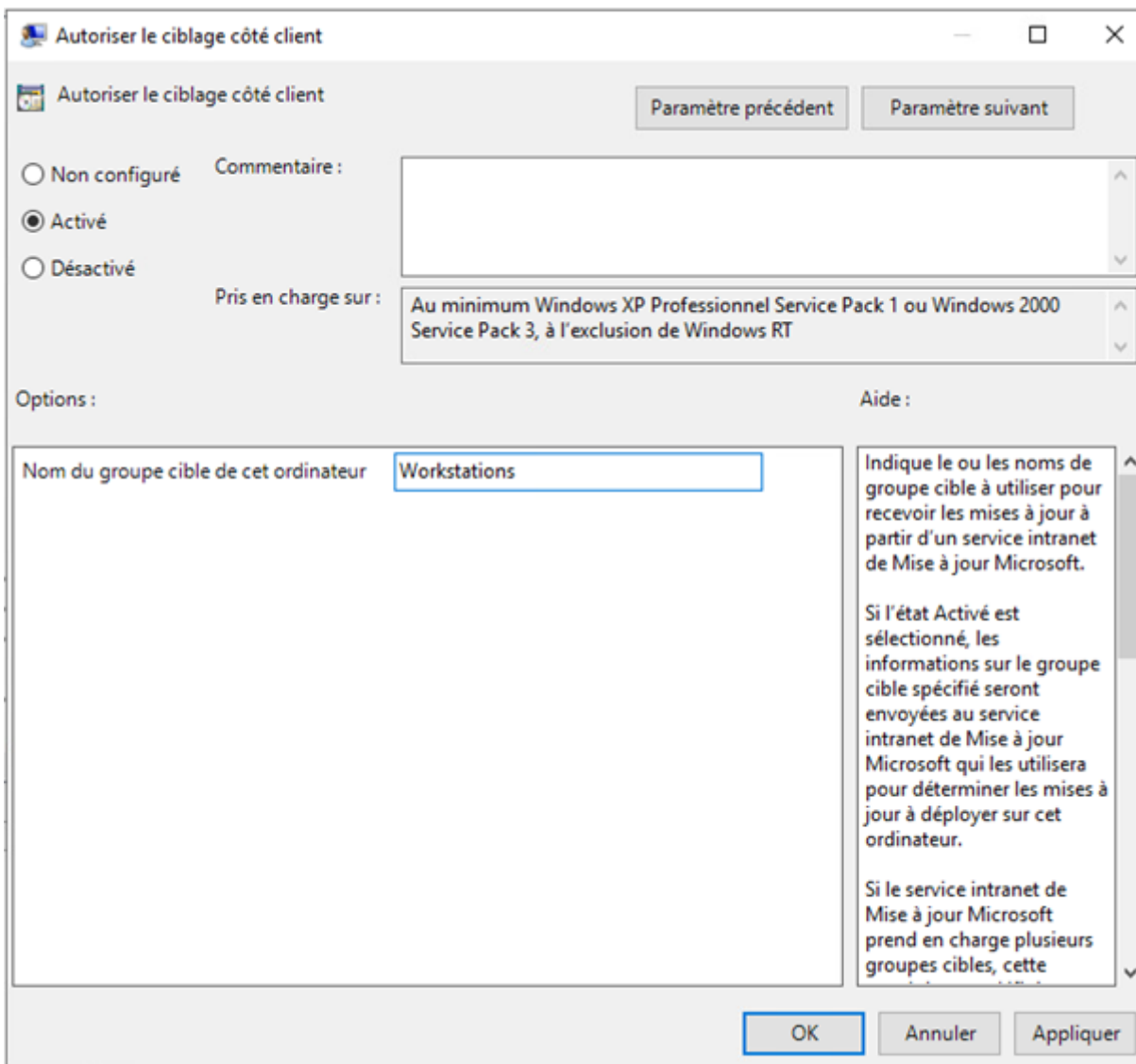
Chaque semaine

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.

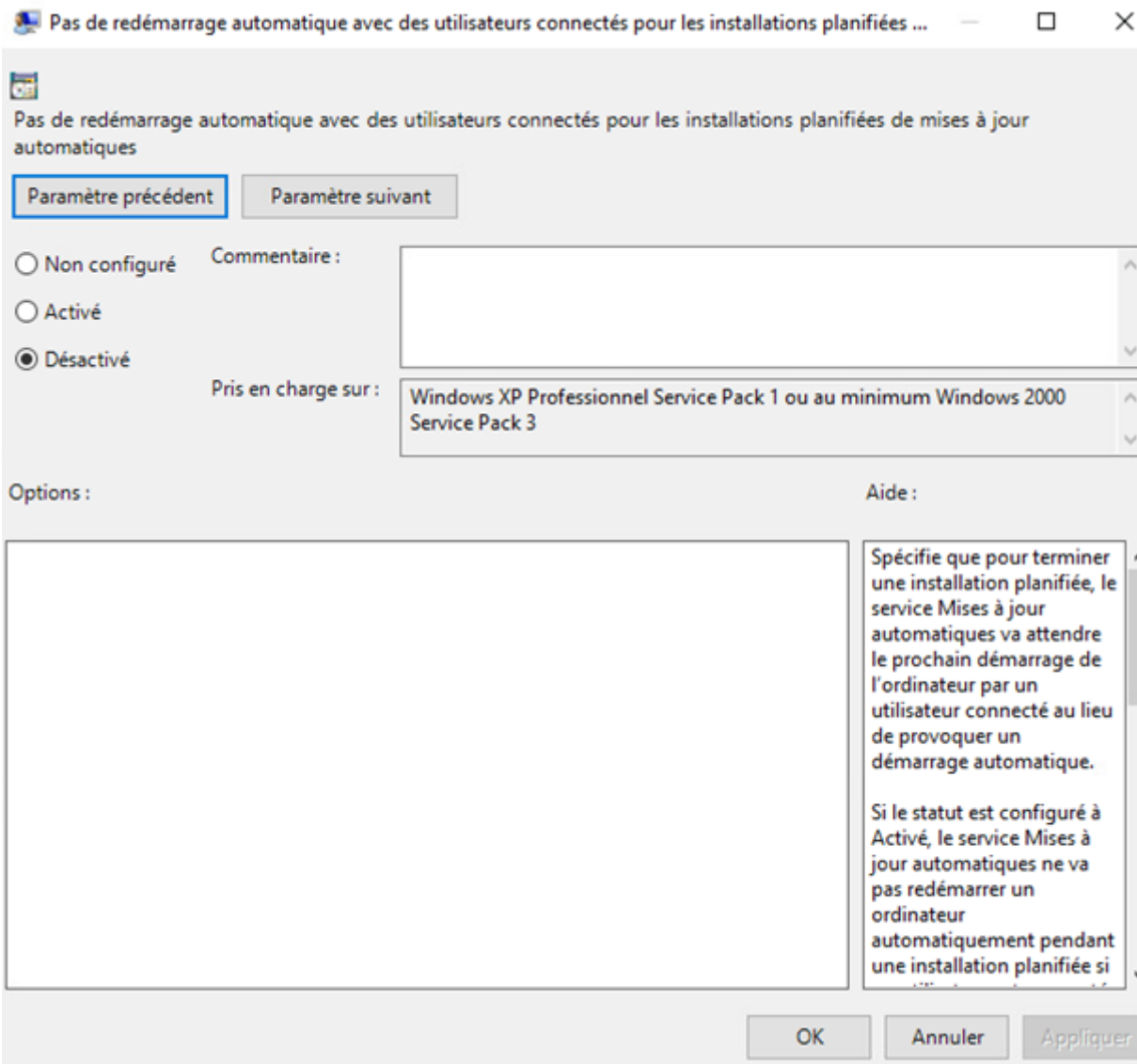
Ce paramètre de stratégie vous permet de spécifier si les mises à jour automatiques sont activées sur cet ordinateur. Si le service est activé, vous devez sélectionner l'une des quatre options du paramètre de stratégie de



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](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

Commentaire :

Activé

Désactivé

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 redémarrage, les heures

OK

Annuler

Appliquer

Spécifier une date d'échéance avant le redémarrage automatique pour l'installation de la mise à jour

Paramètre précédent

Paramètre suivant

Non configuré

Commentaire :

Activé

Désactivé

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) :

Mises à jour des fonctionnalités (jours) :

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.

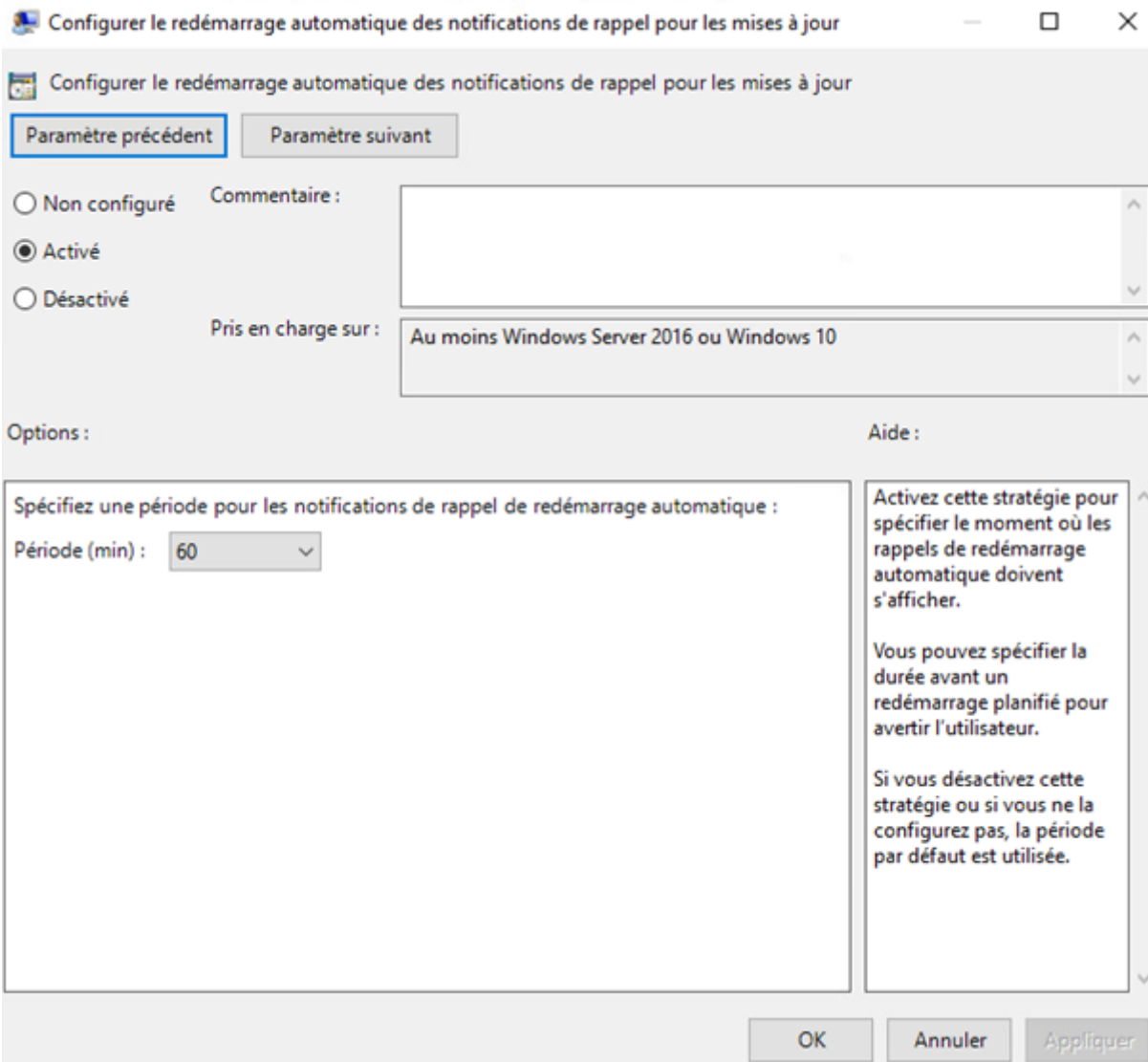
Le redémarrage peut se produire dans les heures d'activité.

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

Commentaire :

Activé

Désactivé

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 avec le service pack le plus récent

Options :

Aide :

Empty text area for options.

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 prêtes à être installées.

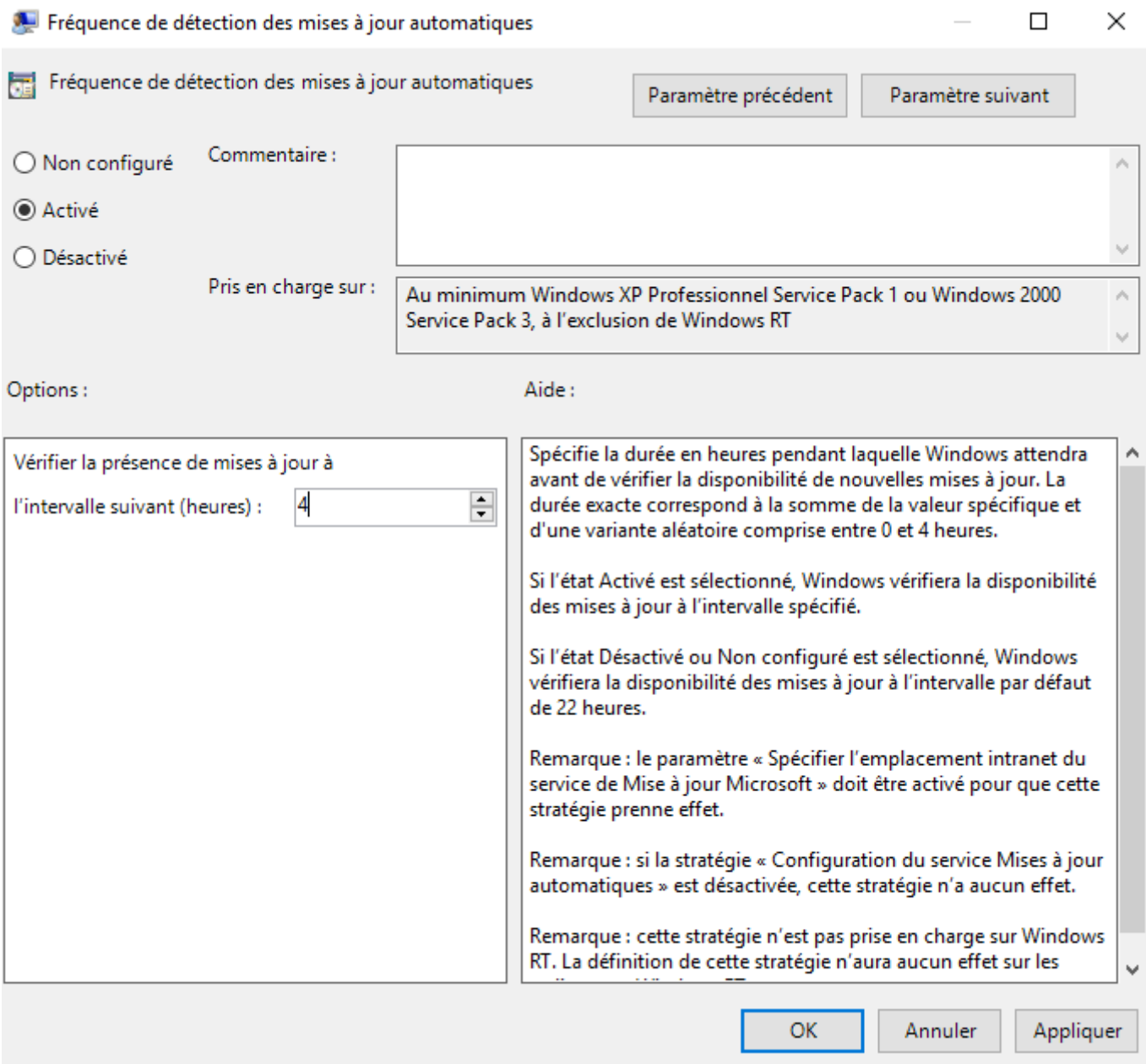
Si l'état Désactivé est sélectionné, ce type de mise à jour ne sera pas installé immédiatement.

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 :

- 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 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

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 :

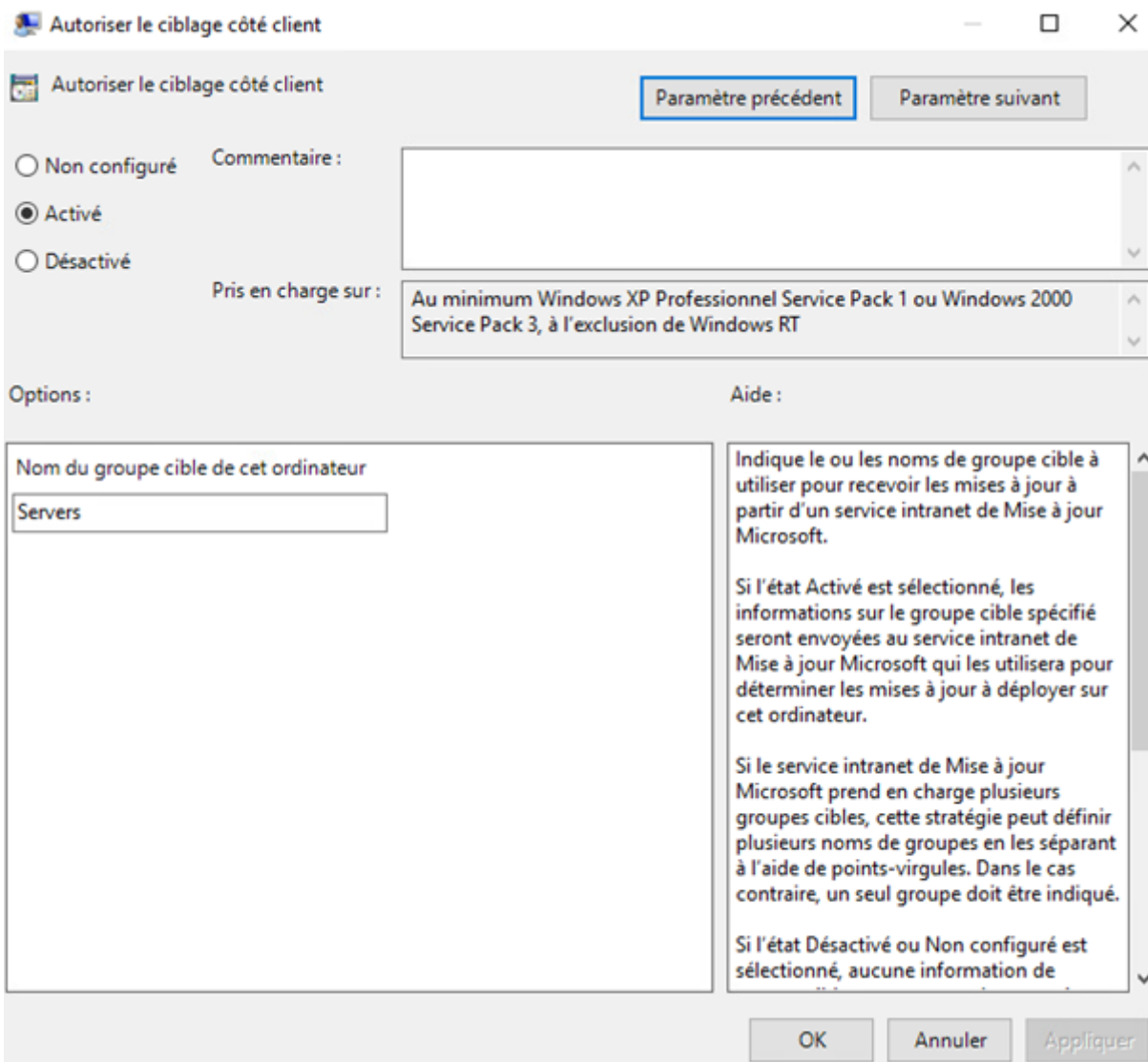
2 = Avertir avant de télécharger et d'installer des mises à jour.

Lorsque Windows trouve des mises à jour s'appliquant à l'ordinateur, un message indique à l'utilisateur que des

OK

Annuler

Appliquer



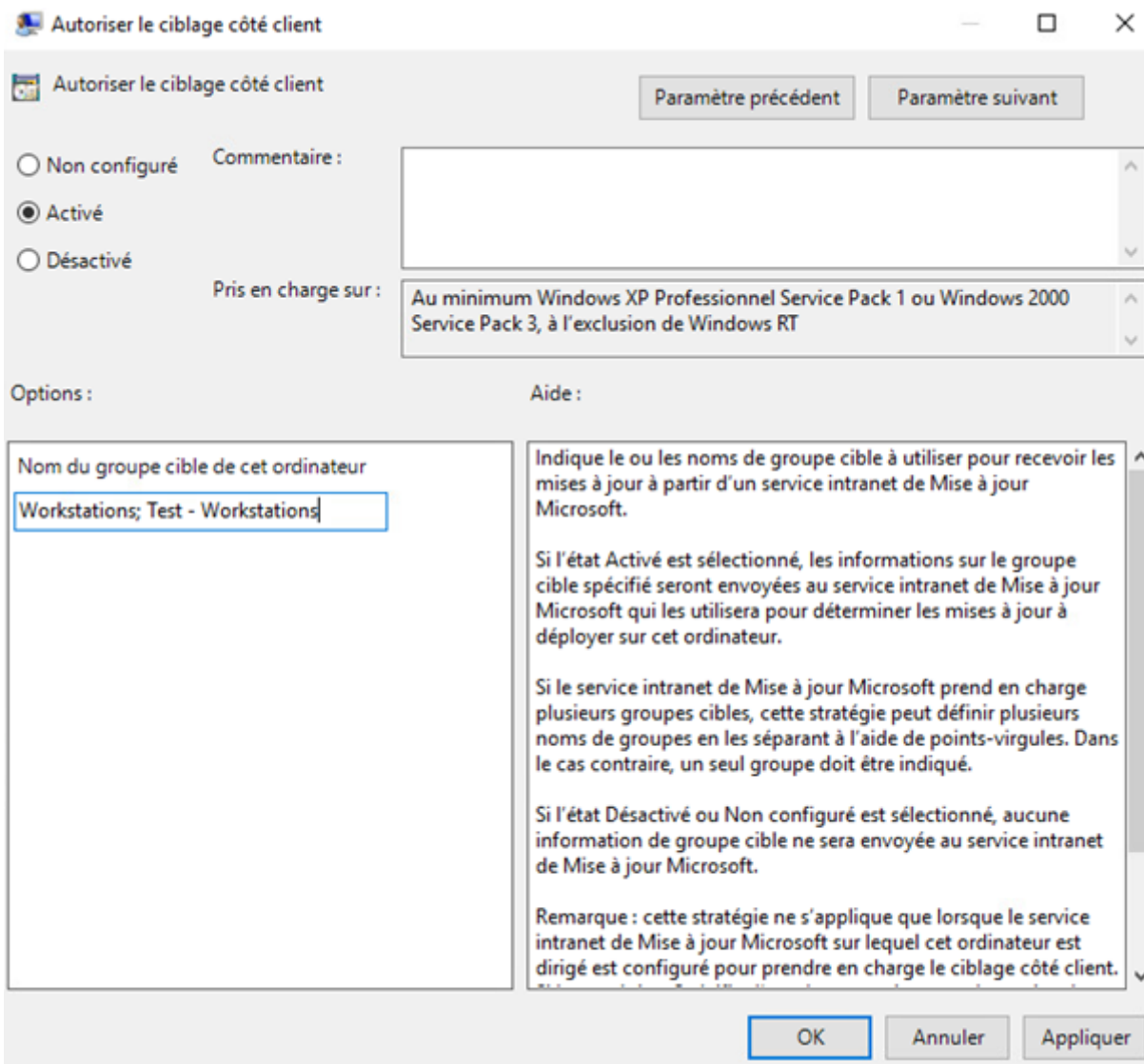
Si on a une farm de serveurs, il est préférable de créer plusieurs 'anneaux' de planifications et groupes, en choisissant l'option 4 : "Téléchargement automatique et planifier l'installation" et forcer le redémarrage lors de la maintenance des serveurs.

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

**Autoriser le ciblage côté client**

**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

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.

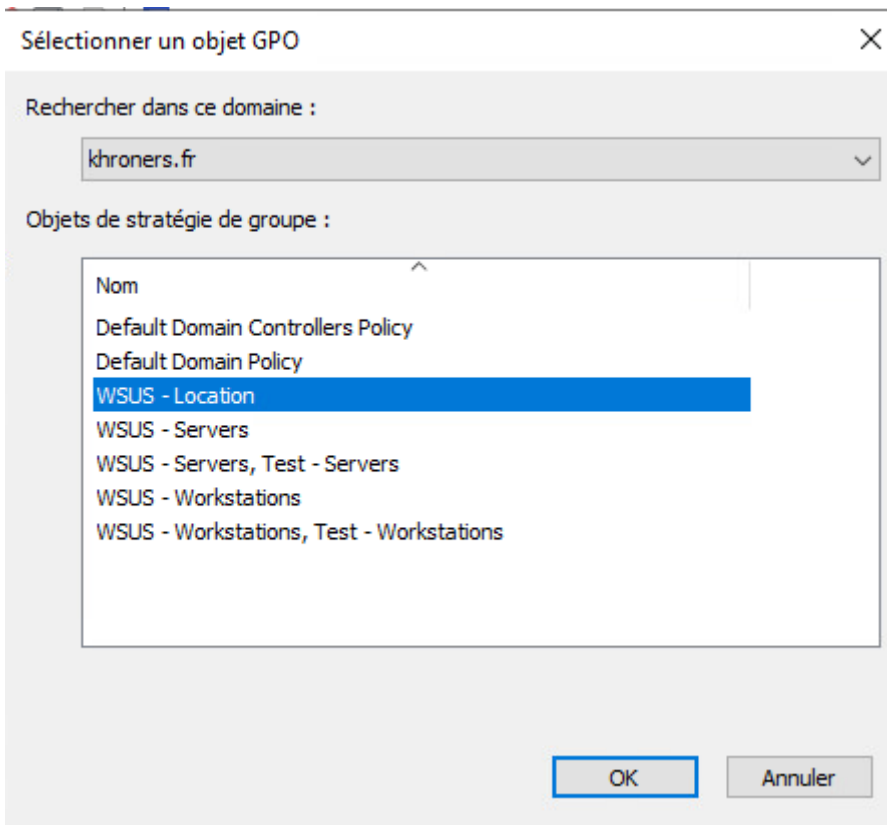
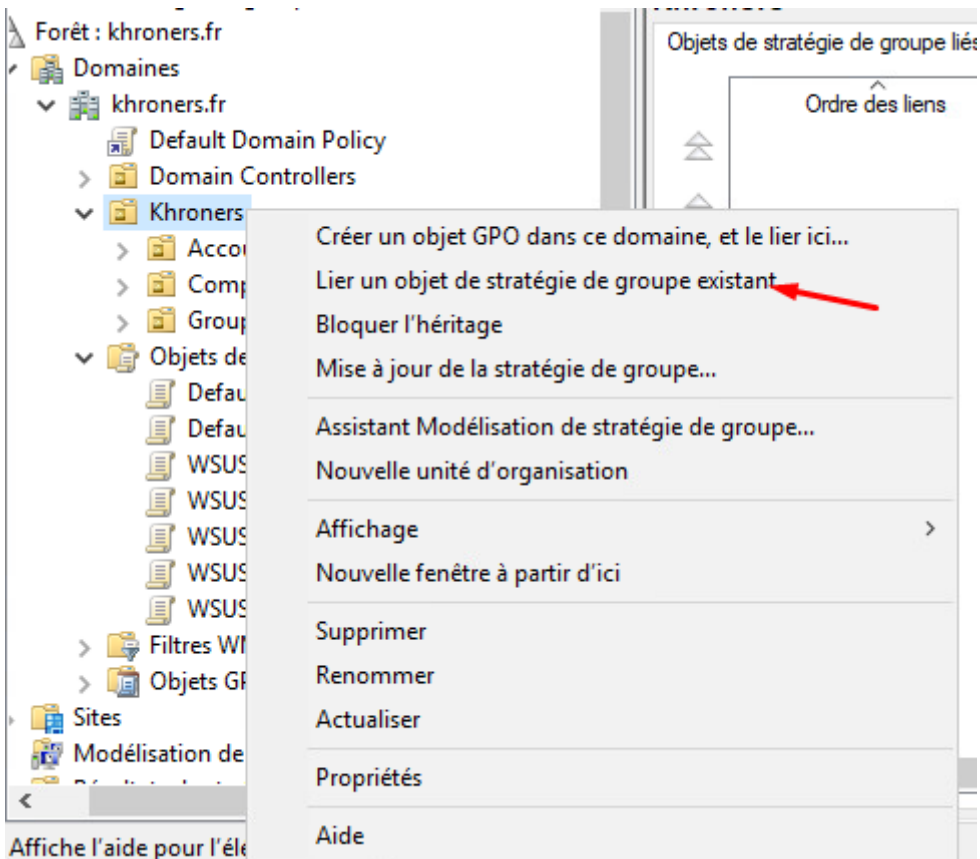
Si l'état Désactivé ou Non configuré est sélectionné, aucune information de groupe cible ne sera envoyée au service intranet de Mise à jour Microsoft.

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.

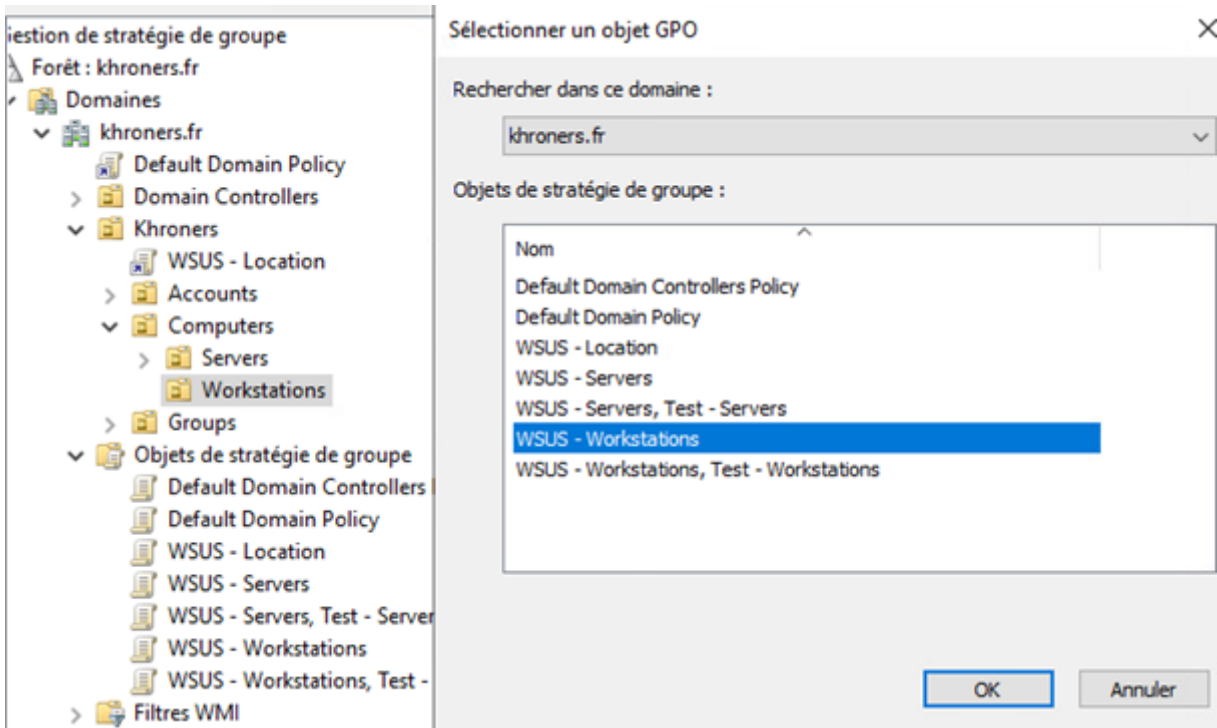
OK Annuler Appliquer

Lier les GPO aux bonnes OU

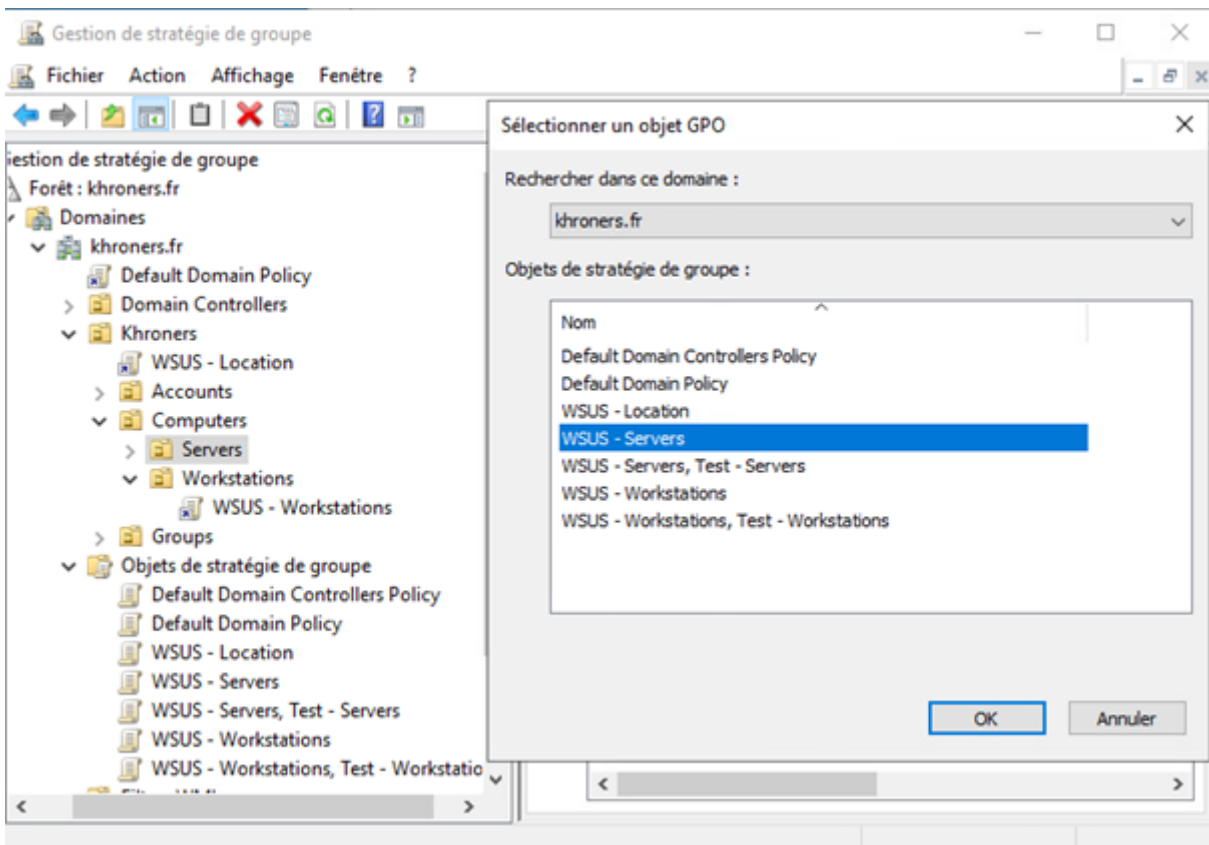
On applique la GPO de l'emplacement à toute l'OU.



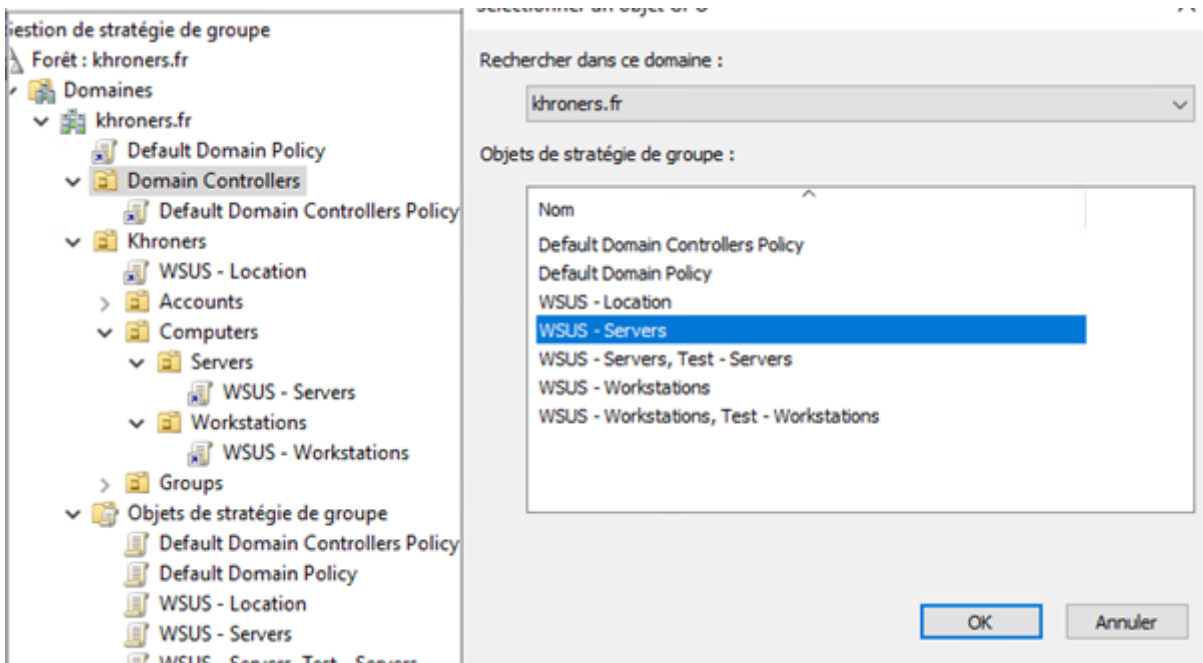
On applique pour les postes de travaux la GPO correspondante.



De même pour les serveurs.



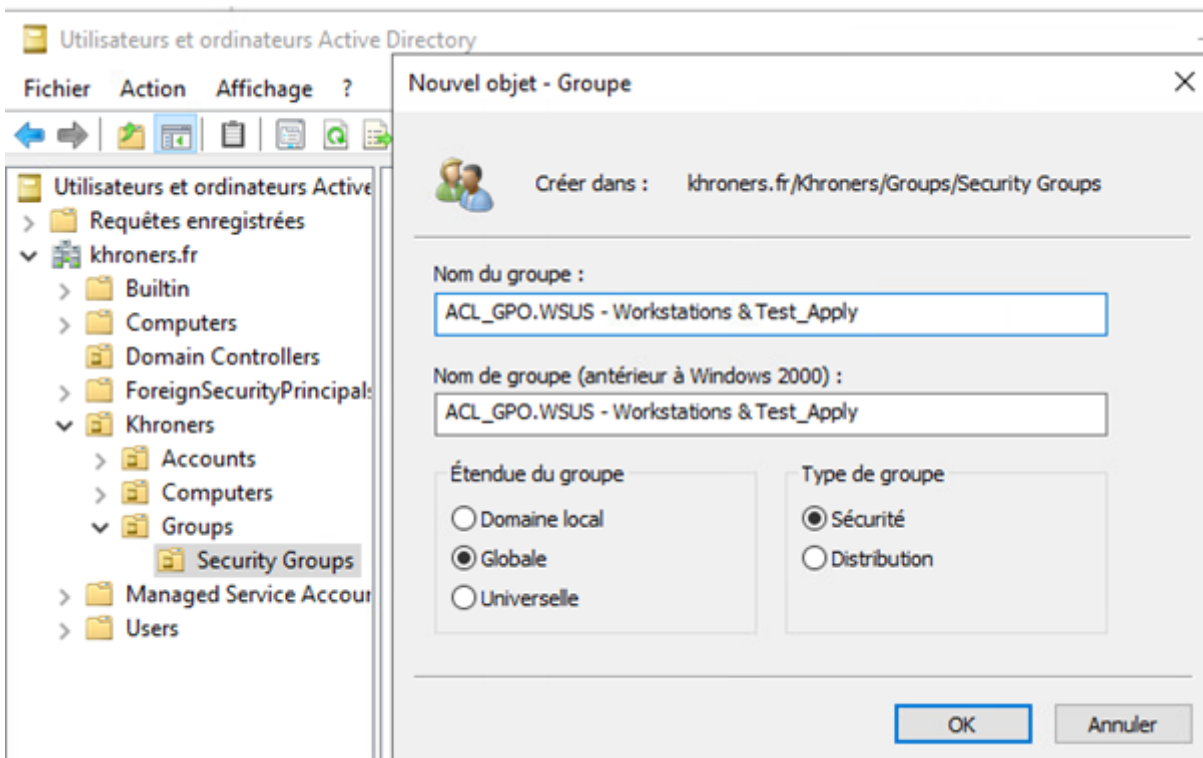
On n'oublie pas les contrôleurs de domaine.



# Création des groupes de tests

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

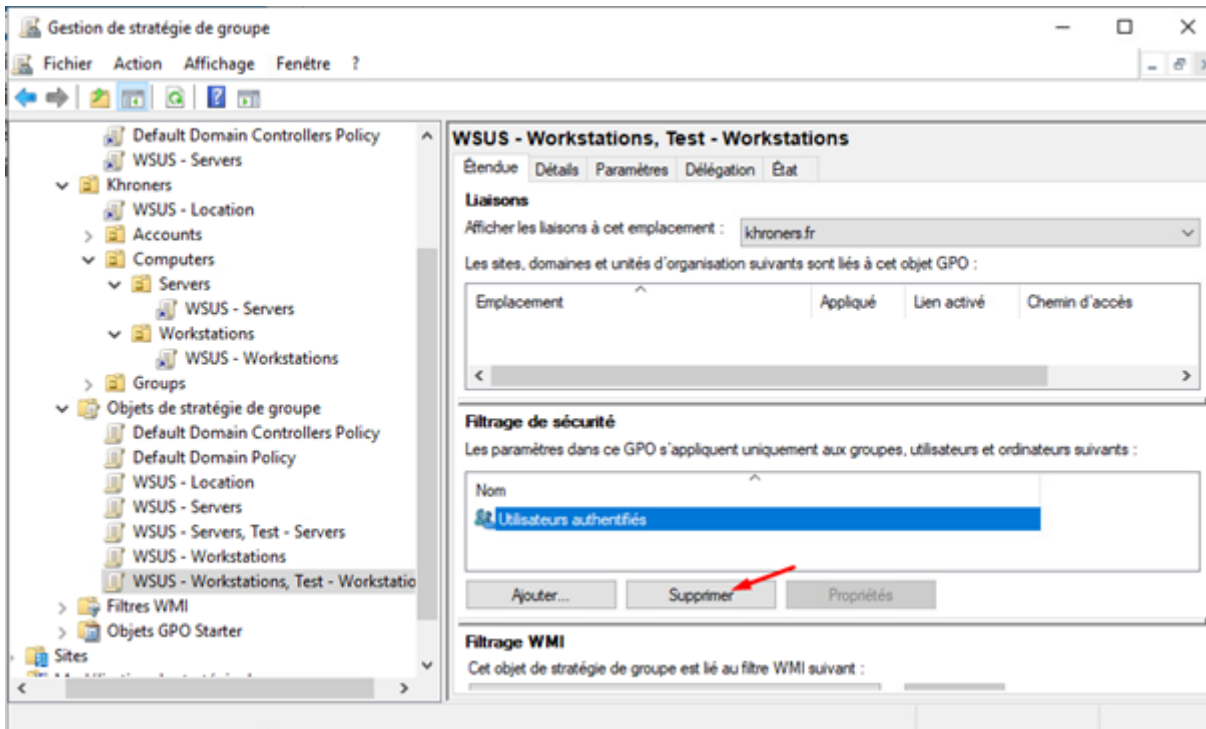
- ACL\_GPO.WSUS - Workstations & Test\_Apply
- ACL\_GPO.WSUS - Workstations & Test\_Deny
- ACL\_GPO.WSUS - Servers & Test\_Apply
- ACL\_GPO.WSUS - Servers & Test\_Deny



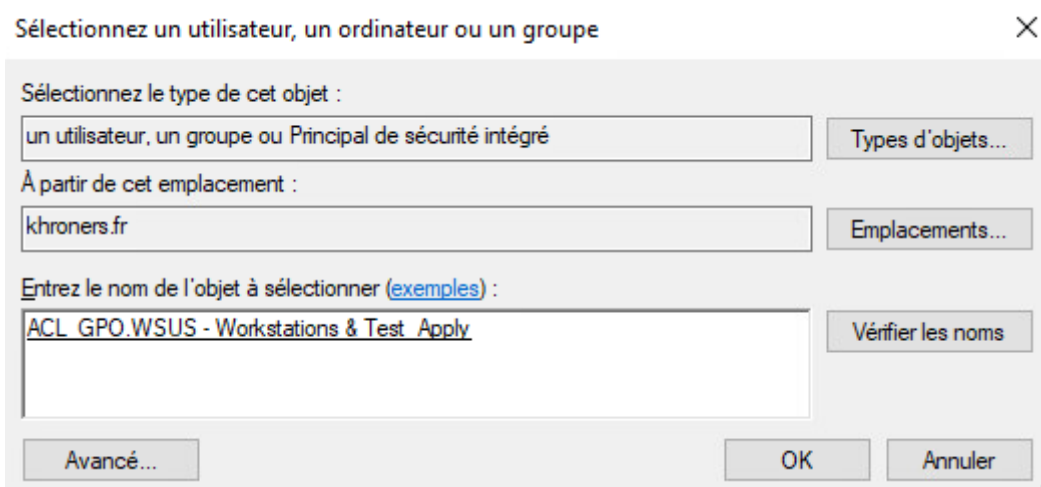
On fait la même chose pour les 3 autres groupes à créer.

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.

Sélectionnez un utilisateur, un ordinateur ou un groupe



Sélectionnez le type de cet objet :

un utilisateur, un groupe ou Principal de sécurité intégré

Types d'objets...

À partir de cet emplacement :

khroners.fr

Emplacements...

Entrez le nom de l'objet à sélectionner (exemples) :

Utilisateurs authentifiés

Vérifier les noms

Avancé... OK Annuler

Ajouter un utilisateur ou un groupe



Nom de groupe ou d'utilisateur :

Utilisateurs authentifiés

Parcourir...

Autorisations :

Lecture

OK Annuler

ACL_GPO.WSUS - Workstation...	Lecture (à partir du filtrage de sécurité)	Non
Administrateurs de l'entreprise (...)	Modifier les paramètres, supprimer, modifi...	Non
Admins du domaine (KHRONER...	Modifier les paramètres, supprimer, modifi...	Non
ENTERPRISE DOMAIN CONT...	Lecture	Non
Système	Modifier les paramètres, supprimer, modifi...	Non
Utilisateurs authentifiés	Lecture	Non

On clique sur Avancé et on ajoute ACL\_GPO.WSUS - Workstations & Test\_Deny avec les permissions refusées.

Nom	Autorisations acceptées	Hérité
ACL_GPO.WSUS - Workstation...	Lecture (à partir du filtrage de sécurité)	Non
ACL_GPO.WSUS - Workstation...	Personnalisé	Non
Administrateurs de l'entreprise (...)	Modifier les paramètres, supprimer, modifi...	Non
Admins du domaine (KHRONER...	Modifier les paramètres, supprimer, modifi...	Non
ENTERPRISE DOMAIN CONT...	Lecture	Non
Système	Modifier les paramètres, supprimer, modifi...	Non
Utilisateurs authentifiés	Lecture	Non

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