Installation automatique des définitions de Microsoft Defender

---

Présentation

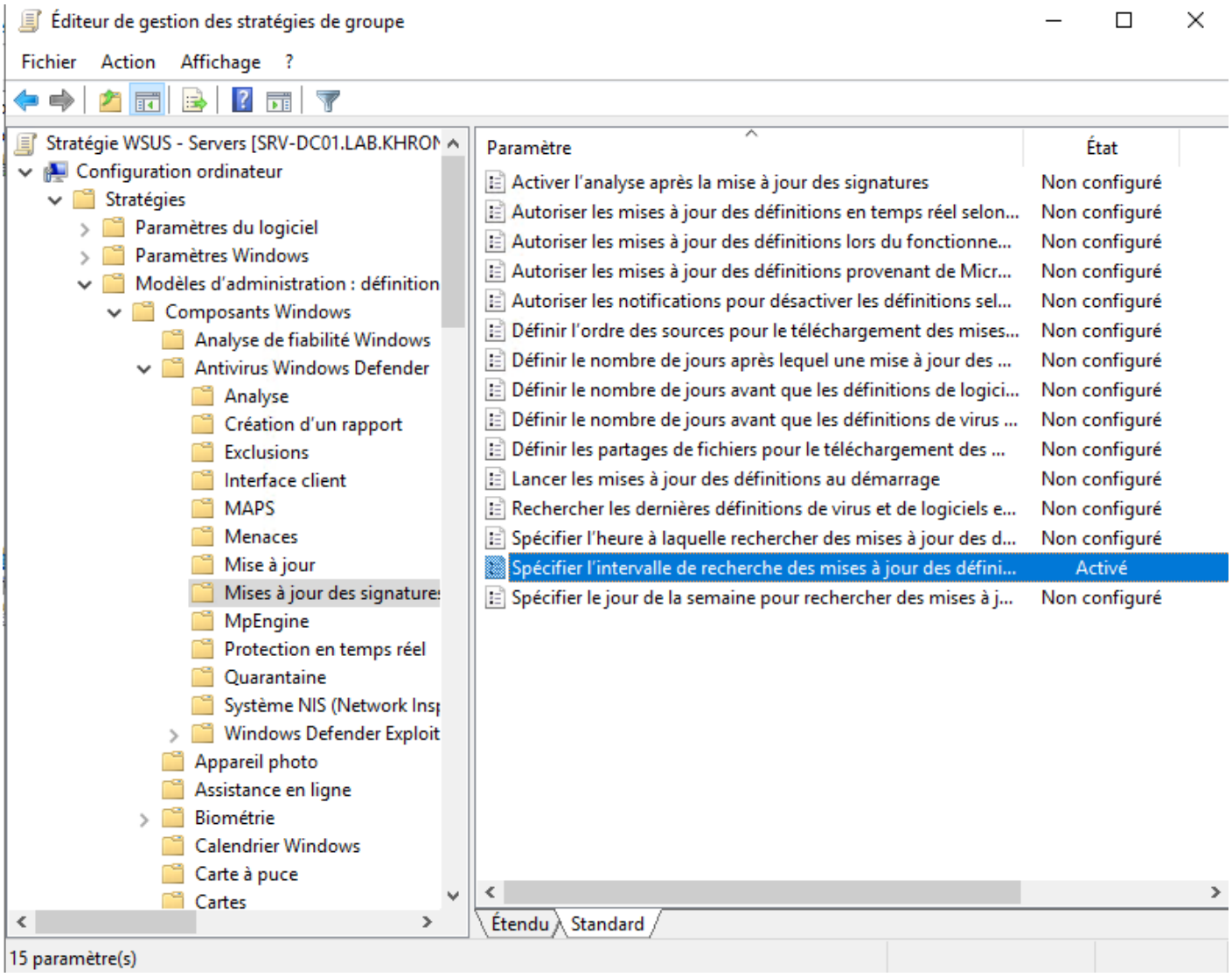
Par défaut, les définitions de Microsoft Defender sont mises à jour toutes les 24 heures, ou via Windows Update selon la fréquence de recherche de mises à jour. Cependant, selon les GPO mises en place précédemment, elles ne s'installent pas automatiquement (sauf à l'heure planifiée pour les Workstations).

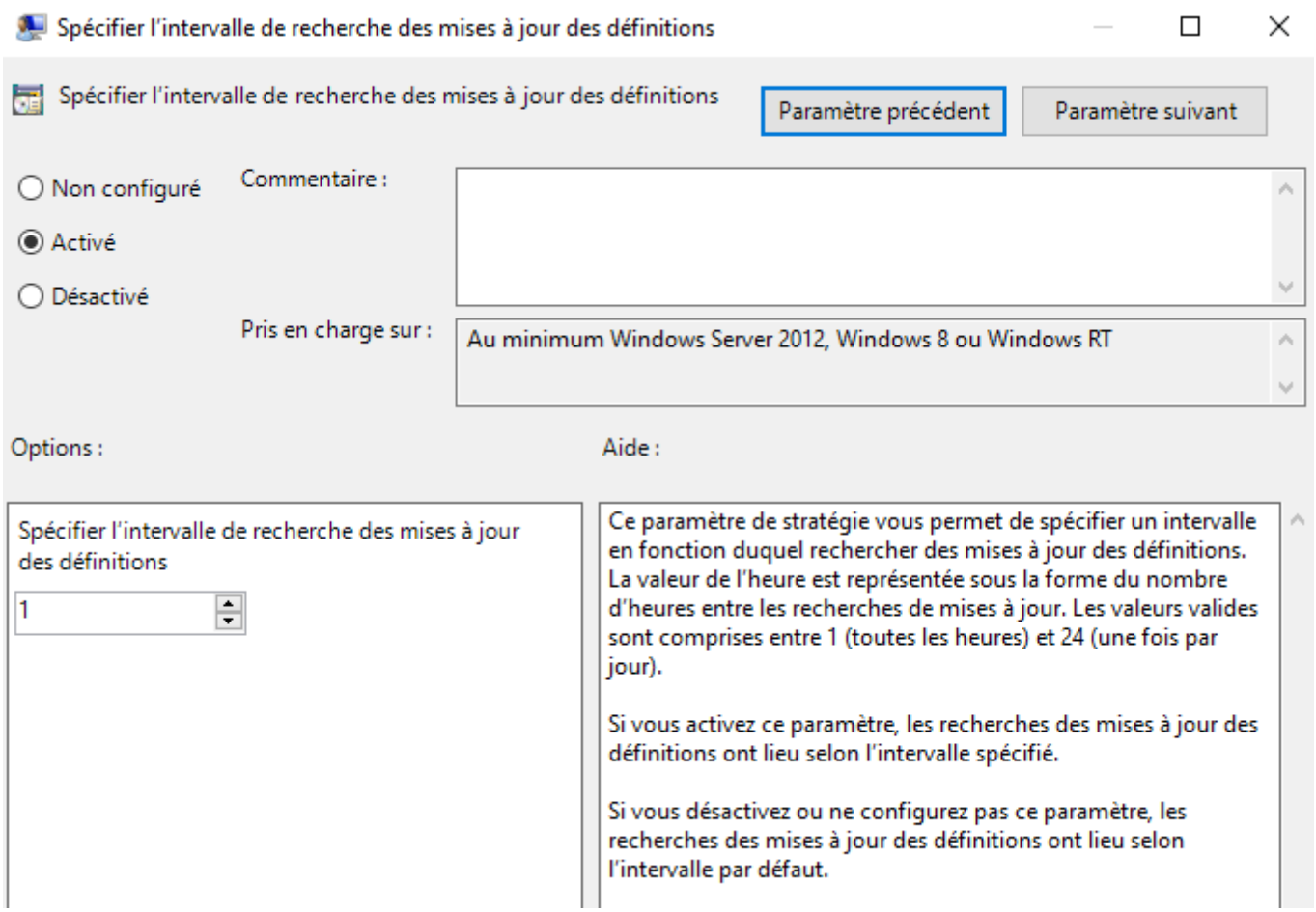
> En soit, déployer les mises à jour de Defender n'est pas primordial. A chaque mise à jour, WSUS retélécharge tout (60-70mo en moyenne pour le moment), alors que de passer d'une mise à jour à une autre prend environ 1mo, selon la mise à jour des définitions.
> Cela peut être utile en cas de déploiement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

Revision #2
Created 31 May 2021 11:43:07 by Khroners
Updated 30 December 2021 23:45:14 by Khroners