

**C**entre  
**A**cadémique de  
**R**essources et de  
**M**aintenance  
**I**nformatique  
**E**quipements  
**P**édagogiques

Le 17/09/13

MINISTÈRE DE  
L'ÉDUCATION NATIONALE

MINISTÈRE DE  
L'ENSEIGNEMENT SUPÉRIEUR  
ET DE LA RECHERCHE



*Equipements - Assistance - Maintenance*

Code fichier :maj\_def\_sav\_sans\_liveupdate.doc

## MAJ définitions de SAV sans Liveupdate

Depuis 07/2013 l'antivirus installé sur les serveurs symantec (Corporate version 10.1.x) dans les établissements de l'académie ne met plus à jour ses définitions de virus via liveupdate. Les clients rattachés aux serveurs parents ne mettent donc pas non plus leurs définitions à jour.

Ceci est dû au fait que ce produit n'est plus maintenu par symantec.

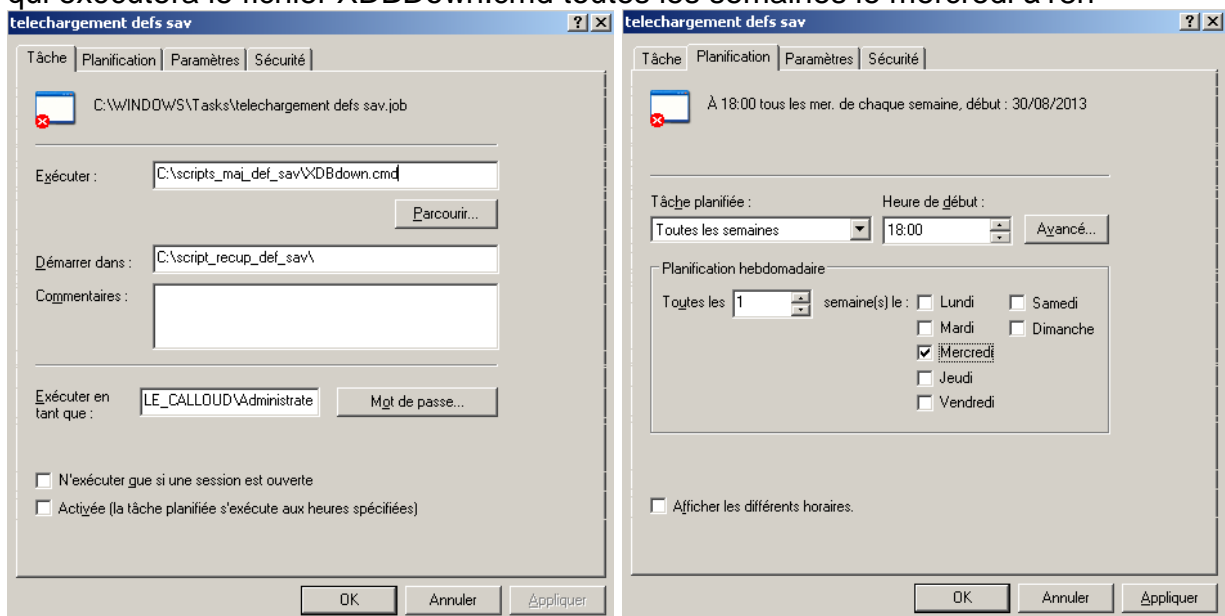
Le problème est le même pour les clients autonomes, liveupdate ne fonctionne plus.

Malgré tout, pour l'instant les définitions de virus compatibles avec ce produit sont encore mises à jour et publiées

### 1) Procédure pour les serveurs antivirus

#### 1<sup>ère</sup> solution :

- Télécharger le script [XDBdown.cmd](#) sur le site assistance technique aux prt
- Sur le serveur, enregistrer ce script C:\ dans un dossier « scripts\_maj\_def\_sav »  
(⚠ Attention, il ne faut pas le mettre dans C:\Program Files\SAV\)
- Réaliser une tâche planifiée (Démarrer/exécuter/tasks)  
nommée "telechargement defs sav"  
qui exécutera le fichier XDBDown.cmd toutes les semaines le mercredi à 18h



- d) Faire un test de bon fonctionnement de la tâche (clic droit-Exécuter)  
une fenêtre de commande s'ouvre et le dernier fichier xdb en cours se télécharge  
Attendre la fin du téléchargement et attendre encore quelques minutes puis vérifier  
que les définitions de virus se sont mises à jour  
Par la suite, les jours suivants, vérifier la colonne dernier résultat de la tâche planifiée  
: il doit afficher 0x0  
Au bout de quelques temps, vérifier que les clients se sont mis à jour aussi.

En cas d'erreur du script, points à vérifier :

- Editer le fichier log qui peut indiquer d'où vient le problème...
- Tester le bon fonctionnement du protocole ftp (port 21 en principe ouvert par défaut sur les slis)
- Ne pas supprimer le fichier xdbdown.lastfile qui doit se créer la 1<sup>ère</sup> fois dans le dossier « scripts\_maj\_def\_sav »
- Vérifier les droits d'écriture dans %temp%

Si après ces vérifications, rien ne semble évident, utiliser la 2<sup>ème</sup> solution...

- e) Aller dans la console symantec center et désactiver la mise à jour planifiée des définitions sur le serveur (sinon l'observateur d'événement se remplit)  
Clic droit sur le serveur principal - toutes les tâches- Symantec antivirus -  
Gestionnaire des définitions de virus - 1er point : mettre à jour le serveur principal -  
configurer - Décocher "Planifier des maj automatiques" et valider OK 2 fois

## **2<sup>ème</sup> solution :**

En cas de dysfonctionnement du script XDBdown.cmd (développé par Symantec) il est possible d'utiliser un autre script développé par un ANT du CG38.

Télécharger [script\\_navup8.cmd](#) et s'inspirer de la procédure décrite dans la 1<sup>ère</sup> solution et créer une tâche planifiée qui l'utilisera.

Au niveau de la planification de la tâche, il est possible de l'exécuter tous les jours, car avec cet autre script, les définitions téléchargées sont publiées quotidiennement.  
A voir selon l'état de vétusté du parc, sachant que les clients mettent un peu plus de temps à démarrer lors de la maj de leurs définitions de virus.

## **2) Procédure pour les clients autonomes**

Pour les clients non rattachés à un serveur parent comme par exemple les serveurs ou stations appartenant à la DMZ (ex : serveur Pronote relais-net, serveur TPWORKS, ...), télécharger le script : [XDBdown\\_autonome.cmd](#) et s'inspirer de la procédure décrite dans la 1<sup>ère</sup> solution et créer une tâche planifiée qui l'utilisera.