### Ministère de l'Education Nationale - Académie de Grenoble - Région Rhône-Alpes



Code fichier : pb\_espace\_disque\_defs\_virus.doc

# En cas d'échec de maj des defs de virus – espace disque insuffisant

#### Symptômes :

Un phénomène de manque de place sur la partition système, et du coup l'impossibilité pour sav

de mettre à jour ses définitions de virus est souvent constaté (quand on va sur le bouclier elles datent de plus de 15 jours ou plus encore)

C'est un cercle vicieux, moins y a de place, plus les .tmp et les . xdb et .vdb s'accumulent, ne s'effaçant pas, et du coup moins y' a de place...comme la tentative de mise à jour est quotidienne, on arrive à des espaces disque de l'ordre de 250 mo...

De même, on a souvent dans ces cas là, des erreurs dans l'observateur d'évènements : - dans Application :

une erreur indique que la quarantaine n'a pas la place minimum définie pour le dossier quarantaine

vénement		
<u>D</u> ate : <u>H</u> eure : <u>Type :</u> Utilisateur : O <u>r</u> dinateur :	18/02/2011 16:41:50 Erreur N/A S1380278	Sourc <u>e</u> : Quarantaine centralisée Catégorie : Aucun ID é <u>v</u> én. : 34054 B
Avertissen	generale de la Qua ient concernant l'es	rantaine centralisée a été détectée. pace disque - Espace disque libre inférieur à la taille de .
Avertissem guarantain Serveur de Adresse : 1 Avertissem dossier Qu- Supprimez	generale de la Qua ient concernant l'es e maximale] quarantaine : S138 72.16.0.11 Nom D ent : L'espace disqu arantaine les échantillons inut	rantaine centralisée a été détectée. pace disque - Espace disque libre inférieur à la taille de 10278 INS : S1380278.LE_CALLOUD.peda le libre est inférieur à la taille maximale définie pour le iles ou libérez de l'espace

- dans "Service de réplication de fichiers" une erreur du service de réplication qui n'a pas assez d'espace sur C

opriétés o	le Erreur		?
vénement			
Date : Heure : Type : Utilisateur Ordinateu	15/02/2011 13:11:14 Erreur : N/A r: \$1380278	Sourc <u>e</u> : NtFrs Catégorie : Aucun ID é <u>v</u> én : 13570	+ + =
Descriptio	n : e de réplication de fic	hiers a détecté que le volume héberg	eant le chemin 🔺
d'accès l fichiers n l'espace	2: ne dispose pas de s e soient pas répliqués disque sur ce volume.	suffisamment d'espace disque. Il se po aussi longtemps que vous ne libérez	eut que les pas de
Vous pou	ivez rechercher de l'e	space disponible sur le volume en tap	ant "dir /a C:".
Pour plus ''rename	d'informations sur la ( /?'', ''del /?'', ''rmdir /	gestion de l'espace sur un volume, tap ?'' et ''dir /?''.	oez "copy /?", 🗕 👻
Données	C Octets C	Mots	
1			ė
			×
2			T se e
		UK Annulei	Appliquer

# Solution : <u>1) Récupérer de l'espace sur C :</u>

## A) Actions par rapport aux dossiers de SAV

a) dans c:\program files\sav et aussi dans le sous dossier I2\_LDVP.VDB supprimer tous les anciens . xdb et .vdb (fichier et dossiers). Ne laisser que les 2 derniers en date.(on ne peut pas faire moins)

puis vérifier le registre :

#### HKEY\_LOCAL\_MACHINE\Software\Intel\Landesk\VirusProtect6\CurrentVersion\PatternsToKeep

 $\rightarrow$  si la valeur dword est à 1 la modifier à 2

 $\rightarrow$  si la clé n'existe pas, la créer avec comme valeur dword 2

la valeur 1 n'est pas supportée

# → pour éviter des erreurs de frappe télécharger le .reg suivant et le fusionner sur le serveur

b) depuis le panneau de configuration lancer symantec liveupdate et aller dans l'onglet "Cache des mises à jour"

(@)C	onfiguration de LiveUpdate	×
	-éral FTP   HTTP   FAI Cache des mises à jour	
diminuer le cache à 200 mo (actuellement le téléchargement des définitions de	Vous pouvez personnaliser la quantité d'espace que LiveUpdate utilisera pour les mises à jour téléchargées dans le cache. aille maximale du cache: Espace disque maximum utilisé pour stocker les mises à jour :	stocker
virus nécessite130		
mo onviron cont	► 200 II No	
necessaires)		
	aille actuelle du cache : 122.24 Mo	cliquer sur "supprimer
	Supprimer tous les fichiers du cache	tous les fichiers du cache"
	OK Annuler Appliquer	Aide

c) vérifier dans c:\program files\sav s'il reste des fichiers .tmp .Si c'est le cas les supprimer (si certains "résistent" car en cours d'utilisation procéder par lots)

d) dans C:\Program Files\Fichiers communs\Symantec Shared\VirusDefs supprimer les éventuels anciens sous dossiers avec d'anciennes définitions de virus, sauf les 2 derniers en date.

e) dans C:\Program Files\Fichiers communs\Symantec Shared\Reporting Agents\Win32 supprimer les éventuels .log

f) dans C:\Program Files\Fichiers communs\Symantec Shared\Reporting Agents\Temp supprimer les éventuel .tmp

g) déplacer la quarantaine symantec sur une autre partition qui a de l'espace libre

Se positionner sur "Quarantaine centralisée symantec (local) et faire clic droit propriétés (si elle n'apparaît pas, c'est qu'elle n'est pas installée)

🚡 Symante	ec System Center - [Racine de la ci	onsole\Symante	c System Cer	nter\Quarant	aine centralisée Sy	mantec (locale)]	
🚡 Eichier	Action Affichage Favoris Fenêt	re <u>?</u>					
🗢 🤿 🗄	E) 🖬 😭 🔄 😫 💷 📑 e la console	Nom du fichier	Utilicateur	Ordinateur	Nom du domaine	Recule	
Racine de la console Symantec System Center Hiérarchie du système Goupes Symantec AntiVirus 1 Groupes Si 380278 Quarantaine centralisée Symantec (loca		Nom du fichier Utilisateur Ordinateur Nom du domaine Reçu le Aucun élément à afficher dan Propriétés de Quarantaine centralisée Symantec (locale) Généralités					
	Remplacer C par D (p exemple)	Emplacement du dossier sur l'ordinateur serveur : C:\Program Files\Symantec\Quarantine\Server\Submis Taille maximale autorisée Seuil d'avertissemer 500 ÷ méga-octets 450 ÷ mo Nombre maximal d'échantillons autorisé 750 ÷ Purger les échantillo				issions ent néga-octets ions si nécessaire	
		Protocoles ✓ Surveillance sous [P Port : 33333 ✓ Surveillance sous SP☆ Port: 0 Console Intervalle d'actualisation auto 5 ✓ minutes					
				эк А	nnuler Appliqu	er Aide	

5ymantec (local	Propriétés de Quarantaine centralisée Symantec (locale)	
	Emplacement du dossier sur l'ordinateur serveur : Dt/Program Files/Symantec/Quarantine/Server/Submissions Taille maximale autorisée <u>Seuil d'avertissement</u> 500. <u>*</u> méga-octets 450 <u>*</u> méga-octets	
Avertissen ?	Voulez-vous déplacer les échantillons déjà en quarantaine vers le nouveau dossier de quarantaine ? Si vous répondez Oui, les échantillons seront déplacés. Si vous répondez Non, ils seront supprimés et QFolder sera actualisé. La réponse Annuler vous ramène à la boîte de dialogue.	
	Console Intervalle d'actualisation auto 5 minutes Cliquer sur Non pour supprimer les échantillons	
	OK Annuler Aide	

#### B) Autres actions indépendantes de SAV

a) supprimer les paquets de désinstallation de mises à jour et service pack (utiliser le script <u>199-</u> <u>Supr-PackUnInstall-KBxxx.vbs</u> sur notre site)

b) supprimer les dossiers et fichiers dans C:\WINDOWS\SoftwareDistribution\Download

c) supprimer les fichiers temporaires et historique de Internet Explorer

d) si le dossier i386 est sur C, déplacer le sur une partition qui a de l'espace libre

e) éventuellement, si après toutes les actions précédentes l'espace disque libre sur C reste inférieur à 1,5 Go, déplacer le fichier d'échange (nécessite un redémarrage)

#### 2) Vérifier qu'on dispose maintenant d'au moins 600 mo sur C et lancer un liveupdate

<u>"manuel" en passant par le bouclier de symantec 俗</u>

Tout doit alors rentrer dans l'ordre.

Pendant la mise à jour, l'espace disque libre baisse à nouveau mais quand tout est fini il remonte. C'est parfois long, être patient.

#### Après la mise à jour, redémarrer le serveur

Au redémarrage vérifier dans c:\program files\sav qu'il ne reste plus que 2 .xdb et .vdb maximum et aussi dans le sous dossier I2\_LDVP.VDB 2 dossiers .vdb et xdb maximum

Vérifier l'espace sur c (il a dû remonter un peu encore) et la date des définitions de virus.(elle doit être celle du jour, à 1 ou 2 jours près)

Dans l'observateur d'évènements, supprimer les erreurs et surveiller que celles évoquées dans ce document ne réapparaissent pas