

Code fichier : procedure\_alerte\_sav.doc

# Procédure d'alerte par mail en cas de virus détecté – AMS pour symantec antivirus 1.6.6010

## 1) Vérifier dans le menu démarrer si ams est installé



→ Après ces 2 vérifications, si AMS n'est pas disponible, l'installer – Pour cela, <u>télécharger ams.zip sur le</u> site assistance technique aux aiprt

[Installation  $\rightarrow$  cliquer sur setup.exe, suivant, j'accepte, suivant, serveur ams, suivant, installer, terminer, redémarrer  $\rightarrow$  oui]

#### 2) Configurer une alerte en cas de virus détecté

Démarrer, Programmes, Serveur Alert Management, Utilitaire AMS Admin (ou depuis la console symantec center)

Laisser coché "Serveur AMS local" et cliquer sur Configurer AMS

🍌 Utilitaire AMS Admin	
Sélection de serveur AMS Serveur AMS local Serveur AMS distant	<u>C</u> onfigurer AMS Afficher journal AMS Quitter
Sélection du produit Produit : Symantec AntiVirus Corporate Edition	

Développer « Symantec Antivirus Corporate Edition »

- M S	ymantec AntiVirus Corporate Edition	Fermer
	Alerte par défaut Démarrage/arrêt de Symantec AntiVirus	Configurer
	<ul> <li>Démarrage/arrêt d'une analyse</li> <li>Echec de réparation du risque</li> </ul>	<u>S</u> upprimer
- 1	Mise à jour du fichier de définitions de virus	⊻érifier l'action
	Modification de la configuration Risque réparé	<u>R</u> afraîchir
A	Virus détecté	Egporter
		Options
		Aide

Cliquer sur Virus détecté



puis sur Configurer

### Cliquer sur Envoi de courrier Internet, puis suivant

(•)) Diffusion		奏 Envoi d'avis de re	cherche de perso
Envoi de courrier Ir	nternet	Exécution d'un pr	ogramme
Boîte de dialogue d	des messages	Cette action envo	ie un piège SNMI
Charger up NLM	1		
E solt see a second sec	des événements		
Ecriture au journal	-		

Sélectionner le serveur qui gère l'antivirus sur le domaine

	Sélectionnez l'ordinateur responsable de l'action. Ordinateur responsable de l'action : Microsoft Windows Network Deptions Pdc-ep.carmi-ep.peda	]
j	< <u>P</u> récédent <u>S</u> uivant > Annuler Aide	

puis Suivant

Renseigner Adresses mail du destinataire (en principe celle de l'aiprt) et de l'expéditeur (en principe celle de l'aiprt), Objet et ip du serveur sortant donc 172.16.0.1 pour un slis

	Entrez les adresses internet du destinataire et de l'expéditeur, l'objet du message et l'adresse du serveur de messagerie SMTP de l'expéditeur.	
	albert.camus@ac-grenoble.fr 📃 💌	
	Adresse Internet de l'expéditeur :	
	albert.camus@ac-grenoble.fr 📃 💌	
	Objet :	
	alerte détection virus	
	Serveur de <u>m</u> essagerie SMTP :	
	172.16.0.1	
		_

puis Suivant

Renseigner le nom de l'action comme par exemple "détection virale"

et ajouter les paramètres "nom du virus", "action réellement effectuée" "utilisateur" et "chemin du fichier" en les passant de droite à gauche, à l'endroit désiré dans la liste

Entrée du contenu du message		×
Nom de l'action : détection virale		
Message d'alerte :	Para <u>m</u> ètres d'alerte :	
Alerte : <nom d'alerte=""> Ordinateur : <nom d'ordinateur=""> <chemin du="" fichier=""> Date : <date> Heure : <heure> Gravité : <gravité> Source : <source/> <utilisateur> <action effectuée="" réellement=""></action></utilisateur></gravité></heure></date></chemin></nom></nom>	Action réellement effec▲ Action requise Chemin du fichier Date Gravité Heure Nom d'alerte Nom de l'hôte Nom d'ordinateur	
Par <u>d</u> éfaut		
< <u>P</u> récédent	Ferminer Annuler Aide	

puis Terminer

# 2) en suivant la même procédure que précédemment, configurer deux autres alertes :- en cas de risque réparé- en cas d'échec de réparation du risque

Vous obtenez alors:

Symantec Anti¥irus Corporate Edition		×
Actions associées aux alertes :		
- 🦗 Symantec AntiVirus Corporate Edition	Fermer	
<ul> <li>Alerte par defaut</li> <li>Démarrage/arrêt de Symantec AntiVirus</li> </ul>	Co <u>n</u> figurer	
A Démarrage/arrêt d'une analyse A Echen de réparation du visque	<u>S</u> upprimer	
<ul> <li>Envoi de courrier Internet [echec réparation</li> </ul>	<u>V</u> érifier l'action	
<ul> <li>A Mise à jour du fichier de définitions de virus</li> <li>A Modification de la configuration</li> </ul>	<u>R</u> afraîchir	
A Risque réparé Envoi de courrier Internet (virus réparé) (S1	Exporter	
<ul> <li>Privoi de courrier internet (virus repare) (51</li> <li></li></ul>	Options	
🤯 Envoi de courrier Internet [détection virale i	Aide	

#### → Fermer

l'arraur ou pour modifier une action, comme par ex l'adresse de messagerie, il est p

En cas d'erreur ou pour modifier une action, comme par ex l'adresse de messagerie, il est possible de modifier cette alerte en cliquant dessus, puis configurer, etc....

Il est possible de créer d'autres alertes, par exemple pour vérifier la bonne mise à jour des définitions de virus, mais attention au nombre important de mails reçus...

Il est possible de tester le bon fonctionnement de l'alerte par messagerie en ouvrant « test-virus.zip » le sur le cd de maintenance 1.39 dans..:\CD-FIC\Test-Virus\

La personne déclarée comme destinataire reçoit un message dès que le virus est détecté et réparé

Il est également possible de faire un test en cliquant sur "vérifier l'action".