Introduction

Au cours des dernières années, l'essor des réseaux de communication, et particulièrement le développement spectaculaire d'Internet, ont eu pour effet d'étendre considérablement l'utilisation du courrier électronique.

Un des principaux avantages du courrier électronique est la possibilité d'envoyer et de recevoir des fichiers. Cet avantage fondamental constitue cependant une nouvelle voie d'accès mise à profit par les virus.

L'échange de documents via le courrier électronique est, à l'heure actuelle, une pratique très courante. Elle a en grande partie favorisé l'importante expansion des virus de Word et d'Excel. Il convient cependant de savoir qu'il est possible d'envoyer et de recevoir tout type de virus et non pas seulement ceux de Word et d'Excel.

Les anti-virus classiques ne sont pas en mesure d'assurer efficacement la détection et la désinfection des virus situés dans les messages de courrier électronique pour les raisons suivantes :

1. D'ordinaire, les messages de courrier électronique sont stockés dans une base de données de courrier sous un format propre à l'aide de techniques de compression et/ou de cryptage qui rendent impossible l'analyse des anti-virus classiques.

2. Il est très fréquent que les messages de courrier électronique et les fichiers qui y sont associés se trouvent sur un serveur auquel un anti-virus classique n'a pas accès.

Par conséquent, un anti-virus pour courrier électronique doit être spécialement conçu pour détecter et supprimer les virus affectant le courrier électronique. Ses principales caractéristiques doivent donc être les suivantes :

- Analyse, entièrement automatique, des messages au moment même de leur réception.
- Analyse automatique de chaque message lors de leur ouverture.
- Analyse automatique de chaque message allant être envoyé. Le risque d'envoyer des messages contaminés par des virus disparaît ainsi.
- Analyse automatique de chaque message enregistré.
- Analyse de tous les messages de courrier, à tout moment, sur demande de l'utilisateur.
- Intégration au programme de courrier électronique.
- Possibilité d'analyser des fichiers comprimés.
- Possibilité d'analyser des messages nichés (messages situés dans d'autres messages).

Panda Antivirus pour Exchange/Outlook est un anti-virus pour courrier électronique qui comprend toutes les caractéristiques décrites ainsi que de nombreuses autres. Il est ainsi doté d'une fonctionnalité complète et constitue un outil d'une grande puissance, et cependant extrêmement configurable, qui permet d'utiliser le courrier électronique sans aucun risque.

NOTE
Le présent manuel décrit les produits suivants :

- Panda Antivirus Exchange/Outlook

- Panda Antivirus Exchange/Outlook Network Client

Le premier produit permet d'installer directement Panda Antivirus Exchange/Outlook sur un ordinateur. Le deuxième produit permet de distribuer le même anti-virus sur toutes les stations d'un réseau, simplifiant ainsi la tâche du gestionnaire du réseau.

Reportez-vous à la rubrique du manuel correspondant au produit que vous avez acheté.

Installation

Conditions requises

Panda Antivirus Exchange/Outlook requiert les éléments suivants :

- Ordinateur compatible IBM capable d'exécuter Windows 95, 98 ou Windows NT Workstation 3.51 ou 4.0.
- MS-Exchange et/ou MS-Outlook
- 3 Mb d'espace sur le disque dur.

Installation

Pour installer Panda Antivirus Exchange/Outlook, vous devez introduire la disquette numéro 1 dans le lecteur correspondant puis exécuter le programme SETUP.EXE.

Le processus d'installation comprend une série de fenêtres où les différentes données nécessaires à l'installation vous sont sollicitées.

Une fois l'installation terminée, il est conseillé de redémarrer l'ordinateur. L'anti-virus pour Exchange/Outlook ne commence à fonctionner que quand Exchange/Outlook est à nouveau lancé.

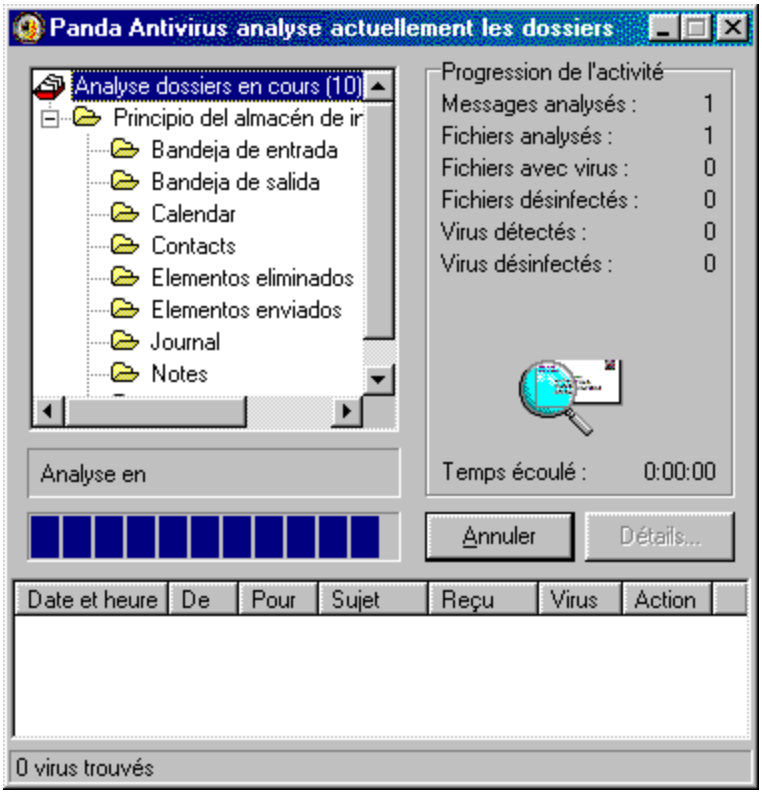
Désinstallation

Pour désinstaller Panda Antivirus Exchange/Outlook, vous devez fermer le programme de courrier Exchange/Outlook, vous rendre dans le *Panneau de Configuration*, choisir l'option *Ajout/suppression de programmes* puis choisir dans la liste Panda Antivirus Exchange/Outlook. Vous devez ensuite cliquer sur le bouton *Ajouter/Supprimer*. La désinstallation ne dure que quelques minutes. Il est fortement déconseillé d'effacer le dossier contenant la version pour désinstaller celle-ci. Il est impératif de suivre la procédure indiquée.

Comment analyser avec Panda Antivirus Exchange/Outlook

Analyse sur demande

Pour analyser un dossier afin d'y détecter des virus, sélectionnez-le d'abord. Si vous choisissez un dossier contenant d'autres dossiers (par exemple, une boîte aux lettres), tous ces dossiers sont analysés. Une fois le dossier choisi, cliquez sur le bouton Analyser situé dans la barre des boutons standard de MS-Exchange/Outlook ou sélectionnez l'option Analyser comprise dans l'option Outil du menu principal de MS-Exchange/Outlook. La fenêtre d'analyse suivante s'affiche alors :



Une fois l'analyse terminée, vous pouvez consulter le rapport des résultats décrivant en détail tout incident survenu au cours de l'analyse.

Panda Antivirus Exchange/Outlook permet également d'analyser un ou plusieurs messages. Sélectionnez le ou les messages que vous souhaitez analyser puis cliquez sur le bouton Analyser afin de lancer l'analyse.

Pour sélectionner plusieurs messages, cliquez dessus tout en maintenant enfoncée la touche Contrôle. Si vous souhaitez sélectionner un groupe de messages, sélectionnez le premier d'entre eux puis, tout en maintenant enfoncée la touche Maj., cliquez sur le dernier.

Protection en temps réel

La protection permanente vous permet d'utiliser en toute tranquillité votre courrier sans vous soucier des virus. En effet, Panda Antivirus Exchange/Outlook surveille toutes les opérations suspectes à votre place.

La protection permanente se charge d'analyser, afin d'y détecter des virus, les éléments suivants :

- Tous les nouveaux messages que vous recevez.
- Tous les messages que vous souhaitez envoyer.
- Tous les messages que vous ouvrez, qu'ils aient été reçus avant ou après l'installation de l'anti-virus.
- Tous les messages que vous souhaitez enregistrer.

Pour activer la protection permanente, il vous suffit de cliquer sur le bouton à cet effet, situé dans la barre des boutons standard de MS-Exchange/Outlook. Pour la désactiver, cliquez à nouveau sur le même bouton afin d'annuler sa sélection.

Panda Antivirus Exchange/Outlook étant en mesure d'analyser des fichiers comprimés et des messages nichés (messages situés dans d'autres messages) il assure ainsi une protection optimale.

Fonctionnement de Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook s'intègre totalement à MS-Exchange/Outlook. Par conséquent, l'anti-virus est entièrement géré depuis le programme de courrier lui-même.

Panda Antivirus Exchange/Outlook ajoute quatre boutons à la barre des boutons standard de MS-Exchange/Outlook. Ces quatre boutons sont les suivants :

Analyser : ce bouton lance l'analyse du dossier ou des messages préalablement sélectionnés à cet effet. Tous les sous-dossiers compris dans le dossier sont analysés. Une fenêtre permet de suivre la progression de la procédure d'analyse en affichant l'ensemble des dossiers qui vont être analysés, le dossier en cours d'analyse et une barre de progression.

Rapport des résultats : ce bouton affiche le rapport sur les incidents détectés par l'anti-virus. Ce rapport est maintenu d'une séance à l'autre jusqu'à ce que l'utilisateur décide de l'effacer.

Activer ou désactiver l'anti-virus : ce bouton permet d'activer ou de désactiver la protection permanente de Panda Antivirus. Si vous la désactivez, Panda Antivirus Exchange/Outlook n'analysera, afin d'y détecter des virus, ni les nouveaux messages que vous allez recevoir ou envoyer ni les messages que vous allez ouvrir pour les lire. Il analysera en revanche tout dossier ou message spécifique sélectionné que vous souhaitez analyser. L'analyse au démarrage de Exchange/Outlook sera effectuée même si vous avez annulé la protection permanente.

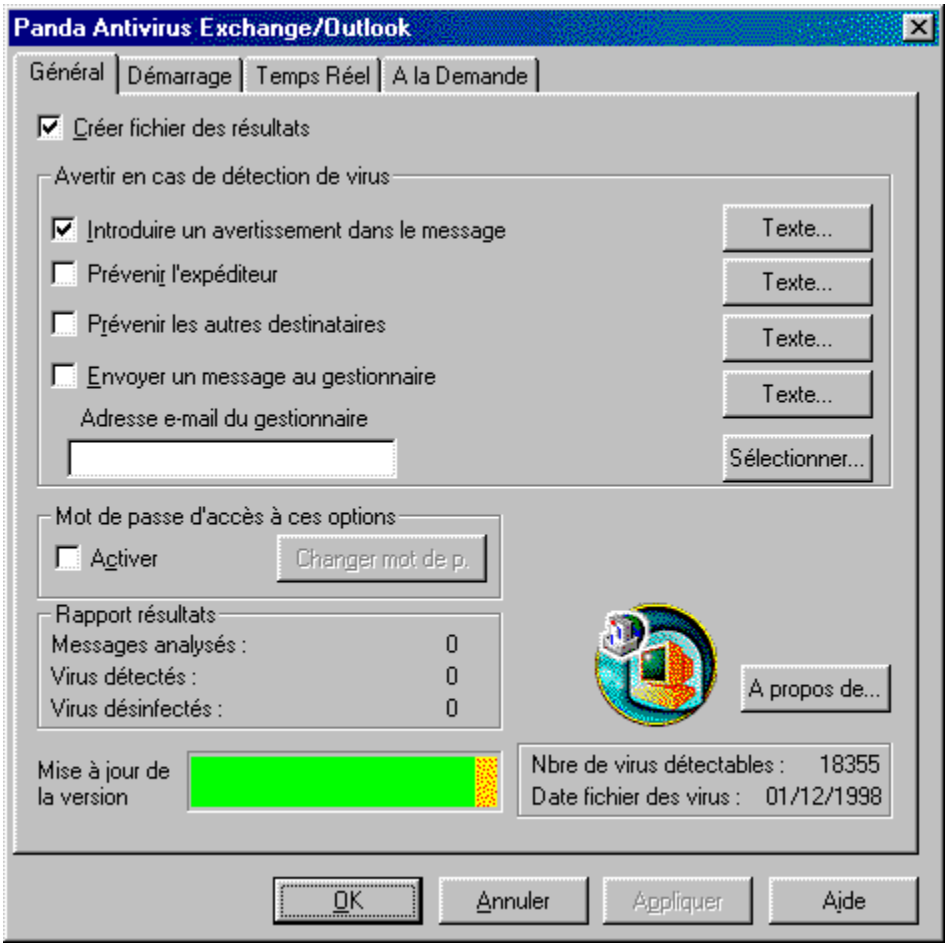
Configurer : ce bouton affiche la fenêtre de configuration de Panda Antivirus Exchange/Outlook. Elle vous permet de configurer le comportement général de l'anti-virus, son comportement au démarrage du programme de courrier ainsi que son comportement en tant que protection permanente et en tant que protection sur demande. Vous pouvez également accéder à la configuration de Panda Antivirus Exchange/Outlook en sélectionnant Options dans Outils au sein du menu principal de MS-Exchange/Outlook. La fenêtre d'options contient une page appelée Panda Antivirus Exchange/Outlook à l'aide de laquelle vous pouvez configurer l'anti-virus.

Configuration de Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook permet une grande souplesse de configuration pour chaque fonction. La fenêtre de configuration est divisée en plusieurs pages qui se réfèrent chacune à une partie spécifique de l'anti-virus.

Général

Les options regroupées sur cette page ont un caractère général et conditionnent en toutes circonstances le comportement de l'anti-virus. Il s'agit des options suivantes :



Créer fichier des résultats. Si vous sélectionnez cette option, toutes les opérations d'analyse de l'anti-virus consignent les différents incidents survenus dans un fichier des résultats.

Introduire un avertissement dans le message. Si vous sélectionnez cette option, chaque fois qu'un virus est détecté dans un message, un texte d'avertissement est ajouté dans celui-ci. Ce texte est ajouté quelle que soit l'action à entreprendre lors de la détection d'un virus. Il peut être personnalisé et chaque utilisateur peut donc choisir la formulation qui lui convient.

Prévenir l'expéditeur. Si vous sélectionnez cette option, chaque fois qu'un virus est détecté dans un message, une communication est envoyée à son expéditeur afin de l'informer de la contamination. Le texte de cette communication étant totalement configurable, il peut être personnalisé.

Prévenir les autres destinataires. Si vous sélectionnez cette option et qu'un virus est détecté dans un message, une communication est, le cas échéant, envoyée aux autres destinataires du message contaminé. Il est ainsi possible de prévenir les éventuels utilisateurs dépourvus d'une protection

contre les virus. Le texte de la communication en question peut être personnalisé.

Envoyer un message au gestionnaire. Si vous sélectionnez cette option et que vous indiquez l'adresse électronique du gestionnaire, chaque fois qu'un virus est détecté dans un message, un avertissement est envoyé au gestionnaire du système. Le texte de cet avertissement peut être totalement personnalisé.

Activer mot de passe. Si vous sélectionnez cette option, la configuration de Panda Antivirus Exchange/Outlook est protégée par un mot de passe. Vous évitez ainsi qu'un utilisateur non autorisé change la configuration de l'anti-virus.

Changer mot de passe. Ce bouton permet de changer le mot de passe protégeant la configuration de Panda Antivirus Exchange/Outlook.

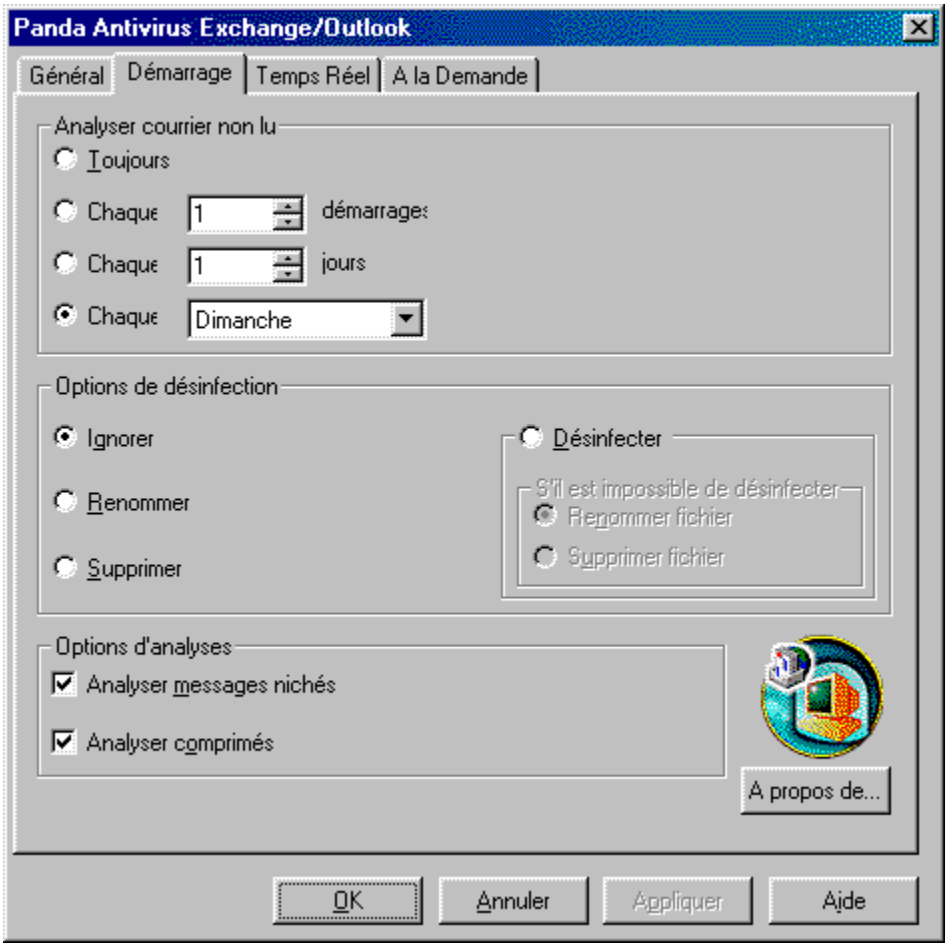
Rapport des résultats. Cette option affiche des informations indiquant le nombre de messages analysés, de virus détectés et de virus désinfectés.

Mise à jour de la version. Cette option indique graphiquement le niveau de mise à jour de l'anti-virus.

Infos sur la version. Le nombre des virus détectables et la date du fichier des virus vous renseignent sur la version de l'anti-virus installée.

Démarrage

Cette page permet de configurer le comportement de l'anti-virus lors du démarrage du programme de courrier électronique MS-Exchange/Outlook. Les options disponibles sont les suivantes :



Analyser toujours le courrier non lu. Si vous sélectionnez cette option, chaque fois que vous démarrez MS-Exchange/Outlook tous les messages non lus situés dans la boîte de réception sont analysés.

Analyser le courrier non lu tous les x démarrages. Si vous sélectionnez cette option, les messages non lus situés dans la boîte de réception sont analysés tous les x démarrages du programme de courrier conformément au chiffre que vous avez indiqué.

Analyser le courrier non lu tous les x jours. Si vous sélectionnez cette option, l'analyse des messages non lus de la boîte de réception n'est effectuée que tous les x jours conformément au chiffre que vous avez indiqué.

Analyser le courrier un jour spécifique. Si vous sélectionnez cette option, les messages non lus de la boîte de réception ne sont analysés, chaque semaine, que le jour que vous avez choisi.

Désinfection – **Ignorer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus n'effectue aucune action si ce n'est d'afficher une fenêtre signalant l'existence du virus.

Désinfection – **Renommer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus renomme le fichier contaminé par le virus.

Désinfection – **Supprimer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus supprime le fichier infecté.

Désinfection – **Désinfecter :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus tente de désinfecter le fichier infecté.

Désinfection – **S'il est impossible de désinfecter, renommer :** si l'anti-virus ne peut désinfecter un fichier contaminé, il le renomme.

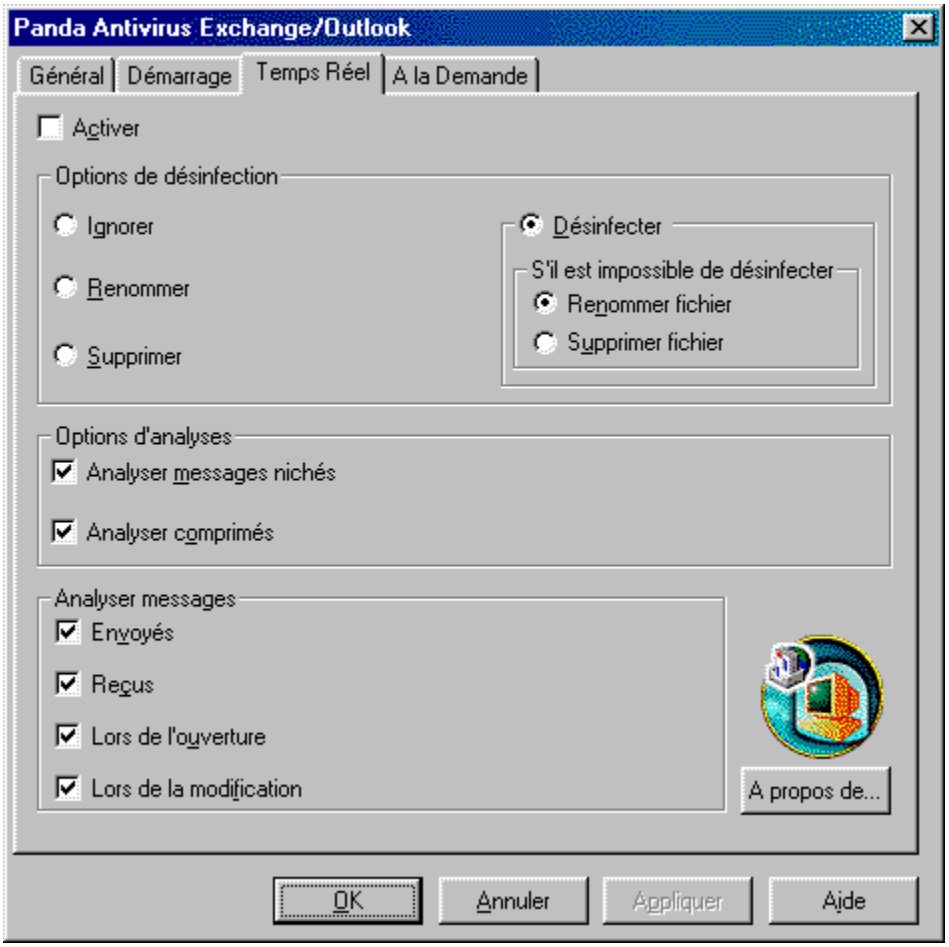
Désinfection – **S'il est impossible de désinfecter, supprimer :** si l'anti-virus ne peut désinfecter un fichier infecté, il le supprime.

Analyser messages nichés : si vous sélectionnez cette option, les messages nichés sont analysés. En d'autres termes, si un message est situé dans un autre message, tous deux sont analysés. Le nombre de couches de messages pouvant être analysé dépend des ressources de chaque ordinateur.

Analyser comprimés : si vous sélectionnez cette option et qu'il existe un fichier comprimé, celui-ci est analysé comme s'il s'agissait d'un fichier normal.

Temps réel

Cette page vous permet de configurer la protection permanente fournie par l'anti-virus. Les options disponibles sont les suivantes :



Activer : si vous activez cette option, vous activez la protection permanente. En d'autres termes, tous les messages que vous allez recevoir, envoyer, ouvrir ou enregistrer sont automatiquement analysés.

Désinfection – **Ignorer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus n'effectue aucune action si ce n'est d'afficher une fenêtre signalant l'existence du virus.

Désinfection – **Renommer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus renomme le fichier contaminé par le virus.

Désinfection – **Supprimer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus supprime le fichier infecté.

Désinfection – **Désinfecter :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus

tente de désinfecter le fichier infecté.

Désinfection – S'il est impossible de désinfecter, renommer : si l'anti-virus ne peut désinfecter un fichier contaminé, il le renomme.

Désinfection – S'il est impossible de désinfecter, supprimer : si l'anti-virus ne peut désinfecter un fichier infecté, il le supprime.

Analyser messages nichés : si vous sélectionnez cette option, les messages nichés sont analysés. En d'autres termes, si un message est situé dans autre message, tous deux sont analysés. Le nombre de couches de messages pouvant être analysé dépend des ressources de chaque ordinateur.

Analyser comprimés : si vous sélectionnez cette option et qu'il existe un fichier comprimé, celui-ci est analysé comme s'il s'agissait d'un fichier normal.

Analyser messages envoyés : si vous sélectionnez cette option, les messages que vous souhaitez envoyer sont analysés avant leur envoi. Vous évitez ainsi d'envoyer des fichiers contaminés.

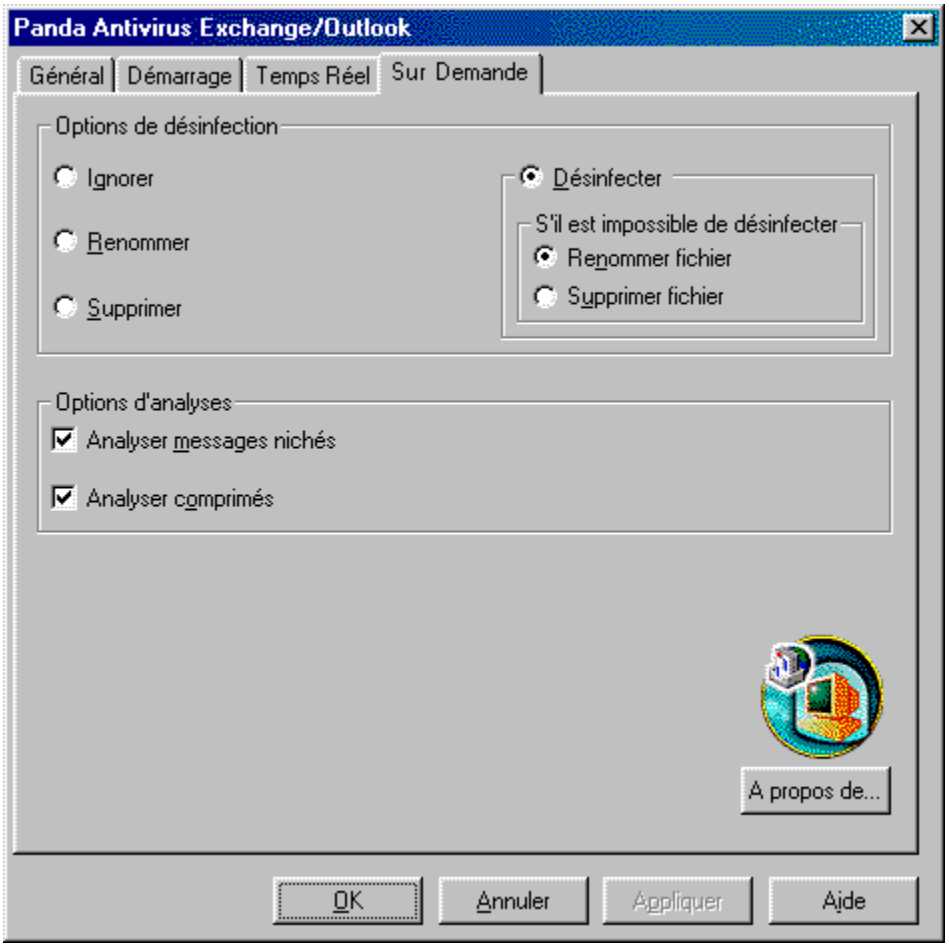
Analyser messages reçus : si vous sélectionnez cette option, tous les messages reçus sont analysés au moment même de leur réception avant qu'ils ne soient ouverts.

Analyser messages lors de l'ouverture : si vous sélectionnez cette option, tous les messages ouverts sont analysés quelle que soit la date de leur réception.

Analyser messages lors de la modification : si vous sélectionnez cette option, tous les messages enregistrés sont analysés.

Sur demande

Cette page vous permet de configurer l'analyse sur demande fournie par l'anti-virus. Les options disponibles sont les suivantes :



Désinfection – **Ignorer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus n'effectue aucune action si ce n'est d'afficher une fenêtre signalant l'existence du virus.

Désinfection – **Renommer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus renomme le fichier contaminé par le virus.

Désinfection – **Supprimer :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus supprime le fichier infecté.

Désinfection – **Désinfecter :** si vous sélectionnez cette option et qu'un virus est détecté, l'anti-virus tente de désinfecter le fichier infecté.

Désinfection – **S'il est impossible de désinfecter, renommer :** si l'anti-virus ne peut désinfecter un fichier contaminé, il le renomme.

Désinfection – S'il est impossible de désinfecter, supprimer : si l'anti-virus ne peut désinfecter un fichier infecté, il le supprime.

Analyser messages nichés : si vous sélectionnez cette option, les messages nichés sont analysés. En d'autres termes, si un message est situé dans un autre message, tous deux sont analysés. Le nombre de couches de messages pouvant être analysé dépend des ressources de chaque ordinateur.

Analyser comprimés : si vous sélectionnez cette option et qu'il existe un fichier comprimé, celui-ci est analysé comme s'il s'agissait d'un fichier normal.

Introduction à la distribution à travers un réseau

La distribution de l'anti-virus à travers un réseau répond au besoin de faciliter la tâche du gestionnaire de réseau souhaitant protéger, facilement et sans peine, un ensemble de postes.

Le principe est le suivant :

1. Le gestionnaire du réseau copie l'anti-virus sur un répertoire du serveur ou sur un répertoire partagé auquel tous les utilisateurs ont accès. Cette copie s'effectue à l'aide d'un programme d'installation conçu à cet effet. Il est important de savoir que vous n'installez PAS l'anti-virus sur le serveur mais que vous ne copiez que les fichiers nécessaires à l'installation de l'anti-virus sur les postes.

2. Chaque fois qu'un poste se connecte au réseau, le système s'assure que l'anti-virus y est bien installé et mis à jour. Si c'est le cas, aucune action n'est effectuée mais si l'anti-virus n'est pas installé ou mis à jour, l'installation ou la mise à jour ont lieu de façon totalement automatique.

Comme nous l'avons vu, le rôle du serveur (ou ressource partagée) consiste exclusivement à servir de moyen de distribution de l'anti-virus sur les stations.

Cette procédure générale peut être appliquée à l'ensemble des réseaux. Cependant, selon les types de réseaux, elle comprend de légères différences. Nous décrirons plus loin cette procédure pour les types de réseaux les plus courants à l'heure actuelle.

Comment distribuer l'anti-virus à travers un réseau

Conditions requises

La distribution de Panda Antivirus Exchange/Outlook à travers un réseau exige les éléments suivants :

- Ordinateur compatible IBM capable d'exécuter Windows 95, 98 ou Windows NT Workstation 3.51 ou 4.0.
- 3 Mb d'espace sur le disque dur du serveur allant être utilisé comme moyen de distribution.
- 3 Mb d'espace sur le disque dur de chaque ordinateur où l'anti-virus va être installé.

Comment distribuer facilement l'anti-virus sur tous les postes du réseau

Le processus de distribution de l'anti-virus sur tous les postes du réseau comprend deux étapes :

1. Copie de l'anti-virus sur un répertoire auquel tous les utilisateurs ont accès.

2. Distribution de l'anti-virus sur tous les postes se connectant au réseau à l'aide du programme RINSTALL.

Nous expliquons en détail ci-dessous comment effectuer les deux étapes mentionnées. Il est nécessaire d'avoir des connaissances sur le type de réseau sur lequel va être distribué l'anti-virus pour pouvoir suivre certains points de ce processus. Vous trouverez la description des connaissances concernant les principaux types de réseau dans les chapitres correspondants. N'hésitez pas à les consulter en cas de doute.

Copie de l'anti-virus sur un répertoire auquel tous les utilisateurs ont accès

Le premier pas à effectuer pour distribuer un anti-virus à travers le réseau consiste à copier des fichiers sur un répertoire dans l'un des disques durs du serveur. Il est très important de savoir que la copie des fichiers sur le serveur doit être réalisée dans un environnement libre de virus afin d'éviter de contaminer les fichiers de l'anti-virus. Ces fichiers allant être distribués sur toutes les stations se connectant au réseau, le virus peut se propager avec eux. Pour obtenir une copie des fichiers fiable et garantir que ces fichiers ne seront contaminés à l'avenir par aucune station, vous devez faire la copie en appliquant la démarche suivante :

1. Le gestionnaire doit s'assurer que l'ordinateur est libre de virus. Il doit donc y installer l'anti-virus de Panda Software adéquat et activer la protection permanente correspondante. Il doit en revanche éviter de poursuivre l'installation tant qu'il n'est pas certain que l'ordinateur à partir duquel il effectue l'installation est libre de virus.

2. Il doit ensuite choisir le répertoire du serveur correspondant où il va copier les fichiers. Il est conseillé de créer un nouveau répertoire et de l'appeler PAVEXCLI, pouvant être lu par tous les utilisateurs. En revanche, il est fondamental qu'aucun utilisateur ne soit autorisé à écrire sur ce répertoire ou à l'effacer. En effet, aucun utilisateur ne peut ainsi infecter ou effacer les fichiers de l'anti-virus par mégarde ou à propos et vous êtes à l'abri des graves conséquences que ces opérations peuvent entraîner.

3. Une fois le répertoire cible créé, il suffit d'insérer la disquette numéro 1 ou le CD-Rom, de se rendre dans l'unité correspondante puis d'exécuter le programme SETUP.EXE.

Au cours du processus d'installation le système affiche une série de fenêtres sollicitant les données requises pour effectuer l'installation sur l'ordinateur. Une de ces données concerne le répertoire cible. Il faut alors indiquer le répertoire créé à cet effet pour que les fichiers de l'anti-virus y soient copiés.

Distribution de l'anti-virus

Cette opération souligne particulièrement les performances de notre anti-virus pour les PC connectés à un réseau. En effet, il n'est pas nécessaire d'installer l'anti-virus sur chaque station puisqu'il est automatiquement installé dès qu'une station se connecte au réseau.

En général, quand une station se connecte à un réseau, une série de commandes ou de programmes sont exécutés afin de préparer le travail en réseau tout comme lorsqu'un ordinateur est mis en route. Cette série de commandes et/ou de programmes est appelée *Login Script* (ou script d'entrée).

Notre anti-virus à capacité de distribution à travers le réseau, est accompagné d'un programme appelé **RINSTALL** qui se charge de la distribution automatique de l'anti-virus. Par conséquent, il est aussi facile d'obtenir la distribution automatique de l'anti-virus que de situer l'exécution de **RINSTALL** dans le *Login Script*.

RINSTALL est exécuté chaque fois qu'une station se connecte au réseau. **RINSTALL** s'assure tout d'abord que l'anti-virus est installé sur la station connectée. S'il est installé et mis à jour, le programme n'effectue aucune action et l'exécution des autres commandes du *Login Script* a lieu normalement. Si l'anti-virus n'est pas installé sur la station ou qu'il n'est pas à jour, **RINSTALL** installe l'anti-virus et ce n'est qu'ensuite que l'exécution des autres commandes du *Login Script* a lieu normalement.

Le fonctionnement du programme **RINSTALL** étant totalement automatique, le gestionnaire du réseau n'a qu'à copier les fichiers et modifier le *Login Script* pour installer la protection anti-virus qui se propagera aux stations au fur et à mesure qu'elles se connectent.

Distribution de l'anti-virus sur un réseau Novell NetWare

Pour que l'anti-virus soit automatiquement distribué sur toutes les stations qui se connectent à un réseau Novell NetWare, il est indispensable de saisir la ligne suivante dans le *System Login Script* :

```
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Consultez la rubrique Novell NetWare afin d'obtenir une explication plus détaillée de ces points.

Comme vous pouvez le constater dans l'exemple, vous devez indiquer à quel endroit du serveur se trouvent les fichiers de l'anti-virus. Il convient par conséquent que cette ligne suive le mappage des unités. Cette partie du *System Login Script* se présente comme suit :

```
MAP ROOT F:=ALPHA\SYS:
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(dans l'hypothèse où le serveur est appelé Alpha et que les fichiers se trouvent sur le volume SYS).

Distribution de l'anti-virus sur un réseau Windows NT

Pour que l'anti-virus soit automatiquement distribué sur les stations du réseau au fur et à mesure

qu'elles s'y connectent, vous devez ajouter la ligne suivante au *Fichier des commandes du début des séances* à l'aide du programme Profile Manager:

Consultez la rubrique Windows NT pour obtenir une explication plus détaillée de ces points.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Comme vous pouvez le constater dans l'exemple, vous devez indiquer l'emplacement où ont été copiés les fichiers de l'anti-virus. Il convient par conséquent que cette ligne suive le mappage des ressources partagées. Cette partie du *Fichier des commandes du début des séances* se présente comme suit :

```
NET USE F: \\ALPHA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(dans l'hypothèse où le serveur est appelé Alpha et la ressource partagée Sys).

Distribution de l'anti-virus sur un réseau OS/2

Pour que l'anti-virus soit automatiquement distribué aux stations du réseau au fur et à mesure qu'elles s'y connectent, vous devez ajouter la ligne suivante au fichier PROFILE.BAT (ou PROFILE.CMD):

Consultez la rubrique OS/2 pour obtenir une explication plus détaillée de ces points.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Comme vous pouvez le constater dans l'exemple, vous devez indiquer l'emplacement où ont été copiés les fichiers de l'anti-virus. Il convient par conséquent que cette ligne *suive* le mappage des ressources partagées. Cette partie du fichier PROFILE.BAT se présente comme suit :

```
NET USE F: \\ALPHA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(dans l'hypothèse où le serveur est appelé Alpha et la ressource partagée Sys).

Distribution de l'anti-virus sur un réseau Pathworks

Pour que l'anti-virus soit automatiquement distribué sur les stations du réseau au fur et à mesure de leur connexion, vous devez ajouter la ligne suivante dans la séquence de connexion d'un groupe réunissant tous les utilisateurs que vous souhaitez doter de l'anti-virus :

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Comme vous pouvez le constater dans l'exemple, vous devez indiquer l'emplacement où ont été copiés les fichiers de l'anti-virus. Il convient donc de définir le mappage des unités avant d'exécuter RINSTALL.

Distribution de l'anti-virus sur un réseau Banyan-Vines

Pour que l'anti-virus soit automatiquement distribué sur les stations du réseau au fur et à mesure qu'elles s'y connectent, vous devez ajouter la ligne suivante dans le profil de chaque utilisateur dont

vous souhaitez protéger l'ordinateur. Le profil d'un utilisateur est la séquence d'ordres s'exécutant chaque fois que cet utilisateur se connecte au réseau.

Il suffit d'éditer ce profil à l'aide de l'instruction MUSER et d'ajouter la ligne suivante :

```
POSTLOGIN F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

si l'unité du serveur correspond à F et si les fichiers ont été copiés sur le répertoire **PAVEXCLI**.

Il convient de définir le mappage des unités avant d'exécuter **RINSTALL** afin de s'assurer que le disque dur du serveur correspond à la même référence sur toutes les stations.

Le fait de modifier l'un après l'autre tous les profils de l'utilisateur peut s'avérer être une tâche laborieuse si les utilisateurs sont nombreux. En général il existe un profil commun utilisé par tous les utilisateurs. Il est possible d'accéder à ce profil à partir des différents profils des utilisateurs à l'aide de la commande suivante :

```
USE Sample_Profile@groupe@organisation
```

Sample_Profile représente un utilisateur fictif et groupe et organisation se réfèrent à la structure de l'entreprise.

Il suffit ainsi d'effectuer les modifications adéquates sur le profil *Sample_Profile* pour qu'elles affectent tous les utilisateurs y accédant à partir de leur propre profil.

Installation de l'anti-virus sur un poste non connecté au réseau

Si vous souhaitez installer Panda Antivirus Exchange/Outlook sur un poste non connecté au réseau, vous devez appliquer la démarche ci-dessous :

1. Insérez la disquette numéro 1 ou le CD-Rom de Panda Antivirus Exchange/Outlook, rendez-vous sur l'unité correspondante puis exécutez le programme SETUP.EXE. Au cours du processus d'installation, le système affiche une série de fenêtres vous sollicitant les données requises pour effectuer l'installation sur l'ordinateur. Une des données concerne le répertoire cible. Vous devez alors choisir un répertoire de l'ordinateur lui-même et non pas du serveur comme indiqué précédemment.

2. Une fois le processus d'installation terminé, exécutez la commande suivante :

   ```
   C:\PAVEXCLI\RINSTALL PAVEX.SCR
   ```

   (indiquez l'unité ou le répertoire où vous avez installé l'anti-virus).

3. Une fois le processus de distribution terminé, le programme anti-virus pour MS-Exchange/Outlook est installé sur votre ordinateur.

4. Supprimez le répertoire où vous avez installé l'anti-virus au cours de l'étape 1. Il est désormais inutile.

Solution des problèmes de distribution

Si l'anti-virus n'est pas correctement distribué sur un ou plusieurs ordinateurs, vous devez y vérifier les aspects suivants :

1. Il est possible, depuis cet ordinateur, de se connecter au serveur où vous avez copié l'anti-virus.

2. Il est possible d'exécuter directement le programme **RINSTALL**. Situez-vous dans le répertoire du serveur où vous avez copié l'anti-virus puis exécutez **RINSTALL** PAVEX.SCR.

Si vous pouvez effectuer les deux opérations ci-dessus, vérifiez le script d'entrée en vous assurant que le script adéquat a été modifié et que la ligne correspond aux instructions données plus haut.

Caractéristiques avancées

Comment éviter que les utilisateurs modifient la configuration de Panda Antivirus Exchange/Outlook

Si vous souhaitez éviter que les utilisateurs qui vont être automatiquement dotés de Panda Antivirus Exchange/Outlook puissent altérer sa configuration, vous devez appliquer la procédure décrite ci-dessous :

1. Installez Panda Antivirus Exchange/Outlook sur l'ordinateur du gestionnaire du réseau.

2. Ouvrez le programme de courrier MS-Exchange/Outlook et configurez l'anti-virus à votre guise.

3. Protégez la configuration avec un mot de passe. Cette opération s'effectue dans la fenêtre de configuration de l'anti-virus.

4. Copiez le fichier PAVEXCLI.CFG, situé dans le répertoire WINDOWS\SYSTEM de l'ordinateur du gestionnaire, dans le répertoire du réseau à partir duquel l'anti-virus va être distribué.

5. Modifiez le *login script* afin de lancer la distribution de l'anti-virus sur tous les postes du réseau.

Il est important de savoir que la procédure décrite ci-dessus doit être réalisée avant de lancer la distribution de l'anti-virus à travers le réseau.

Connaissances nécessaires sur Novell NetWare

La distribution de l'anti-virus à travers un réseau Novell NetWare requiert une connaissance minimum de ce système. Nous allons ci-dessous décrire les notions que vous devez connaître et les illustrer à l'aide d'exemples sur la préparation adéquate du système.

Commandes exécutées au début d'une séance sur le réseau

Lors du démarrage d'un ordinateur, il est normal qu'une série de commandes définies dans un fichier soit exécutée. Sous MS-DOS ou Windows, ce fichier est AUTOEXEC.BAT.

Il est également normal que, lorsqu'un ordinateur se connecte à un réseau, une série de commandes soit exécutée. Cette série de commandes et/ou de programmes est connue sous le nom de *login script* ou script d'entrée.

Le *login script* peut être général (un seul script pour tous les utilisateurs) ou particulier (un script pour chaque utilisateur). Il existe également une solution mixte comprenant un script d'entrée général commun à tous les utilisateurs et un script d'entrée particulier pour chaque utilisateur.

Le *login script* étant exécuté chaque fois qu'un utilisateur se connecte au réseau, il constitue l'endroit idéal pour distribuer l'anti-virus sur les postes. Il suffit d'exécuter le programme de distribution d'anti-virus de Panda Software dans le *login script* pour que l'anti-virus soit distribué sur tous les postes au fur et à mesure qu'ils se connectent au réseau.

System Login Script

Dans le cas de Novell NetWare, le script d'entrée général commun à tous les utilisateurs est connu sous le nom de *System Login Script*. Vous devez éditer ce fichier pour y ajouter l'exécution du programme de distribution de l'anti-virus de Panda Software. Pour éditer le *System Login Script* vous devez effectuer la démarche suivante :

1. Si vous disposez d'une version Novell NetWare 3.x vous devez utiliser le programme SYSCON. Si vous disposez d'une version Novell NetWare 4.x vous devez utiliser le programme NETADMIN. Tous les serveurs Novell NetWare comprennent un volume appelé SYS qui contient à son tour un répertoire PUBLIC. Les deux programmes cités (SYSCON et NETADMIN) se trouvent dans ce répertoire.

2. Pour éditer le *System Login Script* à l'aide du programme SYSCON, vous devez exécuter le programme, sélectionner l'option *Supervisor Options* puis l'option *System Login Script*.

3. Pour éditer le *System Login Script* à l'aide du programme NETADMIN, vous devez exécuter le programme et sélectionner les deux points (..) situés dans l'encadré de gauche jusqu'à ce que l'option cesse d'apparaître. Une seule option est dès lors affichée (elle est décrite sur la droite comme une *organisation*). Vous devez ensuite sélectionner cette option unique puis enfoncer la touche F10. Sélectionnez, dans le menu s'affichant alors, l'option *Afficher ou éditer propriétés de l'objet* puis, dans le menu apparaissant ensuite, l'option *Script d'entrée*. Vous pouvez dès lors modifier le *System Login Script*.

Vous devez introduire deux lignes dans le *System Login Script* : la première concerne le *mappage* (cette notion est expliquée dans la rubrique ci-dessous) et la deuxième se réfère à la distribution automatique de l'anti-virus.

Association de la lettre d'une unité

Nous allons, dans cette rubrique, expliquer la notion de *mappage*. Dans un ordinateur, le disque dur est généralement identifié avec la lettre C, le lecteur de disquettes avec la lettre A ou B et le lecteur de CD-Rom avec un D, un E, etc. en fonction des disques durs installés.

Les volumes ("disques durs") du serveur Novell NetWare doivent également être identifiés avec la lettre d'une unité pour pouvoir ainsi, à partir des stations, faire référence sans aucun problème à des répertoires et à des fichiers situés dans ces volumes. L'opération consistant à associer la lettre d'une unité à un volume est appelée *mappage*.

Il convient que toutes les stations aient le même *mappage* afin d'être certain que, dans tous les cas, les différents volumes du serveur répondent à une même référence. Il suffit pour cela de placer l'ordre de mappage dans le *System Login Script*. Généralement, le nom des volumes commence à partir du F, mais il est possible d'utiliser toute autre lettre d'unité n'étant pas utilisée. L'ordre de mappage se présente donc comme suit :

```
MAP ROOT F:=NOM_SERVEUR\NOM_VOLUME
```

Si le nom du serveur est ALPHA et celui du volume SYS, l'ordre est le suivant :

```
MAP ROOT F:=ALPHA\SYS:
```

Connaissances nécessaires sur Windows NT

La distribution de l'anti-virus à travers un réseau Windows NT requiert une connaissance minimum de ce système. Nous allons ci-dessous décrire les notions que vous devez connaître et les illustrer à l'aide d'exemples sur la préparation adéquate du système.

Commandes exécutées au début d'une séance sur le réseau

Lors du démarrage d'un ordinateur, il est normal qu'une série de commandes définies dans un fichier soit exécutée. Sous MS-DOS ou Windows, ce fichier est AUTOEXEC.BAT.

Il est également normal que, lorsqu'un ordinateur se connecte à un réseau, une série de commandes soit exécutée. Cette série de commandes et/ou de programmes est connue sous le nom de *login script* ou script d'entrée. Sous Windows NT on parle de *Fichier de commandes du début des séances*.

Sous Windows NT, chaque utilisateur a son fichier propre de commandes du début des séances. Il faut donc, en principe, modifier les fichiers de commandes du début des séances des ordinateurs de tous les utilisateurs où l'anti-virus va être distribué. Afin d'éviter cette tâche fastidieuse, Panda Software a conçu un utilitaire appelé Profile Manager dont nous expliquons ci-dessous le fonctionnement.

Le fichier des commandes du début des séances étant exécuté chaque fois qu'un utilisateur se connecte au réseau, il constitue l'endroit idéal pour distribuer l'anti-virus sur les postes. Il suffit d'exécuter le programme de distribution d'anti-virus de Panda Software dans le fichier des commandes du début des séances pour que l'anti-virus soit distribué sur tous les postes au fur et à mesure qu'ils se connectent au réseau.

Fichiers des commandes du début de séance - Profile Manager

Pour installer le programme Profile Manager permettant de modifier simultanément tous les fichiers des commandes du début des séances, vous devez insérer le disque portant l'étiquette *Editeur des commandes de début pour Windows NT* ou vous rendre dans le répertoire correspondant du CD-Rom puis exécuter le programme **SETUP.EXE**. Par exemple :

```
A:\SETUP
```

Effectuez ensuite la démarche suivante :

1. Exécutez le programme.
2. Sélectionnez le mode simplifié.
3. Sélectionnez *Editer commandes du début du domaine* dans le menu Fichier.
4. Un éditeur de texte s'affiche dans la partie inférieure de la fenêtre. Vous devez effectuer les modifications nécessaires, qui vont affecter tous les fichiers des commandes du début des séances, dans cet éditeur de texte.
5. Quittez le programme en enregistrant les modifications.

Vous devez introduire, dans le *Fichier des commandes du début des séances,* deux lignes: La première se réfère au *mappage* (cette notion est expliquée dans la rubrique ci-dessous) et la deuxième à la distribution automatique de l'anti-virus.

Association de la lettre d'une unité

Nous allons, dans cette rubrique, expliquer la notion de *mappage*. Dans un ordinateur, le disque dur est généralement identifié avec la lettre C, le lecteur de disquettes avec la lettre A ou B et le lecteur de CD-Rom avec un D, un E, etc. en fonction des disques durs installés.

Dans un réseau Windows NT, la notion de *mappage* est liée à celle de *ressource partagée*. La totalité ou toute partie du disque dur du serveur (ou des disques si vous en avez plusieurs) peut être partagée et devenir ainsi une *ressource partagée*. Vous devez effectuer le mappage de ces ressources partagées afin de pouvoir y faire référence à partir des stations.

Il convient que toutes les stations aient le même *mappage* afin d'être certain que, dans tous les cas, les différentes ressources partagées du serveur répondent à une même référence. Il suffit pour cela de placer l'ordre de mappage dans le *Fichier des commandes du début des séances*. Généralement, le nom des ressources partagées commence à partir du F, mais il est possible d'utiliser toute autre lettre d'unité n'étant pas utilisée. L'ordre de mappage se présente donc comme suit :

```
NET USE  F: \\NOM_SERV\NOM_RESSOURCE
```

Si le nom du serveur est ALPHA et celui de la ressource partagée SYS, l'ordre est le suivant :

```
NET USE F: \\ALPHA\SYS
```

Connaissances nécessaires sur OS/2

La distribution de l'anti-virus à travers un réseau OS/2 requiert une connaissance minimum de ce système. Nous allons ci-dessous décrire les notions que vous devez connaître et les illustrer à l'aide d'exemples sur la préparation adéquate du système.

Commandes exécutées au début d'une séance sur le réseau

Lors du démarrage d'un ordinateur, il est normal qu'une série de commandes définies dans un fichier soit exécutée. Sous MS-DOS ou Windows, ce fichier est AUTOEXEC.BAT.

Il est également normal que, lorsqu'un ordinateur se connecte à un réseau, une série de commandes soit exécutée. Cette série de commandes et/ou de programmes est connue sous le nom de *login script* ou script d'entrée. Sous OS/2, chaque utilisateur a un fichier appelé PROFILE.BAT (ou PROFILE.CMD) exécuté chaque fois que l'utilisateur se connecte au réseau.

Chaque utilisateur ayant son propre fichier des commandes du début des séances, il est nécessaire de modifier le fichier PROFILE.BAT situé dans chaque ordinateur allant participer à la distribution. L'inconvénient est que les futures modifications impliquent également l'édition de tous les fichiers PROFILE.BAT. Il est possible d'éviter ce désagrément en créant un fichier BAT contenant les lignes nécessaires à la distribution de l'anti-virus et en accédant à ce fichier à partir des fichiers PROFILE.BAT correspondants. Il suffit ainsi d'effectuer toute modification future sur le fichier BAT créé pour qu'elle affecte tous les utilisateurs.

Le script d'entrée étant exécuté chaque fois qu'un utilisateur se connecte au réseau, il constitue l'endroit idéal pour distribuer l'anti-virus sur les postes. Il suffit d'exécuter le programme de distribution d'anti-virus de Panda Software dans le script d'entrée pour que l'anti-virus soit distribué sur tous les postes au fur et à mesure qu'ils se connectent au réseau.

Association de la lettre d'une unité

Nous allons, dans cette rubrique, expliquer la notion de *mappage*. Dans un ordinateur, le disque dur est généralement identifié avec la lettre C, le lecteur de disquettes avec la lettre A ou B et le lecteur de CD-Rom avec un D, un E, etc. en fonction des disques durs installés.

Dans un réseau OS/2, la notion de *mappage* est liée à celle de *ressource partagée*. La totalité ou toute partie du disque dur du serveur (o des disques si vous en avez plusieurs) peut être partagée et devenir ainsi une *ressource partagée*. Vous devez effectuer le mappage de ces ressources partagées afin de pouvoir y faire référence à partir des stations.

Il convient que toutes les stations aient le même *mappage* afin d'être certain que, dans tous les cas, les différentes ressources partagées du serveur répondent à une même référence. Il suffit pour cela de placer l'ordre de mappage dans le fichier PROFILE de chaque utilisateur. Généralement, le nom des ressources partagées commence à partir de la lettre F, mais il est possible d'utiliser toute autre lettre d'unité n'étant pas utilisée. L'ordre de mappage se présente donc comme suit :

```
NET USE  F: \\NOM_SERV\NOM_RESSOURCE
```

Si le nom du serveur est ALPHA et celui de la ressource partagée SYS, l'ordre est le suivant :

```
NET USE F: \\ALPHA\SYS
```

Syntaxe des commandes des scripts (.SRC)

Vous avez sans doute constaté tout au long du présent document qu'un paramètre est toujours glissé dans le programme **RINSTALL**. Ce paramètre est le nom d'un fichier à l'extension SCR (fichiers de script). Un fichier de script est un fichier de texte divisé en sections où chaque ligne contient une commande. Le fichier de script détermine le comportement du programme **RINSTALL**.

Les fichiers SCR appropriés pour **RINSTALL** peuvent avoir 6 sections différentes :

Section commune **[COMMON]** : ces instructions sont toujours exécutées.

Section DOS **[DOS]** : les instructions de cette section sont exécutées sous DOS, Windows 3.1x et Windows 95.

Section Windows 3.1x **[WIN]** : les instructions de cette section sont exécutées sous DOS, Windows 3.1x et Windows 95 à condition de localiser le répertoire de Windows 3.1x dans le disque dur de la station de travail.

Section Windows 95 **[WIN95]** : les instructions de cette section sont exécutées sous DOS, Windows 3.1x et Windows 95 à condition de localiser le répertoire de Windows 95 dans le disque dur de la station de travail.

Section Windows NT **[WINNT]** : les instructions de cette section ne sont exécutées que sous Windows NT.

Section OS/2 **[OS/2]** : les instructions de cette section ne sont exécutées que sous OS/2.

Il existe trois types d'instructions :

1. **Fichiers à copier :** toutes les lignes NE commençant pas par le caractère #, indique un fichier qui devra être présent dans le répertoire source et qui devra être copié sur le répertoire cible. Par défaut, les fichiers ne sont copiés que s'ils n'existent pas sur le répertoire cible ou si le fichier présent sur le répertoire cible est plus ancien que celui se trouvant sur le répertoire source.

2. **Attributions :** ces instructions commencent par le caractère # et ont la structure suivante : #Variable = valeur. Elles sont utilisées pour attribuer une certaine valeur à une variable. Nous allons maintenant décrire en détail les différentes variables disponibles dans les fichiers de script (SCR).

Nom de variable	**Description**
Win3xDir	Répertoire de Windows 3.1x
Win95Dir	Répertoire de Windows 95
WinNTDir	Répertoire de Windows NT
BaseSourcePath	Répertorie source base

BaseTargetPath	Répertoire cible base
RelSourcePath	Répertoire source relatif
RelTargetPath	Répertoire cible relatif
SourcePath	BaseSourcePath + RelSourcePath
TargetPath	BaseTargetPath + RelTargetPath

CopyMode	Indique les conditions pour copier les fichiers. Peut présenter trois valeurs. COPY indique que les fichiers ne sont copiés que s'ils n'existent pas sur le répertoire cible. UPDATE indique que les fichiers ne sont copiés que si la version à copier est plus récente que celle du répertoire cible. OVERWRITE indique que les fichiers sont toujours copiés.
ErrorMode	Indique si les messages d'erreur doivent ou pas être affichés. Vous pouvez lui attribuer la valeur 0 (les messages ne sont pas affichés) ou la valeur 1 (les messages sont affichés).

3. **Fonctions :** ces instructions commencent également par le caractère #, et sont utilisées pour effectuer des opérations spécifiques. Leur syntaxe est la suivante : #Fonction paramètre1, paramètre2, ... Las différentes fonctions disponibles sont :

AddProfileEntry

Cette fonction ajoute une entrée à une section d'un fichier de type INI. Elle présente 4 paramètres :

Paramètre 1 :	indique la section où l'entrée doit être créée.
Paramètre 2 :	indique le champ (1ère partie de l'entrée).
Paramètre 3 :	indique la valeur (2ème partie de l'entrée).
Paramètre 4 :	indique le chemin menant au fichier INI.

Exemple :

```
#AddProfileEntry Windows, Load,
f:\pavfn\winkir.exe, c:\windows\win.ini
```

AppendLine

Cette fonction ajoute une ligne à un fichier de texte. Elle présente 3 paramètres :

Paramètre 1 :	indique le chemin menant au fichier de texte.
Paramètre 2 :	indique la ligne de texte à ajouter.
Paramètre 3 :	LITTERAL (facultatif). Si vous utilisez ce paramètre, vous avez la certitude que la ligne de texte correspond exactement à celle que vous avez écrite et que toute modification éventuelle a été supprimée.

Exemple :

```
#AppendLine c:\autoexec.bat,
```

```
c:\pavfn\sentinel.com
```

AppendLineBefore
Cette fonction ajoute une ligne à un fichier de texte et ajoute toujours avant une ligne spécifiée. Elle présente 4 paramètres :

Paramètre 1 : indique le chemin menant au fichier de texte.
Paramètre 2 : indique la ligne de texte à ajouter.
Paramètre 3 : indique la ligne de texte suivant celle qui est insérée.
Paramètre 4 : LITTERAL (facultatif). Si vous utilisez ce paramètre, vous avez la certitude que la ligne de texte correspond exactement à celle que vous avez écrite et que toute modification éventuelle a été supprimée.

Exemple :

```
#AppendLineBefore c:\autoexec.bat,
c:\pavfn\sentinel.com, win, LITTERAL
```

DeleteLine
Cette fonction sert à effacer une ligne d'un fichier de texte. Elle présente 2 paramètres :

Paramètre 1 : indique le chemin menant au fichier de texte.
Paramètre 2 : indique la ligne de texte à effacer.

Exemple :

```
#DeleteLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

InsertLine
Cette fonction sert à insérer une ligne au début d'un fichier de texte. Elle présente 3 paramètres :

Paramètre 1 : indique le chemin menant au fichier de texte.
Paramètre 2 : indique la ligne de texte à insérer.
Paramètre 3 : LITTERAL (facultatif). Si vous utilisez ce paramètre, vous avez la certitude que la ligne de texte correspond exactement à celle que vous avez écrite et que toute modification éventuelle a été supprimée.

Exemple :

```
#InsertLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

MakeDir
Cette fonction crée un répertoire. Elle présente un paramètre :

Paramètre 1 : indique le chemin menant au répertoire à créer.

Exemple :

```
#MakeDir c:\pavfn
```

NoWinLoad
Le fichier WIN.INI comprend une section [Windows] ayant une entrée appelée Load. Cette commande sert à charger une série de programmes lors de l'ouverture de Windows. Il peut y avoir plus d'un programme dans une même commande Load. L'instruction NoWinLoad supprime le programme souhaité de la commande Load. Elle présente un paramètre :

Paramètre 1 : indique le programme ne devant pas être chargé.

Exemple :

```
#NoWinLoad c:\pavfn\winkir.exe
```

ReplaceLine
Cette fonction remplace une ligne d'un fichier de texte. Elle présente 3 paramètres :

Paramètre 1 : indique le chemin menant au fichier de texte.
Paramètre 2 : indique la ligne de texte à remplacer.
Paramètre 3 : indique la nouvelle ligne de texte.

Exemple :

```
#ReplaceLine c:\autoexec.bat,
«TargetPath»SENTINEL.COM,
«TargetPath»SENTINEL.COM /OE
```

SetProfileEntry
Cette fonction attribue une valeur à une entrée dans une section donnée d'un fichier INI. La fonction tente de trouver cette section. Si elle réussit, elle lui attribue la valeur. Dans le cas contraire, elle crée l'entrée et lui attribue la valeur. Si la section n'existe pas, elle est également créée. La fonction présente 4 paramètres :

Paramètre 1 : indique la section du fichier INI
Paramètre 2 : indique le champ (1ère partie de l'entrée)
Paramètre 3 : indique la valeur (2ème partie de l'entrée)
Paramètre 4 : indique le chemin menant au fichier INI.

Exemple :

```
#SetProfileEntry Windows, Load,
c:\pavfn\winkir.exe, c:\windows\win.ini
```

WinLoad
Le fichier WIN.INI comprend une section [Windows] ayant une entrée appelée Load. Cette commande a pour effet de charger une série de programme lors de l'ouverture de Windows. Il peut y

avoir plus d'un programme dans une même commande Load. L'instruction WinLoad ajoute le programme souhaité à la commande Load. La fonction présente un paramètre :

Paramètre 1 : indique le programme devant être chargé.

Exemple :

```
#WinLoad c:\pavfn\winkir.exe
```